GIAC Intrusion Detection Curriculum Practical Assignment
SANS Security DC 2000

John S Best Jr.

Table of Contents

Assignment 1 - Network Detects

Detect 1 - Detect 2 - Detect 3 - Detect 4 - Detect 5

Assignment 1 - Detect 1

```
[**] SCAN-SYN FIN [**]
08/05-12:08:24.453654 194.186.233.10:27374 -> x.y.z.168:27374
TCP TTL:13 TOS:0x0 ID:39426
**S*F*** Seq: 0x7B5E3230   Ack: 0x4F807AA5   Win: 0x404

[**] SCAN-SYN FIN [**]
07/28-21:20:29.990498 130.83.134.42:109 -> x.y.z.168:109
TCP TTL:15 TOS:0x0 ID:39426
**S*F*** Seq: 0x30278CDC   Ack: 0x58E4BB3A   Win: 0x404

[**] SCAN-SYN FIN [**]
08/03-18:34:44.515671 203.197.140.68:111 -> x.y.z.168:111
TCP TTL:29 TOS:0x0 ID:39426
**S*F*** Seq: 0xC98095A   Ack: 0x1C5030AD   Win: 0x404

[**] SCAN-SYN FIN [**]
08/05-12:53:30.308868 203.197.140.68:111 -> x.y.z.168:111
TCP TTL:29 TOS:0x0 ID:39426
**S*F*** Seq: 0x1A7523FA   Ack: 0x1E260C6B   Win: 0x404
```

Detect 1

1. Source of trace
2. Detect was generated by
3. Probability the source address was spoofed
4. Description of attack
5. Attack mechanism
6. Correlations
7. Evidence of active targeting
8. Severity

1. Detect 1 - Source of trace

These Traces were collected on my home network which is connected by cable modem.

2. Detect 1 - Detect was generated by

Snort intrusion detection system.

3. Detect 1 - Probability the source address was spoofed

Doubtful that these address are spoofed as it appears that the attacker is trying to gain access to commonly exploited ports. I believe that these traces are part of a portscanning tool.

4. Detect 1 - Description of attack

Attack against a block of network addresses to seek out commonly exploited ports. In the trace above we see portmapper(111), POP2(109), and Subseven(27374). The SYN / FIN flags are an attempt to evade intrusion detection systems.

5. Detect 1 - Attack mechanism

This attack appears to be part of a mapping tool that will seek out systems with exploitable ports open.Once the attacker has identified systems with these vulnerabilities he/she would most likely use a script or pre-written tool to compromise the box based on the vulnerable ports.

6. Detect 1 - Correlations

I have been collecting these traces for some time and after reviewing the information noticed that the source port and destination port are always the same and the IP ID is always 39426
GIAC for 08/07/2000 also has a direct correlation from Stephen P. Berry.

7. Detect 1 - Evidence of active targeting

I believe that this was a general scan of the cable modem IP space.

8. Detect 1 - Severity

(5 + 1) - (5 + 4) = -3
(Criticality + lethality) - (System + Net Countermeasures) = Severity

9. Detect 1 - Defensive recommendation

Defenses are in place for this and the operating system has been hardened against these kind of attacks.

10. Detect 1 - Multiple choice test question

What characteristic of the trace above would lead you to believe that these are crafted packets created by the same tool?

a. The Source port and Destination port are all the same.
b. The IP ID is always set to 39426.
c. Window size is always `Win: 0x404`.
d. All of the above.

answer is d

Back to the Assignment 1 menu ^

Assignment 1 - Detect 2

```
[**] MISC-WinGate-1080-Attempt [**]
08/02-20:36:37.200505 24.1.247.148:3273 -> x.y.z.168:1080
TCP TTL:48 TOS:0x0 ID:5846  DF
**S***** Seq: 0xDA071C5C   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 228522422 0 NOP WS: 0
```

Detect 2

Detect 2 - Source of trace

This trace was collected from my home network which is attached to a cable modem.

Detect 2 - Detect was generated by

Snort intrusion detection system.

Detect 2 - Probability the source address was spoofed

This is a detect from an apparent WinGate scanning tool. The attacker would want to receive a response in order validate the WinGate port was open.

Detect 2 - Description of attack

CVE-1999-0291
Attacker was probing for WinGate ports.
The attacker was hoping for a WinGate proxy installed without a password, which allows remote attackers to redirect connections without authentication.

Detect 2 - Attack mechanism

Had the attacker found this port open, it is highly likely that he/she would have used the target computer as launching point for other probes or Denial of Service attacks.

Detect 2 - Correlations

This is a well known attack. The holes in the WinGate program are well documented. Since so many are implemented it is not surprising to see a probe of the cable modem space for this exploit.

Detect 2 - Evidence of active targeting

I believe that this was a general scan of the cable modem space.

Detect 2 - Severity

(5 + 1) - (5 + 4) = -3

(Criticality + lethality) - (System + Net Countermeasures) = Severity

Detect 2 - Defensive recommendation

Defenses are fine since WinGate is not running on this PC and the intrusion detection caught the trace.

Detect 2 - Multiple choice test question

This packet was mostly likely ...

a. Part of a large scan of a network.
b. A direct attack at this particular host.
c. A buffer overflow attack directed at a proxy server.
d. A FTPD bounce attack.

answer is a

Back to the Assignment 1 menu ^

Assignment 1 - Detect 3

```
FWIN,2000/06/07,07:19:54 -5:00
GMT,62.108.20.25:4056,24.28.9.107:27374,TCP
```

Detect 3

1. Source of trace
2. Detect was generated by
3. Probability the source address was spoofed
4. Description of attack
5. Attack mechanism
6. Correlations
7. Evidence of active targeting
8. Severity
9. Defensive Recommendation
10. Multiple choice test question

Detect 3 - Source of trace

This trace was collected from my home network which is attached to a cable modem.

Detect 3 - Detect was generated by

Zone alarm personal firewall software by Zone Labs.
Log Format: FWIN means this was a Inbound packet.
`2000/06/07, 07:19:54 - 5:00 GMT` : Date and Time stamp.
`62.108.20.25:4056 --->` Source Address and port.
`x.y.x.107:27374 ------->` Destination Address.
`, TCP ---->` Transport protocol.

Detect 3 - Probability the source address was spoofed

Low. The attacker was depending on a response. This was probably a scan of the cable modem space in attempt to find Subseven machines.

Detect 3 - Description of attack

Attacker was probing for well known trojan SubSeven

Detect 3 - Attack mechanism

This attacker was likely looking for an Ack response from the host on this port indicating that it was infected with the SubSeven trojan.

