Global Information Assurance Certification Paper

Capitol SANS
GIAC
Intrusion Detection Practical Assignment

Name: Chan Lee
Date: February 20, 2001

ASSIGNMENT 1 – NETWORK DETECTS

Attack 1

Network Detect:

```
Scan report: slip139-92-139-249.stp.ru.ibm.net [139.92.139.249].
===================== 1/2/01 PST (GMT -8)===============
(335): 12:32:27 src slip139-92-139-249.stp.ru.ibm.net s_port 2528 dst
  aaa.bbb.ccc.0 TCP 3389
(346): 12:32:27 src slip139-92-139-249.stp.ru.ibm.net s_port 2539 dst
  aaa.bbb.ccc.11 TCP 3389
(347): 12:32:27 src slip139-92-139-249.stp.ru.ibm.net s_port 2540 dst
  aaa.bbb.ccc.12 TCP 3389
(348): 12:32:27 src slip139-92-139-249.stp.ru.ibm.net s_port 2541 dst
  aaa.bbb.ccc.13 TCP 3389
(349): 12:32:27 src slip139-92-139-249.stp.ru.ibm.net s_port 2542 dst
  aaa.bbb.ccc.14 TCP 3389
...
(840): 12:33:00 src slip139-92-139-249.stp.ru.ibm.net s_port 3034 dst
  aaa.bbb.ccd.250 TCP 3389
(841): 12:33:00 src slip139-92-139-249.stp.ru.ibm.net s_port 3035 dst
  aaa.bbb.ccd.251 TCP 3389
(842): 12:33:00 src slip139-92-139-249.stp.ru.ibm.net s_port 3036 dst
  aaa.bbb.ccd.252 TCP 3389
(843): 12:33:00 src slip139-92-139-249.stp.ru.ibm.net s_port 3037 dst
  aaa.bbb.ccd.253 TCP 3389
(844): 12:33:00 src slip139-92-139-249.stp.ru.ibm.net s_port 3038 dst
 aaa.bbb.ccd.254 TCP 3389
```

Source of Trace:

The source of the trace is http://www.sans.org/y2k/010901-1300.htm.

Detect was generated by:

This detect seems to be from an IDS like Snort. The format is as follows:

> (***AlertIDNumber***): ***Time*** src ***ResolvedSourceIP*** s_port ***SourcePort*** dst ***DestinationSourceIP DestinationPortNumber***

Probability that the source address was spoofed:

Likely. This targeted scan for port 3389 seems to have been conducted for reconnaissance purposes; however, the host name itself, slip139-92-139-249.stp.ru.ibm.net advertises its function, ip address, and organization name. If the source address is not spoofed, the attacker is making himself extremely visible (he may be a novice attacker). However, there is a possibility that the source is spoofed. The

host, slip139-92-139-249.stp.ru.ibm.net, may have been compromised by the attacker via a trojan, to execute the scans and to bounce the responses of the scan back to the attacker himself. This seems like a viable possibility since the source host seems to be a SLIP server that users may dial into to connect to the network by dial-up.

Description of the attack:

CVE Number: CVE-2000-1149
The attack is a scan for port 3389. Microsoft's Transaction server uses this port. There is a known buffer overflow vulnerability in Microsoft's Transaction server (http://www.microsoft.com/TechNet/security/bulletin/MS00-087.asp). If an attacker finds a host running Microsoft Terminal Server without the patch, the attacker can execute any code on the Terminal Server. For example, he would be able to add, change, or delete data, run code already on the server, or upload and run new code on it as well.

Attack Mechanism:

If an attacker finds a host running Microsoft Terminal Server without the patch, the attacker can execute any code on the Terminal Server. For example, he would be able to add, change, or delete data, run code already on the server, or upload and run new code on it as well.
The vulnerability lies in an unchecked buffer where Windows NT 4.0 Terminal Server handles the user name when the user logs onto the server. The unchecked buffer is vulnerable to a buffer overrun attack to run arbitrary code on the machine.

Correlations:

Reading through the SANS Windows Security Digest at http://www.sans.org/newlook/digests/ntarchives/113000.htm, it reports that the organization Core-SDI has discovered this vulnerability, and provides links for a fix and other links for additional information.

Also, port 3389 is on the list of "Top Ports" for 1/3/01, which implies that one should watch for traffic to 3389 carefully.

Evidence of active targeting:

There is no active targeting in this scan. However it is obvious, that the attacker is targeting a specific port. The attacker is using an automated scanning tool (the source port numbers increase sequentially and the times are very close together) to step through a set of IP addresses consecutively. The destination IP addresses increase by one. There is no attempt to throw off IDS's by scanning IP addresses in a random-like order.

Severity:

Criticality=4

I chose this value, because the target of the scan was a Windows Terminal Server. Although it is just a mere scan, if the attacker was lucky and did find a host running a Terminal Server, the exploit could be quite dangerous.

Lethality=5

If a Terminal Server is found, the attacker could introduce code that could take any action on the server with Administrator privileges.

System=5

This vulnerability is present only on hosts that run Windows NT 4.0 Terminal Server. There is a patch available, and I am assuming that all NT Terminal Server's have the patch. It is not certain whether there was a NT Terminal Server at all in the target network.

Net=4

I am assuming that the target network has a restrictive firewall with some external connections. A firewall can block this attack from being exploited over the Internet.

Severity = (4+5) – (5+4) = 0

Defensive recommendation:

The administrator of the target network should first see if they have any Windows NT Terminal Servers running. If so, the administrator should first filter TCP port 3389 and only allow traffic on that port from legitimate IP addresses that need to set up Terminal Server sessions. While that is in place, the administrator should download the patch available for the Windows NT Terminal Server.

Multiple Choice Question:

In the scan above, what detail could lead you to believe that the source IP was spoofed?

a) the destination port
b) the pattern of the source ports
c) the resolved hostname of the source ip
d) the rate at which the scan was done

Answer: C

Attack 2

Network Detect:

```
Jan 09 12:55:52 [firewall.ip.address] %PIX-2-106001: Inbound TCP
connection
  denied from cidr.net.addr.97/35394 to cidr.net.addr.98/23
  flags SYN  on interface outside
Jan 09 12:55:54 [firewall.ip.address] %PIX-2-106001: Inbound TCP
connection
  denied from cidr.net.addr.97/35394 to cidr.net.addr.98/23
  flags SYN  on interface outside
Jan 09 12:55:58 [firewall.ip.address] %PIX-2-106001: Inbound TCP
connection
  denied from cidr.net.addr.97/35394 to cidr.net.addr.98/23
  flags SYN  on interface outside
Jan 09 12:56:06 [firewall.ip.address] %PIX-2-106001: Inbound TCP
connection
  denied from cidr.net.addr.97/35394 to cidr.net.addr.98/23
  flags SYN  on interface outside
```

Source of Trace:

The source of the trace is from: http://sans.org/y2k/011901.htm

Detect was generated by:

This detect was from a PIX firewall. The format is as follows:

Month Day Time [***Firewall IP Address***] %PIX-2-106001: ***Incident*** from ***SourceIP***/***SourcePort*** to ***DestinationIP***/***DestinationPort*** flags ***TCPflags*** on interface ***LocationofIncident(Inside/Outside)***

Probability the source address was spoofed:

The source was spoofed.

Description of the attack:

CVE Number:
If the target host was a Windows NT machine then CVE-2000-0328 would apply.

The attacker spoofed the source IP in hopes to establish a telnet session with a host inside the firewall by pretending to be a host in the same subnet. The attacker probably used a spoofing tool or another hacking tool with a spoofing function to spoof the source IP.

Attack Mechanism:

I can only speculate what the attacker was attempting. The attacker may have been a disgruntled employee of the organization and had an ftp account or knew of another ftp account. If the attacker was successful in getting past the firewall (which he was not), the attacker could have ran a DOS on the host with the IP of cidr.net.addr.97 busy with a SYN flood. While cidr.net.addr.97 is kept busy, the attacker could have used the spoofed telnet attempts (with the DOS victim's IP address) shown above to establish a telnet session with cidr.net.addr.98. The attacker would also have to correctly guess the corresponding sequence numbers for the attack to work. The attacker would be doing this attack blindly, because he would not be receiving the responses to the spoofed SYN requests he is sending.

Also, another possibility is that the attacker was assuming that there was a telnet session existing between cidr.net.addr.97 and cidr.net.addr.98. It could be possible that the attacker may have been a disgruntled employee that left a telnet session running between the two hosts to hijack the session later. Then the attacker could have used hi-jack tools like Hunt, Juggernaut, T-sight, and IP-watcher to hi jack the telnet session.

A good resource for session hi-jacking I found was "What's Luring in the Ether" at http://www.sans.org/infosecFAQ/firewall/ethernet.htm.

Correlations:

Jose Nazario, in the GIAC report of November 9,2000, reported that he experienced attempted Hunt-style hijacks. http://www.sans.org/y2k/110900-1300.htm

Evidence of active targeting:

Yes. There was only one host that was targeted and only the attacker tried to only connect to the ftp port on that host.

Severity:

Criticality=3

I chose this value, because the attacker was looking for a target that he/she could telnet to. This could be any Unix/Linux/Solaris machine or a Windows machine running a telnet server.

Lethality=5

If the attacker was successful in executing a telnet hijack, the attacker could introduce backdoors into the targeted host and infect other hosts on the network as well.

System=4

This attack is a bit difficult to run successfully on modern machines when you try to guess the sequence numbers. However, if the attacker was using a hi-jack tool like Hunt, odds do improve, because it uses a combination of more sophisticated means like ARP spoofing to hi-jack the session.

Net=4

I am assuming that the target network has a restrictive firewall with some external connections. A firewall that blocks inbound FTP requests (such as the one in this trace) can block this attack from being exploited over the Internet.

Severity = (3+5) – (5+4) = -1

Defensive recommendation:

Defenses are fine, the attack was successfully blocked by the firewall. I would monitor the telnet ports to see if subsequent attacks with spoofed source IPs occur.

Multiple Choice Question:

According to the trace above, which of the following are true?

a) ingress filtering was used on port 23
b) the packets were crafted by a tool
c) someone in the target organization was trying to start a telnet session with a host that does not run telnet
d) all of the above

Answer: a and b

Attack 3

Network Detect:

```
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.44.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.45.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.46.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.47.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.48.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.49.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.51.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.52.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.53.9704  F
15 Feb 01 18:18:52      tcp    211.46.7.194.9704   ?>
130.216.2.55.9704  F

Source: 211.46.7.194
Ports: tcp-9704
Incident type: Network_scan
re-distribute: yes
timezone: UTC + 1300
reply: no
Time: Thu 15 Feb 2001 at 05:18 (UTC)
```

Source of the Trace:

The source of the trace is: http://www.sans.org/y2k/021701.htm

Detect was generated by:

This detect was probably generated by an IDS or a packet filter. The format is as follows:

Day Month Year Time Protocol SourceIP.SourcePort ?> ***DestinationIP.DestinationPort TCPFlag(s)***

Probability the source address was spoofed:

Somewhat likely. I looked up the source IP address, 211.46.7.194, on whois, and it was not able to resolve a domain name for it. The attacker may have placed a network sniffer

on the network that the host 211.46.7.194 is on, and could be sniffing the scan responses. That way, the attacker does not make himself visible as the originator of the scan.

Quite simply, it could also be a person just carelessly conducting a scan for port 9704, to see if any Linux hosts on the net that may have been already compromised by the RPC stat exploit to possibly reap the benefits of another hacker's labor.

Description of the attack:

CVE Number: CAN-2000-0666

This attack uses a vulnerability in rpc.statd in hosts running Linux. The CVE description for this vulernability states that "in rpc.statd in the nfs-utils package in various Linux distributions does not properly cleanse untrusted format strings, which allows remote attackers to gain root privileges."

Attack Mechanism:

The attacker targets hosts that are running Linux, and then executes a script that runs the exploit on these hosts sending commands to append a line (with root privilege) to inetd.conf for starting a shell on port 9704 and restarting inetd. The attacker can then, at another time, enter through the shell to continue his attack or he can start covering up his tracks.

Also, it should be noted that FINs were used rather than SYNs. This may have been done to improve the probability of getting a response back from the scanned hosts.

In my research, the best explanation is given by Joakim Bergkvist at http://www.sans.org/y2k/082200.htm.

Correlations:

Joakim Bergkvist has been a victim of this exploit and has described how the attack occurs at http://www.sans.org/y2k/082200.htm.

Laurie@edu has also submitted a similar scan for port 9704 at http://www.sans.org/y2k/102700.htm.

This attack has also been seen in other forums as well:
http://lists.insecure.org/incidents/2000/Sep/0054.html
www.securityfocus.com (searchword = port 9704)

Evidence of active targeting:

No. There was no active targeting. The attacker was trying to see if any hosts had been compromised by the rpc statd exploit. Port 9704 was consistently targeted in every packet.

Severity:

Criticality=3

I chose this value, because the attacker was looking for any Linux host. It could be various distributions of Linux. It is not certain if the attacker was targeting a Linux server or just a Linux workstation.

Lethality=5

If the attacker was successful in finding a host that had been compromised already by the exploit, the attacker could then enter through the created shell and continue his damage on the compromised host and begin to infect other hosts as well.

System=4

It is quite possible to have a vulnerable Linux system. Joakim Bergkvist specifically mentions Linux Redhat 6.x machines, and the CVE description mentions "various" Linux distributions.

Net=4

I am assuming that the target network has a restrictive firewall with some external connections. You can block port 9704 to prevent anyone from connecting to this port from the Internet.

Severity = (3+5) – (4+4) = 0

Defensive Recommendation:

I recommend getting the fix for the vulnerability for the specific version of Linux that is used. Also, as a safety precaution, I also recommend blocking port 9704.

Multiple Choice Question:

According to the scan above, which of the following are true:

a) a script or tool was used to generate the packets
b) the source host is disconnecting its connections with the target hosts
c) the attacker is scanning for a compromised host that has a port listening on port 9704
d) all of the above

Answer: a and c

Attack 4

Trace:

```
Nov 23 09:49:59 199.239.94.98:1116 -> 192.169.1.11:515 SYN **S*****
Nov 23 09:49:59 199.239.94.98:1117 -> 192.169.1.12:515 SYN **S*****
Nov 23 09:49:59 199.239.94.98:1118 -> 192.169.1.13:515 SYN **S*****
Nov 23 09:49:59 199.239.94.98:1250 -> 192.169.1.145:515 SYN **S*****
Nov 23 09:49:59 199.239.94.98:1253 -> 192.169.1.148:515 SYN **S*****
Nov 23 09:49:59 199.239.94.98:1254 -> 192.169.1.149:515 SYN **S*****
Nov 23 09:49:59 199.239.94.98:1119 -> 192.169.1.14:515 SYN **S*****

....

Nov 23 09:51:13 199.239.94.98:2436 -> 192.169.99.88:515 SYN **S*****
Nov 23 09:51:13 199.239.94.98:2437 -> 192.169.99.89:515 SYN **S*****
Nov 23 09:51:13 199.239.94.98:2438 -> 192.169.99.90:515 SYN **S*****
Nov 23 09:51:13 199.239.94.98:2439 -> 192.169.99.91:515 SYN **S*****
Nov 23 09:51:13 199.239.94.98:2440 -> 192.169.99.92:515 SYN **S*****
Nov 23 09:51:13 199.239.94.98:2442 -> 192.169.99.94:515 SYN **S*****
Nov 23 09:51:13 199.239.94.98:2447 -> 192.169.99.99:515 SYN **S*****
```

Source of Trace:

The source of this trace is from Assignment 2 of this practical assignment. Specifically it is from a concatenated file of all the scan files that are in snorts.zip. To concatenate all the scan files I ran the following command:

Grep –h '^[SON][eco][ptv]' SnortSca.txt SnortS[0-9]*.txt >allscans.txt

Then I changed the "MY.NET" in the file to "192.169" by issuing the following command:

Sed –e 's/MY.NET/192.169/g' allscans.txt >allscans2.txt

To obtain the trace above I execute the following command:

Grep ':515 ' allscans2.txt | grep '199.239.94.98' | sort –u +5 > scan199-239-94-98

Detect was generated by:

The Snort Intrusion Detection System. The format is as follows:

Month Day Time SourceIP : ***SourcePort*** -> ***DestinationIP*** : ***DestinationPort TCPFlags***

Probability that the source was spoofed:

Somewhat likely. I performed a whois on the source IP address, and it was unable to resolve a domain name for it. Another reason why I think this source IP may be spoofed is because this was a pretty large scan. There were a total of 4,719 hosts scanned in little over a minute. Any IDS would pick this scan up, and the attacker used ordinary SYNs to perform the scan. This makes the attacker highly visible if the source was not spoofed.

