Global Information Assurance Certification Paper

GCIA

Practical Assignment
Version 4.0

Write an Intrusion Report

Security Audit Report

Lin Han

November 18, 2004

Table of Contents

Executive Summary

The purpose of this security audit report is to provide a clear view of the overall security health of the University network.

In the report we analyze one-day intrusion detection system logs provided by the University. The data was obtained on November 18, 2003, spanning 1 hour and 19 minutes.

Findings

There are 55 different detects captured with around 27 thousand hits in total. Among these, scan activity is listed as top one. This is usually the reconnaissance of further attacks.

Our analysis on the three most critical intrusion attempts demonstrates that

- Some file transfer servers are under attacker's complete control;
- System password files are exposed;
- Possibly confidential information is read and modified intentionally and unauthorizedly.

Observations and Recommendations

As a permissive environment, the current security status of the University network is basically acceptable. However, our analysis does show some areas need to be improved. For instance, out-of-date operating systems are still being used; applications do not have required patches installed.

The following defensive recommendations should be considered seriously.

- Conduct vulnerability assessment periodically against the University network;
- Develop a strong patch management process and procedure to keep systems up-to-date;
- Introduce a (stateful) firewall/packet filter to each subnet;
- Enhance password policy. Use strong passwords;
- Investigate and cleanup the compromised systems;
- If possible, install a host-based intrusion detection system on the system where confidential information is stored;
- Raise user awareness of security.

Detailed Analysis

Our analysis is based on the following files contained in an archived file named *2003.12.15.tgz*[1].

[1] Available at http://isc.sans.org/logs/Raw/ (October 3, 2004).

Name	Size	Modified
2003.12.15.1	3,000,033	12/15/2003 10:10p
2003.12.15.2	3,000,058	12/15/2003 10:10p
2003.12.15.3	3,000,036	12/15/2003 10:10p
2003.12.15.4	3,000,017	12/15/2003 10:10p
2003.12.15.5	3,000,006	12/15/2003 10:10p
2003.12.15.6	3,000,044	12/15/2003 10:10p
2003.12.15.7	3,000,026	12/15/2003 10:10p
2003.12.15.8	3,000,004	12/15/2003 10:10p
2003.12.15.9	3,000,003	12/15/2003 10:10p
2003.12.15.10	3,000,026	12/15/2003 10:10p
2003.12.15.11	3,000,020	12/15/2003 10:10p
2003.12.15.12	3,000,051	12/15/2003 10:10p
2003.12.15.13	3,000,055	12/15/2003 10:10p
2003.12.15.14	59,954	12/15/2003 10:11p

All the files were generated by Snort intrusion detection systems at the time between 14:57:23 and 16:15:58 on November 18, 2003.

1. Data Relationship

According to the nature of Snort output files, we can use WinDump (version 3.6.2) to interpret the acquired data. After running the following command, we extract all the traffic flowing on the networks.

```
C:\GCIA\Practical\Data\2003.12.15>for /L %i in (1,1,14) do windump -r 2003.12.15.%i -n >> ./log/Traffic.txt
```

Basically we capture 449,144 packets, which can be categorized into six types (see Table 1). 56 source IP addresses and 1,581 destination IP addresses are found associated with these packets (refer to Appendix 1 for the details).

Protocol	# of Packet	Protocol	# of Packet
TCP	375778	IGMP	29
UDP	63343	IP-Proto-63	1
ICMP	9992	EGP	1

Table 1 Network Traffic

Most of the source and destination IP addresses fall into three internal IP address ranges, 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16, as listed in Table 2.

Source	Source	Destination	Destination
10.10.10.0/24	192.168.17.0/24	10.3.200.0/24	172.22.201.0/24
10.30.30.0/24	192.168.22.0/24	10.10.10.0/24	172.27.1.0/24
172.16.8.0/24	192.168.84.0/24	172.20.11.0/24	192.168.17.0/24
172.16.9.0/24	192.168.117.0/24	172.20.12.0/24	192.168.22.0/24
172.20.11.0/24	192.168.213.0/24	172.20.102.0/24	
172.20.201.0/24	192.168.222.0/24	172.20.201.0/24	

Table 2 Source and Destination Subnets

A network topology can then be derived from the knowledge of these source and destination IP addresses. A border router in the subnets 10.0.0.0/8 and 172.16.0.0/12 is 10.10.10.141 and 172.20.11.2, respectively (This is concluded from the EGP packet in the log).

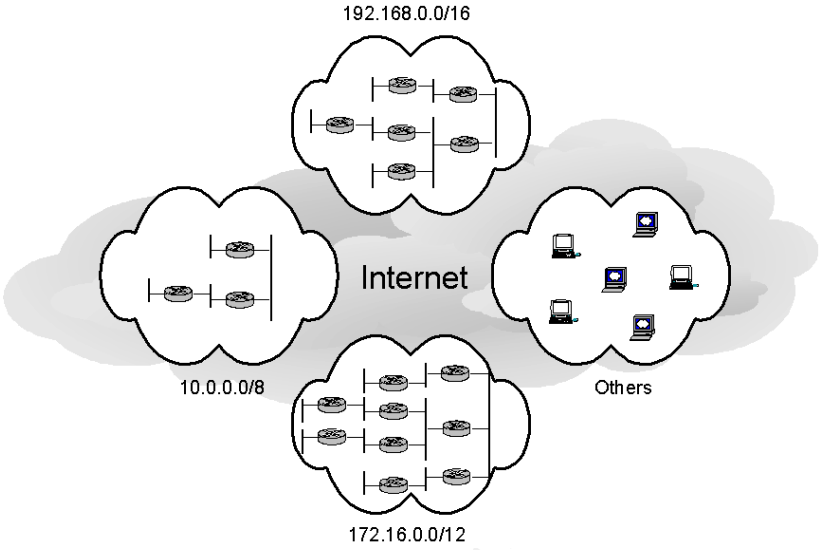

Figure 1 Network Topology

To demonstrate a relationship between different hosts and/or attacks, which is not readily apparent from looking at the log traces themselves, we choose some captured data and present the corresponding relationship in the following link graph (refer to Appendix 2 for the details).

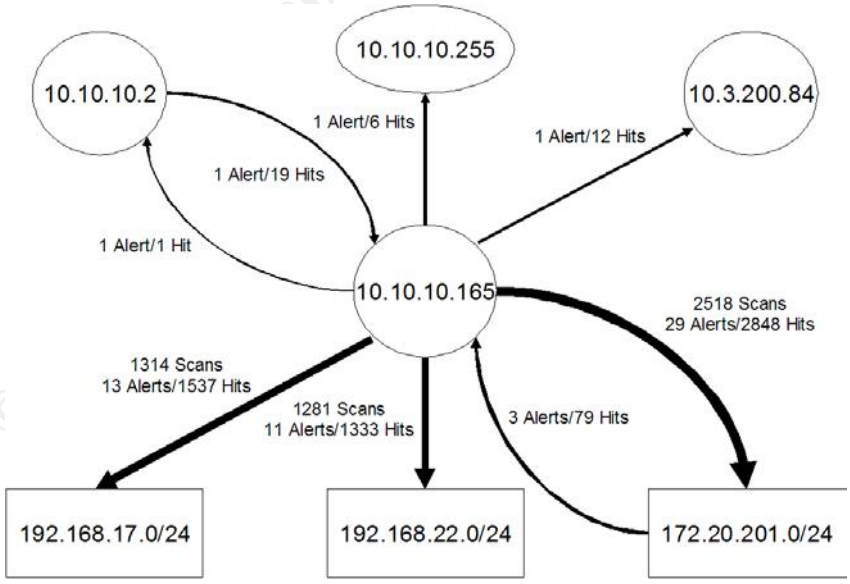

Figure 2 Link Graph

Besides the links (vectors) between the hosts (nodes), we can see from the link graph that host 10.10.10.165 is an attacking center, which could be a

compromised computer controlled by attackers. This host is mainly interested in three internal subnets, 172.20.201.0/24, 192.168.17.0/24 and 192.168.22.0/24.

2. Detect Overview

Running Snort version 2.2.0 with the rule set 2.2 against data files *2003.12.15.1* through *2003.12.15.14*, we obtain all alerts generated.

```
C:\GCIA\Practical\Data\2003.12.15>for /L %i in (1,1,14) do snort -d -y -c C:\Snort\rules\snort.conf -r 2003.12.15.%i -l ./log
```

After further processing under Cygwin environment,

```
$ cat alert.ids | grep '\[\*\*\]' | sed 's/ \[\*\*\]//g' | sed 's/\[\*\*\] //g' | sed 's/\] /\]\t/g' | sort | uniq -c > Alert.txt
```

we summarize the alerts in Appendix 3.

Search in the Snort Signature Database [1] for each Sid listed in Appendix 3 provides us with the impact and possibility of false positive associated with the corresponding alert. Appendix 4 includes such information.

Based on the impact, description of signature, and source/destination IP address, we categorize all detects and determine a severity level (high, medium or low) for each category (refer to Appendix 5 for the details).

Severity	Category	Count
High	Buffer overflow	2
	Arbitrary command execution	4
	Privileged remote access	2
	Password retrieval	3
Medium	Arbitrary command execution with users' privilege	2
	Information disclosure	6
	Attempted (D)DoS	6
	Access attempt	3
Low	Information gathering	23
	Unknown	4

Table 3 Categorization and Severity of Alerts

3. In-depth Analysis

In order to identify security issues existing on the University network, we select the three most critical detects and perform an in-depth analysis.

3.1 FTP Site Exec Format String Attempt Detect

The most critical detect we consider is the "FTP site exec format string attempt". In this section we analyze the detect in detail.

Description

File Transfer Protocol (FTP) is the Internet standard for transferring files from one system to another [2]. Wu-ftpd is a replacement for the FTP daemon on Unix

systems developed at Washington University. It is the most popular FTP daemon on the Internet, used on many anonymous FTP sites all around the world [3].

Site exec is a non-standard or UNIX specific command supported by a wu-ftp server. It can be used to execute a program [4]. For example,

$ site exec *program_name params*

Because of insufficient checking in the user input passed directly into a format string argument in several function calls (such as *printf()* and *sprintf()*) that implement the *site exec* command, a malicious user can pass character format strings consisting of carefully constructed conversion characters (%f, %p, %n, etc.) when executing a *site exec* command. If successful, the FTP daemon may be tricked into executing arbitrary code as root [5][6][7].

Running a vulnerable version of wu-ftpd as an anonymous FTP server increases the exploitability dramatically since any user can log into the FTP server from anywhere and run *site exec* command to exploit the vulnerability [5].

"FTP site exec format string attempt" detect indicates an attacker has successfully attempted a format string attack against an input validation vulnerability in wu-ftpd version 2.6.1 and earlier [5]. This allows the attacker to execute arbitrary commands via the *site exec* command (CVE-2000-0573 [8]).

Reason of Selection

A successful exploitation of the wu-ftpd site exec vulnerability may allow local and remote users, including the "ftp" and "anonymous" user, to gain root privileges. The widespread use of wu-ftpd, especially on a large number of anonymous FTP sites, makes the impact of the vulnerability very severe [5].

Detect Generation

The raw data was captured by Snort intrusion detection systems and posted on SANS website[2]. When we process the data using Snort, the following rule (Sid 1971) in the rule set is triggered and the "FTP site exec format string attempt" detect is generated (see Section Detect Overview).

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP SITE EXEC format string attempt"; flow:to_server,established; content:"SITE"; nocase; content:"EXEC"; distance:0; nocase; pcre:"/^SITE\s+EXEC\s[^\n]*?%[^\n]*?%/smi"; classtype:bad-unknown; sid:1971; rev:4;)
```

Appendix 6 lists the alerts logged. Here is one instance.

```
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:04:32.812057 10.10.10.186:32802 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:37735 IpLen:20 DgmLen:76 DF
***AP*** Seq: 0x15CC0B8C  Ack: 0x367F26B5  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 956557 1892741
```

Some fields in the alert are explained in Table 4.

[2] http://isc.sans.org/logs/Raw/2003.12.15.tgz (October 11, 2004).

Field	Explanation
11/18/03-15:04:32.812057	Date and time of packet capturing
10.10.10.186	Source IP address
32802	Source port
172.20.201.198	Destination IP address
21	Destination port
TCP	Protocol employed
TTL:64	Time to live
TOS:0x0	Type of service
ID:37735	Identification number
IpLen:20	Length of IP header (in byte)
DgmLen:76	Length of the whole packet (in byte)
DF	Do not fragment flag set
AP	TCP flags with flags ACK and PSH set
Seq: 0x15CC0B8C	TCP sequence number
Ack: 0x367F26B5	TCP acknowledge number
Win: 0x16D0	TCP window size
TcpLen: 32	Length of TCP header (in byte)
TS: 956557 1892741	Timestamp

Table 4 Snort Alert Format

In order to inspect the packets triggering the alert, we need to dump traffic in hexadecimal format. First, we extract the distinct source/destination IP address pairs from the alerts in Appendix 6.

Source Destination

10.10.10.186 ←→ 172.20.201.198
10.10.10.196 ←→ 172.20.201.198
10.10.10.165 ←→ 172.20.201.135
10.10.10.228 ←→ 172.20.201.135

Then we run WinDump with some specific options to catch the FTP traffic (port 21) associated with the source and destination IP addresses.

```
C:\GCIA\Practical\Data\2003.12.15>for /L %i in (1,1,14) do windump -r 2003.12.15.%i -s0 -S -v -x
-X ip proto \tcp and ((src host 10.10.10.186 and dst host 172.20.201.198) or (src host
172.20.201.198 and dst host 10.10.10.186) or (src host 10.10.10.196 and dst host
172.20.201.198) or (src host 172.20.201.198 and dst host 10.10.10.196) or (src host
10.10.10.165 and dst host 172.20.201.135) or (src host 172.20.201.135 and dst host
10.10.10.165) or (src host 10.10.10.228 and dst host 172.20.201.135) or (src host
172.20.201.135 and dst host 10.10.10.228)) and port 21 >>
windump_ftp_site_exec_format_string.txt
```

-r	read packets from file
-s0	set snaplen to 0 to use the required length to catch whole packets
-S	print absolute, rather than relative, TCP sequence numbers
-v	slightly more verbose output
-x	print each packet (minus its link level header) in hex
-X	print ascii while printing hex. If -x is also set, the packet is printed in hex/ascii

The following is the hexadecimal with ASCII output of the packet which triggers the above alert (refer to Appendix 7 for the details). Table 5 provides some explanation for the format.

```
15:04:32.812057 10.10.10.186.32802 > 172.20.201.198.21: P [tcp sum ok]
365693836:365693860(24) ack 914302645 win 5840 <nop,nop,timestamp 956557 1892741>
(DF) (ttl 64, id 37735, len 76)
0x0000  4500 004c 9367 4000 4006 1ca6 0a0a 0aba      E..L.g@.@.......
0x0010  ac14 c9c6 8022 0015 15cc 0b8c 367f 26b5      ....."......6.&.
0x0020  8018 16d0 0753 0000 0101 080a 000e 988d      .....S..........
0x0030  001c e185 5349 5445 2045 5845 4320 2530      ....SITE.EXEC.%0
0x0040  3230 647c 252e 6625 2e66 7c0a                20d|%.f%.f|.
```

Field	Explanation
15:04:32.812057	Time of packet capturing
10.10.10.186	Source IP address
32802	Source port
172.20.201.198	Destination IP address
21	Destination port
P	TCP flag PSH set
365693836	Starting TCP sequence number
365693860	Ending TCP sequence number
(24)	Length of TCP payload (in byte)
ack 914302645	TCP acknowledge number
win 5840	TCP window size
timestamp 956557 1892741	Timestamp
(DF)	Do not fragment flag set
ttl 64	Time to live
id 37735	Identification number
len 76	Length of the whole packet (in byte)

Table 5 WinDump Output Format

The highlighted data is the TCP payload in the packet, which is 24 bytes long. It is the attack signature that causes the “FTP site exec format string attempt” detect to be logged.

Probability of Spoofed Source Address

To exploit the wu-ftpd site exec vulnerability, an attacker needs to login into an FTP server first using a valid account. This requires the completion of the TCP three-way handshake. Therefore, spoofed source IP address will not work under normal conditions. We can confirm this by demonstrating the communication between an attacker and FTP server, such as 10.10.10.186 and 172.20.201.198 (see Appendix 7).

Attack Mechanism

“FTP site exec format string attempt” targets the FTP service, which is popular on the Internet used for file transfer. Imagine a famous FTP site were compromised

with root access. Then attackers could put whatever contents they wanted on the site, e.g., viruses, exploit codes, and backdoors, and give them some "good" filenames. When innocent users tried to download such files from the FTP site, their computers would get compromised right away. This makes hacking an FTP server appealing.

Due to the availability of multiple exploit scripts for the wu-ftpd site exec vulnerability, it is simple to attack such a vulnerable FTP server [5]. An attacker could log into an FTP server using an "anonymous" or "ftp" account, and check to see if the *site exec* command functionality is enabled. If it were, the attacker could initiate exploit codes for the format string attack, and then execute arbitrary commands on the server. By default, most implementations of wu-ftpd run the daemon as root and allow anonymous login. Thence, the attacker would have root access to the system.

This process can be seen from the dumped log in Appendix 7. We summarize the traffic as follows.

1. three-way handshake
2. banner information returned (marked in blue)
3. the attacker logged in as the "ftp" user (marked in turquoise) with a password (marked in bright green)
4. login succeeded and access permitted (marked in yellow)
5. attack signature detected (marked in red)
6. exploit code sent (marked in pink)

Gradually, the attacker gets root privilege (proved by the user id and group id), obtains a list of user names and encrypted passwords from the server, impersonates another user, and browses and modifies an important proposal file[3] (refer to Appendix 8 for the details). So far the FTP server is under full control of the attacker.

Correlations

In mid-2000, several security advisories, such as CVE-2000-0573 [8], AusCERT Advisory [6], and CERT® Advisory [7], were published discussing the site exec vulnerability and providing solutions. At the same time, some exploit codes were posted on BugTraq [9][10][11][12]. An excellent list of cross-references on this wu-ftpd vulnerability can be found from SecuritySpace [13].

Many resources provide deep insight into "FTP site exec format string" attack. Andreas Thuemmel researched the mechanism of format string exploits and illustrated how it works against wu-ftpd site exec vulnerability [14]. In [15], Jason Testart investigated in detail a similar attack detected on his network. Some GCIA students also did good job in analyzing such attacks [16][17][18].

[3] This is only for the example of attacker 10.10.10.186 exploiting FTP server 172.20.201.198. Content inspection on the file *important-proposal.txt* brings us into thinking that the attacked host might be a honeypot.

Evidence of Active Targeting

From the WinDump log (part is presented in Appendix 7), we can see the attack is directed at specific hosts, 172.20.201.135 and 172.20.201.198. This means some reconnaissance has been done beforehand to identify the FTP service and gather information needed, such as the version number.

Severity

On the basis of the following formula, we calculate the severity of the attack, which should be high.

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

with each value ranked on a scale from 1 (lowest) to 5 (highest).

- Criticality: 5

The targets are FTP servers, used for file transfer. If attackers could take over a site's FTP server, they might be able to manipulate trust relationships and thereby compromise most or all of a site's systems (In fact the attacker 10.10.10.186 does try this but fails – see Appendix 8).

Furthermore, the systems may hold highly confidential information (e.g., server 172.20.201.198 has an *important-proposal.txt* file stored on it).

- Lethality: 5

The attack exploits a buffer overflow vulnerability, which results in a root compromise. This can cause very severe damage to the targeted system since the system is under the attacker's control.

- System Countermeasures: 2

We do not know the countermeasures placed on the targeted systems. But it is clear that the systems are still running a vulnerable version of wu-ftpd (version 2.6.0) three years after the wu-ftpd site exec vulnerability was addressed. In addition, the FTP servers allow guest access to them.

- Network Countermeasures: 2

There is a Snort IDS located in the border of the target network. Other defensive mechanisms in place are not clear to us. However, whatever the countermeasure is, it does not block certain specific attacks (e.g., format string attempt).

Therefore, the calculated severity is (5 + 5) - (2 + 2) = 6, which meets our prediction.

3.2 FTP Passwd/Shadow Retrieval Attempt Detect

The "FTP passwd/shadow retrieval attempt" is regarded as the second critical detect. A detailed analysis on the detect is presented in this section.

Description

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called */etc/passwd*. This file needs to be readable by all system users so that they can be verified when logging into the system. Consequently, it can be of a security risk.

An alternative is to use shadow password scheme, which stores account information in the */etc/passwd* file in a compatible format, and encrypted passwords in a separate file, called */etc/shadow*. The */etc/passwd* file is readable by everyone, whereas */etc/shadow* file is readable only by the root account and is therefore more secure.

"FTP passwd/shadow retrieval attempt" detect is indicative of an attempt to retrieve user account information and/or encrypted passwords from a Unix FTP server [19][20].

With password cracking tools in hands, such as L0phtcrack and John-the-Ripper, it is possible for attackers to obtain decrypted passwords. Then they may use the information to gain unauthorized access to the victim host or some other hosts which the same users may have access to.

Reason of Selection

Successful *passwd/shadow* file retrieval from an FTP server may result in unauthorized access to the system. If a super-user account were compromised by either password cracking or privilege escalation, the system would be under control of the attacker.

Detect Generation

During our data processing, the following Snort rules (Sid 356 and Sid 1928) are triggered and the detects "FTP passwd retrieval attempt" and "FTP shadow retrieval attempt" are generated, respectively (see Section Detect Overview).

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP passwd retrieval attempt"; flow:to_server,established; content:"RETR"; nocase; content:"passwd"; reference:arachnids,213; classtype:suspicious-filename-detect; sid:356; rev:5;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP shadow retrieval attempt"; flow:to_server,established; content:"RETR"; nocase; content:"shadow"; classtype:suspicious-filename-detect; sid:1928; rev:3;)

Alerts triggered are listed in the following.

[**] [1:356:5] FTP passwd retrieval attempt [**]
[Classification: A suspicious filename was detected] [Priority: 2]
11/18/03-15:00:51.375643 10.10.10.122:59909 -> 192.168.17.135:21
TCP TTL:64 TOS:0x10 ID:42537 IpLen:20 DgmLen:65 DF
AP Seq: 0x24B13BC4 Ack: 0xB5B6A7AC Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 174671 5005060
[Xref => http://www.whitehats.com/info/IDS213][4]

[4] Field [Xref => http://www.whitehats.com/info/IDS213] points out the cross references for the alert.

```
--
[**] [1:1928:3] FTP shadow retrieval attempt [**]
[Classification: A suspicious filename was detected] [Priority: 2]
11/18/03-15:01:00.322287 10.10.10.122:59909 -> 192.168.17.135:21
TCP TTL:64 TOS:0x10 ID:42542 IpLen:20 DgmLen:65 DF
***AP*** Seq: 0x24B13BD7  Ack: 0xB5B6A83A  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 175565 5005955
--
[**] [1:356:5] FTP passwd retrieval attempt [**]
[Classification: A suspicious filename was detected] [Priority: 2]
11/18/03-15:21:04.263547 10.10.10.212:4638 -> 192.168.17.135:21
TCP TTL:128 TOS:0x0 ID:26429 IpLen:20 DgmLen:53 DF
***AP*** Seq: 0xE3F9B922  Ack: 0xFB5E8581  Win: 0xF6A2  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS213]
```

There are two source IP addresses and one destination IP address involved in the alerts.

Source	Destination
10.10.10.122 ←→	192.168.17.135
10.10.10.212 ←→	192.168.17.135

Appendix 9 shows part of the WinDump results from the following scripts.

```
C:\GCIA\Practical\Data\2003.12.15>for /L %i in (1,1,14) do windump -r 2003.12.15.%i -s0 -S -v -x
-X ip proto \tcp and ((src host 10.10.10.122 and dst host 192.168.17.135) or (src host
192.168.17.135 and dst host 10.10.10.122) or (src host 10.10.10.212 and dst host
192.168.17.135) or (src host 192.168.17.135 and dst host 10.10.10.212)) and port 21 >>
windump_ftp_passwd_or_shadow_retrieval.txt
```

The highlighted data is the TCP payload in the packets used for attacking. The red-marked data indicates that /etc/*passwd* file is retrieved successfully from the FTP server.

Probability of Spoofed Source Address

In order to retrieve *passwd/shadow* file from a Unix FTP server, an attacker must login into the server using a valid account, which means the TCP three-way handshake needs to be completed. Thus, spoofed source IP address will not work under normal conditions. This can be confirmed by the communication between the attacker (10.10.10.122 or 10.10.10.212) and FTP server (192.168.17.135) (see Appendix 9).

Attack Mechanism

"FTP passwd/shadow retrieval attempt" intends to retrieve user account information together with passwords from an FTP server. If such information fell into wrong hand, attackers would (1) use the information contained in the *passwd* file to launch a dictionary attack against the server so as to obtain unauthorized access; or (2) crack the passwords of several user accounts, and then proceed to login to the system remotely and possibly gain escalated privileges via a local exploit on the system. Especially, if the root account were cracked or root privilege were acquired, attackers could control the FTP server completely and make it a malicious site to distribute virus or exploit other hosts which were used

to download files from the compromised server. This makes it attractive to get the password file of an FTP server.

Taking advantage of a system misconfiguration or directory traversal technique, an attacker logging into a Unix FTP server through guest access might have access to the */etc* directory, where *passwd* and/or *shadow* file is stored. In some rare circumstances, a system administrator may have accidentally left a copy of a *passwd* file in a directory accessible for "anonymous" or other FTP users, which presents a high security risk and simplifies the password file retrieval attack [19][20].

Such a process can be seen from the extracted WinDump log in Appendix 9.The traffic flow is summarized in the following.

1. three-way handshake
2. banner information returned (marked in blue)
3. the attacker logged in as the "ftp" user (from 10.10.10.122) / "anonymous" user (from 10.10.10.212) (marked in turquoise) with a password (marked in bright green)
4. login succeeded and access permitted (marked in yellow)
5. directory content listed by traversing the directory structure (marked in pink)
6. access gained to the */etc* directory by utilizing a system misconfiguration (marked in violet)
7. successful *passwd* file retrieval (marked in red)
8. *shadow* file retrieval tried but failed (marked in teal)[5]
9. some *site* commands trial[6]
10. exit

Correlations

FTP password file retrieval is a common attack. It might be the result of other attacks or system misconfiguration [19]. There is no CVE entry associated with this attack.

Some resources provide detailed analysis on "FTP passwd/shadow retrieval attempt" attack [21].

Evidence of Active Targeting

The WinDump log in Appendix 9 shows the attack is directed at a specific host, 192.168.17.135. This indicates reconnaissance has been done previously to identify the FTP service and gather information needed.

Severity

We can make calculation on the severity of the attack according to the following formula. The severity should be high.

[5] This is only for the example of attacker 10.10.10.122 exploiting FTP server 192.168.17.135.

[6] This is only for the example of attacker 10.10.10.122 exploiting FTP server 192.168.17.135.

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

with each value ranked on a scale from 1 (lowest) to 5 (highest).

- Criticality: 4

The target is an FTP server, used for file transfer. If the system user account information were disclosed, attackers could gain privileged access to the server. This might lead attackers to take over a site's FTP server, manipulate trust relationships, and compromise most or all of a site's systems.

- Lethality: 5

FTP password file retrieval attack retrieves the user account information with passwords, which can result in unauthorized, ultimately super-user access. Severe damage to the targeted system will happen if this succeeds.

- System Countermeasures: 1

We do not know the countermeasures placed on the targeted system. But it is clear that the system is misconfigured and vulnerable to directory traversal. Guest access to the FTP server is allowed. Additionally, the Unix system does not use shadow password scheme (When the attacker tries to retrieve /etc/*shadow* file, it is said no such file or directory – See Appendix 9), which implies a very old operating system is in use.

- Network Countermeasures: 2

There is a Snort IDS located in the border of the target network. Other defensive mechanisms in place are not clear to us. However, whatever the countermeasure is, it does not block certain specific attacks (e.g., password file retrieval attempt).

Therefore, the calculated severity is (4 + 5) - (1 + 2) = 6, which is the same as we predicted.

3.3 Rservices Rsh Froot Detect

The third detect that causes our special attention is the "rservices rsh froot" detect. We investigate this detect in the following section.

Description

Unix remote services (r-services) provide users with the ability to execute commands on remote hosts.

Remote shell (rsh) is one of these services. It is used to connect to a remote host and execute a specified command. If no command is specified, the user will be logged in to the remote host using rlogin[7] [22].

[7] Rlogin (remote login) is another remote service. It allows an authorized user to login to a host on a network and interact as if the user were physically at the host. If permitted, the user can read, edit, or delete files.

A vulnerability exists in some implementations of the rsh daemon. By exploiting this, an attacker can gain unauthorized root access to a system which is running such a vulnerable service.

"Rservices rsh froot" detect gives us an indication of the use of a suspicious login attempt – a connection is made using rsh whilst passing the parameter *-froot* [23]. This may lead the attacker to gain super-user access to the host (CVE-1999-0113 [24]).

Reason of Selection

If "rservices rsh froot" attempt is successful, an attacker can login to the vulnerable system as root without being asked for a password [25]. Moreover, the attack is very simple to launch with no exploit software required. These make the attack have serious impact [23].

Detect Generation

Processing the dumped data using Snort triggers the following rule (Sid 604) and generates the "rservices rsh froot" detect (see Section Detect Overview).

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 513 (msg:"RSERVICES rsh froot"; flow:to_server,established; content:"-froot|00|"; reference:arachnids,387; classtype:attempted-admin; sid:604; rev:5;)
```

In the following are the alerts generated.

```
[**] [1:604:5] RSERVICES rsh froot [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
11/18/03-15:06:31.997166 10.10.10.165:1003 -> 172.20.201.135:513
TCP TTL:128 TOS:0x0 ID:32972 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x236B43A9  Ack: 0x2E30A118  Win: 0x4470  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS387]
--
[**] [1:604:5] RSERVICES rsh froot [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
11/18/03-15:06:41.489412 10.10.10.165:1010 -> 172.20.201.198:513
TCP TTL:128 TOS:0x0 ID:34005 IpLen:20 DgmLen:62 DF
***AP*** Seq: 0x25A1059B  Ack: 0x3F2A031A  Win: 0x4470  TcpLen: 20
[Xref => http://www.whitehats.com/info/IDS387]
--
[**] [1:604:5] RSERVICES rsh froot [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
11/18/03-15:12:16.405633 10.10.10.186:1023 -> 172.20.201.198:513
TCP TTL:64 TOS:0x0 ID:61201 IpLen:20 DgmLen:69 DF
***AP*** Seq: 0x3328D8EF  Ack: 0x53827ABC  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1193959 1939034
[Xref => http://www.whitehats.com/info/IDS387]
```

Three pairs of source-destination IP address are associated with the above alerts.