Detect 3 - Correlations

This particular attack is well known. In Detect 1, there is similar attack as part of a scan.

Detect 3 - Evidence of active targeting

This was a general scan of cable modem space for the SubSeven trojan.

Detect 3 - Severity

(5 + 1) - (5 + 5) = -4
(Criticality + lethality) - (System + Net Countermeasures) = Severity

Detect 3 - Defensive recommendation

Defenses are fine. The attack was blocked and logged by the Zone Labs software.

Detect 3 - Multiple choice test question

Which well known trojan does port 27374 represent?

a. Back Orifice.
b. Subseven.
c. Barak.
d. Trin00.

answer is b

Back to the Assignment 1 menu ^

Assignment 1 - Detect 4

```
FWIN,2000/06/07,16:02:58 -5:00 GMT,141.24.191.63:1024,x.y.z.168:34555,UDP
FWIN,2000/06/07,16:03:08 -5:00 GMT,141.24.191.63:1024,x.y.z.168:27444,UDP
FWIN,2000/06/07,16:03:16 -5:00 GMT,141.24.191.63:53,x.y.z.168:32768,UDP
FWIN,2000/06/07,16:04:16 -5:00 GMT,141.24.191.63:0,x.y.z.168:0,ICMP

FWIN,2000/06/07,16:04:26 -5:00 GMT,141.24.191.63:17415,x.y.z.168:0,TCP
FWIN,2000/06/07,16:04:26 -5:00 GMT,141.24.191.63:17416,x.y.z.168:0,TCP
FWIN,2000/06/07,16:04:28 -5:00 GMT,141.24.191.63:17417,x.y.z.168:0,TCP
FWIN,2000/06/07,16:04:28 -5:00 GMT,141.24.191.63:17418,x.y.z.168:0,TCP

FWIN,2000/06/07,16:04:28 -5:00 GMT,141.24.191.63:17419,x.y.z.168:0,TCP
FWIN,2000/06/07,16:04:28 -5:00 GMT,141.24.191.63:17420,x.y.z.168:0,TCP
FWIN,2000/06/07,16:04:28 -5:00 GMT,141.24.191.63:17421,x.y.z.168:0,TCP
FWIN,2000/06/07,16:04:30 -5:00 GMT,141.24.191.63:10003,x.y.z.168:21,TCP

FWIN,2000/06/07,16:04:40 -5:00 GMT,141.24.191.63:1515,x.y.z.168:0,TCP
FWIN,2000/06/07,16:05:00 -5:00 GMT,141.24.191.63:0,x.y.z.168:0,ICMP
FWIN,2000/06/07,16:05:10 -5:00 GMT,141.24.191.63:1035,x.y.z.168:161,UDP
```

```
FWIN,2000/06/07,16:05:26 -5:00 GMT,141.24.191.63:1036,x.y.z.168:162,UDP


FWIN,2000/06/07,16:05:40 -5:00 GMT,141.24.191.63:1036,x.y.z.168:161,UDP
FWIN,2000/06/07,16:08:20 -5:00 GMT,141.24.191.63:1024,x.y.z.168:18753,UDP
FWIN,2000/06/07,16:08:30 -5:00 GMT,141.24.191.63:139,x.y.z.168:139,TCP
FWIN,2000/06/07,16:09:40 -5:00 GMT,141.24.191.63:923,x.y.z.168:111,UDP


FWIN,2000/06/07,16:10:40 -5:00 GMT,141.24.191.63:924,x.y.z.168:111,UDP
FWIN,2000/06/07,16:11:40 -5:00 GMT,141.24.191.63:1036,x.y.z.168:137,UDP
FWIN,2000/06/07,16:11:54 -5:00 GMT,141.24.191.63:137,x.y.z.168:137,TCP
FWIN,2000/06/07,16:13:04 -5:00 GMT,141.24.191.63:1036,x.y.z.168:17,UDP


FWIN,2000/06/07,16:13:20 -5:00 GMT,141.24.191.63:1036,x.y.z.168:10167,UDP
FWIN,2000/06/07,16:13:34 -5:00 GMT,141.24.191.63:500,x.y.z.168:500,UDP
FWIN,2000/06/07,16:13:44 -5:00 GMT,141.24.191.63:1036,x.y.z.168:518,UDP
FWIN,2000/06/07,16:14:00 -5:00 GMT,141.24.191.63:1516,x.y.z.168:15104,TCP


FWIN,2000/06/07,16:14:20 -5:00 GMT,141.24.191.63:65535,x.y.z.168:10498,UDP
FWIN,2000/06/07,16:14:30 -5:00 GMT,141.24.191.63:65535,x.y.z.168:7983,UDP
FWIN,2000/06/07,16:14:40 -5:00 GMT,141.24.191.63:0,x.y.z.168:0,ICMP
FWIN,2000/06/07,16:14:50 -5:00 GMT,141.24.191.63:0,x.y.z.168:0,ICMP


FWIN,2000/06/07,16:15:00 -5:00 GMT,141.24.191.63:1036,x.y.z.168:7,UDP
FWIN,2000/06/07,16:15:14 -5:00 GMT,141.24.191.63:1036,x.y.z.168:2140,UDP
FWIN,2000/06/07,16:15:28 -5:00 GMT,141.24.191.63:1036,x.y.z.168:13,UDP
FWIN,2000/06/07,16:15:44 -5:00 GMT,141.24.191.63:1036,x.y.z.168:19,UDP


FWIN,2000/06/07,16:15:58 -5:00 GMT,141.24.191.63:1036,x.y.z.168:53,UDP
FWIN,2000/06/07,16:16:14 -5:00 GMT,141.24.191.63:1036,x.y.z.168:31337,UDP
FWIN,2000/06/07,16:16:28 -5:00 GMT,141.24.191.63:1036,x.y.z.168:22,UDP
FWIN,2000/06/07,16:16:58 -5:00 GMT,141.24.191.63:1517,x.y.z.168:15858,TCP


FWIN,2000/06/07,16:17:18 -5:00 GMT,141.24.191.63:1518,x.y.z.168:17300,TCP
FWIN,2000/06/07,16:17:38 -5:00 GMT,141.24.191.63:1519,x.y.z.168:20034,TCP
FWIN,2000/06/07,16:17:58 -5:00 GMT,141.24.191.63:1520,x.y.z.168:21554,TCP
FWIN,2000/06/07,16:18:18 -5:00 GMT,141.24.191.63:1521,x.y.z.168:30100,TCP
FWIN,2000/06/07,16:18:38 -5:00 GMT,141.24.191.63:1036,x.y.z.168:69,UDP
```

Detect 4

Detect 4 - Source of trace

This trace was collected from my home network which is attached to a cable modem

Detect 4 - Detect was generated by

Zone alarm personal firewall software by Zone Labs.
Log Format: FWIN means this was a Inbound packet.
`2000/06/07, 16:18:38 - 5:00 GMT` : Date and Time stamp.
`141.24.191.63:1036 --->` Source Address and port.
`x.y.z.168:69 ------->` Destination Address.
`, UDP ---->` Transport protocol.

