Mark Limesand

GCIA DC

Assignment 4

Analysis of Laurie's Network from January to August

The following is an analysis based on detects posted by Laurie@edu from January 1 to August 17 on the GIAC web site. This analysis will provide a list of the top ten attacks Laurie detected and posted at GIAC, the ten most common attacker address families, and a characterization of ISP load balancing detects on Laurie's site.

Laurie primarily uses Snort as her network IDS and Port Sentry for her host based IDS, so detects included in this report will be in these formats.

Top Ten Attacks Detected

Sun RPC Port mapper/RPCBIND:

Laurie detected several scans looking for Port mapper (port 111) and many attempts to retrieve the RPCBind version. If an attacker gains access to portmapper, it allows the attacker to scan a system for all enabled RPC services, such as rpc.mountd, NFS, rpc.statd, rpc.csmd, rpc.ttybd, amd, etc. If the intruder finds the appropriate service enabled, the intruder could then run an exploit against the port where the service is running

Example of Laurie's RPCBind attempt:

```
Feb 19 04:03:24 dns3 rpcbind: refused connect from 171.64.139.21 to dump()
```

CVE Number: CVE-1999-0190

FTP scans and logins:

Laurie detected several scans looking for FTP (port 21), she also detected a large number of failed ftp access attempts. The attackers may have been looking for open anonymous servers with directories that can be written to and read from. The attacker can use these machines to hide pirated programs or store other illegal information. The failed login attempts could have been an attempt to acquire user passwords for the same purpose.

Example of FTP SYN scan:

```
Jun 23 12:23:33 212.49.228.67:61323 -> a.b.c.33:21 SYN **S*****
Jun 23 12:23:36 212.49.228.67:61344 -> a.b.c.54:21 SYN **S*****
Jun 23 12:23:34 212.49.228.67:61352 -> a.b.c.62:21 SYN **S*****
Jun 23 12:23:34 212.49.228.67:61361 -> a.b.c.71:21 SYN **S*****
Jun 23 12:23:34 212.49.228.67:61391 -> a.b.c.101:21 SYN **S*****
Jun 23 12:23:38 212.49.228.67:61505 -> a.b.c.214:21 SYN **S*****
Jun 23 12:23:39 212.49.228.67:61511 -> a.b.c.220:21 SYN **S*****
Jun 23 12:23:37 212.49.228.67:61424 -> a.b.c.134:21 SYN **S*****
Jun 23 12:23:37 212.49.228.67:61460 -> a.b.c.170:21 SYN **S*****
```

Example of an attempt to acquire the sysadmin FTP Password.

```
[**] SYSADMIN - FTP-Password [**]
03/16-19:13:47.326701 141.35.5.23:61389 -> a.b.c.34:21
TCP TTL:246 TOS:0x0 ID:5175 DF
*****PA* Seq: 0xE8950A83 Ack: 0x34C9F6D2 Win: 0x2238
55 53 45 52 20 66 74 70 0D 0A 50 41 53 53 20 2D USER ftp..PASS -
6D 6F 7A 69 6C 6C 61 40 0D 0A 4D 4B 44 20 66 6F mozilla@..MKD fo
6F 0D 0A 52 4D 44 20 66 6F 6F 0D 0A 53 54 41 54 o..RMD foo..STAT
20 2F 65 74 63 0D 0A 51 55 49 54 0D 0A 00 85 /etc..QUIT....
```

Telnet scans and logins:

Laurie detected several scans looking for Telnet (port 23), she also detected a large number of failed telnet access attempts. The Attacker's where probably scanning this port looking for banners that could give them more information on the system, such as the type of operating system being used. The failed login attempts could also have been attackers trying to guess passwords to gain remote access.

