Global Information Assurance Certification Paper

SANS
GCIA Certification Practical
Version 2.9

Ryan A. Quan
July 2001

Table of Contents

Assignment 1 – Network Detects (5)

Network Detect #1 Analysis

Apr 14 06:25:54 63.80.245.138:4708 -> a.b.c.9:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4719 -> a.b.c.20:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4725 -> a.b.c.26:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4729 -> a.b.c.30:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4732 -> a.b.c.33:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4749 -> a.b.c.50:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4750 -> a.b.c.51:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4770 -> a.b.c.71:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4771 -> a.b.c.72:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4779 -> a.b.c.80:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4781 -> a.b.c.82:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4800 -> a.b.c.101:53 SYN ******S*
Apr 14 06:25:52 63.80.245.138:4802 -> a.b.c.103:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:4813 -> a.b.c.114:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:4820 -> a.b.c.121:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:4826 -> a.b.c.127:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:4891 -> a.b.c.192:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:4894 -> a.b.c.195:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:4906 -> a.b.c.207:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:4924 -> a.b.c.225:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:1282 -> a.b.c.225:53 UDP
Apr 14 06:25:53 63.80.245.138:4943 -> a.b.c.244:53 SYN ******S*
Apr 14 06:25:53 63.80.245.138:1030 -> a.b.d.52:53 SYN ******S*

Apr 14 06:25:53 hostka named[17373]: security: notice: denied query from [63.80.245.138].1282 for "VERSION.BIND"
Apr 14 06:25:13 hosth /kernel: Connection attempt to TCP a.b.c.62:53 from 63.80.245.138:4761
Apr 14 06:25:53 hostka named[17373]: security: notice: denied query from [63.80.245.138].1282 for "VERSION.BIND"
Apr 14 06:25:53 hostka snort: DNS named version attempt: 63.80.245.138:1282 -> a.b.c.225:53

Source of Trace:
The GIAC URL: http://www.sans.org/y2k/042401.htm

Detect was generated by:
The above detect was generated from Snort IDS program.

Probability the source address was spoofed:

It is highly unlikely that the source IP was spoofed. A typical 3-way handshake requires a SYN, SYN-ACK, and ACK before any data can be transferred. So, if the IP was indeed spoofed there would be no way that the handshake could be completed, thus the attacker would not be able to gather information from the targeted hosts for any attacks. The attacker hijack a 3rd party machine to launch the SYN scan, but probably unlikely.

Description of attack:

This piece of a log generated from Snort shows that a Source host from IP 63.80.245.138 was sending SYN packets to a range of IP addresses directed at port 53. The attacker is sending SYN packets and awaiting a SYN-ACK from a destination machine, which would indicate to the attacker that a machine is running DNS services on port 53. The attacker would then attempt query the DNS server for which BIND version it was running. From this information, the attacker can then choose which BIND exploit to use. It usually involves a Denial of Service or a root privilege exploit.

CVE Reference Numbers
CVE-1999-0009
CVE-1999-0010
CVE-1999-0011
Note: There are a total of 20 CVE entries listed for BIND, and for space considerations, the others are referenced below:
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=BIND

Attack mechanism:

The attacker is looking for machines that are running BIND DNS services (port 53). If a machine would reply with a SYN-ACK, the attacker would then know that the machine is indeed a DNS server or running something on port 53. Then if a machine responds, query for which version of BIND it was running by an inverse DNS query and then according to which version, run an exploit against the machine in order to compromise it or create a Denial of Service attack. This can also reveal hostnames and IP addresses through a DNS zone transfer for possible future attacks. The Denial of Service would cripple the machine so no one would be able to access it. While gaining root access would allow a hacker to possibly place a Trojan on the machine or actually change the DNS entries on the machine so that it would redirect people accessing web sites for instance to another web server.

Correlations:

This particular attack is very common according to the numerous entries on the GIAC website submitted using SYN scanning for DNS servers. The BIND exploit is listed as the number 1 on SANS top 10 Internet security threat page. (http://www.sans.org/topten.htm)
Laurie@.edu also reported similar traffic toward port 53 on an almost weekly basis. One example is listed at http://www.sans.org/y2k/042401.htm

Evidence of active targeting:

Yes. The attacker is trying or connecting to machines where service port 53 is open. The attacker knows exactly what to look for, in this case, DNS servers.

Severity:
The formula used to rank the severity of the incident is given below:

(Criticality + Lethality) - (System countermeasures + Network countermeasures)

Each element is ranked 1 to 5, 1 being low, 5 being high. The maximum score, i.e. the worst-case scenario, is 8. The minimum score, i.e. the best-case scenario, is -8.

Criticality = 5. Assuming that the targeted machines are actually DNS servers running BIND.
Lethality = 5. The attacker would have root access or be able to take down the machine through a Denial of Service.

System countermeasures = 4. Unknown if latest patches are in place. BIND version query was blocked.
Network countermeasures = 3. No blocking of port 53 at the firewall, but a Snort IDS was in place.

Thus, severity = (5 + 5) - (4 + 3) = **3**.

Defensive recommendation:
Blocking the BIND version request is a good start. Going by the Snort detect along is not enough information to determine if the targeted machines were in fact compromised in any other way. You would also need to monitor all firewall and router logs for traffic directed at those targeted machines. I would also configure the router to silently drop any ICMP packets directed at those machines in order to prevent anyone enumerating the hosts which would then lead to SYN scanning of open service port 53. Restrict any zone transfer requests to untrusted hosts. If the machines do in fact need to run DNS services, then I would definitely setup something other then Snort. A good choice would be tcpdump with filters to capture the traffic both ways, in order to determine if the targeted machine was responding to any stimulus from that attacker. Be sure all the latest patches and fixes are applied as well.

Multiple choice test question:
The above detect appears to be a?

a) A failed DNS zone transfer.
b) DNS BIND exploit attempt.
c) The famous "Mitnick DNS Attack".
d) None of the above.

Answer: b

Network Detect #2 Analysis

[**] spp_http_decode: IIS Unicode attack detected [**]
04/12-05:44:29.537613 213.121.247.193:61522 -> x.x.x.23:80
TCP TTL:41 TOS:0x0 ID:2938 IpLen:20 DgmLen:289 DF
AP Seq: 0xEF818D34 Ack: 0x844F3E92 Win: 0x7D78 TcpLen: 32
TCP Options (3) => NOP NOP TS: 15433327 0

```
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E 25 63 30  GET /msadc/..%c0
25 61 66 2E 2E 2F 2E 2E 25 63 30 25 61 66 2E 2E  %af../..%c0%af..
2F 2E 2E 25 63 30 25 61 66 2E 2E 2F 77 69 6E 6E  /..%c0%af../winn
74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65  t/system32/cmd.e
78 65 3F 2F 63 2B 64 69 72 2B 63 3A 5C 20 48 54  xe?/c+dir+c:\ HT
54 50 2F 31 2E 30 0D 0A 56 69 61 3A 20 31 2E 30  TP/1.0..Via: 1.0
20 50 72 6F 78 79 3A 33 31 32 38 20 28 53 71 75   Proxy:3128 (Squ
69 64 2F 32 2E 33 2E 53 54 41 42 4C 45 31 29 0D  id/2.3.STABLE1).
0A 58 2D 46 6F 72 77 61 72 64 65 64 2D 46 6F 72  .X-Forwarded-For
3A 20 36 32 2E 34 31 2E 33 38 2E 31 30 0D 0A 48  : 62.41.38.10..H
6F 73 74 3A 20 31 34 30 2E 31 37 38 2E 33 33 2E  ost: x.x.x.
32 33 0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F  23..Cache-Contro
6C 3A 20 6D 61 78 2D 61 67 65 3D 32 35 39 32 30  l: max-age=25920
30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B  0..Connection: k
65 65 70 2D 61 6C 69 76 65 0D 0A 0D 0A           eep-alive....

[**] spp_http_decode: IIS Unicode attack detected [**]
04/12-05:44:29.589223 213.121.247.193:61528 -> x.x.x.23:80
TCP TTL:39 TOS:0x0 ID:2943 IpLen:20 DgmLen:292 DF
***AP*** Seq: 0xEFCCA502  Ack: 0x8450CA83  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 15433329 0
47 45 54 20 2F 5F 76 74 69 5F 62 69 6E 2F 2E 2E  GET /_vti_bin/..
25 63 30 25 61 66 2E 2E 2F 2E 2E 25 63 30 25 61  %c0%af../..%c0%a
66 2E 2E 2F 2E 2E 25 63 30 25 61 66 2E 2E 2F 77  f../..%c0%af../w
69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 6D  innt/system32/cm
64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A 5C  d.exe?/c+dir+c:\
20 48 54 54 50 2F 31 2E 30 0D 0A 56 69 61 3A 20   HTTP/1.0..Via:
31 2E 30 20 50 72 6F 78 79 3A 33 31 32 38 20 28  1.0 Proxy:3128 (
53 71 75 69 64 2F 32 2E 33 2E 53 54 41 42 4C 45  Squid/2.3.STABLE
31 29 0D 0A 58 2D 46 6F 72 77 61 72 64 65 64 2D  1)..X-Forwarded-
46 6F 72 3A 20 36 32 2E 34 31 2E 33 38 2E 31 30  For: 62.41.38.10
0D 0A 48 6F 73 74 3A 20 31 34 30 2E 31 37 38 2E  ..Host: x.x.
33 33 2E 32 33 0D 0A 43 61 63 68 65 2D 43 6F 6E  x.23..Cache-Con
74 72 6F 6C 3A 20 6D 61 78 2D 61 67 65 3D 32 35  trol: max-age=25
39 32 30 30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E  9200..Connection
3A 20 6B 65 65 70 2D 61 6C 69 76 65 0D 0A 0D 0A  : keep-alive....

[**] spp_http_decode: IIS Unicode attack detected [**]
04/12-05:44:30.335189 213.121.247.193:61550 -> x.x.x.23:80
TCP TTL:41 TOS:0x0 ID:3033 IpLen:20 DgmLen:296 DF
***AP*** Seq: 0xEFD1578B  Ack: 0x84617566  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 15433377 0
47 45 54 20 2F 69 69 73 61 64 6D 70 77 64 2F 2E  GET /iisadmpwd/.
2E 25 63 30 25 61 66 2E 2E 2F 2E 2E 25 63 30 25  .%c0%af../..%c0%
61 66 2E 2E 2F 2E 2E 25 63 30 25 61 66 2E 2E 2F  af../..%c0%af../
77 69 6E 6E 74 33 35 31 2F 73 79 73 74 65 6D 33  winnt351/system3
```

```
32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72  2/cmd.exe?/c+dir
2B 63 3A 5C 20 48 54 54 50 2F 31 2E 30 0D 0A 56  +c:\ HTTP/1.0..V
69 61 3A 20 31 2E 30 20 50 72 6F 78 79 3A 33 31  ia: 1.0 Proxy:31
32 38 20 28 53 71 75 69 64 2F 32 2E 33 2E 53 54  28 (Squid/2.3.ST
41 42 4C 45 31 29 0D 0A 58 2D 46 6F 72 77 61 72  ABLE1)..X-Forwar
64 65 64 2D 46 6F 72 3A 20 36 32 2E 34 31 2E 33  ded-For: 62.41.3
38 2E 31 30 0D 0A 48 6F 73 74 3A 20 31 34 30 2E  8.10..Host: x.
31 37 38 2E 33 33 2E 32 33 0D 0A 43 61 63 68 65  x.x.23..Cache
2D 43 6F 6E 74 72 6F 6C 3A 20 6D 61 78 2D 61 67  -Control: max-ag
65 3D 32 35 39 32 30 30 0D 0A 43 6F 6E 6E 65 63  e=259200..Connec
74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65  tion: keep-alive
0D 0A 0D 0A                                      ....
```

Source of Trace:

The GIAC URL: http://www.sans.org/y2k/041901.htm

Detect was generated by:

The above detect was generated from Snort IDS

Probability the source address was spoofed:

It is highly unlikely that the source IP was spoofed. The attacking machine 213.121.247 is trying to conduct a Microsoft IIS Unicode code exploit attack. The attacker would not be able to do this attack without a TCP 3-way handshake. It could be a 3rd party hijacked machine, but most likely not.

Description of attack:

Microsoft IIS versions 4.0 and 5.0 contained a flaw which enabled someone visiting an IIS website to execute code under the IUSR_*machinename* account. This IUSR_*machinename* account is basically the anonymous account that is created when installing IIS 4.0 or 5.0 for anonymous web or ftp access. This account is a member of the "everyone" and "users" groups by default. Replacing the "." and "/" with the Unicode or Hex equivalent, the attacker is able to break out of the website and into the local machine. The attacker has created a remote shell where they can change HTML code, traverse the directories, setup backdoors for future use or maliciously destroy data by using the newly created "cmd.exe" shell.

CVE Reference Numbers
CVE-1999-0407
CVE-2000-0884
Note: There are a total of 66 CVE entries listed under IIS, and for space considerations, the others are referenced below:
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=IIS

Attack mechanism:

This attack works by first completing the 3-way handshake in order to transmit data to the targeted machine. The attacker then constructs URL commands to move within the machine. In

this particular case, the attacker first did a "dir" command, to view the contents of the hard drive. This is accomplished by placing "../" within the url.
For example: http://<any server name>/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\
You can see in the Snort trace that the attacker did the same Unicode replacements in the above detect.

47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E 25 63 30 GET /msadc/..%c0
25 61 66 2E 2E 2F 2E 2E 25 63 30 25 61 66 2E 2E %af../..%c0%af..
2F 2E 2E 25 63 30 25 61 66 2E 2E 2F 77 69 6E 6E /..%c0%af../winn
74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65 t/system32/cmd.e
78 65 3F 2F 63 2B 64 69 72 2B 63 3A 5C 20 48 54 xe?/c+dir+c:\ HT

In the third Snort entry, it appears that the attacker is trying to password attack the IISADMPWD directory. This is a directory that Microsoft IIS installs to allow network users to change their passwords via HTTP.

47 45 54 20 2F 69 69 73 61 64 6D 70 77 64 2F 2E GET /iisadmpwd/.
2E 25 63 30 25 61 66 2E 2E 2F 2E 2E 25 63 30 25 .%c0%af../..%c0%
61 66 2E 2E 2F 2E 2E 25 63 30 25 61 66 2E 2E 2F af../..%c0%af../
77 69 6E 6E 74 33 35 31 2F 73 79 73 74 65 6D 33 winnt351/system3
32 2F 63 6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2/cmd.exe?/c+dir
2B 63 3A 5C 20 48 54 54 50 2F 31 2E 30 0D 0A 56 +c:\ HTTP/1.0..V

This is also known as the "Web Server Folder Traversal" attack.

Correlations:

There are numerous references on Bugtraq, Microsoft Technet Pages, GIAC, Security Focus, and other discussion security web pages.
Additional information of this exploit can be found at:
http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D2110
Kevin Peterson reported actual buffer overflow attempts on his IIS servers.
http://www.sans.org/y2k/041101.htm

CERT VU# 111677 - http://www.kb.cert.org/vuls/id/111677

Evidence of active targeting:
Yes this is active targeting in this Snort detect. The attacker is specifically using Microsoft IIS exploits known in the security field.

Severity:
The formula used to rank the severity of the incident is given below:

(Criticality + Lethality) - (System countermeasures + Network countermeasures)

Each element is ranked 1 to 5, 1 being low, 5 being high. The maximum score, i.e. the worst-case scenario, is 8. The minimum score, i.e. the best-case scenario, is -8.

Criticality = 5. The targeted machines are Windows IIS web servers.

Lethality = 5. The attacker is using a known IIS exploit that would compromise the machine.

System countermeasures = 2. Unknown if the targeted machines had the latest patches, but it appears that one machine does not.
Network countermeasures = 3. The attack was detected with Snort IDS.

Thus, severity = (5 + 5) - (2 + 3) = **5**.

Defensive recommendation:
Since most sites want anonymous website traffic to be allowed through, this exploit code is extremely dangerous. You cannot do much to the firewall in regards to port blocking, since you need to have port 80 traffic go through to the web server. Recommendation would be applying hot fixes from Microsoft that patch this vulnerability as soon as possible, if not already done. Maintain monitoring of web server machine for future attacks with Snort, tcpdump and/or another IDS program. This would also entail continuous monitoring of all logs with any abnormal traffic directed at the web server machine.

Microsoft Security Bulletin (MS00-057)
http://www.microsoft.com/technet/security/bulletin/MS00-057.asp
Microsoft Security Bulletin (MS00-078)
http://www.microsoft.com/technet/security/bulletin/MS00-078.asp
Microsoft Security Bulletin (MS00-086)
http://www.microsoft.com/technet/security/bulletin/MS00-086.asp

Multiple choice test question:
The attacker is using what kind of exploit in the above detects?

a) SMURF attack.
b) Loki attack.
c) Microsoft Web Server Folder Traversal attack.
d) CGI PHP mylog script allows an attacker to read any file on the target server.