Detect 4 - Probability the source address was spoofed

Low. This is a slow portscan for possible attempts on vulnerabilities.
Attacker would want the resulting packets for the analysis.

Detect 4 - Description of attack

It could be a NMap fingerprinting scan or scanning tool like Nesuss (which also uses NMap). It's hard to tell without the Flags.
CAN-1999-0454

Detect 4 - Attack mechanism

This tool uses odd packet signatures and can be setup to use Decoy addresses. An attacker targets a system or network and sets up a scan using various options within the software to achieve different purposes.

Detect 4 - Correlations

This is a well known tool to find vulnerabilities and identify operating systems on hosts, mapping networks using stealth techniques.

Detect 4 - Evidence of active targeting

High. This attack went on for almost 15 minutes based on the spacing of the packets. It is doubtful that other hosts were being scanned simultaneously. The IP address is from Denmark which may account for the slowness of the scan.

Detect 4 - Severity

(5 + 1) - (5 + 5) = -4
(Criticality + lethality) - (System + Net Countermeasures) = Severity

Detect 4 - Defensive recommendation

Defenses are fine. The attack was blocked and logged by the Zone Labs software.

Detect 4 - Multiple choice test question

Traffic above is evidence of a ...

a. General scan of a network.
b. A portscan of a specific host.
c. A fragmented buffer overflow attack.
d. A LOKI covert Traffic Tunnel.

answer is b

Back to the Assignment 1 menu ^

Assignment 1 - Detect 5

```
[**] PING-ICMP Destination Unreachable [**]
08/08-18:15:00.549370 x.y.z.168 -> 192.168.100.18
ICMP TTL:64 TOS:0xC0 ID:41012
DESTINATION UNREACHABLE: PORT UNREACHABLE


[**] PING-ICMP Destination Unreachable [**]
08/08-18:15:01.940415 x.y.z.168 -> 192.168.100.18
ICMP TTL:64 TOS:0xC0 ID:41173
DESTINATION UNREACHABLE: PORT UNREACHABLE


[**] PING-ICMP Destination Unreachable [**]
08/08-18:15:02.279938 x.y.z.168 -> 192.168.100.18
ICMP TTL:64 TOS:0xC0 ID:41203
DESTINATION UNREACHABLE: PORT UNREACHABLE


[**] PING-ICMP Destination Unreachable [**]
08/08-18:15:02.280601 x.y.z.168 -> 192.168.100.18
ICMP TTL:64 TOS:0xC0 ID:41204
DESTINATION UNREACHABLE: PORT UNREACHABLE
```

ETC ETC ETC . . . . .

```
[**] PING-ICMP Destination Unreachable [**]
08/08-18:15:04.100748 x.y.z.168 -> 192.168.100.18
ICMP TTL:64 TOS:0xC0 ID:41401
DESTINATION UNREACHABLE: PORT UNREACHABLE
```

Detect 5

Detect 5 - Source of trace

This trace was collected from my home network which is attached to a cable modem. It should be noted that for the sake of clarity, I have removed 70 packets from this scan in order to fit this format.

Detect 5 - Detect was generated by

Snort intrusion detection system.

Detect 5 - Probability the source address was spoofed

High. This appears to be a response to a portscan with a spoofed address or interleaved with a spoofed address (192.168.100.18 is a RFC 1918 reserved address space).

Detect 5 - Description of attack

It would appear that a port probing tool of some sort was directed at my outside interface.

The ICMP port unreachable responses were the result of probe of a UDP port that wasn't listening. I also believe that there were TCP packets intermingled in this. Snort didn't catch the actual scan but did log the ICMP port unreachable messages from my host back to the unreachable address.

Detect 5 - Attack mechanism

There is not a lot information to work with here. Apparently the scanning tool that generated these messages is able to evade the snort rules.

Detect 5 - Correlations

I don't have enough information to correlate this attack. NMAP is capable of hiding it's source IP address by interleaving it with decoys. It is possible that this tool was directed at my interface. With so many packets being sent it is also possible that this was attempted DOS.

Detect 5 - Evidence of active targeting

Medium. This scan was directed at my address for a period of 4 seconds and managed to generate over 100 ICMP port unreachable messages. Snort didn't catch the rest of the packets. It is impossible to rule out a high speed scan of the cable modem space as 4 to 10 seconds per host is not unreasonable. This was a very fast tool.

Detect 5 - Severity

(5 + 1) - (5 + 5) = -4
(Criticality + lethality) - (System + Net Countermeasures) = Severity

Detect 5 - Defensive recommendation

Update Snort rules to collect any packets from RFC 1918 address. Put these rules first in the file.

Detect 5 - Multiple choice test question

In the trace above, what would lead you to believe that this is a response to a spoofed packet?

a. The TOS is set 0xC0.
b. ICMP port unreachable messages are only generated in response to spoofed addresses.
c. The destination address is in a RFC 1918 reserved address.
d. The time stamp.

answer is c

Back to the Practical menu ^

Assignment 2 - Evaluate an Attack

Assignment 2 - Give the URL, location, or command that you acquired the attack from.

I have chosen to evaluate a reconnaissance attack. I initially found out about this tool on security focus. I

downloaded the actual file from the Korean web site listed below.

TWWWSCAN
TWWWscan 0.45
by twenty sad soul,
search@iland.co.kr
http://search.iland.co.kr/twww/
Platforms: Windows 2000, Windows 95/98 and Windows NT

Includes Windows NT 4, Windows 2000 Patch Information, (~30/05/2000) 186 bugs checked, changed scan interface. Bug fixed, add Internet Information.

Back to the Assignment 2 menu ^

Assignment 2 - Describe the attack, including how it works.

Command line CGI vulnerability scanner. When executed it will run through a predefined set of scripts that determine the kind of web server software running on the target and any vulnerabilities it finds.

Once the tool reports back the weaknesses of the web server, it is up to the user to either use the exploits that are found or the administrator to patch the holes that were found.

