Global Information Assurance Certification Paper

Grade: **82**

Practical Exam

Student: Robert Neel

All scans were taken from the Giac website.

SCAN #1 -- http://www.sans.org/y2k/032200-1700.htm

Active Targeting Yes

History This series of scans took place over a 5-day period.

Technique The first log was from Friday 3/17. This was a series of NULL and SYN-FIN scans. The scans came in low and slow (the rate of approximately 2 an hour) and spanned a range of IPS and ports – including port 20 (FTP). By Saturday (3/18) the person begins by scanning 3 different IPS and then changes tactics and addresses a barrage of packets to a single IP. The packets are directed towards port 32771. (Note at this point I would want to check this port to see if their were any services running here and look at the server logs to see how performance was at this time. This does not appear to have been a denial of service attack. That in mind I would want to look at the packets to see if they contained a pay load … possible buffer over flow attempt?). On Sunday (3/19) the attacker moved to scanning port 53 on a series of addresses, likely looking for DNS servers. By this time the person has given up on slow scan, which might avoid detection. By Monday the attacker is again trying to find an opening but has moved from DNS to looking for port 513 (remote login). Again he has moved to a slow approach sending approximately 2 to 3 packets an hour. And on Tuesday (3/21) the attacker went after two different IPS (using two different HIGH PORTS). An examination of several of the packets sent during this day shows that it may have been an attempt to Deny Service by using mal formed packets (ones with a variety of invalid flag combinations). It appears that some automation tools were utilized (like NMAP). Also note the Queso footprint .. indicating that this person was also trying to determine OS versions.

Intent The intent here is malicious in nature. Likely the attacker wanted to break into the system and when those attempts failed tried a Denial of Service attack instead. It does not appear that we responded to any of the packets (though logs should be checked). Despite that I consider Criticality to be medium, the targeted systems should be reviewed.

```
**********************************************************
Snort Alert Report at Fri Mar 17 00:07:51 2000
**********************************************************
[**] Null scan! [**]
03/16-01:27:57.485769 24.64.19.140:3063 -> MY.NET.206.142:2991
[**] Null scan! [**]
03/16-01:30:31.674565 24.64.19.140:3063 -> MY.NET.206.142:2991
[**] GIAC 08-feb-2000 [**]
03/16-01:37:33.676675 195.11.50.204:30973 -> MY.NET.179.77:49172
```

03/16-11:41:46.460762 212.179.103.67:2002 -> MY.NET.203.122:1569
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/16-11:43:21.251424 212.179.103.67:2002 -> MY.NET.203.122:1574
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/16-11:43:24.635912 212.179.103.67:2002 -> MY.NET.203.122:1574
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
03/16-11:43:27.585184 212.179.103.67:2002 -> MY.NET.203.122:1574
[**] Watchlist 000220 IL-ISDNNET-990517 [**]

****

Snort Alert Report at Sat Mar 18 00:07:03 2000

****

[**] Null scan! [**]
03/17-00:50:52.356514 24.112.101.113:6688 -> MY.NET.203.222:1224
[**] Null scan! [**]
03/17-00:56:44.127909 128.187.245.108:1869 -> MY.NET.10.119:6699
[**] Null scan! [**]
03/17-00:56:58.992306 128.187.245.108:1869 -> MY.NET.10.119:6699
[**] Null scan! [**]
03/17-01:06:25.280756 194.159.250.7:27055 -> MY.NET.202.66:2540
[**] SUNRPC highport access! [**]
03/17-01:16:18.869972 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]
03/17-01:16:18.871746 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]
03/17-01:16:18.958701 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]
03/17-01:16:18.962787 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]
03/17-01:16:19.145445 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]
03/17-01:16:19.205452 216.18.11.237:5501 -> MY.NET.213.50:32771
03/17-01:16:20.347234 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]
03/17-01:16:20.361265 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]
03/17-01:16:20.365529 216.18.11.237:5501 -> MY.NET.213.50:32771
[**] SUNRPC highport access! [**]

****

Snort Alert Report at Sun Mar 19 00:09:40 2000

****

[**] SYN-FIN scan! [**]
03/18-02:25:46.587048 194.112.42.193:53 -> MY.NET.1.1:53
[**] SYN-FIN scan! [**]
03/18-02:25:46.608902 194.112.42.193:53 -> MY.NET.1.2:53