Answer: c

Network Detect #3 Analysis

```
Apr  4 15:47:25 172.148.21.149:2351 -> a.b.c.9:21 SYN ******S*
Apr  4 15:47:22 172.148.21.149:2372 -> a.b.c.30:21 SYN ******S*
Apr  4 15:47:22 172.148.21.149:2375 -> a.b.c.33:21 SYN ******S*
Apr  4 15:47:22 172.148.21.149:2409 -> a.b.c.67:21 SYN ******S*
Apr  4 15:47:22 172.148.21.149:2413 -> a.b.c.71:21 SYN ******S*
Apr  4 15:47:22 172.148.21.149:2422 -> a.b.c.80:21 SYN ******S*
Apr  4 15:47:24 172.148.21.149:2424 -> a.b.c.82:21 SYN ******S*
Apr  4 15:47:25 172.148.21.149:2443 -> a.b.c.101:21 SYN ******S*
Apr  4 15:47:30 172.148.21.149:2480 -> a.b.c.138:21 SYN ******S*
Apr  4 15:47:30 172.148.21.149:2509 -> a.b.c.167:21 SYN ******S*
```

```
Apr  4 15:47:33 172.148.21.149:2512 -> a.b.c.170:21 SYN ******S*
Apr  4 15:47:32 172.148.21.149:2534 -> a.b.c.192:21 SYN ******S*
Apr  4 15:47:32 172.148.21.149:2537 -> a.b.c.195:21 SYN ******S*
Apr  4 15:47:32 172.148.21.149:2551 -> a.b.c.209:21 SYN ******S*
Apr  4 15:47:32 172.148.21.149:2554 -> a.b.c.212:21 SYN ******S*
Apr  4 15:47:33 172.148.21.149:2567 -> a.b.c.225:21 SYN ******S*
Apr  4 15:47:35 172.148.21.149:2586 -> a.b.c.244:21 SYN ******S*
Apr  4 15:48:00 172.148.21.149:2798 -> a.b.d.202:21 SYN ******S*
Apr  4 15:48:03 172.148.21.149:2829 -> a.b.d.233:21 SYN ******S*
Apr  4 15:48:03 172.148.21.149:2832 -> a.b.d.236:21 SYN ******S*

Apr  4 15:47:58 hostmf /kernel: Connection attempt to TCP a.b.f.167:21 from
  172.148.21.149:3271
Apr 04 15:47:36 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): connected - local  : a.b.c.57:21
Apr 04 15:47:36 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): connected - remote : 172.148.21.149:2399
Apr 04 15:47:36 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): FTP session opened.
Apr 04 15:47:37 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): received: USER anonymous
Apr 04 15:47:37 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): received: PASS (hidden)
Apr 04 15:47:37 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): ANON anonymous: Login successful.
Apr 04 15:47:37 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): Preparing to chroot() the environment, path = '/var/local/ftp'
Apr 04 15:47:37 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): Environment successfully chroot()ed.
Apr 04 15:47:38 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): received: CWD /pub/
Apr 04 15:47:38 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): received: MKD 010404214816p
Apr 04 15:47:39 hostl proftpd[28482] hostl (AC941595.ipt.aol.com
  [172.148.21.149]): received: CWD /public/
```

Source of Trace:

http://www.sans.org/y2k/040901-1500.htm

Detect was generated by:

The above detect was generated by Snort IDS and the syslog.

Probability the source address was spoofed:

Highly unlikely since a connection was made on the FTP services port and a TCP 3-way handshake is needed to do that. The fact that the attacker previously scanned the targeted

machines before actually connecting to one is also a good indication that the source IP is not spoofed.

Description of attack:

The attack was targeted at TCP port 21 FTP. The attacker is using a buffer overflow to break out of the root FTP directory by first logging on anonymously and overflowing the buffer. The attacker then proceeds to change out of the root FTP directory and do any one of many things such as attack the passwd file, copy files off the machine,

CVE Reference Numbers
CVE-1999-0368
CAN-1999-0911 – CVE Candidate Under Review

Other CVE Reference Numbers for other ProFTP vulnerabilities
CVE-2001-0316
CVE-2001-0317
CVE-2001-0318
CAN-2000-0574 – CVE Candidate Under Review
CAN-2001-0027 – CVE Candidate Under Review
CAN-2001-0136 – CVE Candidate Under Review
CAN-2001-0456 – CVE Candidate Under Review

Attack mechanism:

Then the attacker overflows the buffer to break out of the root as shown on these lines:

Apr 04 15:47:37 hostl proftpd[28482] hostl (AC941595.ipt.aol.com [172.148.21.149]): Preparing to chroot() the environment, path = '/var/local/ftp'
Apr 04 15:47:37 hostl proftpd[28482] hostl (AC941595.ipt.aol.com [172.148.21.149]): Environment successfully chroot()ed.
Apr 04 15:47:38 hostl proftpd[28482] hostl (AC941595.ipt.aol.com [172.148.21.149]): received: CWD /pub/

Then the attacker creates another directory

Apr 04 15:47:38 hostl proftpd[28482] hostl (AC941595.ipt.aol.com [172.148.21.149]): received: MKD 010404214816p

Finally he changed to the public directory

Apr 04 15:47:39 hostl proftpd[28482] hostl (AC941595.ipt.aol.com [172.148.21.149]): received: CWD /public/

Correlations:

There are many references for FTP attacks on security focus, Buqtraq, and other security discussion web pages.
Laurie@edu reported past proftpd scans and connection attempts
http://www.sans.org/y2k/122200-1000.htm
http://www.sans.org/y2k/011601-1430.htm

Evidence of active targeting:
There is active targeting of this machine. After the SYN scan discovery, the attacker reconnects and runs the FTP buffer overflow exploit on the machine.

Severity:
The formula used to rank the severity of the incident is given below:

(Criticality + Lethality) - (System countermeasures + Network countermeasures)

Each element is ranked 1 to 5, 1 being low, 5 being high. The maximum score, i.e. the worst-case scenario, is 8. The minimum score, i.e. the best-case scenario, is -8.

Criticality = 4. FTP systems are the targets.
Lethality = 5. The attacker has gained access to the machines through an exploit.

System countermeasures = 2. Some systems had no countermeasures and did appear to have the latest security patches.
Network countermeasures = 3. No blocking of port 21 at the firewall even though detected with IDS.

Thus, severity = (4 + 5) - (2 + 3) = **4**.

Defensive recommendation:
Remove the machine from the network and determine the exact extent of the damage done by the exploit. If possible, transfer the important data off and rebuild the machine, making sure to use the latest version of ProFTP and the latest patches. If the machine were not being used as a FTP server, I would remove the unneeded services from the machine. Extra care would be taken before re-integrating the machine back into the network so no backdoor Trojans and such are introduced into the network. Block the FTP port at the firewall and create rules that only allow FTP traffic to machines that you want to allow external traffic to connect to.

Multiple choice test question:
Most exploits deal with which of the following?

a) Insufficient security countermeasures.
b) Latest updates and patches not applied when available.
c) Personnel not monitoring the firewall, router and machine logs.
d) Unknowledgeable personnel in the security aspects of technology.
e) All of the above.

Answer: e

Network Detect #4 Analysis

Mar 29 19:56:00 24.214.63.27:2839 -> a.b.c.24:111 SYN ******S*
Mar 29 19:55:57 24.214.63.27:2845 -> a.b.c.30:111 SYN ******S*
Mar 29 19:55:57 24.214.63.27:2848 -> a.b.c.33:111 SYN ******S*

```
Mar 29 19:55:57 24.214.63.27:2866 -> a.b.c.51:111 SYN ******S*
Mar 29 19:56:00 24.214.63.27:2863 -> a.b.c.48:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:3880 -> a.b.c.71:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:3889 -> a.b.c.80:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:3920 -> a.b.c.111:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:3930 -> a.b.c.121:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:3976 -> a.b.c.167:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4001 -> a.b.c.192:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4004 -> a.b.c.195:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4006 -> a.b.c.197:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4010 -> a.b.c.201:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4016 -> a.b.c.207:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4024 -> a.b.c.215:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4034 -> a.b.c.225:111 SYN ******S*
Mar 29 19:55:59 24.214.63.27:4053 -> a.b.c.244:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1294 -> a.b.d.202:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1299 -> a.b.d.207:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1301 -> a.b.d.209:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1326 -> a.b.d.234:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1329 -> a.b.d.237:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1331 -> a.b.d.239:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1328 -> a.b.d.236:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1337 -> a.b.d.245:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1335 -> a.b.d.243:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1332 -> a.b.d.240:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1334 -> a.b.d.242:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1338 -> a.b.d.246:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1336 -> a.b.d.244:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1339 -> a.b.d.247:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1342 -> a.b.d.250:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1343 -> a.b.d.251:111 SYN ******S*
Mar 29 19:56:05 24.214.63.27:1382 -> a.b.e.34:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1400 -> a.b.e.52:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1404 -> a.b.e.56:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1427 -> a.b.e.79:111 SYN ******S*
Mar 29 19:56:02 24.214.63.27:1436 -> a.b.e.88:111 SYN ******S*

Mar 29 19:56:18 hostman rpc.statd: invalid hostname to sm_stat:
^X÷ÿ¿^X÷ÿ¿^Y÷ÿ¿^Y÷ÿ¿^Z÷ÿ¿^Z÷ÿ¿^[÷ÿ¿^[÷ÿ¿
%8x%8x%8x%8x%8x%8x%8x%8x%8x%236x%n%137x%n%10x%n%192x%nM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
```

```
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^P!
 M-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^P
```

Source of Trace:

The GIAC URL: http://www.sans.org/y2k/040301-1300.htm

Detect was generated by:

The above detect was generated by Snort IDS and the syslog.

Probability the source address was spoofed:

Highly unlikely since a connection was eventually made to the Portmap (RPC) service port and a TCP 3-way handshake is needed to do that. It could be a 3rd party machine that was taken over, but the fact that the attacker previously scanned the targeted machines before actually connecting to one is also a good indication that the source IP is not spoofed.

Description of attack:

The attacker systematically sends a SYN packet to a group of IP addresses directed at port 111, Portmap or RPC services. The attacker is trying to find a machine that has the Portmap (RPC) service running. When a machine responds, the attacker then connects to that machine's Portmap (RPC) services and proceeds to do an rpc.statd buffer overflow. If successful, this will allow the attacker to compromise the machine and do whatever they want. The attacker would then delete any logs showing their existence to cover their tracks.

CVE Reference Numbers
CVE-1999-0018
CVE-1999-0019
CVE-1999-0493
CVE-2000-0666

Attack mechanism:

The attacker first sends out SYN packets to a group of IP addresses directed at port 111. This is done to elicit a response from a machine that is running the Portmap (RPC), port 111 service.

```
Mar 29 19:56:02 24.214.63.27:1436 -> a.b.e.88:111 SYN ******S*
```

Once the attacker receives a SYN-ACK response, the attacker then will send a RST in response to the SYN-ACK and break the TCP 3 way handshake. Since a SYN-ACK was sent, it means that the machine is listening on port 111 and it responded with a SYN-ACK when provoked by

the SYN packet. The attacker then connects back to the machine that is listening on port 111 and sends a bunch of characters repeatedly to overflow the rpc.statd.

Mar 29 19:56:18 hostman rpc.statd: invalid hostname to sm_stat:
^X÷ÿ¿^X÷ÿ¿^Y÷ÿ¿^Y÷ÿ¿^Z÷ÿ¿^Z÷ÿ¿^[÷ÿ¿^[÷ÿ¿
%8x%8x%8x%8x%8x%8x%8x%8x%8x%236x%n%137x%n%10x%n%192x%nM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM-^PM
(snippet)

Correlations:
There are numerous references on Bugtraq, GIAC, CERT, and other discussion security web pages. The rpc.statd exploit is number 3 on SANS top 10 list of Security Threats list (http://www.sans.org/topten.htm).
This activity was also shown in Miika Turkia and Marc Bayerkohler practicals.
http://www.sans.org/y2k/practical/Miika_Turkia_GCIA.html
http://www.sans.org/y2k/practical/Marc_Bayerkohler_GCIA.html#Trace_2__RPC_scan

Evidence of active targeting:
Yes there is active targeting. There is a specific attempt to find machines that have the Portmap (RPC) service running and then attempt to overflow the buffer.

Severity:
The formula used to rank the severity of the incident is given below:

(Criticality + Lethality) - (System countermeasures + Network countermeasures)

Each element is ranked 1 to 5, 1 being low, 5 being high. The maximum score, i.e. the worst-case scenario, is 8. The minimum score, i.e. the best-case scenario, is -8.

Criticality = 4. Assuming that machines were a mix of Windows and Unix machines running critical software.
Lethality = 5. If successful, the attacker can gain total control.

System countermeasures = 3. There is no way to determine if system countermeasures are in place so a average rating is used.
Network countermeasures = 3 The Portmap (RPC) service was not blocked by the firewall, but detected by Snort.

Thus, severity = (4 + 5) - (3 + 3) = **3**.

Defensive recommendation:
First determine if the machine was compromised by removing it from the network and examining it for damage. Block port 111 and the other RPC ports at the outer firewall and make sure that all the latest OS and security patches have been applied. Be sure and watch the machine

as it is being put back into the network for any abnormal packet activity. Continue to monitor Snort logs for any additional traffic and you can also reference the CERT.org page (http://www.cert.org/advisories/CA-99-05-statd-automountd.html) for more information regarding this.

Multiple choice test question:

A buffer overflow attempt on the Portmap service is done by?

a) Placing "/" in a URL to create a remote command line shell.
b) SYN flooding a particular machine.
c) Poisoning the ARP cache of the targeted machine.
d) By sending repeating characters to overflow the buffer.
e) None of the above.

Answer: d

Network Detect #5 Analysis

```
Mar  2 21:02:06 hosth /kernel: Connection attempt to TCP a.b.c.62:27374 from
  65.8.47.74:3200
Mar  2 21:02:18 hostmf /kernel: Connection attempt to TCP a.b.f.167:27374 from
  65.8.47.74:4067
Mar  2 21:02:18 hostmf /kernel: Connection attempt to TCP a.b.f.167:27374 from
  65.8.47.74:4067

Mar  2 21:02:06 65.8.47.74:3164 -> a.b.c.26:27374 SYN ******S*
Mar  2 21:02:06 65.8.47.74:3168 -> a.b.c.30:27374 SYN ******S*
Mar  2 21:02:06 65.8.47.74:3171 -> a.b.c.33:27374 SYN ******S*
Mar  2 21:02:06 65.8.47.74:3189 -> a.b.c.51:27374 SYN ******S*
Mar  2 21:02:07 65.8.47.74:3200 -> a.b.c.62:27374 SYN ******S*
Mar  2 21:02:06 65.8.47.74:3209 -> a.b.c.71:27374 SYN ******S*
Mar  2 21:02:07 65.8.47.74:3218 -> a.b.c.80:27374 SYN ******S*
Mar  2 21:02:07 65.8.47.74:3239 -> a.b.c.101:27374 SYN ******S*
Mar  2 21:02:07 65.8.47.74:3241 -> a.b.c.103:27374 SYN ******S*
Mar  2 21:02:07 65.8.47.74:3252 -> a.b.c.114:27374 SYN ******S*
Mar  2 21:02:07 65.8.47.74:3259 -> a.b.c.121:27374 SYN ******S*
Mar  2 21:02:08 65.8.47.74:3266 -> a.b.c.128:27374 SYN ******S*
Mar  2 21:02:08 65.8.47.74:3271 -> a.b.c.133:27374 SYN ******S*
Mar  2 21:02:08 65.8.47.74:3276 -> a.b.c.138:27374 SYN ******S*
Mar  2 21:02:08 65.8.47.74:3305 -> a.b.c.167:27374 SYN ******S*
Mar  2 21:02:09 65.8.47.74:3335 -> a.b.c.197:27374 SYN ******S*
Mar  2 21:02:09 65.8.47.74:3337 -> a.b.c.199:27374 SYN ******S*
Mar  2 21:02:09 65.8.47.74:3345 -> a.b.c.207:27374 SYN ******S*
Mar  2 21:02:09 65.8.47.74:3350 -> a.b.c.212:27374 SYN ******S*
Mar  2 21:02:09 65.8.47.74:3353 -> a.b.c.215:27374 SYN ******S*
Mar  2 21:02:09 65.8.47.74:3360 -> a.b.c.222:27374 SYN ******S*
```

Mar 2 21:02:09 65.8.47.74:3362 -> a.b.c.224:27374 SYN ******S*

Source of Trace:
The GIAC URL: http://www.sans.org/y2k/030701-1200.htm

Detect was generated by:
The above detect was generated by Snort IDS.

Probability the source address was spoofed:
Not likely since the attacking host would not have a way to receive the reply back from the SYN request according to the TCP 3-way handshake rules. If the attacker spoofed the IP, there would be no way to know for the attacker to know if the targets were running the Sub Seven Trojan

Description of attack:
Attacker is scanning for a backdoor Trojan service Sub Seven installed on the a.b.c subnet. Once found, the attacker will try to connect to the server program running on an unsuspecting target through a remote client program. Once connected, the attacker has full run of the entire system. The attacker can reboot the machine, run through the registry and even remote IP scanning to name a few. Sub Seven runs only on Windows 95/98, so Unix and NT/2000 systems are not affected by this to date. Sub Seven tries to connect to TCP port 27374 by default.

There are no CVE entries for this attack.

Attack mechanism:
The attacker first SYN scans for the open service port 27374 used by the Sub Seven server program. Once the attacker receives a SYN-ACK, he will then use the Sub Seven client portion of the program to connect, through TCP port 27374, to the targeted machine. Another trick the attacker may use is sending out mass emails, usually using an Outlook vulnerability to trick the intended user of a machine to execute the Sub Seven server program by including some kind of attachment with the email. This would install the Trojan on the victim's machine and leave the victim susceptible to the attack.