Example of Telnet SYN scan

```
Jul 25 15:08:20 210.104.214.125:3249 -> a.b.c.33:23 SYN **S*****
Jul 25 15:08:20 210.104.214.125:3317 -> a.b.c.101:23 SYN **S*****
Jul 25 15:08:20 210.104.214.125:3333 -> a.b.c.117:23 SYN **S*****
Jul 25 15:08:20 210.104.214.125:3337 -> a.b.c.121:23 SYN **S*****
Jul 25 15:08:21 210.104.214.125:3350 -> a.b.c.134:23 SYN **S*****
Jul 25 15:08:23 210.104.214.125:3258 -> a.b.c.42:23 SYN **S*****
Jul 25 15:08:23 210.104.214.125:3231 -> a.b.c.15:23 SYN **S*****
```

Example of a Failed Telnet attempt

```
Jul 25 15:08:24 hostka in.telnetd[17839]: refused connect from 210.104.214.125
```

DNS:

Laurie detected several scans looking for DNS services on port 53. Attackers may be attempting to do zone transfers , spoof DNS entries, or just trying to hide their attacks because routers and firewalls generally pass traffic destined for port 53. This port is also commonly accessed by load balancing software, which helps determine the best route for traffic.

Example of using DNS to query for BIND

```
[**] MISC-DNS-version-query [**]
03/19-21:50:26.378945 198.146.83.191:1757 -> a.b.c.66:53 UDP TTL:52 TOS:0x0 ID:31183 Len: 38
F7 5F 01 80 00 01 00 00 00 00 00 00 07 76 65 72 ._..........ver
73 69 6F 6E 04 62 69 6E 64 00 00 10 00 03 sion.bind.....
```

CVE Number: CVE-1999-0010, CVE-1999-0024, CVE-1999-0048, CVE-1999-00184, CVE-1999-0274, CVE-1999-0275, CVE-1999-0299.

IMAP

Laurie detected several attackers looking for IMAP (port 143). IMAP servers have numerous buffer overflows that allow compromise during the login. There is also a popular Linux worm that spreads by port 143.

Example of an IMAP access attempt

```
Apr 18 15:08:19 dns1 portsentry[438328]: attackalert: Connect from host:
ppp166.usr198.pioneeris.net/208.3.198.166 to TCP port: 143
```

CVE Number: CVE-1999-0005, CVE-1999-0042

Finger scans and access attempts:

Laurie detected several scans looking for Finger(port 79). Finger is usually used during the reconnaissance phase of an attack, because the finger service provides information about users. Fingering a user will often display the contents of the .plan file or Finger can be used to list all the users who are logged on to the system.

Example of a Finger Null Probe:

```
[**] FINGER-ProbeNull [**]
04/17-12:08:46.778780 210.220.143.254:1539 -> z.y.x.34:79
TCP TTL:46 TOS:0x0 ID:21106 DF
*****PA* Seq: 0xFE7B0DB2 Ack: 0x31F3E22 Win: 0x7D78
6C 70 0D 0A 00 00 lp....
```

Example of a Finger access attempt

```
Apr 7 20:21:23 dns1 portsentry[438328]: attackalert: Connect from host: tide73.microsoft.com/131.107.3.73 to TCP port: 79
```

Proxy Scans:

Laurie detected several scans looking for known proxy such as Wingate (ports 1080 or 8080) and Squid proxies (port 3128). Attackers can use misconfigured wingate services to tunnel through a firewall into a network. The proxy servers can be used to mask an attack or surf the web anonymously.

Example of an Wingate SYN Scan

```
May 21 05:50:58 207.78.247.50:65535 -> a.b.c.51:8080 SYN **S*****
May 21 05:50:58 207.78.247.50:65535 -> a.b.c.80:8080 SYN **S*****
May 21 05:50:58 207.78.247.50:65535 -> a.b.c.83:8080 SYN **S*****
May 21 05:50:59 207.78.247.50:65535 -> a.b.c.114:8080 SYN **S*****
May 21 05:50:59 207.78.247.50:65535 -> a.b.c.134:8080 SYN **S*****
May 21 05:51:00 207.78.247.50:65535 -> a.b.c.186:8080 SYN **S*****
May 21 05:51:00 207.78.247.50:65535 -> a.b.c.189:8080 SYN **S*****
May 21 05:51:13 207.78.247.50:65535 -> a.b.f.39:8080 SYN **S*****
May 21 05:51:13 207.78.247.50:65535 -> a.b.f.41:8080 SYN **S*****
May 21 05:51:14 207.78.247.50:65535 -> a.b.f.86:8080 SYN **S*****
May 21 05:51:15 207.78.247.50:65535 -> a.b.f.145:8080 SYN **S*****
May 21 05:51:17 207.78.247.50:65535 -> a.b.f.242:8080 SYN **S*****
```

CVE Number: CVE-1999-0291, CVE-1999-0471

Ingleslock

Laurie detected several scans looking for Ingleslock services (port 1524). Many attack scripts install a backdoor shell at this port, these backdoors can be utilized for better access by attackers.

