SANS GIAC PRACTICAL

GIAC Intrusion Detection In Depth
Practical Assignment for Aloha II SANS

Prepared by: Bill Phillips

Version: 2.8

Date: May 1 - 8

INDEX

Assignment 1

5 – Network detects

Introduction

All of the following detects were obtained from a large .EDU network. I am a member of the Security Incident Response Team there and face the same trade off that many network security analysts face, namely maintaining security while still providing for usability. In an effort to keep that balance there are some basic countermeasures that have been put in place in our network that I will reference throughout this document. Below is a basic explanation of what they are and how they function.

1. Router Access Control Lists (ACL's) –Filter traffic based on a rule set. Access lists can accomplish many tasks when it comes to security. They are very powerful and yet can be fine tuned to provide a highly granular filter. We utilize a small subset of their functionality to allow or disallow a variety of protocols/ports/services. I have taken a small portion of an access list that is applied to the interfaces coming into our network from the "outside" to offer a better explanation of their function.

```
deny ip 10.0.0.0 0.255.255.255 any
deny ip MY_NET.0.0 0.255.255.255 any
deny ip MY_NET.0.0 0.0.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip MY_NET.0.0 0.0.255.255 any
permit udp MY_NET.16.144 0.0.0.15 any eq netbios-dgm
permit tcp MY_NET.16.144 0.0.0.15 any eq 139
permit udp MY_NET.0.0 0.0.15.255 any eq netbios-ns
permit udp MY_NET.0.0 0.0.15.255 any eq netbios-dgm
```

here is the basic pattern for the access list and a link to follow to a site for securing Cisco routers

1	2	3	4	5	6
Access-list 100-199	permit | Deny	protocol	<source IP address><mask> | any	dest IP address><mask> | any	Protocol specifics

http://secinf.net/info/fw/cisco/cisco.html

2. Cisco Secure IDS – There are two IDS sensors deployed on our network. They collect data and report back to a Management system. The IDS can be thought of as a virus detection program, only on a network level. As a virus detection program has a set of signatures it is looking for in the software that it is scanning, the IDS system has a set of signatures it is attempting to match against traffic that it is monitoring. Once it "sees" a signature it performs a previously decided event . The Cisco IDS actually has the capability of modifying the ACL on the router in front of it to prevent the attacker from gaining access to the network for a set amount of time. Unfortunately this happens quite frequently and as a result the log files become quite large and have to be reduced in size for archiving. The archived logs will be in the following format:

Record type, Record ID, GMT Datestamp, GMT timestamp, Local Datestamp, Local Timestamp, Application ID, Host ID, Organization ID, Source Direction, Destination Direction, Alarm lvl, SigID, Protocol, Source IP, Dest IP, Source port, Dest Port, Router IP

I have included a rough diagram of the sensor locations and our network at the border, please see attachment C.

3. Some of the Windows systems have personal firewalls installed. "A personal firewall is a software application used to protect a single internet-connected computer from intruders". We are currently working to obtain a site license to allow our users free access to personal firewall software. This becomes increasingly important as the number of malicious attacks that we see continues to rise. These vary in manufacturer and include; Black Ice, Zone Alarm and Tiny Firewall (my personal favorite), though there are others that I have yet to test. Many of these are free for personal use, like tiny =).
http://whatis.techtarget.com/definition/0,289893,sid9_gci331881,00.html

4. TCP Wrappers- Is a Unix based method for controlling access to your computer based on the name or IP address of the remote host. They can be used to prevent or log access to the system.

   "TCP Wrappers acts much like a soldier at a checkpoint, verifying a host's clearance prior to entry. Simply put TCP Wrappers capitalizes on the client/server relationship necessary for most TCP/IP applications. TCP Wrappers inserts itself into the middle of the relationship and acts as the server until the client/host is authenticated. TCP Wrappers utilizes its access control feature to authenticate hosts. TCP Wrappers does all of this with no overhead to the system and best of all it is free."
   http://www.sans.org/infosecFAQ/unix/TCP_wrappers2.htm
5. Lastly some formatting information:

   - The 1st 2 octets of our IP address block have been changed to MY_NET. Thus 10.10.128.255 becomes MY_NET.128.255
   - Any of the routers named in the following detects have been changed to CISRTR.

   I hope that the information above will allow for a better understanding of the following detects.

Detect – 1 - FTP Scanning – Possible WUFTP exploit

Source #1
Router Access Lists (ACL's)

```
May  1 03:18:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425283: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(47933) -> XXX.XXX.32.57(21), 1 packet
May  1 03:18:52 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425284: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(47934) -> XXX.XXX.32.57(21), 1 packet
May  1 03:18:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425285: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(47936) -> XXX.XXX.32.57(21), 1 packet
```

- Significant break - appears to be an 8hr respite

```
May  1 11:08:05 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425658: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3162) -> XXX.XXX.189.42(21), 1 packet
May  1 11:08:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425664: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3018) -> XXX.XXX.143.59(21), 1 packet
May  1 11:08:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425665: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3321) -> XXX.XXX.126.100(21), 1 packet
May  1 11:08:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425666: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3330) -> XXX.XXX.181.50(21), 1 packet
May  1 11:08:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425667: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3244) -> XXX.XXX.189.82(21), 1 packet
(CUT) ---------------
May  1 11:11:11 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425841: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4980) -> XXX.XXX.245.44(21), 1 packet
May  1 11:11:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425842: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4997) -> XXX.XXX.183.4(21), 1 packet
May  1 11:11:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425843: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4902) -> XXX.XXX.132.109(21), 1 packet
May  1 11:11:14 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425844: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(1037) -> XXX.XXX.245.63(21), 1 packet
May  1 11:11:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425845: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(1134) -> XXX.XXX.93.182(21), 1 packet
May  1 11:11:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425846: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(1117) -> XXX.XXX.93.170(21), 1 packet
(list has been truncated to those shown above see attachment A for the full log)
--
```

Source #2

Cisco Secure IDS

Format: Record type, Record ID, GMT Datestamp, GMT Timestamp, Local Datestamp, Local Timestamp, Application ID, Host ID, Organization ID, Source Direction, Destination Direction, Alarm Level, Sig ID, SubSigID, Protocol, Source IP, Destination IP, Source Port, Destination Port, Router IP

A.

```
4,1009722,2001/05/01,17:51:55,2001/05/01,10:51:55,10008,HST_ID,ORG_ID,OUT,IN,5,3030,0,TCP/IP,200.191.
142.217,MY_NET.55.195,4171,21,0.0.0.0
```

B.

Date	Sensor	Signature	Sub Sig	Description	Severity	Address	Command
2001-05-01 03:16:25	1	3040	0	TCP Packet, No Flags	5	200.191.142.217	EXEC ShunHost 200.191.142.217 15
2001-05-01 03:16:25	1	3041	0	TCP Packet, SYN & FIN Only	5	200.191.142.217	EXEC ShunHost 200.191.142.217 15

Source #3
TCP Wrappers

```
rsh dns3 'grep 200.191.142.217 /var/log/tcp_wrappers.log
/var/log/tcp_wrappers.log:May  1 10:59:02 dns3.MY_NET ftpd[20907]: twist root@200191142217-dial-user-
UOL.acessonet.com.br to /usr/bin/mailx -s "denied ftpd attempt from 200191142217-dial-user-
UOL.acessonet.com.br [200.191.142.217] user root" staff
rsh dns4 'grep 200.191.142.217 /var/log/tcp_wrappers.log
/var/log/tcp_wrappers.log:May  1 10:59:22 dns4.MY_NET ftpd[20621]: twist root@200191142217-dial-user-
UOL.acessonet.com.br to /usr/bin/mailx -s "denied ftpd attempt from 200191142217-dial-user-
UOL.acessonet.com.br [200.191.142.217] user root" staff
rsh dns5 'grep 200.191.142.217 /var/log/tcp_wrappers.log
/var/log/tcp_wrappers.log:May  1 10:59:39 dns5.MY_NET ftpd[20119]: twist 200191142217-dial-user-
UOL.acessonet.com.br to /usr/bin/mailx -s "denied ftpd attempt from 200191142217-dial-user-
UOL.acessonet.com.br [200.191.142.217] user unknown" staff

mail generated by wrappers:
May  1 10:59:02 dns3MY_NETWORK ftpd[20907]: denied ftpd attempt from 200191142217-dial-user-
UOL.acessonet.com.br [200.191.142.217] user root
```

```
May  1 10:59:22 dns4MY_NETWORK ftpd[20621]: denied ftpd attempt from 200191142217-dial-user-
UOL.acessonet.com.br [200.191.142.217] user root
May  1 10:59:39 dns5MY_NETWORK ftpd[20119]: denied ftpd attempt from 200191142217-dial-user-
UOL.acessonet.com.br [200.191.142.217] user unknown
```

Source of Trace: This detect was gathered from a large .EDU network.

Detect Generated by:
TCP Wrappers, Router ACL's and Cisco IDS

Probability the Source Address was Spoofed:
Unlikely – The exploit requires the completion of the TCP 3-way handshake. (SYN) → - ←(SYN ACK) - (ACK) →. If the address of the attacker were spoofed, the SYN ACK that resulted would have been returned to the spoofed address (not to the attacker). The machine that received the SYN ACK would have been confused, for it had not initiated a connection. This machine in turn would have replied with a RST closing the connection (and not returning any information), not much use to the attacker. It is apparent from the traces below that the attacker was attempting to find machines that were running the FTP service. Additionally we can see from the ACL's that the attacker was in the process of scanning our address space, most likely on a reconnaissance mission. The last hint we have that the address was indeed the address of the attacker is the attempted logins to our three primary DNS servers from the same address of the scans.

Description of the Attack: This attack appears to have been two separate actions, scanning for hosts that are running an FTP server (more than likely looking for WUFTP) followed by the attempt to exploit a vulnerability. We see the scans entering our address space at 03:18:51 as shown in source 1, this corresponds to the time that the Cisco IDS fires and installs a router block for the address as a result of the scanning, source 2B. The 1st three timestamps from the ACL violations show that the attacker was still attempting reconnaissance. The scanning stops at 03:18:54, we could speculate as to why; possibly the attacker realized he/she was being shunned and went on to scan another address space, time to go to work – who knows, all we have in our data is the abrupt stop.

Success! score one for our team - Right? Nope. When the attacker begins again we see the attempt to login to the three main domain name servers at 10:59:02, which run WUFTP. Who fired that shot! Where did that information come from? It would appear that this attacker has already done some reconnaissance of our network. TCP Wrappers deny access to all three systems as seen in source 3. There have been many exploits for nearly all versions of Washington Universities FTP Server**.** The vulnerabilities vary depending on the version of WU FTPD the victim is running. See; CVE-1999-0075, and more see http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wuftpd.

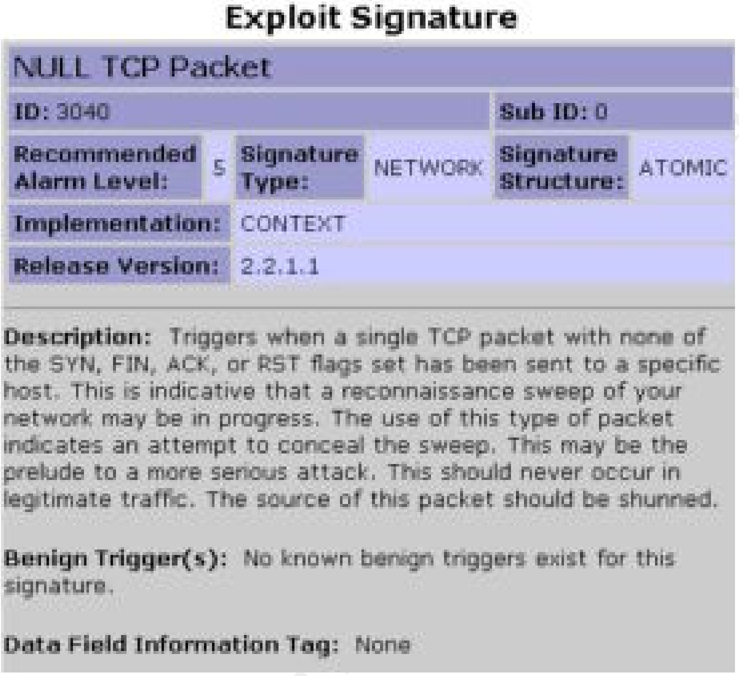
The attacker again begins to scan our address space at 11:08:05, source 1, and is shunned again by the Cisco IDS, source 2A. In the balance of the scans we can tell that the attacker was running an automated script, to walk our address range, by examining the time elapsed between each attempt. The script was attempting to elicit a response from any FTP server on our network by sending stimulus to port 21, source 2A.

Attack Mechanism: There are actually 2 attacks occurring in this detect, scanning and the attempting to exploit the vulnerable service. Attackers often look for vulnerable services by using port sweep programs that connect to several ports. Many network service daemons respond to a connection with a text banner describing their program name and version number. Attackers can use these responses to discover vulnerabilities. The existence of a "listener" on a port can also be useful information that an intruder can use to plan future attacks. It is likely that the attacker used an automated scanning tool. NMAP is a likely candidate as it provides for OS fingerprinting using SYN FIN and null scans as we saw in source 2B. It is unknown, which vulnerability the attacker attempted to exploit but numerous scripts are available from a variety of sources. http://www.antionline.com/cgi-bin/anticode/anticode.pl?dir=ftpd-exploits

Correlation:

- The Cisco IDS confirms the scanning and logs the attacker twice, shunning both times as seen in 2 A and B.
- We have the Router logs for the ACL violations committed by the attacking IP address.
- TCP wrappers denied attempted logins to the FTP server from the attacking IP address.

Additionally here are the descriptions of the alarms that the IDS triggered on. (Exact signatures are not available from Cisco)



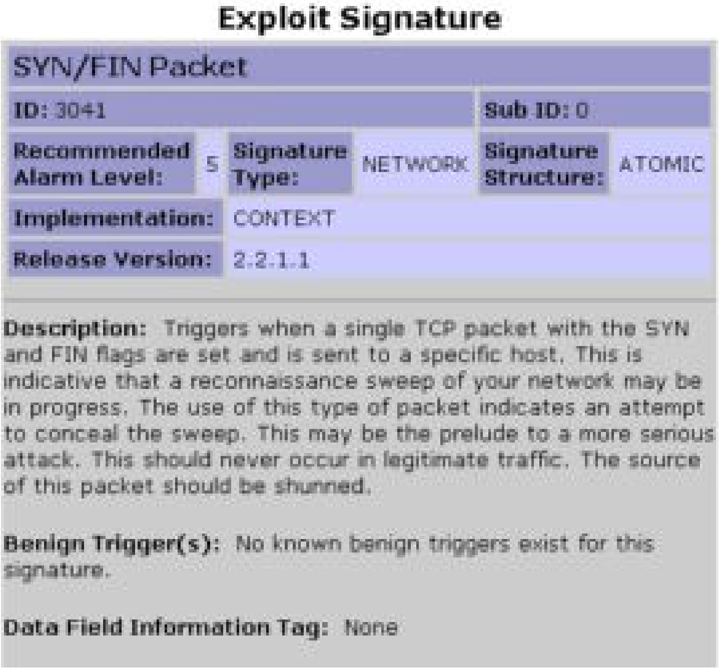
Exploit Signature

NULL TCP Packet					
ID: 3040				**Sub ID:** 0	
Recommended Alarm Level:	5	**Signature Type:**	NETWORK	**Signature Structure:**	ATOMIC
Implementation:	CONTEXT				
Release Version:	2.2.1.1				

Description: Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host. This is indicative that a reconnaissance sweep of your network may be in progress. The use of this type of packet indicates an attempt to conceal the sweep. This may be the prelude to a more serious attack. This should never occur in legitimate traffic. The source of this packet should be shunned.

Benign Trigger(s): No known benign triggers exist for this signature.

Data Field Information Tag: None



Exploit Signature

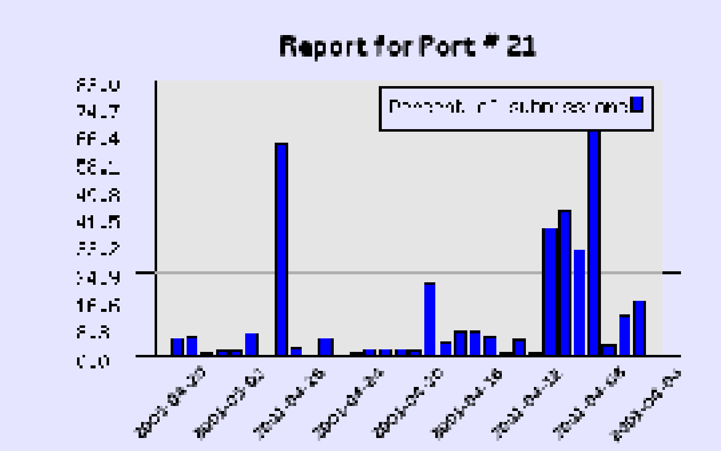
SYN/FIN Packet					
ID: 3041				**Sub ID:** 0	
Recommended Alarm Level:	5	**Signature Type:**	NETWORK	**Signature Structure:**	ATOMIC
Implementation:	CONTEXT				
Release Version:	2.2.1.1				

Description: Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host. This is indicative that a reconnaissance sweep of your network may be in progress. The use of this type of packet indicates an attempt to conceal the sweep. This may be the prelude to a more serious attack. This should never occur in legitimate traffic. The source of this packet should be shunned.

Benign Trigger(s): No known benign triggers exist for this signature.

Data Field Information Tag: None

This is a very common scan, no doubt due in large part to the wide spread use and consequent wide spread vulnerability of WUFTP. Port 21 is Consistently in the top 5 most scanned ports on the Internet.



http://www.dshield.org/

Evidence of Active Targeting: Yes, the attacker is looking for a specific service. The attacker has performed scans looking for systems listening on port 21 FTP. Once those systems have been mapped then the attacker comes back and runs the exploit code against the vulnerable systems depending on the version of FTP they were running. This is supported by the TCP wrappers logs which documents the attempted login of the attacker, source 3.

Severity:
Criticality: 5 the three hosts that the intruder attempted to compromise are the primary DNS servers.
Lethality: 5 the majority of the scripts provide the attacker with a root shell.
System Countermeasures: 5 the servers are well maintained by a knowledgeable admin who is very security conscious. They are regularly patched and are running the patched versions of WUFTP, which is wrapped using tcp wrappers. The systems also have COPS installed.
Network Countermeasures: 4 the IDS system performed its function during scan attempts and shunned the attacker. It would have been nice to be able to see a packet capture of the event so we could determine the exact exploit attempted. Additionally the attacker had obtained the IP addresses of our DNS servers including the primary and both secondary, not too difficult really but rather surprising during the course of the detect. There is no firewall in place for our network.

(System Criticality + Lethality of Attack) – (System Countermeasures + Network Countermeasures) = Severity
(5 + 5) – (5 + 4) = 1

Defensive Recommendations:
The current defenses functioned well; the Cisco IDS detected the scanning and installed a router block to prevent the attacker from gathering further information. TCP wrappers prevented the exploit of the vulnerable FTP service. Install an additional IDS that captures traffic in a TCP Dump like format (i.e. SNORT) and stores it for later analysis. This would provide for a better understanding of the true attacks and help to eliminate the guesswork and false positives that occur with the Cisco IDS.

Question:

NMAP is used:

A. By the Hacking community to directly exploit vulnerabilities in Washington University's FTP server
B. As a tool to perform Zone Transfers
C. By the Security Community to remove the vulnerabilities in Washington University's FTP server
D. As a tool to create GUI FTP maps
E. By both the Security and Hacking communities.