More information can be found at the Sub Seven homepage and Security Focus.
http://subseven.slak.org/
http://www.securityfocus.com/frames/?content=/templates/tools.html%3Fid%3D1405%26msgid%3D4878

Correlations:
There are many correlations for this attack on http://www.incidents.org.
This also showed up in David Oborn's practical.
http://www.sans.org/y2k/practical/David_Oborn_GCIA.html#detect1

Evidence of active targeting:
Yes there is active targeting involved because the attacker is specifically looking for a target machine running the Sub Seven Trojan. If found, no doubt that the attacker will try and connect to which every machine answers on port 23734.

Severity:
The formula used to rank the severity of the incident is given below:

(Criticality + Lethality) - (System countermeasures + Network countermeasures)

Each element is ranked 1 to 5, 1 being low, 5 being high. The maximum score, i.e. the worst-case scenario, is 8. The minimum score, i.e. the best-case scenario, is -8.

Criticality = 4. Assuming that user Windows 9x systems are the targets.
Lethality = 3. The attacker has not appeared to have gained access to the machines through the backdoor. But that is undeterminable with the given information so an average value is used.

System countermeasures = 4. Assuming that the targeted systems have the latest Anti Virus updates on all machines.
Network countermeasures = 2. No blocking of port 27374 at the firewall even though detected with IDS.

Thus, severity = (4 + 3) - (4 + 2) = **1**.

Defensive recommendation:
Block port 27374 at the router and firewall. Any "legitimate" program should not be using that port number. It is possible, but highly unlikely. Most up to date virus detection programs and IDS programs will catch this as well. Configure MS Outlook to not "open" attachments and continue to preach to users the standards of not opening attachments from unknown sources and to be wary even if from reputable sources. Since the Trojan only works on Windows 95/98 machines, better maintenance care can be directed at those machines since at lot of Trojans are directed at Windows 95/98 users.

Multiple choice test question:
The default port that a Sub Seven attack tries to connect to is?

a) 31337
b) 8080
c) 27374
d) 777
e) 515

Answer: c

Assignment 2 – Describe the State of Intrusion Detection

Thinking Your Network Is Safe Is Suicidal?

One day you come into work switch on your monitor expecting to see everything is running smoothly on your servers. You unlock your screen and notice some strange events in your logs, files missing, added files on not just this machine, but numerous other machines and

upon further investigation, and you realize that you have just been a victim of cyber-warfare attack. After 20 minutes of explaining to upper management what had happened, you now come to terms with the fact that it is necessary to use some sort of Intrusion Detection System (IDS) to protect your network from this danger. You contact some companies that tell you that their IDS software can protect your network, but which type of protection do you choose? Host Based, Network Based or do you run both? First you must define what Intrusion Detection is, what Host Based and Network Based are and then needs of your environment.

Intrusion Detection software has the ability to monitor and prevent unauthorized attempts into your network. Unauthorized attempts could be remote attacks such as someone scanning your firewall for open ports or enumerating your machines and services running on that machine for exploitation later on. The attempts can also be local attacks, people within the company trying to steal sensitive information. In theory, the IDS would be able to, notify you of such attempts and log it and/or block them. As Paul Proctor stated in his book, think of IDS software as security monitoring cameras watching your building. Cameras watching your outer perimeter would be the Network IDS. While cameras located inside the building would be the Host IDS.

Host based Intrusion Detection Software (HIDS) is used to watch over a machine's internal file structure often by watching the event logs or syslogs in conjunction with auditing functions. For example, on a Microsoft Windows OS, most HIDS software are able to monitor the system's registry key values for any modification. One of the more popular registry values to watch for is the "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce" key. Hackers could maliciously place an entry into that key which would call upon a program or script to install a backdoor, delete files, or create a connection to a remote machine. The most dangerous part is that there is no way to effectively figure out what has happened until it is too late. A value put into that key is deleted once it has executed, hence the "RunOnce" key name. Another key that can be watched is the Back Orifice registry key that is added whenever some user is tricked or purposely executes the Black Orifice.exe file. Though most up to date antivirus software will detect this, but that is the whole point of HIDS software, to watch out for this type of activity in real time or at specified intervals. Many people assume that attacks are done from an outside source and fail to consider the disgruntled worker. With Back Orifice, one would think that most of the time it is accidentally installed by an unsuspecting user. But what about someone who wants to steal your confidential information from other users? What if they are bored one day and decide to snoop on their neighbor's unknowingly email messages? They could install Back Orifice on selected machines and sit back and monitor the data from afar. The days of shoulder surfing are long gone. So by all accounts HIDS software looks like a godsend, but it does come at a price. HIDS software providing Real Time analysis can produce a lot of false alarms or false positives. For example, an alert monitoring the "boot.ini" file on a Microsoft Windows NT/2000 OS could be triggered in many ways. Most IDS software uses for example, the Windows NT/2000 Auditing and Event Logs as a way of monitoring for changes. If you enable auditing on a NT/2000 system for "logon" success and failure, HIDS software could then monitor the Event Log for logged events because of the auditing setting. Since the software is relying on how the OS records the event, the IDS software can only report on how the event is seen by the OS. By right clicking on My Computer and changing a Windows startup time value will modify the boot.ini file and thus trigger an alert. But is it a malicious attack? Sure it would

be easy if the machine was at the same location where you could easily check the machine. But what happens when you are in a WAN environment spread across remote locations and you cannot physically get to the machine within a reasonable amount of time? Sure there are applications such as PC Anywhere, that can help in monitoring of the WAN environment, but do you really want to open up additional ports on your firewall? So you decide that HIDS software will be a good peace of mind for your company security, but is that the final word?

Now that you understand HIDS software, what about the big buzz lately with network style attacks? HIDS software is limited to internal protection and trend type analysis whereas Network based Intrusion Detection System (NIDS) software is ideal for external protection and Real Time alerting. With many commercial applications available ISS RealSecure, NFR, and NetworkICE to name a few, an excellent freeware NIDS package is Snort by Martin Roesch. Tcpdump is another good freeware product for analysis of the actual TCP/IP packets. Most NIDS software are able to capture the TCP/IP packet either by a "Packet Filter" of some sort placed on the local machine or promiscuous mode sensors (Taps) placed out in strategic locations within the network. Sensors placed directly on the local machine being monitored are often referred to as Network Node IDS (NNIDS) and the latter as NIDS. People often make the mistake of referring to NIDS and NNIDS as one in the same, but you should remember that each are quite different. An easy way to remember is NIDS listens to the entire wire for packets while NNIDS listens on a specific host or node, hence the name Network Node. From here on, NIDS will refer to the IDS software itself, not the particular different types of Network based IDS. NIDS will scan TCP/IP packets for any threat patterns and if found will raise a red flag and send an alert to the NIDS software manager. Though NIDS may sound like the perfect defensive weapon, it is not what it seems. For example, you receive an alert from the NIDS software about strange packets directed to your machines at port 31337, the Back Orifice port. Someone is scanning for open Back Orifice ports; do you panic and call out the black helicopters? As with HIDS software, analysis of the packets is the real key. Calling out the National Guard may seem like a logical conclusion if you see activity directed at port 31337 on one of the machines, but it is not as easy as the HIDS solutions. The reason being is external attacks have a lot more to them in tracking down offenders and if you really want to track them down at all. The time and money spent could be put to other uses. The real key is whether or not the machines are responding to these probes and if so, action must be taken to stop it and evaluate the extent of damage caused by the probes. Scanning for open ports across the Internet occurs on a daily basis and reviewing any of the intrusion logs posted on incidents.org will validate this. Using a tool like tcpdump to listen for packets can actually help in determining if the machine has been in fact compromised and is letting outsiders inside to the internal network. What happens if it is a wrongly configured application that happens to use port 31337? This is not uncommon and unlikely to happen, but it can.

Now you realize you will also need a NIDS software package. A couple of the better choices that are available are the freeware Snort IDS and tcpdump packet-capturing program. Both are fairly customizable, which makes them very popular in the security field. Snort IDS allows great customization of alert rules to capture specific data packets which can alert you of any packet which contains your specified rule filter. Plus with Snort being a freeware product, you have the benefit of other security analysts submitting Snort rules for the latest hacking attempt signatures. This process allows you to have almost instantaneous alert rule updates, since there are other analysts out there in the same predicament as you are in trying to prevent their

networks from falling prey to hacking attempts. One issue with a commercial NIDS is that updates usually take more time to get published and out to the public. Some time frames range from days to weeks to even months as indicated by Richard Power and Rik Farrow's interview, although timeframes are increasing since the printing of this article as most companies will rush out an emergency signature for their customers, but how much testing has gone into it? With exploits having so many different variations, these companies have a hard time keeping up. Would you want an update that has not been through from a company that has not done their due diligence in thoroughly testing it? These delays can cause problems. As an example of this problem, Microsoft had to come out with security patches for its IIS buffer overflow exploit during which many sites fell prey to it. As you can see the time it takes for a patch or update to come out, researched, and tested. All this time waiting can be devastating to your company's machines. Some commercial IDS software does allow for customizable signatures, but with wide use and easy customization of Snort signature rules, this allows you to be on the watch for the latest, up to the minute attacks with a faster reaction time, hopefully minimizing the risks to your machines. Snort combined with tcpdump can effectively monitor your network just as well as most commercial products. With tcpdump you can capture the packets and at a latter time use your Snort data to narrow down the time to analyze the traffic, and notice any anomalies that Snort was not able to pick up and vice versa.

As you can see there are a lot of options to choose from when deciding on a HIDS or NIDS type IDS. Recent events in the e-commerce realm have heightened awareness of network security. The last thing a company needs is bad publicity over a hacker that broke into their systems and stole hundreds of customers' confidential information. If a hacker were to steal a penny from a financial institution, the publicity would be worth millions of dollars of loss to them. So, do you go with a HIDS or NIDS system or both?

With no easy decision in hand, the best thing to implement on the network would be HIDS software installed locally on each machine you want to monitor. This could be something along the lines of Tripwire or Cybersafe Centrax products to monitor the local files and registry settings on a Windows platform. Even with the limitations of HIDS with false alarms and logistic considerations and machines being in different locations, it does have its benefits. The ability to determine if someone has changed a registry setting on a Windows box and to add a program to run when someone logs on, is crucial in identifying local attacks. Since the greatest danger in any network of malicious activity comes within the company itself, HIDS software can be a good preventive measure against this. With most HIDS systems running Real Time alerts, the response time with such attacks can be cut down to a minimum. HIDS software alone cannot complete the job itself. You would definitely need some kind of NIDS software to protect against internal attacks and external attacks that can get past your external firewall and routers. So any IDS plan without some kind of NIDS would be foolish and dangerous.

So you finally decide on a product for your organization and you go out and spend thousands of dollars on an IDS software that supposedly will protect and monitor your network. Then you realize that this one product does not protect the entire network nor fulfills the company's needs. In your evaluations of different products, one is better at HIDS and the other at NIDS. So did you make the correct choice? It comes down to a yes and no. For you to be able to effectively protect your entire enterprise network, you would want to run multiple IDS software.

However in reality, with licensing costs between the products, deployment, training, and interaction between the products to consider, this is not possible. So as a Security Analyst, what would you do? Your decisions will impact the security of the entire company.

With all this information, I would definitely use Snort and tcpdump to help monitor the network side and some kind of HIDS software that can watch for any non-authorized file changes, registry changes and such. Some commercial products out like Centrax have both a HIDS and NIDS built-in, so that is a plus. With Snort and tcpdump being freeware, there would be no cost other than the costs of actual machines, setup and placement throughout your network. With all the software in place, it does not mean your network is totally safe. Even with round the clock coverage, you must balance the false positives and real alerts. One thing to keep in mind is that never assume without further research that every alert is malicious activity. As I mentioned before, especially with HIDS software, there are many false alerts and deleting such signatures also opens up the possibility of missing important data. So it is a "Catch-22" effect with any IDS software. Determining what your company wants to protect from what it perceives as more of a danger is difficult. The best practice is to not let your guard down and always be skeptical of any abnormal activity. Keep in mind to not be overly reactive to the data whether it is Host Based or Network Based. There are some abnormal activities that cannot be explained. We must keep in mind that Intrusion Detection is an analytical job. The more sources of data you have, the better the analysis will be. As Stephen Northcutt said, "If it looks like a duck and quacks like a duck, make sure it has feathers and waddles like a duck."

References

Northcutt, Stephen. Network Intrusion Detection An Analysts Handbook, Second Edition. Indiana: New Riders, 2000

Proctor, Paul, The Practical Intrusion Detection Handbook. New Jersey: Prentice Hall PTR, 2001

Elson, David."Intrusion Detection, Theory and Practice." May 2000
URL:http://www.securityfocus.com/focus/ids/articles/davidelson.html

Lemos, Robert. "Microsoft reveals Web server hole." June 2001
URL:http://news.cnet.com/news/0-1003-200-6312870.html

"IDS Introduction" URL:http://www.nss.co.uk/ids/introduction.htm

Seifried, Kurt "Network Intrustion Detection Systems and Virus Scanners - Are They The Answer?" January 2000
URL:http://www.securityportal.com/closet/closet20000105.html

Power, Richard , Farrow, Rik. "Five vendors answer some no-nonsense questions on IDS." July 1998. URL:http://www.gocsi.com/ques.htm

Assignment 3 – "Analyze This" Scenario

Executive Summary

The following is a summary of the scan files submitted to our company for analysis of your network. These were obtained through the placement of a Snort IDS box placed within your organization from a prior consulting company. This Snort IDS software was running with a standard Snort rule base. We have gathered all the data and are here to present some of our findings to you. In the following pages we will go over each of the file types that were present: alert, scan and Out Of Specification (OOS). First the alert scans were examined and analyzed with the top 5 sources and destination IP addresses for each signature type. Then the scan alerts were examined with the top 5 scan type signature summary and any interesting traffic as well. Last but not least, the OOS files were examined, analyzed, graphed and weighted according to destination port. Finally recommendations for your organization are included.

Snort Alert Data Summary (379,210 Total alerts)

The following is each Snort signature detected along with the top 5 source and destination IP addresses. It should be noted that the top 5 source and destinations' are not the worst offenders per se or the only sources or destinations, but the IP addresses with the most alerts. A brief summary describing each signature is included and any interesting traffic associated with it. Some of the alerts are caused by traffic from internal network to external and might indicate a system compromise.

Signature (click for definition)	# Alerts	# Sources	# Destinations
UDP SRC and DST outside network	368047	47	250
External RPC call	3373	14	1152
High port 65535 udp - possible Red Worm - traffic	2095	11	12
Watchlist 000220 IL-ISDNNET-990517	1766	28	15
Watchlist 000222 NET-NCFC	735	6	8
SMB Name Wildcard	657	247	192
Queso fingerprint	536	31	48
Possible trojan server activity	499	108	196
connect to 515 from outside	449	3	330
WinGate 1080 Attempt	345	60	145
SYN-FIN scan!	157	2	157
Port 55850 tcp - Possible myserver activity – ref.	111	22	21

010313-1			
TCP SRC and DST outside network	98	26	48
High port 65535 tcp - possible Red Worm - traffic	95	17	19
Tiny Fragments - Possible Hostile Activity	66	4	4
NMAP TCP ping!	47	11	11
Null scan!	40	19	13
connect to 515 from inside	37	2	26
Back Orifice	25	2	25
SUNRPC highport access!	19	1	1
Attempted Sun RPC high port access	6	2	2
ICMP SRC and DST outside network	6	5	5
Probable NMAP fingerprint attempt	1	1	1

UDP SRC and DST outside network

Top 5 Sources triggering this attack signature

Source	**# Alerts (sig)**	**# Alerts (total)**	**# Dsts (sig)**	**# Dsts (total))**
63.250.213.119	229539	229539	1	1
63.250.213.73	87472	87472	1	1
63.250.213.26	29222	29222	1	1
63.250.213.122	17369	17369	1	1
63.250.213.165	1380	1380	1	1

Top 5 Destinations receiving this attack signature

Destinations	**# Alerts (sig)**	**# Alerts (total)**	**# Srcs (sig)**	**# Srcs (total))**
233.28.65.62	229539	229539	1	1
233.28.65.227	87472	87472	1	1
233.28.65.164	29222	29222	1	1

233.28.65.222	17369	17369	1	1
233.28.65.59	1380	1380	1	1

Description
This Snort alert is looking for UDP traffic that has a source and destination IP outside the local network. The examination of the data indicates that the top 5 source IP's are Yahoo Broadcast Services and the top 5 destinations were multicast IANA IP's, hence the unusual traffic. There also was some NETBIOS traffic from internal machines that could not get a DHCP lease and are assigned the 169.254.x.x IP or had a 192.168.x.x IP from another network and some DNS requests from other machines as well.

```
06/04-11:19:14.751528 [**] UDP SRC and DST outside network [**] 63.250.213.119:1036-> 233.28.65.62:5779
06/04-11:19:15.945765 [**] UDP SRC and DST outside network [**] 63.250.213.119:1036-> 233.28.65.62:5779
```

Server used for this query: [whois.arin.net]

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

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

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

Domain System inverse mapping provided by:

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

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 29-Jun-2001.
Database last updated on 28-Jul-2001 23:02:36 EDT.