Then again, it could just be someone just trying out a scanning tool he/she just downloaded for the first time.

Description of the attack:

CVE Number: CVE-2000-0917

The attack is a scan for port 515, which is where the UNIX LPR and LPRng services run. SANS has reported that are advisories released concerning LPR service vulnerabilities, for many varities of Linux and for the other UNIX BSD varieties. That report is found at: http://www.sans.org/newlook/alerts/port515.htm.

Attack Mechanism:

LPRng, which is a common replacement to the BSD lpd printing service, contains a missing format-string argument in at least two calls to the syslog function. These missing strings in function calls allow an attacker to supply damaging code to a susceptible snprintf() function call. The attacker can further overwrite memory of the printer service's address space and run arbitrary code.

A good discussion of this attack can be found at:

http://s1.red.cert.org/advisories/CA-2000-22.html

Correlations:

In November, scans were on the rise for port 515, and SANS issued an Alerts and Analysis article: http://www.sans.org/newlook/alerts/port515.htm

On the SANS website, there is an excellent full-featured document on a successful compromise of a Redhat 7 machine using the LPRng exploit giving the attacker root access. The article is named "The Compromise" and can be found at: http://www.sans.org/y2k/the_compromise.htm

Laurie@edu had a scan also on port 515, and is shown at: http://www.sans.org/y2k/111000-1200.htm

Evidence of active targeting:

No. Over 4,719 hosts were scanned in a little over a minute. It appears the attacker was doing broad reconnaissance to see if any hosts had port 515 listening.

Severity:

Criticality=3

I chose this value, because the attacker was looking for any Linux/BSD host running the LPRng service. It could be various distributions of Linux or BSD. If the LPRng service was running on a machine that also had other servers (i.e. DNS, FTP, etc) the criticality would be more severe.

Lethality=5

If the attacker was successful in finding a host that had the LPRng service with the vulnerability (versions before LPRng 3.6.25), he/she would be able to gain root access and the fun begins for the attacker. As documented in "The Compromise", the attacker could then connect to another machine to download various things like backdoor programs, a sniffer, a rootkit, etc.

System=4

It is quite possible to have a vulnerable Linux system. The CERT Advisory mentioned previously mentions that the LPRng is a "popular replacement software package to the BSD lpd printing service".

Net=4

I am assuming that the target network has a restrictive firewall with some external connections. You can block port 515 to prevent anyone from connecting to this port from the Internet.

Severity = (3+5) – (4+4) = 0

Defensive Recommendations:

You should obtain a patch from your specific vendor. A list of vendors and their patch sites are given on the CERT advisory page at:

http://s1.red.cert.org/advisories/CA-2000-22.html.

Also, as a precaution monitor any traffic to port 515 with an IDS, and block inbound connection attempts to port 515 at the firewall.

Multiple choice question:

From the trace shown above, what can be concluded?

a) there is evidence of active targeting
b) the attacker is using a stealth scan
c) the attacker is looking for hosts with the LPRng vulnerability
d) the attacker is using a scanning tool

Answer: c and d

Assignment 2

Overview defining the data

My organization was given about a month's worth of data from GIAC Enterprise's SNORT logs. We were given three types of SNORT logs: alert logs, scan logs, and OOS logs. All the files were saved as text files (*.txt).

The following chart describes the data we used to perform the analysis.

SNORT File Type	Number of Files	Dates Covered
Alert Files	54	9/26-11/22
Scan Files	42	9/27-11/23
OOS Files	19	8/17, 10/1-11/23

*NOTE: The data is not continuous. As explained in the instructions for Assignment 2, from time to time the power failed or the disk was full so we do not have data for all days.

List of Detects Prioritized By Number of Occurrences

The following table lists the attacks and the number of occurrences.

Attack	Frequency (# of occurrences)
SYN-FIN scan	56250
Watchlist 000220 IL-ISDNNET-990517	30998
Spp_portscan: (only portscan status counted)	27572
Watchlist 000222 NET-NCFC	8166
WinGate 1080 Attempt	4802
TCP SMTP Source Port Traffic	2893
Attempted SUN RPC highport access	2542
Broadcast Ping to subnet 70	1813
Back Orifice	1697
SNMP public access	468
Null Scan	283
SMB Name Wildcard	218
Queso fingerprint	142
NMAP TCP Ping	96
SUNRPC highport access	60
Connect to 515 from inside	56
Probable NMAP fingerprint attempt	15
External RPC Call	13
SITE EXEC – Possible wu-ftpd exploit	7
Tiny Fragments-Possible Hostile Activity	7
site exec-Possible wu-ftpd exploit	6
Happy 99 Virus	2

Description of Attacks

SYN-FIN scan: This type of scanning uses an impossible flag combination to probe target hosts for listening ports. These packets are crafted by a scanning tool, because normal packets will never have both the SYN and FIN bits set simultaneously. This scan can be used to possibly avoid detection of IDS systems that only look for SYN only connections. Also Linux will give a distinct response to a SYN-FIN packet (a SYN-FIN-ACK) that will clue the attacker that the target is a Linux host.

Spp_portscan: A scan that is conducted to see what ports are open on a host or a variety of hosts.

Watchlist 000220 IL-ISDNNET-990517 & Watchlist 000222 NET-NCFC: The watchlist contains IP addresses that have a record of unusual activity. We had quite a number of alerts from both watchlists.

WinGate 1080 Attempt: Port 1080 is a common port for Wingate to operate on. Vulnerabilities with certain versions of WinGate have been found where it allows an attacker to access the Wingate server hard disk.

TCP SMTP Source Port Traffic: Both the source port and the destination port is 25 in this alert. The source port is usually one of the higher ephemeral ports. Since the source port is 25, the packet could possibly be crafted.

Attempted SUN RPC highport access: Remote Procedure Calls (RPC) allow a user (or an attacker) to execute programs on another computer. There have been multiple vulnerabilities reported that have been widely exploited. It is one of SANS Top ten Threats.

Broadcast Ping to subnet 70: A broadcast ping is usually performed to receive an ICMP Echo Response from every host on the subnet (particularly subnet 70). If enough of these broadcast pings are sent, a possible ICMP flood could choke the network bandwidth.

BackOrifice: A very common remote administration program used as a trojan horse for Windows hosts. Attacks usually scan for the port BackOrifice listens on, port 31337. If BackOrifice is running on a host, and an attacker finds it, the attacker can connect to it using the Back Orifice client and basically take over the host to do a countless number of evils.

SNMP public access: SNMP consists of two parts: the SNMP manager and the SNMP agent. The SNMP manager retrieves configuration and performance counter information from the agents by issuing "get" commands, and they can also change a network element's configuration by issuing "set" commands. SNMP's authentication is accomplished through the use of a community string. Unfortunately, this community string is often set by default to a predictable string. The most common string for reads is "Public", and the most common string for writes is "Private". Since these read and write community strings are so common, it is easy for an attacker to exploit SNMP. The attacker can do much reconnaissance or change settings in network elements as well. According to SANS Top Ten Threats, default SNMP is number 10.

Null Scan: This type of scan has none of the tcp flag bits set. Null scans can be used to map out a network.

SMB Name Wildcard: The SMB Wildcard is a Netbios name query and this is a sign that an attacker is trying to access a share with poor access control. When improperly configured, sharing via Netbios, can make sensitive information susceptible to an attacker connected to the network. It is written on the SANS top ten list that "When file sharing is enabled on Windows machines they become vulnerable to both information theft and certain types of quick-moving viruses". http://www.sans.org/topten.htm

Queso Fingerprint: Queso is a tool that determines the operating system of the target host. It does so by analyzing the responses to impossible packets that Queso sends.

Queso uses destination port 80 by default but it can use other port that is open on the target host. Once the operating system is determined, an attacker can then use the appropriate exploits on the target host.

NMAP TCP Ping: NMAP is a versatile and powerful tool to map out a network and to see what services are running on the hosts of the targeted network. The TCP Ping is one of its options to scan what hosts are up on a network as opposed to an ICMP ping.

SUNRPC highport access: As mentioned earlier in the description for "Attempted SUN RPC highport access", access to these ports should be closely monitored. This is an alert indicating a SUN RPC port has been accessed; namely 32771.

Connect to 515 from inside: Port 515 is where the UNIX LPR and LPRng services run. SANS has reported that are advisories released concerning LPR service vulnerabilities, for many varities of Linux and for the other UNIX BSD varieties. That report is found at: http://www.sans.org/newlook/alerts/port515.htm. An attacker can exploit the string-format vulnerability present in the LPRng service, and potentially gain root access or execute malicious code.

Probable NMAP fingerprint attempt: NMAP can also be used to determine with fair accuracy the operating system of the target host. Once the operating system is determined, an attacker can then use the appropriate exploits on the target host.

External RPC Call: An external host is attempting to use the RPC services of the target host.

SITE EXEC – Possible wu-ftpd exploit & site exec-Possible wu-ftpd exploit: There are several vulnerabilities in wu-ftpd. Wu-ftpd is a common package used for FTP services. For example, wu-ftpd, has a buffer overflow vulnerability due to improper bounds checking. For more information see http://www.cert.org/advisories/CA-1999-13.html.

Tiny Fragments-Possible Hostile Activity: Usually the TCP header is 20 bytes long; but there are tools that can craft fragmented packets to bypass firewalls or Intrusion Detection Systems. Tiny packets can also be used for reconnaissance purposes.

Happy 99 Virus: The Happy 99 virus is usually attached to an email. When they execute the .exe file, there is a fireworks display to distract the target while the virus infects the target host.

Top Talker's List:

Top 30 Alert Destination Ports

The following table displays how frequent connections to specific ports were attempted. These results are from the Alert data files.

Note: To save space only the TOP 30 ports are shown.

Destination Port	Frequency (# of connection attempts)
21	19639
53	18341
9704	14184
25	11053
6699	9764
4619	5734
4922	4813
1080	4812
27374	3577
6688	3295
32771	2602
31337	1697
4990	1459
1069	648
1255	625
1476	579
6346	474
161	468
4968	420
6700	368
23	349
4410	290
109	267
4752	260
4722	257
4545	243
137	218
4191	217
4519	174
4780	163

Top 30 Scanned Destination Ports

The following table displays how frequent specific ports were scanned. These results are from the Scan data files.

Note: To save space only the TOP 30 ports are shown.

Destination Port	Frequency (# of times scanned)
21	118786
27374	36214
515	25799
53	19521
9704	14168
98	9469
9088	8763
110	8687
139	5648
113	4244
23	3048
67	2297
19000	2081
1080	1897
31337	1219
5232	944
443	358
1057	333
6699	321
2781	317
1041	317
1162	316
1103	284
3083	261
2183	247
2184	239
2981	238
3111	229
1108	208
2187	207

Top 30 Alerting Source Networks

The following table shows which source networks caused the most network alerts. These results are from the Alert data files. **All 192.169.X.X networks is MY.NET**

Note: To save space only the TOP 30 networks are displayed

Network Address	Frequency (# of attacks to MY.NET)
24.X.X.X	144
63.X.X.X	71
159.226.X.X	45
62.X.X.X	39
64.X.X.X	29
193.231.220.X	19
205.188.153.X	17
192.169.97.X	16
193.230.165.X	14
192.169.98.X	14
194.102.93.X	12
216.67.50.X	11
193.231.210.X	10
192.169.101.X	9
216.152.64.X	8
194.206.208.X	8
4.X.X.X	8
212.179.45.X	7
203.155.129.X	7
217.10.201.X	6
216.67.82.X	6
193.230.162.X	6
12.X.X.X	6
151.21.X.X	5
148.233.X.X	5
38.X.X.X	5
213.154.134.X	4
213.154.130.X	4
212.179.95.X	4
212.179.44.X	4

Top 30 Alerting Destination IPs

The following table shows which destination IP addresses that had the most attempted connections. These results are from the Alert data files. **All 192.169.X.X IPs are MY.NET.**

Note: To save space only the TOP 30 destination IPs are displayed

Destination IPs	Frequency (# of Attempted Connections)
192.169.6.7	5808
192.169.211.146	4814
192.169.223.98	3940
192.169.206.90	3918
192.169.203.142	1640
192.169.218.142	1463
192.169.214.170	1371
192.169.100.230	1302
192.169.202.22	952
192.169.201.174	803
192.169.214.74	669
192.169.209.106	655
192.169.221.146	639
192.169.223.254	627
192.169.211.178	610
192.169.253.43	589
192.169.15.215	582
192.169.227.190	565
192.169.101.192	561
192.169.203.206	508
192.169.98.181	501
192.169.221.246	490
192.169.225.58	477
192.169.225.210	437
192.169.220.190	435
192.169.203.118	434
192.169.207.14	413
192.169.206.118	374
192.169.207.158	368
192.169.217.214	366

List of Source Addresses and Registration Information

The following table is a list of source IP's to its registered host name. **All 192.169.X.X IPs are MY.NET addresses.**

Note: When the IP address appears in the Host name field, whois was not able to resolve the IP address.

THIS LIST IS ABOUT 30 PAGES.