[**] SYN-FIN scan! [**]
03/18-02:25:46.630302 194.112.42.193:53 -> MY.NET.1.3:53
[**] SYN-FIN scan! [**]
03/18-02:25:46.651612 194.112.42.193:53 -> MY.NET.1.4:53
[**] SYN-FIN scan! [**]
03/18-02:25:46.672247 194.112.42.193:53 -> MY.NET.1.5:53
[**] SYN-FIN scan! [**]
03/18-02:25:46.692692 194.112.42.193:53 -> MY.NET.1.6:53
03/18-02:25:47.050602 194.112.42.193:53 -> MY.NET.1.24:53
[**] SYN-FIN scan! [**]
03/18-02:25:47.070911 194.112.42.193:53 -> MY.NET.1.25:53
[**] SYN-FIN scan! [**]

****
Snort Alert Report at Mon Mar 20 00:08:06 2000
****
[**] NMAP TCP ping! [**]
03/19-00:00:07.936579 207.26.214.80:43445 -> MY.NET.53.28:513
[**] NMAP TCP ping! [**]
03/19-00:00:39.243471 207.26.214.80:43445 -> MY.NET.53.29:513
[**] NMAP TCP ping! [**]
[**] NMAP TCP ping! [**]
03/19-00:26:18.127953 207.26.214.80:43445 -> MY.NET.53.89:513
[**] NMAP TCP ping! [**]
03/19-00:26:54.265960 207.26.214.80:43445 -> MY.NET.53.90:513
[**] NMAP TCP ping! [**]
03/19-00:27:16.817174 207.26.214.80:43445 -> MY.NET.53.91:513
[**] NMAP TCP ping! [**]

****
Snort Alert Report at Tue Mar 21 00:09:42 2000
****
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:11:31.991596 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:11:32.578088 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:03.682005 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:03.770310 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]

[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:08.557927 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:08.937122 159.226.5.188:25 -> MY.NET.100.230:60885

[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:10.380533 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:10.392163 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:10.960682 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-01:12:11.039891 159.226.5.188:25 -> MY.NET.100.230:60885
[**] Watchlist 000222 NET-NCFC [**]
03/20-02:54:47.855597 159.226.133.85:25 -> MY.NET.100.230:62209
[**] Watchlist 000222 NET-NCFC [**]
03/20-02:54:49.582127 159.226.133.85:25 -> MY.NET.100.230:62209
[**] Watchlist 000222 NET-NCFC [**]
03/20-02:55:00.944415 159.226.133.85:25 -> MY.NET.100.230:62209
[**] Watchlist 000222 NET-NCFC [**]
03/20-02:55:02.281149 159.226.133.85:25 -> MY.NET.100.230:62209
[**] Watchlist 000222 NET-NCFC [**]
03/20-02:55:11.260664 159.226.133.85:25 -> MY.NET.100.230:62209
[**] Watchlist 000222 NET-NCFC [**]

OOS check /usr/LOG/packets/Mar.20.2000.packets.de0.gz

-*> Snort! <*-
Version 1.5
By Martin Roesch (roesch@clark.net, www.clark.net/~roesch)
snaplen = 68
Entering readback mode....
03/20-00:42:35.445056 194.217.172.23:27070 -> MY.NET.140.178:27005
TCP TTL:239 TOS:0x0 ID:8603 DF
SF****21 Seq: 0x7B961C Ack: 0x84C30000 Win: 0x0
TCP Options => Opt 68 (15): 6107 1C00 F086 0000 8045 0064 0000
00 64 .d

03/20-00:42:54.180211 194.217.172.23:27070 -> MY.NET.140.178:27005
TCP TTL:239 TOS:0x0 ID:8622 DF
SF*PAU Seq: 0x5E4278 Ack: 0xE63B0000 Win: 0x0
TCP Options => Opt 68 (15): 0507 1C33 FF0E 0000 8058 0064 0000
EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL EOL
EOL EOL EOL EOL EOL

03/20-00:43:06.075488 194.217.172.23:7744 -> MY.NET.140.178:1065
TCP TTL:239 TOS:0x0 ID:8650 DF
SF**A*2 Seq: 0x2D6B4B Ack: 0x1A45C466 Win: 0xB1B9
TCP Options => Opt 128 (40): D0C6 4D26 17BA 9C90 E714 A168 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
4D 26 17 BA 9C 90 E7 14 A1 68 M&.....h

03/20-01:20:52.930512 MY.NET.201.42:1918 -> 207.158.192.95:443
TCP TTL:126 TOS:0x0 ID:52137 DF
SF***U21 Seq: 0x11C51E6 Ack: 0x2AA7 Win: 0x5010
00 00 2A A7 23 E3 50 10 21 A6 07 EB 20 20 20 20 ..*.#.P.!...
20 00 .