Here is a list of exploits that the software checks for:

```
Exploit: ExAir Sample DoS
Exploit: iCat Carbo Server(carbo.dll)
Exploit: Websites (uploader.exe)
Exploit: search97.vts
Exploit: Remote File create,IIS DoS(newdsn.exe)
Exploit: IIS 3.0 Remote File create(getdrvs.exe)


Exploit: Frontpage98  Hole(_vti_inf.html)
Exploit: Frontpage98  Hole(service.pwd)
Exploit: Frontpage98  Hole(users.pwd)
Exploit: Frontpage98  Hole(authors.pwd)
Exploit: Frontpage98 Hole(administrators.pwd)
Exploit: Frontpage98 Hole(shtml.dll)
Exploit: Frontpage98 Hole(shtml.exe)
Exploit: Frontpage98 Helo(queryhit.htm)


Exploit: Pws,Jana WebServer(dotdotdot)
Exploit: Personal WebServer Hole B


Exploit: IIS Web Password Hole(achg.htr)
Exploit: IIS Web Password Hole(aexp.htr)
Exploit: IIS Web Password Hole(aexp2.htr)
Exploit: IIS Web Password Hole(aexp2b.htr)
Exploit: IIS Web Password Hole(aexp3.htr)
Exploit: IIS Web Password Hole(aexp4.htr)
Exploit: IIS Web Password Hole(aexp4b.htr)
Exploit: IIS Web Password Hole(a.htr)
Exploit: IIS Web Password Hole(a3.htr)


Exploit: Omi HTTPD (visadmin.exe)
Exploit: IIS Perl Security Hole
Exploit: IIS (fpcount.exe) DoS
```

```
Exploit: WebCom Guestbook Hole(rquest.exe)
Exploit: WebCom Guestbook Hole(wguest.exe)


Exploit: IIS Data Stream Hole
Exploit: IIS (codebrws.asp) Hole A
Exploit: IIS (codebrws.asp) Hole B
Exploit: IIS (showcode.asp) Hole


Exploit: SiteServer AdSamples(site.csc)
Exploit: Peer Webservice Hole(ism.dll)
Exploit: ASP Sample ODBC Hole(catalog_type.asp)


Exploit: ColdFusion  Hole(openfile.cfm)
Exploit: ColdFusion  Hole(explcalc.cfm)
Exploit: ColdFusion  Hole(displayopenedfile.cfm)
Exploit: ColdFusion  Hole(sendmail.cfm)
Exploit: ColdFusion  Hole(GetFile.cfm)


Exploit: Alibaba Multiple CGI(get32.exe)
Exploit: Alibaba Multiple CGI(alibara.pl)
Exploit: Alibaba Multiple CGI(tst.bat)


Exploit: IIS Double Byte Hole
Exploit: TeamShare TeamTrack V3.0 Hole
Exploit: OmniHTTPd 1.01,Pro2.04 bof(imagemap.exe)
Exploit: W4-Server2.6a(cgitest.exe)
Exploit: URL Live! 1.0 WebServer Hole
Exploit: WebBBS Hole(webbbs.exe)


Exploit: AN-HTTPd 1.20b Hole(test.bat)
Exploit: AN-HTTPd 1.20b Hole(input.bat)
Exploit: AN-HTTPd 1.20b Hole(input2.bat)
Exploit: AN-HTTPd 1.20b Hole(envout.bat)


Exploit: RDS Securty Hole(msadcs.dll)
Exploit: Frontpage path,bof(htimage.exe)


Exploit: IIS Path Reveal(anything.idc)
Exploit: IIS Path Reveal(anything.idq)
Exploit: IIS Path Reveal(anything.ida)
Exploit: IIS Path Reveal(anything.idw)


Exploit: counter.exe DoS
Exploit: IIS ASP VBScript Error
Exploit: Sambar Server Batch CGI(echo.bat)
Exploit: Sambar Server Batch CGI(hello.bat)
Exploit: Right Fax Web Client (fuwww.dll)


Exploit: CGI Mailer Hole(cgimail.exe)
Exploit: IIS UNC Mapping Hole
Exploit: Trend OfficeScan Hole(jdkRqify.exe)
Exploit: Oracle Web Listener Batch Hole(*.bat)
Exploit: WinMail Hole (winmail.exe)
```

```
Exploit: Malformed Hit-Highlighting Argument
Exploit: Index Server Security Hole(null.htw)
Exploit: MS frontpage98 backdoor,bof(dvwssr.dll)
Exploit: Web Archive version 1.8d bof(wa.exe)


Exploit: Cart32 Backdoor(cart32.exe)
Exploit: Cart32 Backdoor(c32web.exe)
Exploit: DNews News Server bof(gupcgi.exe)
Exploit: DNews News Server bof(dnewsweb.exe)
Exploit: DMailweb bof(dmailweb.exe)


Exploit: Bugzilla 2.8(process_bug.cgi)
Exploit: Bugzilla 2.8(enter_bug.cgi)
Exploit: Rockliffe MailSite bof(wconsole.dll)
Exploit: Pacific Soft Carello(add.exe)


Exploit: PDGsoft Shopping Cart(redirect.exe)
Exploit: PDGsoft Shopping Cart(changepw.exe)
Exploit: Ceilidh 2.60a (ceilidh.exe)
Exploit: Multi JSP Source (JSP)
Exploit: BEA system WebLogic Server(index.jsp)


Exploit: Allaire JRun 2.3.x (SessionServlet)
Exploit: FrontPage 2k <=1.1 Path vul
Exploit: FrontPage 2k <=1.1 DoS (shtml.dll)
Exploit: Cold Fusion 4.5.1 DoS (index.cfm)
Exploit: BB4 Big Brother (bb-hostsvc.sh)


Exploit: Deerfield WorldClient 2.1 Directory vul
Exploit: IIS 4.0/5.0 Source Vul(+.htr)
Exploit: Blackboard 4.0 (user_update_passwd.pl)
Exploit: Blackboard 4.0 (user_update_admin.pl)


Exploit: Alibab Web Piped Vul (post32.exe)
Exploit: Alibab Web Piped Vul (lsindex2.bat)
```

Back to the Assignment 2 menu ^

Assignment 2 - Provide an annotated network trace of the attack in action.