Source IP	Host Name
12.128.180.45	12.128.180.45
12.30.169.12	12.30.169.12
12.30.169.253	12.30.169.253
12.31.176.55	12.31.176.55
12.34.21.196	12.34.21.196
12.43.88.5	12.43.88.5
127.0.0.1	lds
128.113.145.105	shellder-06.dynamic.rpi.edu
128.119.10.51	wash-51.res.umass.edu
128.148.221.203	bootp-203.chapin.brown.edu
128.175.109.52	host109-52.student.udel.edu
128.175.153.19	host153-19.student.udel.edu
128.175.68.159	host68-159.student.udel.edu
128.193.136.218	128.193.136.218
128.193.137.38	trenkelv.RCN.ORST.EDU
128.193.232.142	shoe.RCN.ORST.EDU
128.194.79.228	suprma19.resnet.tamu.edu
128.195.229.11	vp229011.reshsg.uci.edu
128.2.160.98	DASHOCKADELL.RES.CMU.EDU
128.2.81.133	8TH-DWARF.REM.CMU.EDU
128.227.205.209	torrent.cise.ufl.edu
128.253.247.116	tls16.resnet.cornell.edu
128.253.97.158	kcw13.resnet.cornell.edu
128.46.156.117	csociety-ftp.ecn.purdue.edu
128.54.203.218	t8kim.resnet.ucsd.edu
128.59.42.191	dialup-cc3-86.cc.columbia.edu
128.59.42.88	dialup-1-79.cc.columbia.edu
128.61.56.190	r56h190.res.gatech.edu
129.101.18.16	LUKESCOMPUTER
129.123.6.14	avarice.cass.usu.edu
129.130.193.16	STUDY5
129.130.98.92	rn-098-092.reshall.k-state.net
129.137.222.188	cahr285.cah.uc.edu
129.186.67.59	pc116a-09.cs.iastate.edu
129.2.204.249	129-2-204-249.student.umd.edu

Source IP	Host Name
129.2.243.83	ruffryder.student.umd.edu
129.2.246.25	NotRegistered-129-2-246-25.student.umd.edu
129.241.139.224	s224b.studby.ntnu.no
129.242.219.27	nonet.td.org.UiT.No
129.37.159.177	slip129-37-159-177.on.ca.prserv.net
129.49.231.73	129.49.231.73
129.7.141.62	Dorm-36158.RH.UH.EDU
129.93.198.95	pcp020104pcs.unl.edu
129.93.206.170	pcp008790pcs.unl.edu
129.93.211.40	pcp009539pcs.unl.edu
130.126.211.213	isr5981.urh.uiuc.edu
130.127.196.96	WEB3
130.161.78.55	sh39k15.jvb.tudelft.nl
130.227.195.57	KELD
130.231.5.100	yok5100.oulu.fi
130.239.140.108	stipgr294.sn.umu.se
130.39.216.104	spt-4.madstudio.lsu.edu
130.39.251.3	steele.rurallife.lsu.edu
130.49.86.89	dhcp86-89.pittsburgh.resnet.pitt.edu
130.75.178.186	pc10.duese.uni-hannover.de
130.83.253.17	gw.av.wh.tu-darmstadt.de
130.86.31.21	station-21.brhlab.csus.edu
130.89.229.162	cal040012.student.utwente.nl
130.89.229.48	cal032044.student.utwente.nl
130.91.215.192	GRT-215-192.RESNET.UPENN.EDU
131.104.254.193	RN254-193.resnet.uoguelph.ca
131.173.67.58	131.173.67.58
131.204.195.71	fotifor.resnet.auburn.edu
131.238.3.47	balintrc.oca.udayton.edu
132.178.218.181	132.178.218.181
132.199.220.223	rx4016.cip.uni-regensburg.de
132.199.222.167	rx2077.cip.uni-regensburg.de
132.66.90.64	ppp-90-064.tau.ac.il
133.46.212.81	133.46.212.81
134.28.73.132	a301b.whm.tu-harburg.de
134.58.0.50	nat-50.kulnet.kuleuven.ac.be
134.76.63.97	stoffel.cweg.stud.uni-goettingen.de
134.88.222.41	hw00a0d21418a1.res.umassd.edu
137.120.224.68	campusa0068nuts.unimaas.nl
137.99.152.146	d152h146.resnet.uconn.edu
138.4.182.14	138.4.182.14
138.88.47.2	adsl-138-88-47-2.bellatlantic.net
139.130.61.206	alphac.lnk.telstra.net
139.142.171.16	sun-171-16.sunwave.net
139.6.22.107	05-08.stw1.FH-Koeln.DE

Source IP	Host Name
140.186.112.26	funky.ultrashell.net
141.109.81.131	CHERRY
141.157.98.201	adsl-141-157-98-201.bellatlantic.net
141.157.99.21	adsl-141-157-99-21.bellatlantic.net
141.35.38.164	ibz-ce01a.verwaltung.uni-jena.de
142.165.32.27	hss-32-27.sk.sympatico.ca
142.17.160.168	Studio-229.Etudiants.CUSLM.CA
142.176.103.125	142.176.103.125
143.89.13.3	ustlnx6.ust.hk
144.132.229.13	CPE-144-132-229-13.nsw.bigpond.net.au
144.92.245.21	mirror.sit.wisc.edu
147.163.20.147	student7.diepa.unipa.it
147.229.100.147	p3-328A.purk.kn.vutbr.cz
147.46.208.71	147.46.208.71
148.217.14.205	148.217.14.205
148.223.54.176	du-148-223-54-176.prodigy.net.mx
148.233.161.244	du-148-233-161-244.prodigy.net.mx
148.233.234.142	du-148-233-234-142.prodigy.net.mx
148.233.245.203	du-148-233-245-203.prodigy.net.mx
148.233.52.133	du-148-233-52-133.prodigy.net.mx
148.233.60.245	du-148-233-60-245.prodigy.net.mx
148.240.16.23	dial-148-240-16-23.zone-1.dial.net.mx
149.205.110.45	HVD
149.99.98.146	149.99.98.146
151.21.170.71	ppp-71-170.21-151.libero.it
151.21.56.81	ppp-81-56.21-151.libero.it
151.21.78.248	ppp-248-78.21-151.libero.it
151.21.79.104	ppp-104-79.21-151.libero.it
151.21.87.245	ppp-245-87.21-151.libero.it
151.26.19.249	ppp-249-19.26-151.libero.it
151.29.211.18	ppp-18-211.29-151.libero.it
152.2.174.136	dhcp2168.dhcp.unc.edu
152.66.24.68	152.66.24.68
152.9.54.26	152.9.54.26
155.207.25.68	transp.topo.auth.gr
157.182.149.108	bxt3223-108.hrlnet.wvu.edu
157.182.33.208	brs0331-208.hrlnet.wvu.edu
159.226.111.1	MAIL
159.226.113.1	159.226.113.1
159.226.114.1	159.226.114.1
159.226.115.1	159.226.115.1
159.226.118.9	moon.ibp.ac.cn
159.226.120.14	159.226.120.14
159.226.120.19	159.226.120.19
159.226.128.1	server.shcnc.ac.cn

Source IP	Host Name
159.226.144.130	NS
159.226.157.1	159.226.157.1
159.226.158.188	159.226.158.188
159.226.159.1	159.226.159.1
159.226.159.146	159.226.159.146
159.226.172.136	159.226.172.136
159.226.2.20	fruits.cnc.ac.cn
159.226.209.2	apple.cast.ac.cn
159.226.21.3	159.226.21.3
159.226.218.3	159.226.218.3
159.226.22.55	AILAB-SERVER
159.226.22.59	159.226.22.59
159.226.224.1	159.226.224.1
159.226.228.1	RED
159.226.23.3	TEDDY
159.226.247.60	159.226.247.60
159.226.39.1	159.226.39.1
159.226.41.166	159.226.41.166
159.226.41.188	159.226.41.188
159.226.42.9	159.226.42.9
159.226.45.204	dos204.iphy.ac.cn
159.226.45.3	aphy.iphy.ac.cn
159.226.45.60	ssc.iphy.ac.cn
159.226.49.157	159.226.49.157
159.226.5.207	159.226.5.207
159.226.5.222	159.226.5.222
159.226.5.65	159.226.5.65
159.226.5.77	159.226.5.77
159.226.5.83	159.226.5.83
159.226.6.5	search.cnnic.net.cn
159.226.61.62	159.226.61.62
159.226.63.190	lcc.icm.ac.cn
159.226.63.200	159.226.63.200
159.226.64.152	159.226.64.152
159.226.66.130	mail.im.ac.cn
159.226.91.20	159.226.91.20
159.226.92.10	netlib.amss.ac.cn
160.39.225.142	dyn-shp-225-142.dyn.columbia.edu
160.78.49.191	ema.chim.unipr.it
161.142.150.51	161.142.150.51
161.142.194.63	j49.ptl47.jaring.my
161.184.140.162	edtn007274.hs.telusplanet.net
161.53.3.211	161.53.3.211
161.53.3.212	161.53.3.212
161.53.3.232	161.53.3.232

Source IP	Host Name
161.53.3.236	161.53.3.236
161.58.8.77	161.58.8.77
163.10.19.34	decanato.exactas.unlp.edu.ar
163.121.213.100	163.121.213.100
164.8.21.101	164.8.21.101
165.138.35.1	CLEMENS
165.166.177.10	chatserv.infoave.net
165.230.229.40	leenap.resnet.rutgers.edu
167.206.202.18	hicks202-18.optonline.net
168.120.12.33	digit33.aunet.au.ac.th
168.120.16.155	168.120.16.155
168.120.16.250	chat.au.ac.th
168.143.29.9	dparks.clark.net
168.187.27.27	ppp-27-027.kems.net
168.187.31.42	WIN98
168.191.230.220	sdn-ar-002waseatP180.dialsprint.net
168.191.230.42	sdn-ar-001waseatP058.dialsprint.net
168.191.250.64	sdn-ar-001tnnashP104.dialsprint.net
168.191.91.142	sdn-ar-003florlaP252.dialsprint.net
169.132.154.25	ppp-25.ts-6.lax.idt.net
169.232.73.204	s73-204.resnet.ucla.edu
169.233.14.204	cs-d0716.resnet.ucsc.edu
169.254.184.161	169.254.184.161
172.130.97.123	AC82617B.ipt.aol.com
172.134.3.235	AC8603EB.ipt.aol.com
172.141.91.45	AC8D5B2D.ipt.aol.com
172.142.146.152	AC8E9298.ipt.aol.com
172.143.182.224	AC8FB6E0.ipt.aol.com
172.147.75.18	AC934B12.ipt.aol.com
172.152.112.209	AC9870D1.ipt.aol.com
172.154.142.141	AC9A8E8D.ipt.aol.com
172.154.54.107	AC9A366B.ipt.aol.com
172.157.126.93	AC9D7E5D.ipt.aol.com
172.160.164.114	ACA0A472.ipt.aol.com
172.161.70.246	ACA146F6.ipt.aol.com
172.167.118.229	ACA776E5.ipt.aol.com
172.177.231.97	ACB1E761.ipt.aol.com
192.102.197.234	geo197a.cps.intel.com
192.107.104.122	192.107.104.122
192.116.207.178	192.116.207.178
192.148.174.7	mailman.globalkey.com
192.169.101.113	192.169.101.113
192.169.101.142	192.169.101.142
192.169.101.145	192.169.101.145
192.169.101.147	192.169.101.147

Source IP	Host Name
192.169.101.152	192.169.101.152
192.169.101.153	192.169.101.153
192.169.101.160	192.169.101.160
192.169.101.53	192.169.101.53
192.169.101.89	192.169.101.89
192.169.153.135	192.169.153.135
192.169.179.78	192.169.179.78
192.169.222.42	192.169.222.42
192.169.97.108	192.169.97.108
192.169.97.115	192.169.97.115
192.169.97.120	192.169.97.120
192.169.97.130	192.169.97.130
192.169.97.159	192.169.97.159
192.169.97.171	192.169.97.171
192.169.97.178	192.169.97.178
192.169.97.185	192.169.97.185
192.169.97.189	192.169.97.189
192.169.97.192	192.169.97.192
192.169.97.204	192.169.97.204
192.169.97.205	192.169.97.205
192.169.97.207	192.169.97.207
192.169.97.208	192.169.97.208
192.169.97.215	192.169.97.215
192.169.97.219	192.169.97.219
192.169.98.106	192.169.98.106
192.169.98.109	192.169.98.109
192.169.98.111	192.169.98.111
192.169.98.116	192.169.98.116
192.169.98.122	192.169.98.122
192.169.98.123	192.169.98.123
192.169.98.132	192.169.98.132
192.169.98.141	192.169.98.141
192.169.98.154	192.169.98.154
192.169.98.160	192.169.98.160
192.169.98.165	192.169.98.165
192.169.98.174	192.169.98.174
192.169.98.191	192.169.98.191
192.169.98.197	192.169.98.197
192.206.151.152	tweety.tgrace.com
192.216.128.28	protege.linkline.com
193.11.234.79	anan.rotary.studenthem.gu.se
193.136.132.85	andorinha.ist.utl.pt
193.145.235.81	srv1a.pal.ua.es
193.159.101.206	pC19F65CE.dip.t-dialin.net
193.166.0.134	ircg.funet.fi

Source IP	Host Name
193.180.253.2	users.sala.se
193.226.127.19	193.226.127.19
193.226.127.20	193.226.127.20
193.226.127.21	ppp5.icemenerg.vsat.ro
193.226.148.161	port1.Bucharest2.RO.EU.net
193.226.148.167	port7.Bucharest2.RO.EU.net
193.226.161.116	e-Volution-2.iNES.RO
193.226.161.141	DynIP-161-141.Dialup.iNES.RO
193.226.161.156	DynIP-161-156.Dialup.iNES.RO
193.226.161.157	DynIP-161-157.Dialup.iNES.RO
193.226.181.57	193.226.181.57
193.226.46.209	193.226.46.209
193.226.60.179	193.226.60.179
193.226.61.199	ppp06.euroweb.ro
193.226.61.211	ppp18.euroweb.ro
193.226.61.229	ppp36.euroweb.ro
193.230.105.120	193.230.105.120
193.230.129.169	Lubrifin.deltanet.ro
193.230.162.112	193.230.162.112
193.230.162.145	193.230.162.145
193.230.162.155	193.230.162.155
193.230.162.243	193.230.162.243
193.230.162.79	193.230.162.79
193.230.162.89	193.230.162.89
193.230.165.16	193.230.165.16
193.230.165.17	193.230.165.17
193.230.165.19	193.230.165.19
193.230.165.20	193.230.165.20
193.230.165.27	193.230.165.27
193.230.165.37	193.230.165.37
193.230.165.39	193.230.165.39
193.230.165.41	193.230.165.41
193.230.165.42	193.230.165.42
193.230.165.48	193.230.165.48
193.230.165.49	193.230.165.49
193.230.165.53	193.230.165.53
193.230.165.58	193.230.165.58
193.230.165.60	OEMCOMPUTER
193.230.177.149	193.230.177.149
193.230.230.85	ceva.mediafax.ro
193.230.247.95	Moca.CODEC.Ro
193.230.250.251	tel271468.is.necomm.ro
193.231.125.141	ppp-141.dnt.ro
193.231.125.159	ppp-159.dnt.ro
193.231.169.166	193.231.169.166

Source IP	Host Name
193.231.184.221	193.231.184.221
193.231.196.27	lyon.intelsev.ro
193.231.207.26	ppp153.dnttm.ro
193.231.207.72	ppp67.dnttm.ro
193.231.209.130	ppp130.fx.ro
193.231.210.35	ppp25-ph.fx.ro
193.231.210.37	ppp27-ph.fx.ro
193.231.210.38	ppp28-ph.fx.ro
193.231.210.40	ppp30-ph.fx.ro
193.231.210.41	ppp31-ph.fx.ro
193.231.210.42	ppp32-ph.fx.ro
193.231.210.43	ppp33-ph.fx.ro
193.231.210.44	ppp34-ph.fx.ro
193.231.210.45	ppp35-ph.fx.ro
193.231.210.46	ppp36-ph.fx.ro
193.231.220.101	ppp220101.fx.ro
193.231.220.103	ppp220103.fx.ro
193.231.220.106	ppp220106.fx.ro
193.231.220.125	ppp220125.fx.ro
193.231.220.126	ppp220126.fx.ro
193.231.220.128	ppp220128.fx.ro
193.231.220.132	ppp220132.fx.ro
193.231.220.136	ppp220136.fx.ro
193.231.220.17	ppp220017.fx.ro
193.231.220.182	ppp220182.fx.ro
193.231.220.203	ppp220203.fx.ro
193.231.220.208	ppp220208.fx.ro
193.231.220.216	ppp220216.fx.ro
193.231.220.226	ppp220226.fx.ro
193.231.220.65	ppp220065.fx.ro
193.231.220.71	ppp220071.fx.ro
193.231.220.74	ppp220074.fx.ro
193.231.220.77	ppp220077.fx.ro
193.231.220.89	ppp220089.fx.ro
193.231.230.87	193.231.230.87
193.231.236.141	193.231.236.141
193.231.242.90	MIHAIB
193.231.253.224	ady624.interplus.ro
193.231.6.40	atc40.diac.tuiasi.ro
193.231.6.44	atc44.diac.tuiasi.ro
193.251.13.153	ANeuilly-101-1-2-153.abo.wanadoo.fr
193.251.33.61	ALille-201-1-2-61.abo.wanadoo.fr
193.251.42.11	APoncelet-101-2-1-11.abo.wanadoo.fr
193.252.111.116	APh-Aug-101-1-3-116.abo.wanadoo.fr
193.252.63.9	AMarseille-201-2-1-9.abo.wanadoo.fr