>E<

Detect – 2 – ICMP Redirect

Source 1

```
[**] IDS135/icmp-redirect_host [**]
05/05-04:10:55.317265 0:50:B:A8:60:A0 -> 0:4:28:64:41:64 type:0x800 len:0x52
203.208.148.142 -> MY_NET.188.67 ICMP TTL:241 TOS:0xC0 ID:38189 IpLen:20 DgmLen:68
Type:5  Code:1  REDIRECT
0x0000: 00 04 28 64 41 64 00 50 0B A8 60 A0 08 00 45 C0  ..(dAd.P..`...E.
0x0010: 00 44 95 2D 00 00 F1 01 80 A1 CB D0 94 8E XX XX  .D.-............
0x0020: XX XX 05 01 4D E4 CA 3D F3 57 45 00 00 28 D1 DC  .C..M..=.WE..(..
0x0030: 00 00 6F 06 69 93 XX XX XX XX CA 3D F3 57 18 CA  ..o.i....C.=.W..
```

```
0x0040: 0C 35 00 00 00 00 01 20 12 E3 50 14 00 00 66 6E  .5..... ..P...fn
0x0050: 00 00                                            ..

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

Source of Trace: This detect was gathered from a large .EDU network.
Detect Generated by: Snort Version 1.7 watching a span port of the universities main trunks. Generated by:
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS135/icmp-redirect_host"; itype: 5; icode: 1;)

Probability the Source Address was spoofed: I expected the address to be spoofed, but it did not appear to be. A trace route back to the alleged attackers IP address yields a hop count of 13 implying that the TTL of 241 was accurate. The fact that the hop counts indicated that the address might be correct made me curious. I ran NMAP against the address. NMAP returned: Remote operating system guess: Linux 2.1.122 - 2.2.16. However it still is inconclusive – the attacker could have spoofed the address of another system on his/her network, if so the packet was well crafted the only sign of crafting is the C0 for TOS in the IP header.

```
Starting nmap V. 2.54BETA7 ( www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on  (203.208.148.142):
(The 1523 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
79/tcp     open        finger
110/tcp    open        pop-3
113/tcp    open        auth
389/tcp    filtered    ldap
522/tcp    filtered    ulp
587/tcp    open        submission
1503/tcp   filtered    imtc-mcs
```

```
3128/tcp   open       squid-http
8080/tcp   open       http-proxy

Remote operating system guess: Linux 2.1.122 - 2.2.16
Nmap run completed -- 1 IP address (1 host up) scanned in 38 seconds
```

Description of the Attack: CVE-1999-0265

ICMP redirects may be used to change the routing table on a remote host. This is done by sending an ICMP datagram of type 5 code 1 that tells the remote host machine to use a different router to contact a specific host. The attacker may attempt to insert their address into the routing table to allow them to capture packets. To accomplish this, "the attacker must spoof the source address of the ICMP packet so that it appears to come from the victim's normal router. Also, the attacker must pick a destination that is within the same LAN as the victim machine." (Northcutt 254)

<table>
<tr><td>Type (5)</td><td>Code (0-3)</td><td>Checksum</td></tr>
<tr><td colspan="3">Router IP address that should be used</td></tr>
<tr><td colspan="3">IP Header (including options) + first 8 bytes of the Original IP datagram</td></tr>
</table>

code	Description
0	Redirect for network
1	Redirect for host
2	Redirect for type-of-service and network
3	Redirect for type-of-service and host

(Stevens 122)

The fact that this packet shows almost no sign of crafting is confusing; in an effort to try and understand what the intention of the alleged attacker was we look to the packet

```
05 ------------------------------------------------ 8 bit message type
01 ------------------------------------------------ 8 bit message code
4D E4 --------------------------------------------- 16 bit checksum
CA 3D F3 57 = 202.61.243.87 ----------------------- Router IP address that should be used

                              45 00 00 28 D1 DC |
00 00 6F 06 69 93 XX XX XX XX CA 3D F3 57 18 CA |-- IP Header (including options) + first 8 bytes
0C 35 00 00 00 00 01 20 12 E3 50 14 00 00 66 6E |   of the Original IP datagram which shows the source
00 00                                               address of the host machine that initiated this packet
```

```
05 01 4D E4 CA 3D F3 57 45 00 00 28 D1 DC
00 00 6F 06 69 93 XX XX XX XX CA 3D F3 57 18 CA
0C 35 00 00 00 00 01 20 12 E3 50 14 00 00 66 6E
00 00
```

In bold above we see the attempt of this packet is to get the host to use CA 3D F3 57 (202.61.243.87) as the new router. Using the ping and traceroute utilities in an attempt to try and determine if the destination exists we receive a host unreachable from the last router, somewhere in Australia.

```
MY_NET  0 ms  0 ms  0 ms
MY_NET  1 ms  1 ms  1 ms
 CLOSER_NET  23 ms  23 ms  22 ms
 4  den-core-02.inet.qwest.net (205.171.16.137)  22 ms  22 ms  22 ms
 5  sea-core-01.inet.qwest.net (205.171.5.27)  58 ms  58 ms  58 ms
 6  208.173.50.1 (208.173.50.1)  59 ms  58 ms  59 ms
 7  acr2-loopback.Seattlesel.cw.net (208.172.82.62)  59 ms  59 ms  59 ms
 8  acr2-loopback.SanFranciscosfd.cw.net (206.24.210.62)  115 ms  74 ms  74 ms
 9  optus-networks.SanFranciscosfd.cw.net (206.24.209.206)  75 ms  74 ms  74 ms
10  POS11-1-0.rr1.optus.net.au (192.65.89.229)  226 ms  226 ms  226 ms
11  GigEth3-0.sg1.optus.net.au (202.139.190.1)  226 ms  226 ms  226 ms
12  POS2-2.mg2.optus.net.au (202.139.124.142)  240 ms  240 ms  240 ms
```

```
13  GigEth12-0-0.mb1.optus.net.au (202.139.188.132)  240 ms  240 ms  240 ms
14  Paradox2.mb1.optus.net.au (202.139.134.74)  245 ms  243 ms  244 ms
15  eth0.bdr0.mel.paradox.net.au (202.61.240.50)  245 ms  246 ms  245 ms
16  203.208.148.142 (203.208.148.142)  771 ms
18  * * *
19  * *^C *
```

The fact that host is unreachable would seem to fit with our scenario that the attempt here was to change the route to a particular host such that the routing table would send packets for that host to a non-existent router. It is equally as likely that the destination network does not permit ICMP traffic to enter their network. Additionally the "destination address to be diverted via the new router" is the same address as the new router address as shown in the second bold hex. This corresponds to the first 20 bytes of the original IP header that ICMP included in the redirect message. So what is going on here? It would appear that there is indeed a configuration or hardware problem somewhere along the way. The problem is probably in 202.61.243.87.

Had this been an actual DOS attack there are several tools that would have aided in the execution of this alleged attack that require mention:
One developed by Yuri Volobuev in September 1997 available at http://www.insecure.org/sploits_all.html . And another developed more recently by Delmore called Winfreez, developed Mar 1999 available at http://www.attrition.org/security/denial/w/win-icmp.dos.html . Neither of these would fit the pattern we have seen in the detect above.

Attack Mechanism: The packet that was captured does not meet the requirements as laid out in "*Intrusion Signatures and Analysis*":

- ICMP Host redirect messages must originate from the normal router that redirected host would use- the detect does not
- The new router specified by the redirect must be on the same LAN as the victims machine- the router in the detect, is not.

(Northcutt 254)

Correlation: I performed a search for the offending address in the MySQL database we use as a back-end for the Cisco IDS. I found that there were no previous exploits or scans recorded by the CISCO IDS for this address. The CISCO IDS default alarm level for SIG 2003 (ICMP redirect) is 0, meaning that it does not alarm or log the signature. This has been changed in our configuration, which in the future will provide better correlation data.

Evidence of Active Targeting: Yes – There is no question that the packet was directed at the MY_NET host. Whether or not it was an attempted DOS.

Severity:
Criticality: 1 the system is a user node in our network with no critical information
Lethality: 4 if successful the targeted sytem will hang, crash or be unreachable.
System countermeasures: 1 the scans that I performed indicated that no firewall was present
Network countermeasures: 1 I was not aware that we allowed ICMP redirects into our network until this detect. As stated above the IDS we have in place did not alert on this signature. Had I not been running Snort, which I had temporarily installed in an attempt to gather some detects this would never have been noticed. There is no firewall in place for our network.

(System Criticality + Lethality of Attack) – (System Countermeasures + Network Countermeasures) = Severity
(1 + 4) – (1 + 1) = 3
Defensive Recommendations: Turn off ICMP redirects in all routers. enable > config t > Int eth0 > no ip redirect

Question: ICMP redirects

A. Are not routed
B. Prevent a sniffer from being used
C. Serve no purpose
D. Can be used to perform a DOS against a host
E. Help provide security for the network

>D<

Detect – 3 STATD Buffer Oveflow

Source #1
Router Access Lists (ACL's)

rsh SYSTEM grep 211.195.36.62 /var/log/syslog_info:

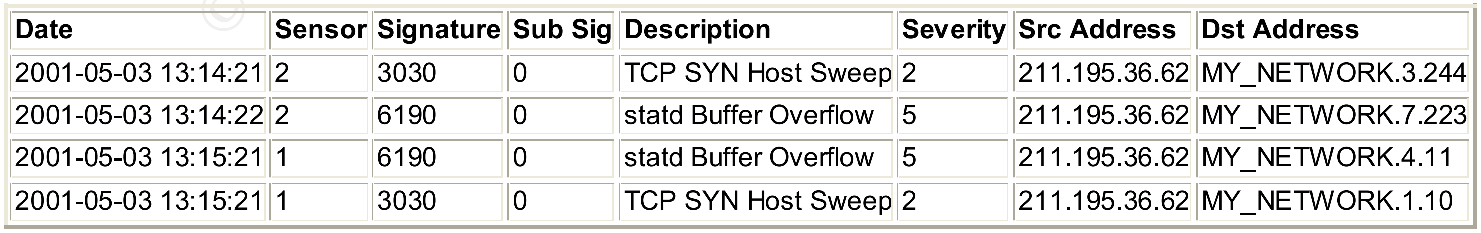
```
May  3 13:16:40 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432498: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1138) ->
MY_NETWORK.35.115(111), 1 packet
May  3 13:16:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432504: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2146) ->
MY_NETWORK.39.93(111), 1 packet
May  3 13:16:44 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432505: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3149) ->
MY_NETWORK.43.73(111), 1 packet
May  3 13:16:46 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432506: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3153) ->
MY_NETWORK.43.77(111), 1 packet
May  3 13:16:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432511: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4034) ->
MY_NETWORK.46.191(111), 1 packet
May  3 13:16:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432512: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1184) ->
MY_NETWORK.51.36(111), 1 packet
May  3 13:16:55 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432513: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2195) ->
MY_NETWORK.55.17(111), 1 packet
May  3 13:16:58 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432514: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3201) ->
MY_NETWORK.59.0(111), 1 packet
May  3 13:17:01 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432515: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4202) ->
MY_NETWORK.62.234(111), 1 packet
May  3 13:17:04 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432516: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1170) ->
MY_NETWORK.66.152(111), 1 packet
May  3 13:17:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432517: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2241) ->
MY_NETWORK.70.193(111), 1 packet
May  3 13:17:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432518: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3244) ->
MY_NETWORK.74.173(111), 1 packet
```

```
May  3 13:17:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432519: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4247) ->
MY_NETWORK.78.154(111), 1 packet
(CUT) ---------------
May  3 13:41:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432651: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 2 packets
May  3 14:09:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432670: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1134) ->
MY_NETWORK.4.111(111), 1 packet
May  3 14:28:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432681: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 1 packet
May  3 15:15:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433334: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1078) ->
MY_NETWORK.4.55(111), 1 packet
May  3 15:15:17 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433335: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1067) ->
MY_NETWORK.4.44(111), 1 packet
May  3 15:20:32 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433339: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1067) ->
MY_NETWORK.4.44(111), 4 packets
May  3 15:25:33 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433344: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1067) ->
MY_NETWORK.4.44(111), 3 packets
(list has been truncated to those shown above see attachment B for the full log)
--
```

Source #2

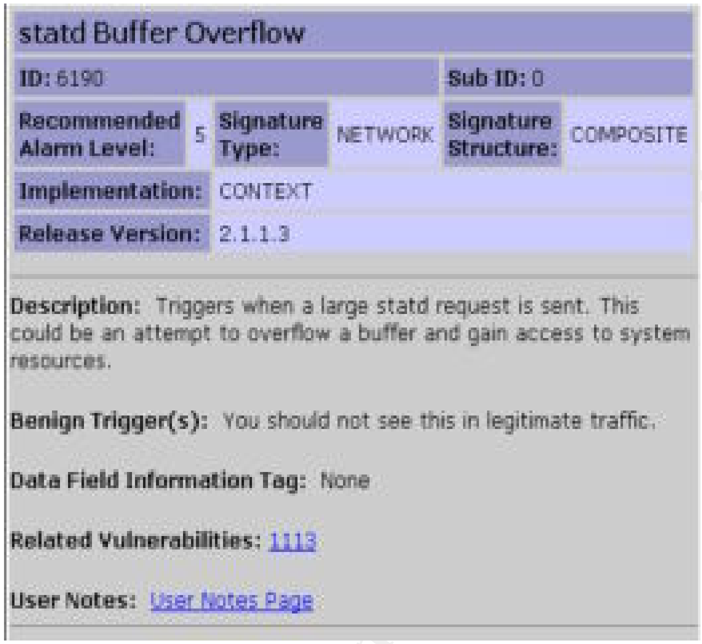
Cisco Secure IDS

A.



Date	Sensor	Signature	Sub Sig	Description	Severity	Src Address	Dst Address
2001-05-03 13:14:21	2	3030	0	TCP SYN Host Sweep	2	211.195.36.62	MY_NETWORK.3.244
2001-05-03 13:14:22	2	6190	0	statd Buffer Overflow	5	211.195.36.62	MY_NETWORK.7.223
2001-05-03 13:15:21	1	6190	0	statd Buffer Overflow	5	211.195.36.62	MY_NETWORK.4.11
2001-05-03 13:15:21	1	3030	0	TCP SYN Host Sweep	2	211.195.36.62	MY_NETWORK.1.10

B.



statd Buffer Overflow

ID: 6190				**Sub ID:** 0	
Recommended Alarm Level:	5	**Signature Type:**	NETWORK	**Signature Structure:**	COMPOSITE
Implementation:	CONTEXT				
Release Version:	2.1.1.3				

Description: Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.

Benign Trigger(s): You should not see this in legitimate traffic.

Data Field Information Tag: None

Related Vulnerabilities: 1113

User Notes: User Notes Page

C

Netranger log:

```
log.200105031308:
4,1071888,2001/05/03,20:15:13,2001/05/03,13:15:13,10008,1,100,OUT,IN,2,3030,0,TCP/IP,211.195.36.62,MY_NETWORK.1.10,42
39,111,0.0.0.0,
log.200105031308:
4,1071893,2001/05/03,20:15:16,2001/05/03,13:15:16,10008,1,100,OUT,IN,5,6190,0,TCP/IP,211.195.36.62,MY_NETWORK.4.11,92
3,32777,0.0.0.0
log.200105031308:
3,313,2001/05/03,20:15:16,2001/05/03,13:15:16,10003,1,100,10008,1,100,EXEC ShunHost 211.195.36.62 15
log.200105031308:
```

```
3,338,2001/05/03,20:30:17,2001/05/03,13:30:17,10003,1,100,10003,1,100,EXEC UnshunHost 211.195.36.62
```

Source #3
TACACS+

```
tacacs.acct.log:Thu May  3 15:36:14 2001       192.80.43.42    ric     tty2    MY_NETWORK.128.46  stop    task_id=9547
start_time=988929374    timezone=UTC    service=shell   priv-lvl=15     cmd=access-list 138 deny ip host 211.195.36.62 any log
```

Source #4
TCP Wrappers

```
tcp_wrappers.log:May  3 13:15:25 dns4.MY_NETWORK rpcbind: refused connect from 211.195.36.62 to getport(status)
```

Source of Trace: This detect was gathered from a large .EDU network.

Detect Generated by: TCP Wrappers, Router ACL's,Cisco IDS and TACAS+ log

Probability the Source Address was Spoofed: Unlikely the attacker is using TCP and would require a connection to receive information from portmapper. Additionally the attempted exploit is launched from the same address.

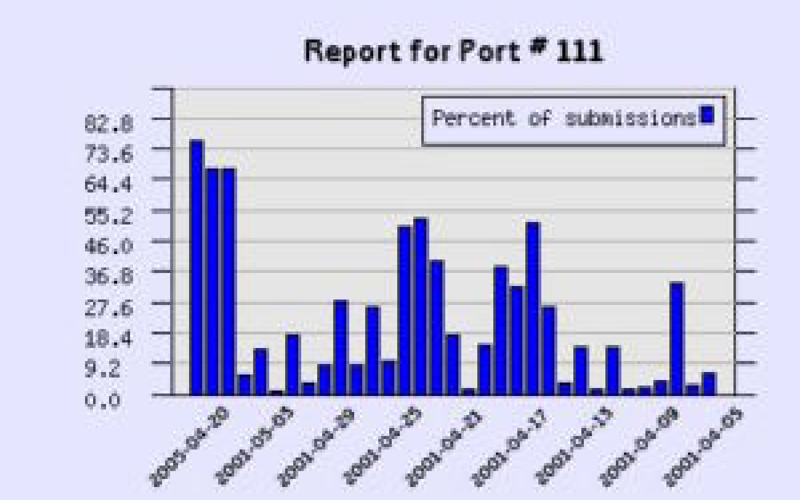
Description of the Attack:
CVE-1999-0018 - Buffer overflow in statd allows root privileges.

Due to insufficient bounds checking on input arguments which may be supplied by local users, as well as remote users, it is possible to overwrite the internal stack space (where a program stores information to be used during its execution) of the statd program while it is executing a specific rpc routine. By supplying a carefully designed input argument to the statd program, intruders may be able to force statd to execute arbitrary commands as the user running statd. In most instances, that user will be *root*. This vulnerability can be exploited by local users. It can also be exploited remotely without the intruder requiring a valid local account if statd is accessible via the network. http://www.wwdsi.com/cgi-bin/doc.pl?document=vulnerability/rpc_statd_access

Attack Mechanism:

The attack once again is in two distinguishable parts, scanning and then the attempted exploit. The attacker is querying the portmmaper, port 111, in an attempt to determine which port statd lives on- see Source 1. If the system responds to the rpcinfo request the attacker would get back a list of ports that the NFS services are bound to. The attacker would then attempts to exploit the vulnerable service he/she chose. In this case it happens to be the statd buffer overflow. There are a variety of scripts that take advantage of the exploit.
http://www.antionline.com/cgi-bin/anticode/anticode.pl

Correlation: . This is a common scan and well-known vulnerability and is listed with other rpc vulnerabilities at number three on the SANS top ten vulnerabilities. Nonetheless in the last 3 weeks we have had 4 systems, that were reported, that have been compromised exploiting the rpc.statd vulnerability. As seen below in the last month we have had over 1100 attempted buffer overflows relating to NFS. Once again we must take the IDS's word for it that there were attempted exploit attempts. The Cisco IDS does not currently capture the packet that triggers an alarm. In Cisco's defense however the next upgrade available in June of 2001 will provide for this necessity, and is reported to disclose their signature set and provide for custom signatures.



6194	0	631	5	sadmind Buffer Overflow
6190	0	553	5	statd Buffer Overflow

Evidence of Active Targeting:

There is no evidence of actively targeting one specific machine; there is blatant active targeting of the portmaper service and subsequently statd. Beyond the scanning we see two statd Buffer Overflow attempts to MY_NETWORK.7.223 and MY_NETWORK.3.244, see Source 2A and B.

Severity:

Criticality: 3 the two hosts that the intruder attempted to compromise are desktop nodes in our network. The attempts vary from the systems they target on a daily basis – core systems have been the focus of similar attacks before.
Lethality: 5 the exploit, if successful, provides the attacker with a root shell.
System Countermeasures: 2 on a whole across the University there are many systems that are out of the box installs that have no countermeasures in place at the host level. Also many of these systems are not regularly patched. The core systems are well protected.
Network Countermeasures: 3 the IDS system logged the scan attempts and shunned the attacker once the exploit was initiated. Was it in time to prevent success? - we cannot say. Again it would have been nice to be able to obtain a packet captures of the exploit. The IDS allowed the attacker to test for open portmapers on port 111. There is no firewall in place for our network.

(System Criticality + Lethality of Attack) – (System Countermeasures + Network Countermeasures) = Severity
(3 + 5) – (2 + 3) = 3

Defensive Recommendations: Install a Firewall on our commodity Internet links that prevents requests for NFS services from being allowed into the network. This would cut down on the success of scans looking for these services and also take some load off of the IDS. Install a packet capturing IDS to detect those hosts on the internal network that are scanning for the portmapper service. Verify that the systems are patched with the latest patches and that the NFS services are wrapped using TCP Wrappers.

Question:
tcp_wrappers.log:May 3 13:15:25 dns4.MY_NETWORK rpcbind: refused connect from 192.168.36.62 to getport(status)

The String above is a TCP wrappers log of

A. A failed attempt to bind to the printer port on a remote machine
B. A failed reset port status message
C. A failed rpcinfo –p command
D. An example of TCP Wrappers providing NFS information to the remote host

>C<

Detect – 4 Large ICMP Packets - Stacheldraht

Source #1

```
[**] IDS246/dos-large-icmp [**]
05/05-05:50:15.992134 0:50:B:A8:60:A0 -> 0:4:28:64:41:64 type:0x800 len:0x5EA
141.79.128.4 -> MY_NET.11.233 ICMP TTL:228 TOS:0x0 ID:45526 IpLen:20 DgmLen:1500 DF
Type:8  Code:0  ID:0   Seq:2  ECHO
0x0000: 00 04 28 64 41 64 00 50 0B A8 60 A0 08 00 45 00  ..(dAd.P..`...E.