Source	Destination
10.10.10.165	←→ 172.20.201.135
10.10.10.165	←→ 172.20.201.198
10.10.10.186	←→ 172.20.201.198

After running the following script, we extract the WinDump data which triggers the alerts (refer to Appendix 10 for part of the output).

```
C:\GCIA\Practical\Data\2003.12.15>for /L %i in (1,1,14) do windump -r 2003.12.15.%i -s0 -S -v -x
-X ip proto \tcp and ((src host 10.10.10.165 and dst host 172.20.201.135) or (src host
172.20.201.135 and dst host 10.10.10.165) or (src host 10.10.10.165 and dst host
172.20.201.198) or (src host 172.20.201.198 and dst host 10.10.10.165) or (src host
10.10.10.186 and dst host 172.20.201.198) or (src host 172.20.201.198 and dst host
10.10.10.186)) and port 513 >> windump_rservices_rsh_froot.txt
```

The red-marked data is the TCP payload in the packet used for exploiting. The pink-marked data indicates that the attacker logged in as root successfully.

Probability of Spoofed Source Address

The purpose of "rservices rsh froot" attempt is to login to a vulnerable system as root. The packet that causes the alert is normally a part of an established TCP session. Attackers expect or desire a response to their packets. So it is most likely that the source IP address is not spoofed. Communications between the attackers (10.10.10.165 and 10.10.10.186) and victims (172.20.201.135 and 172.20.201.198) can prove this.

Attack Mechanism

"Rservices rsh froot" attempt aims at exploiting Unix r-services, e.g., rsh service, to gain remote access to a system with root privilege. Once succeeded, an attacker would have full control over the system. In particular, if the targeted system is an FTP server (which is true in this case, see Section 3.1), a successful attacker could launch attacks through FTP service, such as distributing malicious codes, or manipulate trust relationships to compromise other systems. This attracts attackers into such an access attempt.

As a result of the vulnerability in some rsh daemon implementations, remote root access is allowed by using the *-froot* parameter for the *rsh* command. If a UNIX system has the rsh service running and is vulnerable, an attacker can exploit it simply by running the *rsh* command with *-froot* parameter. For example,

$ rlogin *vulnerable-system* -l -froot[8]

Voila! The attacker logins to the system with unauthorized root privilege [23][25][26].

We can see this process from the log in Appendix 10. The following lists the simplified traffic flow.

1. three-way handshake
2. the attacker remotely logged in using r-command with *-froot* parameter (marked in red)

[8] When executed with no specified command, rsh invokes rlogin to remotely login a user [22]. In fact, this command line is the result of the following.

$ rsh *vulnerable-system* -l -froot

3. login succeeded and root access permitted (deduced by the following *id* command)
4. user id checked (marked in pink)
5. exit

We also tried to use Ethereal (version 0.10.7) to get more details about this traffic flow. The filter applied is shown in the following.

ip.addr == 10.10.10.186 and (ip.addr == 172.20.201.198 and tcp.port == 513)

After searching, we found in the file *2003.12.15.9* the data triggering the alert "rservices rsh froot". The screen snapshot is displayed in Figure 3 with the suspicious data highlighted. Seen from the screenshot, the r-command mentioned previously is actually *rlogin*. After successful login, an *id* command is issued to check whether the logged-in user is root.

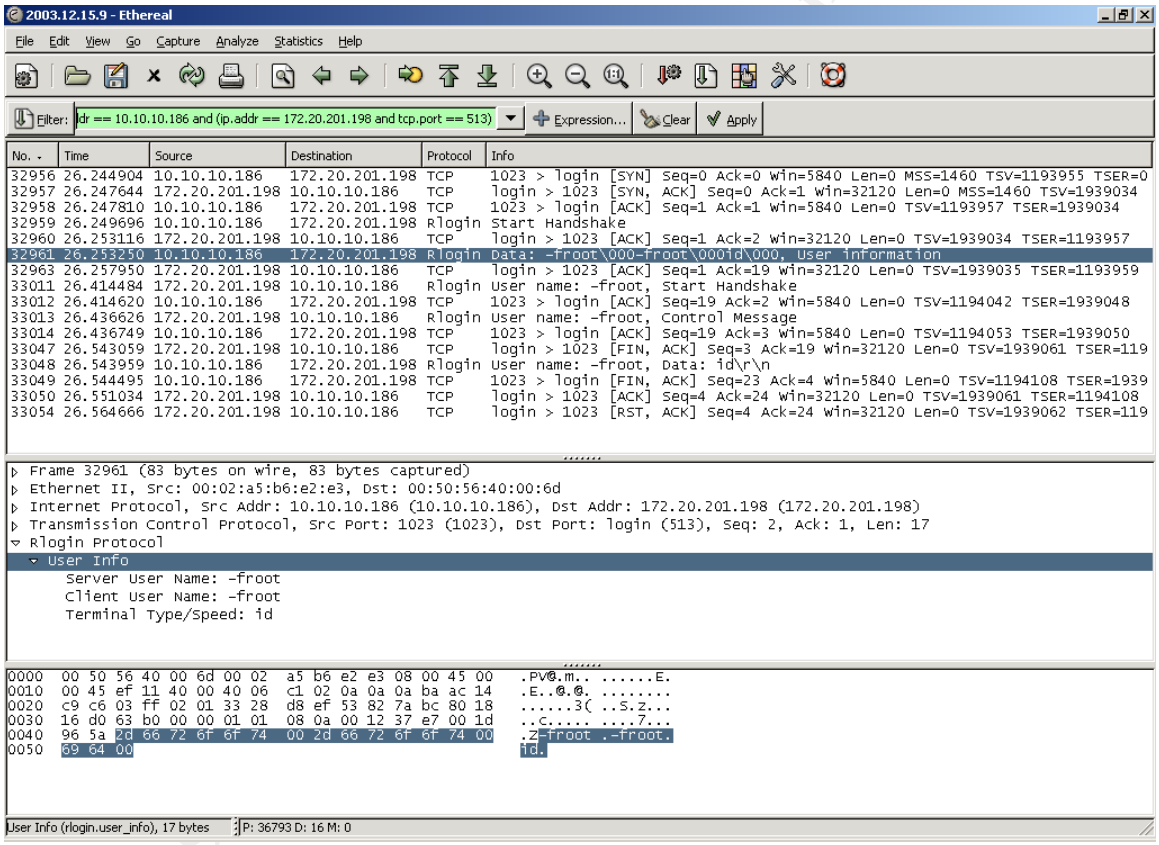

Figure 3 Ethereal Screen Snapshot

Correlations

At the end of April 1994, Internet Security Systems X-Force raised a security issue – *rlogin -froot* command could allow remote root access [25]. A month later, CERT® Coordination Center published an advisory on rlogin vulnerability and suggested some workaround [26]. The related CVE entry was created in 1999 [24].

Some discussion about the rlogin bug can be found on BugTraq [27][28][29].

Evidence of Active Targeting

As shown in the WinDump log (partially displayed in Appendix 10), the attack is directed at specific hosts, 172.20.201.135 and 172.20.201.198, respectively. This reveals some reconnaissance has been done in advance to identify the provided remote services and gather information needed.

Severity

The severity of the attack can be calculated based on the following formula. It should be high.

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

with each value ranked on a scale from 1 (lowest) to 5 (highest).

- Criticality: 5

The targets have FTP servers running on them (see Section 3.1), used for file transfer. If rsh -froot attack succeeded, attackers could access the systems remotely with root privilege. With a site's FTP server under complete control, attackers might be able to manipulate trust relationships to compromise most or all of the site's systems.

Particularly, the systems may hold confidential information (see Section 3.1).

- Lethality: 5

Rsh -froot attack exploits a vulnerability in Unix r-services to acquire remote root access. Successful exploitation can result in severe damage to the targeted systems.

- System Countermeasures: 2

We do not know the countermeasures placed on the targeted systems. But it is clear that the systems are running an insecure application (rlogin) [30] on some Unix operating system which is not up-to-date [26][31]. The systems have a vulnerable version of wu-ftpd running with guest access allowed (see Section 3.1).

- Network Countermeasures: 2

There is a Snort IDS located in the border of the target network. Other defensive mechanisms in place are not clear to us. However, whatever the countermeasure is, it does not block certain specific attacks (e.g., rsh -froot attempt).

As we predicted, the calculated severity is high – (5 + 5) - (2 + 2) = 6.

4. Network Statistics

For the network statistics purpose, we analyze the captured log from the perspective of IP address and port number. Our basic criterion is the number of hits – the higher the number, the noisier the IP address or port number (service).

The following two files are the basis of this analysis.

- *Traffic.txt*, which includes all the network packets and associated source-destination IP address pairs (see Section Data Relationship).
- *Alert.ids*, which includes all the alerts triggered and associated source-destination IP address pairs (see Section Detect Overview).

4.1 Top Talkers

As we can see from Section Data Relationship, there are six different types of network traffic captured (see Table 1). After processing the file *Traffic.txt*, we obtain all source IP addresses involved and the number of hits they generate (refer to Appendix 11 for the details).

The top five noisiest talkers are listed in Table 6.

Source IP Address	# of Hit
10.10.10.165	100547
10.10.10.195	58619
172.20.11.80	49341
172.20.201.198	41108
10.10.10.112	28247

Table 6 Top Five Noisiest Talkers (1)

When we take consideration of the security factor – the impact of network traffic, the file *Alert.ids* becomes the resource. Data processing brings up all source IP addresses triggering Snort alerts and the number of hits (refer to Appendix 12 for the details).

The top five noisiest talkers are listed in Table 7, together with the information about different alerts triggered and unique destination hosts targeted.

Source IP Address	# of Hit	Distinct Alert	Unique Destination
10.10.10.113	18222	6	4
10.10.10.165	5737	30	765
10.10.10.231	559	5	511
10.10.10.164	549	5	258
10.10.10.234	429	1	4

Table 7 Top Five Noisiest Talkers (2)

4.2 Top Targeted Services

Using the same criteria as those in Section 4.1, we can derive top five targeted services, which are listed in Table 8 (from the perspective of the network traffic) and Table 9 (from the perspective of the alerts triggered) (Due to the huge amount of data, we do not provide the details).

Port Number	# of Hit	Service[9] [32]
22	24645	SSH Remote Login Protocol
21	2663	File Transfer (Control)
80	2428	World Wide Web HTTP
1050	2402	CORBA Management Agent
8080	2156	HTTP Alternate

Table 8 Top Five Targeted Services (1)

Port Number	# of Hit	Service[10] [32]
0	1190	Reserved
161	599	SNMP
69	223	TFTP
162	212	SNMP Trap
705	140	AgentX

Table 9 Top Five Targeted Services (2)

4.3 Profile of External Addresses

From the source IP address list (see Appendix 11), we find only two external addresses, 169.254.135.50 and 238.122.10.140.

Profile 1

WinDump log reveals that host 169.254.135.50 generates 18 NBT (NetBIOS over TCP/IP) broadcast packets for NetBIOS name service and datagram service (refer to Appendix 13 for the details). Investigation on the file *Alert.ids* shows the host triggers an alert six times because of some corrupted UDP packets (refer to Appendix 14 for the details). Unfortunately, we do not succeed in capturing the corresponding hexadecimal output using WinDump.

From the ARIN's WHOIS database [33], we can retrieve the registration information on host 169.254.135.50.

Search results for: 169.254.135.50

OrgName: Internet Assigned Numbers Authority
OrgID: IANA
Address: 4676 Admiralty Way, Suite 330
City: Marina del Rey
StateProv: CA
PostalCode: 90292-6695
Country: US

NetRange: 169.254.0.0 - 169.254.255.255
CIDR: 169.254.0.0/16
NetName: LINKLOCAL
NetHandle: NET-169-254-0-0-1

[9] Both TCP and UDP ports represent the same service.

[10] Both TCP and UDP ports represent the same service.

Parent:	NET-169-0-0-0-0
NetType:	IANA Special Use
NameServer:	BLACKHOLE-1.IANA.ORG
NameServer:	BLACKHOLE-2.IANA.ORG
Comment:	Please see RFC 3330 for additional information.
RegDate:	1998-01-27
Updated:	2002-10-14
OrgAbuseHandle:	IANA-IP-ARIN
OrgAbuseName:	Internet Corporation for Assigned Names and Number
OrgAbusePhone:	+1-310-301-5820
OrgAbuseEmail:	abuse@iana.org
OrgTechHandle:	IANA-IP-ARIN
OrgTechName:	Internet Corporation for Assigned Names and Number
OrgTechPhone:	+1-310-301-5820
OrgTechEmail:	abuse@iana.org

The Time to Live (TTL) value of the packets (128) and the use of NBT make it very possible that host 169.254.135.50 is a Windows system.

Profile 2

Only three packets are originated from host 238.122.10.140. They look like the final acknowledgement of a TCP three-way handshake (refer to Appendix 15 for the details). But we do not find any stimuli associated with these ACK packets (The starting time of packet capturing could not be the reason since the first captured packet originated from host 172.20.11.2 is at 20:58:21.682437, nearly 10 minutes before the ACK packets). According to the fact that the same source port, destination port, packet identification number, and the time difference between each packet are used, we conclude that this is an ACK scan against host 172.20.11.2 (a border router).

Search in the ARIN's WHOIS database [33] gives us the registration information on host 238.122.10.140.

Search results for: 238.122.10.140

OrgName:	Internet Assigned Numbers Authority
OrgID:	IANA
Address:	4676 Admiralty Way, Suite 330
City:	Marina del Rey
StateProv:	CA
PostalCode:	90292-6695
Country:	US
NetRange:	224.0.0.0 - 239.255.255.255
CIDR:	224.0.0.0/4
NetName:	MCAST-NET
NetHandle:	NET-224-0-0-0-1
Parent:	
NetType:	IANA Special Use
NameServer:	FLAG.EP.NET
NameServer:	STRUL.STUPI.SE
NameServer:	NS.ISI.EDU
NameServer:	NIC.NEAR.NET
Comment:	This block is reserved for special purposes.

Comment:	Please see RFC 3171 for additional information.
Comment:	
RegDate:	1991-05-22
Updated:	2002-09-16
OrgAbuseHandle:	IANA-IP-ARIN
OrgAbuseName:	Internet Corporation for Assigned Names and Number
OrgAbusePhone:	+1-310-301-5820
OrgAbuseEmail:	abuse@iana.org
OrgTechHandle:	IANA-IP-ARIN
OrgTechName:	Internet Corporation for Assigned Names and Number
OrgTechPhone:	+1-310-301-5820
OrgTechEmail:	abuse@iana.org

Besides, we can make a guess on the operating system based on the Time to Live (TTL) value of the packets (255). It is most likely a Sun Solaris system.

5. Correlations

In Section In-depth Analysis, we investigate three most critical detects. It is easy to find out that the attacking hosts (six in total) reside in subnet 10.10.10.0/24. This could be the result that some computers in the subnet are compromised and controlled by attackers.

Further investigation on the alerts Snort IDS generated demonstrates that some other alerts are triggered at the same time when the targets under attack.

Attack	Attacker	Target	Other Alerts Triggered
FTP site exec format string attempt	10.10.10.165	172.20.201.135	1. FTP site exec attempt 2. FTP format string attempt
	10.10.10.228	172.20.201.135	
	10.10.10.186	172.20.201.198	
	10.10.10.196	172.20.201.198	
RSERVICES rsh froot	10.10.10.165	172.20.201.135	
	10.10.10.165	172.20.201.198	
	10.10.10.186	172.20.201.198	
FTP passwd retrieval attempt	10.10.10.122	192.168.17.135	1. FTP list directory traversal attempt 2. FTP shadow retrieval attempt
	10.10.10.212	192.168.17.135	

Table 10 Alert Correlation

If we examine the captured data from the attacker-target perspective, we can outline all attacks the six attackers have launched against three targets (refer to Appendix 16 for the details).

Attacker	Target	Distinct Alerts
10.10.10.165	172.20.201.135	29
10.10.10.228	172.20.201.135	9
10.10.10.186	172.20.201.198	13
10.10.10.196	172.20.201.198	3
10.10.10.165	172.20.201.198	27

10.10.10.122	192.168.17.135	3
10.10.10.212	192.168.17.135	1

Table 11 Attacker-Target View

In addition to the internal self referencing correlation presented above, we build external correlation from other resources, including some GCIA students' analysis work (see Section In-depth Analysis).

6. Observations

During our detect analysis, we have observed that all attacked hosts, 172.20.201.135, 172.20.201.198, and 192.168.17.135, are compromised. Table 12 summarizes the compromises happened on each host.

Host	Compromise
172.20.201.135	– Root privilege compromised
172.20.201.198	– Root privilege compromised – Password file exposed – Possibly confidential information read and modified intentionally and unauthorizedly
192.168.17.135	– Password file exposed

Table 12 Compromises on the Attacked Hosts

Inspecting the file *Alert.ids* shows us the alerts generated by the above attacked hosts (see Table 13).

Host	Alert	Target	Hit	Starting Time
172.20.201.135	TELNET access	10.10.10.165	23	15:04:02.042202
	TELNET login incorrect	10.10.10.165	1	15:08:36.787122
172.20.201.198	(snort_decoder): Short UDP packet, length field > payload length	10.10.10.165	31	15:07:04.632204
	TELNET access	10.10.10.165	23	15:04:02.775670
		10.10.10.186	11	15:12:22.881280
	TELNET login incorrect	10.10.10.165	1	15:08:58.188982
192.168.17.135	None			

Table 13 Alerts Triggered by the Attacked Hosts

Considering the starting time of the above alerts and the three analyzed attacks (see Table 14), we would conclude that they might not relate to each other.

Attack	Target	Starting Time
FTP site exec format string attempt	172.20.201.135	15:15:49.451015
	172.20.201.198	15:04:32.812057
RSERVICES rsh froot attempt	172.20.201.135	15:06:31.997166
	172.20.201.198	15:06:41.489412
FTP passwd/shadow retrieval attempt	192.168.17.135	15:00:51.375643

Table 14 Overview of Attacking Time

So far, no suspicious activity from the compromised hosts is detected. There might be several reasons for this. For example,

- Data capture time might be too short.
- Other communication paths might exist.

7. Defensive Recommendations

Based upon our analysis, we highly recommend that the on-site security team take the following defensive actions.

- Conduct vulnerability assessment periodically against the University network. Fix the identified system misconfiguration and security holes;
- Develop a strong patch management process and procedure. Keep systems up-to-date;
- Introduce a (stateful) firewall/packet filter to each subnet. If possible, filter at the perimeter the packets with suspicious content;
- Encrypt confidential information stored on systems. Some host-based intrusion detection system, such as Tripwire is suggested to be installed on such systems;
- Enhance password policy. Use strong passwords. Change the potentially compromised passwords as soon as possible;
- Investigate and cleanup the compromised systems to ensure no malicious code installed;
- Verify the suspicious activities, such as DDoS handler calling for agent, to see whether they are false positives;
- Disable unnecessary services, e.g., r-services;
- Use secure applications instead of insecure ones. For example, replace telnet with SSH;
- Avoid giving out banner information about operating systems or applications;
- Raise user awareness of security.

Analysis Process

Our analysis platform is an Intel Pentium III 1 GHz desktop with 256 MB memory and a 20 GB hard drive. The operating system is Microsoft Windows 2000 (version 5.00.2195) with Service Pack 4.

The following lists all software we used to tackle the logs.

- WinPcap 2.3
- Snort 2.2.0 with the rule set 2.2

- WinDump 3.6.2
- Ethereal 0.10.7
- Cygwin (for standard Unix tools *grep*, *awk*, *sed*, *sort*, *uniq*, *head*, *cat*, *wc*, etc.)
- Microsoft Excel 2000

1. Methodology

In general, we employ "Top Down" methodology when we analyze the obtained IDS log files. We start from overviewing the entire logs. Step by step, we end up with capturing specific detects. The whole process consists of three parts – building data relationship, creating detect overview and performing in-depth analysis.

Steps in Building Data Relationship

- Verify the date and time window;
- Identify traffic types;
- Determine the monitored IP address range;
- Derive the network topology.

Steps in Creating Detect Overview

- Create a list of unique alerts with their number of hits;
- Research on each alert for its impact and the possibility of false positive;
- Categorize alerts;
- Determine a severity level for each category.

Steps in Performing In-depth Analysis

- Choose the most critical detects (with highest severity);
- Extract the source and destination IP addresses and port numbers;
- Dump the traffic flow for the selected detects;
- Examine the dumped log;
- Correlate with other detects.

2. Discussion

During our analysis on the third critical detect – "rservices rsh froot" attempt, the information WinDump (with options to print out each packet in hexadecimal and ASCII) provided was not enough to understand the traffic flow. Hence, we tried to use Ethereal to get some more details, such as the command used. Ethereal version 0.10.6 was the latest version at the time we processed the data. Unfortunately, it could read all the original data files but the file *2003.12.15.9* – we received an application error. After Ethereal version 0.10.7 was released, we succeeded in interpreting the traffic flow – the new version works well with the file *2003.12.15.9* (see Figure 3).

One interesting issue we would like to point out. When we correlated the three most critical attacks with other events included in the dumped log, it happened to be the first day after the Daylight Saving Time was over. We found that the newly processed data using WinDump changed its timestamp accordingly. In

order to look for data correlation, we had to adjust the computer system time back to the Daylight Saving Time.

References

[1] Snort. “Snort Signature Database.” URL: http://www.snort.org/cgi-bin/done.cgi (October 9, 2004).

[2] Stevens, W. Richard. TCP/IP Illustrated, Volume 1: The Protocols. Addison Wesley Longman, Inc., 1994. Page 419 – 439.

[3] WU-FTPD Development Group. “Frequently Asked Questions about WU-FTPD.” April 15, 2004. URL: http://www.wu-ftpd.org/wu-ftpd-faq.html (October 11, 2004).

[4] WU-FTPD Development Group. “WU-FTPD Man Pages.” January 10, 1997. URL: http://www.wu-ftpd.org/man/ (October 11, 2004).

[5] Snort. “FTP Site Exec Format String Attempt.” URL: http://www.snort.org/snort-db/sid.html?sid=1971 (October 10, 2004).

[6] Australian Computer Emergency Response Team (AusCERT). “WU-FTPD Site Exec Vulnerability.” AusCERT Reference #: AA-2000.02. June 26, 2000. URL: http://www.auscert.org.au/render.html?it=1911 (October 11, 2004).

[7] CERT® Coordination Center. “CERT® Advisory CA-2000-13 Two Input Validation Problems in FTPD.” November 21, 2000. URL: http://www.cert.org/advisories/CA-2000-13.html (October 11, 2004).

[8] CVE. “CVE-2000-0573.” Common Vulnerabilities and Exposures. CVE Version: 20040901. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0573 (October 11, 2004).

[9] TF8. “WUFTPD: Providing *Remote* Root since at Least 1994.” June 22, 2000. URL:http://marc.theaimsgroup.com/?l=bugtraq&m=96171893218000&w=2 (October 14, 2004).

[10] Frasunek, Przemyslaw. “WUFTPD 2.6.0 Remote Root Exploit.” June 23, 2000. URL:http://marc.theaimsgroup.com/?l=bugtraq&m=96179429114160&w=2 (October 14, 2004).

[11] Hines, Eric. “New Released Version of the WUFTPD Sploit.” July 7, 2000. URL: http://marc.theaimsgroup.com/?l=bugtraq&m=96299933720862&w=2 (October 14, 2004).

[12] Argamal, Lamagra. “FTPD: the Advisory Version.” June 23, 2000. URL:http://www.securityfocus.com/templates/archive.pike?list=1&msg=20000623091822.3321.qmail@fiver.freemessage.com (October 14, 2004).

[13] E-Soft Inc. “SecuritySpace – CVE-2000-0573.” Vulnerability Search. URL: http://www.securityspace.com/smysecure/catid.html?ctype=cve&id=CVE-2000-0573 (October 14, 2004).

[14] Thuemmel, Andreas. “Analysis of Format String Bugs.” Version 1.0. February 15, 2001. URL: http://downloads.securityfocus.com/library/format-bug-analysis.pdf (November 9, 2004).

[15] Testart, Jason. “Analysis of October’s Scan of the Month (Scan 19).” URL: http://www.honeynet.org/scans/scan19/scan/som10/scan19.html (October 14, 2004).

[16] Church, Joseph B. “SANS Intrusion Detection & Analysis Certification.” July 10, 2000. URL: http://www.giac.org/practical/Joe_Church_GCIA.doc (October 14, 2004).

[17] Compton, Chris. “Data Visualization for the Intrusion Analyst.” February 22, 2004. URL: http://www.giac.org/practical/GCIA/Chris_Compton_GCIA.pdf (October 14, 2004).

[18] Patel, Hitendra. “GIAC Certified Intrusion Analyst (GCIA) Practical Assignment Version 3.4.” March 2, 2004. URL: http://www.giac.org/practical/GCIA/Hitendra_Patel_GCIA.pdf (October 14, 2004).

[19] Snort. “FTP Passwd Retrieval Attempt.” URL: http://www.snort.org/snort-db/sid.html?sid=356 (October 15, 2004).

[20] Snort. “FTP Shadow Retrieval Attempt.” URL: http://www.snort.org/snort-db/sid.html?sid=1928 (October 15, 2004).

[21] Lalla, Gregory. “GCIA Intrusion Detection Practical v3.4.” January 19, 2004. URL: http://www.giac.org/practical/GCIA/Gregory_Lalla_GCIA.pdf (October 17, 2004).

[22] Software Engineering Lab. “Man Page for Rsh.” January 31, 2003. URL: http://www.doc.ic.ac.uk/lab/labman/lookup-man.cgi?rsh(1) (October 27, 2004).

[23] Snort. “Rservices Rsh Froot.” URL: http://www.snort.org/snort-db/sid.html?sid=604 (October 18, 2004).

[24] CVE. “CVE-1999-0113.” Common Vulnerabilities and Exposures. CVE Version: 20040901. URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0113 (October 18, 2004).

[25] Internet Security Systems, Inc. “Rlogin -Froot Command Could Allow Remote Root Access.” May 1, 1994. URL: http://xforce.iss.net/xforce/xfdb/104 (October 18, 2004).

[26] CERT® Coordination Center. “CERT® Advisory CA-1994-09 /bin/login Vulnerability.” March 10, 1998. URL: http://www.cert.org/advisories/CA-1994-09.html (October 11, 2004).

[27] Wedaa, Eric. “-Froot??? (AIX Rlogin Bug).” July 29, 1994. URL: http://archives.neohapsis.com/archives/bugtraq/1994_3/0098.html (October 27, 2004).

[28] Scheuern, Mark G. “Re: -Froot??? (AIX Rlogin Bug).” July 30, 1994. URL: http://archives.neohapsis.com/archives/bugtraq/1994_3/0100.html (October 27, 2004).

[29] Eppert, Aaron. “Re: -Froot??? (AIX Rlogin Bug).” July 29, 1994. URL: http://archives.neohapsis.com/archives/bugtraq/1994_3/0101.html (October 27, 2004).

[30] SANS Institute. “SANS/FBI Top 20 List.” Version 3.23. May 29, 2003. URL: http://www.sans.org/top20/oct02.php (October 27, 2004).

[31] Internet Security Systems, Inc. “Rlogin -Froot Backdoor.” Advice: 2002101. URL: http://www.iss.net/security_center/advice/Intrusions/2002101/default.htm (October 27, 2004).

[32] Internet Assigned Numbers Authority. “Port Numbers.” October 26, 2004. URL: http://www.iana.org/assignments/port-numbers (October 28, 2004).

[33] American Registry for Internet Numbers. “ARIN WHOIS Database Search.” URL: http://www.arin.net/whois/ (October29, 2004).