Source IP	Host Name
193.254.36.29	dial14-tl0.logicnet.ro
193.254.42.138	bz0-l0.logictl.net
193.254.47.67	193.254.47.67
193.6.166.178	vpk012.date.hu
193.6.17.183	isdn55.ts53.iif.hu
193.6.6.104	di4.diakir.uni-miskolc.hu
193.64.114.10	net10.printeq.fi
193.71.202.51	freedu-193-71-202-51.libertysurf.no
193.77.28.84	193.77.28.84
193.89.244.61	ip695.boanxx1.adsl.tele.dk
194.102.143.114	194.102.143.114
194.102.143.125	194.102.143.125
194.102.181.77	194.102.181.77
194.102.188.29	194.102.188.29
194.102.213.8	194.102.213.8
194.102.224.129	ns.petar.ro
194.102.242.65	194.102.242.65
194.102.242.67	194.102.242.67
194.102.242.71	194.102.242.71
194.102.250.30	iq.kappa.ro
194.102.253.109	hagi.kappa.ro
194.102.254.101	dialup-56K-101.kappa.ro
194.102.254.108	dialup-56K-108.kappa.ro
194.102.254.16	dialup-56K-16.kappa.ro
194.102.93.104	ppp11-2.digiro.net
194.102.93.111	ppp18-2.digiro.net
194.102.93.31	ppp1-1.digiro.net
194.102.93.37	ppp7-1.digiro.net
194.102.93.43	ppp13-1.digiro.net
194.102.93.50	ppp20-1.digiro.net
194.102.93.52	ppp22-1.digiro.net
194.102.93.53	ppp23-1.digiro.net
194.102.93.55	ppp25-1.digiro.net
194.102.93.60	ppp30-1.digiro.net
194.102.93.74	ppp4-v90.digiro.net
194.102.93.91	ppp21-v90.digiro.net
194.102.99.58	novell.iasi.osf.ro.99.102.194.in-addr.arpa
194.151.106.20	194.151.106.20
194.153.247.222	194.153.247.222
194.154.146.160	nic-c53s02-l152.spidernet.net
194.154.148.147	nic-c53s04-l019.spidernet.net
194.176.38.194	boxer.MACTEP.org
194.204.195.126	194.204.195.126
194.204.195.164	M1M0O7
194.205.220.45	194.205.220.45

Source IP	Host Name
194.206.208.153	194.206.208.153
194.206.208.169	194.206.208.169
194.206.208.173	194.206.208.173
194.206.208.194	194.206.208.194
194.206.208.201	194.206.208.201
194.206.208.230	194.206.208.230
194.206.208.238	194.206.208.238
194.206.208.249	194.206.208.249
194.208.52.150	194-208-052-150.TELE.NET
194.213.72.25	karo.algonet.se
194.239.155.193	194.239.155.193
194.247.82.105	WINGATE_PC
194.251.101.198	qn-lpr4-198.quicknet.inet.fi
194.42.130.110	limassol137.cylink.com.cy
194.47.102.147	hlunt98.univ.vxu.se
194.47.144.22	sorcerynet.fukt.hk-r.se
194.67.168.11	194.67.168.11
194.75.152.237	dalnet.lineone.net
194.77.98.148	hs2-148.handshake.de
194.84.208.118	hellfire.sparc2000.com
194.87.13.86	top100.rambler.ru
194.88.77.240	monopoly.fulham.vi.net
194.9.222.251	sbsi-251.222.rev.fr.colt.net
195.10.46.143	195.10.46.143
195.103.69.159	proxy.guest.net
195.115.7.2	Cegetel-fw.entreprises.cegetel.fr
195.127.250.109	udial609.a-city.de
195.132.153.115	r153m115.cybercable.tm.fr
195.132.238.183	r238m183.cybercable.tm.fr
195.132.238.93	r238m93.cybercable.tm.fr
195.132.57.32	r57m32.cybercable.tm.fr
195.132.76.194	r76m194.cybercable.tm.fr
195.132.96.165	r96m165.cybercable.tm.fr
195.138.224.45	195.138.224.45
195.139.15.242	darkwing.contempus.com
195.14.128.135	ni-6-7.cytanet.com.cy
195.14.128.90	ni-5-90.cytanet.com.cy
195.14.132.112	pa-1-112.cytanet.com.cy
195.14.132.43	pa-1-43.cytanet.com.cy
195.14.143.248	ni-8-120.cytanet.com.cy
195.14.144.187	ni-12-67.cytanet.com.cy
195.14.144.228	ni-12-108.cytanet.com.cy
195.14.145.45	ni-2-45.cytanet.com.cy
195.154.188.66	195.154.188.66
195.154.54.33	ppp33-net1-idf7-bas1.isdnet.net

Source IP	Host Name
195.159.0.151	login1.powertech.no
195.162.221.167	cable-195-162-221-167.upc.chello.be
195.162.222.156	cable-195-162-222-156.upc.chello.be
195.17.14.159	195.17.14.159
195.190.96.205	ts6-195-190-96-205.Spb.dial.sovam.com
195.214.168.11	195.214.168.11
195.214.168.84	195.214.168.84
195.215.15.130	irc.dk.quakenet.eu.org
195.34.150.82	TK150082.tuwien.teleweb.at
195.34.28.117	dialup-28117.dialup.ptt.ru
195.44.205.143	195.44.205.143
195.54.105.6	wsd-vccsc.framfab.se
195.6.226.46	ca-ol-valence-3-46.abo.wanadoo.fr
195.87.131.36	195.87.131.36
195.97.49.52	vdp020.lam01.gwc.hol.gr
198.139.244.22	philly.pa.us.dal.net
198.182.76.100	irc.blackened.com
198.63.2.192	198.63.2.192
198.78.16.3	198.78.16.3
198.82.82.82	br.campus.vt.edu
198.88.16.33	barovia.dal.net
198.88.88.99	barovia.dal.net
198.92.138.226	mail.ihostit.net
198.96.37.34	beta1-009.complex2.resnet.yorku.ca
199.120.223.5	premis.lod.com
199.224.86.36	thyme.epix.net
199.234.153.12	shell.lazerlink.net
199.36.49.2	199.36.49.2
2.2.2.2	2.2.2.2
200.182.206.65	dl-adsl-sao-C8B6CE41.sao.terra.com.br
200.191.80.181	200-191-80-181-as.acessonet.com.br
200.191.80.206	200-191-80-206-as.acessonet.com.br
200.244.177.239	200.244.177.239
200.31.30.155	dialgye107.impsat.net.ec
200.37.103.207	200.37.103.207
200.37.198.88	USER08
200.37.7.18	facf.unjbg.edu.pe
200.41.34.79	200.41.34.79
200.41.35.175	200.41.35.175
200.43.18.59	200.43.18.59
200.48.187.195	200.48.187.195
200.48.188.199	200.48.188.199
200.48.213.143	ALFA1
200.48.214.207	200.48.214.207
200.48.23.20	200.48.23.20

Source IP	Host Name
200.48.54.99	200.48.54.99
200.48.88.82	MS-12
200.48.93.2	PC1
200.50.11.20	200.50.11.20
200.50.9.33	MARK
200.50.9.72	200.50.9.72
200.51.51.201	mq1.concejomdp.gov.ar
200.53.184.66	isp66.ifxnw.com.mx
200.59.36.121	lineaAE121.velocom.com.ar
200.59.36.206	lineaAE206.velocom.com.ar
202.1.193.167	202.1.193.167
202.1.193.178	202.1.193.178
202.100.34.235	202.100.34.235
202.128.69.135	tttbbs.ppp.netpci.com
202.138.27.222	222.0612.mel.iprimus.net.au
202.142.66.15	202.142.66.15
202.142.66.156	202.142.66.156
202.147.18.158	me-as-01-158.free.net.au
202.147.18.17	me-as-01-017.free.net.au
202.147.25.168	me-as-08-168.free.net.au
202.147.251.152	202.147.251.152
202.147.27.153	me-as-10-153.free.net.au
202.152.13.131	gateway.bim.co.id
202.152.22.146	ns.widyadharma.ac.id
202.153.112.222	202.153.112.222
202.156.51.76	mcns76.docsis51.singa.pore.net
202.159.45.146	202.159.45.146
202.163.254.79	RDIMEN
202.187.24.3	202.187.24.3
202.188.217.155	202.188.217.155
202.188.26.44	lbn-26-44.tm.net.my
202.188.37.29	202.188.37.29
202.188.85.53	202.188.85.53
202.46.249.87	paue.ugm.ac.id
202.61.169.26	202.61.169.26
202.77.125.162	DATA
202.87.115.131	202.87.115.131
202.9.134.7	202.9.134.7
202.9.188.89	202.9.188.89
202.93.66.66	imam-66.pworld.net.ph
202.93.70.60	ap-sultan-60.pworld.net.ph
203.101.6.206	async205-syd-isp-6.nas.one.net.au
203.102.177.83	203.102.177.83
203.108.42.138	slpen52p10.ozemail.com.au
203.108.42.142	slpen52p14.ozemail.com.au

Source IP	Host Name
203.108.42.183	slpen52p55.ozemail.com.au
203.114.231.2	host31002.EZnet.co.th
203.114.231.33	host31033.EZnet.co.th
203.134.130.127	127.b.001.mel.iprimus.net.au
203.134.132.11	011.d.001.mel.iprimus.net.au
203.134.132.134	134.d.001.mel.iprimus.net.au
203.134.133.79	079.a.002.mel.iprimus.net.au
203.134.172.240	240.e.003.mel.iprimus.net.au
203.134.27.6	006.d.002.mel.iprimus.net.au
203.134.52.183	183.0403.mel.iprimus.net.au
203.134.7.16	016.a.002.syd.iprimus.net.au
203.135.55.113	203.135.55.113
203.143.253.35	pptp35.dyn253.pacific.net.au
203.143.253.40	pptp40.dyn253.pacific.net.au
203.148.182.108	203.148.182.108
203.148.183.22	203.148.183.22
203.148.183.44	203.148.183.44
203.149.50.79	ppp13.tsknet.org
203.155.129.101	l129ppp101.ksc.net.th
203.155.129.119	l129ppp119.ksc.net.th
203.155.129.15	l129ppp015.ksc.net.th
203.155.129.50	l129ppp050.ksc.net.th
203.155.129.78	l129ppp078.ksc.net.th
203.155.129.86	l129ppp086.ksc.net.th
203.155.129.99	l129ppp099.ksc.net.th
203.155.130.111	l130ppp111.ksc.net.th
203.155.132.140	l132ppp140.ksc.net.th
203.155.132.186	l132ppp186.ksc.net.th
203.164.23.11	co3023113-a.belrs1.nsw.optushome.com.au
203.164.90.252	co3032774-a.rivrw1.nsw.optushome.com.au
203.165.24.144	cj3069157-a.yoksk1.kt.home.ne.jp
203.167.138.158	203-167-138-158.dialup.clear.net.nz
203.168.13.13	ilo-13-13.i-next.net
203.17.149.59	203.17.149.59
203.170.144.127	203.170.144.127
203.170.154.9	203.170.154.9
203.170.157.154	203.170.157.154
203.170.157.178	203.170.157.178
203.176.33.49	203.176.33.49
203.198.110.152	203.198.110.152
203.199.79.135	203.199.79.135
203.23.238.144	modem025.ramoth.comcen.com.au
203.29.154.221	nme-56k-221.tpgi.com.au
203.32.161.197	adnet.imgserv.com
203.33.188.165	dialup293.canberra.net.au

Source IP	Host Name
203.59.106.194	reggae-00-194-106.nv.iinet.net.au
203.59.78.195	reggae-03-195.nv.iinet.net.au
203.59.80.29	reggae-18-29.nv.iinet.net.au
203.59.80.84	reggae-18-84.nv.iinet.net.au
203.59.83.169	reggae-06-169.nv.iinet.net.au
203.59.87.133	reggae-22-133.nv.iinet.net.au
203.66.42.129	203.66.42.129
203.75.25.62	203.75.25.62
203.96.91.36	203.96.91.36
204.100.64.150	204.100.64.150
204.117.70.5	security.enterthegame.com
204.123.28.11	crawler1.webresearch.pa-x.dec.com
204.152.184.80	kechara.sorcery.net
204.155.48.3	204.155.48.3
204.184.0.2	GIDEON4
204.185.36.100	SCUZZLE
204.185.36.109	BANKS1
204.185.36.187	M0P5Q0
204.210.104.40	a204b210n104client40.hawaii.rr.com
204.210.104.69	a204b210n104client69.hawaii.rr.com
204.210.160.90	dhcp204-210-160-090.insight.rr.com
204.30.99.123	204.30.99.123
204.30.99.29	204.30.99.29
205.128.11.157	205.128.11.157
205.136.57.121	fox3.foxlink.net
205.188.1.105	205.188.1.105
205.188.153.100	fes-d004.icq.aol.com
205.188.153.101	fes-d005.icq.aol.com
205.188.153.102	fes-d006.icq.aol.com
205.188.153.104	fes-d008.icq.aol.com
205.188.153.105	fes-d009.icq.aol.com
205.188.153.106	fes-d010.icq.aol.com
205.188.153.107	fes-d011.icq.aol.com
205.188.153.108	fes-d012.icq.aol.com
205.188.153.109	fes-d013.icq.aol.com
205.188.153.110	fes-d014.icq.aol.com
205.188.153.111	fes-d015.icq.aol.com
205.188.153.114	fes-d018.icq.aol.com
205.188.153.115	fes-d019.icq.aol.com
205.188.153.116	fes-d020.icq.aol.com
205.188.153.97	fes-d001.icq.aol.com
205.188.153.98	fes-d002.icq.aol.com
205.188.153.99	fes-d003.icq.aol.com
205.188.179.33	fes-d021.icq.aol.com
205.188.3.211	205.188.3.211

Source IP	Host Name
205.188.3.239	205.188.3.239
205.188.4.2	205.188.4.2
205.197.182.100	beast.toad.net
205.251.201.36	wiley-1-153636.roadrunner.nf.net
205.251.246.87	wiley246h087.roadrunner.nf.net
205.252.23.236	205.252.23.236
206.101.105.16	commcenter16.citynet.net
206.105.235.137	bay-137-b3.codetel.net.do
206.111.102.155	USA
206.128.219.83	206.128.219.83
206.140.182.244	206.140.182.244
206.167.181.162	206.167.181.162
206.183.143.241	chapterhouse.sugar-river.net
206.190.24.156	206.190.24.156
206.204.3.253	ftp1.encmpss1.com
206.231.46.1	206.231.46.1
206.253.63.135	uly-usr1-135.pld.com
206.71.111.183	hh1111183.direcpc.com
207.106.84.176	leda.jtan.com
207.114.4.46	ProxyScan.MD.US.Undernet.Org
207.123.161.43	www.itsecure.bbn.com
207.126.106.118	mandarin.peopleweb.com
207.144.250.50	207.144.250.50
207.144.250.88	207.144.250.88
207.172.148.202	207-172-148-202.s11.as3.anp.md.dialup.rcn.com
207.172.195.166	207-172-195-166.s166.tnt1.clm.md.dialup.rcn.com
207.172.195.21	207-172-195-21.s21.tnt1.clm.md.dialup.rcn.com
207.211.106.40	207.211.106.40
207.33.111.32	207.33.111.32
208.151.64.137	pcd088137.netvigator.com
208.160.245.162	ppp-e01.iloilo.net
208.160.255.78	208.160.255.78
208.184.156.138	208.184.156.138.available
208.185.24.251	mildly.arrogant.org
208.185.24.8	voyager.straynet.com
208.185.83.2	unknown.lomag.net
208.191.243.101	adsl-208-191-243-101.dsl.ltrkar.swbell.net
208.194.160.1	208.194.160.1
208.194.161.155	proxy.monitor.twisted.ma.us.dal.net
208.204.44.103	208.204.44.103
208.212.171.140	COMPUTER_10
208.212.171.155	208.212.171.155
208.224.126.73	s14.Pm2.t-one.net
208.226.155.242	lcl242.cvzoom.net
208.47.92.164	owb.kellyandwilmore.com