External RPC call

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
202.98.10.70	1304	1304	595	595
129.186.213.89	614	614	462	462
203.252.231.161	311	311	311	311
128.95.96.58	269	269	269	269
211.202.178.130	253	253	231	231

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.137.64	8	9	6	7
10.10.137.53	8	11	5	7
10.10.132.104	7	7	4	4
10.10.133.141	7	7	5	5
10.10.137.88	7	9	5	6

Description
This Snort alert is looking for any traffic directed at the Unix RPC or Portmapper port, port 111. There are many exploits that take advantage of this service. The most directed attacks were at hosts' 10.10.137.64 and 10.10.137.53. The top source attacker was 202.98.10.70. This exploit is currently number 3 on the SANS top ten exploits. (http://www.sans.org/topten.htm) The highest RPC scanner whois, listed below, is from an ISP located in China. A snippet of the obvious scanning is below:

```
06/04-08:56:25.825101 [**] External RPC call [**] 202.98.10.70:34141-> 10.10.100.130:111
06/04-08:56:29.315042 [**] External RPC call [**] 202.98.10.70:34141-> 10.10.100.130:111
```

Server used for this query: [whois.apnic.net]

% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois5.apnic.net)

inetnum: 202.98.0.0 - 202.98.31.255

netname: CHINANET-JL
descr: CHINANET Jilin province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: XY1-AP
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINANET-JL
changed: hostmaster@ns.chinanet.cn.net 20000101
source: APNIC

person: Chinanet Hostmaster
address: A12,Xin-Jie-Kou-Wai Street
country: CN
phone: +86-10-62370437
fax-no: +86-10-62053995
e-mail: hostmaster@ns.chinanet.cn.net
nic-hdl: CH93-AP
mnt-by: MAINT-CHINANET
changed: hostmaster@ns.chinanet.cn.net 20000101
source: APNIC

person: Xu Yongzhong
address: Data Communication Bireau
address: Ministry of Posts and Telecommunications
address: A12 Xin-jie-kou-wai Street
address: Beijing 100088
country: CN
phone: +86-10-62053991
fax-no: +86-10-62053995
e-mail: yzxu@publicf.bta.net.cn
nic-hdl: XY1-AP
mnt-by: MAINT-NULL
changed: hostmaster@apnic.net 19960319
source: APNIC

High port 65535 udp - possible Red Worm – traffic

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
216.169.36.189	2064	2064	1	1
10.10.98.121	7	7	2	2

132.208.250.1	6	6	2	2
10.10.70.242	4	4	3	3
10.10.217.62	3	3	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.70.242	2064	2064	1	1
217.11.136.21	6	6	2	2
10.10.1.3	5	10	1	5
10.10.98.121	4	5	2	3
195.200.18.28	4	4	2	2

Description
This Snort alert is looking for UDP traffic that has a relatively high source port 65535. Technically speaking, a destination port could be any ephemeral port, but one specific attack designated the Red Worm attack uses port 65535. The host 10.10.70.242 was engaged in using the online gaming program Quake, which resulted in the unusual high UDP port number. Port 27960 is associated as a Quake3 port.

```
06/07-19:47:12.676197 [**] High port 65535 udp - possible Red Worm - traffic [**] 216.169.36.189:65535-> 10.10.70.242:27960
06/07-19:47:12.708682 [**] High port 65535 udp - possible Red Worm - traffic [**] 216.169.36.189:65535-> 10.10.70.242:27960
```

Watchlist 000220 IL-ISDNNET-990517

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
212.179.72.226	1268	1268	1	1
212.179.5.184	281	281	2	2
212.179.4.50	59	59	1	1
212.179.27.6	28	28	1	1

212.179.81.12	18	18	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.97.210	1268	1268	1	1
10.10.218.78	278	278	1	1
10.10.150.133	120	184	10	14
10.10.150.220	29	39	4	8
10.10.218.166	16	16	2	2

Description

This Snort alert is triggered from any source IP from a particular class C network that has been identified as a potential source of malicious traffic. A whois done on any of the top 5 source IP block, 212.179.x.x comes away with locations within Israel. Here is the whois for 212.179.5.184

```
inetnum:     212.179.4.48 - 212.179.4.63
netname:     SCP-SYSTEMS-LTD
descr:       SCP-SYSTEMS-LAN
country:     IL
admin-c:     ES4966-RIPE
tech-c:      NP469-RIPE
status:      ASSIGNED PA
notify:      hostmaster@isdn.net.il
mnt-by:      RIPE-NCC-NONE-MNT
changed:     hostmaster@isdn.net.il 20000628
source:      RIPE

route:       212.179.0.0/17
descr:       ISDN Net Ltd.
origin:      AS8551
notify:      hostmaster@isdn.net.il
mnt-by:      AS8551-MNT
changed:     hostmaster@isdn.net.il 19990610
source:      RIPE

person:      Eran Shchori
address:     BEZEQ INTERNATIONAL
address:     40 Hashacham Street
address:     Petach-Tikva 49170 Israel
phone:       +972 3 9257710
fax-no:      +972 3 9257726
```

e-mail: hostmaster@bezeqint.net
nic-hdl: ES4966-RIPE
changed: registrar@ns.il 20000309
source: RIPE

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE

```
06/06-14:40:32.342488 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.72.226:31611->
10.10.97.210:41003
06/06-14:40:32.363208 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.72.226:31611->
10.10.97.210:41003
```

The software Audio Galaxy Satellite, a music-searching program similar to Napster, is responsible for this unusual traffic and uses TCP ports 41000-50000.

```
06/03-14:07:10.223907 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.5.184:3847-> 10.10.70.27:6346
```

```
06/03-07:09:28.274029 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.4.50:1247->
10.10.150.133:1214
06/03-07:09:28.699990 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.4.50:1247->
10.10.150.133:1214
```

Primarily the traffic to the internal hosts was caused by Gnutella and a similar program called KaZaa as shown above. KaZaa uses port 1214 and Gnutella uses 6346. Some similar scans were seen in Paul Asadoorian's GCIA practical.
http://www.sans.org/y2k/practical/Paul_Asadoorian_GIAC.doc

Watchlist 000222 NET-NCFC

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))

159.226.45.3	655	655	4	4
159.226.39.26	59	59	1	1
159.226.47.195	14	14	1	1
159.226.116.2	5	5	1	1
159.226.208.40	1	2	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.253.42	500	553	1	4
10.10.253.43	145	193	2	3
10.10.70.33	59	59	1	1
10.10.6.7	23	28	1	4
10.10.253.41	5	63	1	4

Description
This Snort alert is looking for any traffic for the specified class B network, 159.226.x.x. This has been identified as the following:

> Server used for this query: [whois.arin.net]
>
> The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
> P.O. Box 2704-10,
> Institute of Computing Technology Chinese Academy of Sciences
> Beijing 100080, China
> CN
>
> Netname: NCFC
> Netblock: 159.226.0.0 - 159.226.255.255
>
> Coordinator:
> Qian, Haulin (QH3-ARIN) hlqian@NS.CNC.AC.CN
> +86 1 2569960
>
> Domain System inverse mapping provided by:
>
> NS.CNC.AC.CN 159.226.1.1
> GINGKO.ICT.AC.CN 159.226.40.1

The source IP's were primarily scanning internal hosts for services such as mail, DNS, and authentication. It can also be normal mail traffic or perhaps mail spamming. IP 159.226.45.3 was also found to be involved in some malicious traffic in Herschel Gelman's GCIA practical as well.
http://www.sans.org/y2k/practical/Herschel_Gelman.html#3

```
06/03-21:19:59.631188 [**] Watchlist 000222 NET-NCFC [**] 159.226.39.26:1117-> 10.10.70.33:8765
06/03-21:19:59.695639 [**] Watchlist 000222 NET-NCFC [**] 159.226.39.26:1119-> 10.10.70.33:8765
```

This unusual traffic is directed a port 8765, which is used by Ultraseek. Ultraseek is a searching software originally by Ultraseek, now known as Inktomi. There is an exploit for this on Buqtraq that allows an attacker to obtain source code to any Ultraseek scripts, which could be used to support further attacks. The Bugtraq ID is 2061 and is listed below at the securityfocus.com link.

References for Ultraseek:
http://www.securityfocus.com/bid/2061
http://www.searchtools.com/tools/inktomi-search.html

SMB Name Wildcard

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
217.32.146.116	10	10	1	1
192.168.0.1	9	10	5	6
10.10.162.199	9	9	1	1
130.13.85.245	9	9	5	5
130.13.164.9	8	8	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.132.10	31	36	8	12
10.10.132.1	12	16	5	9
10.10.133.132	11	11	5	5
10.10.50.154	9	9	1	1
10.10.135.183	8	9	2	3

Description
This Snort alert is looking for UDP traffic from port 137 directed to port 137. Port 137 is associated with Microsoft's NetBIOS name lookups. Most of the alerts were generated from internal hosts, but there were some external hosts doing some NetBIOS commands. There was Windows NetBIOS information sharing was listed on SANS top 10 Internet Security threats. http://www.sans.org/topten.htm

```
06/06-04:38:44.209711 [**] SMB Name Wildcard [**] 217.32.146.116:137-> 10.10.132.10:137
06/06-04:38:47.170496 [**] SMB Name Wildcard [**] 217.32.146.116:137-> 10.10.132.10:137
```

This traffic should be investigated and could be remote users causing this. The unknown source IP's should be checked to verify if they are remote users.

Queso fingerprint

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
129.206.170.20	158	158	2	2
199.183.24.194	155	155	3	3
64.64.58.194	59	59	1	1
212.181.52.7	57	57	1	1
158.75.57.4	30	30	13	13

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.202.54	157	157	1	1
10.10.130.135	59	61	1	3
10.10.253.41	57	63	2	4
10.10.217.18	57	57	1	1
10.10.253.42	51	553	1	4

Description
This Snort alert is looking for activity triggered by the Queso tool. Queso is an O/S fingerprinting tool that sends packets and awaits the response from the targeted machine. From this, Queso is able to identify the O/S based on these responses. All the source IP's listed above

were conducting scans on various services. One was using the Gnutella destination port, which could be an attempt to mask the Queso fingerprint as Gnutella traffic since Queso can specify which destination port to use.

```
06/02-03:23:36.489765 [**] Queso fingerprint [**] 158.75.57.4:51104-> 10.10.202.158:6346
06/02-03:23:45.489060 [**] Queso fingerprint [**] 158.75.57.4:51104-> 10.10.202.158:6346
```

Possible trojan server activity

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
10.10.60.16	153	192	34	35
199.77.233.177	27	27	12	12
203.249.80.54	26	26	19	19
210.151.21.120	18	18	14	14
10.10.105.120	15	15	6	6

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.218.150	13	43	5	11
10.10.60.16	9	16	9	14
216.15.246.27	9	11	1	1
10.10.105.120	7	8	3	4
216.15.246.8	7	8	1	1

Description
This Snort alert is looking for activity trying to connect to a known Trojan port. The top source IP is an internal address 10.10.60.16 appears to be connecting to a machine 216.15.246.2 at port 27374, known for the Sub Seven port. See Detect # 5 above for more information on this attack.

```
06/02-12:46:33.056143 [**] Possible trojan server activity [**] 10.10.60.16:4970-> 216.15.246.2:27374
06/02-12:46:33.056508 [**] Possible trojan server activity [**] 10.10.60.16:1067-> 216.15.246.2:27374
```

This could be an indication that the host 10.10.60.16 has been compromised with the Sub Seven Trojan and is responding to stimulus from a Sub Seven client.

```
06/02-12:34:46.277215 [**] Possible trojan server activity [**] 202.186.124.1:27374-> 10.10.60.16:2656
06/02-12:43:33.550831 [**] Possible trojan server activity [**] 216.15.246.1:27374-> 10.10.60.16:1062
06/02-12:44:58.591243 [**] Possible trojan server activity [**] 216.15.129.3:27374-> 10.10.60.16:1213
```

connect to 515 from outside

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
210.68.134.22	223	223	201	201
216.223.43.1	221	221	151	151
255.255.255.255	5	5	5	5

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.137.123	4	8	3	6
10.10.137.132	3	5	2	4
10.10.132.83	3	6	2	5
10.10.132.81	3	5	2	4
10.10.132.59	3	4	2	3

Description
This Snort alert is looking for machines trying to connect to port 515 from outside the local network. Port 515 is the Linux printer daemon. This daemon provides printing for remote users to a local printer. An attacker can exploit this by overflowing the buffer to crash the daemon or execute code as "super user." The hosts' 210.68.134.22 and 216.223.43.1 are actively scanning for any Linux machine running the daemon to respond.

```
06/03-09:50:07.073071 [**] connect to 515 from outside [**] 210.68.134.22:1815-> 10.10.132.41:515
06/03-09:50:07.076112 [**] connect to 515 from outside [**] 210.68.134.22:1828-> 10.10.132.54:515
```

06/07-06:21:58.516517 [**] connect to 515 from outside [**] 216.223.43.1:2477-> 10.10.137.132:515
06/07-06:21:58.516616 [**] connect to 515 from outside [**] 216.223.43.1:2475-> 10.10.137.130:515

The traffic from host 255.255.255.255 appears to have been crafted, as this is not a valid IP and usually associated with a broadcast address.

06/03-14:36:30.623742 [**] connect to 515 from outside [**] 255.255.255.255:31337-> 10.10.132.32:515
06/04-09:56:22.301178 [**] connect to 515 from outside [**] 255.255.255.255:31337-> 10.10.132.51:515

Reference for Linux printer daemon:
http://www.securityfocus.com/frames/?content=/templates/advisory.html%3Fid%3D3374

WinGate 1080 Attempt

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
216.209.172.30	77	77	67	67
217.10.143.54	57	57	14	14
204.117.70.5	21	21	5	5
216.15.205.2	20	20	9	9
195.66.170.8	17	17	4	4

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.218.150	30	43	7	11
10.10.217.58	26	30	5	8
10.10.60.38	15	19	7	10
10.10.60.11	14	22	7	10
10.10.60.39	14	17	3	5

Description
This Snort alert is looking for attackers trying to use Wingate, a proxy software package, which allows multiple computers to share a single Internet connection. Attackers try to bounce traffic

off the proxy machine to maliciously attack another machine so that it appears that the proxy machine is the attacker. All the source IP's listed above were involved with attempting connections to the internal hosts as a point of attack. It appears that a script was used to run down through a internal subnet and attempt to find any machines running the proxy software. Then the attacker would use the internal host's proxy software.

```
06/04-20:49:32.456967 [**] WinGate 1080 Attempt [**] 216.209.172.30:2771-> 10.10.1.12:1080
06/04-20:49:33.256210 [**] WinGate 1080 Attempt [**] 216.209.172.30:2786-> 10.10.1.15:1080
```

```
06/02-17:35:34.193671 [**] WinGate 1080 Attempt [**] 217.10.143.54:33882-> 10.10.217.58:1080
06/02-17:35:43.173253 [**] WinGate 1080 Attempt [**] 217.10.143.54:33882-> 10.10.217.58:1080
```

SYN-FIN scan!

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
211.114.44.2	156	156	156	156
194.159.245.16	1	1	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.223.140	1	1	1	1
10.10.15.101	1	1	1	1
10.10.183.233	1	1	1	1
10.10.71.12	1	1	1	1
10.10.215.172	1	1	1	1

Description
This Snort alert is looking at the TCP header for the SYN and FIN flags set simultaneously, which does not occur under normal circumstances. The SYN and FIN flags are set when a attacker crafts the packet in an attempt to evade detection by an IDS software or perform an O/S fingerprint. In this case, attacks primarily came from host 211.114.44.2 and all 156 SYN-FIN scans were directed at port 21, the FTP service on various machines within the local network. A good indication of this was also detected in the Snort scan files and is listed below in that analysis section. The ports listed below for the source IP are definitely not normal.

```
06/06-13:35:53.331536 [**] SYN-FIN scan! [**] 211.114.44.2:21-> 10.10.2.111:21
06/06-13:36:03.124093 [**] SYN-FIN scan! [**] 211.114.44.2:21-> 10.10.4.90:21
```

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

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
10.10.253.24	20	39	3	5
10.10.6.34	16	19	1	2
207.172.4.98	15	15	1	1
141.211.14.27	10	10	1	1
12.18.36.220	10	10	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.253.24	19	22	3	5
207.172.4.98	16	16	1	1
10.10.6.34	15	16	1	2
141.211.14.27	10	10	1	1
10.10.253.112	10	10	1	1

Description
This Snort alert is looking at TCP traffic with port 55850, which has been associated with myserver activity. Myserver is a DDOS tool that binds to port 55850 and installs a root kit that runs under “ls” and “ps”. Looking at the Snort alert files, it appears that some internal hosts have been compromised as suggested by the 2-way traffic below.

```
06/06-10:09:54.638665 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 10.10.253.24:55850-> 141.211.14.27:25
```

```
06/06-10:09:55.898236 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 141.211.14.27:25-> 10.10.253.24:55850
```

06/06-01:37:45.400610 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 10.10.6.34:55850-> 207.172.4.98:25

06/06-01:37:45.430704 [**] Port 55850 tcp - Possible myserver activity - ref. 010313-1 [**] 207.172.4.98:25-> 10.10.6.34:55850

TCP SRC and DST outside network

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
172.140.92.219	16	17	6	7
172.140.52.198	16	16	8	8
192.168.1.101	11	11	2	2
172.140.47.155	8	8	4	4
172.140.88.120	6	6	5	5

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
202.158.92.81	6	6	2	2
205.188.6.110	6	6	1	1
64.4.13.51	5	5	1	1
24.45.107.108	4	4	2	2
202.158.92.72	4	4	2	2

Description
This Snort alert is looking for any TCP traffic that has a source and destination IP address outside the local network. Since all internal IP addresses are in the 10.10.x.x range, any source traffic that does not have this designation could be considered spoofing by another party using the 10.10.x.x network as actual return path. The following traffic could be Sub Seven traffic since a majority of the alerts have a source port of 27374.