Appendix 1

Source IP Address List

10.10.10.1	10.10.10.147	10.10.10.212	10.30.30.2	172.20.201.1	192.168.17.68
10.10.10.111	10.10.10.160	10.10.10.214	169.254.135.50	172.20.201.135	192.168.213.1
10.10.10.112	10.10.10.164	10.10.10.222	172.16.8.189	172.20.201.198	192.168.22.207
10.10.10.113	10.10.10.165	10.10.10.224	172.16.8.229	172.20.201.2	192.168.222.1
10.10.10.117	10.10.10.174	10.10.10.226	172.16.9.13	192.168.117.1	192.168.84.1
10.10.10.122	10.10.10.186	10.10.10.228	172.20.11.1	192.168.17.129	238.122.10.140
10.10.10.123	10.10.10.194	10.10.10.230	172.20.11.2	192.168.17.135	
10.10.10.141	10.10.10.195	10.10.10.231	172.20.11.3	192.168.17.2	
10.10.10.142	10.10.10.196	10.10.10.232	172.20.11.52	192.168.17.65	
10.10.10.144	10.10.10.2	10.10.10.234	172.20.11.80	192.168.17.66	

Destination IP Address List

10.10.10.111	172.20.11.70	172.20.12.79	172.20.201.87	172.22.201.95	192.168.22.102
10.10.10.112	172.20.11.71	172.20.12.8	172.20.201.88	172.22.201.96	192.168.22.103
10.10.10.113	172.20.11.72	172.20.12.80	172.20.201.89	172.22.201.97	192.168.22.104
10.10.10.117	172.20.11.73	172.20.12.81	172.20.201.9	172.22.201.98	192.168.22.105
10.10.10.122	172.20.11.74	172.20.12.82	172.20.201.90	172.22.201.99	192.168.22.106
10.10.10.123	172.20.11.75	172.20.12.83	172.20.201.91	172.27.1.8	192.168.22.107
10.10.10.141	172.20.11.76	172.20.12.84	172.20.201.92	192.168.17.1	192.168.22.108
10.10.10.142	172.20.11.77	172.20.12.85	172.20.201.93	192.168.17.10	192.168.22.109
10.10.10.147	172.20.11.78	172.20.12.86	172.20.201.94	192.168.17.100	192.168.22.11
10.10.10.160	172.20.11.79	172.20.12.87	172.20.201.95	192.168.17.101	192.168.22.110
10.10.10.164	172.20.11.8	172.20.12.88	172.20.201.96	192.168.17.102	192.168.22.111
10.10.10.165	172.20.11.80	172.20.12.89	172.20.201.97	192.168.17.103	192.168.22.112
10.10.10.174	172.20.11.81	172.20.12.9	172.20.201.98	192.168.17.104	192.168.22.113
10.10.10.186	172.20.11.82	172.20.12.90	172.20.201.99	192.168.17.105	192.168.22.114
10.10.10.194	172.20.11.83	172.20.12.91	172.22.201.1	192.168.17.106	192.168.22.115
10.10.10.195	172.20.11.84	172.20.12.92	172.22.201.10	192.168.17.107	192.168.22.116
10.10.10.196	172.20.11.85	172.20.12.93	172.22.201.100	192.168.17.108	192.168.22.117
10.10.10.2	172.20.11.86	172.20.12.94	172.22.201.101	192.168.17.109	192.168.22.118
10.10.10.212	172.20.11.87	172.20.12.95	172.22.201.102	192.168.17.11	192.168.22.119
10.10.10.214	172.20.11.88	172.20.12.96	172.22.201.103	192.168.17.110	192.168.22.12
10.10.10.222	172.20.11.89	172.20.12.97	172.22.201.104	192.168.17.111	192.168.22.120

10.10.10.224	172.20.11.9	172.20.12.98	172.22.201.105	192.168.17.112	192.168.22.121
10.10.10.226	172.20.11.90	172.20.12.99	172.22.201.106	192.168.17.113	192.168.22.122
10.10.10.228	172.20.11.91	172.20.201.0	172.22.201.107	192.168.17.114	192.168.22.123
10.10.10.230	172.20.11.92	172.20.201.1	172.22.201.108	192.168.17.115	192.168.22.124
10.10.10.231	172.20.11.93	172.20.201.10	172.22.201.109	192.168.17.116	192.168.22.125
10.10.10.232	172.20.11.94	172.20.201.100	172.22.201.11	192.168.17.117	192.168.22.126
10.10.10.234	172.20.11.95	172.20.201.101	172.22.201.110	192.168.17.118	192.168.22.127
10.10.10.255	172.20.11.96	172.20.201.102	172.22.201.111	192.168.17.119	192.168.22.128
10.3.200.84	172.20.11.97	172.20.201.103	172.22.201.112	192.168.17.12	192.168.22.129
102.168.17.62	172.20.11.98	172.20.201.104	172.22.201.113	192.168.17.120	192.168.22.13
12.162.170.196	172.20.11.99	172.20.201.105	172.22.201.114	192.168.17.121	192.168.22.130
127.0.0.1	172.20.12.1	172.20.201.106	172.22.201.115	192.168.17.122	192.168.22.131
134.248.127.21	172.20.12.10	172.20.201.107	172.22.201.116	192.168.17.123	192.168.22.132
149.134.30.62	172.20.12.100	172.20.201.108	172.22.201.117	192.168.17.124	192.168.22.133
149.134.52.149	172.20.12.101	172.20.201.109	172.22.201.118	192.168.17.125	192.168.22.134
169.254.255.255	172.20.12.102	172.20.201.11	172.22.201.119	192.168.17.126	192.168.22.135
172.10.11.80	172.20.12.103	172.20.201.110	172.22.201.12	192.168.17.127	192.168.22.136
172.11.11.80	172.20.12.104	172.20.201.111	172.22.201.120	192.168.17.128	192.168.22.137
172.20.102.198	172.20.12.105	172.20.201.112	172.22.201.121	192.168.17.129	192.168.22.138
172.20.11.0	172.20.12.106	172.20.201.113	172.22.201.122	192.168.17.13	192.168.22.139
172.20.11.1	172.20.12.107	172.20.201.114	172.22.201.123	192.168.17.130	192.168.22.14
172.20.11.10	172.20.12.108	172.20.201.115	172.22.201.124	192.168.17.131	192.168.22.140
172.20.11.100	172.20.12.109	172.20.201.116	172.22.201.125	192.168.17.132	192.168.22.141
172.20.11.101	172.20.12.11	172.20.201.117	172.22.201.126	192.168.17.133	192.168.22.142
172.20.11.102	172.20.12.110	172.20.201.118	172.22.201.127	192.168.17.134	192.168.22.143
172.20.11.103	172.20.12.111	172.20.201.119	172.22.201.128	192.168.17.135	192.168.22.144
172.20.11.104	172.20.12.112	172.20.201.12	172.22.201.129	192.168.17.136	192.168.22.145
172.20.11.105	172.20.12.113	172.20.201.120	172.22.201.13	192.168.17.137	192.168.22.146
172.20.11.106	172.20.12.114	172.20.201.121	172.22.201.130	192.168.17.138	192.168.22.147
172.20.11.107	172.20.12.115	172.20.201.122	172.22.201.131	192.168.17.139	192.168.22.148
172.20.11.108	172.20.12.116	172.20.201.123	172.22.201.132	192.168.17.14	192.168.22.149
172.20.11.109	172.20.12.117	172.20.201.124	172.22.201.133	192.168.17.140	192.168.22.15
172.20.11.11	172.20.12.118	172.20.201.125	172.22.201.134	192.168.17.141	192.168.22.150
172.20.11.110	172.20.12.119	172.20.201.126	172.22.201.135	192.168.17.142	192.168.22.151
172.20.11.111	172.20.12.12	172.20.201.127	172.22.201.136	192.168.17.143	192.168.22.152
172.20.11.112	172.20.12.120	172.20.201.128	172.22.201.137	192.168.17.144	192.168.22.153
172.20.11.113	172.20.12.121	172.20.201.129	172.22.201.138	192.168.17.145	192.168.22.154
172.20.11.114	172.20.12.122	172.20.201.13	172.22.201.139	192.168.17.146	192.168.22.155
172.20.11.115	172.20.12.123	172.20.201.130	172.22.201.14	192.168.17.147	192.168.22.156
172.20.11.116	172.20.12.124	172.20.201.131	172.22.201.140	192.168.17.148	192.168.22.157
172.20.11.117	172.20.12.125	172.20.201.132	172.22.201.141	192.168.17.149	192.168.22.158
172.20.11.118	172.20.12.126	172.20.201.133	172.22.201.142	192.168.17.15	192.168.22.159
172.20.11.119	172.20.12.127	172.20.201.134	172.22.201.143	192.168.17.150	192.168.22.16
172.20.11.12	172.20.12.128	172.20.201.135	172.22.201.144	192.168.17.151	192.168.22.160
172.20.11.120	172.20.12.129	172.20.201.136	172.22.201.145	192.168.17.152	192.168.22.161
172.20.11.121	172.20.12.13	172.20.201.137	172.22.201.146	192.168.17.153	192.168.22.162
172.20.11.122	172.20.12.130	172.20.201.138	172.22.201.147	192.168.17.154	192.168.22.163
172.20.11.123	172.20.12.131	172.20.201.139	172.22.201.148	192.168.17.155	192.168.22.164
172.20.11.124	172.20.12.132	172.20.201.14	172.22.201.149	192.168.17.156	192.168.22.165
172.20.11.125	172.20.12.133	172.20.201.140	172.22.201.15	192.168.17.157	192.168.22.166
172.20.11.126	172.20.12.134	172.20.201.141	172.22.201.150	192.168.17.158	192.168.22.167
172.20.11.127	172.20.12.135	172.20.201.142	172.22.201.151	192.168.17.159	192.168.22.168
172.20.11.128	172.20.12.136	172.20.201.143	172.22.201.152	192.168.17.16	192.168.22.169
172.20.11.129	172.20.12.137	172.20.201.144	172.22.201.153	192.168.17.160	192.168.22.17
172.20.11.13	172.20.12.138	172.20.201.145	172.22.201.154	192.168.17.161	192.168.22.170
172.20.11.130	172.20.12.139	172.20.201.146	172.22.201.155	192.168.17.162	192.168.22.171
172.20.11.131	172.20.12.14	172.20.201.147	172.22.201.156	192.168.17.163	192.168.22.172
172.20.11.132	172.20.12.140	172.20.201.148	172.22.201.157	192.168.17.164	192.168.22.173
172.20.11.133	172.20.12.141	172.20.201.149	172.22.201.158	192.168.17.165	192.168.22.174
172.20.11.134	172.20.12.142	172.20.201.15	172.22.201.159	192.168.17.166	192.168.22.175
172.20.11.135	172.20.12.143	172.20.201.150	172.22.201.16	192.168.17.167	192.168.22.176
172.20.11.136	172.20.12.144	172.20.201.151	172.22.201.160	192.168.17.168	192.168.22.177

172.20.11.137	172.20.12.145	172.20.201.152	172.22.201.161	192.168.17.169	192.168.22.178
172.20.11.138	172.20.12.146	172.20.201.153	172.22.201.162	192.168.17.17	192.168.22.179
172.20.11.139	172.20.12.147	172.20.201.154	172.22.201.163	192.168.17.170	192.168.22.18
172.20.11.14	172.20.12.148	172.20.201.155	172.22.201.164	192.168.17.171	192.168.22.180
172.20.11.140	172.20.12.149	172.20.201.156	172.22.201.165	192.168.17.172	192.168.22.181
172.20.11.141	172.20.12.15	172.20.201.157	172.22.201.166	192.168.17.173	192.168.22.182
172.20.11.142	172.20.12.150	172.20.201.158	172.22.201.167	192.168.17.174	192.168.22.183
172.20.11.143	172.20.12.151	172.20.201.159	172.22.201.168	192.168.17.175	192.168.22.184
172.20.11.144	172.20.12.152	172.20.201.16	172.22.201.169	192.168.17.176	192.168.22.185
172.20.11.145	172.20.12.153	172.20.201.160	172.22.201.17	192.168.17.177	192.168.22.186
172.20.11.146	172.20.12.154	172.20.201.161	172.22.201.170	192.168.17.178	192.168.22.187
172.20.11.147	172.20.12.155	172.20.201.162	172.22.201.171	192.168.17.179	192.168.22.188
172.20.11.148	172.20.12.156	172.20.201.163	172.22.201.172	192.168.17.18	192.168.22.189
172.20.11.149	172.20.12.157	172.20.201.164	172.22.201.173	192.168.17.180	192.168.22.19
172.20.11.15	172.20.12.158	172.20.201.165	172.22.201.174	192.168.17.181	192.168.22.190
172.20.11.150	172.20.12.159	172.20.201.166	172.22.201.175	192.168.17.182	192.168.22.191
172.20.11.151	172.20.12.16	172.20.201.167	172.22.201.176	192.168.17.183	192.168.22.192
172.20.11.152	172.20.12.160	172.20.201.168	172.22.201.177	192.168.17.184	192.168.22.193
172.20.11.153	172.20.12.161	172.20.201.169	172.22.201.178	192.168.17.185	192.168.22.194
172.20.11.154	172.20.12.162	172.20.201.17	172.22.201.179	192.168.17.186	192.168.22.195
172.20.11.155	172.20.12.163	172.20.201.170	172.22.201.18	192.168.17.187	192.168.22.196
172.20.11.156	172.20.12.164	172.20.201.171	172.22.201.180	192.168.17.188	192.168.22.197
172.20.11.157	172.20.12.165	172.20.201.172	172.22.201.181	192.168.17.189	192.168.22.198
172.20.11.158	172.20.12.166	172.20.201.173	172.22.201.182	192.168.17.19	192.168.22.199
172.20.11.159	172.20.12.167	172.20.201.174	172.22.201.183	192.168.17.190	192.168.22.2
172.20.11.16	172.20.12.168	172.20.201.175	172.22.201.184	192.168.17.191	192.168.22.20
172.20.11.160	172.20.12.169	172.20.201.176	172.22.201.185	192.168.17.192	192.168.22.200
172.20.11.161	172.20.12.17	172.20.201.177	172.22.201.186	192.168.17.193	192.168.22.201
172.20.11.162	172.20.12.170	172.20.201.178	172.22.201.187	192.168.17.194	192.168.22.202
172.20.11.163	172.20.12.171	172.20.201.179	172.22.201.188	192.168.17.195	192.168.22.203
172.20.11.164	172.20.12.172	172.20.201.18	172.22.201.189	192.168.17.196	192.168.22.204
172.20.11.165	172.20.12.173	172.20.201.180	172.22.201.19	192.168.17.197	192.168.22.205
172.20.11.166	172.20.12.174	172.20.201.181	172.22.201.190	192.168.17.198	192.168.22.206
172.20.11.167	172.20.12.175	172.20.201.182	172.22.201.191	192.168.17.199	192.168.22.207
172.20.11.168	172.20.12.176	172.20.201.183	172.22.201.192	192.168.17.2	192.168.22.208
172.20.11.169	172.20.12.177	172.20.201.184	172.22.201.193	192.168.17.20	192.168.22.209
172.20.11.17	172.20.12.178	172.20.201.185	172.22.201.194	192.168.17.200	192.168.22.21
172.20.11.170	172.20.12.179	172.20.201.186	172.22.201.195	192.168.17.201	192.168.22.210
172.20.11.171	172.20.12.18	172.20.201.187	172.22.201.196	192.168.17.202	192.168.22.211
172.20.11.172	172.20.12.180	172.20.201.188	172.22.201.197	192.168.17.203	192.168.22.212
172.20.11.173	172.20.12.181	172.20.201.189	172.22.201.198	192.168.17.204	192.168.22.213
172.20.11.174	172.20.12.182	172.20.201.19	172.22.201.199	192.168.17.205	192.168.22.214
172.20.11.175	172.20.12.183	172.20.201.190	172.22.201.2	192.168.17.206	192.168.22.215
172.20.11.176	172.20.12.184	172.20.201.191	172.22.201.20	192.168.17.207	192.168.22.216
172.20.11.177	172.20.12.185	172.20.201.192	172.22.201.200	192.168.17.208	192.168.22.217
172.20.11.178	172.20.12.186	172.20.201.193	172.22.201.201	192.168.17.209	192.168.22.218
172.20.11.179	172.20.12.187	172.20.201.194	172.22.201.202	192.168.17.21	192.168.22.219
172.20.11.18	172.20.12.188	172.20.201.195	172.22.201.203	192.168.17.210	192.168.22.22
172.20.11.180	172.20.12.189	172.20.201.196	172.22.201.204	192.168.17.211	192.168.22.220
172.20.11.181	172.20.12.19	172.20.201.197	172.22.201.205	192.168.17.212	192.168.22.221
172.20.11.182	172.20.12.190	172.20.201.198	172.22.201.206	192.168.17.213	192.168.22.222
172.20.11.183	172.20.12.191	172.20.201.199	172.22.201.207	192.168.17.214	192.168.22.223
172.20.11.184	172.20.12.192	172.20.201.2	172.22.201.208	192.168.17.215	192.168.22.224
172.20.11.185	172.20.12.193	172.20.201.20	172.22.201.209	192.168.17.216	192.168.22.225
172.20.11.186	172.20.12.194	172.20.201.200	172.22.201.21	192.168.17.217	192.168.22.226
172.20.11.187	172.20.12.195	172.20.201.201	172.22.201.210	192.168.17.218	192.168.22.227
172.20.11.188	172.20.12.196	172.20.201.202	172.22.201.211	192.168.17.219	192.168.22.228
172.20.11.189	172.20.12.197	172.20.201.203	172.22.201.212	192.168.17.22	192.168.22.229
172.20.11.19	172.20.12.198	172.20.201.204	172.22.201.213	192.168.17.220	192.168.22.23
172.20.11.190	172.20.12.199	172.20.201.205	172.22.201.214	192.168.17.221	192.168.22.230
172.20.11.191	172.20.12.2	172.20.201.206	172.22.201.215	192.168.17.222	192.168.22.231
172.20.11.192	172.20.12.20	172.20.201.207	172.22.201.216	192.168.17.223	192.168.22.232

172.20.11.193	172.20.12.200	172.20.201.208	172.22.201.217	192.168.17.224	192.168.22.233
172.20.11.194	172.20.12.201	172.20.201.209	172.22.201.218	192.168.17.225	192.168.22.234
172.20.11.195	172.20.12.202	172.20.201.21	172.22.201.219	192.168.17.226	192.168.22.235
172.20.11.196	172.20.12.203	172.20.201.210	172.22.201.22	192.168.17.227	192.168.22.236
172.20.11.197	172.20.12.204	172.20.201.211	172.22.201.220	192.168.17.228	192.168.22.237
172.20.11.198	172.20.12.205	172.20.201.212	172.22.201.221	192.168.17.229	192.168.22.238
172.20.11.199	172.20.12.206	172.20.201.213	172.22.201.222	192.168.17.23	192.168.22.239
172.20.11.2	172.20.12.207	172.20.201.214	172.22.201.223	192.168.17.230	192.168.22.24
172.20.11.20	172.20.12.208	172.20.201.215	172.22.201.224	192.168.17.231	192.168.22.240
172.20.11.200	172.20.12.209	172.20.201.216	172.22.201.225	192.168.17.232	192.168.22.241
172.20.11.201	172.20.12.21	172.20.201.217	172.22.201.226	192.168.17.233	192.168.22.242
172.20.11.202	172.20.12.210	172.20.201.218	172.22.201.227	192.168.17.234	192.168.22.243
172.20.11.203	172.20.12.211	172.20.201.219	172.22.201.228	192.168.17.235	192.168.22.244
172.20.11.204	172.20.12.212	172.20.201.22	172.22.201.229	192.168.17.236	192.168.22.245
172.20.11.205	172.20.12.213	172.20.201.220	172.22.201.23	192.168.17.237	192.168.22.246
172.20.11.206	172.20.12.214	172.20.201.221	172.22.201.230	192.168.17.238	192.168.22.247
172.20.11.207	172.20.12.215	172.20.201.222	172.22.201.231	192.168.17.239	192.168.22.248
172.20.11.208	172.20.12.216	172.20.201.223	172.22.201.232	192.168.17.24	192.168.22.249
172.20.11.209	172.20.12.217	172.20.201.224	172.22.201.233	192.168.17.240	192.168.22.25
172.20.11.21	172.20.12.218	172.20.201.225	172.22.201.234	192.168.17.241	192.168.22.250
172.20.11.210	172.20.12.219	172.20.201.226	172.22.201.235	192.168.17.242	192.168.22.251
172.20.11.211	172.20.12.22	172.20.201.227	172.22.201.236	192.168.17.243	192.168.22.252
172.20.11.212	172.20.12.220	172.20.201.228	172.22.201.237	192.168.17.244	192.168.22.253
172.20.11.213	172.20.12.221	172.20.201.229	172.22.201.238	192.168.17.245	192.168.22.254
172.20.11.214	172.20.12.222	172.20.201.23	172.22.201.239	192.168.17.246	192.168.22.26
172.20.11.215	172.20.12.223	172.20.201.230	172.22.201.24	192.168.17.247	192.168.22.27
172.20.11.216	172.20.12.224	172.20.201.231	172.22.201.240	192.168.17.248	192.168.22.28
172.20.11.217	172.20.12.225	172.20.201.232	172.22.201.241	192.168.17.249	192.168.22.29
172.20.11.218	172.20.12.226	172.20.201.233	172.22.201.242	192.168.17.25	192.168.22.3
172.20.11.219	172.20.12.227	172.20.201.234	172.22.201.243	192.168.17.250	192.168.22.30
172.20.11.22	172.20.12.228	172.20.201.235	172.22.201.244	192.168.17.251	192.168.22.31
172.20.11.220	172.20.12.229	172.20.201.236	172.22.201.245	192.168.17.252	192.168.22.32
172.20.11.221	172.20.12.23	172.20.201.237	172.22.201.246	192.168.17.253	192.168.22.33
172.20.11.222	172.20.12.230	172.20.201.238	172.22.201.247	192.168.17.254	192.168.22.34
172.20.11.223	172.20.12.231	172.20.201.239	172.22.201.248	192.168.17.26	192.168.22.35
172.20.11.224	172.20.12.232	172.20.201.24	172.22.201.249	192.168.17.27	192.168.22.36
172.20.11.225	172.20.12.233	172.20.201.240	172.22.201.25	192.168.17.28	192.168.22.37
172.20.11.226	172.20.12.234	172.20.201.241	172.22.201.250	192.168.17.29	192.168.22.38
172.20.11.227	172.20.12.235	172.20.201.242	172.22.201.251	192.168.17.3	192.168.22.39
172.20.11.228	172.20.12.236	172.20.201.243	172.22.201.252	192.168.17.30	192.168.22.4
172.20.11.229	172.20.12.237	172.20.201.244	172.22.201.253	192.168.17.31	192.168.22.40
172.20.11.23	172.20.12.238	172.20.201.245	172.22.201.254	192.168.17.32	192.168.22.41
172.20.11.230	172.20.12.239	172.20.201.246	172.22.201.255	192.168.17.33	192.168.22.42
172.20.11.231	172.20.12.24	172.20.201.247	172.22.201.26	192.168.17.34	192.168.22.43
172.20.11.232	172.20.12.240	172.20.201.248	172.22.201.27	192.168.17.35	192.168.22.44
172.20.11.233	172.20.12.241	172.20.201.249	172.22.201.28	192.168.17.36	192.168.22.45
172.20.11.234	172.20.12.242	172.20.201.25	172.22.201.29	192.168.17.37	192.168.22.46
172.20.11.235	172.20.12.243	172.20.201.250	172.22.201.3	192.168.17.38	192.168.22.47
172.20.11.236	172.20.12.244	172.20.201.251	172.22.201.30	192.168.17.39	192.168.22.48
172.20.11.237	172.20.12.245	172.20.201.252	172.22.201.31	192.168.17.4	192.168.22.49
172.20.11.238	172.20.12.246	172.20.201.253	172.22.201.32	192.168.17.40	192.168.22.5
172.20.11.239	172.20.12.247	172.20.201.254	172.22.201.33	192.168.17.41	192.168.22.50
172.20.11.24	172.20.12.248	172.20.201.26	172.22.201.34	192.168.17.42	192.168.22.51
172.20.11.240	172.20.12.249	172.20.201.27	172.22.201.35	192.168.17.43	192.168.22.52
172.20.11.241	172.20.12.25	172.20.201.28	172.22.201.36	192.168.17.44	192.168.22.53
172.20.11.242	172.20.12.250	172.20.201.29	172.22.201.37	192.168.17.45	192.168.22.54
172.20.11.243	172.20.12.251	172.20.201.3	172.22.201.38	192.168.17.46	192.168.22.55
172.20.11.244	172.20.12.252	172.20.201.30	172.22.201.39	192.168.17.47	192.168.22.56
172.20.11.245	172.20.12.253	172.20.201.31	172.22.201.4	192.168.17.48	192.168.22.57
172.20.11.246	172.20.12.254	172.20.201.32	172.22.201.40	192.168.17.49	192.168.22.58
172.20.11.247	172.20.12.255	172.20.201.33	172.22.201.41	192.168.17.5	192.168.22.59
172.20.11.248	172.20.12.26	172.20.201.34	172.22.201.42	192.168.17.50	192.168.22.6

172.20.11.249	172.20.12.27	172.20.201.35	172.22.201.43	192.168.17.51	192.168.22.60
172.20.11.25	172.20.12.28	172.20.201.36	172.22.201.44	192.168.17.52	192.168.22.61
172.20.11.250	172.20.12.29	172.20.201.37	172.22.201.45	192.168.17.53	192.168.22.62
172.20.11.251	172.20.12.3	172.20.201.38	172.22.201.46	192.168.17.54	192.168.22.63
172.20.11.252	172.20.12.30	172.20.201.39	172.22.201.47	192.168.17.55	192.168.22.64
172.20.11.253	172.20.12.31	172.20.201.4	172.22.201.48	192.168.17.56	192.168.22.65
172.20.11.254	172.20.12.32	172.20.201.40	172.22.201.49	192.168.17.57	192.168.22.66
172.20.11.255	172.20.12.33	172.20.201.41	172.22.201.5	192.168.17.58	192.168.22.67
172.20.11.26	172.20.12.34	172.20.201.42	172.22.201.50	192.168.17.59	192.168.22.68
172.20.11.27	172.20.12.35	172.20.201.43	172.22.201.51	192.168.17.6	192.168.22.69
172.20.11.28	172.20.12.36	172.20.201.44	172.22.201.52	192.168.17.60	192.168.22.7
172.20.11.29	172.20.12.37	172.20.201.45	172.22.201.53	192.168.17.61	192.168.22.70
172.20.11.3	172.20.12.38	172.20.201.46	172.22.201.54	192.168.17.62	192.168.22.71
172.20.11.30	172.20.12.39	172.20.201.47	172.22.201.55	192.168.17.63	192.168.22.72
172.20.11.31	172.20.12.4	172.20.201.48	172.22.201.56	192.168.17.64	192.168.22.73
172.20.11.32	172.20.12.40	172.20.201.49	172.22.201.57	192.168.17.65	192.168.22.74
172.20.11.33	172.20.12.41	172.20.201.5	172.22.201.58	192.168.17.66	192.168.22.75
172.20.11.34	172.20.12.42	172.20.201.50	172.22.201.59	192.168.17.67	192.168.22.76
172.20.11.35	172.20.12.43	172.20.201.51	172.22.201.6	192.168.17.68	192.168.22.77
172.20.11.36	172.20.12.44	172.20.201.52	172.22.201.60	192.168.17.69	192.168.22.78
172.20.11.37	172.20.12.45	172.20.201.53	172.22.201.61	192.168.17.7	192.168.22.79
172.20.11.38	172.20.12.46	172.20.201.54	172.22.201.62	192.168.17.70	192.168.22.8
172.20.11.39	172.20.12.47	172.20.201.55	172.22.201.63	192.168.17.71	192.168.22.80
172.20.11.4	172.20.12.48	172.20.201.56	172.22.201.64	192.168.17.72	192.168.22.81
172.20.11.40	172.20.12.49	172.20.201.57	172.22.201.65	192.168.17.73	192.168.22.82
172.20.11.41	172.20.12.5	172.20.201.58	172.22.201.66	192.168.17.74	192.168.22.83
172.20.11.42	172.20.12.50	172.20.201.59	172.22.201.67	192.168.17.75	192.168.22.84
172.20.11.43	172.20.12.51	172.20.201.6	172.22.201.68	192.168.17.76	192.168.22.85
172.20.11.44	172.20.12.52	172.20.201.60	172.22.201.69	192.168.17.77	192.168.22.86
172.20.11.45	172.20.12.53	172.20.201.61	172.22.201.7	192.168.17.78	192.168.22.87
172.20.11.46	172.20.12.54	172.20.201.62	172.22.201.70	192.168.17.79	192.168.22.88
172.20.11.47	172.20.12.55	172.20.201.63	172.22.201.71	192.168.17.8	192.168.22.89
172.20.11.48	172.20.12.56	172.20.201.64	172.22.201.72	192.168.17.80	192.168.22.9
172.20.11.49	172.20.12.57	172.20.201.65	172.22.201.73	192.168.17.81	192.168.22.90
172.20.11.5	172.20.12.58	172.20.201.66	172.22.201.74	192.168.17.82	192.168.22.91
172.20.11.50	172.20.12.59	172.20.201.67	172.22.201.75	192.168.17.83	192.168.22.92
172.20.11.51	172.20.12.6	172.20.201.68	172.22.201.76	192.168.17.84	192.168.22.93
172.20.11.52	172.20.12.60	172.20.201.69	172.22.201.77	192.168.17.85	192.168.22.94
172.20.11.53	172.20.12.61	172.20.201.7	172.22.201.78	192.168.17.86	192.168.22.95
172.20.11.54	172.20.12.62	172.20.201.70	172.22.201.79	192.168.17.87	192.168.22.96
172.20.11.55	172.20.12.63	172.20.201.71	172.22.201.8	192.168.17.88	192.168.22.97
172.20.11.56	172.20.12.64	172.20.201.72	172.22.201.80	192.168.17.89	192.168.22.98
172.20.11.57	172.20.12.65	172.20.201.73	172.22.201.81	192.168.17.9	192.168.22.99
172.20.11.58	172.20.12.66	172.20.201.74	172.22.201.82	192.168.17.90	198.123.30.132
172.20.11.59	172.20.12.67	172.20.201.75	172.22.201.83	192.168.17.91	198.41.0.5
172.20.11.6	172.20.12.68	172.20.201.76	172.22.201.84	192.168.17.92	224.0.0.2
172.20.11.60	172.20.12.69	172.20.201.77	172.22.201.85	192.168.17.93	224.0.0.22
172.20.11.61	172.20.12.7	172.20.201.78	172.22.201.86	192.168.17.94	224.0.0.5
172.20.11.62	172.20.12.70	172.20.201.79	172.22.201.87	192.168.17.95	224.0.0.6
172.20.11.63	172.20.12.71	172.20.201.8	172.22.201.88	192.168.17.96	229.55.150.208
172.20.11.64	172.20.12.72	172.20.201.80	172.22.201.89	192.168.17.97	238.122.10.140
172.20.11.65	172.20.12.73	172.20.201.81	172.22.201.9	192.168.17.98	239.255.255.250
172.20.11.66	172.20.12.74	172.20.201.82	172.22.201.90	192.168.17.99	239.255.255.253
172.20.11.67	172.20.12.75	172.20.201.83	172.22.201.91	192.168.22.1	255.255.255.255
172.20.11.68	172.20.12.76	172.20.201.84	172.22.201.92	192.168.22.10	
172.20.11.69	172.20.12.77	172.20.201.85	172.22.201.93	192.168.22.100	
172.20.11.7	172.20.12.78	172.20.201.86	172.22.201.94	192.168.22.101	