Source IP	Host Name
208.5.7.19	intouch2085719.intouch.com
208.52.105.204	208.52.105.204
208.58.42.162	macalpine.cornfed.com
208.61.112.254	adsl-61-112-254.mia.bellsouth.net
208.61.142.104	adsl-61-142-104.mia.bellsouth.net
208.61.4.207	adsl-61-4-207.mia.bellsouth.net
208.61.44.215	adsl-61-44-215.mia.bellsouth.net
208.61.45.79	adsl-61-45-79.mia.bellsouth.net
208.63.176.26	adsl-63-176-26.clt.bellsouth.net
208.9.110.30	starfish.intercom.net
209.1.233.136	209.1.233.136
209.10.218.248	irc.wwf.com
209.10.218.250	java.webmaster.com
209.10.218.251	irc.webmaster.com
209.10.77.201	Security.Gameslink.Net
209.115.197.52	tmmi197-052.telusvelocity.net
209.133.28.137	webmaster.ca.us.webchat.org
209.133.35.87	irc2.bondage.com
209.133.35.89	irc3.bondage.com
209.143.63.7	wapa-ras2-1-cs-4.dial.bright.net
209.148.136.22	spc-isp-wsr-uas-04-21.sprint.ca
209.160.56.44	209.160.56.44
209.176.88.16	irc.advizexweb.net
209.180.159.92	209-180-159-92.customers.uswest.net
209.185.131.251	law-www.hotmail.com
209.190.223.101	prime.atlantech.net
209.191.146.4	shell.25bway.compuhelp.com
209.206.104.75	bronx-ip-11-75.dynamic.ziplink.net
209.206.105.239	bronx-ip-12-239.dynamic.ziplink.net
209.206.107.152	bronx-ip-14-152.dynamic.ziplink.net
209.206.114.199	spartenburg-ip-3-199.dynamic.ziplink.net
209.209.68.157	209-209-68-157.la.inreach.net
209.211.58.28	shell.jaxn.com
209.212.128.41	vader.fdt.net
209.212.128.47	watto.fdt.net
209.214.7.30	host-209-214-7-30.mia.bellsouth.net
209.214.80.53	host-209-214-80-53.fll.bellsouth.net
209.214.82.86	host-209-214-82-86.fll.bellsouth.net
209.218.228.201	ATHM-209-218-xxx-201.Home.net
209.221.143.119	ops.netscan.org
209.222.168.101	roberti.transport.com
209.245.10.173	dialup-209.245.10.173.Denver1.Level3.net
209.246.136.110	COOLLINK5
209.249.77.28	host9.webmaster.com
209.25.94.109	209.25.94.109

Source IP	Host Name
209.253.109.139	A010-0139.TUSC.splitrock.net
209.254.185.128	A060-0636.MINN.splitrock.net
209.255.208.114	A030-0114.PHL2.splitrock.net
209.255.209.93	A030-0347.PHL2.splitrock.net
209.255.210.204	A030-0712.PHL2.splitrock.net
209.255.211.58	A030-0820.PHL2.splitrock.net
209.30.248.102	p102.amax37.dialup.dal1.flash.net
209.50.1.64	bea-pm1-020.inetnebr.com
209.51.166.13	neowarp.com
209.58.17.3	FreeHostingUSA.Teleglobe.net
209.61.155.53	irc.turkiye.com
209.73.164.126	tv33.sv.av.com
209.85.3.25	tmtowtdi.perl.org
209.86.44.104	user-38lcb38.dialup.mindspring.com
209.92.40.32	dslcv1-32.fast.net
209.94.100.151	209.94.100.151
209.94.199.141	cuscon1035.tstt.net.tt
209.94.199.186	cuscon1080.tstt.net.tt
209.94.224.13	server9.vonl.com
210.101.101.110	210.101.101.110
210.113.89.200	ASIC_WEB
210.154.33.43	210.154.33.43
210.23.114.185	210.23.114.185
210.9.19.185	ppp-185.cust210-9-19.ghr.chariot.net.au
211.124.193.36	zaqd37cc124.zaq.ne.jp
211.178.76.232	211.178.76.232
211.46.110.81	211.46.110.81
212.0.107.107	212.0.107.107
212.122.97.183	212.122.97.183
212.123.8.136	D47B0888.kabel.telenet.be
212.125.18.8	212.125.18.8
212.125.18.97	212.125.18.97
212.127.170.138	qn-212-127-170-138.quicknet.nl
212.139.33.169	212.139.33.169
212.143.48.167	ADSLT1-p167.adsl.netvision.net.il
212.146.28.87	baana-87.raketti.net
212.156.183.126	212.156.183.126
212.158.123.66	irc.ins.net.uk
212.160.78.75	iif3.kki.krakow.pl
212.171.112.182	212.171.112.182
212.171.123.135	212.171.123.135
212.175.252.14	212.175.252.14
212.177.241.101	212.177.241.101
212.179.125.105	bzq-125-105.bezeqint.net
212.179.125.114	bzq-125-114.bezeqint.net

Source IP	Host Name
212.179.125.92	bzq-125-92.bezeqint.net
212.179.126.227	cable-95227.bezeqint.net
212.179.127.25	bzq-128-25.bezeqint.net
212.179.15.122	clnt-15122.bezeqint.net
212.179.16.228	clnt-16228.bezeqint.net
212.179.175.216	212.179.175.216
212.179.19.134	clnt-19134.bezeqint.net
212.179.23.95	clnt-23095.bezeqint.net
212.179.24.136	clnt-24136.bezeqint.net
212.179.27.111	clnt-27111.bezeqint.net
212.179.27.189	clnt-27189.bezeqint.net
212.179.27.6	clnt-27006.bezeqint.net
212.179.29.170	clnt-29170.bezeqint.net
212.179.29.196	clnt-29196.bezeqint.net
212.179.29.213	clnt-29213.bezeqint.net
212.179.30.113	clnt-30113.bezeqint.net
212.179.30.74	clnt-30074.bezeqint.net
212.179.33.242	PT10-33242.bezeqint.net
212.179.33.254	PT10-33254.bezeqint.net
212.179.34.194	clnt-34194.bezeqint.net
212.179.38.200	clnt-38200.bezeqint.net
212.179.39.194	clnt-39194.bezeqint.net
212.179.41.137	fr-c41137.bezeqint.net
212.179.41.148	fr-c41148.bezeqint.net
212.179.41.226	fr-c41226.bezeqint.net
212.179.41.24	fr-c41024.bezeqint.net
212.179.42.2	fr-c42002.bezeqint.net
212.179.42.71	fr-c42071.bezeqint.net
212.179.42.80	fr-c42080.bezeqint.net
212.179.42.95	fr-c42095.bezeqint.net
212.179.44.106	bzq-44-106.bezeqint.net
212.179.44.114	bzq-44-114.bezeqint.net
212.179.44.115	bzq-44-115.bezeqint.net
212.179.44.66	bzq-44-66.bezeqint.net
212.179.45.241	fr-c27241.bezeqint.net
212.179.45.69	fr-c27069.bezeqint.net
212.179.45.72	fr-c27072.bezeqint.net
212.179.45.76	fr-c27076.bezeqint.net
212.179.45.79	fr-c27079.bezeqint.net
212.179.45.81	fr-c27081.bezeqint.net
212.179.45.82	fr-c27082.bezeqint.net
212.179.48.199	fr-c48199.bezeqint.net.48.179.212.IN-ADDR.ARPA
212.179.50.77	fr-c50077.bezeqint.net
212.179.56.5	212.179.56.5
212.179.58.191	212.179.58.191

Source IP	Host Name
212.179.63.10	212.179.63.10
212.179.64.189	PT712189.bezeqint.net
212.179.66.2	PT712002.bezeqint.net
212.179.67.186	212.179.67.186
212.179.67.29	212.179.67.29
212.179.7.36	clnt-7036.bezeqint.net
212.179.7.58	clnt-7058.bezeqint.net
212.179.72.226	212.179.72.226
212.179.77.49	212.179.77.49
212.179.79.115	ASSAF_G
212.179.79.2	212.179.79.2
212.179.95.16	cable-95016.bezeqint.net
212.179.95.26	cable-95026.bezeqint.net
212.179.95.45	cable-95045.bezeqint.net
212.179.95.5	cable-95005.bezeqint.net
212.18.172.177	p177-07.netc.pt
212.187.106.231	c106231.upc-c.chello.nl
212.187.21.156	c21156.upc-c.chello.nl
212.187.65.135	c65135.upc-c.chello.nl
212.198.123.8	e008.dhcp212-123.cybercable.fr
212.2.215.217	212.2.215.217
212.204.233.231	vinxs.com
212.216.228.242	a-mx1-51.tin.it
212.216.25.87	a-bg13-56.tin.it
212.216.33.168	a-bl5-41.tin.it
212.217.124.187	212.217.124.187
212.242.29.75	msx-sla-13-10.ppp.cybercity.dk
212.242.29.84	msx-sla-13-19.ppp.cybercity.dk
212.246.193.4	ip5-004.dial.tpo.fi
212.252.30.182	asy182.as30.sol.superonline.com
212.253.18.249	212.253.18.249
212.253.190.242	212.253.190.242
212.32.167.113	h21232167113.kommunicera.umea.se
212.35.129.78	212.35.129.78
212.41.53.127	user53-127.jakinternet.co.uk
212.43.196.5	inco.fr.eu.dal.net
212.43.238.183	212.43.238.183
212.46.67.212	london.afternet.org
212.46.76.30	212.46.76.30
212.54.110.175	212.54.110.175
212.54.110.250	212.54.110.250
212.54.116.79	212.54.116.79
212.54.96.169	dialup-169.totalnet.ro
212.54.97.138	212.54.97.138
212.55.140.11	212.55.140.11

Source IP	Host Name
212.64.12.65	33dyn65.com21.casema.net
212.64.26.120	5dyn120.rijswzh.casema.net
212.64.35.26	8dyn26.utr.casema.net
212.64.35.27	8dyn27.utr.casema.net
212.72.72.66	irc.traced.net
212.72.72.77	babs.BNV.BayCIX.de
212.72.75.236	212.72.75.236
212.78.153.242	dom2-242.menta.net
212.86.129.227	toolnine.argh.org
212.89.31.158	cm05998.telecable.es
212.90.79.63	cs79063.pp.htv.fi
212.93.138.217	212.93.138.217
212.93.145.67	212.93.145.67
213.1.203.250	host213-1-203-250.btinternet.com
213.1.64.35	host213-1-64-35.btinternet.com
213.112.156.148	ua-213-112-156-148.cust.bredbandsbolaget.se
213.112.23.188	ua-213-112-23-188.cust.bredbandsbolaget.se
213.112.23.46	ua-213-112-23-46.cust.bredbandsbolaget.se
213.112.62.183	ua-213-112-62-183.cust.bredbandsbolaget.se
213.123.33.189	host213-123-33-189.dialup.lineone.co.uk
213.131.74.250	host-213-131-74-250.link.net
213.132.133.168	cable-213-132-133-168.upc.chello.be
213.154.129.100	ppp94.pcnet.ro
213.154.129.28	ppp28.pcnet.ro
213.154.129.86	ppp82.pcnet.ro
213.154.130.116	ppp253.pcnet.ro
213.154.130.135	ppp272.pcnet.ro
213.154.130.184	ppp321.pcnet.ro
213.154.130.77	ppp214.pcnet.ro
213.154.131.131	ns.endzone.ro
213.154.133.190	stan.pcnet.ro
213.154.134.74	PC09
213.154.134.78	PC13
213.154.134.80	PC15
213.154.134.81	PC16
213.167.196.192	213.167.196.192
213.167.196.25	213.167.196.25
213.167.197.194	213-167-197-194.flat.galactica.it
213.167.198.191	213.167.198.191
213.167.198.8	213-167-198-8.flat.galactica.it
213.167.199.96	213.167.199.96
213.167.206.183	213-167-206-183.flat.galactica.it
213.167.209.112	213-167-209-112.flat.galactica.it
213.167.210.123	213.167.210.123
213.167.213.178	213-167-213-178.flat.galactica.it

Source IP	Host Name
213.167.215.19	213.167.215.19
213.171.130.93	213.171.130.93
213.186.134.31	NAS-213-186-134-31.ixir.com
213.186.155.47	irc.ixir.net
213.196.4.2	hosting02.truehosting.nl
213.204.134.251	251.ppp134.rsd.worldonline.se
213.213.8.223	h213-8-223.BO.infinito.it
213.224.155.131	D5E09B83.kabel.telenet.be
213.224.98.219	D5E062DB.kabel.telenet.be
213.237.14.117	213.237.14.117.adsl.hum.worldonline.dk
213.237.16.122	213.237.16.122.adsl.sd.worldonline.dk
213.255.22.98	h255-22-98.MI2.albacom.net
213.35.133.153	213.35.133.153
213.41.69.52	hosting-52.69.rev.fr.colt.net
213.43.60.144	NAS-213-43-60-144.ixir.com
213.43.69.126	213.43.69.126
213.43.69.72	213.43.69.72
213.43.72.158	213.43.72.158
213.43.77.66	213.43.77.66
213.43.80.51	213.43.80.51
213.43.86.72	213.43.86.72
213.45.155.149	a-pv15-22.tin.it
213.46.113.179	d113179.upc-d.chello.nl
213.46.128.88	d128088.upc-d.chello.nl
213.46.95.210	d95210.upc-d.chello.nl
213.48.182.156	usr999-wol.cableinet.co.uk
213.51.64.167	cc39695-a.assen1.dr.nl.home.com
213.6.220.212	Adcd4.pppool.de
213.61.112.10	gordon-shumway.alf-in-space.de
213.64.152.159	h159n1fls21o908.telia.com
213.64.65.174	h174n3fls1o843.telia.com
213.65.70.48	h48n3fls21o906.telia.com
213.76.114.60	pa60.konin.cvx.ppp.tpnet.pl
213.77.220.3	pa3.przemysl.cvx.ppp.tpnet.pl
213.8.121.25	213.8.121.25
213.8.52.189	213.8.52.189
213.96.160.88	213.96.160.88
213.96.27.142	FLUNFERT
216.10.12.2	kinetic.cpanel.net
216.10.12.30	gravity.cpanel.net
216.104.228.102	non-invasive-proximity-checking-device.safeweb.com
216.111.239.130	awww.jeah.net
216.111.248.10	216.111.248.10
216.145.193.212	mke0920.excel.net
216.148.218.160	head.rwc.rhns.redhat.com