06/07-21:52:42.918765 [**] TCP SRC and DST outside network [**] 172.140.92.219:27374-> 202.158.92.81:4957

06/07-21:52:45.846096 [**] TCP SRC and DST outside network [**] 172.140.92.219:27374-> 202.158.92.81:4957

06/07-19:21:06.341783 [**] TCP SRC and DST outside network [**] 172.140.52.198:27374-> 213.236.223.42:3244

This traffic is a internal machine that appears to still have an old assigned 192.168.x.x. IP, which would be an indication that it did not receive a new IP from the DHCP server. The destination port 5190 is known for the AOL Instant Messenger port and port 1863 is known for MSN Messenger.

06/04-02:25:17.121475 [**] TCP SRC and DST outside network [**] 192.168.1.101:1109-> 205.188.6.110:5190

06/04-02:25:26.504091 [**] TCP SRC and DST outside network [**] 192.168.1.101:1026-> 64.4.13.51:1863

06/07-16:06:04.134055 [**] TCP SRC and DST outside network [**] 172.140.47.155:27374-> 208.233.253.86:4126

06/07-16:06:12.982149 [**] TCP SRC and DST outside network [**] 172.140.47.155:27374-> 208.233.253.86:4126

06/07-14:47:05.845686 [**] TCP SRC and DST outside network [**] 172.140.88.120:27374-> 165.1.20.210:2976

06/07-15:01:01.326996 [**] TCP SRC and DST outside network [**] 172.140.88.120:27374-> 213.96.184.30:3390

High port 65535 tcp - possible Red Worm – traffic

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
10.10.253.24	19	39	2	5
10.10.6.47	15	16	2	3
10.10.6.44	9	14	1	1
10.10.253.53	9	9	1	1
10.10.253.51	8	8	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
64.12.136.5	13	13	2	2
193.252.19.156	12	12	1	1
64.50.191.56	9	14	1	1
136.159.34.53	9	9	1	1
207.239.96.242	8	8	1	1

Description

This Snort alert is looking at TCP traffic with port 65535, which has been known to be associated with the Adore Worm exploit, previously known as the Red Worm. Adore scans the Internet checking Linux hosts to determine whether they are vulnerable to any of the following well-known exploits: LPRng, rpc-statd, wu-ftpd and BIND. The following snippet of alerts shows that some internal hosts could be infected with this exploit.

```
06/03-22:16:31.121115 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.253.24:25->
193.252.19.156:65535
06/03-22:17:01.404797 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.253.24:25->
193.252.19.156:65535
```

```
06/07-20:28:15.267798 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.6.47:25->
24.0.95.81:65535
06/07-20:28:15.493789 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.6.47:25->
24.0.95.81:65535
```

```
06/05-13:52:37.559418 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.6.44:110->
64.50.191.56:65535
06/05-13:52:37.560758 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.6.44:110->
64.50.191.56:65535
```

```
06/03-09:08:15.029475 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.253.53:65535->
136.159.34.53:25
```

06/03-09:08:15.067896 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.253.53:65535-> 136.159.34.53:25

06/05-10:54:05.901493 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.253.51:65535-> 207.239.96.242:25

06/05-10:54:06.055085 [**] High port 65535 tcp - possible Red Worm - traffic [**] 10.10.253.51:65535-> 207.239.96.242:25

Reference on Adore (Red) Worm:
http://www.sans.org/y2k/adore.htm

Tiny Fragments - Possible Hostile Activity

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
66.72.115.95	60	60	1	1
211.35.66.163	3	3	1	1
212.58.180.135	2	2	1	1
202.39.78.125	1	1	1	1

All Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.150.133	60	184	1	14
10.10.153.243	3	3	1	1
10.10.70.27	2	25	1	9
10.10.98.121	1	5	1	3

Description
This Snort alert is looking for tiny fragments, which sometimes occur when a destination machine tells a sending machine that the packet is too large, so the sending machine will break up the packet into fragments that are assembled at the destination machine. Attackers were able to maliciously craft the packet so that the fragment ID numbers would overlap and cause the destination machine to crash or avoid detection since some IDS software only checked the very first fragmented packet as well as evading firewalls. One well-known fragmentation attack is the Teardrop attack.

06/02-21:13:30.692894 [**] Tiny Fragments - Possible Hostile Activity [**] 66.72.115.95 -> 10.10.150.133
06/02-21:13:30.782870 [**] Tiny Fragments - Possible Hostile Activity [**] 66.72.115.95 -> 10.10.150.133
06/07-11:27:20.313192 [**] Tiny Fragments - Possible Hostile Activity [**] 211.35.66.163 -> 10.10.153.243
06/07-11:27:21.083467 [**] Tiny Fragments - Possible Hostile Activity [**] 211.35.66.163 -> 10.10.153.243

06/02-18:35:36.634455 [**] Tiny Fragments - Possible Hostile Activity [**] 212.58.180.135 -> 10.10.70.27
06/02-18:36:06.828035 [**] Tiny Fragments - Possible Hostile Activity [**] 212.58.180.135 -> 10.10.70.27
06/06-16:38:31.016308 [**] Tiny Fragments - Possible Hostile Activity [**] 202.39.78.125 -> 10.10.98.121

NMAP TCP ping!

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
209.135.37.205	32	32	3	3
202.187.24.3	4	4	3	3
199.197.130.21	2	2	2	2
216.0.105.48	2	2	2	2
206.26.196.253	1	1	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.1.8	20	20	1	1
10.10.1.10	6	6	1	1
10.10.1.9	6	7	1	2
10.10.1.3	4	10	4	5
10.10.100.165	3	3	2	2

Description
This Snort alert is looking for traffic generated by using the NMAP tool. NMAP can ping a target with certain TCP characteristics. NMAP, like Queso, is an O/S fingerprinting tool that

sends packets and awaits the response in order to determine the O/S. This traffic is interesting, as it appears that the attacker is trying to mask NMAP tool as DNS requests and web server access.

06/02-10:01:29.854224 [**] NMAP TCP ping! [**] 209.135.37.205:80-> 10.10.1.8:53
06/02-10:01:29.854290 [**] NMAP TCP ping! [**] 209.135.37.205:53-> 10.10.1.8:53
06/02-10:01:34.852592 [**] NMAP TCP ping! [**] 209.135.37.205:80-> 10.10.1.8:53
06/02-10:01:34.852656 [**] NMAP TCP ping! [**] 209.135.37.205:53-> 10.10.1.8:53

Null scan!

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.29.186.167	7	7	1	1
24.79.67.190	6	6	1	1
134.91.241.144	4	4	1	1
24.3.23.47	4	4	1	1
24.201.107.143	3	5	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.150.220	9	39	3	8
10.10.217.62	7	7	1	1
10.10.5.29	4	6	1	2
10.10.98.194	4	4	1	1
10.10.150.133	4	184	3	14

Description
This Snort alert is looking at the TCP header with no flags set. This as with the above SYN-FIN alert is abnormal TCP header activity. This is another attempt for hackers to evade detection by IDS software or performing an O/S fingerprint by crafting a packet with no options set, thus breaking the TCP/IP rules. The ports were destined to included KaZaa, Gnutella, SSL, Westwood Online and the Ultors Trojan to name some. The IP address range is mostly with the @Home network known for Cable modems.

06/05-02:12:48.953593 [**] Null scan! [**] 24.29.186.167:3872-> 10.10.217.62:512

06/05-02:12:59.798522 [**] Null scan! [**] 24.29.186.167:3872-> 10.10.217.62:6

06/05-01:28:59.283573 [**] Null scan! [**] 24.79.67.190:1847-> 10.10.150.220:1234

06/05-01:37:43.005096 [**] Null scan! [**] 24.79.67.190:1847-> 10.10.150.220:1234

06/03-09:14:44.943099 [**] Null scan! [**] 134.91.241.144:1586-> 10.10.98.194:1214

06/03-09:16:33.096232 [**] Null scan! [**] 134.91.241.144:1586-> 10.10.98.194:1214

06/04-11:41:33.699486 [**] Null scan! [**] 24.3.23.47:3750-> 10.10.5.29:443

06/04-11:43:31.017347 [**] Null scan! [**] 24.3.23.47:3750-> 10.10.5.29:443

06/06-19:14:33.558163 [**] Null scan! [**] 24.201.107.143:6346-> 10.10.218.22:1750

06/06-19:16:15.027522 [**] Queso fingerprint [**] 24.201.107.143:13-> 10.10.218.22:6346

connect to 515 from inside

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
10.10.60.16	35	192	25	35
10.10.179.78	2	3	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
216.15.246.10	4	10	1	1
216.15.246.9	4	11	1	1
24.13.123.8	2	3	1	1
216.15.246.3	2	9	1	1
216.15.246.20	2	6	1	1

Description
This Snort alert is looking for machines trying to connect to port 515 from inside the local network. Port 515 is the Linux printer daemon. This is similar to the connect to 515 from outside alert signature above. This is more then likely false positive as the destinations were mainly directed at Cybercon and are probably authorized. There was one @Home cable network IP that should be looked at if printing to an offsite is against company policy.

Server used for this query: [whois.arin.net]

Cybercon, Inc. (NETBLK-CYBERCON-BLK1)
4534 N. Lindbergh Blvd, Suite 430 - 438
St. Louis, MO 63044
US

Netname: CYBERCON-BLK1
Netblock: 216.15.128.0 - 216.15.255.255
Maintainer: CBCN

Coordinator:
CHEN, JOSHUA (JZC-ARIN) josh@cybercon.com
314-621-9991 (FAX) 314-212-9530

Domain System inverse mapping provided by:

NS1.CYBERCON.COM 216.15.129.2
NS2.CYBERCON.COM 216.15.129.3

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 04-May-2001.
Database last updated on 30-Jul-2001 23:01:54 EDT.

```
06/02-12:43:33.716013 [**] connect to 515 from inside [**] 10.10.60.16:1242-> 216.15.246.1:515
06/02-12:43:34.015849 [**] connect to 515 from inside [**] 10.10.60.16:1430-> 216.15.246.1:515
```

```
06/07-12:34:02.553850 [**] connect to 515 from inside [**] 10.10.179.78:56805-> 24.13.123.8:515
```

Back Orifice

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))

203.107.244.130	21	21	21	21
203.45.203.107	4	4	4	4

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.98.67	1	1	1	1
10.10.98.69	1	1	1	1
10.10.98.220	1	1	1	1
10.10.98.212	1	1	1	1
10.10.97.234	1	4	1	2

Description
This Snort alert is looking for traffic directed at port 31337, which is the default port of the Trojan Back Orifice. Back Orifice is a backdoor Trojan that allows a hacker to be able to view files and shutdown the system to name a few. All modern Anti-Virus software with the latest updates usually will detect this if found on a system.

```
06/07-09:23:22.635046 [**] Back Orifice [**] 203.107.244.130:31338-> 10.10.98.56:31337
06/07-09:23:22.680619 [**] Back Orifice [**] 203.107.244.130:31338-> 10.10.98.67:31337
```

```
06/03-08:59:02.366265 [**] Back Orifice [**] 203.45.203.107:1466-> 10.10.98.165:31337
06/03-09:56:00.685103 [**] Back Orifice [**] 203.45.203.107:3897-> 10.10.97.234:31337
```

SUNRPC highport access!

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
35.9.37.225	19	19	1	1

All Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.100.153	19	19	1	1

Description
This Snort alert is looking for traffic with high port numbers which in most indications, an attempt to exploit the Sun RPC daemon. RPC server programs are remote procedures that use ephemeral ports, not well-known ports. This requires a "registrar" of some sort that keeps track of which RPC programs are using which ports. In Sun RPC this registrar is called the portmapper. One of the ports Sun systems RPC uses is 32771. The following snippet of alerts shows a definite attempt to connect. The IP is within the Michigan State University's network and schools have been notorious for malicious traffic.

```
06/04-08:56:30.671990 [**] SUNRPC highport access! [**] 35.9.37.225:21-> 10.10.100.153:32771
06/04-08:56:30.804900 [**] SUNRPC highport access! [**] 35.9.37.225:21-> 10.10.100.153:32771
```

Server used for this query: [whois.arin.net]

```
Merit Network Inc. (NET-MERIT)  MERIT          35.0.0.0 - 35.255.255.255
Michigan State University (NETBLK-MICH-618) MICH-618  35.8.0.0 - 35.10.255.25
```

Attempted Sun RPC high port access

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
205.188.153.99	5	5	1	1
128.183.10.134	1	1	1	1

All Destinations receiving this attack signature

Destinations	**# Alerts (sig)**	**# Alerts (total)**	**# Srcs (sig)**	**# Srcs (total))**
10.10.217.226	5	5	1	1
10.10.98.196	1	1	1	1

Description
This Snort alert is looking for traffic that attempts to access high ports usually associated with the Sun RPC daemon. Refer to SUNRPC highport access signature alert above for more information.

```
06/04-20:12:01.404170 [**] Attempted Sun RPC high port access [**] 205.188.153.99:4000->
10.10.217.226:32771
06/04-20:12:28.924052 [**] Attempted Sun RPC high port access [**] 205.188.153.99:4000->
```

10.10.217.226:32771

This detect could be a response to a DNS query hence the alerted high port access.

06/06-23:46:39.149770 [**] Attempted Sun RPC high port access [**] 128.183.10.134:53-> 10.10.98.196:32771

ICMP SRC and DST outside network

Top 5 Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
192.168.1.4	2	39	1	3
172.166.173.212	1	1	1	1
172.136.202.36	1	1	1	1
172.140.92.219	1	17	1	7
172.128.219.132	1	1	1	1

Top 5 Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
216.158.50.7	2	5	1	1
24.28.80.186	1	1	1	1
212.251.59.178	1	1	1	1
206.109.96.42	1	1	1	1
38.233.249.15	1	1	1	1

Description
This Snort alert is looking at ICMP traffic with source and destination IP addresses outside the local network. This could be an indication of IP spoofing of the internal addresses. Most likely this particular alert is an internal machine, from a different network that uses the 192.168.x.x IP assignment, which did not receive a new IP address from the DHCP server.

06/05-17:00:33.342664 [**] ICMP SRC and DST outside network [**] 192.168.1.4 -> 216.158.50.7

06/05-17:00:39.393799 [**] ICMP SRC and DST outside network [**] 192.168.1.4 -> 216.158.50.7

Probable NMAP fingerprint attempt

All Sources triggering this attack signature

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total))
24.201.107.143	1	5	1	1

All Destinations receiving this attack signature

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total))
10.10.218.22	1	6	1	2

Description
This Snort alert is looking for traffic that has characteristics of the NMAP fingerprinting tool. See the NMAP TCP ping above for more information regarding NMAP. In this case, the source IP24.201.107.143 is sending data back on a known Gnutella port. This is most likely what is occurring since Gnutella can use TCP 6346 as a possible port.

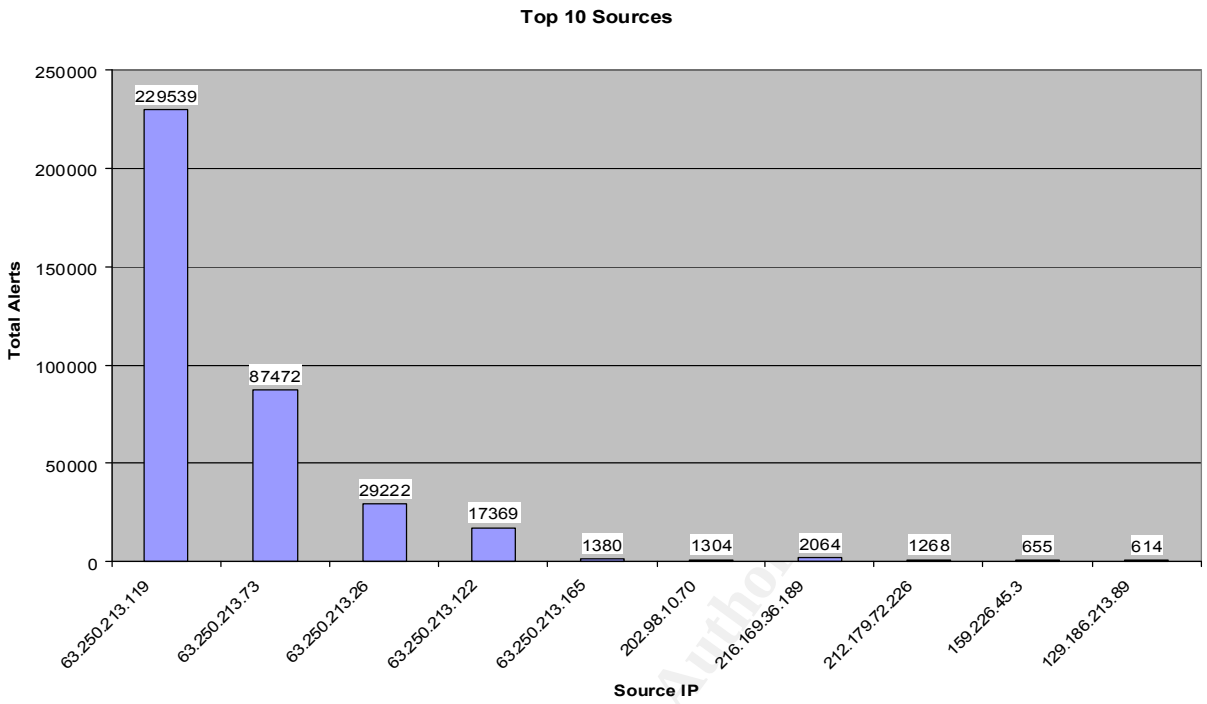
```
06/06-19:18:05.103859 [**] Probable NMAP fingerprint attempt [**] 24.201.107.143:6346-> 10.10.218.22:1750
```

Top Talkers by Source

The following are the biggest offenders and the top talker targets out of all the Snort alerts. Whois queries were done for the top 10 sources of Snort alerts.