Appendix 2

Source	Destination	Alert	# of Hit

10.10.10.165	10.10.10.2	(snort_decoder): Short UDP packet, length field > payload length	1
10.10.10.2	10.10.10.165	(snort_decoder): Short UDP packet, length field > payload length	19
10.10.10.165	10.10.10.255	(snort_decoder): Short UDP packet, length field > payload length	6
10.10.10.165	10.3.200.84	(snort_decoder): Short UDP packet, length field > payload length	12
10.10.10.165	172.20.201.0/24	(snort_decoder): Short UDP packet, length field > payload length	24
		SNMP public access udp	48
		SNMP request udp	98
		SNMP request tcp	21
		SNMP trap udp	40
		SNMP trap tcp	21
		SNMP AgentX/tcp request	10
		TFTP GET passwd	8
		TFTP Get	8
		FTP CWD ~ attempt	4
		FTP EXPLOIT STAT * dos attempt	8
		RPC sadmind UDP PING	6
		FTP SITE EXEC format string attempt	1
		DDOS Trin00 Master to Daemon default password attempt	3
		FTP format string attempt	1
		FINGER root query	2
		FINGER remote command execution attempt	2
		FINGER remote command pipe execution attempt	2
		FINGER redirection attempt	2
		FINGER 0 query	2
		FTP CWD ~root attempt	2
		FTP SITE EXEC attempt	5
		ICMP ISS Pinger	2501
		ICMP Nemesis v1.1 Echo	4
		ICMP PING NMAP	13
		TFTP parent directory	4
		TFTP root directory	4
		RSERVICES rsh froot	2
		SMTP expn decode	2
172.20.201.0/24	10.10.10.165	(snort_decoder): Short UDP packet, length field > payload length	31
		TELNET access	46
		TELNET login incorrect	2
10.10.10.165	192.168.17.0/24	(snort_decoder): Short UDP packet, length field > payload length	6
		(http_inspect) BARE BYTE UNICODE ENCODING	9
		SNMP public access udp	8
		SNMP request udp	16
		SNMP request tcp	16
		SNMP trap tcp	16
		SNMP AgentX/tcp request	8
		TFTP GET passwd	48
		TFTP Get	48
		ICMP ISS Pinger	1270

		ICMP Nemesis v1.1 Echo	44
		TFTP parent directory	24
		TFTP root directory	24
10.10.10.165	192.168.22.0/24	SNMP public access udp	2
		SNMP request udp	4
		SNMP request tcp	4
		SNMP trap tcp	4
		SNMP AgentX/tcp request	2
		TFTP GET passwd	12
		TFTP Get	12
		ICMP ISS Pinger	1270
		ICMP Nemesis v1.1 Echo	11
		TFTP parent directory	6
		TFTP root directory	6

Appendix 3

[Gen:Sid:Rev]	Alert	# of Hit
[1:623:5]	SCAN NULL	18162
[1:465:3]	ICMP ISS Pinger	5041
[116:97:1]	(snort_decoder): Short UDP packet, length field > payload length	1183
[1:474:4]	ICMP superscan echo	1020
[1:1417:9]	SNMP request udp	363
[1:1420:11]	SNMP trap tcp	156
[1:1418:11]	SNMP request tcp	150
[1:1421:11]	SNMP AgentX/tcp request	128
[1:1444:3]	TFTP Get	71
[1:1443:4]	TFTP GET passwd	70
[1:1411:10]	SNMP public access udp	60
[1:467:3]	ICMP Nemesis v1.1 Echo	59
[1:716:11]	TELNET access	57
[1:1419:9]	SNMP trap udp	46
[1:519:6]	TFTP parent directory	35
[1:520:5]	TFTP root directory	35
[1:1228:6]	SCAN nmap XMAS	24
[1:469:3]	ICMP PING NMAP	23
[1:361:14]	FTP SITE EXEC attempt	14
[1:524:8]	BAD-TRAFFIC tcp port 0 traffic	14
[1:2049:3]	MS-SQL ping attempt	12
[1:1413:10]	SNMP private access udp	10
[119:4:1]	(http_inspect) BARE BYTE UNICODE ENCODING	9
[1:1971:4]	FTP SITE EXEC format string attempt	9
[1:2417:1]	FTP format string attempt	9
[1:1777:5]	FTP EXPLOIT STAT * dos attempt	8
[1:1672:11]	FTP CWD ~ attempt	7
[105:1:1]	(spo_bo) Back Orifice Traffic detected	6

[1:1504:6]	MISC AFS access	6
[1:1867:1]	MISC xdmcp info query	6
[1:1893:4]	SNMP missing community string attempt	6
[1:1957:5]	RPC sadmind UDP PING	6
[1:528:5]	BAD-TRAFFIC loopback traffic	6
[1:1992:7]	FTP LIST directory traversal attempt	5
[1:237:2]	DDOS Trin00 Master to Daemon default password attempt	4
[1:336:10]	FTP CWD ~root attempt	4
[1:500:4]	MISC source route lssr	3
[1:501:4]	MISC source route lssre	3
[1:604:5]	RSERVICES rsh froot	3
[1:323:5]	FINGER root query	2
[1:326:9]	FINGER remote command execution attempt	2
[1:327:8]	FINGER remote command pipe execution attempt	2
[1:330:9]	FINGER redirection attempt	2
[1:332:8]	FINGER 0 query	2
[1:356:5]	FTP passwd retrieval attempt	2
[1:659:8]	SMTP expn decode	2
[1:718:7]	TELNET login incorrect	2
[1:1928:3]	FTP shadow retrieval attempt	1
[1:221:4]	DDOS TFN Probe	1
[1:236:6]	DDOS Stacheldraht client check gag	1
[1:239:2]	DDOS shaft handler to agent	1
[1:245:3]	DDOS mstream handler ping to agent	1
[1:255:12]	DNS zone transfer TCP	1
[1:335:5]	FTP .rhosts	1
[1:624:6]	SCAN SYN FIN	1
	Total	**26857**

Appendix 4

Alert	Impact	False Positive
(http_inspect) BARE BYTE UNICODE ENCODING		
(snort_decoder): Short UDP packet, length field > payload length		
(spo_bo) Back Orifice Traffic detected		
BAD-TRAFFIC loopback traffic	Possible reconnaissance.	None known
BAD-TRAFFIC tcp port 0 traffic	Possible reconnaissance. This may be an attempt to verify the existence of a host or hosts at a particular address or address range.	None known
DDOS mstream handler ping to agent	Severe. If the listed source IP is in your network, it may be an mstream handler. If the listed destination IP is in your network, it may be an mstream agent.	None known
DDOS shaft handler to	Attempted DDoS. If the listed source IP is in your network, it may	None known

agent	be a Shaft handler or a host attempting to discover Shaft agents. If the listed destination IP is in your network, it may be a Shaft agent.	
DDOS Stacheldraht client check gag	Severe. This indicates that a Stacheldraht handler may exist on the source host and an agent may exist on the destination host.	None known
DDOS TFN Probe	Reconnaissance. If the listed source IP is in your network, it may be a TFN attacker or it may be probing for another attacker's TFN clients. If the listed destination IP is in your network, it may be a TFN client.	None known
DDOS Trin00 Master to Daemon default password attempt	Attempted DDoS. If the listed source IP is in your network, it may be a trin00 master. If the listed destination IP is in your network, it may be a trin00 daemon.	None known
DNS zone transfer TCP	Information disclosure.	None known
FINGER 0 query	The attacker may obtain information about user accounts on the target system.	None known
FINGER redirection attempt	The attacker may obtain information about a third party host without making a direct connection to that host.	None known
FINGER remote command execution attempt	Serious. The attacker may be presented with the opportunity to run a command of his choice on the target UNIX system.	None known
FINGER remote command pipe execution attempt	Serious. The attacker may be presented with the opportunity to run a command of his choice on the target UNIX system.	None known
FINGER root query	The attacker may obtain detailed information about the administrative super user account.	None known
FTP .rhosts	Serious. An attacker might gain the ability to remotely connect to a server via r-commands without using a password.	If the string ".rhosts" is contained within the filename that is being uploaded to a server or within other FTP client responses, the rule will generate an event.
FTP CWD ~ attempt	Reconnaissance. An attacker may be able to examine records from the password shadow file.	None known
FTP CWD ~root attempt	Serious. Information disclosure.	None known
FTP EXPLOIT STAT * dos attempt	Severe. This vulnerability is remotely exploitable, and is present on systems that are widely deployed.	None known
FTP format string attempt	Varies from information gathering to a serious compromise of an ftp server.	None known
FTP LIST directory traversal attempt	Information disclosure. This is a directory traversal attempt which can lead to information disclosure and possible exposure of sensitive system information.	None known
FTP passwd retrieval attempt	Serious. The attacker may obtain a valid list of user names and/or encrypted passwords from the server.	If the string "passwd" is contained within an otherwise innocuous filename being retrieved from a server, the rule will generate an event. Also, the anonymous FTP account often has a separate password file within the chrooted anonymous FTP directory (e.g. /var/ftp/etc/passwd). This file does not usually contain valid system usernames and passwords. While technically not a false positive, this may be considered a false alarm.
FTP shadow retrieval attempt	Varies from information gathering to a serious compromise of an ftp server. To search for traffic.	None known
FTP SITE EXEC attempt	Arbitrary code execution, leading to remote root compromise. The attacker must have a valid, non-anonymous FTP account on the server to attempt this exploit.	None known

FTP SITE EXEC format string attempt	Severe. Remote root compromise possible if user is running a version of WU-FTPD prior to 2.6.2 as root.	None known
ICMP ISS Pinger	Information gathering. An ICMP echo request can determine if a host is active.	An ICMP echo request may be used to legitimately troubleshoot networking problems.
ICMP Nemesis v1.1 Echo	Information gathering. An ICMP echo request can determine if a host is active.	None known
ICMP PING NMAP	This could indicate a full scan by nmap which is sometimes indicative of potentially malicious behavior.	Possible. The only current identifying feature of nmap's ICMP ping is that the data size is 0. It is entirely possible that other tools may send ICMP pings with zero data. Kontiki delivery manager used on windows platforms to download multimedia files is known to produce ICMP pings that can cause this rule to generate many events. avast! Antivirus update feature is reported to produce ICMP pings with zero data when connecting to the avast servers. This can occur every 40 seconds if no reply is received by the client.
ICMP superscan echo	Information gathering.	Tools other than SuperScan may generate echo requests with the same content.
MISC AFS access	Serious. Unauthorized file access.	None known
MISC source route lssr	Information could be gathered about network topology, and machines routing packets onto trusted links could be abused.	None known
MISC source route lssre	Loose source routing permits the dictation of a route to and from the destination rather than relying on standard dynamic routing.	This even will trigger if you allow loose source routed packets into your network.
MISC xdmcp info query	Reconnaissance. An attacker may obtain a list of usernames on the remote host.	None
MS-SQL ping attempt	Disclosure of an instance of MS-SQL running on a host.	None known
RPC sadmind UDP PING	Intelligence gathering activity. The sadmind ping will verify if the daemon is running.	None known
RSERVICES rsh froot	Serious. If successful the attacker may have gained superuser access to the host.	None known
SCAN nmap XMAS	System reconnaissance that may include open/closed/firewalled ports, ACLs.	None Known. The FIN PSH and URG flags should never be seen together in normal TCP traffic.
SCAN NULL	Information regarding firewall rulesets, open/closed ports, ACLs, and possibly even OS type is possible. This technique can also be used to bypass certain firewalls or traffic filtering/shaping devices.	None known
SCAN SYN FIN	Information regarding firewall rulesets, open/closed ports, ACLs, and possibly even OS type is possible. This technique can also be used to bypass certain firewalls or traffic filtering/shaping devices.	None known
SMTP expn decode	Intelligence gathering activity. This event could be an indication of reconnaissance or an actual attempt to overwrite a sensitive file. If the decode alias is present on the SMTP server, an attacker may use it to overwrite files.	None known
SNMP AgentX/tcp request	Varies depending on the implementation. Ranges from Denial of Service (DoS) to code execution.	None known
SNMP missing community string attempt	Medium to Serious. Depending on if the community string was for read-only, read-create or read-write an attacker could gain a varying level of access to a system.	None known

SNMP private access udp	Information gathering	None known
SNMP public access udp	Information gathering	None known
SNMP request tcp	Information gathering	None known
SNMP request udp	Information gathering	None known
SNMP trap tcp	Information gathering	None known
SNMP trap udp	Information gathering	None known
TELNET access	Remote access. This event may be an indication of a successful telnet connection by an authorized or unauthorized user.	An attacker may attempt to connect to a telnet server after sniffing a username and password.
TELNET login incorrect	Attempted remote access. This event may indicate that an attacker is attempting to guess username and password combinations. Alternately, it may indicate that an authorized user has entered an incorrect username and password combination.	This event may be triggered by a failed telnet login attempt from a remote user.
TFTP Get		None known
TFTP GET passwd	The "passwd" file normally stores users names for Unix based systems. If this file is being transferred over the network using TFTP it is normally an indication of a system compromise. In some situations this rule may only indicate a generic TFTP scan attempt, as the attacker may be scanning a large range of IP addresses for TFTP improperly configured TFTP servers.	This rule was created to catch TFTP GET requests for "passwd"; if this file name is being used during a legitimate TFTP session this rule will generate a false positive.
TFTP parent directory	TFTP servers that allow files to be placed outside the configured root directory for the server may allow remote attackers to execute arbitrary commands on the system. Additionally if the TFTP server allows directory transversal using the ".." designator it may be possible to retrieve files from other directories on the system.	None known
TFTP root directory	TFTP servers that allow files to be placed outside the configured root directory for the server may allow remote attackers to execute arbitrary commands on the system. Additionally if the TFTP server allows directory transversal using the "/" designator it may be possible to retrieve files from other directories on the system.	None known

Appendix 5

Alert	Category	Severity
FTP SITE EXEC format string attempt	Buffer overflow	High
FTP format string attempt	Buffer overflow	High
FTP SITE EXEC attempt	Arbitrary command execution	High
SNMP AgentX/tcp request	Arbitrary command execution	High
TFTP parent directory	Arbitrary command execution	High
TFTP root directory	Arbitrary command execution	High
RSERVICES rsh froot	Privileged remote access	High
FTP .rhosts	Privileged remote access	High
FTP passwd retrieval attempt	Password retrieval	High
FTP shadow retrieval attempt	Password retrieval	High
TFTP GET passwd	Password retrieval	High
FINGER remote command execution attempt	Arbitrary command execution with users' privilege	Medium
FINGER remote command pipe execution attempt	Arbitrary command execution with users' privilege	Medium
DNS zone transfer TCP	Information disclosure	Medium

FTP CWD ~root attempt	Information disclosure	Medium
FTP LIST directory traversal attempt	Information disclosure	Medium
MISC AFS access	Information disclosure	Medium
MISC source route lssre	Information disclosure	Medium
MS-SQL ping attempt	Information disclosure	Medium
FTP EXPLOIT STAT * dos attempt	Attempted DoS	Medium
DDOS mstream handler ping to agent	Attempted DDoS	Medium
DDOS shaft handler to agent	Attempted DDoS	Medium
DDOS Stacheldraht client check gag	Attempted DDoS	Medium
DDOS TFN Probe	Attempted DDoS	Medium
DDOS Trin00 Master to Daemon default password attempt	Attempted DDoS	Medium
SNMP missing community string attempt	Access attempt	Medium
TELNET access	Access attempt	Medium
TELNET login incorrect	Access attempt	Medium
BAD-TRAFFIC loopback traffic	Information gathering	Low
BAD-TRAFFIC tcp port 0 traffic	Information gathering	Low
FINGER 0 query	Information gathering	Low
FINGER redirection attempt	Information gathering	Low
FINGER root query	Information gathering	Low
FTP CWD ~ attempt	Information gathering	Low
ICMP ISS Pinger	Information gathering	Low
ICMP Nemesis v1.1 Echo	Information gathering	Low
ICMP PING NMAP	Information gathering	Low
ICMP superscan echo	Information gathering	Low
MISC source route lssr	Information gathering	Low
MISC xdmcp info query	Information gathering	Low
RPC sadmind UDP PING	Information gathering	Low
SCAN nmap XMAS	Information gathering	Low
SCAN NULL	Information gathering	Low
SCAN SYN FIN	Information gathering	Low
SMTP expn decode	Information gathering	Low
SNMP private access udp	Information gathering	Low
SNMP public access udp	Information gathering	Low
SNMP request tcp	Information gathering	Low
SNMP request udp	Information gathering	Low
SNMP trap tcp	Information gathering	Low
SNMP trap udp	Information gathering	Low
(http_inspect) BARE BYTE UNICODE ENCODING	Unknown	Low
(snort_decoder): Short UDP packet, length field > payload length	Unknown	Low
(spo_bo) Back Orifice Traffic detected	Unknown	Low
TFTP Get	Unknown	Low

Appendix 6

[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]

11/18/03-15:04:32.812057 10.10.10.186:32802 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:37735 IpLen:20 DgmLen:76 DF
AP Seq: 0x15CC0B8C Ack: 0x367F26B5 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 956557 1892741
--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:07:22.279657 10.10.10.186:32805 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:33337 IpLen:20 DgmLen:76 DF
AP Seq: 0x216A6951 Ack: 0x4134EBA2 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1043340 1909682
--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:09:46.369311 10.10.10.186:32806 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:50984 IpLen:20 DgmLen:76 DF
AP Seq: 0x2A9ACC60 Ack: 0x4A30697D Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1117127 1924087
--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:13:59.495652 10.10.10.186:48253 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:7320 IpLen:20 DgmLen:76 DF
AP Seq: 0x3A83198E Ack: 0x59BDAB90 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1246751 1949388
--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:14:06.566384 10.10.10.196:52927 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:58960 IpLen:20 DgmLen:76 DF
AP Seq: 0x30958577 Ack: 0x59FEF9C9 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 7562077 1950094
--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:15:49.451015 10.10.10.165:3419 -> 172.20.201.135:21
TCP TTL:128 TOS:0x0 ID:21284 IpLen:20 DgmLen:64 DF
AP Seq: 0x3747A303 Ack: 0x51927484 Win: 0x4393 TcpLen: 20

--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:15:55.395214 10.10.10.196:52928 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:14395 IpLen:20 DgmLen:76 DF
AP Seq: 0x371504FD Ack: 0x614A002C Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 7617810 1960977
--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:21:22.209882 10.10.10.228:35886 -> 172.20.201.135:21
TCP TTL:64 TOS:0x0 ID:17681 IpLen:20 DgmLen:76 DF
AP Seq: 0x9BDB285C Ack: 0x65F595B6 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 355668 2547428
--
[**] [1:1971:4] FTP SITE EXEC format string attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
11/18/03-15:24:06.328937 10.10.10.186:48313 -> 172.20.201.198:21
TCP TTL:64 TOS:0x0 ID:35845 IpLen:20 DgmLen:76 DF
AP Seq: 0x5F9A4FDB Ack: 0x8050534A Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1557505 2010052

Appendix 7

```
15:04:32.581173 10.10.10.186.32802 > 172.20.201.198.21: S [tcp sum ok] 365693812:365693812(0) win
5840 <mss 1460,sackOK,timestamp 956438 0,nop,wscale 0> (DF) (ttl 64, id 37730, len 60)
0x0000   4500 003c 9362 4000 4006 1cbb 0a0a 0aba        E..<.b@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0b74 0000 0000        ....."....t....
0x0020   a002 16d0 6cfc 0000 0204 05b4 0402 080a        ....l...........
0x0030   000e 9816 0000 0000 0103 0300                  ............
15:04:32.588173 172.20.201.198.21 > 10.10.10.186.32802: S [tcp sum ok] 914302449:914302449(0) ack
365693813 win 32120 <mss 1460,sackOK,timestamp 1892719 956438,nop,wscale 0> (DF) (ttl 62, id 33480,
len 60)
0x0000   4500 003c 82c8 4000 3e06 2f55 ac14 c9c6        E..<..@.>./U....
0x0010   0a0a 0aba 0015 8022 367f 25f1 15cc 0b75        ......."6.%....u
0x0020   a012 7d78 c846 0000 0204 05b4 0402 080a        ..}x.F..........
0x0030   001c e16f 000e 9816 0103 0300                  ...o........
15:04:32.588434 10.10.10.186.32802 > 172.20.201.198.21: . [tcp sum ok] ack 914302450 win 5840
<nop,nop,timestamp 956442 1892719> (DF) (ttl 64, id 37731, len 52)
0x0000   4500 0034 9363 4000 4006 1cc2 0a0a 0abaE       ..4.c@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0b75 367f 25f2        ....."....u6.%.
0x0020   8010 16d0 5db0 0000 0101 080a 000e 981a        ....]...........
0x0030   001c e16f                                      ...o
15:04:32.771863 172.20.201.198.21 > 10.10.10.186.32802: P 914302450:914302529(79) ack 365693813
win 32120 <nop,nop,timestamp 1892737 956442> (DF) [tos 0x10]  (ttl 62, id 33492, len 131)
0x0000   4510 0083 82d4 4000 3e06 2ef2 ac14 c9c6        E.....@.>.......
0x0010   0a0a 0aba 0015 8022 367f 25f2 15cc 0b75        ......."6.%....u
0x0020   8018 7d78 a773 0000 0101 080a 001c e181        ..}x.s..........
0x0030   000e 981a 3232 3020 6c61 7a79 2046 5450        ....220.lazy.FTP
0x0040   2073 6572 7665 7220 2856 6572 7369 6f6e        .server.(Version
0x0050   2077                                           .w
15:04:32.772021 10.10.10.186.32802 > 172.20.201.198.21: . [tcp sum ok] ack 914302529 win 5840
<nop,nop,timestamp 956536 1892737> (DF) (ttl 64, id 37732, len 52)
0x0000   4500 0034 9364 4000 4006 1cc1 0a0a 0aba        E..4.d@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0b75 367f 2641        ....."....u6.&A
0x0020   8010 16d0 5cf1 0000 0101 080a 000e 9878        ....\..........x
0x0030   001c e181                                      ....
15:04:32.772664 10.10.10.186.32802 > 172.20.201.198.21: P [tcp sum ok] 365693813:365693822(9) ack
914302529 win 5840 <nop,nop,timestamp 956537 1892737> (DF) (ttl 64, id 37733, len 61)
0x0000   4500 003d 9365 4000 4006 1cb7 0a0a 0aba        E..=.e@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0b75 367f 2641        ....."....u6.&A
0x0020   8018 16d0 2363 0000 0101 080a 000e 9879        ....#c.........y
0x0030   001c e181 5553 4552 2066 7470 0a               ....USER.ftp.
15:04:32.781695 172.20.201.198.21 > 10.10.10.186.32802: . [tcp sum ok] ack 365693822 win 32120
<nop,nop,timestamp 1892738 956537> (DF) [tos 0x10]  (ttl 62, id 33494, len 52)
0x0000   4510 0034 82d6 4000 3e06 2f3f ac14 c9c6        E..4..@.>./?....
0x0010   0a0a 0aba 0015 8022 367f 2641 15cc 0b7e        ......."6.&A...~
0x0020   8010 7d78 f63d 0000 0101 080a 001c e182        ..}x.=..........
0x0030   000e 9879                                      ...y
15:04:32.799895 172.20.201.198.21 > 10.10.10.186.32802: P 914302529:914302597(68) ack 365693822
win 32120 <nop,nop,timestamp 1892740 956537> (DF) [tos 0x10]  (ttl 62, id 33496, len 120)
0x0000   4510 0078 82d8 4000 3e06 2ef9 ac14 c9c6        E..x..@.>.......
0x0010   0a0a 0aba 0015 8022 367f 2641 15cc 0b7e        ......."6.&A...~
0x0020   8018 7d78 0c4b 0000 0101 080a 001c e184        ..}x.K..........
0x0030   000e 9879 3333 3120 4775 6573 7420 6c6f        ...y331.Guest.lo
0x0040   6769 6e20 6f6b 2c20 7365 6e64 2079 6f75        gin.ok,.send.you
0x0050   7220                                           r.
15:04:32.800478 10.10.10.186.32802 > 172.20.201.198.21: P [tcp sum ok] 365693822:365693836(14) ack
914302597 win 5840 <nop,nop,timestamp 956551 1892740> (DF) (ttl 64, id 37734, len 66)
0x0000   4500 0042 9366 4000 4006 1cb1 0a0a 0aba        E..B.f@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0b7e 367f 2685        ....."....~6.&.
0x0020   8018 16d0 1328 0000 0101 080a 000e 9887        .....(..........
0x0030   001c e184 5041 5353 206d 6f7a 696c 6c61        ....PASS.mozilla
```

```
0x0040   400a                                      @.
15:04:32.811589 172.20.201.198.21 > 10.10.10.186.32802: P 914302597:914302645(48) ack 365693836
win 32120 <nop,nop,timestamp 1892741 956551> (DF) [tos 0x10]  (ttl 62, id 33498, len 100)
0x0000   4510 0064 82da 4000 3e06 2f0b ac14 c9c6   E..d..@.>./.....
0x0010   0a0a 0aba 0015 8022 367f 2685 15cc 0b8c   .......".6.&.....
0x0020   8018 7d78 49bc 0000 0101 080a 001c e185   ..}xI...........
0x0030   000e 9887 3233 3020 4775 6573 7420 6c6f   ....230.Guest.lo
0x0040   6769 6e20 6f6b 2c20 6163 6365 7373 2072   gin.ok,.access.r
0x0050   6573                                     es
15:04:32.812057 10.10.10.186.32802 > 172.20.201.198.21: P [tcp sum ok] 365693836:365693860(24) ack
914302645 win 5840 <nop,nop,timestamp 956557 1892741> (DF) (ttl 64, id 37735, len 76)
0x0000   4500 004c 9367 4000 4006 1ca6 0a0a 0aba   E..L.g@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0b8c 367f 26b5   ....."......6.&.
0x0020   8018 16d0 0753 0000 0101 080a 000e 988d   .....S..........
0x0030   001c e185 5349 5445 2045 5845 4320 2530   ....SITE.EXEC.%0
0x0040   3230 647c 252e 6625 2e66 7c0a             20d|%.f%.f|.
15:04:32.841367 172.20.201.198.21 > 10.10.10.186.32802: P 914302645:914302676(31) ack 365693860
win 32120 <nop,nop,timestamp 1892744 956557> (DF) [tos 0x10]  (ttl 62, id 33506, len 83)
0x0000   4510 0053 82e2 4000 3e06 2f14 ac14 c9c6   E..S..@.>./.....
0x0010   0a0a 0aba 0015 8022 367f 26b5 15cc 0ba4   .......".6.&.....
0x0020   8018 7d78 7daa 0000 0101 080a 001c e188   ..}x}...........
0x0030   000e 988d 3230 302d 3030 3030 3030 3030   ....200-00000000
0x0040   3030 3030 3030 3030 3030 3439 7c30 2d32   000000000049|0-2
0x0050   7c0d                                     |.
15:04:32.879928 10.10.10.186.32802 > 172.20.201.198.21: . [tcp sum ok] ack 914302676 win 5840
<nop,nop,timestamp 956592 1892744> (DF) (ttl 64, id 37736, len 52)
0x0000   4500 0034 9368 4000 4006 1cbd 0a0a 0aba   E..4.h@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0ba4 367f 26d4   ....."......6.&.
0x0020   8010 16d0 5bf0 0000 0101 080a 000e 98b0   ....[...........
0x0030   001c e188                                 ....
15:04:32.882851 172.20.201.198.21 > 10.10.10.186.32802: P 914302676:914302707(31) ack 365693860
win 32120 <nop,nop,timestamp 1892748 956592> (DF) [tos 0x10]  (ttl 62, id 33507, len 83)
0x0000   4510 0053 82e3 4000 3e06 2f13 ac14 c9c6   E..S..@.>./.....
0x0010   0a0a 0aba 0015 8022 367f 26d4 15cc 0ba4   .......".6.&.....
0x0020   8018 7d78 f4bc 0000 0101 080a 001c e18c   ..}x............
0x0030   000e 98b0 3230 3020 2028 656e 6420 6f66   ....200..(end.of
0x0040   2027 2530 3230 647c 252e 6625 2e66 7c27   .'%020d|%.f%.f|'
0x0050   290d                                     ).
15:04:32.883170 10.10.10.186.32802 > 172.20.201.198.21: . [tcp sum ok] ack 914302707 win 5840
<nop,nop,timestamp 956593 1892748> (DF) (ttl 64, id 37737, len 52)
0x0000   4500 0034 9369 4000 4006 1cbc 0a0a 0aba   E..4.i@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0ba4 367f 26f3   ....."......6.&.
0x0020   8010 16d0 5bcc 0000 0101 080a 000e 98b1   ....[...........
0x0030   001c e18c                                 ....
15:04:32.883447 10.10.10.186.32802 > 172.20.201.198.21: P 365693860:365694276(416) ack 914302707
win 5840 <nop,nop,timestamp 956593 1892748> (DF) (ttl 64, id 37738, len 468)
0x0000   4500 01d4 936a 4000 4006 1b1b 0a0a 0aba   E....j@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0ba4 367f 26f3   ....."......6.&.
0x0020   8018 16d0 9b17 0000 0101 080a 000e 98b1   ................
0x0030   001c e18c 5349 5445 2045 5845 4320 3720   ....SITE.EXEC.7.
0x0040   6d6d 6d6d 6e6e 6e6e 252e 6625 2e66 252e   mmmmnnnn%.f%.f%.
0x0050   6625                                     f%
15:04:32.892904 172.20.201.198.21 > 10.10.10.186.32802: P 914302707:914302894(187) ack 365694276
win 32120 <nop,nop,timestamp 1892749 956593> (DF) [tos 0x10]  (ttl 62, id 33508, len 239)
0x0000   4510 00ef 82e4 4000 3e06 2e76 ac14 c9c6   E.....@.>..v....
0x0010   0a0a 0aba 0015 8022 367f 26f3 15cc 0d44   .......".6.&....D
0x0020   8018 7d78 7c72 0000 0101 080a 001c e18d   ..}x|r..........
0x0030   000e 98b1 3230 302d 3720 6d6d 6d6d 6e6e   ....200-7.mmmmnn
0x0040   6e6e 2d32 2d32 3230 302d 3230 3730 3030   nn-2-2200-207000
0x0050   3030                                     00
15:04:32.930715 10.10.10.186.32802 > 172.20.201.198.21: . [tcp sum ok] ack 914302894 win 6432
<nop,nop,timestamp 956618 1892749> (DF) (ttl 64, id 37739, len 52)
```

```
0x0000   4500 0034 936b 4000 4006 1cba 0a0a 0aba      E..4.k@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0d44 367f 27ae      .....".....D6.'.
0x0020   8010 1920 5707 0000 0101 080a 000e 98ca      ....W...........
0x0030   001c e18d                                    ....
15:04:33.020609 172.20.201.198.21 > 10.10.10.186.32802: P 914302894:914303317(423) ack 365694276
win 32120 <nop,nop,timestamp 1892760 956618> (DF) [tos 0x10]  (ttl 62, id 33526, len 475)
0x0000   4510 01db 82f6 4000 3e06 2d78 ac14 c9c6      E.....@.>.-x....
0x0010   0a0a 0aba 0015 8022 367f 27ae 15cc 0d44      ......."6.'....D
0x0020   8018 7d78 8662 0000 0101 080a 001c e198      ..}x.b..........
0x0030   000e 98ca 3230 3020 2028 656e 6420 6f66      ....200..(end.of
0x0040   2027 3720 6d6d 6d6d 6e6e 6e6e 252e 6625      .'7.mmmmnnnn%.f%
0x0050   2e66                                        .f
15:04:33.020809 10.10.10.186.32802 > 172.20.201.198.21: . [tcp sum ok] ack 914303317 win 7504
<nop,nop,timestamp 956664 1892760> (DF) (ttl 64, id 37740, len 52)
0x0000   4500 0034 936c 4000 4006 1cb9 0a0a 0aba      E..4.l@.@.......
0x0010   ac14 c9c6 8022 0015 15cc 0d44 367f 2955      ....."....D6.)U
0x0020   8010 1d50 50f7 0000 0101 080a 000e 98f8      ...PP...........
0x0030   001c e198                                    ....
```