Source IP	Host Name
216.15.153.106	ilke.ilkenet.net
216.15.182.66	s1.elitedesign.net
216.151.96.4	lithium.theshell.com
216.152.64.129	sauron.ca.us.webchat.org
216.152.64.130	glass.webmaster.com
216.152.64.137	glass2.webmaster.com
216.152.64.142	java.ca.us.webchat.org
216.152.64.143	webmaster.ca.us.webchat.org
216.152.64.150	stable.ca.us.webchat.org
216.152.64.151	katana.ca.us.webchat.org
216.152.64.213	w2k.webmaster.com
216.164.109.15	jwp3.erols.com
216.164.165.190	216-164-165-190.s190.tnt2.clm.md.dialup.rcn.com
216.170.155.148	hyky2pool1-a19.hyden.tds.net
216.176.130.250	finger-for-port-scan-info-at-hebron.in.us.dal.net
216.177.0.32	spider.603.com
216.179.0.32	suarez.bestweb.net
216.179.0.37	services.gamesnet.net
216.186.190.125	bt-125-190.cust.blacktopdsl.com
216.209.104.95	HSE-Kitchener-ppp105100.sympatico.ca
216.209.216.104	HSE-Montreal-ppp103077.sympatico.ca
216.209.219.108	HSE-Montreal-ppp103843.sympatico.ca
216.217.217.11	rs2.RisingNet.net
216.22.147.226	relic.net
216.228.142.102	v1r11.org
216.232.101.167	a0gs45y4y500j.bc.hsia.telus.net
216.232.113.15	am0g19gjb575j.bc.hsia.telus.net
216.234.161.197	mircx.com
216.238.39.101	216.238.39.101
216.247.183.4	216.247.183.4
216.252.154.115	host-216-252-154-115.interpacket.net
216.33.20.80	ftp.angelfire.com
216.35.103.79	si4000.inktomi.com
216.35.103.80	si4001.inktomi.com
216.35.103.81	si4002.inktomi.com
216.35.116.90	si3000.inktomi.com
216.35.116.91	si3001.inktomi.com
216.35.116.92	si3002.inktomi.com
216.35.217.59	216.35.217.59
216.35.217.72	216.35.217.72
216.36.20.154	bc1s3p2.dashmail.net
216.43.55.44	ats-3ccpe-0806.mcleodusa.net
216.6.117.11	ns2.hyperia.com
216.65.3.242	supercom.puternet.com
216.65.46.2	Mercury.unixrules.net

Source IP	Host Name
216.67.50.103	nas-50-103.houston.navipath.net
216.67.50.126	nas-50-126.houston.navipath.net
216.67.50.179	nas-50-179.houston.navipath.net
216.67.50.18	nas-50-18.houston.navipath.net
216.67.50.189	nas-50-189.houston.navipath.net
216.67.50.19	nas-50-19.houston.navipath.net
216.67.50.212	nas-50-212.houston.navipath.net
216.67.50.37	nas-50-37.houston.navipath.net
216.67.50.57	nas-50-57.houston.navipath.net
216.67.50.72	nas-50-72.houston.navipath.net
216.67.50.94	nas-50-94.houston.navipath.net
216.67.51.43	nas-51-43.houston.navipath.net
216.67.82.100	nas-82-100.houston.navipath.net
216.67.82.139	nas-82-139.houston.navipath.net
216.67.82.153	nas-82-153.houston.navipath.net
216.67.82.235	nas-82-235.houston.navipath.net
216.67.82.243	nas-82-243.houston.navipath.net
216.67.82.32	nas-82-32.houston.navipath.net
216.67.84.99	ip-67-84-99.orlando-t.navipath.net
216.77.213.91	host-216-77-213-91.fll.bellsouth.net
216.77.214.109	host-216-77-214-109.fll.bellsouth.net
216.79.213.87	host-216-79-213-87.sld.bellsouth.net
216.79.215.34	host-216-79-215-34.sld.bellsouth.net
216.86.203.177	adsl-gte-la-216-86-203-177.mminternet.com
216.87.208.170	ns.time-warp.net
216.94.134.20	dirk2.holoweb.net
216.95.146.101	hideout.sorcery.net
217.10.196.170	217.10.196.170
217.10.201.154	2dial154.xnet.ro
217.10.201.164	2dial164.xnet.ro
217.10.201.171	2dial171.xnet.ro
217.10.201.68	2dial68.xnet.ro
217.10.201.80	2dial80.xnet.ro
217.10.201.99	2dial99.xnet.ro
217.10.204.52	5dial52.xnet.ro
217.10.206.79	7dial79.xnet.ro
217.10.206.93	7dial93.xnet.ro
24.0.198.25	cc212886-a.bnapk1.occa.home.com
24.0.39.207	cx460178-b.fed1.sdca.home.com
24.1.251.2	24.1.251.2
24.108.117.65	24.108.117.65
24.108.140.159	24.108.140.159
24.112.119.218	cr744829-e.lngly1.bc.wave.home.com
24.112.147.180	cr648783-a.pr1.on.wave.home.com
24.112.150.20	cr518339-a.wlfdle1.on.wave.home.com

Source IP	Host Name
24.112.21.195	cr777912-a.hnsn1.on.wave.home.com
24.112.51.119	cr1021515-c.lndn1.on.wave.home.com
24.113.148.32	cr653462-a.nvcr1.bc.wave.home.com
24.113.168.58	24.113.168.58
24.113.99.78	cr1006732-a.rchmd1.bc.wave.home.com
24.114.111.229	cr304893-c.slnt1.on.wave.home.com
24.114.140.136	cr573159-a.lndn1.on.wave.home.com
24.114.251.248	cr326386-a.lndn1.on.wave.home.com
24.114.91.40	cr401913-a.lndn1.on.wave.home.com
24.128.48.165	atsatsulin.ne.mediaone.net
24.129.217.184	24.129.217.184
24.129.69.120	ss69-120.jacksonville.net
24.129.81.199	dar-81-199.jacksonville.net
24.129.82.105	dar-82-105.jacksonville.net
24.129.82.132	dar-82-132.jacksonville.net
24.13.101.55	cc1037108-a.twsn1.md.home.com
24.13.195.174	c638286-a.btnrug1.la.home.com
24.132.169.189	node1a9bd.a2000.nl
24.141.100.254	d141-100-254.home.cgocable.net
24.141.141.171	d141-141-171.home.cgocable.net
24.147.20.20	h00c0dfe990f7.ne.mediaone.net
24.15.181.254	cj588095-a.dlcty1.va.home.com
24.150.7.166	d150-7-166.home.cgocable.net
24.156.144.237	24.156.144.237
24.160.111.26	cs160111-26.houston.rr.com
24.160.248.216	mke-160-248-216.wi.rr.com
24.161.236.91	24161236hfc91.tampabay.rr.com
24.161.28.113	cm-24-161-28-113.nycap.rr.com
24.163.114.140	ffaxvahe3-3-140.cox.rr.com
24.163.205.231	nic-163-c205-231.mw.mediaone.net
24.163.42.82	rdu163-42-082.nc.rr.com
24.169.186.32	syr-24-169-186-32.twcny.rr.com
24.169.61.162	bgm-24-169-61-162.stny.rr.com
24.169.66.96	syr-24-169-66-96.twcny.rr.com
24.169.75.46	syr-24-169-75-46.twcny.rr.com
24.17.40.25	c296932-a.wtrlo1.ia.home.com
24.176.160.236	c220610-a.saltlk1.ut.home.com
24.176.165.218	c652433-f.saltlk1.ut.home.com
24.178.64.55	c783201-a.sprgfld1.mo.home.com
24.18.194.110	cx923278-b.provd1.ri.home.com
24.18.84.210	cc671589-a.abdn1.md.home.com
24.18.90.197	cc53440-a.catv1.md.home.com
24.180.134.156	cc349491-a.hwrd1.md.home.com
24.180.152.148	cc1037029-a.burl1.nj.home.com
24.180.195.78	cc438173-a.abdn1.md.home.com

Source IP	Host Name
24.180.235.62	cc1017685-f.essx1.md.home.com
24.180.92.40	cc236578-a.union1.nj.home.com
24.188.153.23	ool-18bc9917.dyn.optonline.net
24.19.23.143	c393974-a.iowact1.ia.home.com
24.191.241.82	ool-18bff152.dyn.optonline.net
24.200.122.185	modemcable185.122-200-24.mtl.mc.videotron.ca
24.200.14.91	modemcable091.14-200-24.que.mc.videotron.ca
24.200.140.155	modemcable155.140-200-24.mtl.mc.videotron.ca
24.200.171.66	modemcable066.171-200-24.mtl.mc.videotron.ca
24.200.80.101	modemcable101.80-200-24.mtl.mc.videotron.ca
24.200.9.10	modemcable010.9-200-24.que.mc.videotron.ca
24.200.91.109	modemcable109.91-200-24.mtl.mc.videotron.ca
24.201.112.10	modemcable010.112-201-24.timi.mc.videotron.ca
24.201.72.26	modemcable026.72-201-24.mtl.mc.videotron.ca
24.201.86.191	modemcable191.86-201-24.timi.mc.videotron.ca
24.201.96.70	modemcable070.96-201-24.mtl.mc.videotron.ca
24.21.108.133	cx600416-b.irvn1.occa.home.com
24.21.80.190	cx692004-a.santab1.ca.home.com
24.214.18.65	user-24-214-18-65.knology.net
24.214.77.118	user-24-214-77-118.knology.net
24.218.41.5	h0090272aeec8.ne.mediaone.net
24.22.255.128	cc133072-a.lwrnc1.in.home.com
24.222.84.30	u84n30.hfx.eastlink.ca
24.222.92.233	u92n233.hfx.eastlink.ca
24.226.167.52	167-52.tr.cgocable.ca
24.228.45.172	cv220967-a.norwlk1.ct.home.com
24.228.60.34	24.228.60.34
24.229.67.16	Computer-1.msns.str.ptd.net
24.23.151.112	cx673530-a.vbch1.va.home.com
24.23.158.27	cx386650-c.vbch1.va.home.com
24.232.14.61	OL61-14.fibertel.com.ar
24.232.24.26	OL26-24.fibertel.com.ar
24.232.63.148	OL148-63.fibertel.com.ar
24.234.93.60	dhcp060.93.lvcm.com
24.24.105.86	m12bhPs1n86.midsouth.rr.com
24.24.138.13	we-24-24-138-13.we.mediaone.net
24.24.98.22	m4bhSs5n22.midsouth.rr.com
24.240.33.192	24-240-33-192.hsacorp.net
24.26.55.231	24.26.55.231
24.27.222.61	24.27.222.61
24.27.230.65	PAVILION
24.28.238.136	gso28-238-136.triad.rr.com
24.28.70.200	cs2870-200.austin.rr.com
24.29.206.229	rm02-24-29-206-229.ce.mediaone.net
24.3.161.193	cc287787-b.union1.nj.home.com

Source IP	Host Name
24.3.52.127	cc537169-a.essx1.md.home.com
24.3.52.236	cc816150-a.essx1.md.home.com
24.31.150.211	ubr02-24-31-150-211.maine.rr.com
24.31.240.83	mkc-31-240-83.kc.rr.com
24.31.88.99	a24b31n88client99.hawaii.rr.com
24.4.251.183	cc211413-a.mdltwn1.nj.home.com
24.40.46.225	cn17773-a.newcas1.de.home.com
24.42.132.240	cr59109-a.yec1.on.wave.home.com
24.42.164.65	cr833142-a.wlfdle1.on.wave.home.com
24.42.193.203	cr381257-a.etob1.on.wave.home.com
24.43.119.84	cr498384-a.slnt1.on.wave.home.com
24.48.16.119	dynamic-16-119.pha.adelphia.net
24.51.197.148	fl-wbu1-c4-197-148.pbc.adelphia.net
24.6.151.155	cc941502-a.hwrd1.md.home.com
24.6.176.79	cx419097-a.chspk1.va.home.com
24.64.188.44	24.64.188.44.on.wave.home.com
24.65.121.98	h24-65-121-98.ss.shawcable.net
24.65.126.116	h24-65-126-116.ss.shawcable.net
24.65.145.247	24.65.145.247
24.65.78.210	24.65.78.210.on.wave.home.com
24.65.80.127	24.65.80.127.on.wave.home.com
24.66.231.148	h24-66-231-148.ed.shawcable.net
24.68.160.31	h24-68-160-31.ed.shawcable.net
24.68.89.6	24.68.89.6.on.wave.home.com
24.69.177.12	24.69.177.12.on.wave.home.com
24.69.209.73	24.69.209.73
24.69.214.58	h24-69-214-58.du.shawcable.net
24.7.227.215	c921627-a.alntn1.tx.home.com
24.72.12.211	static24-72-12-211.reverse.accesscomm.ca
24.9.152.152	cc882301-a.abdn1.md.home.com
24.9.64.57	ci532059-a.ruthfd1.tn.home.com
24.92.122.5	dt11q1n05.elp.rr.com
24.92.207.46	dt173n2e.tampabay.rr.com
24.92.249.27	syr-24-92-249-27.twcny.rr.com
24.92.249.28	syr-24-92-249-28.twcny.rr.com
24.92.30.130	dt0c1n82.tampabay.rr.com
24.93.201.55	a2-2b055.neo.rr.com
24.94.224.180	okc-94-224-180.mmcable.com
24.94.47.81	bgm-24-94-47-81.stny.rr.com
24.95.110.53	m10bhXs2n53.midsouth.rr.com
24.95.18.23	dt052n17.maine.rr.com
24.95.192.51	roc-24-95-192-51.rochester.rr.com
24.95.207.144	roc-24-95-207-144.rochester.rr.com
24.95.24.100	dt0c0n64.maine.rr.com
24.95.244.128	ubr-95.244.128.stcloud.cfl.rr.com

Source IP	Host Name
24.95.93.59	dhcp9593059.columbus.rr.com
32.101.117.246	slip-32-101-117-246.va.us.prserv.net
35.10.185.26	alfafara.user.msu.edu
35.9.37.225	ike.egr.msu.edu
38.15.52.5	WEBTRENDS1
38.196.148.130	38.196.148.130
38.200.223.8	38.200.223.8
38.33.36.114	ip114.milwaukee11.wi.pub-ip.psi.net
38.38.25.126	ip126.laurel11.md.pub-ip.psi.net
4.19.104.226	net104-226.jal.cc.il.us
4.35.184.141	lsanca1-ar8-184-141.dsl.gtei.net
4.4.56.174	PPPa17-ResaleTampaB1-2R7028.dialinx.net
4.4.56.194	PPPa37-ResaleTampaB1-2R7028.dialinx.net
4.4.56.220	PPPa63-ResaleTampaB1-2R7028.dialinx.net
4.48.8.114	PPPa53-ResaleTampaB3-1R7356.dialinx.net
4.48.8.84	PPPa23-ResaleTampaB3-1R7356.dialinx.net
4.54.73.153	PPPa60-ResaleOlympia4-4R7164.dialinx.net
61.11.233.113	IMRAN
61.11.234.170	61.11.234.170
61.11.234.73	61.11.234.73
61.11.238.86	61.11.238.86
62.108.8.119	node0877.a2000.nl
62.11.153.125	ca1-125.dialup.tiscalinet.it
62.11.155.27	ca1-539.dialup.tiscalinet.it
62.136.10.186	modem-186.sodium.dialup.pol.co.uk
62.136.2.72	modem-72.lithium.dialup.pol.co.uk
62.136.216.9	modem-9.kleins-butterfly.dialup.pol.co.uk
62.136.235.97	modem-97.blue-head-tilefish.dialup.pol.co.uk
62.136.46.136	modem-136.cesium.dialup.pol.co.uk
62.136.90.120	modem-120.dextroamphetam.dialup.pol.co.uk
62.137.44.152	modem-24.orbic-cardinal.dialup.pol.co.uk
62.137.81.199	modem-199.new-jersey.dialup.pol.co.uk
62.226.88.88	p3EE25858.dip.t-dialin.net
62.252.177.197	m453-mp1-cvx2a.lan.ntl.com
62.252.4.220	m220-mp1-cvx1a.gui.ntl.com
62.253.44.15	m15-mp1-cvx1c.nth.ntl.com
62.253.44.42	m42-mp1-cvx1c.nth.ntl.com
62.253.45.130	m386-mp1-cvx1c.nth.ntl.com
62.253.46.27	m539-mp1-cvx1c.nth.ntl.com
62.253.47.14	m782-mp1-cvx1c.nth.ntl.com
62.253.72.79	m79-mp1-cvx1b.bre.ntl.com
62.253.88.38	m38-mp1-cvx2c.bre.ntl.com
62.255.97.29	m285-mp1-cvx3a.bre.ntl.com
62.27.247.90	dialin-port2139.access.nacamar.de
62.29.12.114	62.29.12.114