03/20-07:42:35.043376 MY.NET.206.130:3607 -> 195.205.246.2:6699
TCP TTL:126 TOS:0x0 ID:51561 DF
SF*PA*2 Seq: 0x212DF506 Ack: 0x2BB0 Win: 0x5010
TCP Options => Opt 32 (32): 2020 2000 1213 1415 1617 1819 0000
0000 0000 0000 0000 0000 0000 0000 0000 EOL EOL EOL EOL EOL EOL EOL EOL

SCAN #2 -- http://www.sans.org/y2k/032600.htm

Active Targeting Yes

History Unknown .. access to previous logs was not available.

Technique A series of TCP packets directed at several ports on a single address. The ports are high ports indicating that the person may be looking for a service available for exploit, I would want to follow up by trying a getport (Good) on these to see if something is running on them. The packets were all received within an hour timeframe.

Intent Likely malicious in nature .. I would log this as an attempted port scan incident. Again, logs need to be reviewed to see if we responded – if not low criticality.

Any known trojans or signatures associated with 5317, 7877, 18117, …??? **-2**

All are from 3/25/2000

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/5317 13:26

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/7877 13:31

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/18117 13:39

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/15557 13:53

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/20677 13:56

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/25797 14:07

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/23237 14:19

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/25797 14:29

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/28357 14:39

Message: Deny inbound tcp src outside:200.249.238.9/8803

dst DMZ:my.net.60.98/28357 14:39

SCAN #3 -- http://www.sans.org/y2k/032600.htm

Active Targeting Yes

History Unknown .. access to previous logs was not available.

Technique A series of TCP packets directed at general ports on two different IP addresses. Note that the person has particular interest in port 27960. This port is not known for carrying a vulnerability (Trojan, etc..) so I would likely check to see what, if any, services were running on it. It should also be noted that this is directed as the user is using a variety of techniques to try and map the system, including a Null scan and SYN-FIN scan.

Intent Likely malicious in nature .. I would log it as a port scanning attempt and watch for future traffic. Did we respond (need to review logs)? Criticality low.

03/21-14:11:36.709202 212.238.134.99:27960 ->

MY.NET.10.119:27960 [**] Null scan! [**]

03/21-14:17:03.577695 212.238.134.99:27998 ->

MY.NET.10.119:27960 [**] Null scan! [**]

03/21-14:19:54.502156 212.238.134.99:27035 ->

MY.NET.10.119:3387 [**] Null scan! [**]

03/21-14:28:33.842668 212.238.134.99:9000 ->

MY.NET.10.119:9000 [**] Null scan! [**]
03/21-14:44:33.440931 212.238.134.99:21033 ->
MY.NET.10.119:2310 [**] Null scan! [**]
03/21-14:47:54.144549 212.238.134.99:27025 ->
MY.NET.10.119:2867 [**] Null scan! [**]
03/21-14:49:43.116595 212.238.134.99:27980 ->
MY.NET.10.119:27960 [**] Null scan! [**]
03/21-21:15:56.588060 194.217.188.53:27970 ->
MY.NET.98.133:27960 [**] SUNRPC highport access! [**]
03/21-21:17:31.168603 194.217.188.53:7788 ->
MY.NET.98.133:32771 [**] SYN-FIN scan! [**]
03/21-21:23:21.544496 194.217.188.53:27995 ->
MY.NET.98.133:10832 [**] Null scan! [**]
03/21-21:23:32.619598 194.217.188.53:7799 ->
MY.NET.98.133:2294 [**] Null scan! [**]
03/21-21:23:35.824415 194.217.188.53:27990 ->
MY.NET.98.133:27960 [**] Null scan! [**]
03/21-21:24:15.050650 194.217.188.21:27970 ->
MY.NET.98.130:29898 [**] Null scan! [**]
03/21-21:25:16.015794 194.217.188.53:27990 ->
MY.NET.98.133:27960