Appendix 8

```
15:15:00.370833 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690005:981690008(3) ack
1505645155 win 32736 <nop,nop,timestamp 1277925 1955158> (DF) (ttl 64, id 7456, len 55)
0x0000   4500 0037 1d20 4000 4006 9302 0a0a 0aba      E..7..@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6695 59be 5263      .....}..:.f.Y.Rc
0x0020   8018 7fe0 9995 0000 0101 080a 0013 7fe5      ................
0x0030   001d d556 6964 0a                            ...Vid.
15:15:00.391372 172.20.201.198.21 > 10.10.10.186.48253: P 1505645155:1505645194(39) ack 981690008
win 32120 <nop,nop,timestamp 1955478 1277925> (DF) [tos 0x10]  (ttl 62, id 195, len 91)
0x0000   4510 005b 00c3 4000 3e06 b12b ac14 c9c6      E..[..@.>..+....
0x0010   0a0a 0aba 0015 bc7d 59be 5263 3a83 6698      .......}Y.Rc:.f.
0x0020   8018 7d78 5cfe 0000 0101 080a 001d d696      ..}x\...........
0x0030   0013 7fe5 7569 643d 3028 726f 6f74 2920      ....uid=0(root).
0x0040   6769 643d 3028 726f 6f74 2920 6772 6f75      gid=0(root).grou
0x0050   7073                                        ps
15:15:00.391518 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505645194 win 32736
<nop,nop,timestamp 1277935 1955478> (DF) (ttl 64, id 7457, len 52)
0x0000   4500 0034 1d21 4000 4006 9304 0a0a 0aba      E..4.!@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6698 59be 528a      .....}..:.f.Y.R.
0x0020   8010 7fe0 0b91 0000 0101 080a 0013 7fef      ................
0x0030   001d d696                                    ....
15:15:09.291850 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690008:981690015(7) ack
1505645194 win 32736 <nop,nop,timestamp 1282493 1955478> (DF) (ttl 64, id 7458, len 59)
0x0000   4500 003b 1d22 4000 4006 92fc 0a0a 0aba      E..;."@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6698 59be 528a      .....}..:.f.Y.R.
0x0020   8018 7fe0 fc87 0000 0101 080a 0013 91bd      ................
0x0030   001d d696 6364 2064 6f63 0a                  ....cd.doc.
15:15:09.311491 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690015 win 32120
<nop,nop,timestamp 1956371 1282493> (DF) [tos 0x10]  (ttl 62, id 1024, len 52)
0x0000   4510 0034 0400 4000 3e06 ae15 ac14 c9c6      E..4..@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 528a 3a83 669f      .......}Y.R.:.f.
0x0020   8010 7d78 f8a6 0000 0101 080a 001d da13      ..}x............
0x0030   0013 91bd                                    ....
15:15:09.852869 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690015:981690018(3) ack
1505645194 win 32736 <nop,nop,timestamp 1282780 1956371> (DF) (ttl 64, id 7459, len 55)
0x0000   4500 0037 1d23 4000 4006 92ff 0a0a 0aba      E..7.#@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 669f 59be 528a      .....}..:.f.Y.R.
0x0020   8018 7fe0 7ea1 0000 0101 080a 0013 92dc      ....~...........
0x0030   001d da13 6c73 0a                            ....ls.
15:15:09.872874 172.20.201.198.21 > 10.10.10.186.48253: P [tcp sum ok] 1505645194:1505645208(14)
ack 981690018 win 32120 <nop,nop,timestamp 1956426 1282780> (DF) [tos 0x10]  (ttl 62, id 1037, len 66)
```

```
0x0000   4510 0042 040d 4000 3e06 adfa ac14 c9c6        E..B..@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 528a 3a83 66a2        .......}Y.R.:.f.
0x0020   8018 7d78 e157 0000 0101 080a 001d da4a        ..}x.W.........J
0x0030   0013 92dc 7775 2d66 7470 642d 322e 362e        ....wu-ftpd-2.6.
0x0040   300a                                          0.
……
15:17:29.010129 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505655762 win 49232
<nop,nop,timestamp 1354042 1970336> (DF) (ttl 64, id 7487, len 52)
0x0000   4500 0034 1d3f 4000 4006 92e6 0a0a 0aba        E..4.?@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 66ef 59be 7bd2        .....}..:.f.Y.{.
0x0020   8010 c050 3e2b 0000 0101 080a 0014 a93a        ...P>+.........:
0x0030   001e 10a0                                      ....
15:17:32.055378 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690095:981690106(11) ack
1505655762 win 49232 <nop,nop,timestamp 1355601 1970336> (DF) (ttl 64, id 7488, len 63)
0x0000   4500 003f 1d40 4000 4006 92da 0a0a 0aba        E..?.@@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 66ef 59be 7bd2        .....}..:.f.Y.{.
0x0020   8018 c050 fb45 0000 0101 080a 0014 af51        ...P.E.........Q
0x0030   001e 10a0 6361 7420 7061 7373 7764 0a          ....cat.passwd.
15:17:32.078609 172.20.201.198.21 > 10.10.10.186.48253: P 1505655762:1505656274(512) ack
981690106 win 32120 <nop,nop,timestamp 1970642 1355601> (DF) [tos 0x10] (ttl 62, id 6466, len 564)
0x0000   4510 0234 1942 4000 3e06 96d3 ac14 c9c6        E..4.B@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 7bd2 3a83 66fa        .......}Y.{.:.f.
0x0020   8018 7d78 2629 0000 0101 080a 001e 11d2        ..}x&).........
0x0030   0014 af51 726f 6f74 3a78 3a30 3a30 3a72        ...Qroot:x:0:0:r
0x0040   6f6f 743a 2f72 6f6f 743a 2f62 696e 2f62        oot:/root:/bin/b
0x0050   6173                                          as
15:17:32.078826 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505656274 win 49232
<nop,nop,timestamp 1355613 1970642> (DF) (ttl 64, id 7489, len 52)
0x0000   4500 0034 1d41 4000 4006 92e4 0a0a 0aba        E..4.A@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 66fa 59be 7dd2        .....}..:.f.Y.}.
0x0020   8010 c050 34cb 0000 0101 080a 0014 af5d        ...P4.........]
0x0030   001e 11d2                                      ....
15:17:32.095186 172.20.201.198.21 > 10.10.10.186.48253: P 1505656274:1505656829(555) ack
981690106 win 32120 <nop,nop,timestamp 1970644 1355613> (DF) [tos 0x10] (ttl 62, id 6473, len 607)
0x0000   4510 025f 1949 4000 3e06 96a1 ac14 c9c6        E.._.I@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 7dd2 3a83 66fa        .......}Y.}.:.f.
0x0020   8018 7d78 ddc5 0000 0101 080a 001e 11d4        ..}x............
0x0030   0014 af5d 6368 653a 783a 3438 3a34 383a        ...]che:x:48:48:
0x0040   4170 6163 6865 3a2f 7661 722f 7777 773a        Apache:/var/www:
0x0050   2f62                                          /b
15:17:32.095389 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505656829 win 49232
<nop,nop,timestamp 1355621 1970644> (DF) (ttl 64, id 7490, len 52)
0x0000   4500 0034 1d42 4000 4006 92e3 0a0a 0aba        E..4.B@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 66fa 59be 7ffd        .....}..:.f.Y...
0x0020   8010 c050 3296 0000 0101 080a 0014 af65        ...P2.........e
0x0030   001e 11d4                                      ....
15:17:48.180033 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690106:981690118(12) ack
1505656829 win 49232 <nop,nop,timestamp 1363858 1970644> (DF) (ttl 64, id 7491, len 64)
0x0000   4500 0040 1d43 4000 4006 92d6 0a0a 0aba        E..@.C@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 66fa 59be 7ffd        .....}..:.f.Y...
0x0020   8018 c050 195c 0000 0101 080a 0014 cf92        ...P.\..........
0x0030   001e 11d4 7375 202d 206a 736d 6974 680a        ....su.-.jsmith.
15:17:48.237956 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690118 win 32120
<nop,nop,timestamp 1972258 1363858> (DF) [tos 0x10] (ttl 62, id 7377, len 52)
0x0000   4510 0034 1cd1 4000 3e06 9544 ac14 c9c6        E..4..@.>..D....
0x0010   0a0a 0aba 0015 bc7d 59be 7ffd 3a83 6706        .......}Y...:.g.
0x0020   8010 7d78 4ee7 0000 0101 080a 001e 1822        ..}xN..........."
0x0030   0014 cf92                                      ....
15:17:49.529878 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690118:981690121(3) ack
1505656829 win 49232 <nop,nop,timestamp 1364550 1972258> (DF) (ttl 64, id 7492, len 55)
0x0000   4500 0037 1d44 4000 4006 92de 0a0a 0aba        E..7.D@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6706 59be 7ffd        .....}..:.g.Y...
```

```
0x0020   8018 c050 95eb 0000 0101 080a 0014 d246          ...P...........F
0x0030   001e 1822 6964 0a                                ..."id.
15:17:49.549078 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690121 win 32120
<nop,nop,timestamp 1972388 1364550> (DF) [tos 0x10]  (ttl 62, id 7411, len 52)
0x0000   4510 0034 1cf3 4000 3e06 9522 ac14 c9c6          E..4..@.>.."....
0x0010   0a0a 0aba 0015 bc7d 59be 7ffd 3a83 6709          .......}Y...:.g.
0x0020   8010 7d78 4bae 0000 0101 080a 001e 18a4          ..}xK...........
0x0030   0014 d246                                        ...F
15:17:49.557690 172.20.201.198.21 > 10.10.10.186.48253: P 1505656829:1505656878(49) ack 981690121
win 32120 <nop,nop,timestamp 1972389 1364550> (DF) [tos 0x10]  (ttl 62, id 7412, len 101)
0x0000   4510 0065 1cf4 4000 3e06 94f0 ac14 c9c6          E..e..@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 7ffd 3a83 6709          .......}Y...:.g.
0x0020   8018 7d78 e714 0000 0101 080a 001e 18a5          ..}x............
0x0030   0014 d246 7569 643d 3530 3028 6a73 6d69          ...Fuid=500(jsmi
0x0040   7468 2920 6769 643d 3130 3028 7573 6572          th).gid=100(user
0x0050   7329                                             s)
……
15:18:06.248418 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690143:981690155(12) ack
1505656990 win 49232 <nop,nop,timestamp 1373111 1973461> (DF) (ttl 64, id 7500, len 64)
0x0000   4500 0040 1d4c 4000 4006 92cd 0a0a 0aba          E..@.L@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 671f 59be 809e          .....}..:.g.Y...
0x0020   8018 c050 1cc2 0000 0101 080a 0014 f3b7          ...P............
0x0030   001e 1cd5 6364 202e 2e2f 776f 726b 2a0a          ....cd.../work*.
15:18:06.269005 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690155 win 32120
<nop,nop,timestamp 1974061 1373111> (DF) [tos 0x10]  (ttl 62, id 10056, len 52)
0x0000   4510 0034 2748 4000 3e06 8acd ac14 c9c6          E..4'H@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 809e 3a83 672b          .......}Y...:.g+
0x0020   8010 7d78 22f1 0000 0101 080a 001e 1f2d          ..}x"..........-
0x0030   0014 f3b7                                        ....
15:18:06.898480 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690155:981690158(3) ack
1505656990 win 49232 <nop,nop,timestamp 1373444 1974061> (DF) (ttl 64, id 7501, len 55)
0x0000   4500 0037 1d4d 4000 4006 92d5 0a0a 0aba          E..7.M@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 672b 59be 809e          .....}..:.g+Y...
0x0020   8018 c050 684d 0000 0101 080a 0014 f504          ...PhM..........
0x0030   001e 1f2d 6c73 0a                                ..-ls.
15:18:06.915056 172.20.201.198.21 > 10.10.10.186.48253: P [tcp sum ok] 1505656990:1505657013(23)
ack 981690158 win 32120 <nop,nop,timestamp 1974125 1373444> (DF) [tos 0x10]  (ttl 62, id 10097, len 75)
0x0000   4510 004b 2771 4000 3e06 8a8d ac14 c9c6          E..K'q@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 809e 3a83 672e          .......}Y...:.g.
0x0020   8018 7d78 9da9 0000 0101 080a 001e 1f6d          ..}x...........m
0x0030   0014 f504 696d 706f 7274 616e 742d 7072          ....important-pr
0x0040   6f70 6f73 616c 2e74 7874 0a                      oposal.txt.
15:18:06.915199 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505657013 win 49232
<nop,nop,timestamp 1373452 1974125> (DF) (ttl 64, id 7502, len 52)
0x0000   4500 0034 1d4e 4000 4006 92d7 0a0a 0aba          E..4.N@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 672e 59be 80b5          .....}..:.g.Y...
0x0020   8010 c050 de69 0000 0101 080a 0014 f50c          ...P.i..........
0x0030   001e 1f6d                                        ...m
15:18:10.377297 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690158:981690167(9) ack
1505657013 win 49232 <nop,nop,timestamp 1375225 1974125> (DF) (ttl 64, id 7503, len 61)
0x0000   4500 003d 1d4f 4000 4006 92cd 0a0a 0aba          E..=.O@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 672e 59be 80b5          .....}..:.g.Y...
0x0020   8018 c050 1c52 0000 0101 080a 0014 fbf9          ...P.R..........
0x0030   001e 1f6d 6361 7420 696d 702a 0a                 ...mcat.imp*.
15:18:10.399352 172.20.201.198.21 > 10.10.10.186.48253: P 1505657013:1505657057(44) ack 981690167
win 32120 <nop,nop,timestamp 1974473 1375225> (DF) [tos 0x10]  (ttl 62, id 10329, len 96)
0x0000   4510 0060 2859 4000 3e06 8990 ac14 c9c6          E..`(Y@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 80b5 3a83 6737          .......}Y...:.g7
0x0020   8018 7d78 4d9f 0000 0101 080a 001e 20c9          ..}xM...........
0x0030   0014 fbf9 426c 6168 2062 6c61 6820 626c          ....Blah.blah.bl
0x0040   6168 2e2e 2e0a 0a28 736f 756e 6473 2069          ah.....(sounds.i
0x0050   6d70                                             mp
```

```
15:18:10.399495 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505657057 win 49232
<nop,nop,timestamp 1375237 1974473> (DF) (ttl 64, id 7504, len 52)
0x0000   4500 0034 1d50 4000 4006 92d5 0a0a 0aba          E..4.P@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6737 59be 80e1          .....}..:.g7Y...
0x0020   8010 c050 d5df 0000 0101 080a 0014 fc05          ...P............
0x0030   001e 20c9                                        ....
15:18:23.778393 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690167:981690193(26) ack
1505657057 win 49232 <nop,nop,timestamp 1382088 1974473> (DF) (ttl 64, id 7505, len 78)
0x0000   4500 004e 1d51 4000 4006 92ba 0a0a 0aba          E..N.Q@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6737 59be 80e1          .....}..:.g7Y...
0x0020   8018 c050 8c0d 0000 0101 080a 0015 16c8          ...P............
0x0030   001e 20c9 7669 2069 6d70 6f72 7461 6e74          ....vi.important
0x0040   2d70 726f 706f 7361 6c2e 7478 740a               -proposal.txt.
15:18:23.814743 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690193 win 32120
<nop,nop,timestamp 1975814 1382088> (DF) [tos 0x10]  (ttl 62, id 10938, len 52)
0x0000   4510 0034 2aba 4000 3e06 875b ac14 c9c6          E..4*.@.>..[....
0x0010   0a0a 0aba 0015 bc7d 59be 80e1 3a83 6751          .......}Y...:.gQ
0x0020   8010 7d78 f89d 0000 0101 080a 001e 2606          ..}x..........&.
0x0030   0015 16c8                                        ....
15:18:23.841841 172.20.201.198.21 > 10.10.10.186.48253: P 1505657057:1505657099(42) ack 981690193
win 32120 <nop,nop,timestamp 1975817 1382088> (DF) [tos 0x10]  (ttl 62, id 10941, len 94)
0x0000   4510 005e 2abd 4000 3e06 872e ac14 c9c6          E..^*.@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 80e1 3a83 6751          .......}Y...:.gQ
0x0020   8018 7d78 8a0a 0000 0101 080a 001e 2609          ..}x..........&.
0x0030   0015 16c8 5669 6d3a 2057 6172 6e69 6e67          ....Vim:.Warning
0x0040   3a20 4f75 7470 7574 2069 7320 6e6f 7420          :.Output.is.not.
0x0050   746f                                             to
15:18:23.841950 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505657099 win 49232
<nop,nop,timestamp 1382120 1975817> (DF) (ttl 64, id 7506, len 52)
0x0000   4500 0034 1d52 4000 4006 92d3 0a0a 0aba          E..4.R@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6751 59be 810b          .....}..:.gQY...
0x0020   8010 c050 b578 0000 0101 080a 0015 16e8          ...P.x..........
0x0030   001e 2609                                        ..&.
15:18:23.845753 172.20.201.198.21 > 10.10.10.186.48253: P 1505657099:1505657142(43) ack 981690193
win 32120 <nop,nop,timestamp 1975818 1382120> (DF) [tos 0x10]  (ttl 62, id 10942, len 95)
0x0000   4510 005f 2abe 4000 3e06 872c ac14 c9c6          E.._*.@.>..,....
0x0010   0a0a 0aba 0015 bc7d 59be 810b 3a83 6751          .......}Y...:.gQ
0x0020   8018 7d78 57a0 0000 0101 080a 001e 260a          ..}xW.........&.
0x0030   0015 16e8 5669 6d3a 2057 6172 6e69 6e67          ....Vim:.Warning
0x0040   3a20 496e 7075 7420 6973 206e 6f74 2066          :.Input.is.not.f
0x0050   726f                                             ro
15:18:23.845908 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505657142 win 49232
<nop,nop,timestamp 1382123 1975818> (DF) (ttl 64, id 7507, len 52)
0x0000   4500 0034 1d53 4000 4006 92d2 0a0a 0aba          E..4.S@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6751 59be 8136          .....}..:.gQY..6
0x0020   8010 c050 b549 0000 0101 080a 0015 16eb          ...P.I..........
0x0030   001e 260a                                        ..&.
15:18:25.873364 172.20.201.198.21 > 10.10.10.186.48253: P 1505657142:1505657174(32) ack 981690193
win 32120 <nop,nop,timestamp 1976020 1382123> (DF) [tos 0x10]  (ttl 62, id 11051, len 84)
0x0000   4510 0054 2b2b 4000 3e06 86ca ac14 c9c6 E..T++@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 8136 3a83 6751          .......}Y..6:.gQ
0x0020   8018 7d78 6fc3 0000 0101 080a 001e 26d4          ..}xo.........&.
0x0030   0015 16eb 0c1b 5b32 343b 3148 2269 6d70          ......[24;1H"imp
0x0040   6f72 7461 6e74 2d70 726f 706f 7361 6c2e          ortant-proposal.
0x0050   7478                                            tx
15:18:25.873504 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505657174 win 49232
<nop,nop,timestamp 1383161 1976020> (DF) (ttl 64, id 7508, len 52)
0x0000   4500 0034 1d54 4000 4006 92d1 0a0a 0aba          E..4.T@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6751 59be 8156          .....}..:.gQY..V
0x0020   8010 c050 b051 0000 0101 080a 0015 1af9          ...P.Q..........
0x0030   001e 26d4                                        ..&.
```

```
15:18:25.880347 172.20.201.198.21 > 10.10.10.186.48253: P 1505657174:1505658622(1448) ack
981690193 win 32120 <nop,nop,timestamp 1976021 1382123> (DF) [tos 0x10]  (ttl 62, id 11054, len 1500)
0x0000   4510 05dc 2b2e 4000 3e06 813f ac14 c9c6          E...+.@.>..?....
0x0010   0a0a 0aba 0015 bc7d 59be 8156 3a83 6751          .......}Y..V:.gQ
0x0020   8018 7d78 887f 0000 0101 080a 001e 26d5          ..}x..........&.
0x0030   0015 16eb 2034 4c2c 2034 3443 1b5b 313b          .....4L,.44C.[1;
0x0040   3148 426c 6168 2062 6c61 6820 626c 6168 1        HBlah.blah.blah
0x0050   2e2e                                            ..
……
15:18:33.135748 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690201:981690204(3) ack
1505658944 win 52128 <nop,nop,timestamp 1386880 1976668> (DF) (ttl 64, id 7515, len 55)
0x0000   4500 0037 1d5b 4000 4006 92c7 0a0a 0aba          E..7.[@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6759 59be 8840          .....}..:.gYY..@
0x0020   8018 cba0 1682 0000 0101 080a 0015 2980          ..............).
0x0030   001e 295c 6c73 0a                                ..)\ls.
15:18:33.153382 172.20.201.198.21 > 10.10.10.186.48253: P [tcp sum ok] 1505658944:1505658967(23)
ack 981690204 win 32120 <nop,nop,timestamp 1976748 1386880> (DF) [tos 0x10]  (ttl 62, id 11247, len 75)
0x0000   4510 004b 2bef 4000 3e06 860f ac14 c9c6          E..K+.@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 8840 3a83 675c          .......}Y..@:.g\
0x0020   8018 7d78 571e 0000 0101 080a 001e 29ac          ..}xW.........).
0x0030   0015 2980 696d 706f 7274 616e 742d 7072          ..).important-pr
0x0040   6f70 6f73 616c 2e74 7874 0a                      oposal.txt.
15:18:33.153525 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505658967 win 52128
<nop,nop,timestamp 1386889 1976748> (DF) (ttl 64, id 7516, len 52)
0x0000   4500 0034 1d5c 4000 4006 92c9 0a0a 0aba          E..4.\@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 675c 59be 8857          .....}..:.g\Y..W
0x0020   8010 cba0 8c8d 0000 0101 080a 0015 2989          ..............).
0x0030   001e 29ac                                        ..).
15:18:45.509880 10.10.10.186.48253 > 172.20.201.198.21: P 981690204:981690249(45) ack 1505658967
win 52128 <nop,nop,timestamp 1393216 1976748> (DF) (ttl 64, id 7517, len 97)
0x0000   4500 0061 1d5d 4000 4006 929b 0a0a 0aba          E..a.]@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 675c 59be 8857          .....}..:.g\Y..W
0x0020   8018 cba0 97af 0000 0101 080a 0015 4240          ..............B@
0x0030   001e 29ac 6361 7420 2279 6573 2c20 6974          ..).cat."yes,.it
0x0040   2064 6f65 732e 2220 3e3e 696d 706f 7274          .does.".>>import
0x0050   616e                                            an
15:18:45.526131 172.20.201.198.21 > 10.10.10.186.48253: P [tcp sum ok] 1505658967:1505658972(5) ack
981690249 win 32120 <nop,nop,timestamp 1977985 1393216> (DF) [tos 0x10]  (ttl 62, id 11674, len 57)
0x0000   4510 0039 2d9a 4000 3e06 8476 ac14 c9c6          E..9-.@.>..v....
0x0010   0a0a 0aba 0015 bc7d 59be 8857 3a83 6789          .......}Y..W:.g.
0x0020   8018 7d78 c553 0000 0101 080a 001e 2e81          ..}x.S..........
0x0030   0015 4240 6361 743a 20                           ..B@cat:.
15:18:45.526267 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505658972 win 52128
<nop,nop,timestamp 1393225 1977985> (DF) (ttl 64, id 7518, len 52)
0x0000   4500 0034 1d5e 4000 4006 92c7 0a0a 0aba          E..4.^@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6789 59be 885c          .....}..:.g.Y..\
0x0020   8010 cba0 6ec6 0000 0101 080a 0015 4249          ....n.........BI
0x0030   001e 2e81                                        ....
15:18:45.530590 172.20.201.198.21 > 10.10.10.186.48253: P 1505658972:1505659013(41) ack 981690249
win 32120 <nop,nop,timestamp 1977985 1393225> (DF) [tos 0x10]  (ttl 62, id 11675, len 93)
0x0000   4510 005d 2d9b 4000 3e06 8451 ac14 c9c6          E..]-.@.>..Q....
0x0010   0a0a 0aba 0015 bc7d 59be 885c 3a83 6789          .......}Y..\:.g.
0x0020   8018 7d78 9eb0 0000 0101 080a 001e 2e81          ..}x............
0x0030   0015 4249 7965 732c 2069 7420 646f 6573          ..BIyes,.it.does
0x0040   2e3a 204e 6f20 7375 6368 2066 696c 6520          .:.No.such.file.
0x0050   6f72                                             or
15:18:45.530714 10.10.10.186.48253 > 172.20.201.198.21: . [tcp sum ok] ack 1505659013 win 52128
<nop,nop,timestamp 1393227 1977985> (DF) (ttl 64, id 7519, len 52)
0x0000   4500 0034 1d5f 4000 4006 92c6 0a0a 0aba          E..4._@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6789 59be 8885          .....}..:.g.Y...
0x0020   8010 cba0 6e9b 0000 0101 080a 0015 424b          ....n.........BK
0x0030   001e 2e81                                        ....
```

```
15:18:59.821941 10.10.10.186.48253 > 172.20.201.198.21: P 981690249:981690295(46) ack 1505659013
win 52128 <nop,nop,timestamp 1400546 1977985> (DF) (ttl 64, id 7520, len 98)
0x0000   4500 0062 1d60 4000 4006 9297 0a0a 0aba          E..b.`@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 6789 59be 8885          .....}..:.g.Y...
0x0020   8018 cba0 f3f6 0000 0101 080a 0015 5ee2          ..............^.
0x0030   001e 2e81 6563 686f 2022 7965 732c 2069          ....echo."yes,.i
0x0040   7420 646f 6573 2e22 203e 3e69 6d70 6f72          t.does.".>>impor
0x0050   7461                                            ta
15:18:59.845928 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690295 win 32120
<nop,nop,timestamp 1979417 1400546> (DF) [tos 0x10]  (ttl 62, id 12102, len 52)
0x0000   4510 0034 2f46 4000 3e06 82cf ac14 c9c6          E..4/F@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 8885 3a83 67b7          .......}Y...:.g.
0x0020   8010 7d78 9a66 0000 0101 080a 001e 3419          ..}x.f........4.
0x0030   0015 5ee2                                        ..^.
15:19:01.977748 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690295:981690296(1) ack
1505659013 win 52128 <nop,nop,timestamp 1401650 1979417> (DF) (ttl 64, id 7521, len 53)
0x0000   4500 0035 1d61 4000 4006 92c3 0a0a 0aba          E..5.a@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 67b7 59be 8885          .....}..:.g.Y...
0x0020   8018 cba0 3de5 0000 0101 080a 0015 6332          ....=.........c2
0x0030   001e 3419 0a                                     ..4..
15:19:02.036645 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690296 win 32120
<nop,nop,timestamp 1979636 1401650> (DF) [tos 0x10]  (ttl 62, id 12130, len 52)
0x0000   4510 0034 2f62 4000 3e06 82b3 ac14 c9c6          E..4/b@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 8885 3a83 67b8          .......}Y...:.g.
0x0020   8010 7d78 953a 0000 0101 080a 001e 34f4          ..}x.:........4.
0x0030   0015 6332                                        ..c2
15:19:04.506075 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690296:981690307(11) ack
1505659013 win 52128 <nop,nop,timestamp 1402944 1979636> (DF) (ttl 64, id 7522, len 63)
0x0000   4500 003f 1d62 4000 4006 92b8 0a0a 0aba          E..?.b@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 67b8 59be 8885          .....}..:.g.Y...
0x0020   8018 cba0 1468 0000 0101 080a 0015 6840          .....h........h@
0x0030   001e 34f4 6361 7420 696d 706f 722a 0a            ..4.cat.impor*.
15:19:04.532002 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690307 win 32120
<nop,nop,timestamp 1979885 1402944> (DF) [tos 0x10]  (ttl 62, id 12223, len 52)
0x0000   4510 0034 2fbf 4000 3e06 8256 ac14 c9c6          E..4/.@.>..V....
0x0010   0a0a 0aba 0015 bc7d 59be 8885 3a83 67c3          .......}Y...:.g.
0x0020   8010 7d78 8f28 0000 0101 080a 001e 35ed          ..}x.(........5.
0x0030   0015 6840                                        ..h@
15:19:04.532151 172.20.201.198.21 > 10.10.10.186.48253: P 1505659013:1505659071(58) ack 981690307
win 32120 <nop,nop,timestamp 1979885 1402944> (DF) [tos 0x10]  (ttl 62, id 12224, len 110)
0x0000   4510 006e 2fc0 4000 3e06 821b ac14 c9c6          E..n/.@.>.......
0x0010   0a0a 0aba 0015 bc7d 59be 8885 3a83 67c3          .......}Y...:.g.
0x0020   8018 7d78 4ac1 0000 0101 080a 001e 35ed          ..}xJ.........5.
0x0030   0015 6840 426c 6168 2062 6c61 6820 626c          ..h@Blah.blah.bl
0x0040   6168 2e2e 2e0a 0a28 736f 756e 6473 2069          ah.....(sounds.i
0x0050   6d70                                            mp
……
15:19:41.050383 10.10.10.186.48253 > 172.20.201.198.21: P [tcp sum ok] 981690326:981690345(19) ack
1505660671 win 55024 <nop,nop,timestamp 1421658 1980857> (DF) (ttl 64, id 7531, len 71)
0x0000   4500 0047 1d6b 4000 4006 92a7 0a0a 0aba          E..G.k@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 67d6 59be 8eff          .....}..:.g.Y...
0x0020   8018 d6f0 77b9 0000 0101 080a 0015 b15a          ....w.........Z
0x0030   001e 39b9 726c 6f67 696e 2031 3732 2e32          ..9.rlogin.172.2
0x0040   302e 3131 2e31 0a                                0.11.1.
15:19:41.121099 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690345 win 32120
<nop,nop,timestamp 1983538 1421658> (DF) [tos 0x10]  (ttl 62, id 16284, len 52)
0x0000   4510 0034 3f9c 4000 3e06 7279 ac14 c9c6          E..4?.@.>.ry....
0x0010   0a0a 0aba 0015 bc7d 59be 8eff 3a83 67e9          .......}Y...:.g.
0x0020   8010 7d78 3129 0000 0101 080a 001e 4432          ..}x1).........D2
0x0030   0015 b15a                                        ...Z
15:19:44.723913 10.10.10.186.48253 > 172.20.201.198.21: F [tcp sum ok] 981690345:981690345(0) ack
1505660671 win 55024 <nop,nop,timestamp 1423539 1983538> (DF) (ttl 64, id 7532, len 52)
```

```
0x0000   4500 0034 1d6c 4000 4006 92b9 0a0a 0aba          E..4.l@.@.......
0x0010   ac14 c9c6 bc7d 0015 3a83 67e9 59be 8eff          .....}..:.g.Y...
0x0020   8011 d6f0 d056 0000 0101 080a 0015 b8b3          .....V..........
0x0030   001e 4432                                        ..D2
15:19:44.726728 172.20.201.198.21 > 10.10.10.186.48253: . [tcp sum ok] ack 981690346 win 32120 <nop,nop,timestamp 1983903 1423539> (DF) [tos 0x10]  (ttl 62, id 16358, len 52)
0x0000   4510 0034 3fe6 4000 3e06 722f ac14 c9c6          E..4?.@.>.r/....
0x0010   0a0a 0aba 0015 bc7d 59be 8eff 3a83 67ea          .......}Y...:.g.
0x0020   8010 7d78 2862 0000 0101 080a 001e 459f          ..}x(b........E.
0x0030   0015 b8b3                                        ....
15:20:12.216689 172.20.201.198.21 > 10.10.10.186.48253: P 1505660671:1505660703(32) ack 981690346 win 32120 <nop,nop,timestamp 1986651 1423539> (DF) [tos 0x10]  (ttl 62, id 16681, len 84)
0x0000   4510 0054 4129 4000 3e06 70cc ac14 c9c6          E..TA)@.>.p.....
0x0010   0a0a 0aba 0015 bc7d 59be 8eff 3a83 67ea          .......}Y...:.g.
0x0020   8018 7d78 0de9 0000 0101 080a 001e 505b          ..}x..........P[
0x0030   0015 b8b3 3137 322e 3230 2e31 312e 313a          ....172.20.11.1:
0x0040   2043 6f6e 6e65 6374 696f 6e20 7265 6675          .Connection.refu
0x0050   7365                                            se
15:20:12.216824 10.10.10.186.48253 > 172.20.201.198.21: R [tcp sum ok] 981690346:981690346(0) win 0 (DF) [tos 0x10]  (ttl 64, id 0, len 40)
0x0000   4510 0028 0000 4000 4006 b021 0a0a 0aba          E..(..@.@..!....
0x0010   ac14 c9c6 bc7d 0015 3a83 67ea 0000 0000          .....}..:.g.....
0x0020   5004 0000 c641 0000 0000 0000 0000 0000          P....A........
```