Source IP	Host Name
62.29.9.21	62.29.9.21
62.36.132.126	62.36.132.126
62.4.170.59	62.4.170.59
62.59.137.4	ppp4-137-59-62.rtm.zonnet.nl
62.6.71.0	62.6.71.0
62.83.112.21	21-LASP-X13.libre.retevision.es
62.83.7.229	229-MADR-X30.libre.retevision.es
62.96.171.103	m-dialin-583.addcom.de
62.98.122.66	62.98.122.66
62.98.125.11	OEMCOMPUTER
62.98.131.42	62.98.131.42
62.98.158.213	62.98.158.213
62.98.166.33	62.98.166.33
62.98.33.172	62.98.33.172
62.98.68.221	62.98.68.221
63.102.143.205	mal-asc3-ppp205.sheltonbbs.com
63.103.51.141	COMPUACTION
63.103.51.158	63.103.51.158
63.104.49.126	irv-hh-gw.headhunter.net
63.119.91.2	63.119.91.2
63.119.91.3	63.119.91.3
63.144.122.4	63.144.122.4
63.147.197.27	bend-over.ill.get.the.kay-why.com
63.160.118.8	cols631601188.cols.net
63.160.119.113	shahd63160119113.shahd.com
63.162.239.69	63_162_239_69.belz.com
63.164.155.131	63.164.155.131
63.167.58.13	63.167.58.13
63.168.242.7	legend.KIREnet.com
63.193.210.208	adsl-63-193-210-208.dsl.snfc21.pacbell.net
63.195.56.20	adsl-63-195-56-20.dsl.snfc21.pacbell.net
63.197.150.195	adsl-63-197-150-195.dsl.snfc21.pacbell.net
63.202.13.20	adsl-63-202-13-20.dsl.snfc21.pacbell.net
63.206.169.128	adsl-63-206-169-128.dsl.sktn01.pacbell.net
63.209.84.218	dialup-63.209.84.218.LosAngeles1.Level3.net
63.214.82.65	dialup-63.214.82.65.Boston1.Level3.net
63.216.170.100	63.216.170.100
63.216.241.185	63-216-241-185.sdsl.cais.net
63.227.180.164	dsl-gw2-c164.clsp.uswest.net
63.227.65.135	desmdslgw3poolB135.desm.uswest.net
63.229.75.205	phnxdslgw7poole205.phnx.uswest.net
63.238.214.65	irc.friendlynet.com
63.248.225.22	3ff8e116.dsl.flashcom.net
63.252.119.242	A030-0750.LAUR.splitrock.net
63.253.225.174	A060-0174.SNFC.splitrock.net

Source IP	Host Name
63.26.138.103	1Cust103.tnt2.carbondale.il.da.uu.net
63.26.138.110	1Cust110.tnt2.carbondale.il.da.uu.net
63.26.138.12	1Cust12.tnt2.carbondale.il.da.uu.net
63.26.138.250	1Cust250.tnt2.carbondale.il.da.uu.net
63.26.7.170	1Cust170.tnt1.wilmington.nc.da.uu.net
63.26.7.189	1Cust189.tnt1.wilmington.nc.da.uu.net
63.26.7.24	1Cust24.tnt1.wilmington.nc.da.uu.net
63.27.120.10	1Cust10.tnt1.carbondale.il.da.uu.net
63.27.120.12	1Cust12.tnt1.carbondale.il.da.uu.net
63.27.120.122	1Cust122.tnt1.carbondale.il.da.uu.net
63.27.120.133	1Cust133.tnt1.carbondale.il.da.uu.net
63.27.120.147	1Cust147.tnt1.carbondale.il.da.uu.net
63.27.120.163	1Cust163.tnt1.carbondale.il.da.uu.net
63.27.120.173	1Cust173.tnt1.carbondale.il.da.uu.net
63.27.120.179	1Cust179.tnt1.carbondale.il.da.uu.net
63.27.120.18	1Cust18.tnt1.carbondale.il.da.uu.net
63.27.120.204	1Cust204.tnt1.carbondale.il.da.uu.net
63.27.120.214	1Cust214.tnt1.carbondale.il.da.uu.net
63.27.120.235	1Cust235.tnt1.carbondale.il.da.uu.net
63.27.120.24	1Cust24.tnt1.carbondale.il.da.uu.net
63.27.120.241	1Cust241.tnt1.carbondale.il.da.uu.net
63.27.120.254	1Cust254.tnt1.carbondale.il.da.uu.net
63.27.120.37	1Cust37.tnt1.carbondale.il.da.uu.net
63.27.120.38	1Cust38.tnt1.carbondale.il.da.uu.net
63.27.120.66	1Cust66.tnt1.carbondale.il.da.uu.net
63.27.120.67	1Cust67.tnt1.carbondale.il.da.uu.net
63.27.120.89	1Cust89.tnt1.carbondale.il.da.uu.net
63.27.120.91	1Cust91.tnt1.carbondale.il.da.uu.net
63.27.120.98	1Cust98.tnt1.carbondale.il.da.uu.net
63.39.89.1	1Cust1.tnt10.tco2.da.uu.net
63.46.46.143	1Cust143.tnt2.sierra-vista.az.da.uu.net
63.64.208.20	host20.208.64.63
63.66.18.6	pimpin.yerbox.org
63.66.18.8	webmail.haylan.net
63.69.211.217	63.69.211.217
63.70.26.91	63.70.26.91
63.81.226.70	ppp.63.81.226.070.dragonbbs.com
63.83.225.106	63.83.225.106
63.94.12.3	onramp.i2k.com
63.94.12.5	offramp.i2k.com
63.98.143.10	63.98.143.10
64.110.122.243	host-64-110-122-243.interpacket.net
64.180.54.112	ak0a19wxb134i.bc.hsia.telus.net
64.193.123.121	dsl-64-193-123-121.telocity.com
64.197.163.152	A070-0978.CMB2.splitrock.net

Source IP	Host Name
64.197.163.41	A070-0867.CMB2.splitrock.net
64.197.163.45	A070-0871.CMB2.splitrock.net
64.20.129.230	ip-20-129-230.nyc-t.navipath.net
64.20.134.227	ip-20-134-227.nyc-t.navipath.net
64.208.37.55	crawler2.googlebot.com
64.229.0.11	HSE-Hamilton-ppp191376.sympatico.ca
64.24.44.141	c04-141.012.popsite.net
64.252.0.93	93.0.252.64.snet.net
64.252.1.124	124.1.252.64.snet.net
64.252.4.55	55.4.252.64.snet.net
64.37.114.73	server5.twistedhumor.com
64.37.114.76	server13.twistedhumor.com
64.38.143.132	ip-64-38-143-132.dialup.seanet.com
64.64.226.2	64.64.226.2
64.65.0.178	python.ircore.net
64.65.0.206	64.65.0.206
64.65.0.83	ns.thisnet.org
64.65.2.253	ns.eliteorbit.com
64.65.56.114	ns.hostingtower.com
64.7.75.82	64.7.75.82
64.80.63.121	kkr121.parklink.com
64.81.30.185	dsl081-030-185-sea1.dsl-isp.net
64.84.40.12	12-40.84.64.master-link.com
64.86.5.250	proxy3.monitor.dal.net
64.86.6.250	proxy2.monitor.dal.net
65.1.218.215	65.1.218.215
65.26.138.18	mkc-65-26-138-18.kc.rr.com
65.27.52.68	wks-65-27-52-68.kscable.com
65.5.30.2	c623920-c.ptlum1.sfba.home.com
66.26.46.225	rdu26-46-225.nc.rr.com

Insights and Correlations from Previous Students' Practicals

Watchlist (NET-NCFC)

As member of the Watchlist (NET-NCFC), Network 159.226.X.X, continues to display hostile behavior. This network, according to a whois query, is The Computer Network Center Chinese Academy of Sciences. It is ranked #3 on my list of Top 30 Source Networks list, which ranks source networks by the number of alerts that originated from them. It was interesting to find that 96% (7852 SMTP alerts/8166 total alerts) of the alerts were SMTP alerts. This activity pattern was also noted by Clark Crist, GCIA at http://www.sans.org/y2k/practical/Crist_Clark_GCIA.html. He, too, noted "significant SMTP traffic" from the 159.226.X.X network.

Top 10 Most Attempted Access MY.NET IPs from 159.226.X.X:

MY.NET IPs	Frequency (# of Alerts from 159.226.X.X)
192.169.6.7	5801
192.169.100.230	1299
192.169.253.43	461
192.169.253.41	186
192.169.253.42	155
192.169.99.51	70
192.169.100.81	53
192.169.145.9	41
192.169.6.34	13
192.169.145.18	13

DNS-DNS Traffic

MY.NET had much DNS-DNS (udp 53-udp 53) traffic. Although there is nothing technically wrong with this kind of traffic, large traffic to your DNS server from external sources could mean that hostile activity is taking place. The most active source ip, 160.78.49.191, did not resolve on a whois query. The second-most active source ip, 130.89.229.48, was registered to a Netherlands University school computer, and the website is http://www.utwente.nl . I am uncertain whether you have any affiliation with these two networks, but if you have no connection with them, you may want to have this investigated. Unregistered networks and school networks are good places for attackers to launch their attacks. Donald MacLeod, GCIA also saw the same suspicious traffic from different source IPs at http://www.sans.org/y2k/practical/D_MACLEOD_GCIA.doc.

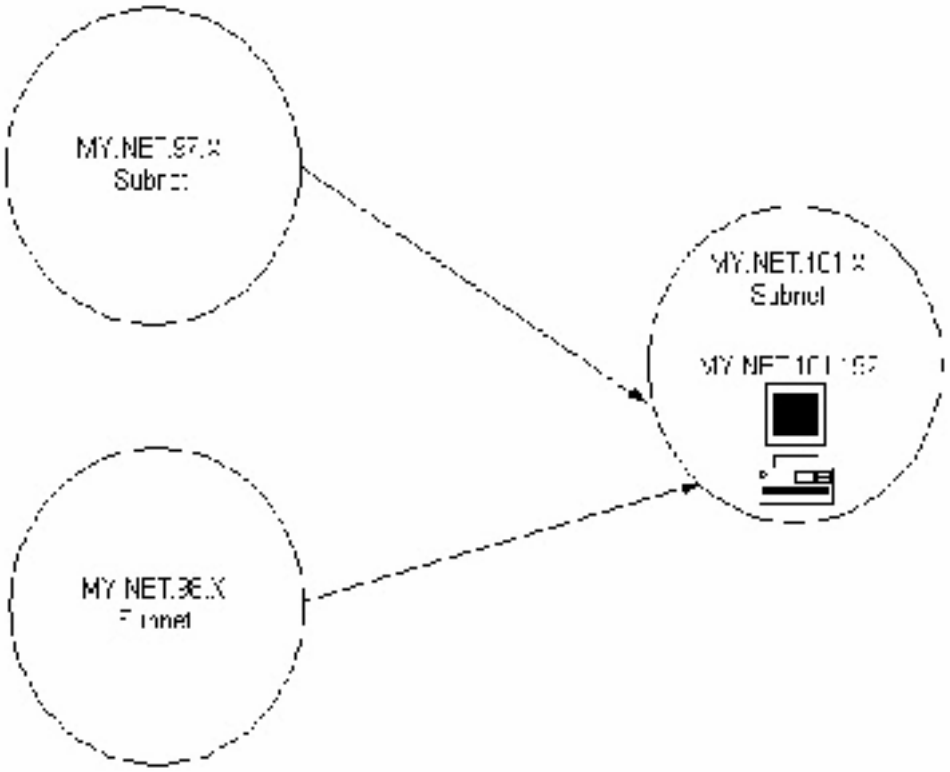
Source IP	Frequency (# of Accesses)
160.78.49.191	7199
130.89.229.48	3860
195.103.69.159	3292
212.0.107.107	2338
143.89.13.3	1584
192.102.197.234	23
205.128.11.157	4
63.104.49.126	3

SNMP with Public String

SNMP with the default strings is a major security hazard and is noted on SANS top ten list. The SNORT alarms informed me that hosts in the MY.NET.97.X network and in the MY.NET.98.X network were sending SNMP traffic to MY.NET.101.192 using the common "public" string. This poses a risk to MY.NET, and the community string should be changed to a better one. The link graph on the following page displays the SNMP traffic. William Stearns, GCIA, has also seen similar SNMP traffic of hosts reporting to a single manager. http://www.sans.org/y2k/practical/william_stearns_gcia.html

Assignment 2 LINK GRAPH

SNMP Traffic Link Graph



Statistics

Total SNMP Alerts = 450
Total SNMP Alerts sourcing from MY.SUBNET.97.X = 23
Total SNMP Alerts sourcing from MY.SUBNET.90.X = 207

Conclusions

- All SNMP Traffic originated from either the MY.NET.97.X or the MY.NET.90.X subnet.

- All SNMP Traffic was directed towards one specific host: MY.NET.101.192.

From the statistics, one can assume that MY.NET.101.192 is the SNMP manager, and the hosts that produced the SNMP Alerts are the SNMP agents.

- checked for any SNMP Alerts that were either from an external source or destined to an external source, and there was none.

SUNRPC High Port Access

This is another alert that is on SANS Top ten list. As mentioned previously, access to the SUNRPC ports should be monitored closely especially if the source is from outside the network. The top nine source IPs were not resolvable by a whois query. Compared to Clark Crist's practical (http://www.sans.org/y2k/practical/Crist_Clark_GCIA.html), I have relatively small number of SUNRPC port accesses (60 SUNRPC high port access alerts). The most active source IP, 216.10.12.30, constantly used port 2078 to connect to the SUN RPC port 32771. The same activity (with a different souce port however) is shown also in Clark Crist's practical.

Source Ips	Frequency (# of Accesses)
216.10.12.30	33
216.148.218.160	6
205.188.3.211	4
24.18.90.197	3
205.188.3.239	3
195.34.28.117	3
205.188.4.2	2
24.40.46.225	1
216.10.12.2	1
212.86.129.227	1
211.46.110.81	1
205.188.1.105	1
129.123.6.14	1

Telnet Activity – Possible Prelude to Compromise

Probing deeper into the activities of the Watchlist IPs, I decided to explore telnet as did Clark Crist. I came up with similar findings. There are Watchlist hosts that try to establish a telnet session with one MY.NET. host. There does seem to be telnet activity going on. This is my recreation of the scene:

1. It seems that the first connect is shown in the first alert where the source host port: 1665 is connecting to telnet port 23 on the MY.NET. host.
2. Then for the next four packets, it appears the telnet session continues. I thought that this maybe a TCP retry but the retry times are not consistent and they are sometimes 34 seconds apart.
3. On the sixth alert shown, it appears the attacker tries to establish another telnet connection (shown by the new source port 1509) with the same MY.NET host. It appears he is not able to do so this time.
4. It appears though the original telnet session is still going on all the way till the end where no more further data is provided. I am assuming either the connection was terminated or logging ceased for one reason or another.
5. Then the last two alerts show a new telnet session trying to be established from a different Watchlist host (`159.226.45.3`).