I executed this trace from my firewall PC (a windows 98 box). Snort running on a Windows 98 machine was used with the following rule set to capture the output.

```
alert tcp My.Firewall.PC/32 any -> My.Web.Server/32 any (msg:"Twwwscan Filter";)
alert tcp My.Web.Server/32 any -> My.Firewall.PC/32 any (msg:"Twwwscan Filter";)
alert UDP My.Firewall.PC/32 any -> My.Web.Server/32 any (msg:"Twwwscan Filter";)
alert UDP My.Web.Server/32 any -> My.Firewall.PC/32 any (msg:"Twwwscan Filter";)
alert icmp My.Firewall.PC/32 any -> My.Web.Server/32 any (msg:"Twwwscan Filter";)
alert icmp My.Web.Server/32 any -> My.Firewall.PC/32 any (msg:"Twwwscan Filter";)
```

I also disconnected the Internet and ran Windump before I executed this software to make sure the tool was not also delivering it's results to any other device. The Windump trace showed no signs of any traffic other than My.FireWall.PC and the My.Web.Server.

I have truncated this trace as it is extremely long and repetitive. Interesting observations include the fact that it opens and closes connections gracefully as it probes the target.

Back to the Assignment 2 menu ^

Back to the Practical menu ^

Checking for Remote File create,IIS DoS(newdsn.exe) vulnerability.

```
[**] Twwwscan Filter [**]
08/09-04:24:49.887782 My.Firewall.PC:61900 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:14818  DF
**S***** Seq: 0xE63F27C   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK


[**] Twwwscan Filter [**]
08/09-04:24:49.966633 My.Web.Server:80 -> My.Firewall.PC:61900
TCP TTL:109 TOS:0x0 ID:36963  DF
**S***A* Seq: 0x189255   Ack: 0xE63F27D   Win: 0x2238
TCP Options => MSS: 1460


[**] Twwwscan Filter [**]
08/09-04:24:49.968877 My.Firewall.PC:61900 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:15074  DF
******A* Seq: 0xE63F27D   Ack: 0x189256   Win: 0x2238


[**] Twwwscan Filter [**]
08/09-04:24:49.975468 My.Firewall.PC:61900 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:15330  DF
*****PA* Seq: 0xE63F27D   Ack: 0x189256   Win: 0x2238
48 45 41 44 20 2F 73 63 72 69 70 74 73 2F 74 6F  HEAD /scripts/to
6F 6C 73 2F 6E 65 77 64 73 6E 2E 65 78 65 20 48  ols/newdsn.exe H
54 54 50 2F 31 2E 30 0A 0A                       TTP/1.0..
```

Here is where they check for the file . . .

```
[**] Twwwscan Filter [**]
08/09-04:24:50.063410 My.Web.Server:80 -> My.Firewall.PC:61900
TCP TTL:109 TOS:0x0 ID:37219  DF
*****PA* Seq: 0x189256   Ack: 0xE63F2A6   Win: 0x220F
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4F 62 6A  HTTP/1.1 404 Obj
65 63 74 20 4E 6F 74 20 46 6F 75 6E 64 0D 0A 53  ect  Found..S
65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F 66 74  erver: Microsoft
2D 49 49 53 2F 34 2E 30 0D 0A 44 61 74 65 3A 20  -IIS/4.0..Date:
57 65 64 2C 20 30 39 20 41 75 67 20 32 30 30 30  Wed, 09 Aug 2000
20 30 37 3A 31 38 3A 34 30 20 47 4D 54 0D 0A 43  07:18:40 GMT..C
6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
36 31 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65  61..Content-Type
3A 20 74 65 78 74 2F 68 74 6D 6C 0D 0A 0D 0A     : text/html....
```

The web Server responds and let's them know that this particular attack will work.

```
[**] Twwwscan Filter [**]
08/09-04:24:50.063456 My.Web.Server:80 -> My.Firewall.PC:61900
TCP TTL:109 TOS:0x0 ID:37475  DF
****F*A* Seq: 0x1892E5   Ack: 0xE63F2A6   Win: 0x220F
```

```
[**] Twwwscan Filter [**]
08/09-04:24:50.066602 My.Firewall.PC:61900 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:15586  DF
******A* Seq: 0xE63F2A6   Ack: 0x1892E6   Win: 0x21A9


[**] Twwwscan Filter [**]
08/09-04:24:50.075630 My.Firewall.PC:61900 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:15842  DF
****F*A* Seq: 0xE63F2A6   Ack: 0x1892E6   Win: 0x21A9


[**] Twwwscan Filter [**]
08/09-04:24:50.155015 My.Web.Server:80 -> My.Firewall.PC:61900
TCP TTL:109 TOS:0x0 ID:37731  DF
******A* Seq: 0x1892E6   Ack: 0xE63F2A7   Win: 0x220F
```

Close the connection.

Back to Exploits ^

Back to the Practical menu ^

Checking for Frontpage98 Holes (shtml.exe) First Check

```
[**] Twwwscan Filter [**]
08/09-04:27:24.425801 My.Firewall.PC:62092 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:63717  DF
**S***** Seq: 0xE664E27   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK


[**] Twwwscan Filter [**]
08/09-04:27:24.509979 My.Web.Server:80 -> My.Firewall.PC:62092
TCP TTL:109 TOS:0x0 ID:32358  DF
**S***A* Seq: 0x1A8E4F   Ack: 0xE664E28   Win: 0x2238
TCP Options => MSS: 1460


[**] Twwwscan Filter [**]
08/09-04:27:24.513097 My.Firewall.PC:62092 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:63973  DF
******A* Seq: 0xE664E28   Ack: 0x1A8E50   Win: 0x2238


[**] Twwwscan Filter [**]
08/09-04:27:24.514015 My.Firewall.PC:62092 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:64229  DF
*****PA* Seq: 0xE664E28   Ack: 0x1A8E50   Win: 0x2238
48 45 41 44 20 2F 5F 76 74 69 5F 62 69 6E 2F 73  HEAD /_vti_bin/s
68 74 6D 6C 2E 64 6C 6C 20 48 54 54 50 2F 31 2E  html.dll HTTP/1.
30 0A 0A                                         0..
```

Back to Exploits ^

Back to the Practical menu ^

Sending request for the File shtml.dll

```
[**] Twwwscan Filter [**]
08/09-04:27:24.601926 My.Web.Server:80 -> My.Firewall.PC:62092
TCP TTL:109 TOS:0x0 ID:32614  DF
*****PA* Seq: 0x1A8E50   Ack: 0xE664E4B   Win: 0x2215
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D  HTTP/1.1 200 OK.
0A 53 65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F  .Server: Microso
66 74 2D 49 49 53 2F 34 2E 30 0D 0A 44 61 74 65  ft-IIS/4.0..Date
3A 20 57 65 64 2C 20 30 39 20 41 75 67 20 32 30  : Wed, 09 Aug 20
30 30 20 30 37 3A 32 31 3A 31 35 20 47 4D 54 0D  00 07:21:15 GMT.
0A.
```