SCAN #4 -- http://www.sans.org/y2k/032500-2200.htm --- Second part

Active Targeting Yes

History	Unknown – access to previous logs unavailable.
Technique	Two SYN FIN scans directed at port 53 (DNS). Note that the scans are directed to broadcast addresses (xxx.xxx.xxx.1). This is an attempt to scan an two different subnets for DNS servers. Note that this person is likely looking for Unix based systems (do to the broadcast address .. most windows systems respond to the 255 broadcast).
Intent	Malicious in nature .. I would follow up on the source IP address to see where it originated from. Any responses from our systems (or do I even have a DNS server on those subnets?).

[**] IDS198/SYN FIN Scan [**]

03/25-02:42:56.289241 210.169.244.35:53 -> XXX.XXX.2.1:53

TCP TTL:21 TOS:0x0 ID:39426

SF** Seq: 0x4221C521 Ack: 0x2B4C5230 Win: 0x404

[**] IDS198/SYN FIN Scan [**]

03/25-02:43:01.438218 210.169.244.35:53 -> XXX.XXX.3.1:53

TCP TTL:21 TOS:0x0 ID:39426

SF** Seq: 0x27DC4B2F Ack: 0x746310E3 Win: 0x404

SCAN #5 -- http://www.sans.org/y2k/032300.htm

Active Targeting	Yes
History	Unknown – access to previous logs unavailable.
Technique	This appears to be a reconnaissance mission with the probable intent of locating a proxy (port 3128).
Intent	Malicious in nature. Port 3128 is a known exploit and appears to have been targeted. In addition, I would devote attention to examining logs to see if there was any unusual outbound (especially FTP) traffic (Possible Ring-0??). (PROXY not exploit SRN)

Mar 23 02:50:58 beer kernel: Packet log: input DENY ppp0

PROTO=6 202.102.129.59:1719 139.130.12.177:3128

L=48 S=0x00 I=50768 F=0x4000 T=112 SYN (#18)

Mar 23 02:51:07 beer kernel: Packet log: input DENY ppp0

PROTO=6 202.102.129.59:1719 139.130.12.177:3128

L=48 S=0x00 I=12114 F=0x4000 T=112 SYN (#18)

SCAN #6 -- http://www.sans.org/y2k/032200-1730.htm

Active Targeting Yes

History A series of scans/attacks of port 111 over a three-day period.

Technique It appears that the person started with port scanning for the RPC service on TCP Port 111 to see if he could get a response from one of several IPS. The scan was low and slow and appears to have been from two originated from two different places (possible two different accounts..the timing is too coincidental). Soon following appears to have been an attempt to compromise or overload UDP port 111 (interesting as TCP port 111 contains the RPC service). It should also be noted that the HEX dumps of the packets starting on March 22 shows packets that were likely crafted (notice the interesting MS size and repetitive ack number). I would not be surprised to find that this was a compromised machine .. I would follow up with the .edu (if the address was legitimate). Also notice that the TTL is 51 on all these packets possibly lending in site into which program was used to craft the packets.

Intent Malicious in nature with the intention of trying to locate / compromise TCP port 111 with the possible follow up of an attempt at a denial of service attack (fast number of packets suddenly directed at UDP port 111). Good.

Mar 20 23:00:59 myhost portsentry[176]: attackalert:

Connect from host: swift.ee.umist.ac.uk/130.88.118.27

to TCP port: 109

Mar 20 23:00:52 myhost portsentry[8303]: attackalert:

Connect from host: swift.ee.umist.ac.uk/130.88.118.27

to TCP port: 109

Mar 21 07:04:15 myhost portsentry[8303]: attackalert:

Connect from host: 210.222.56.101/210.222.56.101

to TCP port: 111
Mar 22 05:50:28 myhost portsentry[176]: attackalert:
Connect from host: 203.239.174.82/203.239.174.82
to TCP port: 111
Mar 22 15:30:44 myhost portsentry[176]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to TCP port: 111
Mar 22 15:30:28 myhost portsentry[8303]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to TCP port: 111
Mar 22 15:33:38 myhost portsentry[178]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to UDP port: 111
Mar 22 15:33:43 myhost portsentry[178]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to UDP port: 111
Mar 22 15:33:48 myhost portsentry[178]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to UDP port: 111
Mar 22 15:33:53 myhost portsentry[178]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to UDP port: 111
Mar 22 15:33:58 myhost portsentry[178]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to UDP port: 111
Mar 22 15:34:03 myhost portsentry[178]: attackalert:
Connect from host: cdu6-251.gu.net/195.123.249.251
to UDP port: 111

15:27:06.961763 209.203.237.176.22 > 10.0.3.40.1153:
S 1074448401:1074448401(0) ack 674711610 win 8192 <mss 16>
(ttl 51, id 28329)
0000: 4500 002c 6ea9 0000 3306 901a d1cb edb0 E..,n...3.....
0010: 0a00 0328 0016 0481 400a c811 2837 483a ...(....@...(7H:
0020: 6012 2000 778d 0000 0204 0010 0000 `. .w.....

16:27:44.950630 209.203.237.176.22 > 10.1.7.96.1700:
S 2485173332:2485173332(0) ack 674711610 win 8192 <mss 65528>
(ttl 51, id 17767)
0000: 4500 002c 4567 0000 3306 5a19 d1cb edb0 E..,Eg..3.Z.....
0010: 0a01 0760 0016 06a4 9420 bc54 2837 483a ...`..... .T(7H:
0020: 6012 2000 cde4 0000 0204 fff8 0000 `. ....

16:56:00.226219 209.203.237.176.22 > 10.1.7.107.1555:
S 2535447425:2535447425(0) ack 674711610 win 8192 <mss 16>
(ttl 51, id 59846)
0000: 4500 002c e9c6 0000 3306 b5ae d1cb edb0 E..,....3.......
0010: 0a01 076b 0016 0613 971f db81 2837 483a ...k........(7H:
0020: 6012 2000 ac27 0000 0204 0010 0000 `. ..'........

SCAN #7 -- http://www.sans.org/y2k/032100.htm

Active Targeting	Yes
History	Unknown .. past logs not available
Technique	A quick series of TCP packets directed at port 27374 (of a single IP). This appears to be a Trojan scan (searching for SubSeven). As this attack was directed towards one IP I would likely look at the machine to make sure the Trojan was not running on it. Good.
Intent	Malicious.

Mar 20 19:03:12 spirit /kernel: ipfw: 30000
Deny TCP 24.18.2.223:2674 10.11.48.
22:27374 in via ed1
Mar 20 19:03:12 spirit snort: ALERT: 24.18.2.223:2674 ->
10.18.48.22:27374

Snort Packet decode:

03/20-19:03:12.289836 24.18.2.223:2674 -> 10.11.48.22:27374

TCP TTL:116 TOS:0x0 ID:44122 DF

S***** Seq: 0xEF3884 Ack: 0x0 Win: 0x2000

TCP Options => MSS: 1460 NOP NOP Opt 4:

SCAN #8 -- http://www.sans.org/y2k/032100-2000.htm

Active Targeting Yes

History Unknown .. past logs not available

Technique A series of HTTP requests aimed at using some known CGI exploits. Notice that this person performed one request every hour .. very patient and trying to avoid detection. Good.

Intent Malicious. If using CGI check directories for common exploits .. criticality low.

```
strauss.udel.edu - - [19/Mar/2000:11:41:23 -0500] "GET
/cgi-bin/counterfiglet/nc/f=;echo;echo%20{_begin-counterfiglet_};
uname%20-a;id;w;echo%20{_end-counterfiglet_};echo
HTTP/1.0" 404 301
strauss.udel.edu - - [19/Mar/2000:21:44:53 -0500] "POST /cgi-bin/test-cgi
HTTP/1.0" 404 210
strauss.udel.edu - - [20/Mar/2000:18:47:53 -0500] "POST /cgi-bin/perl
HTTP/1.0" 404 206
strauss.udel.edu - - [21/Mar/2000:00:31:37 -0500] "POST /cgi-bin/sh
HTTP/1.0" 404 204
strauss.udel.edu - - [21/Mar/2000:01:16:06 -0500] "GET
/cgi-bin/query?x=%3C%21%2D%2D%23%65%78%65%63%20%63%6D%64
%3D%22%2F%75%73%72%2F%62%69%6E%2F%69%64%22%2D%2D%3E
HTTP/1.0" 404 207
```

SCAN #9

Active Targeting Yes

History	Unknown .. past logs not available
Technique	It appears that this person is trying to fingerprint our systems by sending a series of TCP packets with bad flag combinations and waiting to see how our systems handle them.(Good) The response of systems to impossible flag sets helps in determining what operating system is being run.
Intent	Malicious. I would want a full log to see if any our systems responded to anything. The criticality of this attack (depending on if we responded) is fairly low.