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

Source #2

```
[**] IDS246/dos-large-icmp [**]
05/05-01:45:19.313117 0:50:B:A8:60:A0 -> 0:4:28:64:41:64 type:0x800 len:0x422
131.161.83.242 -> MY_NET.64.26 ICMP TTL:54 TOS:0x0 ID:20176 IpLen:20 DgmLen:1044
Type:0  Code:0  ID:6666  Seq:0  ECHO REPLY
0x0000: 00 04 28 64 41 64 00 50 0B A8 60 A0 08 00 45 00  ..(dAd.P..`...E.
0x0010: 04 14 4E D0 00 00 36 01 99 A7 83 A1 53 F2 XX XX  ..N...6.....S...
0x0020: 40 1A 00 00 9C A3 1A 0A 00 00 00 00 00 00 00 00  @...............
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 6B  ..............sk
0x0040: 69 6C 6C 7A 00 00 00 00 00 00 00 00 00 00 00 00  illz............
0x0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
0x0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
(CUT) ---------------
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS246/dos-large-icmp [**]
05/05-05:12:43.207854 0:50:B:A8:60:A0 -> 0:4:28:64:41:64 type:0x800 len:0x422
131.161.83.242 -> MY_NET.64.26 ICMP TTL:54 TOS:0x0 ID:25290 IpLen:20 DgmLen:1044
Type:0  Code:0  ID:6666  Seq:0  ECHO REPLY
0x0000: 00 04 28 64 41 64 00 50 0B A8 60 A0 08 00 45 00  ..(dAd.P..`...E.
0x0010: 04 14 62 CA 00 00 36 01 85 AD 83 A1 53 F2 XX XX  ..b...6.....S...
0x0020: 40 1A 00 00 9C A3 1A 0A 00 00 00 00 00 00 00 00  @...............
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 6B  ..............sk
0x0040: 69 6C 6C 7A 00 00 00 00 00 00 00 00 00 00 00 00  illz............
0x0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x00B0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
(CUT) ---------------
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS246/dos-large-icmp [**]
05/05-01:59:51.775871 0:50:B:A8:60:A0 -> 0:4:28:64:41:64 type:0x800 len:0x422
216.164.64.12 -> MY_NET.64.26 ICMP TTL:47 TOS:0x0 ID:15343 IpLen:20 DgmLen:1044
Type:0  Code:0  ID:6666  Seq:0  ECHO REPLY
0x0000: 00 04 28 64 41 64 00 50 0B A8 60 A0 08 00 45 00  ..(dAd.P..`...E.
0x0010: 04 14 3B EF 00 00 2F 01 72 6B D8 A4 40 0C XX XX  ..;.../.rk..@...
0x0020: 40 1A 00 00 9C A3 1A 0A 00 00 00 00 00 00 00 00  @...............
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 6B  ..............sk
0x0040: 69 6C 6C 7A 00 00 00 00 00 00 00 00 00 00 00 00  illz............
0x0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
0x0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
(CUT) ---------------
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS246/dos-large-icmp [**]
05/05-02:05:57.738645 0:50:B:A8:60:A0 -> 0:4:28:64:41:64 type:0x800 len:0x422
216.164.64.12 -> MY_NET.64.26 ICMP TTL:47 TOS:0x0 ID:15699 IpLen:20 DgmLen:1044
Type:0  Code:0  ID:6666  Seq:0  ECHO REPLY
0x0000: 00 04 28 64 41 64 00 50 0B A8 60 A0 08 00 45 00  ..(dAd.P..`...E.
0x0010: 04 14 3D 53 00 00 2F 01 71 07 D8 A4 40 0C XX XX  ..=S../.q...@...
0x0020: 40 1A 00 00 9C A3 1A 0A 00 00 00 00 00 00 00 00  @...............
0x0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 73 6B  ..............sk
0x0040: 69 6C 6C 7A 00 00 00 00 00 00 00 00 00 00 00 00  illz............
0x0050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
(CUT) ---------------
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source #3

```
[**] IDS246/dos-large-icmp [**]
05/05-02:23:08.250099 0:50:B:A8:60:A0 -> 0:4:28:64:41:64 type:0x800 len:0x59A
167.216.150.117 -> MY_NET.11.233 ICMP TTL:245 TOS:0x0 ID:30577 IpLen:20 DgmLen:1420 DF
Type:8  Code:0  ID:229   Seq:38019  ECHO
0x0000: 00 04 28 64 41 64 00 50 0B A8 60 A0 08 00 45 00  ..(dAd.P..`...E.
0x0010: 05 8C 77 71 40 00 F5 01 3E 04 A7 D8 96 75 XX XX  ..wq@...>....u..
0x0020: 0B E9 08 00 C3 79 00 E5 94 83 6D 61 69 6C 74 6F  .....y....mailto
0x0030: 3A 6F 70 73 40 64 69 67 69 73 6C 65 2E 63 6F 6D  :ops@digisle.com
0x0040: 20 66 6F 72 20 71 75 65 73 74 69 6F 6E 73 20 20   for questions
0x0050: 20 20 54 68 69 73 20 49 43 4D 50 20 45 43 48 4F    This ICMP ECHO
0x0060: 20 52 45 51 55 45 53 54 2F 52 45 50 4C 59 20 69   REQUEST/REPLY i
0x0070: 73 20 70 61 72 74 20 6F 66 20 74 68 65 20 72 65  s part of the re
0x0080: 61 6C 2D 74 69 6D 65 20 6E 65 74 77 6F 72 6B 20  al-time network
```

```
0x0090: 6D 6F 6E 69 74 6F 72 69 6E 67 70 65 72 66 6F 72  monitoringperfor
0x00A0: 6D 65 64 20 62 79 20 44 69 67 69 74 61 6C 20 49  med by Digital I
0x00B0: 73 6C 61 6E 64 20 49 6E 63 2E 20 20 49 74 20 69  sland Inc.  It i
0x00C0: 73 20 6E 6F 74 20 61 6E 20 61 74 74 61 63 6B 2E  s not an attack.
0x00D0: 20 20 49 66 20 79 6F 75 20 68 61 76 65 71 75 65    If you haveque
0x00E0: 73 74 69 6F 6E 73 20 70 6C 65 61 73 65 20 63 6F  stions please co
0x00F0: 6E 74 61 63 74 20 6F 70 73 40 64 69 67 69 73 6C  ntact ops@digisl
0x0100: 65 2E 63 6F 6D 00 00 00 00 00 00 00 00 00 00 00  e.com...........
0x0110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0x0120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
(CUT) ---------------
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source #4

Sig Id	Sig Sub Id	Sig Description	Src IP Address	Dst IP Address	Time
2151	1024	Large ICMP	131.161.83.242	MY_NET.64.26	2001-05-04 15:44:20
2151	1024	Large ICMP	216.125.196.12	MY_NET.64.26	2001-05-04 15:44:21
2151	1024	Large ICMP	24.157.236.160	MY_NET.64.26	2001-05-04 15:44:22
2151	1024	Large ICMP	163.51.63.101	MY_NET.64.26	2001-05-04 15:44:22
2151	81480	Large ICMP	216.74.151.137	MY_NET.171.132	2001-05-04 15:44:22
2151	1480	Large ICMP	12.42.232.138	MY_NET.163.68	2001-05-04 15:44:23
2151	1024	Large ICMP	209.69.145.112	MY_NET.64.26	2001-05-04 15:44:23
2151	81480	Large ICMP	24.185.178.1	MY_NET.141.188	2001-05-04 15:44:23
2151	1024	Large ICMP	216.164.64.12	MY_NET.64.26	2001-05-04 15:44:23
2151	1480	Large ICMP	12.42.231.154	MY_NET.163.68	2001-05-04 15:44:24
2151	1024	Large ICMP	131.161.83.242	MY_NET.64.26	2001-05-04 15:45:20
2151	81480	Large ICMP	18.30.2.64	MY_NET.135.222	2001-05-04 15:45:20

2151	1024	Large ICMP	216.125.196.12	MY_NET.64.26	2001-05-04 15:45:21
2151	1024	Large ICMP	163.51.63.101	MY_NET.64.26	2001-05-04 15:45:22
2151	81480	Large ICMP	216.74.151.137	MY_NET.171.132	2001-05-04 15:45:22
2151	1480	Large ICMP	64.124.124.162	MY_NET.163.68	2001-05-04 15:45:23
2151	1480	Large ICMP	24.177.33.118	MY_NET.185.51	2001-05-04 15:45:23
2151	1024	Large ICMP	216.164.64.12	MY_NET.64.26	2001-05-04 15:45:23

Source of Trace: This detect was gathered from a large .EDU network.

Detect Generated by: Cisco IDS and Snort Version 1.7 watching a span port of the universiyy's main trunks. Snort signature:
Alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS246/dos-large-icmp"; dsize: >800;)

Probability the Source Address was Spoofed: Nearly certain, "Spoofing ICMP and UDP Packets is a trivial exercise. Both protocols are connectionless and stateless" (Northcutt 135) Additionally the "skillz" string embedded in the packet and the non-changing ID of 6666 are very good indications that the packet has been crafted.

Description of the Attack: CAN-2000-0138- A system has a distributed denial of service (DDOS) attack master, agent, or zombie installed, such as (1) Trinoo, (2) Tribe Flood Network (TFN), (3) Tribe Flood Network 2000 (TFN2K), (4) stacheldraht, (5) mstream, or (6) shaft. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0138
MY_NET is currently getting hammered with these packets. It is as yet unclear what the attack is. It appears to be a Distributed Denial of service against a specific host. In fact it seems to be an effort to clog up the network on a massive scale. There may be several attacks happening simultaneously that are being blurred together.

MY_NET.64.26 is receiving what appears to be a smurf attack. On the order of 7000 ICMP echo replies daily, see source 4, and Attachment D for a small sample. We have receieved rougly 8 million of these packets since 4-23-01. These replies have no corresponding request coming from the MY_NET host. This would lead us to the conclusion that someone is Spoofing our

MY_NET.64.26 address and sending ICMP echo requests to an "amplifier" address, the broadcast address of a network or subnet. This address then replicates the packet to every system that is listening on its broadcast domain. In turn all of these hosts reply back to the address of the victim host with ICMP echo replies. This would be bad enough with normal ping packets; the packets we are seeing are 1500 bytes.

We are also seeing many thousands of packets leaving our network with a supposed local address of 195.238.0.13, which is nowhere in our IP address range. The majority of the packets are targeted to likely broadcast addresses all over the Internet. These packets are most likely ICMP echo requests with the spoofed address of the 195.238 host in Brussels. We are currently attempting to silence this host. These conditions could imply that the host on our network is infected with a Trojan of some kind. The packet craft seems to have a unique signature, Skillz embedded in the packet and the id of 6666, source 2, this may be the result of a script or a Trojan.

The closest attack to the current traffic we are seeing meets nearly all of the packets profiles, with the exception of the ICMP id of 6666, for Stacheldraht. Very likely that this is a variation. Ruleset for Stacheldraht signature from Vision-

```
ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS190/ddos-stacheldraht client-check"; itype: 0; icmp_id: 666; content: "skillz";)
```

To add to the confusion there are actual legitimate ICMP echo packets of this size. Some companies, like the one which announces its intention in source 3, perform network monitoring using large ICMP packets. Additionally it would seem that some versions of Macintosh computers generate large ICMP packets.

> "While doing research on Internet hacker activities, I saw probe packets coming to a Macintosh that I did not understand. I noticed the large ICMP datagrams that the Macintosh sent back that did not conform to Internet protocol standards. I wrote and used a special computer program to send similar probe datagrams to a section of the Georgia Tech network which connects to many types of computers. Only OS9 Macintoshes responded in any unusual way. I concluded this particular probe datagram was designed to detect OS9 Macintoshes.
> http://people.atl.mediaone.net/jacopeland/faq.html

Attack Mechanism: This would appear to be a Smurf attack or some variation of Stacheldraht. We will not be able to determine if a Trojan is in place until we find the system that is spoofing the 195.238 address.

- The attacker/Trojan spoofs the source address
- The attacker or trojan sends out numerous ICMP echo requests to addresses that are typically used for the broadcast address of a network/subnet. known as Amplifiers.

Correlation: When looking at the ICMP packets in source 2 there is a heavy signature that screams Stacheldraht. That information with the logs provided in attachment D and looking at the number of hosts hitting MY_NET.64.26 with echo-replies from all over the internet. and further by examining the volume of large ICMP packets it would be very likely that this is indeed some variant of the infamous DDOS tool.

Evidence of Active Targeting: It would appear from the logs, a small portion provided in attachment D, that there is evidence of active targeting, although it is difficult to discern through the rest of the "noise" of the ICMP traffic currently barraging our network.

Severity:

Criticality: 1 the two host that the intruder attempted to DOS is a desktop nodes in our network

Lethality: 4 the attack may disrupt use of the machine but does not provide access to the system or its files.

System Countermeasures: 1 Many systems on our network are out of the box installs or are not regularly patched. Also most systems do not have personal firewalls and are not behind a network firewall

Network Countermeasures: 2 the IDS logs the signature but is not currently blocking large ICMP packets. Additionally we allow Spoofed traffic to leave our network.

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

(1 + 4) – (1 + 2) = 2

Defensive Recommendations: Install ip-cahins/personal firewalls on the all systems. Keep all systems patched**.** Unfortunately there is no real defense, short of turning off ICMP on the network.

Question:

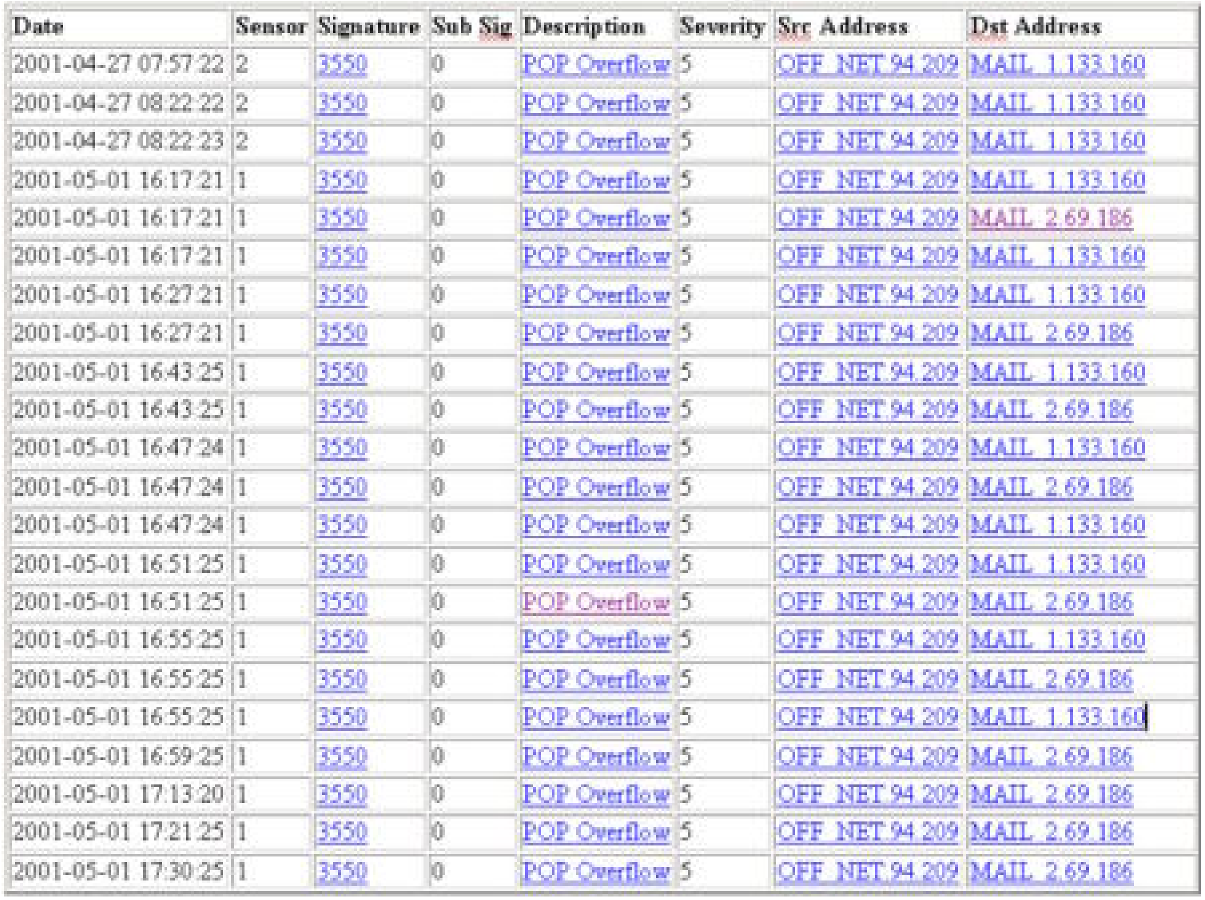
Stacheldraht:

A. Exploits an overflow condition in rcp.statd
B. Employs the use of the TCP 3 way hand shake
C. Makes use of the connectionless UDP protocal
D. Is a European Computer Security Consortium

>C<

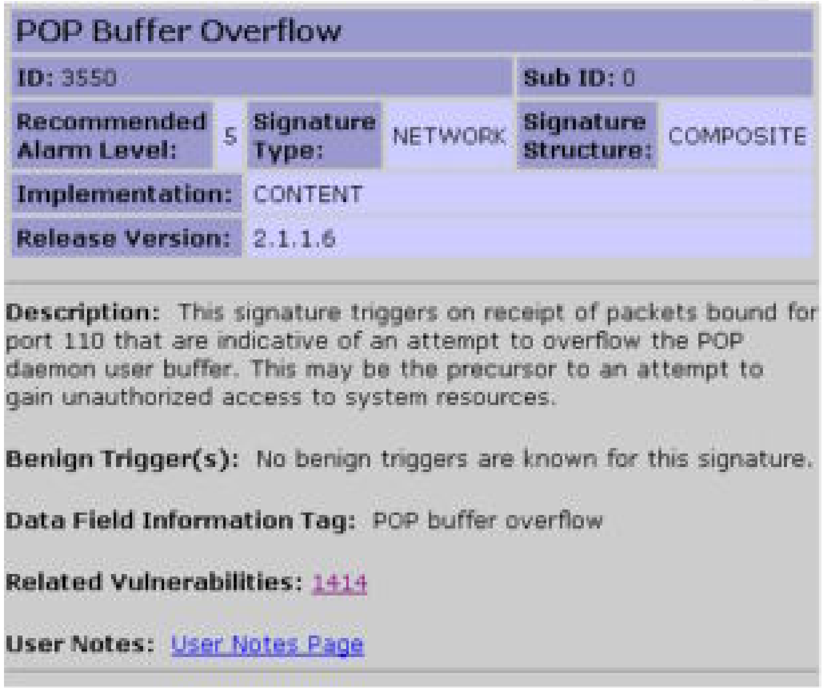
Detect – 5 POP3 Buffer Overflow

Source #1A



Date	Sensor	Signature	Sub Sig	Description	Severity	Src Address	Dst Address
2001-04-27 07:57:22	2	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-04-27 08:22:22	2	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-04-27 08:22:23	2	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:17:21	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:17:21	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 16:17:21	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:27:21	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:27:21	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 16:43:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:43:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 16:47:24	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:47:24	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 16:47:24	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:51:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:51:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 16:55:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:55:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 16:55:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_1.133.160
2001-05-01 16:59:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 17:13:20	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 17:21:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186
2001-05-01 17:30:25	1	3550	0	POP Overflow	5	OFF_NET 94.209	MAIL_2.69.186

1B)



POP Buffer Overflow

ID: 3550				**Sub ID:** 0	
Recommended Alarm Level:	5	**Signature Type:**	NETWORK	**Signature Structure:**	COMPOSITE
Implementation:	CONTENT				
Release Version:	2.1.1.6				

Description: This signature triggers on receipt of packets bound for port 110 that are indicative of an attempt to overflow the POP daemon user buffer. This may be the precursor to an attempt to gain unauthorized access to system resources.