Request returns good data. Front Page extensions are installed on this host

```
[**] Twwwscan Filter [**]
08/09-04:27:24.605709 My.Firewall.PC:62092 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:64485  DF
****F*A* Seq: 0xE664E4B   Ack: 0x1A8EA1   Win: 0x21E7
```

We try to close connection

```
[**] Twwwscan Filter [**]
08/09-04:27:24.605719 My.Web.Server:80 -> My.Firewall.PC:62092
TCP TTL:109 TOS:0x0 ID:32870  DF
****FPA* Seq: 0x1A8EA1   Ack: 0xE664E4B   Win: 0x2215
43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 74 65  Content-Type: te
78 74 2F 68 74 6D 6C 0A 0A 3C 48 54 4D 4C 3E 3C  xt/html..<HTML><
48 32 3E 46 72 6F 6E 74 50 61 67 65 20 45 72 72  H2>FrontPage Err
6F 72 2E 3C 2F 48 32 3E 0A 0A 3C 50 3E 0A 3C 42  or.</H2>..<P>.<B
3E 55 73 65 72 3A 3C 2F 42 3E 20 70 6C 65 61 73  >User:</B> pleas
65 20 72 65 70 6F 72 74 20 64 65 74 61 69 6C 73  e report details
20 74 6F 20 74 68 69 73 20 73 69 74 65 27 73 20  to this site's
77 65 62 6D 61 73 74 65 72 2E 0A 3C 50 3E 0A 0A  webmaster..<P>..
3C 50 3E 0A 3C 42 3E 57 65 62 6D 61 73 74 65 72  <P>.<B>Webmaster
3A 3C 2F 42 3E 20 70 6C 65 61 73 65 20 73 65 65  :</B> please see
20 74 68 65 20 73 65 72 76 65 72 27 73 20 61 70  the server's ap
70 6C 69 63 61 74 69 6F 6E 20 65 76 65 6E 74 20  plication event
6C 6F 67 20 66 6F 72 20 6D 6F 72 65 20 64 65 74  log for more det
61 69 6C 73 2E 0A 3C 2F 50 3E                    ails..</P>
```

Server sends back error message after further processing request

```
[**] Twwwscan Filter [**]
08/09-04:27:24.608382 My.Firewall.PC:62092 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:64997  DF
***R**** Seq: 0xE664E4C   Ack: 0x0   Win: 0x0

[**] Twwwscan Filter [**]
08/09-04:27:24.687486 My.Web.Server:80 -> My.Firewall.PC:62092
TCP TTL:109 TOS:0x0 ID:33126  DF
******A* Seq: 0x1A8F7C   Ack: 0xE664E4C   Win: 0x2215

[**] Twwwscan Filter [**]
08/09-04:27:24.688791 My.Firewall.PC:62092 -> My.Web.Server:80
TCP TTL:109 TOS:0x0 ID:33382  DF
***R**** Seq: 0xE664E4C   Ack: 0x0   Win: 0x0
```

Connection is finally Closed

Exploit: Frontpage98 Hole(administrators.pwd)

```
[**] Twwwscan Filter [**]
08/09-04:27:24.607802 My.Firewall.PC:62093 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:64741  DF
**S***** Seq: 0xE664EDD   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK


[**] Twwwscan Filter [**]
08/09-04:27:24.687925 My.Web.Server:80 -> My.Firewall.PC:62093
TCP TTL:109 TOS:0x0 ID:33382  DF
**S***A* Seq: 0x1A8E5A   Ack: 0xE664EDE   Win: 0x2238
TCP Options => MSS: 1460


[**] Twwwscan Filter [**]
08/09-04:27:24.690886 My.Firewall.PC:62093 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:65253  DF
******A* Seq: 0xE664EDE   Ack: 0x1A8E5B   Win: 0x2238


[**] Twwwscan Filter [**]
08/09-04:27:24.699201 My.Firewall.PC:62093 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:65509  DF
*****PA* Seq: 0xE664EDE   Ack: 0x1A8E5B   Win: 0x2238
48 45 41 44 20 2F 63 66 69 64 65 2F 61 64 6D 69  HEAD /cfide/admi
6E 69 73 74 72 61 74 6F 72 2F 69 6E 64 65 78 2E  nistrator/index.
63 66 6D 20 48 54 54 50 2F 31 2E 30 0A 0A        cfm HTTP/1.0..
```

Here the software Query's for the Vulnerability.

```
[**] Twwwscan Filter [**]
08/09-04:27:24.783400 My.Web.Server:80 -> My.Firewall.PC:62093
TCP TTL:109 TOS:0x0 ID:33638  DF
*****PA* Seq: 0x1A8E5B   Ack: 0xE664F0C   Win: 0x220A
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4F 62 6A  HTTP/1.1 404 Obj
65 63 74 20 4E 6F 74 20 46 6F 75 6E 64 0D 0A 53  ect  Found..S
65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F 66 74  erver: Microsoft
2D 49 49 53 2F 34 2E 30 0D 0A 44 61 74 65 3A 20  -IIS/4.0..Date:
57 65 64 2C 20 30 39 20 41 75 67 20 32 30 30 30  Wed, 09 Aug 2000
20 30 37 3A 32 31 3A 31 35 20 47 4D 54 0D 0A 43  07:21:15 GMT..C
6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
36 31 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65  61..Content-Type
3A 20 74 65 78 74 2F 68 74 6D 6C 0D 0A 0D 0A     : text/html....
```

Again the server responds that it is vulnerable to this type of attack

```
[**] Twwwscan Filter [**]
08/09-04:27:24.783447 My.Web.Server:80 -> My.Firewall.PC:62093
TCP TTL:109 TOS:0x0 ID:33894  DF
****F*A* Seq: 0x1A8EEA   Ack: 0xE664F0C   Win: 0x220A


[**] Twwwscan Filter [**]
```

```
08/09-04:27:24.786065 My.Firewall.PC:62093 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:230  DF
******A* Seq: 0xE664F0C   Ack: 0x1A8EEB   Win: 0x21A9


[**] Twwwscan Filter [**]
08/09-04:27:24.794356 My.Firewall.PC:62093 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:486  DF
****F*A* Seq: 0xE664F0C   Ack: 0x1A8EEB   Win: 0x21A9


[**] Twwwscan Filter [**]
08/09-04:27:24.878302 My.Web.Server:80 -> My.Firewall.PC:62093
TCP TTL:109 TOS:0x0 ID:34150  DF
******A* Seq: 0x1A8EEB   Ack: 0xE664F0D   Win: 0x220A
```

Close the Connection.