Appendix 9

```
15:00:18.021986 10.10.10.122.59909 > 192.168.17.135.21: S [tcp sum ok] 615594842:615594842(0) win 5840 <mss 1460,sackOK,timestamp 171340 0,nop,wscale 0> (DF) (ttl 64, id 42518, len 60)
0x0000   4500 003c a616 4000 4006 adf2 0a0a 0a7a          E..<..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b5a 0000 0000          ........$.;Z....
0x0020   a002 16d0 630f 0000 0204 05b4 0402 080a          ....c...........
0x0030   0002 9d4c 0000 0000 0103 0300                    ...L........
15:00:18.027669 192.168.17.135.21 > 10.10.10.122.59909: S [tcp sum ok] 3048646128:3048646128(0) ack 615594843 win 5792 <mss 1460,sackOK,timestamp 5001726 171340,nop,wscale 0> (DF) (ttl 61, id 0, len 60)
0x0000   4500 003c 0000 4000 3d06 5709 c0a8 1187          E..<..@.=.W.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a5f0 24b1 3b5b          ...z........$.;[
0x0020   a012 16a0 b53c 0000 0204 05b4 0402 080a          .....<..........
0x0030   004c 51fe 0002 9d4c 0103 0300                    .LQ....L....
15:00:18.027816 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646129 win 5840 <nop,nop,timestamp 171340 5001726> (DF) (ttl 64, id 42519, len 52)
0x0000   4500 0034 a617 4000 4006 adf9 0a0a 0a7a          E..4..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b5b b5b6 a5f1          ........$.;[....
0x0020   8010 16d0 e3d1 0000 0101 080a 0002 9d4c          ...............L
0x0030   004c 51fe                                        .LQ.
15:00:28.092163 192.168.17.135.21 > 10.10.10.122.59909: P 3048646129:3048646223(94) ack 615594843 win 5792 <nop,nop,timestamp 5002732 171340> (DF) [tos 0x10]  (ttl 61, id 62478, len 146)
0x0000   4510 0092 f40e 4000 3d06 6294 c0a8 1187          E.....@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a5f1 24b1 3b5b          ...z........$.;[
0x0020   8018 16a0 1ccc 0000 0101 080a 004c 55ec          .............LU.
0x0030   0002 9d4c 3232 3020 7375 7365 3732 616c          ...L220.suse72al
0x0040   6c2e 7461 7267 6574 2e6c 6162 732e 7665          l.target.labs.ve
0x0050   7269                                            ri
15:00:28.092377 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646223 win 5840 <nop,nop,timestamp 172347 5002732> (DF) [tos 0x10]  (ttl 64, id 42520, len 52)
0x0000   4510 0034 a618 4000 4006 ade8 0a0a 0a7a          E..4..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b5b b5b6 a64f          ........$.;[...O
0x0020   8010 16d0 db96 0000 0101 080a 0002 a13b          ...............;
0x0030   004c 55ec                                        .LU.
15:00:30.280307 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594843:615594853(10) ack 3048646223 win 5840 <nop,nop,timestamp 172563 5002732> (DF) [tos 0x10]  (ttl 64, id 42521, len 62)
```

```
0x0000   4510 003e a619 4000 4006 addd 0a0a 0a7a        E..>..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b5b b5b6 a64f        ........$.;[...O
0x0020   8018 16d0 9e26 0000 0101 080a 0002 a213        .....&..........
0x0030   004c 55ec 5553 4552 2066 7470 0d0a             .LU.USER.ftp..
15:00:30.284460 192.168.17.135.21 > 10.10.10.122.59909: . [tcp sum ok] ack 615594853 win 5792
<nop,nop,timestamp 5002951 172563> (DF) [tos 0x10]  (ttl 61, id 62479, len 52)
0x0000   4510 0034 f40f 4000 3d06 62f1 c0a8 1187        E..4..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a64f 24b1 3b65        ...z.......O$.;e
0x0020   8010 16a0 da09 0000 0101 080a 004c 56c7        .............LV.
0x0030   0002 a213                                      ....
15:00:30.284590 192.168.17.135.21 > 10.10.10.122.59909: P 3048646223:3048646272(49) ack 615594853
win 5792 <nop,nop,timestamp 5002951 172563> (DF) [tos 0x10]  (ttl 61, id 62480, len 101)
0x0000   4510 0065 f410 4000 3d06 62bf c0a8 1187        E..e..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a64f 24b1 3b65        ...z.......O$.;e
0x0020   8018 16a0 1b03 0000 0101 080a 004c 56c7        .............LV.
0x0030   0002 a213 3333 3120 4775 6573 7420 6c6f        ....331.Guest.lo
0x0040   6769 6e20 6f6b 2c20 7479 7065 2079 6f75        gin.ok,.type.you
0x0050   7220                                          r.
15:00:30.284697 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646272 win 5840
<nop,nop,timestamp 172564 5002951> (DF) [tos 0x10]  (ttl 64, id 42522, len 52)
0x0000   4510 0034 a61a 4000 4006 ade6 0a0a 0a7a        E..4..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b65 b5b6 a680        ........$.;e....
0x0020   8010 16d0 d9a7 0000 0101 080a 0002 a214        ................
0x0030   004c 56c7                                      .LV.
15:00:32.469666 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594853:615594874(21) ack
3048646272 win 5840 <nop,nop,timestamp 172782 5002951> (DF) [tos 0x10]  (ttl 64, id 42523, len 73)
0x0000   4510 0049 a61b 4000 4006 add0 0a0a 0a7a        E..I..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b65 b5b6 a680        ........$.;e....
0x0020   8018 16d0 1155 0000 0101 080a 0002 a2ee        .....U..........
0x0030   004c 56c7 5041 5353 2073 6470 6f66 6940        .LV.PASS.sdpofi@
0x0040   7364 7064 6f66 690d 0a                         sdpdofi..
15:00:32.477337 192.168.17.135.21 > 10.10.10.122.59909: P 3048646272:3048646320(48) ack 615594874
win 5792 <nop,nop,timestamp 5003171 172782> (DF) [tos 0x10]  (ttl 61, id 62481, len 100)
0x0000   4510 0064 f411 4000 3d06 62bf c0a8 1187        E..d..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a680 24b1 3b7a        ...z........$.;z
0x0020   8018 16a0 2bee 0000 0101 080a 004c 57a3        ....+........LW.
0x0030   0002 a2ee 3233 3020 4775 6573 7420 6c6f        ....230.Guest.lo
0x0040   6769 6e20 6f6b 2c20 6163 6365 7373 2072        gin.ok,.access.r
0x0050   6573                                          es
15:00:32.477563 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646320 win 5840
<nop,nop,timestamp 172783 5003171> (DF) [tos 0x10]  (ttl 64, id 42524, len 52)
0x0000   4510 0034 a61c 4000 4006 ade4 0a0a 0a7a        E..4..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b7a b5b6 a6b0        ........$.;z....
0x0020   8010 16d0 d7ab 0000 0101 080a 0002 a2ef        ................
0x0030   004c 57a3                                      .LW.
15:00:32.477637 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594874:615594880(6) ack
3048646320 win 5840 <nop,nop,timestamp 172783 5003171> (DF) [tos 0x10]  (ttl 64, id 42525, len 58)
0x0000   4510 003a a61d 4000 4006 addd 0a0a 0a7a        E..:..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b7a b5b6 a6b0        ........$.;z....
0x0020   8018 16d0 23e6 0000 0101 080a 0002 a2ef        ....#...........
0x0030   004c 57a3 5359 5354 0d0a                       .LW.SYST..
15:00:32.480482 192.168.17.135.21 > 10.10.10.122.59909: P [tcp sum ok] 3048646320:3048646339(19)
ack 615594880 win 5792 <nop,nop,timestamp 5003171 172783> (DF) [tos 0x10]  (ttl 61, id 62482, len 71)
0x0000   4510 0047 f412 4000 3d06 62db c0a8 1187        E..G..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a6b0 24b1 3b80        ...z........$.;.
0x0020   8018 16a0 706a 0000 0101 080a 004c 57a3        ....pj.......LW.
0x0030   0002 a2ef 3231 3520 554e 4958 2054 7970        ....215.UNIX.Typ
0x0040   653a 204c 380d 0a                              e:.L8..
15:00:32.511835 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646339 win 5840
<nop,nop,timestamp 172787 5003171> (DF) [tos 0x10]  (ttl 64, id 42526, len 52)
0x0000   4510 0034 a61e 4000 4006 ade2 0a0a 0a7a        E..4..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b80 b5b6 a6c3        ........$.;.....
```

```
0x0020   8010 16d0 d78e 0000 0101 080a 0002 a2f3          ................
0x0030   004c 57a3                                        .LW.
15:00:37.439359 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594880:615594886(6) ack
3048646339 win 5840 <nop,nop,timestamp 173279 5003171> (DF) [tos 0x10]  (ttl 64, id 42527, len 58)
0x0000   4510 003a a61f 4000 4006 addb 0a0a 0a7a          E..:..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b80 b5b6 a6c3          ........$.;.....
0x0020   8018 16d0 24f3 0000 0101 080a 0002 a4df          ....$...........
0x0030   004c 57a3 5041 5356 0d0a                         LW.PASV..
15:00:37.443371 192.168.17.135.21 > 10.10.10.122.59909: P 3048646339:3048646391(52) ack 615594886
win 5792 <nop,nop,timestamp 5003667 173279> (DF) [tos 0x10]  (ttl 61, id 62483, len 104)
0x0000   4510 0068 f413 4000 3d06 62b9 c0a8 1187          E..h..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a6c3 24b1 3b86          ...z........$.;.
0x0020   8018 16a0 05f4 0000 0101 080a 004c 5993          .............LY.
0x0030   0002 a4df 3232 3720 456e 7465 7269 6e67          ....227.Entering
0x0040   2050 6173 7369 7665 204d 6f64 6520 2831          .Passive.Mode.(1
0x0050   3932                                            92
15:00:37.443598 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646391 win 5840
<nop,nop,timestamp 173280 5003667> (DF) [tos 0x10]  (ttl 64, id 42528, len 52)
0x0000   4510 0034 a620 4000 4006 ade0 0a0a 0a7a          E..4..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b86 b5b6 a6f7          ........$.;.....
0x0020   8010 16d0 d377 0000 0101 080a 0002 a4e0          .....w..........
0x0030   004c 5993                                        .LY.
15:00:37.456462 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594886:615594913(27) ack
3048646391 win 5840 <nop,nop,timestamp 173281 5003667> (DF) [tos 0x10]  (ttl 64, id 42529, len 79)
0x0000   4510 004f a621 4000 4006 adc4 0a0a 0a7a          E..O.!@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3b86 b5b6 a6f7          ........$.;.....
0x0020   8018 16d0 38d8 0000 0101 080a 0002 a4e1          ....8...........
0x0030   004c 5993 4c49 5354 202e 2e2f 2e2e 2f2e          .LY.LIST.../../.
0x0040   2e2f 2e2e 2f2e 2e2f 2e2e 2f2e 2e0d 0a            ./../../../...
15:00:37.469053 192.168.17.135.21 > 10.10.10.122.59909: P 3048646391:3048646447(56) ack 615594913
win 5792 <nop,nop,timestamp 5003669 173281> (DF) [tos 0x10]  (ttl 61, id 62484, len 108)
0x0000   4510 006c f414 4000 3d06 62b4 c0a8 1187          E..l..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a6f7 24b1 3ba1          ...z........$.;.
0x0020   8018 16a0 91af 0000 0101 080a 004c 5995          .............LY.
0x0030   0002 a4e1 3135 3020 4f70 656e 696e 6720          ....150.Opening.
0x0040   4249 4e41 5259 206d 6f64 6520 6461 7461          BINARY.mode.data
0x0050   2063                                            .c
15:00:37.502147 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646447 win 5840
<nop,nop,timestamp 173286 5003669> (DF) [tos 0x10]  (ttl 64, id 42530, len 52)
0x0000   4510 0034 a622 4000 4006 adde 0a0a 0a7a          E..4."@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3ba1 b5b6 a72f          ........$.;..../
0x0020   8010 16d0 d31c 0000 0101 080a 0002 a4e6          ................
0x0030   004c 5995                                        .LY.
15:00:37.504268 192.168.17.135.21 > 10.10.10.122.59909: P [tcp sum ok] 3048646447:3048646471(24)
ack 615594913 win 5792 <nop,nop,timestamp 5003674 173286> (DF) [tos 0x10]  (ttl 61, id 62485, len 76)
0x0000   4510 004c f415 4000 3d06 62d3 c0a8 1187          E..L..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a72f 24b1 3ba1          ...z......./$.;.
0x0020   8018 16a0 0432 0000 0101 080a 004c 599a          .....2.......LY.
0x0030   0002 a4e6 3232 3620 5472 616e 7366 6572          ....226.Transfer
0x0040   2063 6f6d 706c 6574 652e 0d0a                    .complete...
15:00:37.524307 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646471 win 5840
<nop,nop,timestamp 173288 5003674> (DF) [tos 0x10]  (ttl 64, id 42531, len 52)
0x0000   4510 0034 a623 4000 4006 addd 0a0a 0a7a          E..4.#@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3ba1 b5b6 a747          ........$.;....G
0x0020   8010 16d0 d2fd 0000 0101 080a 0002 a4e8          ................
0x0030   004c 599a                                        .LY.
15:00:47.082513 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594913:615594934(21) ack
3048646471 win 5840 <nop,nop,timestamp 174243 5003674> (DF) [tos 0x10]  (ttl 64, id 42532, len 73)
0x0000   4510 0049 a624 4000 4006 adc7 0a0a 0a7a          E..I.$@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3ba1 b5b6 a747          ........$.;....G
0x0020   8018 16d0 5e15 0000 0101 080a 0002 a8a3          ....^...........
0x0030   004c 599a 4357 4420 2e2e 2f2e 2e2f 2e2e          .LY.CWD.../../..
```

```
0x0040   2f2e 2e2f 6574 630d 0a                  /../etc.
15:00:47.127667 192.168.17.135.21 > 10.10.10.122.59909: P [tcp sum ok] 3048646471:3048646500(29)
ack 615594934 win 5792 <nop,nop,timestamp 5004635 174243> (DF) [tos 0x10]  (ttl 61, id 62486, len 81)
0x0000   4510 0051 f416 4000 3d06 62cd c0a8 1187  E..Q..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a747 24b1 3bb6  ...z.......G$.;.
0x0020   8018 16a0 ee12 0000 0101 080a 004c 5d5b  .............L][
0x0030   0002 a8a3 3235 3020 4357 4420 636f 6d6d  ....250.CWD.comm
0x0040   616e 6420 7375 6363 6573 7366 756c 2e0d  and.successful..
0x0050   0a                                      .
15:00:47.127910 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646500 win 5840
<nop,nop,timestamp 174248 5004635> (DF) [tos 0x10]  (ttl 64, id 42533, len 52)
0x0000   4510 0034 a625 4000 4006 addb 0a0a 0a7a  E..4.%@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bb6 b5b6 a764  ........$.;....d
0x0020   8010 16d0 cb4a 0000 0101 080a 0002 a8a8  .....J..........
0x0030   004c 5d5b                                .L][
15:00:51.365183 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594934:615594942(8) ack
3048646500 win 5840 <nop,nop,timestamp 174670 5004635> (DF) [tos 0x10]  (ttl 64, id 42534, len 60)
0x0000   4510 003c a626 4000 4006 add2 0a0a 0a7a  E..<.&@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bb6 b5b6 a764  ........$.;....d
0x0020   8018 16d0 f7a2 0000 0101 080a 0002 aa4e  ..............N
0x0030   004c 5d5b 5459 5045 2049 0d0a            .L][TYPE.I..
15:00:51.367556 192.168.17.135.21 > 10.10.10.122.59909: P [tcp sum ok] 3048646500:3048646520(20)
ack 615594942 win 5792 <nop,nop,timestamp 5005060 174670> (DF) [tos 0x10]  (ttl 61, id 62487, len 72)
0x0000   4510 0048 f417 4000 3d06 62d5 c0a8 1187  E..H..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a764 24b1 3bbe  ...z.......d$.;.
0x0020   8018 16a0 3524 0000 0101 080a 004c 5f04  ....5$.......L_.
0x0030   0002 aa4e 3230 3020 5479 7065 2073 6574  ...N200.Type.set
0x0040   2074 6f20 492e 0d0a                      .to.I...
15:00:51.367780 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646520 win 5840
<nop,nop,timestamp 174670 5005060> (DF) [tos 0x10]  (ttl 64, id 42535, len 52)
0x0000   4510 0034 a627 4000 4006 add9 0a0a 0a7a  E..4.'@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bbe b5b6 a778  ........$.;....x
0x0020   8010 16d0 c7df 0000 0101 080a 0002 aa4e  ..............N
0x0030   004c 5f04                                .L_.
15:00:51.367852 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594942:615594948(6) ack
3048646520 win 5840 <nop,nop,timestamp 174670 5005060> (DF) [tos 0x10]  (ttl 64, id 42536, len 58)
0x0000   4510 003a a628 4000 4006 add2 0a0a 0a7a  E..:.(@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bbe b5b6 a778  ........$.;....x
0x0020   8018 16d0 1730 0000 0101 080a 0002 aa4e  .....0.........N
0x0030   004c 5f04 5041 5356 0d0a                 .L_.PASV..
15:00:51.373495 192.168.17.135.21 > 10.10.10.122.59909: P 3048646520:3048646572(52) ack 615594948
win 5792 <nop,nop,timestamp 5005060 174670> (DF) [tos 0x10]  (ttl 61, id 62488, len 104)
0x0000   4510 0068 f418 4000 3d06 62b4 c0a8 1187  E..h..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a778 24b1 3bc4  ...z.......x$.;.
0x0020   8018 16a0 f920 0000 0101 080a 004c 5f04  ..............L_.
0x0030   0002 aa4e 3232 3720 456e 7465 7269 6e67  ...N227.Entering
0x0040   2050 6173 7369 7665 204d 6f64 6520 2831  .Passive.Mode.(1
0x0050   3932                                    92
15:00:51.375643 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594948:615594961(13) ack
3048646572 win 5840 <nop,nop,timestamp 174671 5005060> (DF) [tos 0x10]  (ttl 64, id 42537, len 65)
0x0000   4510 0041 a629 4000 4006 adca 0a0a 0a7a  E..A.)@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bc4 b5b6 a7ac  ........$.;.....
0x0020   8018 16d0 bd8f 0000 0101 080a 0002 aa4f  ...............O
0x0030   004c 5f04 5245 5452 2070 6173 7377 640d  .L_.RETR.passwd.
0x0040   0a                                       .
15:00:51.416514 192.168.17.135.21 > 10.10.10.122.59909: P 3048646572:3048646638(66) ack 615594961
win 5792 <nop,nop,timestamp 5005061 174671> (DF) [tos 0x10]  (ttl 61, id 62489, len 118)
0x0000   4510 0076 f419 4000 3d06 62a5 c0a8 1187  E..v..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a7ac 24b1 3bd1  ...z........$.;.
0x0020   8018 16a0 34f1 0000 0101 080a 004c 5f05  ....4........L_.
0x0030   0002 aa4f 3135 3020 4f70 656e 696e 6720  ...O150.Opening.
0x0040   4249 4e41 5259 206d 6f64 6520 6461 7461  BINARY.mode.data
```

```
0x0050   2063                                      .c
15:00:51.453037 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646638 win 5840
<nop,nop,timestamp 174679 5005061> (DF) [tos 0x10]  (ttl 64, id 42538, len 52)
0x0000   4510 0034 a62a 4000 4006 add6 0a0a 0a7a   E..4.*@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bd1 b5b6 a7ee   ........$.;.....
0x0020   8010 16d0 c74c 0000 0101 080a 0002 aa57   .....L.........W
0x0030   004c 5f05                                 .L_.
15:00:51.455104 192.168.17.135.21 > 10.10.10.122.59909: P [tcp sum ok] 3048646638:3048646662(24)
ack 615594961 win 5792 <nop,nop,timestamp 5005068 174679> (DF) [tos 0x10]  (ttl 61, id 62490, len 76)
0x0000   4510 004c f41a 4000 3d06 62ce c0a8 1187   E..L..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a7ee 24b1 3bd1   ...z........$.;.
0x0020   8018 16a0 f85f 0000 0101 080a 004c 5f0c   ....._.......L_.
0x0030   0002 aa57 3232 3620 5472 616e 7366 6572   ...W226.Transfer
0x0040   2063 6f6d 706c 6574 652e 0d0a             .complete...
15:00:51.461145 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646662 win 5840
<nop,nop,timestamp 174679 5005068> (DF) [tos 0x10]  (ttl 64, id 42539, len 52)
0x0000   4510 0034 a62b 4000 4006 add5 0a0a 0a7a   E..4.+@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bd1 b5b6 a806   ........$.;.....
0x0020   8010 16d0 c72d 0000 0101 080a 0002 aa57   .....-.........W
0x0030   004c 5f0c                                 .L_.
15:01:00.309874 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594961:615594967(6) ack
3048646662 win 5840 <nop,nop,timestamp 175564 5005068> (DF) [tos 0x10]  (ttl 64, id 42540, len 58)
0x0000   4510 003a a62c 4000 4006 adce 0a0a 0a7a   E..:.,@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bd1 b5b6 a806   ........$.;.....
0x0020   8018 16d0 1309 0000 0101 080a 0002 adcc   ................
0x0030   004c 5f0c 5041 5356 0d0a                  .L_.PASV..
15:01:00.318651 192.168.17.135.21 > 10.10.10.122.59909: P 3048646662:3048646714(52) ack 615594967
win 5792 <nop,nop,timestamp 5005955 175564> (DF) [tos 0x10]  (ttl 61, id 62491, len 104)
0x0000   4510 0068 f41b 4000 3d06 62b1 c0a8 1187   E..h..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a806 24b1 3bd7   ...z........$.;.
0x0020   8018 16a0 f082 0000 0101 080a 004c 6283   .............Lb.
0x0030   0002 adcc 3232 3720 456e 7465 7269 6e67   ....227.Entering
0x0040   2050 6173 7369 7665 204d 6f64 6520 2831   .Passive.Mode.(1
0x0050   3932                                     92
15:01:00.318879 10.10.10.122.59909 > 192.168.17.135.21: . [tcp sum ok] ack 3048646714 win 5840
<nop,nop,timestamp 175565 5005955> (DF) [tos 0x10]  (ttl 64, id 42541, len 52)
0x0000   4510 0034 a62d 4000 4006 add3 0a0a 0a7a   E..4.-@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bd7 b5b6 a83a   ........$.;....:
0x0020   8010 16d0 c006 0000 0101 080a 0002 adcd   ................
0x0030   004c 6283                                 .Lb.
15:01:00.322287 10.10.10.122.59909 > 192.168.17.135.21: P [tcp sum ok] 615594967:615594980(13) ack
3048646714 win 5840 <nop,nop,timestamp 175565 5005955> (DF) [tos 0x10]  (ttl 64, id 42542, len 65)
0x0000   4510 0041 a62e 4000 4006 adc5 0a0a 0a7a   E..A..@.@......z
0x0010   c0a8 1187 ea05 0015 24b1 3bd7 b5b6 a83a   ........$.;....:
0x0020   8018 16d0 ab08 0000 0101 080a 0002 adcd   ................
0x0030   004c 6283 5245 5452 2073 6861 646f 770d   .Lb.RETR.shadow.
0x0040   0a                                        .
15:01:00.326963 192.168.17.135.21 > 10.10.10.122.59909: P 3048646714:3048646754(40) ack 615594980
win 5792 <nop,nop,timestamp 5005956 175565> (DF) [tos 0x10]  (ttl 61, id 62492, len 92)
0x0000   4510 005c f41c 4000 3d06 62bc c0a8 1187   E..\..@.=.b.....
0x0010   0a0a 0a7a 0015 ea05 b5b6 a83a 24b1 3be4   ...z.......:$.;.
0x0020   8018 16a0 fa8b 0000 0101 080a 004c 6284   .............Lb.
0x0030   0002 adcd 3535 3020 7368 6164 6f77 3a20   ....550.shadow:.
0x0040   4e6f 2073 7563 6820 6669 6c65 206f 7220   No.such.file.or.
0x0050   6469                                     di
……
15:18:29.606030 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793478:3824793494(16) ack
4217274497 win 64418 (DF) (ttl 128, id 26350, len 56)
0x0000   4500 0038 66ee 4000 8006 acc4 0a0a 0ad4   E..8f.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b786 fb5e 8081   .............^..
0x0020   5018 fba2 1b9c 0000 5553 4552 2061 6e6f   P.......USER.ano
0x0030   6e79 6d6f 7573 0d0a                       nymous..
```

```
15:18:29.612681 192.168.17.135.21 > 10.10.10.212.4638: . [tcp sum ok] ack 3824793494 win 5840 (DF)
[tos 0x10]  (ttl 61, id 30301, len 40)
0x0000   4510 0028 765d 4000 3d06 e055 c0a8 1187          E..(v]@.=..U....
0x0010   0a0a 0ad4 0015 121e fb5e 8081 e3f9 b796          .........^......
0x0020   5010 16d0 8853 0000 0000 0000 0000               P....S........
15:18:29.612812 192.168.17.135.21 > 10.10.10.212.4638: P 4217274497:4217274546(49) ack 3824793494
win 5840 (DF) [tos 0x10]  (ttl 61, id 30302, len 89)
0x0000   4510 0059 765e 4000 3d06 e023 c0a8 1187          E..Yv^@.=..#....
0x0010   0a0a 0ad4 0015 121e fb5e 8081 e3f9 b796          .........^......
0x0020   5018 16d0 c94c 0000 3333 3120 4775 6573          P....L..331.Gues
0x0030   7420 6c6f 6769 6e20 6f6b 2c20 7479 7065          t.login.ok,.type
0x0040   2079 6f75 7220 6e61 6d65 2061 7320 7061          .your.name.as.pa
0x0050   7373                                             ss
15:18:29.719781 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217274546 win 64369 (DF)
(ttl 128, id 26351, len 40)
0x0000   4500 0028 66ef 4000 8006 acd3 0a0a 0ad4          E..(f.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b796 fb5e 80b2          .............^..
0x0020   5010 fb71 a380 0000 0000 0000 0000               P..q..........
15:18:38.467824 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793494:3824793513(19) ack
4217274546 win 64369 (DF) (ttl 128, id 26352, len 59)
0x0000   4500 003b 66f0 4000 8006 acbf 0a0a 0ad4          E..;f.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b796 fb5e 80b2          .............^..
0x0020   5018 fb71 6c7b 0000 5041 5353 2062 6c61          P..ql{..PASS.bla
0x0030   6840 626c 6168 636f 6d0d 0a                      h@blahcom..
15:18:38.542455 192.168.17.135.21 > 10.10.10.212.4638: P 4217274546:4217274594(48) ack 3824793513
win 5840 (DF) [tos 0x10]  (ttl 61, id 30303, len 88)
0x0000   4510 0058 765f 4000 3d06 e023 c0a8 1187          E..Xv_@.=..#....
0x0010   0a0a 0ad4 0015 121e fb5e 80b2 e3f9 b7a9          .........^......
0x0020   5018 16d0 dbf0 0000 3233 3020 4775 6573          P.......230.Gues
0x0030   7420 6c6f 6769 6e20 6f6b 2c20 6163 6365          t.login.ok,.acce
0x0040   7373 2072 6573 7472 6963 7469 6f6e 7320          ss.restrictions.
0x0050   6170                                             ap
……
15:18:46.330444 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793556:3824793565(9) ack
4217274740 win 64175 (DF) (ttl 128, id 26363, len 49)
0x0000   4500 0031 66fb 4000 8006 acbe 0a0a 0ad4          E..1f.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b7d4 fb5e 8174          .............^.t
0x0020   5018 faaf 3f37 0000 4357 4420 7075 620d          P...?7..CWD.pub.
0x0030   0a                                               .
15:18:46.333990 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217274740:4217274769(29) ack
3824793565 win 5840 (DF) [tos 0x10]  (ttl 61, id 30308, len 69)
0x0000   4510 0045 7664 4000 3d06 e031 c0a8 1187          E..Evd@.=..1....
0x0010   0a0a 0ad4 0015 121e fb5e 8174 e3f9 b7dd          .........^.t....
0x0020   5018 16d0 a98f 0000 3235 3020 4357 4420          P.......250.CWD.
0x0030   636f 6d6d 616e 6420 7375 6363 6573 7366          command.successf
0x0040   756c 2e0d 0a                                     ul...
……
15:18:46.994682 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793590:3824793596(6) ack
4217274799 win 64116 (DF) (ttl 128, id 26366, len 46)
0x0000   4500 002e 66fe 4000 8006 acbe 0a0a 0ad4          E...f.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b7f6 fb5e 81af          .............^..
0x0020   5018 fa74 f467 0000 4e4c 5354 0d0a               P..t.g..NLST..
15:18:47.001109 192.168.17.135.21 > 10.10.10.212.4638: P 4217274799:4217274857(58) ack 3824793596
win 5840 (DF) [tos 0x10]  (ttl 61, id 30310, len 98)
0x0000   4510 0062 7666 4000 3d06 e012 c0a8 1187          E..bvf@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 81af e3f9 b7fc          .........^......
0x0020   5018 16d0 d34d 0000 3135 3020 4f70 656e          P....M..150.Open
0x0030   696e 6720 4249 4e41 5259 206d 6f64 6520          ing.BINARY.mode.
0x0040   6461 7461 2063 6f6e 6e65 6374 696f 6e20          data.connection.
0x0050   666f                                             fo
15:18:47.144579 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217274857 win 64058 (DF)
(ttl 128, id 26370, len 40)
```

```
0x0000   4500 0028 6702 4000 8006 acc0 0a0a 0ad4          E..(g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b7fc fb5e 81e9          ..............^..
0x0020   5010 fa3a a31a 0000 0000 0000 0000               P..:............
15:18:47.347376 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217274857:4217274881(24) ack
3824793596 win 5840 (DF) [tos 0x10]  (ttl 61, id 30311, len 64)
0x0000   4510 0040 7667 4000 3d06 e033 c0a8 1187          E..@vg@.=..3....
0x0010   0a0a 0ad4 0015 121e fb5e 81e9 e3f9 b7fc          .........^......
0x0020   5018 16d0 b76f 0000 3232 3620 5472 616e          P....o..226.Tran
0x0030   7366 6572 2063 6f6d 706c 6574 652e 0d0a          sfer.complete...
15:18:47.545165 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217274881 win 64034 (DF)
(ttl 128, id 26371, len 40)
0x0000   4500 0028 6703 4000 8006 acbf 0a0a 0ad4          E..(g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b7fc fb5e 8201          ..............^..
0x0020   5010 fa22 a31a 0000 0000 0000 0000               P.."............
15:18:48.906035 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793596:3824793604(8) ack
4217274881 win 64034 (DF) (ttl 128, id 26372, len 48)
0x0000   4500 0030 6704 4000 8006 acb6 0a0a 0ad4          E..0g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b7fc fb5e 8201          ..............^..
0x0020   5018 fa22 e05a 0000 4357 4420 2e2e 0d0a          P.."Z..CWD.....
15:18:48.908601 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217274881:4217274910(29) ack
3824793604 win 5840 (DF) [tos 0x10]  (ttl 61, id 30312, len 69)
0x0000   4510 0045 7668 4000 3d06 e02d c0a8 1187          E..Evh@.=..-....
0x0010   0a0a 0ad4 0015 121e fb5e 8201 e3f9 b804          .........^......
0x0020   5018 16d0 a8db 0000 3235 3020 4357 4420          P.......250.CWD.
0x0030   636f 6d6d 616e 6420 7375 6363 6573 7366          command.successf
0x0040   756c 2e0d 0a                                     ul...
15:18:49.047314 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217274910 win 64005 (DF)
(ttl 128, id 26373, len 40)
0x0000   4500 0028 6705 4000 8006 acbd 0a0a 0ad4          E..(g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b804 fb5e 821e          ..............^..
0x0020   5010 fa05 a312 0000 0000 0000 0000               P...............
15:18:50.368742 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793604:3824793613(9) ack
4217274910 win 64005 (DF) (ttl 128, id 26374, len 49)
0x0000   4500 0031 6706 4000 8006 acb3 0a0a 0ad4          E..1g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b804 fb5e 821e          ..............^..
0x0020   5018 fa05 4113 0000 4357 4420 6269 6e0d          P...A...CWD.bin.
0x0030   0a                                               .
15:18:50.561360 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217274910:4217274939(29) ack
3824793613 win 5840 (DF) [tos 0x10]  (ttl 61, id 30313, len 69)
0x0000   4510 0045 7669 4000 3d06 e02c c0a8 1187          E..Evi@.=..,....
0x0010   0a0a 0ad4 0015 121e fb5e 821e e3f9 b80d          .........^......
0x0020   5018 16d0 a8b5 0000 3235 3020 4357 4420          P.......250.CWD.
0x0030   636f 6d6d 616e 6420 7375 6363 6573 7366          command.successf
0x0040   756c 2e0d 0a                                     ul...
……
15:18:51.252978 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793638:3824793644(6) ack
4217274969 win 63946 (DF) (ttl 128, id 26377, len 46)
0x0000   4500 002e 6709 4000 8006 acb3 0a0a 0ad4          E...g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b826 fb5e 8259          ...........&.^.Y
0x0020   5018 f9ca f437 0000 4e4c 5354 0d0a               P....7..NLST..
15:18:51.259459 192.168.17.135.21 > 10.10.10.212.4638: P 4217274969:4217275027(58) ack 3824793644
win 5840 (DF) [tos 0x10]  (ttl 61, id 30315, len 98)
0x0000   4510 0062 766b 4000 3d06 e00d c0a8 1187          E..bvk@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 8259 e3f9 b82c          .........^.Y...,
0x0020   5018 16d0 d273 0000 3135 3020 4f70 656e          P....s..150.Open
0x0030   696e 6720 4249 4e41 5259 206d 6f64 6520          ing.BINARY.mode.
0x0040   6461 7461 2063 6f6e 6e65 6374 696f 6e20          data.connection.
0x0050   666f                                             fo
15:18:51.450637 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275027 win 63888 (DF)
(ttl 128, id 26381, len 40)
0x0000   4500 0028 670d 4000 8006 acb5 0a0a 0ad4          E..(g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b82c fb5e 8293          ...........,.^..
```

```
0x0020   5010 f990 a2ea 0000 0000 0000 0000          P.............
15:18:51.600439 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275027:4217275051(24) ack
3824793644 win 5840 (DF) [tos 0x10]  (ttl 61, id 30316, len 64)
0x0000   4510 0040 766c 4000 3d06 e02e c0a8 1187     E..@vl@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 8293 e3f9 b82c     .........^.....,
0x0020   5018 16d0 b695 0000 3232 3620 5472 616e     P.......226.Tran
0x0030   7366 6572 2063 6f6d 706c 6574 652e 0d0a     sfer.complete...
……
15:18:55.985878 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793679:3824793687(8) ack
4217275161 win 63754 (DF) (ttl 128, id 26390, len 48)
0x0000   4500 0030 6716 4000 8006 aca4 0a0a 0ad4     E..0g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b84f fb5e 8319     ...........O.^..
0x0020   5018 f90a e007 0000 4357 4420 2e2e 0d0a     P.......CWD.....
15:18:55.991755 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275161:4217275190(29) ack
3824793687 win 5840 (DF) [tos 0x10]  (ttl 61, id 30320, len 69)
0x0000   4510 0045 7670 4000 3d06 e025 c0a8 1187     E..Evp@.=..%....
0x0010   0a0a 0ad4 0015 121e fb5e 8319 e3f9 b857     .........^.....W
0x0020   5018 16d0 a770 0000 3235 3020 4357 4420     P....p..250.CWD.
0x0030   636f 6d6d 616e 6420 7375 6363 6573 7366     command.successf
0x0040   756c 2e0d 0a                                ul...
……
15:18:59.014878 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793712:3824793722(10) ack
4217275220 win 63695 (DF) (ttl 128, id 26393, len 50)
0x0000   4500 0032 6719 4000 8006 ac9f 0a0a 0ad4     E..2g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b870 fb5e 8354     ...........p.^.T
0x0020   5018 f8cf 7250 0000 4e4c 5354 202d 616c     P...rP..NLST.-al
0x0030   0d0a                                        ..
15:18:59.041282 192.168.17.135.21 > 10.10.10.212.4638: P 4217275220:4217275276(56) ack 3824793722
win 5840 (DF) [tos 0x10]  (ttl 61, id 30322, len 96)
0x0000   4510 0060 7672 4000 3d06 e008 c0a8 1187     E..`vr@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 8354 e3f9 b87a     .........^.T...z
0x0020   5018 16d0 42c2 0000 3135 3020 4f70 656e     P...B...150.Open
0x0030   696e 6720 4249 4e41 5259 206d 6f64 6520     ing.BINARY.mode.
0x0040   6461 7461 2063 6f6e 6e65 6374 696f 6e20     data.connection.
0x0050   666f                                        fo
15:18:59.161718 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275276 win 63639 (DF)
(ttl 128, id 26397, len 40)
0x0000   4500 0028 671d 4000 8006 aca5 0a0a 0ad4     E..(g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b87a fb5e 838c     ...........z.^..
0x0020   5010 f897 a29c 0000 0000 0000 0000          P.............
15:18:59.164812 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275276:4217275300(24) ack
3824793722 win 5840 (DF) [tos 0x10]  (ttl 61, id 30323, len 64)
0x0000   4510 0040 7673 4000 3d06 e027 c0a8 1187     E..@vs@.=..'....
0x0010   0a0a 0ad4 0015 121e fb5e 838c e3f9 b87a     .........^.....z
0x0020   5018 16d0 b54e 0000 3232 3620 5472 616e     P....N..226.Tran
0x0030   7366 6572 2063 6f6d 706c 6574 652e 0d0a     sfer.complete...
15:18:59.361941 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275300 win 63615 (DF)
(ttl 128, id 26398, len 40)
0x0000   4500 0028 671e 4000 8006 aca4 0a0a 0ad4     E..(g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b87a fb5e 83a4     ...........z.^..
0x0020   5010 f87f a29c 0000 0000 0000 0000          P.............
15:19:00.687206 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793722:3824793731(9) ack
4217275300 win 63615 (DF) (ttl 128, id 26399, len 49)
0x0000   4500 0031 671f 4000 8006 ac9a 0a0a 0ad4     E..1g.@.........
0x0010   c0a8 1187 121e 0015 e3f9 b87a fb5e 83a4     ...........z.^..
0x0020   5018 f87f 36a1 0000 4357 4420 6465 760d     P...6...CWD.dev.
0x0030   0a                                          .
15:19:00.694271 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275300:4217275329(29) ack
3824793731 win 5840 (DF) [tos 0x10]  (ttl 61, id 30324, len 69)
0x0000   4510 0045 7674 4000 3d06 e021 c0a8 1187     E..Evt@.=..!....
0x0010   0a0a 0ad4 0015 121e fb5e 83a4 e3f9 b883     .........^......
0x0020   5018 16d0 a6b9 0000 3235 3020 4357 4420     P.......250.CWD.
```

```
0x0030   636f 6d6d 616e 6420 7375 6363 6573 7366          command.successf
0x0040   756c 2e0d 0a                                     ul...
……
15:19:01.894545 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793756:3824793766(10) ack
4217275359 win 63556 (DF) (ttl 128, id 26402, len 50)
0x0000   4500 0032 6722 4000 8006 ac96 0a0a 0ad4          E..2g"@.........
0x0010   c0a8 1187 121e 0015 e3f9 b89c fb5e 83df          ............^..
0x0020   5018 f844 7224 0000 4e4c 5354 202d 616c          P..Dr$..NLST.-al
0x0030   0d0a                                             ..
15:19:01.910708 192.168.17.135.21 > 10.10.10.212.4638: P 4217275359:4217275415(56) ack 3824793766
win 5840 (DF) [tos 0x10]  (ttl 61, id 30326, len 96)
0x0000   4510 0060 7676 4000 3d06 e004 c0a8 1187          E..`vv@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 83df e3f9 b8a6          .........^......
0x0020   5018 16d0 420b 0000 3135 3020 4f70 656e          P...B...150.Open
0x0030   696e 6720 4249 4e41 5259 206d 6f64 6520          ing.BINARY.mode.
0x0040   6461 7461 2063 6f6e 6e65 6374 696f 6e20          data.connection.
0x0050   666f                                             fo
15:19:02.065802 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275415 win 63500 (DF)
(ttl 128, id 26406, len 40)
0x0000   4500 0028 6726 4000 8006 ac9c 0a0a 0ad4          E..(g&@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8a6 fb5e 8417          ............^..
0x0020   5010 f80c a270 0000 0000 0000 0000               P....p........
15:19:02.122771 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275415:4217275439(24) ack
3824793766 win 5840 (DF) [tos 0x10]  (ttl 61, id 30327, len 64)
0x0000   4510 0040 7677 4000 3d06 e023 c0a8 1187          E..@vw@.=..#....
0x0010   0a0a 0ad4 0015 121e fb5e 8417 e3f9 b8a6          .........^......
0x0020   5018 16d0 b497 0000 3232 3620 5472 616e          P.......226.Tran
0x0030   7366 6572 2063 6f6d 706c 6574 652e 0d0a          sfer.complete...
15:19:02.266171 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275439 win 63476 (DF)
(ttl 128, id 26407, len 40)
0x0000   4500 0028 6727 4000 8006 ac9b 0a0a 0ad4          E..(g'@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8a6 fb5e 842f          ............^./
0x0020   5010 f7f4 a270 0000 0000 0000 0000               P....p........
15:19:03.494828 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793766:3824793774(8) ack
4217275439 win 63476 (DF) (ttl 128, id 26408, len 48)
0x0000   4500 0030 6728 4000 8006 ac92 0a0a 0ad4          E..0g(@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8a6 fb5e 842f          ............^./
0x0020   5018 f7f4 dfb0 0000 4357 4420 2e2e 0d0a          P.......CWD.....
15:19:03.602577 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275439:4217275468(29) ack
3824793774 win 5840 (DF) [tos 0x10]  (ttl 61, id 30328, len 69)
0x0000   4510 0045 7678 4000 3d06 e01d c0a8 1187          E..Evx@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 842f e3f9 b8ae          .........^./....
0x0020   5018 16d0 a603 0000 3235 3020 4357 4420          P.......250.CWD.
0x0030   636f 6d6d 616e 6420 7375 6363 6573 7366          command.successf
0x0040   756c 2e0d 0a                                     ul...
……
15:19:04.420980 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793799:3824793809(10) ack
4217275498 win 63417 (DF) (ttl 128, id 26411, len 50)
0x0000   4500 0032 672b 4000 8006 ac8d 0a0a 0ad4          E..2g+@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8c7 fb5e 846a          ............^.j
0x0020   5018 f7b9 71f9 0000 4e4c 5354 202d 616c          P...q...NLST.-al
0x0030   0d0a                                             ..
15:19:04.432622 192.168.17.135.21 > 10.10.10.212.4638: P 4217275498:4217275554(56) ack 3824793809
win 5840 (DF) [tos 0x10]  (ttl 61, id 30330, len 96)
0x0000   4510 0060 767a 4000 3d06 e000 c0a8 1187          E..`vz@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 846a e3f9 b8d1          .........^.j....
0x0020   5018 16d0 4155 0000 3135 3020 4f70 656e          P...AU..150.Open
0x0030   696e 6720 4249 4e41 5259 206d 6f64 6520          ing.BINARY.mode.
0x0040   6461 7461 2063 6f6e 6e65 6374 696f 6e20          data.connection.
0x0050   666f                                             fo
15:19:04.569446 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275554 win 63361 (DF)
(ttl 128, id 26415, len 40)
```

```
0x0000   4500 0028 672f 4000 8006 ac93 0a0a 0ad4          E..(g/@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8d1 fb5e 84a2          ..............^..
0x0020   5010 f781 a245 0000 0000 0000 0000                P....E........
15:19:04.743209 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275554:4217275578(24) ack
3824793809 win 5840 (DF) [tos 0x10]  (ttl 61, id 30331, len 64)
0x0000   4510 0040 767b 4000 3d06 e01f c0a8 1187          E..@v{@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 84a2 e3f9 b8d1          .........^......
0x0020   5018 16d0 b3e1 0000 3232 3620 5472 616e          P.......226.Tran
0x0030   7366 6572 2063 6f6d 706c 6574 652e 0d0a          sfer.complete...
15:19:04.869879 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275578 win 63337 (DF)
(ttl 128, id 26416, len 40)
0x0000   4500 0028 6730 4000 8006 ac92 0a0a 0ad4          E..(g0@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8d1 fb5e 84ba          ..............^..
0x0020   5010 f769 a245 0000 0000 0000 0000                P..i.E........
15:19:06.140660 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793809:3824793818(9) ack
4217275578 win 63337 (DF) (ttl 128, id 26417, len 49)
0x0000   4500 0031 6731 4000 8006 ac88 0a0a 0ad4          E..1g1@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8d1 fb5e 84ba          ..............^..
0x0020   5018 f769 483b 0000 4357 4420 6574 630d          P..iH;..CWD.etc.
0x0030   0a                                               .
15:19:06.255494 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275578:4217275607(29) ack
3824793818 win 5840 (DF) [tos 0x10]  (ttl 61, id 30332, len 69)
0x0000   4510 0045 767c 4000 3d06 e019 c0a8 1187          E..Ev|@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 84ba e3f9 b8da          .........^......
0x0020   5018 16d0 a54c 0000 3235 3020 4357 4420          P....L..250.CWD.
0x0030   636f 6d6d 616e 6420 7375 6363 6573 7366          command.successf
0x0040   756c 2e0d 0a                                     ul...
……
15:20:41.851616 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793843:3824793853(10) ack
4217275637 win 63278 (DF) (ttl 128, id 26420, len 50)
0x0000   4500 0032 6734 4000 8006 ac84 0a0a 0ad4          E..2g4@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8f3 fb5e 84f5          ..............^..
0x0020   5018 f72e 71cd 0000 4e4c 5354 202d 616c          P...q...NLST.-al
0x0030   0d0a                                             ..
15:20:41.869200 192.168.17.135.21 > 10.10.10.212.4638: P 4217275637:4217275693(56) ack 3824793853
win 5840 (DF) [tos 0x10]  (ttl 61, id 30334, len 96)
0x0000   4510 0060 767e 4000 3d06 dffc c0a8 1187          E..`v~@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 84f5 e3f9 b8fd          .........^......
0x0020   5018 16d0 409e 0000 3135 3020 4f70 656e          P...@...150.Open
0x0030   696e 6720 4249 4e41 5259 206d 6f64 6520          ing.BINARY.mode.
0x0040   6461 7461 2063 6f6e 6e65 6374 696f 6e20          data.connection.
0x0050   666f                                             fo
15:20:42.008462 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275693 win 63222 (DF)
(ttl 128, id 26424, len 40)
0x0000   4500 0028 6738 4000 8006 ac8a 0a0a 0ad4          E..(g8@.........
0x0010   c0a8 1187 121e 0015 e3f9 b8fd fb5e 852d          ..............^.-
0x0020   5010 f6f6 a219 0000 0000 0000 0000                P.............
15:20:42.226652 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275693:4217275717(24) ack
3824793853 win 5840 (DF) [tos 0x10]  (ttl 61, id 30335, len 64)
0x0000   4510 0040 767f 4000 3d06 e01b c0a8 1187          E..@v.@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 852d e3f9 b8fd          .........^.-....
0x0020   5018 16d0 b32a 0000 3232 3620 5472 616e          P....*..226.Tran
0x0030   7366 6572 2063 6f6d 706c 6574 652e 0d0a          sfer.complete...
15:20:42.409060 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275717 win 63198 (DF)
(ttl 128, id 26425, len 40)
……
15:20:59.733669 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275747 win 63168 (DF)
(ttl 128, id 26427, len 40)
0x0000   4500 0028 673b 4000 8006 ac87 0a0a 0ad4          E..(g;@.........
0x0010   c0a8 1187 121e 0015 e3f9 b909 fb5e 8563          ..............^.c
0x0020   5010 f6c0 a20d 0000 0000 0000 0000                P.............
```

```
15:21:04.259234 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793865:3824793890(25) ack
4217275747 win 63168 (DF) (ttl 128, id 26428, len 65)
0x0000   4500 0041 673c 4000 8006 ac6d 0a0a 0ad4        E..Ag<@....m....
0x0010   c0a8 1187 121e 0015 e3f9 b909 fb5e 8563        .............^.c
0x0020   5018 f6c0 1c88 0000 504f 5254 2031 302c        P.......PORT.10,
0x0030   3130 2c31 302c 3231 322c 3138 2c33 390d        10,10,212,18,39.
0x0040   0a                                             .
15:21:04.262192 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275747:4217275777(30) ack
3824793890 win 5840 (DF) [tos 0x10]  (ttl 61, id 30337, len 70)
0x0000   4510 0046 7681 4000 3d06 e013 c0a8 1187        E..Fv.@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 8563 e3f9 b922        .........^.c...."
0x0020   5018 16d0 c4d7 0000 3230 3020 504f 5254        P.......200.PORT
0x0030   2063 6f6d 6d61 6e64 2073 7563 6365 7373        .command.success
0x0040   6675 6c2e 0d0a                                 ful...
15:21:04.263547 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793890:3824793903(13) ack
4217275777 win 63138 (DF) (ttl 128, id 26429, len 53)
0x0000   4500 0035 673d 4000 8006 ac78 0a0a 0ad4        E..5g=@....x....
0x0010   c0a8 1187 121e 0015 e3f9 b922 fb5e 8581        ..........."^..
0x0020   5018 f6a2 97df 0000 5245 5452 2070 6173        P.......RETR.pas
0x0030   7377 640d 0a                                   swd..
15:21:04.380204 192.168.17.135.21 > 10.10.10.212.4638: P 4217275777:4217275843(66) ack 3824793903
win 5840 (DF) [tos 0x10]  (ttl 61, id 30338, len 106)
0x0000   4510 006a 7682 4000 3d06 dfee c0a8 1187        E..jv.@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 8581 e3f9 b92f        .........^...../
0x0020   5018 16d0 eee4 0000 3135 3020 4f70 656e        P.......150.Open
0x0030   696e 6720 4249 4e41 5259 206d 6f64 6520        ing.BINARY.mode.
0x0040   6461 7461 2063 6f6e 6e65 6374 696f 6e20        data.connection.
0x0050   666f                                           fo
15:21:04.540598 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275843 win 63072 (DF)
(ttl 128, id 26433, len 40)
0x0000   4500 0028 6741 4000 8006 ac81 0a0a 0ad4        E..(gA@.........
0x0010   c0a8 1187 121e 0015 e3f9 b92f fb5e 85c3        ........../.^..
0x0020   5010 f660 a1e7 0000 0000 0000 0000             P..`...........
15:21:04.543208 192.168.17.135.21 > 10.10.10.212.4638: P [tcp sum ok] 4217275843:4217275867(24) ack
3824793903 win 5840 (DF) [tos 0x10]  (ttl 61, id 30339, len 64)
0x0000   4510 0040 7683 4000 3d06 e017 c0a8 1187        E..@v.@.=.......
0x0010   0a0a 0ad4 0015 121e fb5e 85c3 e3f9 b92f        .........^...../
0x0020   5018 16d0 b262 0000 3232 3620 5472 616e        P....b..226.Tran
0x0030   7366 6572 2063 6f6d 706c 6574 652e 0d0a        sfer.complete...
15:21:04.740892 10.10.10.212.4638 > 192.168.17.135.21: . [tcp sum ok] ack 4217275867 win 64512 (DF)
(ttl 128, id 26434, len 40)
0x0000   4500 0028 6742 4000 8006 ac80 0a0a 0ad4        E..(gB@.........
0x0010   c0a8 1187 121e 0015 e3f9 b92f fb5e 85db        ........../.^..
0x0020   5010 fc00 9c2f 0000 0000 0000 0000             P..../.........
15:22:18.705052 10.10.10.212.4638 > 192.168.17.135.21: P [tcp sum ok] 3824793903:3824793909(6) ack
4217275867 win 64512 (DF) (ttl 128, id 26435, len 46)
0x0000   4500 002e 6743 4000 8006 ac79 0a0a 0ad4        E...gC@....y....
0x0010   c0a8 1187 121e 0015 e3f9 b92f fb5e 85db        ........../.^..
0x0020   5018 fc00 f46d 0000 5155 4954 0d0a             P....m..QUIT..
```