Top 10 Alert Sources

Source IP	# Alerts (total)
63.250.213.119	229539
63.250.213.73	87472
63.250.213.26	29222
63.250.213.122	17369
63.250.213.165	1380
202.98.10.70	1304
216.169.36.189	2064
212.179.72.226	1268
159.226.45.3	655
129.186.213.89	614



Top 10 Alert Sources External Address and Registration Information

Source IP's:
63.250.213.119, 63.250.213.73, 63.250.213.26, 63.250.213.122, 63.250.213.165

Server used for this query: [whois.arin.net]

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

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

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

Domain System inverse mapping provided by:

NS.BROADCAST.COM 206.190.32.2

NS2.BROADCAST.COM 206.190.32.3

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 29-Jun-2001.
Database last updated on 28-Jul-2001 23:02:36 EDT.

Source IP:
202.98.10.70

Server used for this query: [whois.apnic.net]

% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois6.apnic.net)

inetnum: 202.98.0.0 - 202.98.31.255
netname: CHINANET-JL
descr: CHINANET Jilin province network
descr: Data Communication Division
descr: China Telecom
country: CN
admin-c: CH93-AP
tech-c: XY1-AP
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINANET-JL
changed: hostmaster@ns.chinanet.cn.net 20000101
source: APNIC

person: Chinanet Hostmaster
address: A12,Xin-Jie-Kou-Wai Street
country: CN
phone: +86-10-62370437
fax-no: +86-10-62053995
e-mail: hostmaster@ns.chinanet.cn.net
nic-hdl: CH93-AP
mnt-by: MAINT-CHINANET
changed: hostmaster@ns.chinanet.cn.net 20000101
source: APNIC

person: Xu Yongzhong
address: Data Communication Bireau
address: Ministry of Posts and Telecommunications
address: A12 Xin-jie-kou-wai Street
address: Beijing 100088
country: CN
phone: +86-10-62053991

fax-no: +86-10-62053995
e-mail: yzxu@publicf.bta.net.cn
nic-hdl: XY1-AP
mnt-by: MAINT-NULL
changed: hostmaster@apnic.net 19960319
source: APNIC

Source IP:
216.169.36.189

Server used for this query: [whois.arin.net]

Interconnect Services, Inc. (NETBLK-INTERCONNECT)
530 South Tancahua
Corpus Christi, TX 78401
US

Netname: INTERCONNECT
Netblock: 216.169.32.0 - 216.169.63.255
Maintainer: ISVS

Coordinator:
Adams, Brian (BA70-ARIN) badams@INTERCONNECT.NET
361-884-3447 (FAX) 361-882-2280

Domain System inverse mapping provided by:

NS1.INTERCONNECT.NET	216.169.32.2
NS2.INTERCONNECT.NET	216.169.32.3

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 24-Mar-2000.
Database last updated on 28-Jul-2001 23:02:36 EDT.

Source IP:
212.179.72.226

Server used for this query: [whois.ripe.net]

% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 212.179.72.224 - 212.179.72.239
netname: KESHET
descr: KESHET-LAN
country: IL
admin-c: ES4966-RIPE
tech-c: NP469-RIPE
status: ASSIGNED PA
notify: hostmaster@isdn.net.il
mnt-by: RIPE-NCC-NONE-MNT
changed: hostmaster@isdn.net.il 20000320
source: RIPE

route: 212.179.0.0/17
descr: ISDN Net Ltd.
origin: AS8551
notify: hostmaster@isdn.net.il
mnt-by: AS8551-MNT
changed: hostmaster@isdn.net.il 19990610
source: RIPE

person: Eran Shchori
address: BEZEQ INTERNATIONAL
address: 40 Hashacham Street
address: Petach-Tikva 49170 Israel
phone: +972 3 9257710
fax-no: +972 3 9257726
e-mail: hostmaster@bezeqint.net
nic-hdl: ES4966-RIPE
changed: registrar@ns.il 20000309
source: RIPE

person: Nati Pinko
address: Bezeq International
address: 40 Hashacham St.
address: Petach Tikvah Israel
phone: +972 3 9257761
e-mail: hostmaster@isdn.net.il
nic-hdl: NP469-RIPE
changed: registrar@ns.il 19990902
source: RIPE

Source IP:
159.226.45.3

Server used for this query: [whois.arin.net]

The Computer Network Center Chinese Academy of Sciences (NET-NCFC)
P.O. Box 2704-10,
Institute of Computing Technology Chinese Academy of Sciences
Beijing 100080, China
CN

Netname: NCFC
Netblock: 159.226.0.0 - 159.226.255.255

Coordinator:
Qian, Haulin (QH3-ARIN) hlqian@NS.CNC.AC.CN
+86 1 2569960

Domain System inverse mapping provided by:

NS.CNC.AC.CN	159.226.1.1
GINGKO.ICT.AC.CN	159.226.40.1

Record last updated on 25-Jul-1994.
Database last updated on 28-Jul-2001 23:02:36 EDT.

Source IP:
129.186.213.89

Server used for this query: [whois.arin.net]

Iowa State University (NET-CYCLONENET)
291 Durham Hall
Ames, IA 50011
US

Netname: CYCLONENET
Netblock: 129.186.0.0 - 129.186.255.255

Coordinator:
Contact, Technical (TC42-ARIN) tech-contact@IASTATE.EDU
515-294-2256

Domain System inverse mapping provided by:

NS-3.IASTATE.EDU	129.186.142.200
NS-2.IASTATE.EDU	129.186.140.200
NS-1.IASTATE.EDU	129.186.1.200
SCSDS.AMESLAB.GOV	147.155.1.1

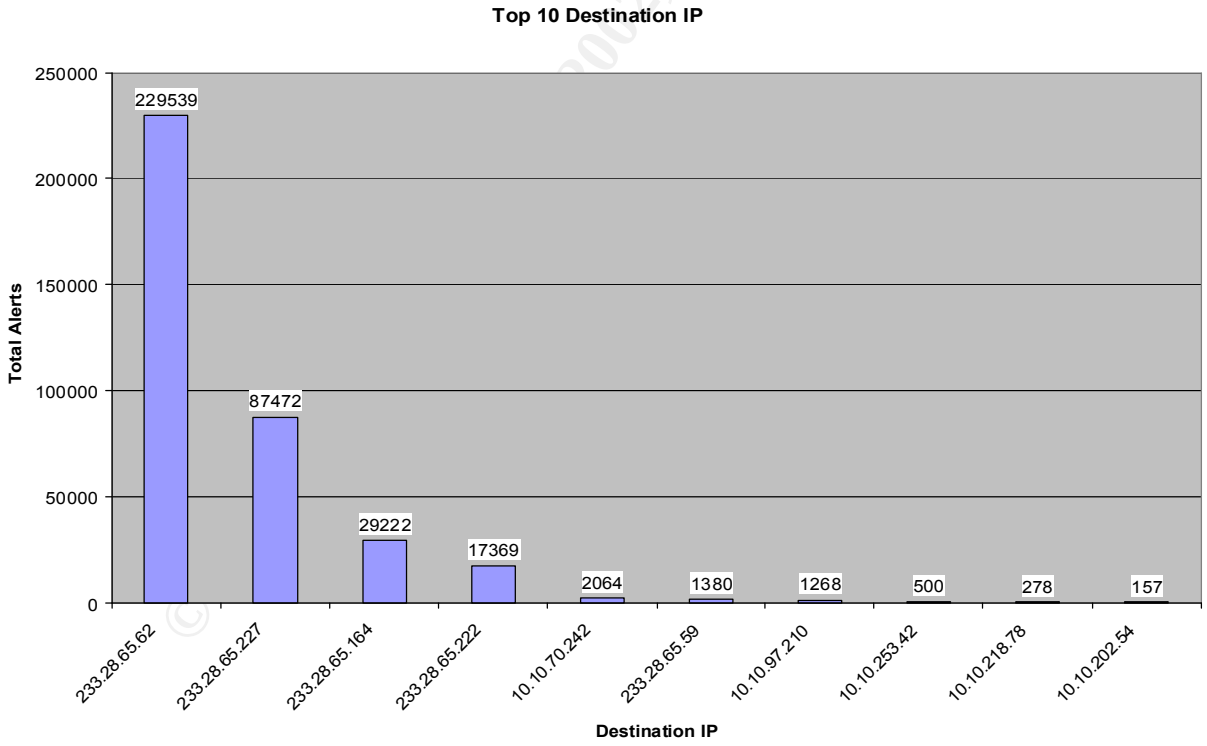
Record last updated on 10-Apr-1998.

Database last updated on 28-Jul-2001 23:02:36 EDT.

Top Talkers by Destination

Top 10 Alert Destinations

Destinations IP	# Alerts (total)
233.28.65.62	229539
233.28.65.227	87472
233.28.65.164	29222
233.28.65.222	17369
10.10.70.242	2064
233.28.65.59	1380
10.10.97.210	1268
10.10.253.42	500
10.10.218.78	278
10.10.202.54	157



Snort Scan Data Summary (297,097 Total Scans)

The top 5 scan signatures were concentrated on since they accounted for approximately 99% of the 297,097 total scans. This by all means does not mean that the other scan signature types should be ignored. It just shows where the majority of the scans were classified as, while others were just not as active as the 5 signatures below were.

Signature (click for definition)	# Alerts	# Sources	# Destinations
TCP **S***** scan	179301	171	33057
UDP scan	116692	190	24719
TCP 21S***** scan	532	32	49
TCP **SF**** scan	157	2	157
TCP ******** scan	50	21	14

TCP **S*** scan**

Looking at the chart above under the TCP SYN scan signature the top 5 scanners were 2 internal hosts and 3 external hosts.

```
Jun 2 12:43:33 10.10.60.16:4878-> 216.15.246.1:211 SYN **S*****
Jun 2 12:43:33 10.10.60.16:4879-> 216.15.246.1:11 SYN **S*****
Jun 2 12:43:33 10.10.60.16:4880-> 216.15.246.1:67 SYN **S*****
```

```
Jun 7 11:32:42 10.10.179.78:37856-> 24.13.123.8:12346 SYN **S*****
Jun 7 11:32:42 10.10.179.78:37846-> 24.13.123.8:233 SYN **S*****
```

Host 10.10.60.16 and 10.10.179.78 appear to be involved with scanning of external IP addresses or have been compromised as the evidence of active scanning for open services. Host 10.10.60.16 was involved in 97,134 SYN scans directed at 45 different IP's. This host scanned every machine within 216.15.246.1 to 216.15.246.34 and 11 other random IP's. While host 10.10.179.78 was involved in 8,603 SYN scans directed at a 4 different machines, particularly IP 24.13.123.8, which saw approximately 99% of the 8,603 scans. There is definite scanning occurring from inside the network.

```
Jun 2 18:52:45 10.10.97.223:2314-> 161.74.133.160:1214 SYN **S*****
Jun 2 18:52:45 10.10.97.223:2312-> 141.18.60.121:1214 SYN **S*****
```

```
Jun 4 00:41:46 10.10.98.161:1101-> 206.142.53.31:1214 SYN **S*****
```

There is more then one host sending SYN packets directed at port 1214 which is used by the KAZAA program. This program is similar to Gnutella or Bearshare, where you connect to peers to engage in file transferring from to individual machines of mp3's, movies, and software. Upon further investigation, it looks like an employee is using the software and told fellow coworkers about it and thus all the external traffic that Snort is alerting on. A Snort rule could be made to specifically look for this KAZAA signature since it uses port 1214.

```
Jun 7 11:12:11 61.219.90.189:21-> 10.10.1.3:21 SYN **S*****
Jun 7 11:12:11 61.219.90.189:21-> 10.10.1.1:21 SYN **S*****
```

```
Jun 2 09:14:20 217.136.37.76:4211-> 10.10.2.35:21 SYN **S*****
Jun 2 09:14:20 217.136.37.76:4231-> 10.10.2.46:21 SYN **S*****
```

```
Jun 5 01:35:19 217.75.226.210:1570-> 10.10.1.83:53 SYN **S*****
Jun 5 01:35:19 217.75.226.210:1577-> 10.10.1.90:53 SYN **S*****
```

Host 61.219.90.189 and 217.136.37.76 were scanning at port 21 within the local network. These hosts are methodically scanning the internal hosts for any FTP servers. Host 217.75.226.210 is actively looking for a DNS server; evidence by the 13,567 scans for port 53. There are numerous DNS exploits posted on Security Focus, SANS and BUGTRAQ mailing list. Port scanning from outside your network is a very common occurrence; please refer to the recommendations section for possible solutions.

UDP scan

Looking at the UDP scans, it has been determined that users in the internal network are using popular online gaming software such as Half Life, Unreal and Starsiege Tribes. Another was connecting to MSN Gaming Zone to participate in online gaming. One host was sending UDP traffic that is used by KProxy, a Internet Connection Sharing software. This may indicate that some users who do not have Internet access are using another machine as a proxy to access the Internet. There was also some Real Player streaming access (port 6970) which depending on your organization's policies may not be warranted.

```
Jun 4 12:59:18 10.10.150.227:28800-> 172.163.117.149:28800 UDP
Jun 4 12:59:18 10.10.150.227:28800-> 62.180.194.176:28800 UDP
```

Jun 5 09:16:58 205.188.233.185:14074-> 10.10.178.188:6970 UDP
Jun 5 09:16:59 205.188.233.185:9010-> 10.10.145.197:6970 UDP

Jun 7 22:11:33 10.10.97.189:9001-> 210.102.61.18:9001 UDP
Jun 7 22:11:33 10.10.97.189:9001-> 211.209.90.7:9001 UDP

TCP 21S*** scan**

The TCP SYN with both reserved bits set scans for the most part was Gnutella traffic when an internal host requested or searched for a certain file. There were also malformed packets directed at some internal machines at the mail services port 25 which could be an indication of O/S Fingerprinting, a DDOS, normal mail traffic with corrupted packets or just a mis-configured application causing errors. TCP/IP rules dictate the SYN packets with any reserved bit set are not normal.

Jun 5 08:26:37 129.206.170.20:35439-> 10.10.202.54:6346 SYN 21S***** RESERVEDBITS
Jun 5 08:26:43 129.206.170.20:35439-> 10.10.202.54:6346 SYN 21S***** RESERVEDBITS

Jun 2 04:14:21 199.183.24.194:57029-> 10.10.253.42:25 SYN 21S***** RESERVEDBITS
Jun 2 05:07:39 199.183.24.194:33048-> 10.10.253.42:25 SYN 21S***** RESERVEDBITS

Jun 7 19:20:22 64.64.58.194:20-> 10.10.130.135:2161 SYN 21S***** RESERVEDBITS
Jun 7 19:20:23 64.64.58.194:20-> 10.10.130.135:2162 SYN 21S***** RESERVEDBITS

Jun 2 15:51:18 212.181.52.7:33156-> 10.10.217.18:1416 SYN 21S***** RESERVEDBITS
Jun 2 15:51:22 212.181.52.7:33158-> 10.10.217.18:1416 SYN 21S***** RESERVEDBITS

TCP **SF** scan**

SYN-FIN scanning for the most part is done by constructing a packet to try and evade an IDS. By setting both the SYN-FIN some IDS software may in fact miss the packet and thereby let into the internal network to the directed machine. TCP/IP rules dictate the SYN-FIN packets are not normal.

```
Jun 6 13:35:53 211.114.44.2:21-> 10.10.2.111:21 SYNFIN **SF****
Jun 6 13:36:03 211.114.44.2:21-> 10.10.4.90:21 SYNFIN **SF****
```

TCP ****** scan**

A TCP packet with no options set is known as a Null scan. This is a crafted packet This as with the above SYN-FIN alert is abnormal TCP header activity. This is another attempt for hackers to evade detection by IDS software or performing an O/S fingerprint by crafting a packet with no options set, thus breaking the TCP/IP rules.