[Back to Exploits](#) ^

[Back to the Practical menu](#) ^

Exploit: BB4 Big Brother (bb-hostsvc.sh)

```
[**] Twwwscan Filter [**]
08/09-04:27:24.795925 My.Firewall.PC:62094 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:742  DF
**S***** Seq: 0xE664F99   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460 NOP NOP SackOK


[**] Twwwscan Filter [**]
08/09-04:27:24.878405 My.Web.Server:80 -> My.Firewall.PC:62094
TCP TTL:109 TOS:0x0 ID:34406  DF
**S***A* Seq: 0x1A8E6F   Ack: 0xE664F9A   Win: 0x2238
TCP Options => MSS: 1460


[**] Twwwscan Filter [**]
08/09-04:27:24.881416 My.Firewall.PC:62094 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:998  DF
******A* Seq: 0xE664F9A   Ack: 0x1A8E70   Win: 0x2238


[**] Twwwscan Filter [**]
08/09-04:27:24.889165 My.Firewall.PC:62094 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:1254  DF
*****PA* Seq: 0xE664F9A   Ack: 0x1A8E70   Win: 0x2238
48 45 41 44 20 2F 63 67 69 2D 62 69 6E 2F 62 62  HEAD /cgi-bin/bb
2D 68 6F 73 74 73 76 63 2E 73 68 20 48 54 54 50  -hostsvc.sh HTTP
2F 31 2E 30 0A 0A                                /1.0..
```

Here is where the software checks for the vulnerability

```
[**] Twwwscan Filter [**]
08/09-04:27:24.984587 My.Web.Server:80 -> My.Firewall.PC:62094
TCP TTL:109 TOS:0x0 ID:34662  DF
*****PA* Seq: 0x1A8E70   Ack: 0xE664FC0   Win: 0x2212
48 54 54 50 2F 31 2E 31 20 34 30 34 20 4F 62 6A  HTTP/1.1 404 Obj
65 63 74 20 4E 6F 74 20 46 6F 75 6E 64 0D 0A 53  ect  Found..S
```

```
65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F 66 74  erver: Microsoft
2D 49 49 53 2F 34 2E 30 0D 0A 44 61 74 65 3A 20  -IIS/4.0..Date:
57 65 64 2C 20 30 39 20 41 75 67 20 32 30 30 30  Wed, 09 Aug 2000
20 30 37 3A 32 31 3A 31 35 20 47 4D 54 0D 0A 43  07:21:15 GMT..C
6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
36 31 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65  61..Content-Type
3A 20 74 65 78 74 2F 68 74 6D 6C 0D 0A 0D 0A     : text/html....
```

Server returns that this object is found. Signaling the software that this vulnerability does exist.

```
[**] Twwwscan Filter [**]
08/09-04:27:24.984634 My.Web.Server:80 -> My.Firewall.PC:62094
TCP TTL:109 TOS:0x0 ID:34918  DF
****F*A* Seq: 0x1A8EFF   Ack: 0xE664FC0   Win: 0x2212


[**] Twwwscan Filter [**]
08/09-04:27:24.987269 My.Firewall.PC:62094 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:1510  DF
******A* Seq: 0xE664FC0   Ack: 0x1A8F00   Win: 0x21A9


[**] Twwwscan Filter [**]
08/09-04:27:24.994803 My.Firewall.PC:62094 -> My.Web.Server:80
TCP TTL:127 TOS:0x0 ID:1766  DF
****F*A* Seq: 0xE664FC0   Ack: 0x1A8F00   Win: 0x21A9


[**] Twwwscan Filter [**]
08/09-04:27:25.097416 My.Web.Server:80 -> My.Firewall.PC:62094
TCP TTL:109 TOS:0x0 ID:35174  DF
******A* Seq: 0x1A8F00   Ack: 0xE664FC1   Win: 0x2212
```

Connection Closed

Back to Exploits ^

Back to the Practical menu ^

Assignment 3 - "Analyze This" Scenario

Assignment 3 - Preface

It's clear from the traces provided that this is a large network that is exposed to the world. After reviewing the data one can conclude that this site has garnered much attention from many countries.

Assignment 3 - Security Issues

In these traces I noticed the following key security issues:

1. Lack of ACL's on outside routers as evidence by the inbound non-established

packets.

2. It appears that all ports and services are open to the outside. (See portscans below)
3. Netbios Traffic being access by outside addresses (SMB wildcard lookups)

```
06/01-09:26:51.737965
        [**] SMB Name Wildcard [**]
                192.168.7.2:137 - MY.NET.14.1:137

06/01-09:26:53.237151
        [**] SMB Name Wildcard [**]
                192.168.7.2:137 - MY.NET.14.1:137

06/01-09:26:54.738994
        [**] SMB Name Wildcard [**]
                192.168.7.2:137 - MY.NET.14.1:137
```

In this particular example the source addresses are most likely spoofed (RFC 1918).

4. There are many proxy hosts available being used by outside addresses. The most used of which is MY.NET.253.105

   It is possible there is a web service running on this machine given the amount of traffic it gets. Quick checks of the users include the Chinese, Canada, Norway and several other countries. If this is an organization that does international business it is possible that this particular trace is a false positive.

   The other option is that this site is posted somewhere as known exploitable WinGate address , this is why it is garnering so much attention.

```
06/22-21:29:52.680784
        [**] WinGate 8080 Attempt [**]
                216.164.241.118:1246 -
                        MY.NET.253.105:8080

06/22-21:29:52.694081
        [**] WinGate 8080 Attempt [**]
                216.164.241.118:1247 -
                        MY.NET.253.105:8080

06/22-21:29:52.705269
        [**] WinGate 8080 Attempt [**]
                216.164.241.118:1248 -
                        MY.NET.253.105:8080

06/22-21:29:56.253092
        [**] WinGate 8080 Attempt [**]
                216.164.241.118:1251 -
                        MY.NET.253.105:8080
```

5. Possibly Compromised systems Nmapping network from the inside (MY.NET.253.12)

```
05/29-00:16:18.955718
        [**] spp_portscan:
                portscan status from MY.NET.253.12:
                        53 connections across 1 hosts:
                                TCP(53), UDP(0) [**]

05/29-00:16:22.104907
        [**] spp_portscan:
```

```
                portscan status from MY.NET.253.12:
                        51 connections across 1 hosts:
                                TCP(51), UDP(0) [**]

05/29-00:16:24.593328
        [**] spp_portscan:
                portscan status from MY.NET.253.12:
                        55 connections across 1 hosts:
                                TCP(55), UDP(0) [**]
```