Appendix 10

```
15:12:16.397287 10.10.10.186.1023 > 172.20.201.198.513: S [tcp sum ok] 858314989:858314989(0) win
5840 <mss 1460,sackOK,timestamp 1193955 0,nop,wscale 0> (DF) (ttl 64, id 61198, len 60)
0x0000   4500 003c ef0e 4000 4006 c10e 0a0a 0aba        E..<..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d8ed 0000 0000        ........3(......
0x0020   a002 16d0 5c8d 0000 0204 05b4 0402 080a        ....\...........
0x0030   0012 37e3 0000 0000 0103 0300                  ..7.........
15:12:16.400027 172.20.201.198.513 > 10.10.10.186.1023: S [tcp sum ok] 1401060027:1401060027(0) ack
858314990 win 32120 <mss 1460,sackOK,timestamp 1939034 1193955,nop,wscale 0> (DF) (ttl 62, id
60235, len 60)
```

```
0x0000   4500 003c eb4b 4000 3e06 c6d1 ac14 c9c6        E..<.K@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abb 3328 d8ee        ........S.z.3(..
0x0020   a012 7d78 911e 0000 0204 05b4 0402 080a        ..}x............
0x0030   001d 965a 0012 37e3 0103 0300                  ...Z..7.....
15:12:16.400193 10.10.10.186.1023 > 172.20.201.198.513: . [tcp sum ok] ack 1401060028 win 5840 <nop,nop,timestamp 1193957 1939034> (DF) (ttl 64, id 61199, len 52)
0x0000   4500 0034 ef0f 4000 4006 c115 0a0a 0aba        E..4..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d8ee 5382 7abc        ........3(..S.z.
0x0020   8010 16d0 268a 0000 0101 080a 0012 37e5        ....&.........7.
0x0030   001d 965a                                      ...Z
15:12:16.402079 10.10.10.186.1023 > 172.20.201.198.513: P [tcp sum ok] 858314990:858314991(1) ack 1401060028 win 5840 <nop,nop,timestamp 1193957 1939034> (DF) (ttl 64, id 61200, len 53)
0x0000   4500 0035 ef10 4000 4006 c113 0a0a 0aba        E..5..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d8ee 5382 7abc        ........3(..S.z.
0x0020   8018 16d0 2681 0000 0101 080a 0012 37e5        ....&.........7.
0x0030   001d 965a 00                                   ...Z.
15:12:16.405499 172.20.201.198.513 > 10.10.10.186.1023: . [tcp sum ok] ack 858314991 win 32120 <nop,nop,timestamp 1939034 1193957> (DF) (ttl 62, id 60236, len 52)
0x0000   4500 0034 eb4c 4000 3e06 c6d8 ac14 c9c6        E..4.L@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abc 3328 d8ef        ........S.z.3(..
0x0020   8010 7d78 bfe0 0000 0101 080a 001d 965a        ..}x...........Z
0x0030   0012 37e5                                      ..7.
15:12:16.405633 10.10.10.186.1023 > 172.20.201.198.513: P [tcp sum ok] 858314991:858315008(17) ack 1401060028 win 5840 <nop,nop,timestamp 1193959 1939034> (DF) (ttl 64, id 61201, len 69)
0x0000   4500 0045 ef11 4000 4006 c102 0a0a 0aba        E..E..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d8ef 5382 7abc        ........3(..S.z.
0x0020   8018 16d0 63b0 0000 0101 080a 0012 37e7        ....c.........7.
0x0030   001d 965a 2d66 726f 6f74 002d 6672 6f6f        ...Z-froot.-froo
0x0040   7400 6964 00                                  t.id.
15:12:16.410333 172.20.201.198.513 > 10.10.10.186.1023: . [tcp sum ok] ack 858315008 win 32120 <nop,nop,timestamp 1939035 1193959> (DF) (ttl 62, id 60237, len 52)
0x0000   4500 0034 eb4d 4000 3e06 c6d7 ac14 c9c6        E..4.M@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abc 3328 d900        ........S.z.3(..
0x0020   8010 7d78 bfcc 0000 0101 080a 001d 965b        ..}x...........[
0x0030   0012 37e7                                      ..7.
15:12:16.566867 172.20.201.198.513 > 10.10.10.186.1023: P [tcp sum ok] 1401060028:1401060029(1) ack 858315008 win 32120 <nop,nop,timestamp 1939048 1193959> (DF) [tos 0x10]  (ttl 62, id 60242, len 53)
0x0000   4510 0035 eb52 4000 3e06 c6c1 ac14 c9c6        E..5.R@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abc 3328 d900        ........S.z.3(..
0x0020   8018 7d78 bfb6 0000 0101 080a 001d 9668        ..}x...........h
0x0030   0012 37e7 00                                   ..7..
15:12:16.567003 10.10.10.186.1023 > 172.20.201.198.513: . [tcp sum ok] ack 1401060029 win 5840 <nop,nop,timestamp 1194042 1939048> (DF) (ttl 64, id 61202, len 52)
0x0000   4500 0034 ef12 4000 4006 c112 0a0a 0aba        E..4..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d900 5382 7abd        ........3(..S.z.
0x0020   8010 16d0 2614 0000 0101 080a 0012 383a        ....&.........8:
0x0030   001d 9668                                      ...h
15:12:16.589009 172.20.201.198.513 > 10.10.10.186.1023: P [tcp sum ok] 1401060029:1401060030(1) ack 858315008 win 32120 urg 1 <nop,nop,timestamp 1939050 1194042> (DF) [tos 0x10]  (ttl 62, id 60243, len 53)
0x0000   4510 0035 eb53 4000 3e06 c6c0 ac14 c9c6        E..5.S@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abd 3328 d900        ........S.z.3(..
0x0020   8038 7d78 3f3f 0001 0101 080a 001d 966a        .8}x??.........j
0x0030   0012 383a 80                                   ..8:.
15:12:16.589132 10.10.10.186.1023 > 172.20.201.198.513: . [tcp sum ok] ack 1401060030 win 5840 <nop,nop,timestamp 1194053 1939050> (DF) (ttl 64, id 61203, len 52)
0x0000   4500 0034 ef13 4000 4006 c111 0a0a 0aba        E..4..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d900 5382 7abe        ........3(..S.z.
0x0020   8010 16d0 2606 0000 0101 080a 0012 3845        ....&.........8E
0x0030   001d 966a                                      ...j
15:12:16.695442 172.20.201.198.513 > 10.10.10.186.1023: F [tcp sum ok] 1401060030:1401060030(0) ack 858315008 win 32120 <nop,nop,timestamp 1939061 1194053> (DF) [tos 0x10]  (ttl 62, id 60250, len 52)
```

```
0x0000   4510 0034 eb5a 4000 3e06 c6ba ac14 c9c6          E..4.Z@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abe 3328 d900          ........S.z.3(..
0x0020   8011 7d78 bf51 0000 0101 080a 001d 9675          ..}x.Q.........u
0x0030   0012 3845                                        ..8E
15:12:16.696342 10.10.10.186.1023 > 172.20.201.198.513: P [tcp sum ok] 858315008:858315012(4) ack
1401060031 win 5840 <nop,nop,timestamp 1194108 1939061> (DF) (ttl 64, id 61204, len 56)
0x0000   4500 0038 ef14 4000 4006 c10c 0a0a 0aba          E..8..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d900 5382 7abf          ........3(..S.z.
0x0020   8018 16d0 af48 0000 0101 080a 0012 387c          .....H........8|
0x0030   001d 9675 6964 0d0a                              ...uid..
15:12:16.696878 10.10.10.186.1023 > 172.20.201.198.513: F [tcp sum ok] 858315012:858315012(0) ack
1401060031 win 5840 <nop,nop,timestamp 1194108 1939061> (DF) (ttl 64, id 61205, len 52)
0x0000   4500 0034 ef15 4000 4006 c10f 0a0a 0aba          E..4..@.@.......
0x0010   ac14 c9c6 03ff 0201 3328 d904 5382 7abf          ........3(..S.z.
0x0020   8011 16d0 25be 0000 0101 080a 0012 387c          ....%.........8|
0x0030   001d 9675                                        ...u
15:12:16.703417 172.20.201.198.513 > 10.10.10.186.1023: . [tcp sum ok] ack 858315013 win 32120
<nop,nop,timestamp 1939061 1194108> (DF) [tos 0x10]  (ttl 62, id 60251, len 52)
0x0000   4510 0034 eb5b 4000 3e06 c6b9 ac14 c9c6          E..4.[@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abf 3328 d905          ........S.z.3(..
0x0020   8010 7d78 bf15 0000 0101 080a 001d 9675          ..}x..........u
0x0030   0012 387c                                        ..8|
15:12:16.717049 172.20.201.198.513 > 10.10.10.186.1023: R [tcp sum ok] 1401060031:1401060031(0) ack
858315013 win 32120 <nop,nop,timestamp 1939062 1194108> (DF) [tos 0x10]  (ttl 62, id 60253, len 52)
0x0000   4510 0034 eb5d 4000 3e06 c6b7 ac14 c9c6          E..4.]@.>.......
0x0010   0a0a 0aba 0201 03ff 5382 7abf 3328 d905          ........S.z.3(..
0x0020   8014 7d78 bf10 0000 0101 080a 001d 9676          ..}x..........v
0x0030   0012 387c                                        ..8|
15:15:46.338420 10.10.10.186.1023 > 172.20.201.198.513: S [tcp sum ok] 1081587309:1081587309(0) win
5840 <mss 1460,sackOK,timestamp 1301464 0,nop,wscale 0> (DF) (ttl 64, id 28085, len 60)
0x0000   4500 003c 6db5 4000 4006 4268 0a0a 0aba          E..<m.@.@.Bh....
0x0010   ac14 c9c6 03ff 0201 4077 b66d 0000 0000          ........@w.m....
0x0020   a002 16d0 cdc7 0000 0204 05b4 0402 080a          ................
0x0030   0013 dbd8 0000 0000 0103 0300                    ............
15:15:46.374160 172.20.201.198.513 > 10.10.10.186.1023: S [tcp sum ok] 1611473452:1611473452(0) ack
1081587310 win 32120 <mss 1460,sackOK,timestamp 1960075 1301464,nop,wscale 0> (DF) (ttl 62, id
1995, len 60)
0x0000   4500 003c 07cb 4000 3e06 aa52 ac14 c9c6          E..<..@.>..R....
0x0010   0a0a 0aba 0201 03ff 600d 222c 4077 b66e          ........`.",@w.n
0x0020   a012 7d78 fc2b 0000 0204 05b4 0402 080a          ..}x.+..........
0x0030   001d e88b 0013 dbd8 0103 0300                    ............
15:15:46.374333 10.10.10.186.1023 > 172.20.201.198.513: . [tcp sum ok] ack 1611473453 win 5840
<nop,nop,timestamp 1301483 1960075> (DF) (ttl 64, id 28086, len 52)
0x0000   4500 0034 6db6 4000 4006 426f 0a0a 0aba          E..4m.@.@.Bo....
0x0010   ac14 c9c6 03ff 0201 4077 b66e 600d 222d          ........@w.n`."-
0x0020   8010 16d0 9186 0000 0101 080a 0013 dbeb          ................
0x0030   001d e88b                                        ....
15:15:46.394724 10.10.10.186.1023 > 172.20.201.198.513: P [tcp sum ok] 1081587310:1081587311(1) ack
1611473453 win 5840 <nop,nop,timestamp 1301493 1960075> (DF) (ttl 64, id 28087, len 53)
0x0000   4500 0035 6db7 4000 4006 426d 0a0a 0aba          E..5m.@.@.Bm....
0x0010   ac14 c9c6 03ff 0201 4077 b66e 600d 222d          ........@w.n`."-
0x0020   8018 16d0 9173 0000 0101 080a 0013 dbf5          .....s..........
0x0030   001d e88b 00                                     .....
15:15:46.412880 172.20.201.198.513 > 10.10.10.186.1023: . [tcp sum ok] ack 1081587311 win 32120
<nop,nop,timestamp 1960080 1301493> (DF) (ttl 62, id 2001, len 52)
0x0000   4500 0034 07d1 4000 3e06 aa54 ac14 c9c6          E..4..@.>..T....
0x0010   0a0a 0aba 0201 03ff 600d 222d 4077 b66f          ........`."-@w.o
0x0020   8010 7d78 2ace 0000 0101 080a 001d e890          ..}x*...........
0x0030   0013 dbf5                                        ....
15:15:46.412984 10.10.10.186.1023 > 172.20.201.198.513: P [tcp sum ok] 1081587311:1081587319(8) ack
1611473453 win 5840 <nop,nop,timestamp 1301502 1960080> (DF) (ttl 64, id 28088, len 60)
0x0000   4500 003c 6db8 4000 4006 4265 0a0a 0aba          E..<m.@.@.Be....
```

```
0x0010   ac14 c9c6 03ff 0201 4077 b66f 600d 222d        ........@w.o`."-
0x0020   8018 16d0 3a11 0000 0101 080a 0013 dbfe        ....:...........
0x0030   001d e890 6e65 7373 7573 0000                  ....nessus..
15:15:46.431594 172.20.201.198.513 > 10.10.10.186.1023: . [tcp sum ok] ack 1081587319 win 32120
<nop,nop,timestamp 1960082 1301502> (DF) (ttl 62, id 2002, len 52)
0x0000   4500 0034 07d2 4000 3e06 aa53 ac14 c9c6        E..4..@.>..S....
0x0010   0a0a 0aba 0201 03ff 600d 222d 4077 b677        ........`."-@w.w
0x0020   8010 7d78 2abb 0000 0101 080a 001d e892        ..}x*...........
0x0030   0013 dbfe                                      ....
15:16:26.393752 10.10.10.186.1023 > 172.20.201.198.513: F [tcp sum ok] 1081587319:1081587319(0) ack
1611473453 win 5840 <nop,nop,timestamp 1321976 1960082> (DF) (ttl 64, id 28089, len 52)
0x0000   4500 0034 6db9 4000 4006 426c 0a0a 0aba        E..4m.@.@.Bl....
0x0010   ac14 c9c6 03ff 0201 4077 b677 600d 222d        ........@w.w`."-
0x0020   8011 16d0 4168 0000 0101 080a 0014 2bf8        ....Ah........+.
0x0030   001d e892                                      ....
15:16:26.407113 172.20.201.198.513 > 10.10.10.186.1023: . [tcp sum ok] ack 1081587320 win 32120
<nop,nop,timestamp 1964077 1321976> (DF) [tos 0x10]  (ttl 62, id 3859, len 52)
0x0000   4510 0034 0f13 4000 3e06 a302 ac14 c9c6        E..4..@.>.......
0x0010   0a0a 0aba 0201 03ff 600d 222d 4077 b678        ........`."-@w.x
0x0020   8010 7d78 cb24 0000 0101 080a 001d f82d        ..}x.$.........-
0x0030   0014 2bf8                                      ..+.
15:16:26.408036 172.20.201.198.513 > 10.10.10.186.1023: F [tcp sum ok] 1611473453:1611473453(0) ack
1081587320 win 32120 <nop,nop,timestamp 1964077 1321976> (DF) [tos 0x10]  (ttl 62, id 3860, len 52)
0x0000   4510 0034 0f14 4000 3e06 a301 ac14 c9c6        E..4..@.>.......
0x0010   0a0a 0aba 0201 03ff 600d 222d 4077 b678        ........`."-@w.x
0x0020   8011 7d78 cb23 0000 0101 080a 001d f82d        ..}x.#.........-
0x0030   0014 2bf8                                      ..+.
15:16:26.408147 10.10.10.186.1023 > 172.20.201.198.513: . [tcp sum ok] ack 1611473454 win 5840
<nop,nop,timestamp 1321984 1964077> (DF) [tos 0x10]  (ttl 64, id 0, len 52)
0x0000   4510 0034 0000 4000 4006 b015 0a0a 0aba        E..4..@.@.......
0x0010   ac14 c9c6 03ff 0201 4077 b678 600d 222e        ........@w.x`.".
0x0020   8010 16d0 31c4 0000 0101 080a 0014 2c00        ....1.........,.
0x0030   001d f82d                                      ...-
```