03/25-05:00:42.965869 169.229.110.69:0 -> MY.NET.201.142:1036
TCP TTL:113 TOS:0x0 ID:16045 DF
SFR*** Seq: 0x1A2000A9 Ack: 0xBE8700A4 Win: 0x5018
TCP Options => EOL EOL Opt 165 (40): FA40 B400 ECF2 868A EE47 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

03/25-05:01:50.296285 169.229.110.69:1039 -> MY.NET.201.142:6688
TCP TTL:113 TOS:0x0 ID:65477 DF
SFRPA* Seq: 0x7F Ack: 0xD6AC00A6 Win: 0x5010
00 00 3E 89 36 39 0D D8 CD 2E EC 4B AB D2 ..>.69.....K..

03/25-08:14:32.936127 24.200.89.143:1105 -> MY.NET.97.80:6688
TCP TTL:114 TOS:0x0 ID:59390 DF
SF***U2 Seq: 0x45 Ack: 0x19205F21 Win: 0x5010
TCP Options => EOL EOL EOL EOL EOL EOL SackOK Opt 20 (21): 1617 1819 0000 0000 0000 0000 0000 0000 0000 0000 0000 EOL EOL EOL EOL EOL EOL EOL

SCAN #10

Active Targeting Yes

History	Unknown .. past logs not available
Technique	This is a scan of a single IP with the intention of trying to locate some common services .. note 8080: Proxy, 110: Pop3, 1080: Socks, and 8080: Proxy.The scan is from a single IP and I would note it and, after identification, would probably follow up with the company (possible compromised host). The scan comes at a quick pace and has a Source port pattern .. indicating possible automation (use of some utility). Good.
Intent	Malicious. I would want a full log to see if any our systems responded to anything. The criticality of this attack (depending on if we responded) is fairly low.

Mar 17 20:33:20 drop in tcp syn 133.11.89.118:2694 209.58.151.30:110 (60)
Mar 17 20:33:41 last message repeated 3 times
Mar 17 22:31:59 permit in icmp (8,0) 137.148.18.185 209.58.151.30 (36)
Mar 17 22:59:10 drop in tcp syn 137.148.18.185:4463 209.58.151.30:1080 (48)
Mar 17 22:59:10 drop in tcp syn 137.148.18.185:4464 209.58.151.30:1745 (48)
Mar 17 22:59:10 drop in tcp syn 137.148.18.185:4465 209.58.151.30:8010 (48)
Mar 17 22:59:13 drop in tcp syn 137.148.18.185:4463 209.58.151.30:1080 (48)
Mar 17 22:59:13 drop in tcp syn 137.148.18.185:4464 209.58.151.30:1745 (48)
Mar 17 22:59:13 drop in tcp syn 137.148.18.185:4465 209.58.151.30:8010 (48)
Mar 17 22:59:13 drop in tcp syn 137.148.18.185:4466 209.58.151.30:8080 (48)
Mar 17 22:59:19 drop in tcp syn 137.148.18.185:4463 209.58.151.30:1080 (48)
Mar 17 22:59:19 drop in tcp syn 137.148.18.185:4464 209.58.151.30:1745 (48)
Mar 17 22:59:19 drop in tcp syn 137.148.18.185:4465 209.58.151.30:8010 (48)
Mar 17 22:59:19 drop in tcp syn 137.148.18.185:4466 209.58.151.30:8080 (48)
Mar 17 22:59:31 drop in tcp syn 137.148.18.185:4463 209.58.151.30:1080 (48)
Mar 17 22:59:31 drop in tcp syn 137.148.18.185:4464 209.58.151.30:1745 (48)
Mar 17 22:59:31 drop in tcp syn 137.148.18.185:4465 209.58.151.30:8010 (48)