6. Outside addresses are telneting directly into hosts.

```
05/24-01:31:53.275464
        [**] Watchlist 000222 NET-NCFC [**]
                159.226.41.99:23 - MY.NET.99.51:54054

05/24-01:32:05.234649
        [**] Watchlist 000222 NET-NCFC [**]
                159.226.41.99:23 - MY.NET.99.51:54054
```

7. Scans from China, Israel, Norway, Japan, AOL, UUNET, Berkley, and UCLA. All of which are suspicious networks.

```
05/24-01:57:26.925579
        [**] Watchlist 000220 IL-ISDNNET-990517 [**]
                212.179.44.36:1213 - MY.NET.217.86:6346

05/24-01:57:27.698640
        [**] Watchlist 000220 IL-ISDNNET-990517 [**]
                212.179.44.36:1213 - MY.NET.217.86:6346
```

8. Trace also showed several instances of ports used in Trin00 attacks usually in conjunction with source port 25.

```
05/25-11:21:29.016239
        [**] GIAC 000218 VA-CIRT port 34555 [**]
                216.64.2.218:25 - MY.NET.253.24:34555
                        <--- Possible Trin00 ports.

05/25-11:21:29.244083
        [**] GIAC 000218 VA-CIRT port 34555 [**]
                216.64.2.218:25 - MY.NET.253.24:34555

05/25-11:21:37.415580
        [**] GIAC 000218 VA-CIRT port 34555 [**]
                216.64.2.218:25 - MY.NET.253.24:34555

05/25-11:21:37.686029
        [**] GIAC 000218 VA-CIRT port 34555 [**]
                216.64.2.218:25 - MY.NET.253.24:34555

06/16-14:37:20.614561
        [**] GIAC 000218 VA-CIRT port 34555 [**]
                209.133.83.16:113 - MY.NET.6.47:34555

05/28-05:37:28.990772
        [**] GIAC 000218 VA-CIRT port 35555 [**]
                146.7.191.66:25 - MY.NET.253.24:35555
                        < ---udP Trin00
```

Miscellaneous

Here are some traces from compromised Unix hosts

MY.NET.218.66 is a compromised Unix host. Many people connecting to this device, mostly from AOL and other dialups.

Here is a recurring trace.

```
06/12-00:00:45.994021
        [**] Attempted Sun RPC high port access [**]
                205.188.153.106:4000 - MY.NET.218.66:32771

06/12-00:01:12.524762
        [**] Attempted Sun RPC high port access [**]
                205.188.153.106:4000 - MY.NET.218.66:32771

06/12-00:02:12.498991
        [**] Attempted Sun RPC high port access [**]
                205.188.153.106:4000 - MY.NET.218.66:32771
```

Here is a scanner looking for DNS probably using a tool like DENS. Note: The SYN-FIN flag is an attempt to evade Intrusion Detection.

```
06/13-01:30:39.786268
        [**] SYN-FIN scan! [**]
                204.60.176.2:53 - MY.NET.1.1:53

06/13-01:30:39.804052
        [**] SYN-FIN scan! [**]
                204.60.176.2:53 - MY.NET.1.2:53

06/13-01:30:39.824597
        [**] SYN-FIN scan! [**]
                204.60.176.2:53 - MY.NET.1.3:53

06/13-01:30:39.846143
        [**] SYN-FIN scan! [**]
                204.60.176.2:53 - MY.NET.1.4:53

06/13-01:30:39.861924
        [**] SYN-FIN scan! [**]
                204.60.176.2:53 - MY.NET.1.5:53
```

Here is a port scan against the network looking for Proxy servers.

```
06/01-01:59:33.328108
        [**] WinGate 8080 Attempt [**]
                202.38.128.188:1758 - MY.NET.4.13:8080

06/01-01:59:33.329885
        [**] WinGate 8080 Attempt [**]
                202.38.128.188:1759 - MY.NET.4.14:8080

06/01-01:59:33.329934
        [**] WinGate 8080 Attempt [**]
                202.38.128.188:1760 - MY.NET.4.15:8080

06/01-01:59:33.334266
        [**] WinGate 8080 Attempt [**]
                202.38.128.188:1761 - MY.NET.4.16:8080
```

Portmapper attempt

```
06/22-20:58:02.395459
        [**] External RPC call [**]
                212.25.68.195:637 - MY.NET.6.15:111

06/22-20:58:02.395531
        [**] External RPC call [**]
                212.25.68.195:637 - MY.NET.6.15:111

06/22-20:58:02.395602
        [**] External RPC call [**]
                212.25.68.195:637 - MY.NET.6.15:111
```

MY.NET.20.10 using port 27960 probably playing Quake

Suspected WinGate Servers

```
MY.NET.16.172
MY.NET.253.105
MY.NET.99.85
MY.NET.97.61
MY.NET.97.127
MY.NET.60.11
MY.NET.97.69
MY.NET.112.129
MY.NET.162.196
MY.NET.97.208
```

Back to the Assignment 3 menu ^

Back to the Practical menu ^

Security Recommendation.

The first task I would recommend is to add some Access Control Lists (ACLs) to the border router. These ACLs should specifically deny inbound traffic to the lower ports (unless needed, I.E. 53 ,25 and other needed services). Stop all RFC 1918 traffic inbound (Prevent Spoofing). Only allow established sessions. I would also disallow ports 1080 and 8080 as inbound. All of this is without knowing the core business of the company. It is possible that some of this traffic is legitimate. It is always important to consult the local administrators before making such changes.

As a follow up task, it would be prudent to address the compromised hosts. There is a long list of suspected WinGate proxy servers that Dialup users have been abusing to hide their addresses. It would also be wise to investigate the Unix hosts allowing RPC access. My.net.218.66 is a heavily used box that aroused some suspicion. Using a portscanner, like port scanner, to check these hosts would allow the local administrator to secure these boxes and lockout unused services.

Implement a security policy that includes host access lists and needed services for these devices. Using the security policy , devise a rule set for a stateful inspection firewall, like checkpoint, and a intrusion detection system. The firewall would protect the network by hiding it's address space and watching for common attacks. The outside router, with the proper rule set, would silently drop most of the packets.

It also appears some rule sets have been created to watch for certain address space. Specifically the NET-NCFC , IL-ISDNNET rule set. China and Israel were two I discovered. The Chinese network continually used email, perhaps using the SMTP hosts for spamming. The Israeli network was portscanning and accessing Unix host ports. If these networks are undesirable and there isn't a business need for anyone from these subnets to

access the network, dropping packets from them on the outside router is recommended. Educating users of the dangers on the Internet is also important. For instance, several false positives were created by a user accessing onlinescanner.com.

Back to the Practical menu ^