Example of an Ingleslock probe attempt:

```
May 19 11:53:02 dns3 portsentry[6017]: attackalert:   Connect from host: 212.72.63.240/212.72.63.240 to TCP port: 1524
```

Trojan Scans

Laurie detected several different types of trojan scans, the most common scans where for Netbus (port 12345 or 12346), Backorfice (port 31337), and Deepthroat (port 2140). Trojan programs can be used to get remote access to a user's machine.

Example of a Deepthroat trojan

```
[**] BACKDOOR SIGNATURE -- DeepThroat 3.1 Client Sending Data
to Server on Network [**]
04/01-20:02:49.845707 216.93.20.248:60000 -> A.B.C.34:2140 UDP TTL:109 TOS:0x0 ID:28665
Len: 10
30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00.............
00 00
```

Host Port Scan

Laurie detected several scan directed at an individual host. The most common scan was the SYN scan, but other scans such as SYN-FIN also appeared regularly on her network. One host appeared to be scanned the most z.y.x.34, this host must contain the students grades or something.

Example of a SYN Host Port Scan:

```
Apr 20 22:44:08 202.101.107.246:3849 -> z.y.x.34:258 SYN **S*****
Apr 20 22:44:09 202.101.107.246:3851 -> z.y.x.34:1080 SYN **S*****
Apr 20 22:44:09 202.101.107.246:3858 -> z.y.x.34:3128 SYN **S*****
Apr 20 22:44:11 202.101.107.246:3855 -> z.y.x.34:1750 SYN **S*****
Apr 20 22:44:11 202.101.107.246:3856 -> z.y.x.34:1795 SYN **S*****
Apr 20 22:44:12 202.101.107.246:3852 -> z.y.x.34:1089 SYN **S*****
Apr 20 22:44:12 202.101.107.246:3853 -> z.y.x.34:1505 SYN **S*****
Apr 20 22:44:12 202.101.107.246:3854 -> z.y.x.34:1745 SYN **S*****
Apr 20 22:44:12 202.101.107.246:3857 -> z.y.x.34:2019 SYN **S*****
Apr 20 22:44:12 202.101.107.246:3859 -> z.y.x.34:8080 SYN **S*****
Apr 20 22:44:12 202.101.107.246:3860 -> z.y.x.34:30303 SYN **S*****
Apr 20 22:44:14 202.101.107.246:3850 -> z.y.x.34:470 SYN **S*****
Apr 20 22:44:17 202.101.107.246:3849 -> z.y.x.34:258 SYN **S*****
```

Top Ten Address Families

Detected IP Number	Netname	Netblock
212.109.2.136	LINKAR-AB-NET	212.109.2.128 – 212.109.2.159
192.255.44.211	XOR Network Engineering	192.255.32.0 – 192.255.56.255
63.70.24.149	Sattech Ltd.	63.70.24.0 – 63.70.27.255
24.0.114.175, 24.1.217.196, 24.1.235.177, 24.1.249.76, 24.13.199.150, 24.15.0.21, 24.2.164.29, 24.2.57.248, 24.3.24.169, 24.4.3.218, 24.5.163.67, 24.5.77.133, 24.8.159.30, 24.8.213.46, 24.9.17.206	@Home Network	24.0.0.0 – 24.23.255.255
207.230.92.2	DeltaCom, Inc	207.230.92.0 – 207.230.92.255
207.246.129.131, 207.246.129.132, 207.246.129.133	Flying Crocodile, Inc.	207.246.129.0 – 207.246.129.255
24.65.93.104, 24.68.186.116	Shaw Fiberlink ltd.	24.64.0.0 – 24.71.255.255
134.157.2.64	University Pierre et Marie Curie	134.157.0.0 – 134.157.255.255
213.8.202.13, 213.8.203.144, 213.8.52.189	Euronet Digital Communications	213.8.0.0 – 213.8.255.255
208.3.198.166	Pioneer Internet Services	208.3.198.0 – 208.3.199.255

Load Balancing Characterization:

Load balancing is a technique used primarily by commercial web sites to distribute their customers across multiple servers. Load balancing allows the commercial web sites to determine which web server is closest to their customers. This information allows the web sites to connect their customers, when they log in, to their closest web server.