Benign Trigger(s): No benign triggers are known for this signature.

Data Field Information Tag: POP buffer overflow

Related Vulnerabilities: 1414

User Notes: User Notes Page

Source #2

```
Here's the log info you requested.  As I mentioned during our phone call
it looks like normal mailreading activity, but if there's anything we need
to know about this guy then of course we're interested.  If there's
anything else we can provide just let me know.
```

```
Script started on Wed May 02 15:00:49 2001
# uname     -n
MAIL.SERVER.EDU
# grep '^May  1' /var/log/syslog | grep   'OFF\ NET \.94\.209'
May  1 00:00:39   MAIL.SERVER.EDU ipop3d[4611]: [ID 868162  mail.info] Login
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32/32
May  1 00:00:40   MAIL.SERVER.EDU ipop3d[4611]: [ID 124204  mail.info] Logout user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32 ndele=0
May  1 00:04:45   MAIL.SERVER.EDU ipop3d[5570]: [ID 868162  mail.info] Login
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32/32
May  1 00:04:45   MAIL.SERVER.EDU ipop3d[5570]: [ID 124204  mail.info] Logout user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32 ndele=0
May  1 00:08:46   MAIL.SERVER.EDU ipop3d[6458]: [ID 868162  mail.info] Login
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32/32
May  1 00:08:46   MAIL.SERVER.EDU ipop3d[6458]: [ID 124204  mail.info] Logout user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32 ndele=0
May  1 00:12:48   MAIL.SERVER.EDU ipop3d[7601]: [ID 868162  mail.info] Login
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32/32
May  1 00:12:48   MAIL.SERVER.EDU ipop3d[7601]: [ID 124204  mail.info] Logout user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32 ndele=0
May  1 00:16:49   MAIL.SERVER.EDU ipop3d[8482]: [ID 868162  mail.info] Login
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32/32
May  1 00:16:49   MAIL.SERVER.EDU ipop3d[8482]: [ID 124204  mail.info] Logout user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32 ndele=0
May  1 00:20:51   MAIL.SERVER.EDU ipop3d[9439]: [ID 868162  mail.info] Login
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32/32
May  1 00:20:51   MAIL.SERVER.EDU ipop3d[9439]: [ID 124204  mail.info] Logout user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32 ndele=0
May  1 00:24:52   MAIL.SERVER.EDU ipop3d[10501]: [ID 868162 mail.info] Login user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
May  1 00:24:53   MAIL.SERVER.EDU ipop3d[10501]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
May  1 00:28:54   MAIL.SERVER.EDU ipop3d[11388]: [ID 868162 mail.info] Login user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
May  1 00:28:54   MAIL.SERVER.EDU ipop3d[11388]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
```

```
(CUT) ---------------
May  1 23:42:18   MAIL.SERVER.EDU ipop3d[21406]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
May  1 23:44:10   MAIL.SERVER.EDU ipop3d[22016]: [ID 868162 mail.info] Login user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
May  1 23:44:10   MAIL.SERVER.EDU ipop3d[22016]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
May  1 23:44:38   MAIL.SERVER.EDU ipop3d[22174]: [ID 868162 mail.info] Login user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
May  1 23:44:39   MAIL.SERVER.EDU ipop3d[22174]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
May  1 23:48:40   MAIL.SERVER.EDU ipop3d[23534]: [ID 868162 mail.info] Login user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
May  1 23:48:40   MAIL.SERVER.EDU ipop3d[23534]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
May  1 23:52:42   MAIL.SERVER.EDU ipop3d[25419]: [ID 868162 mail.info] Login user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
May  1 23:52:42   MAIL.SERVER.EDU ipop3d[25419]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
May  1 23:56:39   MAIL.SERVER.EDU ipop3d[26941]: [ID 868162 mail.info] Login user=USER
      host=OFF_NET_ACCT.city.ISP.net      [OFF_NET.94.209]  nmsgs=32/32
May  1 23:56:39   MAIL.SERVER.EDU ipop3d[26941]: [ID 124204 mail.info] Logout
user=USERhost=OFF_NET_ACCT.city.ISP.net [OFF_NET.94.209] nmsgs=32 ndele=0
# last USER | grep 'May  1'
```

Source of Trace: This detect was gathered from a large .EDU network.
Detect Generated by: Cisco IDS logs and Syslog on the E-mail server
Probability the Source Address was Spoofed:
Description of the Attack: The Cisco IDS alerted on a POP3 Buffer overflow. There are many known exploits for POP3, most of the current CVE's and all of the candidates are buffer overflows attacks.

CVE-1999-0006 Buffer overflow in POP servers based on BSD/Qualcomm's qpopper allows remote attackers to gain root access using a long PASS command.

CVE-1999-0042 Buffer overflow in University of Washington's implementation of IMAP and POP servers.

CVE-1999-0494 Denial of service in WinGate proxy through a buffer overflow in POP3.
CVE-1999-0759 Buffer overflow in FuseMAIL POP service via long USER and PASS commands.
CVE-1999-1004 Buffer overflow in the POP server POProxy for the Norton Anti-Virus protection NAV2000 program via a large USER command.
CVE-2000-0091 Buffer overflow in vchkpw/vpopmail POP authentication package allows remote attackers to gain root privileges via a long username or password.
CVE-2000-0399 Buffer overflow in MDaemon POP server allows remote attackers to cause a denial of service via a long user name.
CVE-2000-0989 Buffer overflow in Intel InBusiness eMail Station 1.04.87 POP service allows remote attackers to cause a denial of service and possibly execute commands via a long username.

Attack Mechanism: The attack is aimed, according to the IDS, at overflowing one of the many vulnerable buffers as listed above. This is a popular attack and is listed as the number 9 top vulnerabilities in the SANS top ten list. A good definition of a buffer overflow was provided in "*Intrusion Signatures and Analysis*"

> "Hackers aim to subvert susceptible programs by providing excessive data. They do not use random bytes. Instead, the data packet is crafted in such a way that it contains executable code. The return address on the stack is overwritten with a new value that points to their code. Therefore when the subroutine exits, the CPU starts to execute the code provided by the Hacker." (Northcutt 272)

Correlation: Following up on IDS alerts I came across the multiple alerts for the pop3 overflow shown above, see source 1A. The IP address of the offending host was not on our network. Additionally it appeared that the host had been detected before by the IDS for the same exploit on 4-27-01. The IDS logs also seemed to indicate that the attacker had done previous reconnaissance of our network, since there were no logs of the host scanning for systems listening on the POP3 port 110.From the log it seemed that the attacker was persistently attempting the buffer overflow.

Additionally I couldn't understand why the attackers attempts were being allowed into our network. The alarm level on the IDS signature returns a level 5 alert. We shun and log all level 5 alerts, that is the IDS installs a router block for the offending IP address that times out after 15 minutes. The consistent time intervals (roughly 4 minutes) seemed odd to me as well.

I got a little excited and called the system administrators for the two systems to let them know what I was seeing and to ask if they had any logs that might help me figure this out. One admin wasn't available but the second sent me the logs shown above, source 2. I went thru the logs and all seemed above board. This sent me back to the IDS to see if there were any packet captures to look at, there were. (*Unfortunately the Cisco IDS log files are only readable by Ethereal, which will not allow me to cut and paste the data out of the file and into this document. I attempted to take a screenshot and edit the file in Photoshop but it became unreadable- the files are available upon request)*. They showed that the traffic was normal, and that the IDS incorrect. FALSE POSITIVE. Hindsight is 20/20 I guess, if I could do it again, I would have gone to look deeper into the IDS logs than I had originally.

Here are the high points:

- The IDS alarmed showing multiple attempts to exploit POP3 buffer overflow
- Queried the database attached to the IDS for all instances of the attacker in the last month
- Called the system administrators for the Victim servers
- Went thru the syslogs and determined the traffic looked "normal"
- Looked deeper into the log files on the IDS sensor and determined that the traffic was indeed normal

Given we have established the traffic is indeed normal, what is going on with the IDS? The reason that the IDS wasn't successfully shunning the host was because the host was on a network block that we lease to a local ISP for student accounts. This address is configured on the IDS to never be shunned. Why was the IDS alarming, and flagging normal traffic as a buffer overflow attempt? Unfortunately, the signature for the Cisco IDS are still proprietary, at least until June, so there is no way to determine this. Additionally we have a case open with Cisco TAC to determine the reason for the false positive.

The repeated Connects from the host were merely the student popping their mail from two different accounts, which exist on separate servers.

Evidence of Active Targeting: Yes, the only traffic we see from the alleged attacker is a supposed POP3 buffer overflow directed at two Departmental E-mail servers.

Severity:
Criticality: 4 the two host that the attack would have compromised are the E-Mail servers for the respective departments.
Lethality: 1 This was a false positive
System Countermeasures: 4 During my conversation with the system administrator for one of the systems, I determined that the machine had been recently patched and that the pop daemon was wrapped using TCP Wrappers. I am not aware of the patch state and level of countermeasures of the second server.
Network Countermeasures: 2 the IDS logs the signature as a POP buffer overflow, but is not correct. Many false positives from this signature may wear down the reaction of analysts, thereby causing slow/no reaction to a true overflow attempt.
(System Criticality + Lethality of Attack) – (System Countermeasures + Network Countermeasures) = Severity
(4 + 1) – (4 + 2) = -1

Defensive Recommendations: Remove the never shun status of the leased student IP address range. Verify that the OS's are current and that they are running the most recent patches on both servers. Install a host based IDS / Firewall.

POP3 uses ____ as a transport protocol

A. UDP
B. TCP
C. TCP & UDP
D. NNTP
E. IMAP

>C<

References

(Northcutt)-Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Freaderick. Intrusion Signatures and Analysis. Indianapolis: New Riders Publishing, 2001.

(Stevens)-Stevens, W. Richard. TCP/IP Illustrated, Volume 1. Reading: Addison Wesley Longman, Inc, 1994.

Web Pages

MITRE Corporation – [web page] http://cve.mitre.org, [Accessed 3 May 2001]

Network Security Library -- [web page] http://secinf.net/info/fw/cisco/cisco.html, [Accessed 3 May 2001]

Whatis.com – "IT Specific Encyclopedia" – [web page] http://whatis.techtarget.com/definition/0,289893,sid9_gci331881,00.html, [Accessed 3 May 2001]

Sans Institute Online – "TCP Wrappers- What are they" – [web page] http://www.sans.org/infosecFAQ/unix/TCP_wrappers2.htm, [Accessed 4 May 2001]

Antionline – [web page] http://www.antionline.com/cgi-bin/anticode/anticode.pl?dir=ftpd-exploits, [Accessed 4 May 2001]

Dsheild – [web page] http://www.dshield.org/, [Accessed 4 May 2001]

Insecure – "ARP and ICMP redirection games" [web page] http://www.insecure.org/sploits_all.html , [Accessed 5 May 2001]

Attrition – "Winfreez.c" [web page] http://www.attrition.org/security/denial/w/win-icmp.dos.html, [Accessed 5 May 2001]

World Wide Digital Security, Inc – " Statd Vulnerability" [web page]. http://www.wwdsi.com/cgi-bin/doc.pl?document=vulnerability/rpc_statd_access [Accessed 5 May 2001]

AT&T RoadRunner Personal Pages Gallery – “Macintosh DOS flood Attack” [web page]. http://people.atl.mediaone.net/jacopeland/faq.html [Accessed 6 May 2001]