I looked at the OOS files hoping that the packets for this telnet activity was captured, but they were not available. It would have been very informative and interesting to see what data was passed back and forth in the payload of the packets.

```
10/09-20:09:09.857962  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:09:19.670104  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:10:53.624198  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:10:56.334002  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:12:56.760300  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:07:59.340476  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1509 -> 192.169.6.7:23
10/09-20:09:09.857962  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:09:19.670104  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:10:53.624198  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:10:56.334002  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/09-20:12:56.760300  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.204:1665 -> 192.169.6.7:23
10/06-00:00:02.864385  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:1201 -> 192.169.6.7:23
10/06-00:00:03.582799  [**] Watchlist 000222 NET-NCFC [**]
159.226.45.3:1201 -> 192.169.6.7:23
```

HAPPY 99 Virus – A possible compromise

There were only two hosts that were recipients of the Happy 99 Virus via email. The destination port 25 (SMTP) shows that the virus was sent via email by two different sources. The first source IP, 216.6.117.11, resolved to NS2.HYPERIA.COM, and the second IP, 209.94.224.13, does not resolve. Again, I checked the OOS files to see if a possible compromise may have occurred, but when I grep'ed the time for both of the alert times, I did not come up with any hits.

```
10/05-03:59:51.460766  [**] Happy 99 Virus [**] 216.6.117.11:41827 ->
192.169.253.41:25
11/06-16:06:44.170359  [**] Happy 99 Virus [**] 209.94.224.13:2708 ->
192.169.6.35:25
```

Defensive Recommendations

1. Since 26% (39,146 Watchlist Alerts/ 151,038 total alerts) of the alerts received were from Watchlist sources, it may be a good idea to block traffic altogether from these Watchlist IPs altogether at the border router or the firewall.

2. As discussed previously, there was much SMTP traffic from a Watchlist source IP. There are various SMTP exploits that have been proven to be very detrimental to a network. As a result, the SANS top ten list recommends that the SMTP port (25 tcp) should be blocked "to all machines, which are not external mail relays".

3. To improve SNMP security, one should block SNMP ports (161 tcp & udp, 162 tcp & udp) on the border router or the firewall to prevent external sources access from sending SNMP traffic to your network. Also, the "public" community string must be changed to an uncommon string.

4. To improve DNS security, DNS ports (53 udp) should be blocked to all machines which are not DNS servers. To prevent exploits on DNS zone transfers, port 53 (tcp) should also be blocked except from external secondary DNS servers.

5. To prevent any exploits on hosts running SUN RPCs, port 32771 should be blocked as well on the border router and firewall. You may also want to do a scan of your own network to see what hosts have the SUN RPC service running, and you may want to turn the RPC services off.

6. Also you may want to consider (stemming from my analysis on a telnet session established by a Watchlist source IP), blocking telnet at the border router and firewall as well. If inbound telnet access is needed then make a specification of what range of IPs are permitted to have inbound telnet sessions. Also you may also want to check the host (MY.NET.6.7) that had the telnet session mentioned above for signs of compromise.

7. Since you have two separate instances of the Happy 99 Virus, you should immediately inspect the hosts that received them and ask the personnel if the attachment was opened. The two hosts were: 192.169.253.41:25 and 192.169.6.35:25.

Other Suggestions

1. If you have the funds and the means to do so, you may want to set up a honey pot in your DMZ, and log traffic going to the honey pot.
2. To avoid lapses in log data, you may want to have a back-up IDS with plenty of disk space and a back-up power source.

3. Set up host IDS systems wherever possible. Real Secure has a host IDS and even NT's Network Monitor logs packets it receives.
4. Pay careful attention to the source ips, destination ports, and destination ips that were mentioned in the Top 30 lists mentioned above.

Summary

Your network is a target of various types of attacks, scans, and probes. It is imperative that security be a main concern for your network. Some attacks may have passed through your current defenses, and closer inspection of probable compromised hosts is needed. The Happy 99 Virus, for example, may have infected other computers of your network. I am not quite sure where the SNORT IDS system was placed (hopefully before your firewall), but in case it is not before your firewall, I believe your border router access control lists and firewall rules need to be updated. As a conclusion, I will briefly summarize my findings. There were many alerts caused by traffic from Watchlist source ips. In one trace, it was interesting to find that 96% of the traffic from one of the watchlist source ip's was for SMTP. DNS was also a hot target as well. MY.NET. is still using the default "public" string for SNMP. There were a few connections to the SUN RPC port, but it only takes one to compromise a host and begin an attack. Telnet sessions were also seen established by a source ip belonging to the Watchlist. The happy Virus may have compromised at least two hosts as well.

Assignment 3 - Analysis Process

Preparation

Before I began anything, I read the analysis processes of other practicals before I began. I needed to know where to start, and I wanted to avoid re-inventing the wheel wherever possible. Before long, I knew what troubles others had to face, and I got some pretty good suggestions on how to handle huge files of data.

After I got a good idea of what others did and what pitfalls to avoid, I mapped out a strategy of how I was going to handle the data. It didn't take me too long to realize that I would have to give up my attachment to Windows and read a good UNIX book and learn some UNIX tools. I read "UNIX Unleashed by SAMS Publishing"; it's a pretty good book. I did not have constant access to a LINUX or UNIX machine, so I took the advice of a friend and downloaded CYGWIN from www.download.com. It puts a Unix shell on your Windows PC and lets you run many of UNIX's basic commands. It suited my needs fine for this assignment.

I, then, downloaded the Alert, Scan, and OOS files and I was practicing sed, grep, awk, and sort. As time progressed, they practically became my best friends. =)

Data Manipulation

I downloaded the zipped files down to my computer, and I created separate directories for each. I then unzipped the files in their respective directories. I then concatenated all the separate files into one large file. I issued the following commands

```
grep –h '^[0-1]' SnortAle.txt SnortA[0-9]*.txt > allalerts
grep –h '^[SON][eco][ptv]' SnortSca.txt SnortS[0-9]*.txt > allscans
cat OOScheck.txt OOSche[0-9]*.txt >alloos
```

These commands get rid of the headings and comments are in the individual data files.

Converting the data files to space delimited format

The awk command works wonders with space delimited data files. The only problem was that the alert data files had spaces in the alert identifier. I needed to get rid of the spaces in the alert name to properly use awk. So I used a a series of sed commands:

```
sed –e 's/\[\*\*\]/,/g' allalerts >z        (turns the [**] into a comma)
sed –e 's/-/,/g' z>z2                       (separates the date and the time by a comma)
sed –e 's/\([0-9][0-9]*\.[0-9][0-9]*\):\([0-9]\)\1/,\2/g' z2 >z3   (parses the time)
sed –e 's/>//g' z3>z4                       (gets rid of extra > mark)
sed –e 's/ //g' z4>z5                       (gets rid of the spaces everywhere)
```

sed –e ‘s/,/ /g’z5>z6 (turn all the commas to spaces)

The scan files were very easy to parse using awk because everything is space delimited already, so you can use awk right away.

Further manipulation of the data to get specific data

The spp_scans threw off my data so I pulled them out and handled them separately.
grep –v ‘spp’ z6> allalerts2

Now you can pick and choose what field you want to print using the awk command. To get a unique listing of attacks you would use:

awk ‘{print $3}’ allalerts2 | sort –u >listofattacks

To pick and choose which fields you want, and to format your logs so that fields are easy to search we use awk again. For example if we want to display the source and destination ip’s only you would do the following:

```
awk ‘{print $5” “$6}’ allalerts2 | sed –e ‘s/:/ /g’ |
        awk ‘{print “sip “$1” dip “$3}’ > alertsourcedestip
```

Now, to get source and destination ports you would do something very similar:

```
awk ‘{print $5” “$6}’ allalerts2 | sed –e ‘s/:/ /g’ |
        awk ‘{print “s_port “$2” d_port “$4}’ > alertsourcedestport
```

For the scan files you would use very similar awk commands as shown above.

To sort through the OOS files, I just resorted to a combination of grep commands to find certain fields I was looking for.

To do a list of source addresses and registration info, I downloaded snort_sort.pl from www.snort.com and used it. It took just under an entire day for the script to resolve all the alert source IPs. Unfortunately for me, sort_sort outputs its data into html format for viewing in a web browser. When the script was through, I went through a long sequence of sed and awk commands to take out the html parts. I finally ended up with a two column data file with source ips and resolved host names. Here are some of the steps I performed

sed –e ‘s/<a href=http:\/\/www.arin.net\/cgi-bin\/whois.pl?queryinput=/ /g’ snortsort.html>z

sed –e ‘s/<\/a>:/ /g’ z >z2

grep '<h3>' z2 (in snort_sort, all the data records began with '<h3>')

etc…

then I used awk to get the columns, I wanted (source ip and resolved host name).

Top Talkers List

Now to do a top talkers list, I needed to make a counting algorithm. For easy and quick counts I used combinations of piped grep commands and wc commands. But for the more laborious counts I needed a program or a script. Due to my limited understanding of scripting, I wrote and compiled a C program called counter.c that counts the number of occurrences of a specific field and outputs to a file called "countresults.txt". The program is in appendix A. This is a very quick and dirty program I wrote; the algorithm is inefficient, but it does its job. If you would like to use it, a little modification may be necessary. With this program, I got all the results for my Top 30 lists (the top talker's lists). It takes in a file called an index which is a list of unique strings (the strings to be searched for), and it takes another file (target file) which is composed of multiple occurrences of the unique strings. It will maintain a count of how many times each unique string occurs in the target file. For you to use it, you must compile it first with a c compiler. I used gcc to compile mine. To compile, issue the command: gcc counter, and it turn gcc will give you an executable so you can run it (usually a.out).

Now for the top talker's list for source IP's, I first used the counter.c program but that proved to be ineffective because there are millions of source IPs. I decided to do a top talker's list by source NETWORKS instead. So I had to modify my count.c code to do a little more, and hence came ipfinder.c (don't ask me why I chose this name). Ipfinder.c will take a list of IP addresses and search for and maintain a count of how many times each ip address in that list appears. It will also categorize each IP address by class. Note: you must feed it two identical data files. Yes, it is inefficient, but quick and dirty. You can find the code for ipfinder.c in appendix B. The program; however, slow it was proved to be quite useful. It ouputs the data to a file called "ipfindercount.txt". In order to use it, you must first compile this program as well. I again used gcc.

Correlations
I performed my correlations by doing searches on SANS, google, securityfocus.com,etc for the topic I wanted to correlate with.

Link Graph
I did my link graph on SNMP traffic analysis. Through various grep and wc commands I came up with how SNMP traffic was going and I did my link graph on VISIO.

Defensive Recommendations
I came up with my analysis and defense recommendations through my readings of other practicals and through searches on other security sites. SANS Top 10 was a good guide to go by.

Appendix A- counter.c

```
#include <stdio.h>
#include <string.h>

int main (void){

int counter = 0;
char stringdescription[100];
char searchedstring[20], currentstring[20];
char indexfile[200], comparisonfile[200];

FILE *index;
FILE *file;
FILE *output;

printf("Enter the index file: ");
gets(indexfile);

index = fopen(indexfile,"r");

if(index==NULL) {
       printf ("Can't open the indexfile.");
       return 1;
  }
output = fopen("countresults.txt","w");

printf("Enter the comparisonfile: ");
gets(comparisonfile);

printf("Enter description: ");
gets(stringdescription);

while(fgets(searchedstring,20,index)!=NULL) {
    file = fopen(comparisonfile,"r");
    if(file==NULL) {
       printf ("Can't open the comparisonfile");
      return 1;
    }

    while(fgets(currentstring,20,file)!=NULL) {
        if(strcmp(currentstring,searchedstring)==0)
            counter++;
    }

    fprintf(output,"count= %d %s
%s",counter,stringdescription,searchedstring);
    counter = 0;
    fclose(file);
}
fclose(index);
fclose(output);
printf("Done.");
}
```

Appendix B- ipfinder.c

```
#include <stdio.h>

int octet1=0,octet2=0,octet3=0,octet4=0,counter=0;
int octet21=0,octet22=0,octet23=0,octet24=0;
char class;
char record[400],record2[400];
char inputfile[400],inputfile2[400];

FILE *datafile, *datafile2;
FILE *outputfile;

int main (void){

printf("Enter the data file:");
gets(inputfile);

datafile =fopen(inputfile,"r");
if(datafile==NULL) {
       printf ("Can't open the datafile.");
       return 1;
}

printf("Enter the second file:");
gets(inputfile2);


outputfile = fopen("ipfindercount.txt","w");

while(fgets(record,400,datafile)!=NULL) {
      sscanf(record," %d %d %d %d ", &octet1, &octet2, &octet3,
&octet4);
/*
      fprintf(outputfile,"ipaddress %d.%d.%d.%d count
%d\n",octet1,octet2,octet3,octet4,counter);
*/

      datafile2 =fopen(inputfile2,"r");
      if(datafile2==NULL) {
                  printf ("Can't open datafile2");
      return 1;
      }

      while(fgets(record2,400,datafile2)!=NULL) {
            sscanf(record2," %d %d %d %d ", &octet21, &octet22,
&octet23, &octet24);

            if ((octet1==10) && (octet21==10)){
                  counter ++;
                  fprintf(outputfile,"class Z PossibleReservedIP
%d.X.X.X count %d\n", octet1,counter);
                  counter=0;
            }
```

```
            if ((octet1==127) && (octet21==127)){
                  counter ++;
                  fprintf(outputfile,"class Z PossibleReservedIP
%d.%d.%d.%d count %d\n", octet1,octet2,octet3,octet4,counter);
                  counter=0;
            }


            if ((octet1==192) && (octet21==192) && (octet2==168) &&
(octet22==168)){
                  counter ++;
                  fprintf(outputfile,"class Z ReservedIP %d.%d.%d.X
count %d\n", octet1,octet2,octet3,counter);
                  counter=0;
            }


            if((octet1 >=1) && (octet1 <=126)){
                  class='A';
                  if (octet1 == octet21){
                        counter ++;
                  }
/*
                  fprintf(outputfile,"class %c ipaddress %d.%d.%d.%d
count %d\n", class,octet1,octet2,octet3,octet4,counter);
*/

            }



            if ((octet1 >=128) && (octet1 <=191)){
                  class='B';

                  if ((octet1 == octet21) && (octet2 ==octet22)){
                        counter ++;
                  }
/*
                  fprintf(outputfile,"class %c ipaddress %d.%d.%d.%d
count %d\n", class,octet1,octet2,octet3,octet4,counter);
*/

            }



            if ((octet1 >=192) && (octet1 <=224)){
                  class='C';

                  if ((octet1 == octet21) && (octet2 ==octet22) &&
(octet3 == octet23)){
                        counter ++;
                  }

            }

      }
```

```
if (counter==0){
      continue;
}

if (class=='A'){
      fprintf(outputfile,"class %c ipaddress %d.X.X.X count
%d\n",class,octet1,counter);
}

if (class=='B'){
      fprintf(outputfile,"class %c ipaddress %d.%d.X.X count
%d\n",class,octet1,octet2,counter);
}

if (class=='C'){
      fprintf(outputfile,"class %c ipaddress %d.%d.%d.X count
%d\n",class,octet1,octet2,octet3,counter);
}

counter=0;
fclose(datafile2);
}

fclose(datafile);
fclose(outputfile);
printf("Done.");
}
```