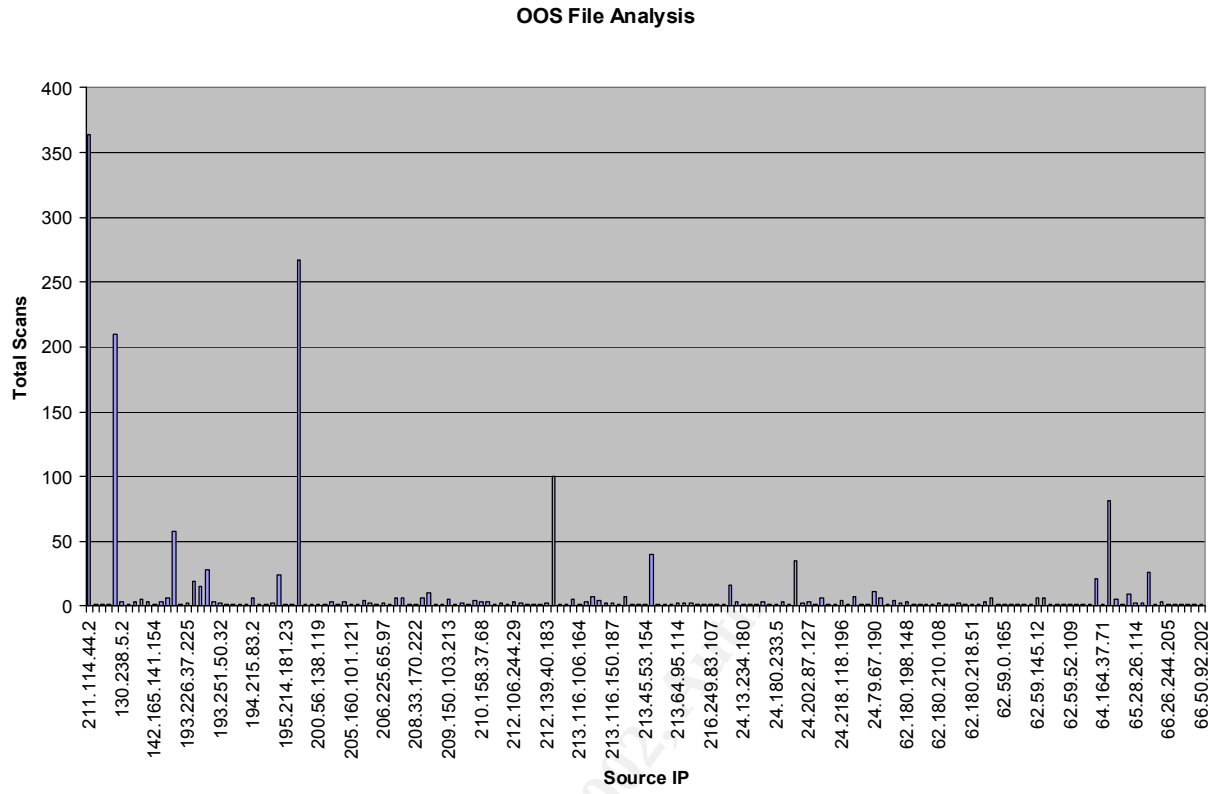
```
Jun 5 02:12:48 24.29.186.167:3872-> 10.10.217.62:512 NULL ********
Jun 5 02:12:59 24.29.186.167:3872-> 10.10.217.62:6 NULL ********
```

Snort OOS Data Summary

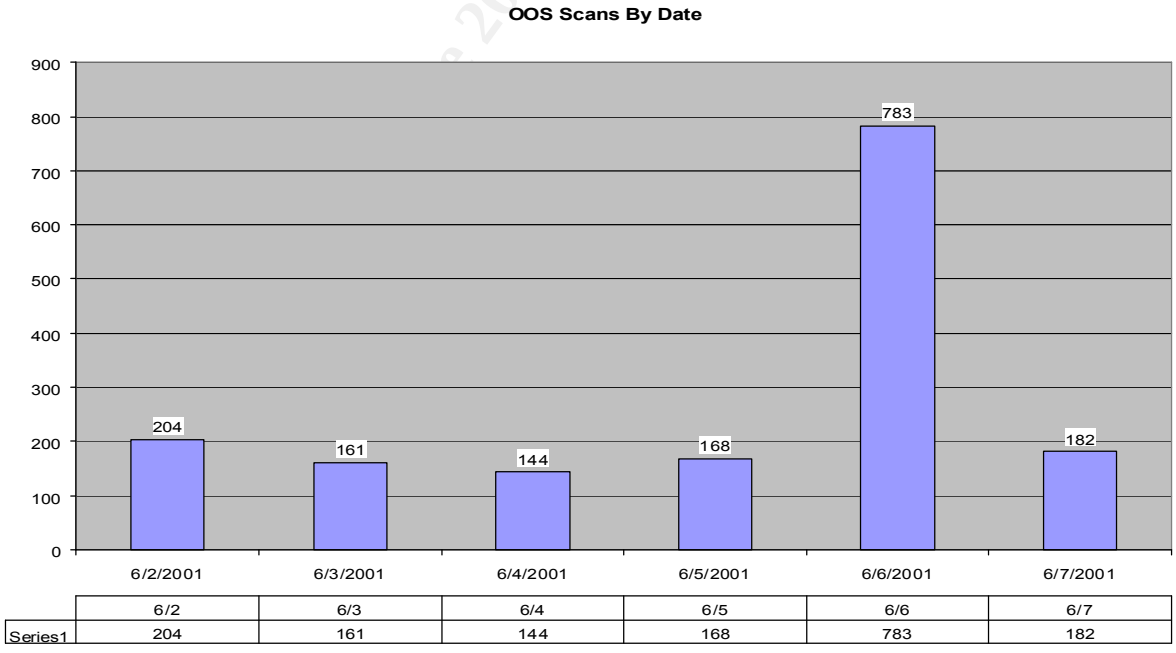
The combined OOS (Out Of Specification) files contained 1642 scan entries. The OOS scans contain alerts that do not fall into any Snort signature and thus are listed as being "out of spec." On the following chart and graph, you can see which hosts were the biggest contributors of OOS scans.

Top 5 OOS Scans by Source

Source IP	Total OOS Scans
211.114.44.2	364
199.183.24.194	267
129.206.170.20	210
212.181.52.7	100
158.75.57.4	58



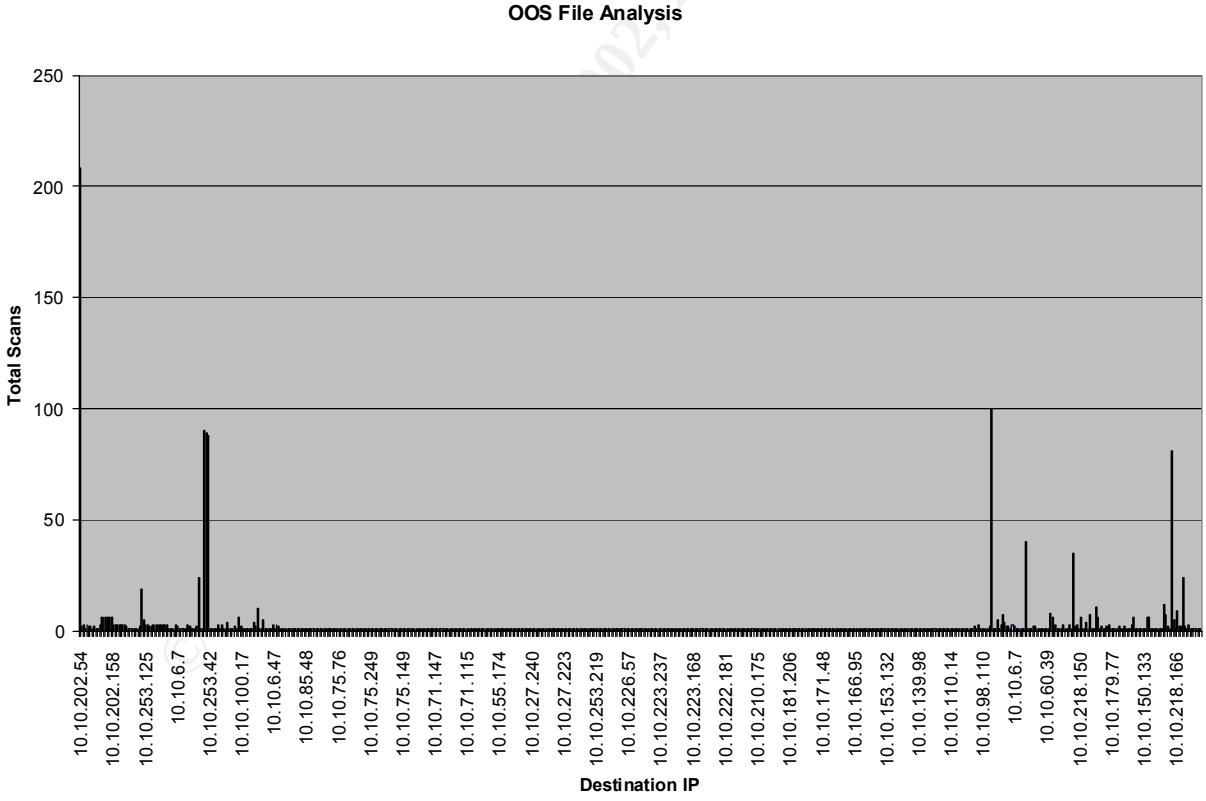
Going further and sorting the alerts by date, the biggest amount of OOS scans occurred on June 6, 2001. Interestingly, June 6 was a Wednesday when most malicious activity you would think would occur on a Friday, Saturday or Sunday.



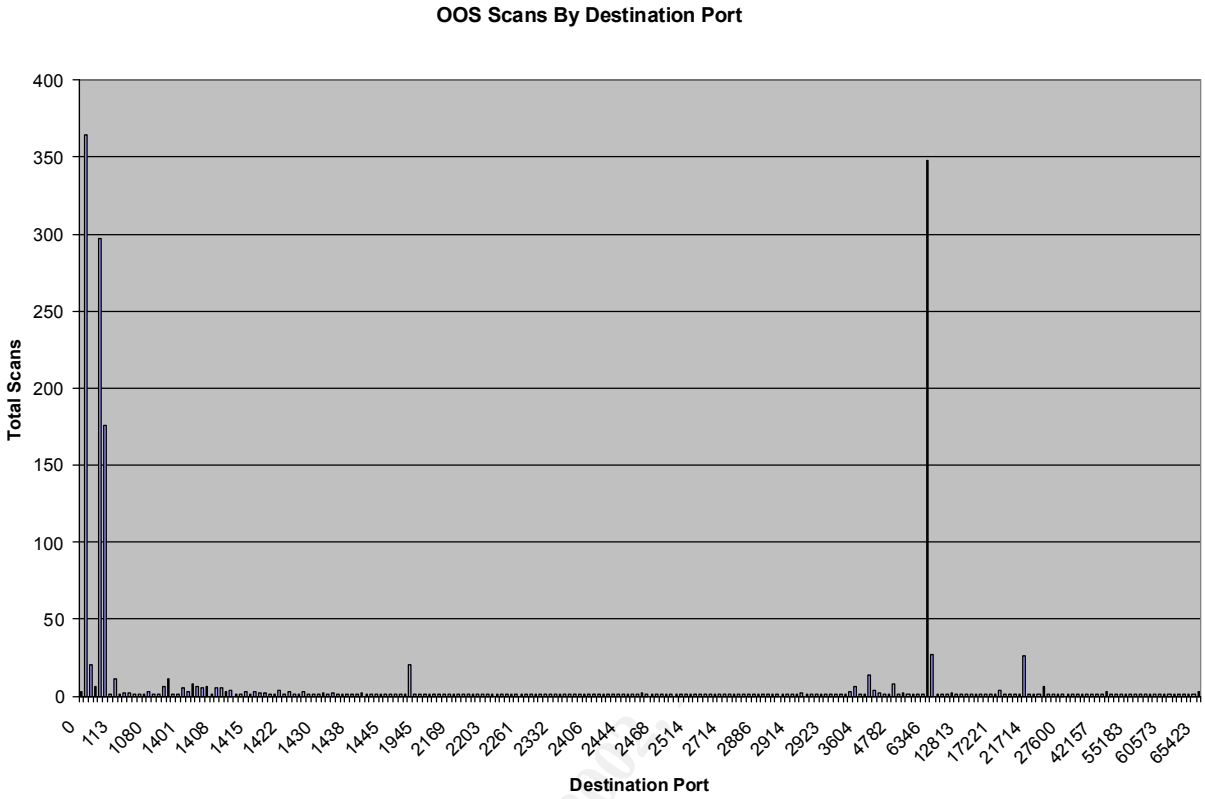
The internal hosts that were most targeted are listed in the following chart and graph. The data was fairly even except for one internal host, which was involved in the most traffic.

Top 10 OOS Destinations

Destination IP	Total Scans
10.10.202.54	208
10.10.217.18	100
10.10.253.43	90
10.10.253.41	89
10.10.253.42	88
10.10.130.135	81
10.10.70.27	40
10.10.253.125	24
10.10.7.98	20
10.10.218.22	15



Then taking the data a bit further to look to where the OOS scans are going to by destination port revealed even more useful information.



The most popular ports stick out quite clearly. The by filtering the data once again to look at the top 20 ports, you can see where in your organization that the most concentrated OOS scans are directed at. These ports alone accounted for roughly 83.5% of all the OOS scans.

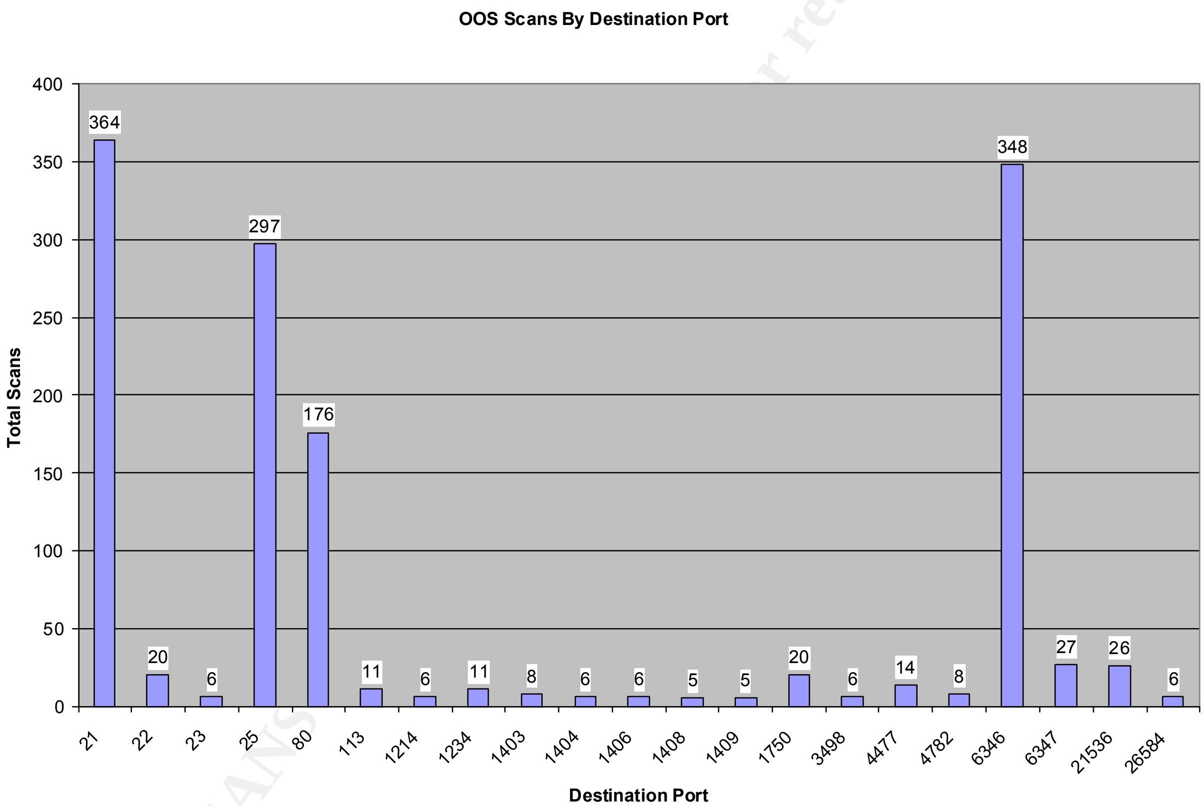
Top 20 Destination Ports

Destination Port	Total Scans	Percentage	Service *
21	364	22.17%	FTP
6346	348	21.19%	Gnutella
25	297	18.09%	SMTP
80	176	10.72%	Web Server
6347	27	1.64%	Gnutella
21536	26	1.58%	See Below
1750	20	1.22%	Simple Socket Library's PortMaster
22	20	1.22%	SSH
4477	14	0.85%	NA
1234	11	0.67%	Infoseek Search Agent / Ultors Trojan Horse
113	11	0.67%	Authentication Service
4782	8	0.49%	NA
1403	8	0.49%	Prospero Resource Manager

26584	6	0.37%	NA
3498	6	0.37%	NA
1406	6	0.37%	NetLabs License Manager
1404	6	0.37%	Infinite Graphics License Manager
1214	6	0.37%	KAZAA
23	6	0.37%	Telnet
1409	5	0.30%	Here License Manager

* These are not the only services that can run on these ports. Most applications can be configured to use any port specified by the user. Some ports do not have any known application using them.

This data was sorted again and graphed to filter down even further the most "hit" upon ports. The top 5 destination ports really stand out now.



Concentrating on the top 5 source IP's of OOS scans revealed some interesting data. Brief summaries follow for each of the top 5 sources.