Load balancing signatures usually appear as probes, because much like an attacker they are gathering information to map a network. A typical load-balancing signature may look like a SYN scan directed towards port 53 or a traceroute.

The following are examples of load balancing, taken from Laurie's detects.

```
[**] IDS118 - MISC-Traceroute ICMP [**]
04/18-15:06:33.797982 208.3.198.166 -> z.y.x.34
ICMP TTL:1 TOS:0x0 ID:30982
ID:256 Seq:3584 ECHO
[**] IDS118 - MISC-Traceroute ICMP [**]
04/18-15:07:14.090114 208.3.198.166 -> z.y.x.34
ICMP TTL:1 TOS:0x0 ID:42246
ID:256 Seq:6912 ECHO
```

This trace looks like it may be load balancing instead of traceroute, the signature for load balancing would be the low TTL number.

Seen exact same connections from both IP's 00/01/26 on different machine

```
Jan 27 09:37:56 dns2 xinetd[17539]: FAIL: echo-stream address from=216.33.138.21
Jan 27 09:37:56 dns2 xinetd[17539]: FAIL: echo-stream address from=192.56.219.56
Feb 2 11:29:33 dns3 xinetd[11611]: FAIL: echo-stream address from=192.56.219.56
Feb 2 11:29:33 dns3 xinetd[11611]: FAIL: echo-stream address from=216.33.138.21
```

These traces look like US West and Exodus Communication are running their load balancing together. The signature for this load balancing would be that pings from different locations continue to show up at the same time.

```
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33441 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33442 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33443 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33444 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33445 UDP
Apr 8 02:23:28 63.236.82.149:33070 -> z.y.x.34:33446 UDP
Apr 8 02:23:29 63.236.82.149:33070 -> z.y.x.34:33447 UDP
Apr 8 02:23:29 63.236.82.149:33070 -> z.y.x.34:33448 UDP
```

```
Apr 6 13:07:18 204.176.88.5:54605 -> a.b.c.66:33651 UDP
Apr 6 13:07:19 204.176.88.5:54605 -> a.b.c.66:33652 UDP
Apr 6 13:07:19 204.176.88.5:54605 -> a.b.c.66:33653 UDP
Apr 6 13:07:20 204.176.88.5:54605 -> a.b.c.66:33654 UDP
Apr 6 13:07:21 204.176.88.5:54605 -> a.b.c.66:33655 UDP
```

More traces that look similar to traceroute, but are probably load balancing.

```
Jan 7 17:30:29 milo named[2095]: security: notice: refused query on non-query socket from [208.32.211.70].53
Jan 7 17:33:37 milo named[2095]: security: notice: refused query on non-query socket from [204.253.104.74].53

Jan 7 17:30:23 jeru named[2121]: security: notice: refused query on non-query socket from [204.253.104.11].53
Jan 7 17:33:27 jeru named[2121]: security: notice: refused query on non-query socket from [199.95.208.86].53
```

Two more load balancing traces, notice that the trace is generated from port 53.

```
[**] MISC-Source Port Traffic2 <1023 [**]
02/10-09:41:20.014491 157.130.34.158:53 -> x.x.x.x:53
TCP TTL:247 TOS:0x0 ID:0
S***A* Seq: 0xBA90A Ack: 0xBA909 Win: 0x1020
TCP Options => MSS: 556
3A EF :.

[**] MISC-Source Port Traffic2 <1023 [**]
02/10-09:41:22.018198 157.130.34.158:53 -> x.x.x.x:53
TCP TTL:247 TOS:0x0 ID:0
S***A* Seq: 0xBA90A Ack: 0xBA909 Win: 0x1020
TCP Options => MSS: 556
2E 5F ._

[**] MISC-Source Port Traffic2 <1023 [**]
02/10-10:29:26.192859 157.130.34.158:53 -> x.x.x.x:53
TCP TTL:247 TOS:0x0 ID:0
S***A* Seq: 0xBC225 Ack: 0xBC224 Win: 0x1020
TCP Options => MSS: 556
BC 52 .R
```

This trace appears to have Cisco Dist Dir load balancing signature, notice the Ack number is always one less than the Seq number.