Attachments

Attachment A

```
May  1 03:18:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425283: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(47933) -> MY_NET.32.57(21), 1 packet
May  1 03:18:52 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425284: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(47934) -> MY_NET.32.57(21), 1 packet
May  1 03:18:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425285: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(47936) -> MY_NET.32.57(21), 1 packet
May  1 11:08:05 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425658: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3162) -> MY_NET.189.42(21), 1 packet
May  1 11:08:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425664: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3018) -> MY_NET.143.59(21), 1 packet
May  1 11:08:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425665: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3321) -> MY_NET.126.100(21), 1 packet
May  1 11:08:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425666: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3330) -> MY_NET.181.50(21), 1 packet
May  1 11:08:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425667: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3244) -> MY_NET.189.82(21), 1 packet
May  1 11:08:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425668: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3049) -> MY_NET.143.74(21), 1 packet
May  1 11:08:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425669: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3372) -> MY_NET.188.114(21), 1 packet
May  1 11:08:14 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425670: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3423) -> MY_NET.181.79(21), 1 packet
May  1 11:08:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425671: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3330) -> MY_NET.181.50(21), 1 packet
```

```
May  1 11:08:16 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425672: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3118) -> MY_NET.184.16(21), 1 packet
May  1 11:08:17 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425673: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3445) -> MY_NET.126.143(21), 1 packet
May  1 11:08:18 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425674: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3430) -> MY_NET.181.83(21), 1 packet
May  1 11:08:19 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425675: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3376) -> MY_NET.188.115(21), 1 packet
May  1 11:08:20 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425676: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3465) -> MY_NET.126.148(21), 1 packet
May  1 11:08:21 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425677: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3223) -> MY_NET.184.65(21), 1 packet
May  1 11:08:22 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425678: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3414) -> MY_NET.181.77(21), 1 packet
May  1 11:08:23 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425679: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3424) -> MY_NET.181.81(21), 1 packet
May  1 11:08:24 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425680: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3431) -> MY_NET.126.137(21), 1 packet
May  1 11:08:24 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425681: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3295) -> MY_NET.184.93(21), 1 packet
May  1 11:08:26 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425682: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3321) -> MY_NET.126.100(21), 1 packet
May  1 11:08:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425683: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3533) -> MY_NET.126.201(21), 1 packet
May  1 11:08:28 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425684: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3341) -> MY_NET.126.107(21), 1 packet
May  1 11:08:29 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425685: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3356) -> MY_NET.188.108(21), 1 packet
May  1 11:08:30 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425686: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3371) -> MY_NET.126.117(21), 1 packet
May  1 11:08:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425688: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3379) -> MY_NET.126.119(21), 1 packet
May  1 11:08:33 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425689: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3393) -> MY_NET.181.69(21), 1 packet
May  1 11:08:33 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425690: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3554) -> MY_NET.126.206(21), 1 packet
May  1 11:08:34 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425695: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3518) -> MY_NET.188.168(21), 1 packet
```

```
May  1 11:08:35 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425696: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3426) -> MY_NET.188.132(21), 1 packet
May  1 11:08:36 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425697: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3588) -> MY_NET.188.191(21), 1 packet
May  1 11:08:37 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425698: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3544) -> MY_NET.188.200(21), 1 packet
May  1 11:08:37 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425699: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3611) -> MY_NET.188.196(21), 1 packet
May  1 11:08:39 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425700: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3656) -> MY_NET.126.242(21), 1 packet
May  1 11:08:41 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425701: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3672) -> MY_NET.126.249(21), 1 packet
May  1 11:08:42 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425702: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3649) -> MY_NET.188.234(21), 1 packet
May  1 11:08:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425703: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3590) -> MY_NET.188.211(21), 1 packet
May  1 11:08:44 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425704: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3600) -> MY_NET.126.197(21), 1 packet
May  1 11:08:45 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425705: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3616) -> MY_NET.126.223(21), 1 packet
May  1 11:08:46 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425706: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3515) -> MY_NET.126.172(21), 1 packet
May  1 11:08:47 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425707: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3705) -> MY_NET.183.32(21), 1 packet
May  1 11:08:48 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425708: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3532) -> MY_NET.188.175(21), 1 packet
May  1 11:08:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425709: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3669) -> MY_NET.188.244(21), 1 packet
May  1 11:08:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425710: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3684) -> MY_NET.183.11(21), 1 packet
May  1 11:08:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425711: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3733) -> MY_NET.183.59(21), 1 packet
May  1 11:08:52 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425712: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3773) -> MY_NET.183.95(21), 1 packet
May  1 11:08:53 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425713: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3781) -> MY_NET.71.219(21), 1 packet
May  1 11:08:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425714: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3791) -> MY_NET.141.9(21), 1 packet
```

```
May  1 11:08:56 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425715: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3600) -> MY_NET.126.197(21), 1 packet
May  1 11:08:57 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425716: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3810) -> MY_NET.171.24(21), 1 packet
May  1 11:08:58 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425717: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3621) -> MY_NET.188.199(21), 1 packet
May  1 11:08:59 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425718: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3639) -> MY_NET.188.228(21), 1 packet
May  1 11:09:00 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425719: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3755) -> MY_NET.183.82(21), 1 packet
May  1 11:09:01 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425720: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3663) -> MY_NET.188.241(21), 1 packet
May  1 11:09:02 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425721: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3774) -> MY_NET.140.7(21), 1 packet
May  1 11:09:03 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425722: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3784) -> MY_NET.141.2(21), 1 packet
May  1 11:09:04 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425723: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3794) -> MY_NET.171.12(21), 1 packet
May  1 11:09:05 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425724: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3804) -> MY_NET.171.19(21), 1 packet
May  1 11:09:06 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425725: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3860) -> MY_NET.171.70(21), 1 packet
May  1 11:09:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425726: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3902) -> MY_NET.71.201(21), 1 packet
May  1 11:09:08 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425727: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3826) -> MY_NET.171.34(21), 1 packet
May  1 11:09:09 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425728: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3835) -> MY_NET.171.43(21), 1 packet
May  1 11:09:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425729: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3905) -> MY_NET.174.11(21), 1 packet
May  1 11:09:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425730: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3956) -> MY_NET.174.59(21), 1 packet
May  1 11:09:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425731: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3967) -> MY_NET.174.72(21), 1 packet
May  1 11:09:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425732: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3980) -> MY_NET.174.85(21), 1 packet
May  1 11:09:14 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425733: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3777) -> MY_NET.183.97(21), 1 packet
```

```
May  1 11:09:14 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425734: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3790) -> MY_NET.141.8(21), 1 packet
May  1 11:09:16 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425735: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3920) -> MY_NET.71.224(21), 1 packet
May  1 11:09:17 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425736: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4012) -> MY_NET.182.20(21), 1 packet
May  1 11:09:18 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425737: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3947) -> MY_NET.174.52(21), 1 packet
May  1 11:09:20 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425738: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3824) -> MY_NET.171.32(21), 1 packet
May  1 11:09:21 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425739: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4037) -> MY_NET.182.44(21), 1 packet
May  1 11:09:22 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425740: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4050) -> MY_NET.182.57(21), 1 packet
May  1 11:09:23 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425741: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4057) -> MY_NET.182.64(21), 1 packet
May  1 11:09:24 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425742: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4066) -> MY_NET.182.73(21), 1 packet
May  1 11:09:25 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425743: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4000) -> MY_NET.185.7(21), 1 packet
May  1 11:09:26 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425744: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3887) -> MY_NET.171.95(21), 1 packet
May  1 11:09:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425745: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3895) -> MY_NET.143.3(21), 1 packet
May  1 11:09:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425746: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3903) -> MY_NET.71.223(21), 1 packet
May  1 11:09:29 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425747: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4110) -> MY_NET.178.140(21), 1 packet
May  1 11:09:30 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425748: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3936) -> MY_NET.174.39(21), 1 packet
May  1 11:09:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425749: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(3949) -> MY_NET.174.54(21), 1 packet
May  1 11:09:32 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425750: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4062) -> MY_NET.182.68(21), 1 packet
May  1 11:09:33 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425751: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4068) -> MY_NET.182.75(21), 1 packet
May  1 11:09:34 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425752: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4079) -> MY_NET.182.86(21), 1 packet
```

```
May  1 11:09:35 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425753: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4093) -> MY_NET.182.2(21), 1 packet
May  1 11:09:36 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425754: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4099) -> MY_NET.182.8(21), 1 packet
May  1 11:09:37 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425755: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4170) -> MY_NET.178.190(21), 1 packet
May  1 11:09:38 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425756: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4115) -> MY_NET.178.143(21), 1 packet
May  1 11:09:39 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425757: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4182) -> MY_NET.178.215(21), 1 packet
May  1 11:09:40 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425758: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4206) -> MY_NET.245.101(21), 1 packet
May  1 11:09:41 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425759: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4213) -> MY_NET.178.236(21), 1 packet
May  1 11:09:42 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425760: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4230) -> MY_NET.245.113(21), 1 packet
May  1 11:09:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425761: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4169) -> MY_NET.178.208(21), 1 packet
May  1 11:09:44 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425762: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4251) -> MY_NET.245.128(21), 1 packet
May  1 11:09:45 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425763: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4069) -> MY_NET.182.76(21), 1 packet
May  1 11:09:46 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425764: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4206) -> MY_NET.245.101(21), 1 packet
May  1 11:09:47 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425765: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4273) -> MY_NET.245.149(21), 1 packet
May  1 11:09:48 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425766: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4301) -> MY_NET.245.200(21), 1 packet
May  1 11:09:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425767: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4290) -> MY_NET.245.170(21), 1 packet
May  1 11:09:50 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425768: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4322) -> MY_NET.245.188(21), 1 packet
May  1 11:09:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425769: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4303) -> MY_NET.245.178(21), 1 packet
May  1 11:09:53 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425770: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4270) -> MY_NET.245.150(21), 1 packet
May  1 11:09:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425771: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4151) -> MY_NET.178.180(21), 1 packet
```

```
May  1 11:09:55 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425772: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4161) -> MY_NET.178.184(21), 1 packet
May  1 11:09:56 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425773: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4293) -> MY_NET.245.169(21), 1 packet
May  1 11:09:57 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425774: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4377) -> MY_NET.125.41(21), 1 packet
May  1 11:09:58 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425775: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4198) -> MY_NET.178.226(21), 1 packet
May  1 11:09:59 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425776: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4318) -> MY_NET.245.187(21), 1 packet
May  1 11:10:00 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425777: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4327) -> MY_NET.245.212(21), 1 packet
May  1 11:10:01 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425778: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4410) -> MY_NET.126.19(21), 1 packet
May  1 11:10:02 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425779: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4251) -> MY_NET.245.128(21), 1 packet
May  1 11:10:03 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425780: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4354) -> MY_NET.245.231(21), 1 packet
May  1 11:10:04 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425781: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4268) -> MY_NET.245.146(21), 1 packet
May  1 11:10:05 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425782: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4425) -> MY_NET.126.36(21), 1 packet
May  1 11:10:06 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425783: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4472) -> MY_NET.126.83(21), 1 packet
May  1 11:10:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425784: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4486) -> MY_NET.174.3(21), 1 packet
May  1 11:10:09 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425785: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4502) -> MY_NET.190.15(21), 1 packet
May  1 11:10:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425786: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4480) -> MY_NET.126.89(21), 1 packet
May  1 11:10:11 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425787: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4487) -> MY_NET.126.96(21), 1 packet
May  1 11:10:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425788: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4327) -> MY_NET.245.212(21), 1 packet
May  1 11:10:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425789: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4339) -> MY_NET.245.220(21), 1 packet
May  1 11:10:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425790: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4548) -> MY_NET.190.61(21), 1 packet
```

```
May  1 11:10:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425791: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4352) -> MY_NET.245.230(21), 1 packet
May  1 11:10:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425792: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4543) -> MY_NET.190.56(21), 1 packet
May  1 11:10:18 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425793: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4376) -> MY_NET.178.102(21), 1 packet
May  1 11:10:19 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425794: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4512) -> MY_NET.190.25(21), 1 packet
May  1 11:10:20 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425795: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4604) -> MY_NET.190.116(21), 1 packet
May  1 11:10:21 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425796: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4398) -> MY_NET.71.228(21), 1 packet
May  1 11:10:22 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425797: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4407) -> MY_NET.126.20(21), 1 packet
May  1 11:10:23 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425798: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4419) -> MY_NET.126.31(21), 1 packet
May  1 11:10:24 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425799: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4614) -> MY_NET.190.126(21), 1 packet
May  1 11:10:25 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425800: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4649) -> MY_NET.190.161(21), 1 packet
May  1 11:10:26 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425801: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4631) -> MY_NET.190.143(21), 1 packet
May  1 11:10:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425802: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4639) -> MY_NET.190.151(21), 1 packet
May  1 11:10:28 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425803: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4651) -> MY_NET.190.162(21), 1 packet
May  1 11:10:29 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425804: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4605) -> MY_NET.190.117(21), 1 packet
May  1 11:10:30 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425805: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4618) -> MY_NET.190.129(21), 1 packet
May  1 11:10:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425806: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4517) -> MY_NET.190.29(21), 1 packet
May  1 11:10:32 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425807: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4527) -> MY_NET.190.39(21), 1 packet
May  1 11:10:33 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425808: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4644) -> MY_NET.190.155(21), 1 packet
May  1 11:10:34 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425809: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4696) -> MY_NET.190.188(21), 1 packet
```

```
May  1 11:10:35 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425810: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4739) -> MY_NET.185.123(21), 1 packet
May  1 11:10:36 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425811: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4759) -> MY_NET.185.133(21), 1 packet
May  1 11:10:37 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425812: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4765) -> MY_NET.185.136(21), 1 packet
May  1 11:10:38 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425813: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4740) -> MY_NET.190.225(21), 1 packet
May  1 11:10:39 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425814: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4757) -> MY_NET.185.132(21), 1 packet
May  1 11:10:40 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425815: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4797) -> MY_NET.185.152(21), 1 packet
May  1 11:10:41 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425816: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4708) -> MY_NET.185.111(21), 1 packet
May  1 11:10:42 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425817: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4621) -> MY_NET.190.133(21), 1 packet
May  1 11:10:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425818: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4732) -> MY_NET.185.120(21), 1 packet
May  1 11:10:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425819: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4831) -> MY_NET.185.182(21), 1 packet
May  1 11:10:45 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425820: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4839) -> MY_NET.185.186(21), 1 packet
May  1 11:10:46 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425821: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4849) -> MY_NET.185.191(21), 1 packet
May  1 11:10:47 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425822: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4854) -> MY_NET.185.193(21), 1 packet
May  1 11:10:48 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425823: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4665) -> MY_NET.190.176(21), 1 packet
May  1 11:10:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425824: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4882) -> MY_NET.132.101(21), 1 packet
May  1 11:10:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425825: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4807) -> MY_NET.185.159(21), 1 packet
May  1 11:10:52 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425826: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4901) -> MY_NET.132.111(21), 1 packet
May  1 11:10:53 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425827: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4700) -> MY_NET.190.191(21), 1 packet
May  1 11:10:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425828: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4835) -> MY_NET.185.184(21), 1 packet
```

```
May  1 11:10:55 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425829: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4929) -> MY_NET.171.2(21), 1 packet
May  1 11:10:56 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425830: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4939) -> MY_NET.245.11(21), 1 packet
May  1 11:10:57 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425831: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4858) -> MY_NET.185.195(21), 1 packet
May  1 11:10:58 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425832: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4946) -> MY_NET.245.18(21), 1 packet
May  1 11:10:59 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425833: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4886) -> MY_NET.132.103(21), 1 packet
May  1 11:11:00 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425834: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4900) -> MY_NET.185.243(21), 1 packet
May  1 11:11:04 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425835: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4797) -> MY_NET.185.152(21), 1 packet
May  1 11:11:05 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425836: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4974) -> MY_NET.245.38(21), 1 packet
May  1 11:11:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425837: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4842) -> MY_NET.185.187(21), 1 packet
May  1 11:11:08 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425838: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4951) -> MY_NET.245.23(21), 1 packet
May  1 11:11:08 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425839: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4956) -> MY_NET.81.11(21), 1 packet
May  1 11:11:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425840: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4876) -> MY_NET.185.228(21), 1 packet
May  1 11:11:11 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425841: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4980) -> MY_NET.245.44(21), 1 packet
May  1 11:11:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425842: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4997) -> MY_NET.183.4(21), 1 packet
May  1 11:11:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425843: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(4902) -> MY_NET.132.109(21), 1 packet
May  1 11:11:14 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425844: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(1037) -> MY_NET.245.63(21), 1 packet
May  1 11:11:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425845: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(1134) -> MY_NET.93.182(21), 1 packet
May  1 11:11:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 425846: 28w6d: %SEC-6-IPACCESSLOGP: list 138 denied
tcp 200.191.142.217(1117) -> MY_NET.93.170(21), 1 packet
--
```

Attachment B

rsh SYSTEM grep 211.195.36.62 /var/log/syslog_info:

```
May  3 13:16:38 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432491: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(0) ->
MY_NETWORK.31.134(0), 1 packet
May  3 13:16:40 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432497: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(0) ->
MY_NETWORK.35.74(0), 1 packet
May  3 13:16:40 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432498: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1138) ->
MY_NETWORK.35.115(111), 1 packet
May  3 13:16:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432504: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2146) ->
MY_NETWORK.39.93(111), 1 packet
May  3 13:16:44 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432505: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3149) ->
MY_NETWORK.43.73(111), 1 packet
May  3 13:16:46 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432506: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3153) ->
MY_NETWORK.43.77(111), 1 packet
May  3 13:16:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432511: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4034) ->
MY_NETWORK.46.191(111), 1 packet
May  3 13:16:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432512: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1184) ->
MY_NETWORK.51.36(111), 1 packet
May  3 13:16:55 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432513: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2195) ->
MY_NETWORK.55.17(111), 1 packet
May  3 13:16:58 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432514: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3201) ->
MY_NETWORK.59.0(111), 1 packet
May  3 13:17:01 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432515: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4202) ->
MY_NETWORK.62.234(111), 1 packet
May  3 13:17:04 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432516: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1170) ->
MY_NETWORK.66.152(111), 1 packet
May  3 13:17:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432517: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2241) ->
MY_NETWORK.70.193(111), 1 packet
May  3 13:17:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432518: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3244) ->
MY_NETWORK.74.173(111), 1 packet
May  3 13:17:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432519: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4247) ->
MY_NETWORK.78.154(111), 1 packet
```

```
May  3 13:17:16 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432520: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1277) ->
MY_NETWORK.82.134(111), 1 packet
May  3 13:17:19 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432521: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2287) ->
MY_NETWORK.86.114(111), 1 packet
May  3 13:17:22 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432522: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3292) ->
MY_NETWORK.90.96(111), 1 packet
May  3 13:17:24 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432523: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4257) ->
MY_NETWORK.94.39(111), 1 packet
May  3 13:17:26 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432524: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4294) ->
MY_NETWORK.94.75(111), 1 packet
May  3 13:17:28 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432525: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1325) ->
MY_NETWORK.98.57(111), 1 packet
May  3 13:17:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432526: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2336) ->
MY_NETWORK.102.38(111), 1 packet
May  3 13:17:34 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432527: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3336) ->
MY_NETWORK.106.17(111), 1 packet
May  3 13:17:37 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432528: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4339) ->
MY_NETWORK.109.253(111), 1 packet
May  3 13:17:40 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432529: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1369) ->
MY_NETWORK.113.234(111), 1 packet
May  3 13:17:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432530: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2380) ->
MY_NETWORK.117.215(111), 1 packet
May  3 13:17:46 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432531: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3383) ->
MY_NETWORK.121.197(111), 1 packet
May  3 13:17:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432532: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4387) ->
MY_NETWORK.125.179(111), 1 packet
May  3 13:17:52 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432533: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1415) ->
MY_NETWORK.129.158(111), 1 packet
May  3 13:17:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432534: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2409) ->
MY_NETWORK.133.124(111), 1 packet
May  3 13:17:55 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432535: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2424) ->
MY_NETWORK.133.139(111), 1 packet
May  3 13:17:57 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432536: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3424) ->
MY_NETWORK.137.118(111), 1 packet
May  3 13:17:58 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432537: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3425) ->
MY_NETWORK.137.119(111), 1 packet
```

```
May  3 13:17:59 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432538: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1888) ->
MY_NETWORK.7.91(111), 1 packet
May  3 13:18:01 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432539: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4428) ->
MY_NETWORK.141.100(111), 1 packet
May  3 13:18:03 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432540: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4427) ->
MY_NETWORK.141.99(111), 1 packet
May  3 13:18:04 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432541: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1458) ->
MY_NETWORK.145.81(111), 1 packet
May  3 13:18:06 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432542: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1457) ->
MY_NETWORK.145.80(111), 1 packet
May  3 13:18:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432543: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2466) ->
MY_NETWORK.149.61(111), 1 packet
May  3 13:18:09 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432544: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2465) ->
MY_NETWORK.149.60(111), 1 packet
May  3 13:18:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432545: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3468) ->
MY_NETWORK.153.42(111), 1 packet
May  3 13:18:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432546: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3467) ->
MY_NETWORK.153.41(111), 1 packet
May  3 13:18:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432547: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4472) ->
MY_NETWORK.157.24(111), 1 packet
May  3 13:18:15 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432548: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1500) ->
MY_NETWORK.161.3(111), 1 packet
May  3 13:18:16 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432549: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1501) ->
MY_NETWORK.161.4(111), 1 packet
May  3 13:18:18 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432550: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1500) ->
MY_NETWORK.161.3(111), 1 packet
May  3 13:18:19 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432551: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2510) ->
MY_NETWORK.164.240(111), 1 packet
May  3 13:18:22 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432553: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(0) ->
MY_NETWORK.168.220(0), 1 packet
May  3 13:18:22 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432554: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3609) ->
MY_NETWORK.169.63(111), 1 packet
May  3 13:18:23 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432560: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4447) ->
MY_NETWORK.172.134(111), 1 packet
May  3 13:18:25 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432566: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4593) ->
MY_NETWORK.173.25(111), 1 packet
```

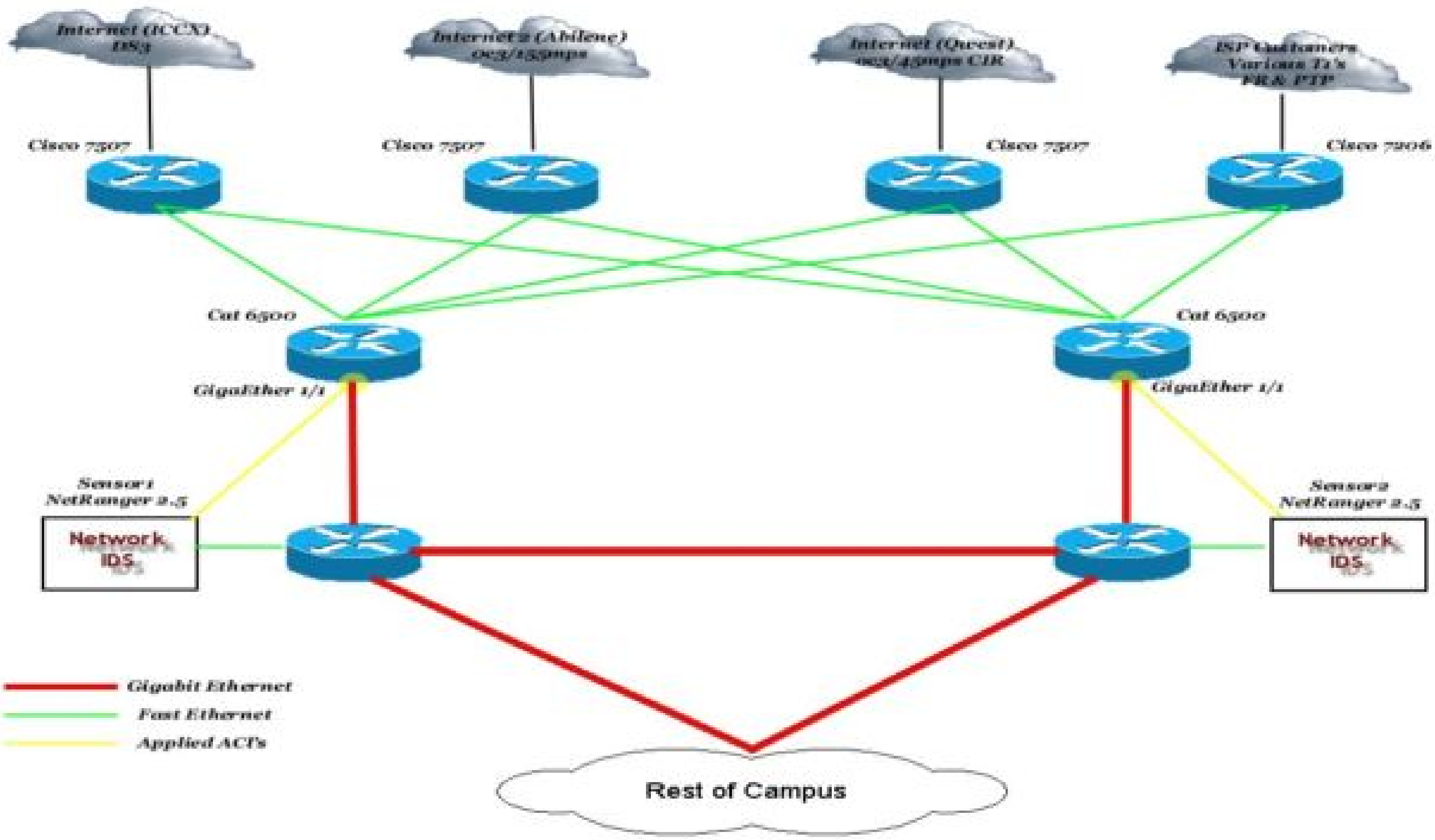
```
May  3 13:18:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432567: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4513) ->
MY_NETWORK.172.200(111), 1 packet
May  3 13:18:28 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432568: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1544) ->
MY_NETWORK.176.182(111), 1 packet
May  3 13:18:28 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432569: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2551) ->
MY_NETWORK.180.161(111), 1 packet
May  3 13:18:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432570: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2553) ->
MY_NETWORK.180.163(111), 1 packet
May  3 13:18:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432571: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2677) ->
MY_NETWORK.181.32(111), 1 packet
May  3 13:18:34 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432572: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(0) ->
MY_NETWORK.180.164(0), 1 packet
May  3 13:18:34 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432577: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3644) ->
MY_NETWORK.184.233(111), 1 packet
May  3 13:18:36 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432578: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3556) ->
MY_NETWORK.184.145(111), 1 packet
May  3 13:18:37 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432579: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4560) ->
MY_NETWORK.188.127(111), 1 packet
May  3 13:18:38 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432580: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1588) ->
MY_NETWORK.192.106(111), 1 packet
May  3 13:18:41 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432582: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2595) ->
MY_NETWORK.196.85(111), 1 packet
May  3 13:18:42 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432583: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1589) ->
MY_NETWORK.192.107(111), 1 packet
May  3 13:18:43 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432584: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2599) ->
MY_NETWORK.196.89(111), 1 packet
May  3 13:18:44 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432585: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3598) ->
MY_NETWORK.200.67(111), 1 packet
May  3 13:18:45 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432586: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2598) ->
MY_NETWORK.196.88(111), 1 packet
May  3 13:18:46 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432587: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2606) ->
MY_NETWORK.196.96(111), 1 packet
May  3 13:18:47 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432588: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4601) ->
MY_NETWORK.204.48(111), 1 packet
May  3 13:18:47 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432589: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3600) ->
MY_NETWORK.200.69(111), 1 packet
```

```
May  3 13:18:49 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432590: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4725) ->
MY_NETWORK.204.172(111), 1 packet
May  3 13:18:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432591: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4603) ->
MY_NETWORK.204.50(111), 1 packet
May  3 13:18:52 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432592: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1634) ->
MY_NETWORK.208.32(111), 1 packet
May  3 13:18:54 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432593: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2642) ->
MY_NETWORK.212.12(111), 1 packet
May  3 13:18:55 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432594: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2645) ->
MY_NETWORK.212.15(111), 1 packet
May  3 13:18:57 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432595: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2642) ->
MY_NETWORK.212.12(111), 1 packet
May  3 13:18:58 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432596: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3646) ->
MY_NETWORK.215.250(111), 1 packet
May  3 13:19:00 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432597: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3644) ->
MY_NETWORK.215.248(111), 1 packet
May  3 13:19:01 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432598: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4650) ->
MY_NETWORK.219.232(111), 1 packet
May  3 13:19:03 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432599: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4647) ->
MY_NETWORK.219.229(111), 1 packet
May  3 13:19:04 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432600: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1685) ->
MY_NETWORK.223.213(111), 1 packet
May  3 13:19:05 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432601: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2685) ->
MY_NETWORK.227.190(111), 1 packet
May  3 13:19:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432602: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2687) ->
MY_NETWORK.227.192(111), 1 packet
May  3 13:19:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432603: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2684) ->
MY_NETWORK.227.189(111), 1 packet
May  3 13:19:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432604: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3689) ->
MY_NETWORK.231.173(111), 1 packet
May  3 13:19:11 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432605: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4690) ->
MY_NETWORK.235.152(111), 1 packet
May  3 13:19:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432606: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4696) ->
MY_NETWORK.235.158(111), 1 packet
May  3 13:19:14 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432607: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1725) ->
MY_NETWORK.239.133(111), 1 packet
```

```
May  3 13:19:16 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432608: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1727) ->
MY_NETWORK.239.135(111), 1 packet
May  3 13:19:17 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432609: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2727) ->
MY_NETWORK.243.112(111), 1 packet
May  3 13:19:19 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432610: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2733) ->
MY_NETWORK.243.118(111), 1 packet
May  3 13:19:20 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432611: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(2728) ->
MY_NETWORK.243.113(111), 1 packet
May  3 13:19:22 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432612: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3734) ->
MY_NETWORK.247.98(111), 1 packet
May  3 13:19:24 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432613: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(3732) ->
MY_NETWORK.247.96(111), 1 packet
May  3 13:19:25 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432614: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4736) ->
MY_NETWORK.251.78(111), 1 packet
May  3 13:19:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432615: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(4735) ->
MY_NETWORK.251.77(111), 1 packet
May  3 13:19:28 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432616: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1774) ->
MY_NETWORK.255.62(111), 1 packet
May  3 13:19:30 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432617: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1770) ->
MY_NETWORK.255.58(111), 1 packet
May  3 13:20:07 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432619: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1888) ->
MY_NETWORK.7.91(111), 1 packet
May  3 13:20:26 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432621: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 1 packet
May  3 13:20:32 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432622: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1849) ->
MY_NETWORK.7.52(111), 1 packet
May  3 13:22:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432624: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1980) ->
MY_NETWORK.7.181(111), 1 packet
May  3 13:24:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432625: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1134) ->
MY_NETWORK.4.111(111), 1 packet
May  3 13:25:09 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432626: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1888) ->
MY_NETWORK.7.91(111), 4 packets
May  3 13:26:10 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432627: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 2 packets
May  3 13:28:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432638: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1980) ->
MY_NETWORK.7.181(111), 1 packet
```

```
May  3 13:30:11 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432640: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1885) ->
MY_NETWORK.7.88(111), 1 packet
May  3 13:31:11 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432643: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 3 packets
May  3 13:34:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432646: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1980) ->
MY_NETWORK.7.181(111), 1 packet
May  3 13:36:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432647: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 2 packets
May  3 13:36:31 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432648: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1663) ->
MY_NETWORK.6.124(111), 1 packet
May  3 13:41:13 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432651: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 2 packets
May  3 14:09:51 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432670: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1134) ->
MY_NETWORK.4.111(111), 1 packet
May  3 14:28:27 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 432681: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1034) ->
MY_NETWORK.4.11(111), 1 packet
May  3 15:15:12 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433334: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1078) ->
MY_NETWORK.4.55(111), 1 packet
May  3 15:15:17 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433335: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1067) ->
MY_NETWORK.4.44(111), 1 packet
May  3 15:20:32 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433339: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1067) ->
MY_NETWORK.4.44(111), 4 packets
May  3 15:25:33 CISRTR-fa5-0-0-CISRTR.telcom.MY_NETWORK 433344: 29w2d: %SEC-6-IPACCESSLOGP: list 138 denied tcp 211.195.36.62(1067) ->
MY_NETWORK.4.44(111), 3 packets
```

Attachment C



Attachment D

Date	Sensor	Signature	Sub Sig	Src Address	Dst Address
2001-04-26 20:51:25	1	6054	0	200.33.22.40	MY_NET.64.26
2001-05-04 15:44:20	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 15:44:21	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 15:44:22	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 15:44:22	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 15:44:23	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 15:44:23	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 15:45:20	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 15:45:21	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 15:45:22	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 15:45:23	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 15:45:23	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 15:45:25	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 15:46:22	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 15:46:23	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 15:46:23	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 15:49:22	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 15:49:23	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 15:49:23	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 15:50:20	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 15:51:21	2	2151	1024	131.161.83.242	MY_NET.64.26

2001-05-04 15:51:22	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 15:51:22	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 15:51:22	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 15:51:23	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 15:51:23	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 15:55:21	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 15:59:22	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 15:59:22	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 15:59:22	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 15:59:23	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 15:59:24	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 15:59:24	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:02:24	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:02:29	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:02:38	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:02:45	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:02:46	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:02:50	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:02:50	1	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:02:50	1	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:02:53	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:02:53	1	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:02:58	1	2151	1024	206.47.27.236	MY_NET.64.26

2001-05-04 16:10:20	2	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 16:10:20	2	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:10:20	2	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:10:20	2	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:10:21	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:10:21	2	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:10:21	2	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:10:21	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:10:21	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:10:22	2	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 16:10:22	2	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 16:10:22	2	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:10:22	2	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 16:10:23	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:10:23	2	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 16:10:23	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:10:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:10:23	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:10:24	2	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 16:10:24	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:10:24	2	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 16:10:24	2	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 16:10:24	1	2151	1024	198.86.245.21	MY_NET.64.26

2001-05-04 16:10:25	2	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 16:10:25	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:10:25	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:10:25	2	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 16:10:25	2	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:11:20	2	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 16:11:20	2	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:11:20	2	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:11:20	2	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:11:20	2	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:11:21	2	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:11:21	2	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:11:21	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:11:21	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:11:22	2	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 16:11:22	2	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:11:22	2	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 16:11:23	2	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 16:11:23	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:11:23	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:11:23	2	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 16:11:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:11:23	1	2151	1024	209.167.93.30	MY_NET.64.26

2001-05-04 16:11:24	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:11:24	2	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 16:11:24	2	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 16:11:24	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:11:24	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:11:25	2	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 16:11:25	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:11:25	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:11:25	2	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 16:11:25	2	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:11:25	2	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 16:12:04	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:12:04	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:12:05	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:12:07	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:12:13	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:12:14	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 16:12:14	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 16:12:20	2	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 16:12:20	2	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:12:20	2	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:12:20	2	2151	1024	216.103.219.35	MY_NET.64.26

2001-05-04 16:12:20	2	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:12:20	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 16:12:21	2	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:12:21	2	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:12:21	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:12:21	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:12:22	2	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 16:12:22	2	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:12:22	2	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 16:12:23	2	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 16:12:23	2	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 16:12:23	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:12:23	2	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 16:12:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:12:23	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:12:24	2	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 16:12:24	2	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 16:12:24	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:12:24	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:12:25	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:12:25	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:12:25	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:12:25	2	2151	1024	24.108.77.10	MY_NET.64.26

2001-05-04 16:12:25	2	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:12:25	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:12:26	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:12:30	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:12:39	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:12:46	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:12:47	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:12:49	1	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 16:12:51	1	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:12:51	1	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:12:54	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:12:54	1	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:13:20	2	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:13:20	2	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:13:20	2	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 16:13:21	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:13:21	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:13:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:13:24	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:14:21	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:14:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:14:23	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:15:21	1	2151	1024	24.176.33.13	MY_NET.64.26

2001-05-04 16:15:22	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:15:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:15:24	2	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 16:15:24	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:15:24	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:15:24	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:16:21	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:16:22	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:16:23	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:16:24	2	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 16:16:25	2	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:16:25	2	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 16:16:25	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:16:25	2	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 16:16:25	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:17:20	2	2151	1024	24.157.236.160	MY_NET.64.26

2001-05-04 16:17:20	2	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 16:17:21	2	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 16:19:25	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:22:05	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:22:05	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:22:06	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:22:08	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:22:11	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:22:15	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 16:22:15	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 16:22:21	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 16:22:24	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:22:26	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:22:26	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:22:31	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:22:35	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 16:22:36	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:22:37	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 16:22:40	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:22:41	1	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 16:22:47	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:22:48	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:27:20	1	2151	1024	198.86.245.21	MY_NET.64.26

2001-05-04 16:29:20	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:29:23	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:30:25	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:31:23	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:31:23	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:32:00	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 16:32:15	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:32:25	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:32:27	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:32:30	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 16:32:32	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:32:32	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:32:41	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:32:45	1	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:32:47	1	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 16:32:49	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:33:25	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:34:25	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:35:25	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:35:25	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:37:24	2	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 16:37:24	2	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:37:24	2	2151	1024	163.26.88.129	MY_NET.64.26

2001-05-04 16:37:25	2	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 16:37:25	2	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 16:37:25	2	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:38:20	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:38:20	2	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 16:38:20	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:38:21	2	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 16:38:21	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:38:21	2	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 16:38:21	2	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 16:38:22	2	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:38:22	2	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:38:22	2	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 16:38:22	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:38:22	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:38:22	2	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 16:38:22	2	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:38:23	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:38:23	2	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 16:38:23	2	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:38:23	2	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:38:24	2	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 16:38:24	2	2151	1024	216.101.146.69	MY_NET.64.26

2001-05-04 16:38:24	2	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:38:25	2	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 16:38:25	2	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:40:24	2	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 16:42:07	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:42:07	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:42:08	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:42:28	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:42:33	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:42:42	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:42:46	1	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:42:49	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:42:50	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:42:53	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:45:20	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:45:20	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:46:22	2	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 16:46:23	2	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 16:46:23	2	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 16:46:23	2	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 16:46:23	2	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 16:46:23	2	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 16:46:23	2	2151	1024	216.164.64.12	MY_NET.64.26

2001-05-04 16:46:23	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:46:23	2	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 16:46:24	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 16:46:25	2	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 16:46:25	2	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:46:25	2	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:47:20	2	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 16:47:20	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:47:21	2	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 16:47:21	2	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 16:47:21	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:47:21	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 16:47:21	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:47:25	2	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 16:47:25	2	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 16:48:25	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:48:25	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:49:21	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:49:25	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:50:22	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:51:25	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 16:51:25	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 16:52:29	2	2151	1024	131.161.83.242	MY_NET.64.26

2001-05-04 16:52:34	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 16:52:43	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 16:52:50	2	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 16:52:51	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 16:53:22	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 16:55:21	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 16:55:21	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 16:56:22	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:12:21	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:12:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:12:25	2	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 17:12:28	2	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 17:12:28	2	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 17:12:33	2	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 17:12:35	2	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 17:12:35	2	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 17:12:38	2	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 17:12:40	2	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 17:12:43	2	2151	1024	209.49.137.10	MY_NET.64.26
2001-05-04 17:12:45	2	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 17:12:45	2	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 17:12:46	2	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 17:12:46	2	2151	1024	24.157.236.160	MY_NET.64.26

2001-05-04 17:12:49	2	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 17:12:51	2	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 17:12:51	2	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 17:12:53	2	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 17:12:54	2	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 17:12:58	2	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 17:20:22	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:20:22	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:21:22	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:22:05	2	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 17:22:06	2	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 17:22:09	2	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 17:22:14	2	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 17:22:15	2	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 17:23:24	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:23:25	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:26:24	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:27:22	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:32:21	2	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 17:35:25	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:35:25	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:37:23	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:39:21	1	2151	1024	198.86.245.21	MY_NET.64.26

2001-05-04 17:41:24	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:42:24	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:42:26	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:43:24	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:44:21	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:47:24	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:47:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:48:20	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:48:21	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:48:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:48:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:48:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:49:21	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:49:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:49:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:49:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:49:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:50:21	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:50:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:50:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:50:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:50:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:51:21	2	2151	1024	199.103.219.200	MY_NET.64.26

2001-05-04 17:51:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:51:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:51:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:52:21	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:52:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:52:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:52:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:52:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:52:25	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:52:27	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:53:21	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:53:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:53:21	1	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 17:53:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:53:22	1	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 17:53:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:53:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:54:21	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:54:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:54:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:54:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:54:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:55:21	2	2151	1024	199.103.219.200	MY_NET.64.26

2001-05-04 17:55:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:55:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:55:23	1	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 17:55:25	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:55:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:56:21	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:56:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:56:22	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:56:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:57:20	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:57:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:57:22	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:57:23	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:57:25	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 17:57:25	1	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 17:58:20	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:58:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:58:21	1	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 17:58:22	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:58:23	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 17:58:24	1	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 17:59:20	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 17:59:20	2	2151	1024	24.176.33.13	MY_NET.64.26

2001-05-04 17:59:21	1	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 17:59:22	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 17:59:22	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 17:59:23	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:02:01	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:02:03	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:02:21	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:02:23	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:02:33	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:10:21	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 18:10:22	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 18:10:22	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 18:10:22	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 18:10:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:10:23	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:10:25	1	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 18:10:25	1	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 18:10:25	1	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 18:10:25	1	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 18:11:20	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:11:20	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:11:21	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:11:21	1	2151	1024	163.26.88.129	MY_NET.64.26

2001-05-04 18:11:22	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 18:11:22	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 18:11:22	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 18:12:02	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:12:04	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:12:20	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:12:20	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:12:21	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:12:22	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:12:23	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 18:12:23	1	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 18:12:24	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 18:12:24	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:12:24	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:12:25	1	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 18:12:25	1	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 18:12:34	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:13:20	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:13:20	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:13:21	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:13:22	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 18:13:23	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:14:20	1	2151	1024	206.47.27.236	MY_NET.64.26

2001-05-04 18:14:20	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:14:21	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:15:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:15:23	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:16:21	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:16:24	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 18:16:24	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:16:24	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 18:17:21	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:17:21	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:17:21	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 18:17:21	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:17:22	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 18:18:22	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 18:18:22	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 18:19:20	1	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 18:19:20	1	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 18:19:20	1	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 18:19:20	1	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 18:19:25	1	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 18:20:20	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:20:20	1	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 18:20:21	1	2151	1024	24.176.33.13	MY_NET.64.26

2001-05-04 18:20:21	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:20:22	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 18:20:22	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:20:22	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 18:20:22	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:20:23	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 18:20:23	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 18:21:24	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 18:22:03	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:22:05	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:22:21	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:22:23	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:22:25	1	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 18:22:25	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:22:25	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 18:22:25	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:22:25	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:22:35	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:22:36	1	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 18:22:44	1	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 18:22:45	1	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 18:23:24	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 18:25:20	1	2151	1024	24.108.77.10	MY_NET.64.26

2001-05-04 18:25:20	1	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 18:26:21	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:26:22	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:26:22	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 18:26:22	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:26:22	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:26:22	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:26:23	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 18:26:25	1	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 18:26:25	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:29:24	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 18:30:25	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:31:25	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 18:31:25	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:32:04	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:32:06	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:32:20	1	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 18:32:20	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:32:20	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 18:32:20	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:32:20	1	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 18:32:24	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:32:26	2	2151	1024	199.103.219.200	MY_NET.64.26

2001-05-04 18:32:36	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:34:22	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:34:22	1	2151	1024	152.101.60.72	MY_NET.64.26
2001-05-04 18:34:22	1	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 18:34:22	1	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 18:34:23	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 18:34:23	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:34:23	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 18:34:23	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:34:23	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:34:24	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 18:34:24	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 18:36:20	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 18:36:22	1	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 18:38:20	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:38:20	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 18:38:20	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:38:21	1	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 18:40:22	1	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 18:40:25	1	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 18:40:25	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 18:42:05	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:42:07	2	2151	1024	65.10.130.173	MY_NET.64.26

2001-05-04 18:42:22	1	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 18:42:22	1	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 18:42:23	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:42:25	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:42:27	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:42:37	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:42:38	1	2151	1024	163.51.63.101	MY_NET.64.26
2001-05-04 18:42:41	1	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 18:43:22	1	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 18:43:25	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 18:43:25	1	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 18:45:20	1	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 18:45:20	1	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 18:45:21	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:45:21	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 18:45:21	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:46:20	1	2151	1024	163.17.123.2	MY_NET.64.26
2001-05-04 18:47:20	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:47:22	1	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 18:49:21	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:49:23	1	2151	1024	24.49.207.210	MY_NET.64.26
2001-05-04 18:49:23	1	2151	1024	209.114.158.7	MY_NET.64.26
2001-05-04 18:49:23	1	2151	1024	152.101.60.72	MY_NET.64.26

2001-05-04 18:49:23	1	2151	1024	216.103.219.35	MY_NET.64.26
2001-05-04 18:49:23	1	2151	1024	24.108.160.123	MY_NET.64.26
2001-05-04 18:50:24	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 18:50:24	1	2151	1024	206.47.27.236	MY_NET.64.26
2001-05-04 18:50:25	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 18:50:25	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:50:25	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 18:50:25	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:51:20	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 18:51:21	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 18:51:21	1	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 18:51:21	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:51:21	1	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 18:51:21	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:52:22	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 18:52:22	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 18:52:22	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 18:53:21	1	2151	1024	209.69.145.112	MY_NET.64.26
2001-05-04 18:53:21	1	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 18:53:21	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 18:53:21	1	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 18:53:21	1	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 18:53:25	1	2151	1024	24.176.33.13	MY_NET.64.26

2001-05-04 18:55:23	1	2151	1024	24.108.77.10	MY_NET.64.26
2001-05-04 18:55:25	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 18:55:25	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 18:55:25	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 18:56:23	1	2151	1024	216.103.89.251	MY_NET.64.26
2001-05-04 18:59:20	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 18:59:20	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 18:59:20	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 18:59:24	1	2151	1024	24.157.236.160	MY_NET.64.26
2001-05-04 18:59:24	1	2151	1024	216.164.64.12	MY_NET.64.26
2001-05-04 19:02:27	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 19:10:20	1	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 19:10:23	1	2151	1024	216.103.109.29	MY_NET.64.26
2001-05-04 19:10:24	1	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 19:10:24	1	2151	1024	216.68.55.83	MY_NET.64.26
2001-05-04 19:11:23	1	2151	1024	216.125.196.12	MY_NET.64.26
2001-05-04 19:11:23	1	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 19:11:23	1	2151	1024	131.161.83.242	MY_NET.64.26
2001-05-04 19:12:21	1	2151	1024	216.101.146.69	MY_NET.64.26
2001-05-04 19:12:21	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 19:12:21	1	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 19:14:21	1	2151	1024	163.10.30.2	MY_NET.64.26
2001-05-04 19:14:21	1	2151	1024	216.101.146.69	MY_NET.64.26

2001-05-04 19:14:21	1	2151	1024	163.26.88.129	MY_NET.64.26
2001-05-04 19:15:21	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 19:15:21	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 19:15:22	1	2151	1024	213.11.168.4	MY_NET.64.26
2001-05-04 19:15:22	1	2151	1024	199.203.94.68	MY_NET.64.26
2001-05-04 19:15:23	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 19:15:23	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 19:15:24	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 19:16:21	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 19:16:21	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 19:16:23	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 19:16:23	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 19:16:24	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 19:17:21	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 19:17:21	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 19:17:24	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 19:17:25	2	2151	1024	198.86.245.21	MY_NET.64.26
2001-05-04 19:18:21	2	2151	1024	24.176.33.13	MY_NET.64.26
2001-05-04 19:18:22	2	2151	1024	65.10.130.173	MY_NET.64.26
2001-05-04 19:18:23	2	2151	1024	209.167.93.30	MY_NET.64.26
2001-05-04 19:18:24	2	2151	1024	199.103.219.200	MY_NET.64.26
2001-05-04 19:22:01	1	2151	1024	209.114.209.6	MY_NET.64.26
2001-05-04 19:22:17	1	2151	1024	163.17.123.2	MY_NET.64.26

2001-05-04 19:32:30	1	2151	1024	63.193.6.62	MY_NET.64.26
2001-05-04 19:32:32	1	2151	1024	216.103.109.29	MY_NET.64.26

Assignment 2

Shadow Security Scanner

The GUI Hacking tool

Introduction

The Internet has changed so many things in our day-to-day lives; it is nearly impossible to conceive of what life was like pre-internet. The sheer volume of information available today is staggering. No longer are we required to go to a library to tap the stores of knowledge. Today, information on any subject is available at the point and click of the mouse via growing broadband technologies. These technologies have allowed users to be continually connected.

With the "always-on" connection, the increasing power of the home desktop machine, and the growing number of people connected to this information "superstore" hackers are sure to be there. The number of hackers/crackers is on the rise, and with the "information sharing" that is occurring, these attackers are arming themselves with more powerful weapons every day. To look for exploitable vulnerabilities, everything from tools that can scan thousands of systems in minutes, to the code used to exploit the vulnerabilities they have discovered, are being used more and more.

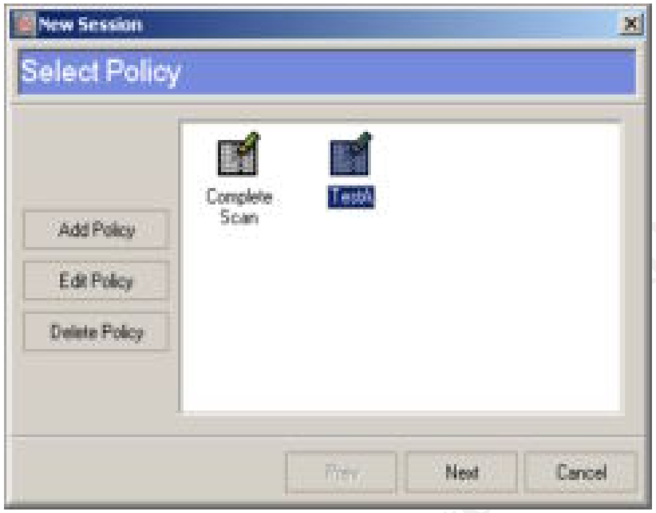
This is largely due to the availability of scripts, or code written to exploit certain vulnerabilities. These scripts are, for the most part, well beyond the understanding of the majority of the attackers using them, also known as “script kiddies”. The attacker merely downloads a piece of code and launches it at a vulnerable system. If the system has countermeasures in place, the attacker may or may not succeed in exploiting the vulnerability. If there are no such countermeasures, (i.e. firewalls TCP wrappers etc.) the attacker more than likely will succeed.

Often these scripts are free and are written for different flavors of Unix systems, due to the backend facilities and command line interface that comes with these operating systems. Typically these tools/scripts are not written for windows, but are ported to the Windows OS as an afterthought. There are a growing number of GUI tools that can be used for security/hacking, Shadow Security Scanner is one of these.

The Shadow Security Scanner (SSS) is a tool I came across a while ago while looking for a good vulnerability assessment tool. SSS is not only a vulnerability assessment tool, but could be called a hacking tool. The interface is straight forward (though it looks suspiciously like Retina from eeye) and easy to use. No cumbersome make files or unfound libraries to deal with. Just download the file and click, click, it is installed and ready to go.

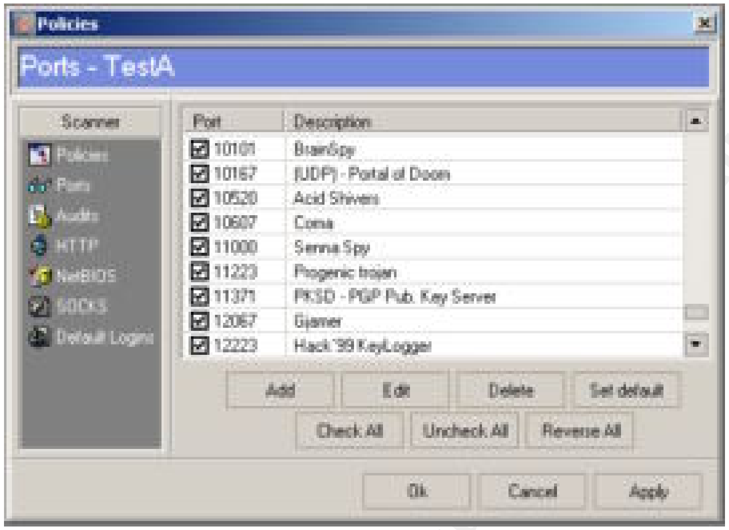
Shadow Interface and Operation

Once the Scanner is installed you merely click on the icon for “new scan session”



You have the choice of using the Default “complete Scan” or creating a new policy. Lets create a new Policy.

By clicking on the different icons in the toolbar we are able to configure SSS to perform a variety of tasks. The ports icon select the port interface in the main window. It has a nice list of both port number and common service associated with the given port number. Ports are selected by checking the box next to the port – service description.



Port	Description
☑ 10101	BrainSpy
☑ 10167	(UDP) - Portal of Doom
☑ 10520	Acid Shivers
☑ 10607	Coma
☑ 11000	Senna Spy
☑ 11223	Progenic trojan
☑ 11371	PKSD - PGP Pub. Key Server
☑ 12067	Gjamer
☑ 12223	Hack'99 KeyLogger

By clicking on the next icon in the toolbar we are able to configure SSS to perform a variety of audits. The audits icon selects the audit interface in the main window; the particular audits, or tests for known vulnerabilities are enabled via the click boxes.

Some of the more noteworthy options are:

DOS checks:

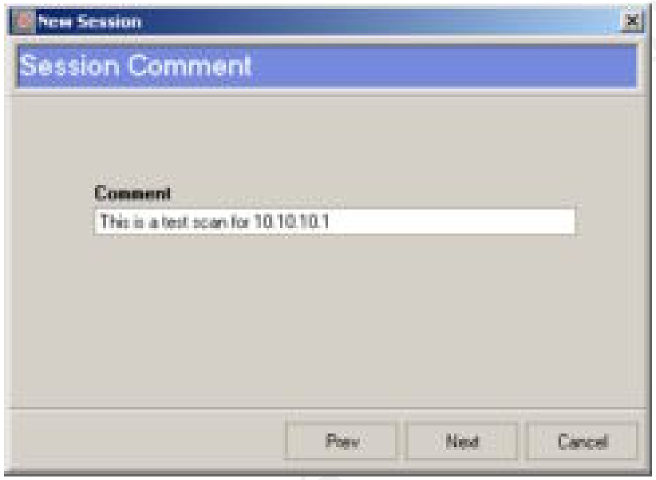
- HTTP
- Pop3
- SMTP
- FTP

These are point and click script exploits for the Overflows associated with the particular service. These are updateable via download.

There is also a password check Available that allows you to specify the targeted service and login and password files to try against the host.

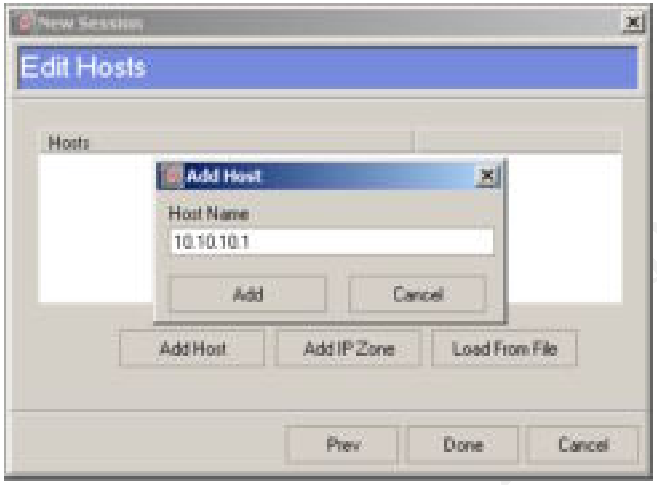
You may continue this process of fine-tuning the policy until you get exactly what you are looking for. Once you configure the policy and click the next button

SSS prompts you for a comment to associate with this session:



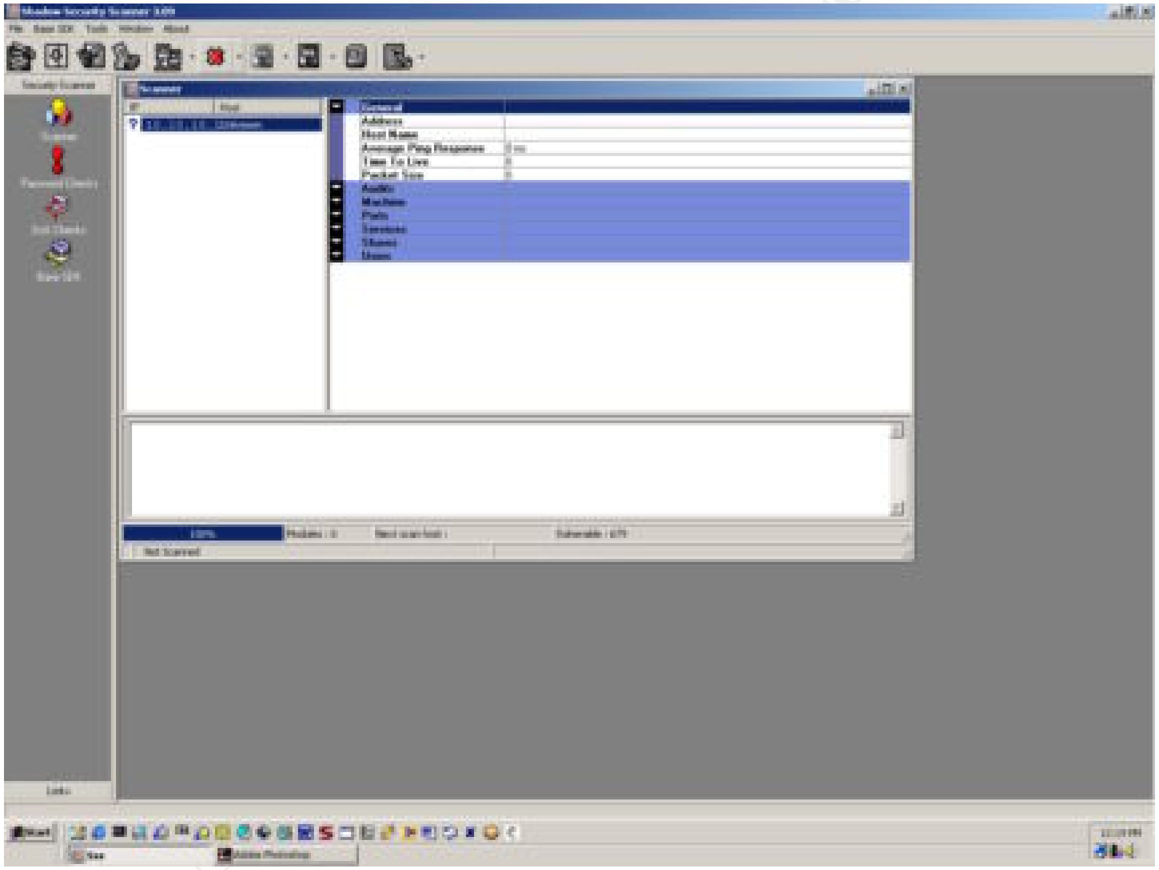
Comment: This is a test scan for 10.10.10.1

SSS asks you for either a specific host to probe or address space to scan. The ability to load a file as input is also available.



Host Name: 10.10.10.1

Once the IP address, or range, is selected the Scanner is ready to go. SSS is flexible in that it can be used to scan a single host, a network subnet, or a group of hosts based on a text file that it can load. All that is left is to click on the start icon.



Address

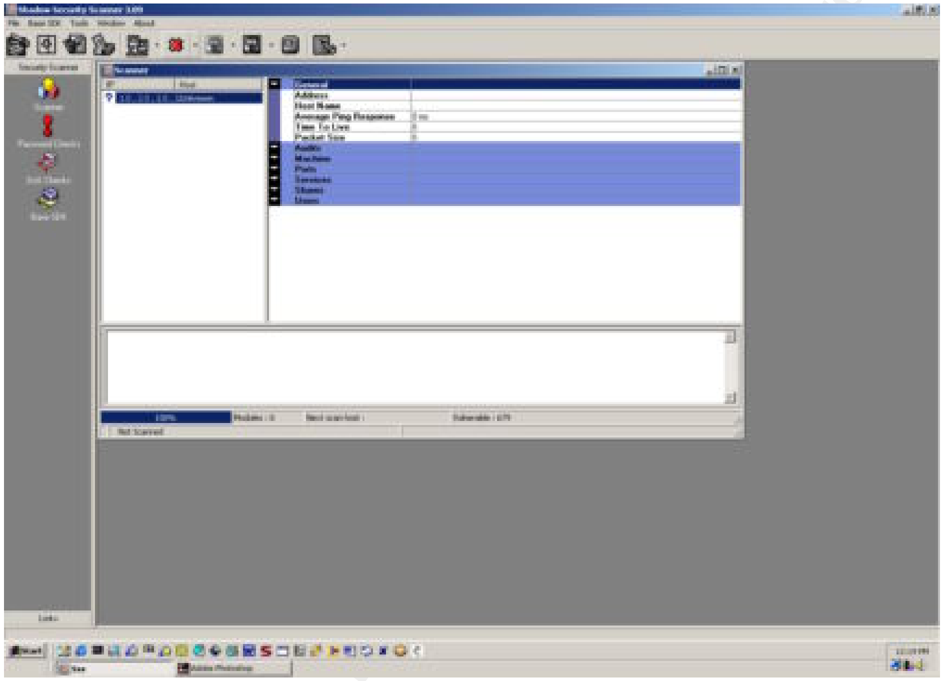
Host Name

Average Ping Response 0 ms

Time To Live 0

Packet Size 0

The true power of SSS is revealed on the completion of the scan, the SSS plug-ins not only check for a port associated with a service during the scan but also test to see if the service expected is there and vulnerable.



Like any of the Vulnerability Scanners SSS produces a reports page (again strangely similar to Retina hmmm…) to detail the open ports and information that it has gleaned from the remote host.

For all of the audits performed it has a definition and the exploit that may be associated with the audit in the lowermost window. Here is where SSS gets a little sinister, when describing the audits and remedies it also includes the exploit. All an attacker must do is click the exploit and SSS executes the code stored in the program. Nice, point and click hacking built in to a vulnerability scanner, what will they think of next. Fortunately or unfortunately, depending on which color hat you wear, the scanner is only available for a 15 day trial, after which time you can either pay $100 for a registration key or $4999 for the full source code. I wonder if any of the money goes to eeye as royalties.

Conclusion

The growth of the Internet has produced both immeasurable rewards and unforeseen consequence. Information is freely available, on nearly everything under the sun. But with freedom comes consequence.

Hacking is becoming easier and easier it doesn't take a knowledgeable person just a web browser pointed to a Google, download the tool of choice, plug in the IP address and start hammering away at the system.

Information flows freely to those that wear White Hats and Black Hats alike. In the early day of the Internet the ability to hack came with a required knowledge of programming. This knowledge is no longer required. Today it is possible to download sophisticated code that does the work for you. As more "tools" like Shadow Security Scanner are made available the job of securing systems and networks will become increasingly difficult.

Assignment 3

1. **Introduction**

   This section is to meet the requirements for the Analyze this section. This is an effort to analyze the170 megabytes of data provided by GIAC Enterprises. The data was gathered from their network using Snort.

2. **Statistics**

Anomalies

There were several anomalies in the data that was provided:

The following files appear to have been altered, or mishandled. As their dates are off in comparison to the rest of the data.

- SnortS27 - Fri Feb 11 00:10:02 2000
- SnortA25 - Sat Feb 12 00:05:02 2000
- UMBCNI3 - Mon Feb 21 00:05:55 2000
- UMBCNI4 - Mon Feb 21 00:10:02 2000
- UMBCNI5 - Mon Feb 21 00:05:01 2000
- UMBCNI32 - Thu Mar 9 00:05:04 2000
- UMBCNI34 - Thu Mar 9 00:10:01 2000
- OOSche4- Fri Feb 2

Additionally the following files were duplicate of each other

- SnortA35 - Wed Feb 7 00:05:02 2001
- SnortA36 - Wed Feb 7 00:05:02 2001

Source of Common Port Connects

21	File Transfer - 14843
22	SSH Remote Login Protocol - 1
23	Telnet – 73
111	Sun Remote Procedure Call – 4

Analysis Tools

Due To the large volume of data, SnortSnarf and Snort_Sort were employed to assist in the correlation and analysis. Additionally a custom script was used to sort the data.

```
!/usr/local/bin/perl
open (SMALLFILE, "$smallfile");
        @ports = <SMALLFILE>;
close SMALLFILE;
foreach $port (@ports) {
        chomp $port;
        chop $port;
        if ($port =~ s/^(.*?)\s(\d*?)\/(\S*?)\s*?((\S).*?)$/$2 $3 $4/) {
print "$port\n";
        $port[$2]{protocol} = $3;
        $port[$2]{tag} = $4;
        }
}
open (BIGFILE, "$bigfile");
while (<BIGFILE>) {
        $line = <BIGFILE>;
        chomp $line;
        chop $line;
        my ($month,$day,$time,$sipport,$arrow,$tipport,$proto) = split (/ | /,
$line, 7);
        my ($sip,$sport) = split (/:/, $sipport);
        my ($tip,$tport) = split (/:/, $tipport);
        if ($proto =~ /$port[$tport]{protocol}/i) {
                $tag = $port[$tport]{tag};
        }
        else {
                $tag = "$port[$tport]{protocol} $port[$tport]{tag}";
        }
#       open (PORTOUT, ">>$source_path/srcport.txt");
#               print PORTOUT "$line -- $tag\n";
#       close PORTOUT;
   close PORTOUT;
        chmod 0777, "$target_path/destport.txt";
}
close BIGFILE;
```

Analysis

Sorted Snort Alerts

(note everything that was MY.NET is now 333.333.x.x)

Tiny Fragments - Possible Hostile Activity

The concept here is that no commercial network equipment that I've ever heard of fragments their traffic to less than 256 bytes, and so anything you see below that threshold value is probably *very* suspicious. FYI, nmap and fragrouter fragment to either 8 or 24 byte fragments. Judging by the volume of alerts you're seeing here, you're either under attack or something is broken.

Sources triggering this attack signature (top 2 offenders)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.89.165.5	116	116	1	1
64.80.90.36	73	73	2	2

We are seeing several connects from a few ip's that triggered this alert.

```
03/06-01:35:45.983271 [**] Tiny Fragments - Possible Hostile Activity [**] 212.89.165.5 -> 333.333.223.42
```

Thru

```
03/06-01:39:16.106940 [**] Tiny Fragments - Possible Hostile Activity [**] 212.89.165.5 -> 333.333.223.42
```

Roughly, every 2 secs 3 or more fragments would come in from the 64.80.90.36 address.

```
03/06-01:35:45.983271 [**] Tiny Fragments - Possible Hostile Activity [**] 212.89.165.5 -> 333.333.223.42
```

Thru

```
03/06-01:38:40.515858 [**] Tiny Fragments - Possible Hostile Activity [**] 212.89.165.5 -> 333.333.223.42
```

a series of connects that where anywhere from .5secs to 4secs apart.

These are possible attacks.

TCP SMTP Source Port traffic

There is a distinct possibility that this is normal traffic. It would greatly depend on our network and what we where allowing in there. The source addresses show only 4 connections to this port. If we know who and what these addresses are then we have little to really worry about. However, if these are unknown sources we may want to pay a little more attention to our mail servers.

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
200.251.185.30	1	1	1	1
17.135.218.56	1	1	1	1
11.125.218.156	1	1	1	1
195.211.49.18	1	1	1	1

If we look more into the destination of these scans we need to ask ourselves two questions; "Do these machines run the SMTP service?" and "Do they need to?" If our the answer to the 1st question is **Yes** and the second is **No** then we need to remove that service and ascertain what else we don't need there. If the answer is **YES** and **YES** then we need to check these machines for evidence of intrusion and assess their level of security.

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
333.333.60.17	2	24	2	23
333.333.158.238	1	2	1	2
333.333.139.54	1	1	1	1

ICMP SRC and DST outside network

If we look into the sources of these alerts we will notice that the majority of the IP's only triggered the alert once or twice. That would lead us to believe that, though they are bound for our network, they might not have been intended for our network. The largest perpetrators of this signature are 10 net addresses. This may mean that someone has incorrectly setup a NAT box with-in our network or that we have a misconfigured router somewhere that is forwarding that traffic. As a general rule 10 neted traffic should not be passed by the router.

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
10.0.0.1	31	31	2	2
10.3.41.11	26	45	1	6
128.249.101.1	8	8	1	1

128.249.104.1	6	6	1	1
128.249.98.1	4	4	1	1
10.10.5.3	3	7	1	3
172.128.235.48	2	2	1	1
140.120.80.254	2	2	1	1
172.128.249.145	2	3	2	3
172.158.83.255	2	2	1	1
217.9.64.248	2	2	1	1
172.158.126.71	2	2	1	1
140.120.93.254	2	2	1	1
172.174.12.110	2	2	1	1
65.9.177.76	1	10	1	4
172.128.122.7	1	1	1	1
172.159.72.255	1	1	1	1
172.167.26.248	1	1	1	1
172.182.21.112	1	2	1	2
172.140.134.18	1	1	1	1

172.128.196.159	1	1	1	1
172.158.121.214	1	1	1	1
172.167.120.189	1	1	1	1
140.120.29.254	1	1	1	1

We should also pay attention to:

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
65.9.177.76	1	10	1	4

due to the "# Alerts (total)" field. This address also triggered the " TCP SRC and DST outside network " alert.

02/11-16:59:09.397549 [**] TCP SRC and DST outside network [**] 65.9.177.76:2265 -> 208.184.216.22:8888
02/11-17:05:03.505670 [**] ICMP SRC and DST outside network [**] 65.9.177.76 -> 172.168.69.200

We may want to find out why we are seeing this address within our network. Please reference the next section for more information on this IP.

TCP SRC and DST outside network

Sources triggering this attack signature (top 6 offenders)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
127.0.0.1	2236	2237	1	2
169.254.101.152	49	49	28	28

192.168.1.51	22	22	12	12
10.3.41.11	19	45	5	6
0.0.0.0	17	17	9	9
65.9.177.76	9	10	3	4

Our main source of this alert happens to be the machine the was capturing the data, or we are again allowing traffic into our network that should NEVER be loud in. However, this is what we are seeing:

```
02/20-03:13:22.022820 [**] TCP SRC and DST outside network [**] 127.0.0.1:110 -> 1.1.1.1:18539
02/20-03:13:22.022820 [**] TCP SRC and DST outside network [**] 127.0.0.1:110 -> 1.1.1.1:18539
02/20-03:13:22.024137 [**] TCP SRC and DST outside network [**] 127.0.0.1:115 -> 1.1.1.1:18544
02/20-03:13:22.024137 [**] TCP SRC and DST outside network [**] 127.0.0.1:115 -> 1.1.1.1:18544
02/20-03:13:22.027876 [**] TCP SRC and DST outside network [**] 127.0.0.1:128 -> 1.1.1.1:18557
02/20-03:13:22.027876 [**] TCP SRC and DST outside network [**] 127.0.0.1:128 -> 1.1.1.1:18557
02/20-03:13:22.027923 [**] TCP SRC and DST outside network [**] 127.0.0.1:129 -> 1.1.1.1:18558
02/20-03:13:22.027923 [**] TCP SRC and DST outside network [**] 127.0.0.1:129 -> 1.1.1.1:18558
```

Notice the source ports. They are incrementing per every connection made to IP 1.1.1.1. If we look through the data more thoroughly we will notice that the source port starts to become more selected as opposed to incrementing.

```
02/24-18:16:53.400791 [**] TCP SRC and DST outside network [**] 127.0.0.1:7777 -> 1.1.1.1:6332
```

```
02/24-18:16:53.400838 [**] TCP SRC and DST outside network [**] 127.0.0.1:7789 -> 1.1.1.1:6333
02/24-18:16:53.403458 [**] TCP SRC and DST outside network [**] 127.0.0.1:8888 -> 1.1.1.1:6342
02/24-18:16:53.408355 [**] TCP SRC and DST outside network [**] 127.0.0.1:9999 -> 1.1.1.1:6359
02/24-18:16:53.408466 [**] TCP SRC and DST outside network [**] 127.0.0.1:10005 -> 1.1.1.1:6360
02/24-18:16:53.408780 [**] TCP SRC and DST outside network [**] 127.0.0.1:10080 -> 1.1.1.1:6362
02/24-18:16:53.408825 [**] TCP SRC and DST outside network [**] 127.0.0.1:10082 -> 1.1.1.1:6363
02/24-18:16:53.412884 [**] TCP SRC and DST outside network [**] 127.0.0.1:12345 -> 1.1.1.1:6374
```

The address space for 1.1.1.1 is reserved by IANA so this traffic definitely deserves a closer look.

Now lets look at some other traffic that just doesn't make a lot of sense. The only legitimate reason that I can think of to have a source port of 0.0.0.0 is when using DHCP and if we are trying to receive DHCP addresses from outside of our network then we need to establish why. But more importantly, lets look at where these packets are going. The destination port for these packets all seems to have a use in everyday life. Leading us to believe that maybe this traffic is crafted for a specific purpose.

The destination ports 5190 are used by AOL.
The destination ports 1029 are used by Microsoft for internal commication or has also been used as a port for an ICQ Trojan.
The destination ports 1034 are used by Microsoft for internal communication.
The destination ports 6688 seems to be unassigned however it has been seen in use by Nmap.
The destination ports 6699 seems to be unassigned however it has been seen in use by Nmap.

```
01/30-18:09:50.215686 [**] TCP SRC and DST outside network [**] 0.0.0.0:1543 -> 64.12.24.228:5190
```

```
02/04-22:35:02.935504 [**] TCP SRC and DST outside network [**] 0.0.0.0:1030 -> 64.12.24.229:5190
02/06-00:25:30.113493 [**] TCP SRC and DST outside network [**] 0.0.0.0:2489 -> 205.188.6.217:5190
02/06-00:25:30.113493 [**] TCP SRC and DST outside network [**] 0.0.0.0:2489 -> 205.188.6.217:5190
02/06-01:24:28.317096 [**] TCP SRC and DST outside network [**] 0.0.0.0:2489 -> 205.188.6.217:5190
02/06-01:24:28.317096 [**] TCP SRC and DST outside network [**] 0.0.0.0:2489 -> 205.188.6.217:5190
02/20-01:33:01.689835 [**] TCP SRC and DST outside network [**] 0.0.0.0:2978 -> 24.9.220.69:1029
02/20-01:33:01.689835 [**] TCP SRC and DST outside network [**] 0.0.0.0:2978 -> 24.9.220.69:1029
02/20-09:42:00.740454 [**] TCP SRC and DST outside network [**] 0.0.0.0:3343 -> 24.9.220.69:1034
02/20-09:42:00.740454 [**] TCP SRC and DST outside network [**] 0.0.0.0:3343 -> 24.9.220.69:1034
02/20-09:42:03.485905 [**] TCP SRC and DST outside network [**] 0.0.0.0:3343 -> 24.9.220.69:1034
02/20-09:42:03.485905 [**] TCP SRC and DST outside network [**] 0.0.0.0:3343 -> 24.9.220.69:1034
02/23-21:32:11.302188 [**] TCP SRC and DST outside network [**] 0.0.0.0:1091 -> 64.12.25.101:8633
02/24-23:42:10.534096 [**] TCP SRC and DST outside network [**] 0.0.0.0:3206 -> 65.4.225.188:6688
02/24-23:42:10.534260 [**] TCP SRC and DST outside network [**] 0.0.0.0:3205 -> 24.153.20.112:6699
02/25-14:44:10.389478 [**] TCP SRC and DST outside network [**] 0.0.0.0:1626 -> 24.88.51.246:1615
03/06-01:30:09.044119 [**] TCP SRC and DST outside network [**] 0.0.0.0:2652 -> 64.12.24.71:5190
```

SNMP public access

This alert triggers when a sting of public is seen a UDP packet with the source or destination port set 161. SNMP is quite possibly one of the largest holes in systems today. This is do to the default read and write strings being set to PUBLIC and PRIVATE. The PRIVATE community string name gives complete (root) access to a system and (in version 1) is passed in clear text. The PUBLIC community string name is a read only community string name that can be used to obtain valuable information concerning the system. The main offenders of this alert are usually prints but when this is seen it is likely that the PRIVATE community string name is also in use. If this is seen by an analyst they should find that machine and change to community string name to a more difficult password to guess. However, because this is passed in the clear across the network we also suggest that (if possible) they upgrade to SNMP version 2 or 3, which provides encryption.
Their has also been several exploits recently released for SNMP on Solaris systems and should be removed before the box is put on the network, if the service is not absolutely necessary.

Signature	# Alerts	# Sources	# Destinations
SNMP public access	1163	4	8

Watchlist 000220 IL-ISDNNET-990517

The Watchlist is a network that has been known for “not happy” activity and it is recommended that we watch for any traffic for it.

Watchlist 000220 IL-ISDNNET-990517	53 sources	78 destinations

We do seem to have some traffic coming from that network and should check the destination addresses for intrusion attempts.

When looking at the traffic we notice that the destination port is 6699 and 6688. Which could be Nmap or could be a Trojan installed on the system. At any rate it is defiantly worth a look

```
02/06-06:15:06.263423 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.21.179:1172 -> 333.333.207.226:6699
02/06-06:15:06.263423 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.21.179:1172 -> 333.333.207.226:6699
```

```
03/10-19:08:35.786696 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.41.169:1113 -> 333.333.213.250:6688
03/10-19:08:37.412848 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.41.169:1113 ->
```

Sources triggering this attack signature (top 5 offenders)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
212.179.21.179	4372	4372	1	1
212.179.41.169	4061	4061	1	1
212.179.79.2	2446	2446	20	20
212.179.33.82	1599	1599	1	1
212.179.125.114	1444	1444	2	2

Queso fingerprint

Queso fingerprint	58 sources	112 destinations

If we look at the packet trace from a Queso scan we will see that the packet has the S*****21 tcp options set and the TTL set to 255.

This is an indication that someone is trying to ascertain the type of operating system that is being used on a system. We should harden the security on those systems and put some of the higher offenders on a watch list:

Sources triggering this attack signature (top 5 offenders)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
194.51.109.194	66	66	5	5
141.30.228.122	38	38	8	8
209.85.60.183	31	31	1	1
141.30.228.134	30	30	7	7
141.30.228.43	30	30	14	14

Null scan!

Null scan!	118 sources	90 destinations

A null scan is another way to establish the type of OS. Different Operation Systems, or OS's, will respond differently. This should be treated similarly to the Queso scan.

Back Orifice

Back Orifice	2 sources	25 destinations

Back Orifice is a “Remote Management Tool” also known as a Trojan. It is currently a window specific Trojan so if the destination machines are not windows machine you are usually safe however a look to see if perhaps another Trojan is running might not be a bad idea. The port that BO listens on is 31337 and in more recent versions is configurable. However, 31337 in haxr is equal to the word ELEET or elite.

```
03/07-08:49:31.283316 [**] Back Orifice [**] 203.170.152.87:31338 -> 333.333.98.23:31337
03/07-08:49:31.349034 [**] Back Orifice [**] 203.170.152.87:31338 -> 333.333.98.35:31337
```

PORTSCAN DETECTED

Various port scans have been detected and those machines should be looked at to see if they have been compromised or if our users are not being good neighbors.

- 02/11-00:16:53.229628 from MY.NET.219.70 (THRESHOLD 7 connections in 2 seconds)
- 02/11-00:17:54.992891 from MY.NET.140.21 (THRESHOLD 7 connections in 2 seconds)
- 02/11-00:24:03.090831 from MY.NET.208.26 (THRESHOLD 7 connections in 2 seconds)
- 02/11-00:33:08.221227 from MY.NET.208.26 (THRESHOLD 7 connections in 2 seconds)
- 02/11-00:34:23.701732 from MY.NET.209.238 (THRESHOLD 7 connections in 2 seconds)
- 02/11-00:36:09.537703 from MY.NET.70.177 (THRESHOLD 7 connections in 2 seconds)
- 02/11-00:39:19.188679 from 134.109.185.77 (STEALTH)
- 02/11-00:46:06.636531 from MY.NET.208.26 (THRESHOLD 7 connections in 2 seconds)
- 02/11-01:01:14.635675 from MY.NET.208.26 (THRESHOLD 7 connections in 2 seconds)
- 02/11-01:04:37.050138 from MY.NET.202.254 (THRESHOLD 7 connections in 2 seconds)

portscan status

Similar to the PORTSCAN DETECTED we need to look into these machines to establish why they are scanning and if it is for a legitimate purpose.

- 02/11-00:34:18.996716 from MY.NET.208.26: 6 connections across 6 hosts: TCP(0), UDP(6)
- 02/11-00:34:21.060415 from MY.NET.208.26: 4 connections across 4 hosts: TCP(0), UDP(4)
- 02/11-00:34:23.280016 from MY.NET.208.26: 5 connections across 5 hosts: TCP(0), UDP(5)
- 02/11-00:34:25.103806 from MY.NET.208.26: 6 connections across 6 hosts: TCP(0), UDP(6)
- 02/11-00:34:25.117296 from MY.NET.209.238: 25 connections across 24 hosts: TCP(0), UDP(25)

SITE EXEC - Possible wu-ftpd exploit - GIAC000623

SITE EXEC - Possible wu-ftpd exploit - GIAC000623	1 sources	1 destinations

This trigger is tell you to get off your can and go check your machine!!!
If we check the Destination machine it is very likely that (if we had no prior security) that this machine has been comprised

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
128.61.136.233	1	1159	1	1159

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
333.333.219.22	1	2	1	2

We should also notice that the offending machine has been seen in several of alerts (1159) and defiantly needs to be put on a watchlist.

SYN-FIN scan!

SYN-FIN scan!	9 sources	10346 destinations

It looks as though 3 machines have been doing some very active OS finger printing on our network.

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
130.234.184.112	9336	9336	8681	8681
211.248.112.67	2216	2216	1108	1108
128.61.136.233	1158	1159	1158	1159

You may also notice our friend that appeared in the previous alert. 128.61.136.233

SMB Name Wildcard

SMB Name Wildcard	307 sources	425 destinations

The SMB wildcard is a simple detect that can also be normal traffic when seem on the internal network. However, if seen from external connections that we have not allowed to connect via NETBIOS then we may have a problem. NETBIOS should NEVER be aloud outside of your network. If you don't believe me, just ask MICROSOFT. They suggest "Strong Perimiter Defense" when designing your MS Network.

```
02/20-10:16:43.820533 [**] SMB Name Wildcard [**] 165.230.77.89:137 -> 333.333.130.185:137
02/20-10:16:43.820533 [**] SMB Name Wildcard [**] 165.230.77.89:137 -> 333.333.130.185:137
02/20-10:55:45.316778 [**] SMB Name Wildcard [**] 165.230.77.89:137 -> 333.333.130.185:137
```

STATDX UDP attack

STATDX UDP attack	2 sources	8 destinations

Statd is a UNIX RPC service that has a great deal of vulnerabilities attached to it. We should immediately check into any UNIX system that matches the destination and apply TCP_Wrappers to those machine in order to disallow those services.

```
02/20-19:41:05.730067 [**] External RPC call [**] 171.65.61.201:1464 -> 333.333.1.15:111
02/20-19:41:05.730067 [**] External RPC call [**] 171.65.61.201:1464 -> 333.333.1.15:111
02/20-19:41:05.731385 [**] External RPC call [**] 171.65.61.201:1462 -> 333.333.1.13:111
```

WinGate 1080 Attempt

WinGate 1080 Attempt	105 sources	229 destinations

These are simply proxy server scans. However, since many of these scans come from outside our network it is important that we check our proxy servers to see if they are allowing relaying. Proxy servers are a commodity in the attacker would as they provide an means of hiding from the destination .

Sources triggering this attack signature (top 3 offenders)

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
199.173.178.2	185	185	32	32
204.117.70.5	51	51	15	15

63.53.52.128	47	47	45	45

External RPC call

External RPC call	4 sources	1466 destinations

From this information we can see 2 hosts that have been doing a great deal of recognizance on our network. We should add these networks to our watch list or block them via the router.

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
171.65.61.201	2534	2548	1225	1230
129.105.107.190	490	492	242	242
209.88.124.3	4	4	4	4
199.174.56.66	1	1	1	1

SUNRPC highport access!

SUNRPC highport access!	7 sources	7 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.9.158.233	197	197	1	1
333.333.70.38	4	7197	1	3814

Possible RAMEN server activity

There is a great deal of Ramen activity on our network. We should look into these machines and try to establish if they are running a Linux system and have been compromised.

Possible RAMEN server activity	2346 sources	5067 destinations

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
24.67.186.244	2438	2438	2414	2414
24.48.226.183	1819	1819	1809	1809
128.138.2.112	728	728	1	1
333.333.201.146	553	553	1	1
333.333.253.12	530	530	530	530
333.333.97.154	330	330	234	234
333.333.60.11	326	326	2	2

148.129.143.2	210	210	1	1

connect to 515 from inside

connect to 515 from inside	6 sources	5 destinations

Recently their have been several exploits for the LPD service we should block this at the router and check into the destination systems to see if they have been compromised.

Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
333.333.98.190	514	514	1	1
333.333.97.88	118	118	1	1
333.333.7.20	15	15	1	1
333.333.179.78	1	3	1	3
333.333.162.71	1	1	1	1
333.333.201.170	1	1	1	1

Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
216.181.129.185	632	632	2	2

216.88.97.58	15	15	1	1
209.50.66.2	1	1	1	1
24.13.123.8	1	1	1	1
209.249.182.79	1	1	1	1