IP 211.114.44.2

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/06-13:35:45.581983 211.114.44.2:21 -> 10.10.2.111:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x5BA239A0   Ack: 0x121329B5   Win: 0x404
00 00 00 00 00 00                              ......
```

=+
06/06-13:35:55.376025 211.114.44.2:21 -> 10.10.4.90:21
TCP TTL:26 TOS:0x0 ID:39426
SF** Seq: 0x78B47348   Ack: 0x2E203945   Win: 0x404
00 00 00 00 00 00 ......

This could be considered normal FTP activity since "normal" active FTP sessions use a source port 20 and the destination port 21. Your organization might also want to see if there are legitimate users based in Korea all of these probes are originating from there. What makes this unusual is that it is a SYN-FIN scan and directed at different hosts within the internal network. This is definitely not normal FTP traffic. This "attacker" could be trying to mask the attack as an active FTP session, while doing an O/S Fingerprint of the internal systems. Definitely keep an eye out for any traffic originating or going to this IP.

Server used for this query: [whois.apnic.net]

% Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
% (whois5.apnic.net)

inetnum: 211.104.0.0 - 211.119.255.255
netname: KRNIC-KR
descr: KRNIC
descr: Korea Network Information Center
country: KR
admin-c: HM127-AP
tech-c: HM127-AP
remarks: **
remarks: KRNIC is the National Internet Registry
remarks: in Korea under APNIC. If you would like to
remarks: find assignment information in detail
remarks: please refer to the KRNIC Whois DB
remarks: http://whois.nic.or.kr/english/index.html
remarks: **
mnt-by: APNIC-HM
mnt-lower: MNT-KRNIC-AP
changed: hostmaster@apnic.net 20000414
changed: hostmaster@apnic.net 20010606
source: APNIC

person: Host Master
address: Korea Network Information Center
address: Narajongkeum B/D 14F, 1328-3, Seocho-dong, Seocho-ku, Seoul, 137-070, Republic of Korea
country: KR

phone: +82-2-2186-4500
fax-no: +82-2-2186-4496
e-mail: hostmaster@nic.or.kr
nic-hdl: HM127-AP
mnt-by: MNT-KRNIC-AP
changed: hostmaster@nic.or.kr 20010514
source: APNIC

IP 199.183.24.194

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/07-12:51:29.683561 199.183.24.194:43542 -> 10.10.253.42:25
TCP TTL:54 TOS:0x0 ID:11916  DF
21S***** Seq: 0x1E2863A2   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 141643054 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/07-13:13:48.047212 199.183.24.194:50495 -> 10.10.253.42:25
TCP TTL:54 TOS:0x0 ID:51194  DF
21S***** Seq: 0x71539010   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 141776874 0 EOL EOL EOL EOL
```

This could be an attack on your mail servers at first glance. From what it appears as, it looks like legitimate mail connection from a machine within Red Hat's organization. 2 possible scenarios come to mind, either a legitimate user from your organization is at Red Hat and connecting to the mail server or one of Red Hat's machines is using connecting to your mail server. By all indications, the second choice sounds the most logical. The packets may come across as unusual with the reserved bits being set, but most likely corrupted packets. Definitely would continue to keep an eye out though.

Server used for this query: [whois.arin.net]

ICG NetAhead, Inc. (NET-ICG-BLK-BLK4-C) ICG-BLK-BLK4-C
199.183.16.0 - 199.183.143.255
Red Hat Software (NET-REDHAT) REDHAT 199.183.24.0 -
199.183.24.255

IP 129.206.170.20

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/07-11:57:30.326835 129.206.170.20:35883 -> 10.10.202.54:6346
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x5200E68C   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 3555453 0 EOL EOL EOL EOL
```

This first scan snippet is more likely Gnutella traffic because of the destination port 6346 and was evident in numerous internal hosts as dictated by the Snort scan and alert files above.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/07-18:52:36.385582 129.206.170.20:52407 -> 10.10.70.66:0
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x715836C3   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6045604 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/07-18:52:39.361770 129.206.170.20:52407 -> 10.10.70.66:0
TCP TTL:50 TOS:0x0 ID:0  DF
21S***** Seq: 0x715836C3   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 6045904 0 EOL EOL EOL EOL
```

These two OOS scans directed at destination port 0 are unusual. This could be in fact Gnutella traffic with unusual destination ports. It appears that the source IP 129.206.170.20 was for the most part, engaged in Gnutella file sharing. Something your organization definitely would want to keep an eye out for and also examination of all machines that received traffic from this IP.

```
University of Heidelberg (NET-HD-NET)
          Im Neuenheimer Feld 293
          D-69120 Heidelberg,
          DE

          Netname: HD-NET
          Netblock: 129.206.0.0 - 129.206.255.255

          Coordinator:
            Hebgen, Michael  (MH255-ARIN)  michael.hebgen@URZ.UNI-
HEIDELBERG.DE
            +49 6221 54-4501 (FAX) +49 6221 54-5581

          Domain System inverse mapping provided by:

          SUN0.URZ.UNI-HEIDELBERG.DE   129.206.100.126
          SUN1.URZ.UNI-HEIDELBERG.DE   129.206.100.127
          DNS1.BELWUE.DE               129.143.2.1

          Record last updated on 14-Dec-1998.
          Database last updated on 28-Jul-2001 23:02:36 EDT.
```

IP 212.181.52.7

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/06-02:08:16.799374 212.181.52.7:59970 -> 10.10.217.18:1444
```

TCP TTL:46 TOS:0x0 ID:4283 DF
21S***** Seq: 0x43FF968A Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 31491633 0 EOL EOL EOL EOL

=+
06/06-02:09:14.224527 212.181.52.7:59974 -> 10.10.217.18:1445
TCP TTL:46 TOS:0x0 ID:16512 DF
21S***** Seq: 0x4786DC1C Ack: 0x0 Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 31497372 0 EOL EOL EOL EOL

This was indeed strange traffic as IP 212.181.52.7 hit the same internal host 10.10.217.18 100 times. This could be an indication of scanning, but looking over all the OOS scans, the destination ports on 10.10.217.18 that were hit ranged from 1401 through 1446. One theory is an application that runs from this host is trying to establish a legitimate connection and is failing and causing all the retries.

% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 212.181.52.0 - 212.181.52.15
netname: BONET
descr: BoNet Broadband G/GTN
descr: Server-LAN
country: SE
admin-c: MB13908-RIPE
tech-c: MB13908-RIPE
status: ASSIGNED PA
mnt-by: TELIANET-LIR
changed: amar@telia.net 20000114
source: RIPE

route: 212.181.0.0/16
descr: TELIANET-BLK
origin: AS3301
mnt-by: TELIANET-RR
changed: rr@telia.net 19990525
source: RIPE

person: Magnus Benngard
address: BoNet
address: Eklanda Hage 28
address: 431 49 Molndal Sweden
phone: +46-70-527 44 41

e-mail: mb@telia.net
nic-hdl: MB13908-RIPE
changed: amar@telia.net 20000103
source: RIPE

IP 158.75.57.4

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/05-17:16:25.684820 158.75.57.4:42935 -> 10.10.202.158:6346
TCP TTL:53 TOS:0x0 ID:55467  DF
21S***** Seq: 0x80980483   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 37674926 0 EOL EOL EOL EOL

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/07-12:29:13.827423 158.75.57.4:57794 -> 10.10.206.226:6346
TCP TTL:53 TOS:0x0 ID:28940  DF
21S***** Seq: 0xBF604736   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 53229417 0 EOL EOL EOL EOL
```

This as with the above address 129.206.170.20 more then likely is involved in Gnutella traffic. File sharing software has a history with strange packets that are caused by it. From this snippet of OOS scan data; it appears that the source IP 158.75.57.4 was connected to various internal hosts within your organization. As stated above, Gnutella traffic is abundant within your network.

Server used for this query: [whois.arin.net]

POLIP (NET-TORUNPOLIP2)
Computer Centre, Nicolaus Copernicus University
ul. Chopina 12/18, 87-100 Torun, Poland
PL

Netname: TORUNPOLIP2
Netblock: 158.75.0.0 - 158.75.255.255

Coordinator:
Szewczak, Zbigniew S. (ZSS-ARIN) zssz@TORUN.PL
(56) 260-17 ext. 70

Domain System inverse mapping provided by:

ALFA.CS.TORUN.PL 158.75.10.75
BILBO.NASK.ORG.PL 148.81.16.51

Record last updated on 11-Oct-1995.
Database last updated on 28-Jul-2001 23:02:36 EDT.

IP 10.10.100.153

Only one internal host, 10.10.100.153, had any kind of OOS scan alert. 10.10.100.153 connected to a @Home IP on the SSH port 22. Going through all the alert, scan and OOS files revealed only 2 entries involving IP 24.3.20.123 as a source. A SYN alert was detected 10 one hundredths of a second earlier. This possibly could be a employee's home system running SSH, but it might be something your organization would want to look at since having any user connect to a computer outside your network could be a policy violation, since there would be no way to verify if the home system was compromised itself. It can also be a compromised internal machine connecting to the attacker's machine to transfer any data.

06/04-08:38:44.761528 10.10.100.153:32780 -> 24.3.20.123:22

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/04-08:38:44.761528 10.10.100.153:32780 -> 24.3.20.123:22
TCP TTL:63 TOS:0x0 ID:46339  DF
21S***** Seq: 0x29789615   Ack: 0x0   Win: 0x16D0
TCP Options => MSS: 1460 SackOK TS: 74518 0 EOL EOL EOL EOL
```

The internal host, 10.10.100.153 was involved in numerous "SUN-RPC Highport attempts" and port 21 SYN scans right before and after the unusual OOS and scan alert. By all accounts, this host could have been compromised by all the alerted traffic and should be examined further.

Jun 2 09:52:33 217.136.37.76:3342 -> 10.10.100.153:21 SYN **S*****

Jun 2 09:52:40 217.136.37.76:3342 -> 10.10.100.153:21 SYN **S*****

06/04-08:56:38.710959 [**] SUNRPC highport access! [**] 35.9.37.225:21 -> 10.10.100.153:32771

06/04-08:56:38.711068 [**] SUNRPC highport access! [**] 35.9.37.225:21 -> 10.10.100.153:32771

Server used for this query: [whois.arin.net]

```
    @Home Network (NETBLK-ATHOME)   ATHOME              24.0.0.0 - 24.23.255.255
     @Home Network (NETBLK-MD-COMCAST-HWRD-1) MD-COMCAST-HWRD-1
                                                        24.3.16.0 - 24.3.23.255
```

Other Miscellaneous OOS Scans

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/03-12:59:39.200777 62.180.198.148:18245 -> 10.10.179.77:21536
TCP TTL:113 TOS:0x0 ID:38423  DF
2*SFRP*U Seq: 0x2F696D61   Ack: 0x6765732F   Win: 0x7374
68 74 6D 6C 20 48                       html H
```

This unusal traffic has been reported from other security professionals. It seems that source port 18245 directed at port 21536 could be a malfunctioning piece of hardware. This is something that should be watched and fixed, if possible.
http://archives.linuxbe.org/arch055/0229.html
http://archives.neohapsis.com/archives/incidents/2001-01/0079.html

Recommendations

The following is recommendations based on the data gathered from the 5 days worth of Snort alert, scan and OOS files.

- Closely examine the internal hosts that are involved in any kind of scanning for examination. Make sure that there are no Trojans or backdoors are installed on these machines or other malicious type scanning software that shouldn't be. If warranted, a complete rebuild of these machines may be in the best order. A copy of the infected machine should be made for forensic information. There are commercial products available for that. You may also want to keep a close watch on employees who have access to these machines since a machine could have been compromised within the organization.
- There is not much you can do with external hosts scanning the internal network except to block it on a case-by-case basis. You wouldn't want to block an IP without investigation because someone could spoof say a client of yours and if you blocked that IP, you would be denying your client from accessing say some of your services. Rules set on your routers and firewalls can achieve this.
- Changing of the Snort rules to filter out traffic from Yahoo broadcasting IP range to reduce Snort alerts. This could have a backfire if malicious attack does occur. This depends on how much hardware considerations since alerts over time will create large amounts of data.
- Changing the firewall rules to allow only FTP traffic to the FTP servers, not open to all internal hosts as it is now or if no firewall exists, install one such as a Cisco PIX or Checkpoint Firewall-1. The same setting of rules applies for web server traffic, port 80 and mail traffic, port 25. The reason you don't want traffic designated for port 80 to be directed to one of your desktops that happens to have be running a web server. This would leave that machine susceptible to attacks. Also be sure and block all other ports and only open new ports on a case-by-case basis with evaluations done on the impact of doing so. Some main culprits are ports 135-139 for Window machines. This would prevent NetBIOS traffic from the Internet to your internal network.
- Be sure and stop all unnecessary services running on all internal machines that don't need to. Stopping NETBIOS services on Windows clients and servers is good example.
- Make sure all machines are hardened according to a good security guideline such as SANS. For Linux machines, there is a script to help harden down some Linux distributions (http://www.bastille-linux.org/).
- Depending on your organization's policies, uninstall all file sharing software such as Napster and Gnutella, instant messaging software such as AOL and MSN Messenger, and all IRC software.
- Consider restricting Internet access with a proxy or socks server.

- Apply all the latest patches to all the OS's and software used within the organization. Be sure and do some testing on a non-production machine especially before implementing on critical servers.
- Use of anti virus software, if not already used, with the latest definitions.
- Make sure firewall and router logs are logging for further evaluation of Snort alerts. This will help it determining more the damage done if any.
- Keep up to date on your router and firewall patches and bugs. There are exploits and bugs out there for practically everything.
- The creation on a Computer Incident Response Team (CIRT) with policies and procedures will help when serious events occur. Members of this team and management should join mailing list groups such as Buqtraq, SANS Intrusions to keep up with the latest findings. The CIRT team should also meet regularly to discuss current security events.
- Backup of all Snort data for any reference that may be used later in correlations with newer alerts.
- Training of all IT personnel including the CIRT team in security practices such as SANS courses.

A good baseline reference for minimal perimeter protection is contained on the SANS Top 10 Security threats page under Appendix A. (http://www.sans.org/topten.htm)

Analysis Process

Snort alert, scan and OOS files were given between the dates 6/2/01 thru 6/7/01. Analysis was done by first using the "sed" command to change all references of MY.NET.x.x to 10.10.x.x. Then the "cat" command was used to merge all the alert files into 1 file and then same for the scan and OOS files. SnortSnarf was used on the scan and alert combined files. Perl scripts were used from Michael Bell's practical and Paul Asadoorian's practical to gain additional data after SnortSnarf was ran. The alert SnortSnarf html files were then imported into Microsoft Excel for the graphs. The OOS combined file was parsed with a perl script, converted to a CSV file and then imported into Excel. The data was then sorted by source IP and number of scans and a graph was created. Excel was used a great deal for sorting of data by IP and number of scans.

Some simple Unix command line commands were used to further analyze the data.

Replaced all spaces with a comma
cat oos |sed 's/ /,/g' >> dest_oos

Replaced all TAB's with a comma
cat dest_oos | tr –s '\t' ',' > oos_dest.csv

Examined the OOS data sorted by destination IP and created a top 10 list from that. Looking at the top 10, parsed the data for each of the top 10 hosts, one by one with the following command.

grep – '10.10.202.54' >> 10.10.202.54.txt

Noticed that there was primarily one destination port 6346, so I then ran through OOS data again with the following command:

grep – '6346' 10.10.202.54.txt | wc –l

This was repeated for all subsequent ports. Unknown ports were searched on numerous security sites and search engines such as Google.com. Other practicals were referenced for any correlations on this as well.

References

Here is the list of references used throughout this paper.

http://www.sans.org/y2k/practical/Paul_Asadoorian_GIAC.doc
http://www.sans.org/y2k/practical/Mike_Bell_GIAC.doc
http://www.sans.org/y2k/practical/Miika_Turkia_GCIA.html
http://www.sans.org/y2k/practical/PJ_Goodwin_GIAC.doc
http://www.os2site.com/sw/internet/info/portlist.txt
http://www.sans.org/y2k/gaming.htm
http://www.sans.org/
http://www.cert.org/
http://www.securityfocus.com/
http://cve.mitre.org/
http://www.snort.org/
http://www.google.com/
http://broadband.earthlink.net/home-networking/networking/NAT_list.html
http://www.geektools.com/cgi-bin/proxy.cgi

Comer, Douglas. Internetworking with TCP/IP - Volume I Principles, Protocols, and Architecture 3rd Edition. New Jersey: Prentice Hall, 1995

Northcutt, Stephen and Cooper, Mark and Fearnow, Matt and Frederick, Karen. Intrusion Signatures and Analysis. Indianapolis: New Riders, 2001

Northcutt, Stephen and Novak, Judy. Network Intrusion Detection An Analysts Handbook, Second Edition.
Indianapolis: New Riders, 2000

Proctor, Paul, The Practical Intrusion Detection Handbook. New Jersey: Prentice Hall PTR, 2001

Elson, David."Intrusion Detection, Theory and Practice." May 2000
URL:http://www.securityfocus.com/focus/ids/articles/davidelson.html

Lemos, Robert. "Microsoft reveals Web server hole." June 2001
URL:http://news.cnet.com/news/0-1003-200-6312870.html

"IDS Introduction" URL:http://www.nss.co.uk/ids/introduction.htm

Seifried, Kurt "Network Intrustion Detection Systems and Virus Scanners - Are They The Answer?" January 2000
URL:http://www.securityportal.com/closet/closet20000105.html

Power, Richard and Farrow, Rik. "Five vendors answer some no-nonsense questions on IDS." July 1998. URL:http://www.gocsi.com/ques.htm