Appendix 11

Source IP Address	# of Hit	Source IP Address	# of Hit
10.10.10.165	100547	10.30.30.2	576
10.10.10.195	58619	10.10.10.2	407
172.20.11.80	49341	192.168.17.68	366
172.20.201.198	41108	192.168.17.66	354
10.10.10.112	28247	192.168.17.135	352
10.10.10.231	21709	10.10.10.226	298
10.10.10.113	18256	10.10.10.122	194
10.10.10.186	17275	10.10.10.194	181
10.10.10.224	16936	192.168.17.2	132
172.20.11.2	13312	192.168.22.207	112
172.20.11.52	10337	192.168.117.1	78
172.20.201.1	8203	192.168.213.1	78
172.20.201.135	7297	10.10.10.222	48
10.10.10.147	6015	10.10.10.230	31
10.10.10.228	5876	192.168.17.129	30
10.10.10.174	5775	169.254.135.50	18
10.10.10.141	5356	192.168.17.65	17

10.10.10.164	4827	10.10.10.123	16
10.10.10.234	4808	0.0.0.0	15
172.20.11.1	4205	10.10.10.111	10
10.10.10.196	3902	172.16.9.13	10
172.20.11.3	3283	192.168.222.1	8
10.10.10.160	2980	192.168.84.1	8
172.20.201.2	1635	172.16.8.229	4
10.10.10.142	1550	238.122.10.140	3
10.10.10.212	1361	10.10.10.117	1
10.10.10.232	1341	10.10.10.144	1
10.10.10.1	892	172.16.8.189	1
10.10.10.214	802		

Appendix 12

Source IP Address	# of Hit	Source IP Address	# of Hit
10.10.10.113	18222	10.10.10.232	20
10.10.10.165	5737	0.0.0.0	15
10.10.10.231	559	10.10.10.228	15
10.10.10.164	549	10.10.10.230	11
10.10.10.234	429	10.10.10.222	9
10.10.10.141	386	172.20.11.2	9
10.10.10.2	375	10.10.10.160	7
10.10.10.195	113	10.10.10.122	6
10.10.10.194	79	10.10.10.212	6
10.10.10.112	67	169.254.135.50	6
172.20.201.198	66	10.10.10.142	3
10.10.10.224	48	10.10.10.226	3
10.10.10.196	35	10.10.10.214	2
10.10.10.186	31	10.10.10.111	1
172.20.201.135	24	10.10.10.144	1
10.10.10.174	22	10.10.10.147	1

Appendix 13

```
15:04:52.922432 169.254.135.50.137 > 169.254.255.255.137:  [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1420, len 78)
15:04:53.673315 169.254.135.50.137 > 169.254.255.255.137:  [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1421, len 78)
15:04:54.424387 169.254.135.50.137 > 169.254.255.255.137:  [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1422, len 78)
15:05:16.966028 169.254.135.50.137 > 169.254.255.255.137:  [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1432, len 78)
15:05:17.716902 169.254.135.50.137 > 169.254.255.255.137:  [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1433, len 78)
```

15:05:18.469078 169.254.135.50.137 > 169.254.255.255.137: [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1434, len 78)
15:06:27.484548 169.254.135.50.137 > 169.254.255.255.137: [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1444, len 78)
15:06:28.235440 169.254.135.50.137 > 169.254.255.255.137: [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1445, len 78)
15:06:28.986488 169.254.135.50.137 > 169.254.255.255.137: [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1446, len 78)
15:06:37.430027 169.254.135.50.138 > 169.254.255.255.138:
WARNING: Short packet. Try increasing the snap length
 (ttl 128, id 1453, len 202)
15:06:37.430120 169.254.135.50.137 > 169.254.255.255.137: [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1455, len 78)
15:06:38.179345 169.254.135.50.137 > 169.254.255.255.137: [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1456, len 78)
15:06:38.930373 169.254.135.50.137 > 169.254.255.255.137: [udp sum ok]
>>> NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
 (ttl 128, id 1457, len 78)
15:07:40.897647 169.254.135.50.138 > 169.254.255.255.138:
WARNING: Short packet. Try increasing the snap length
 (ttl 128, id 1471, len 237)
15:09:49.647326 169.254.135.50.137 > 169.254.255.255.137:
>>> NBT UDP PACKET(137): REGISTRATION; REQUEST; BROADCAST
ResourceRecords:
AdditionalData:
Data: (6 bytes)
[000] 00 00 00 00 00 00   ......
 (ttl 128, id 1490, len 96)
15:09:50.397866 169.254.135.50.137 > 169.254.255.255.137:
>>> NBT UDP PACKET(137): REGISTRATION; REQUEST; BROADCAST
ResourceRecords:
AdditionalData:
Data: (6 bytes)
[000] 00 00 00 00 00 00   ......
 (ttl 128, id 1492, len 96)
15:09:51.148935 169.254.135.50.137 > 169.254.255.255.137:
>>> NBT UDP PACKET(137): REGISTRATION; REQUEST; BROADCAST
ResourceRecords:
AdditionalData:
Data: (6 bytes)
[000] 00 00 00 00 00 00   ......
 (ttl 128, id 1494, len 96)
15:09:51.899998 169.254.135.50.137 > 169.254.255.255.137:
>>> NBT UDP PACKET(137): REGISTRATION; REQUEST; BROADCAST
ResourceRecords:
AdditionalData:
Data: (6 bytes)
[000] 00 00 00 00 00 00   ......
 (ttl 128, id 1497, len 96)

Appendix 14

[**] [116:97:1] (snort_decoder): Short UDP packet, length field > payload length [**]
11/18/03-15:06:37.430027 169.254.135.50:0 -> 169.254.255.255:0
UDP TTL:128 TOS:0x0 ID:1453 IpLen:20 DgmLen:202

UDP header truncated
--
[**] [116:97:1] (snort_decoder): Short UDP packet, length field > payload length [**]
11/18/03-15:07:40.897647 169.254.135.50:0 -> 169.254.255.255:0
UDP TTL:128 TOS:0x0 ID:1471 IpLen:20 DgmLen:237
UDP header truncated
--
[**] [116:97:1] (snort_decoder): Short UDP packet, length field > payload length [**]
11/18/03-15:09:49.647326 169.254.135.50:0 -> 169.254.255.255:0
UDP TTL:128 TOS:0x0 ID:1490 IpLen:20 DgmLen:96
UDP header truncated
--
[**] [116:97:1] (snort_decoder): Short UDP packet, length field > payload length [**]
11/18/03-15:09:50.397866 169.254.135.50:0 -> 169.254.255.255:0
UDP TTL:128 TOS:0x0 ID:1492 IpLen:20 DgmLen:96
UDP header truncated
--
[**] [116:97:1] (snort_decoder): Short UDP packet, length field > payload length [**]
11/18/03-15:09:51.148935 169.254.135.50:0 -> 169.254.255.255:0
UDP TTL:128 TOS:0x0 ID:1494 IpLen:20 DgmLen:96
UDP header truncated
--
[**] [116:97:1] (snort_decoder): Short UDP packet, length field > payload length [**]
11/18/03-15:09:51.899998 169.254.135.50:0 -> 169.254.255.255:0
UDP TTL:128 TOS:0x0 ID:1497 IpLen:20 DgmLen:96
UDP header truncated

Appendix 15

15:09:26.679627 238.122.10.140.42200 > 172.20.11.2.31097: . [tcp sum ok] ack 0 win 2048 [tos 0x8] (ttl 255, id 51276, len 40)
0x0000 4508 0028 c84c 0000 ff06 435e ee7a 0a8c E..(.L....C^.z..
0x0010 ac14 0b02 a4d8 7979 1179 af51 0000 0000 ......yy.y.Q....
0x0020 5010 0800 189b 0000 0000 0000 0000 P.....
15:09:31.778240 238.122.10.140.42200 > 172.20.11.2.31097: . [tcp sum ok] ack 0 win 2048 [tos 0x8] (ttl 255, id 51276, len 40)
0x0000 4508 0028 c84c 0000 ff06 435e ee7a 0a8c E..(.L....C^.z..
0x0010 ac14 0b02 a4d8 7979 1179 af51 0000 0000 ......yy.y.Q....
0x0020 5010 0800 189b 0000 0000 0000 0000 P.....
15:09:36.841060 238.122.10.140.42200 > 172.20.11.2.31097: . [tcp sum ok] ack 0 win 2048 [tos 0x8] (ttl 255, id 51276, len 40)
0x0000 4508 0028 c84c 0000 ff06 435e ee7a 0a8c E..(.L....C^.z..
0x0010 ac14 0b02 a4d8 7979 1179 af51 0000 0000 ......yy.y.Q....
0x0020 5010 0800 189b 0000 0000 0000 0000 P.....

Appendix 16

Attacker-Target	Alerts	# of Hit
10.10.10.165 - 172.20.201.135	[116:97:1] (snort_decoder): Short UDP packet, length field > payload length	7
	[1:1411:10] SNMP public access udp	2
	[1:1417:9] SNMP request udp	14
	[1:1418:11] SNMP request tcp	6
	[1:1419:9] SNMP trap udp	10
	[1:1420:11] SNMP trap tcp	6
	[1:1421:11] SNMP AgentX/tcp request	3
	[1:1443:4] TFTP GET passwd	2

	[1:1444:3] TFTP Get	2
	[1:1672:11] FTP CWD ~ attempt	2
	[1:1777:5] FTP EXPLOIT STAT * dos attempt	4
	[1:1957:5] RPC sadmind UDP PING	3
	[1:1971:4] FTP SITE EXEC format string attempt	1
	[1:237:2] DDOS Trin00 Master to Daemon default password attempt	1
	[1:2417:1] FTP format string attempt	1
	[1:323:5] FINGER root query	1
	[1:326:9] FINGER remote command execution attempt	1
	[1:327:8] FINGER remote command pipe execution attempt	1
	[1:330:9] FINGER redirection attempt	1
	[1:332:8] FINGER 0 query	1
	[1:336:10] FTP CWD ~root attempt	1
	[1:361:14] FTP SITE EXEC attempt	3
	[1:465:3] ICMP ISS Pinger	2
	[1:467:3] ICMP Nemesis v1.1 Echo	1
	[1:469:3] ICMP PING NMAP	5
	[1:519:6] TFTP parent directory	1
	[1:520:5] TFTP root directory	1
	[1:604:5] RSERVICES rsh froot	1
	[1:659:8] SMTP expn decode	1
10.10.10.228 - 172.20.201.135	[116:97:1] (snort_decoder): Short UDP packet, length field > payload length	1
	[1:1228:6] SCAN nmap XMAS	1
	[1:1418:11] SNMP request tcp	1
	[1:1420:11] SNMP trap tcp	1
	[1:1421:11] SNMP AgentX/tcp request	1
	[1:1971:4] FTP SITE EXEC format string attempt	1
	[1:2417:1] FTP format string attempt	1
	[1:361:14] FTP SITE EXEC attempt	1
	[1:469:3] ICMP PING NMAP	1
10.10.10.186 - 172.20.201.198	[116:97:1] (snort_decoder): Short UDP packet, length field > payload length	1
	[1:1228:6] SCAN nmap XMAS	1
	[1:1418:11] SNMP request tcp	1
	[1:1420:11] SNMP trap tcp	1
	[1:1421:11] SNMP AgentX/tcp request	1
	[1:1672:11] FTP CWD ~ attempt	3
	[1:1971:4] FTP SITE EXEC format string attempt	5
	[1:1992:7] FTP LIST directory traversal attempt	2
	[1:2417:1] FTP format string attempt	5
	[1:335:5] FTP .rhosts	1
	[1:336:10] FTP CWD ~root attempt	2
	[1:361:14] FTP SITE EXEC attempt	6
	[1:604:5] RSERVICES rsh froot	1
10.10.10.196 - 172.20.201.198	[1:1971:4] FTP SITE EXEC format string attempt	2
	[1:2417:1] FTP format string attempt	2
	[1:361:14] FTP SITE EXEC attempt	2

10.10.10.165 - 172.20.201.198	[116:97:1] (snort_decoder): Short UDP packet, length field > payload length	11
	[1:1411:10] SNMP public access udp	42
	[1:1417:9] SNMP request udp	56
	[1:1418:11] SNMP request tcp	6
	[1:1419:9] SNMP trap udp	10
	[1:1420:11] SNMP trap tcp	6
	[1:1421:11] SNMP AgentX/tcp request	3
	[1:1443:4] TFTP GET passwd	2
	[1:1444:3] TFTP Get	2
	[1:1672:11] FTP CWD ~ attempt	2
	[1:1777:5] FTP EXPLOIT STAT * dos attempt	4
	[1:1957:5] RPC sadmind UDP PING	3
	[1:237:2] DDOS Trin00 Master to Daemon default password attempt	1
	[1:323:5] FINGER root query	1
	[1:326:9] FINGER remote command execution attempt	1
	[1:327:8] FINGER remote command pipe execution attempt	1
	[1:330:9] FINGER redirection attempt	1
	[1:332:8] FINGER 0 query	1
	[1:336:10] FTP CWD ~root attempt	1
	[1:361:14] FTP SITE EXEC attempt	2
	[1:465:3] ICMP ISS Pinger	2
	[1:467:3] ICMP Nemesis v1.1 Echo	1
	[1:469:3] ICMP PING NMAP	5
	[1:519:6] TFTP parent directory	1
	[1:520:5] TFTP root directory	1
	[1:604:5] RSERVICES rsh froot	1
	[1:659:8] SMTP expn decode	1
10.10.10.122 - 192.168.17.135	[1:1928:3] FTP shadow retrieval attempt	1
	[1:1992:7] FTP LIST directory traversal attempt	3
	[1:356:5] FTP passwd retrieval attempt	1
10.10.10.212 - 192.168.17.135	[1:356:5] FTP passwd retrieval attempt	1

Last Updated: June 25th, 2018

Upcoming Training

SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LA	Jul 30, 2018 - Aug 06, 2018	Live Event
San Antonio 2018 - SEC503: Intrusion Detection In-Depth	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS Brussels October 2018	Brussels, Belgium	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Northern VA Fall- Tysons 2018	Tysons, VA	Oct 13, 2018 - Oct 20, 2018	Live Event
SANS Denver 2018	Denver, CO	Oct 15, 2018 - Oct 20, 2018	Live Event
SANS October Singapore 2018	Singapore, Singapore	Oct 15, 2018 - Oct 27, 2018	Live Event
Mentor Session - SEC503	Ankara, Turkey	Oct 31, 2018 - Dec 19, 2018	Mentor
Mentor Session - SEC503	Ballston, VA	Nov 01, 2018 - Dec 06, 2018	Mentor
SANS Dallas Fall 2018	Dallas, TX	Nov 05, 2018 - Nov 10, 2018	Live Event
San Diego Fall 2018 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Nov 12, 2018 - Nov 17, 2018	vLive
SANS San Diego Fall 2018	San Diego, CA	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Stockholm 2018	Stockholm, Sweden	Nov 26, 2018 - Dec 01, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZ	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DC	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced