Global Information Assurance Certification Paper

*** Northcutt, I think you are on your way to being a strong analyst. 74 *

Brent Spencer
GIAC Practical for SANS 2000 IDIC

I support several small to mid-size customer networks that are "uninteresting" (i.e. no military secrets, no banks, very low profile). I didn't believe that I would learn this much about my own and customers networks. I guess I shouldn't say I was pleasantly surprised when I started seeing detects, but I didn't expect to see any. I listed the ones I have seen here and analyze the rest from the GIAC home page.

After SANS 2000, I configured a single SHADOW system to be a sensor and the analyzer. I moved it from site to site as time allowed. I used the system mainly as a sensor and then manually scanned for detects.

Following the process from the classes at SANS 2000

- Evidence of Active Targeting
- Identify their Techniques
- Evidence of Intent
- Identify their History
- Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Here are my detects.

1) Pinging Broadcast Address

```
23:36:50.940295 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:41:43.170364 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:43:30.358418 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:43:31.349391 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:43:32.349434 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:43:33.349460 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:45:34.349397 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:45:35.349424 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:45:36.349451 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:45:37.349388 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:49:04.349397 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:49:05.349424 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:49:06.349451 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:49:07.349388 > 192.168.1.1 > 172.20.1.255: icmp: echo request
```

Targeting

There is active targeting.

Techniques

From the timing, it looks to be a manual process combined with the ping from a Windows systems (four pings, one second apart). I'm not quite sure why more than once was necessary.

Intent

The intent was to map my subnet with a broadcast ping.

History

Unknown. Most directed broadcasts are disabled on routers

Severity

1

Resolution

I had the network group turn off directed broadcasts on the router.

2) Ping Scan

```
23:36:49.806776 > 192.168.1.1 > 172.20.1.12: icmp: echo request
23:36:49.809115 < 172.20.1.2 > 192.168.1.1: icmp: echo reply
23:36:49.810666 < 172.20.1.3 > 192.168.1.1: icmp: echo reply
23:36:49.810826 < 172.20.1.5 > 192.168.1.1: icmp: echo reply
23:36:49.810893 < 172.20.1.10 > 192.168.1.1: icmp: echo reply
23:36:49.810961 < 172.20.1.6 > 192.168.1.1: icmp: echo reply
23:36:49.811046 < 172.20.1.12 > 192.168.1.1: icmp: echo reply
23:36:49.812065 < 172.20.1.9 > 192.168.1.1: icmp: echo reply
23:36:49.813224 < 172.20.1.4 > 192.168.1.1: icmp: echo reply (DF)
23:36:49.824805 < 172.20.1.7 > 192.168.1.1: icmp: echo reply
23:36:49.949320 > 192.168.1.1 > 172.20.1.1: icmp: echo request
23:36:49.949616 > 192.168.1.1 > 172.20.1.8: icmp: echo request
23:36:50.534861 > 192.168.1.1 > 172.20.1.200: icmp: echo request
23:36:50.537779 < 172.20.1.200 > 192.168.1.1: icmp: echo reply
23:36:50.940295 > 192.168.1.1 > 172.20.1.255: icmp: echo request
23:36:50.941277 < 172.20.1.1 > 192.168.1.1: icmp: echo reply (DF)
23:36:50.946201 < 172.20.1.7 > 192.168.1.1: icmp: echo reply
.
.
.
```

Targeting

There is active targeting.

Techniques

From the timing (very quick), it looks to be an automated process – potentially an NMAP ping scan. This happened several times. Again, I'm not sure why several tries were needed – possibly someone trying out a new "tool"?

Intent

The intent was to map my subnet with a ping scan.

History

Unknown.

Severity

2

Resolution

I am keeping an eye out for this source IP address.

3) IMAP Scan

```
23:37:03.950162 > 192.168.1.1.2686 > 172.20.1.2.imap2: S
317920963:317920963(0)
win 32120 <mss 1460,sackOK,timestamp 2056792 0,nop,wscale 0> (DF)
23:37:04.029787 > 192.168.1.1.2697 > 172.20.1.2.imap2: S
321887606:321887606(0)
win 32120 <mss 1460,sackOK,timestamp 2056800 0,nop,wscale 0> (DF)
23:37:04.109847 > 192.168.1.1.2708 > 172.20.1.2.imap2: S
320722183:320722183(0)
win 32120 <mss 1460,sackOK,timestamp 2056808 0,nop,wscale 0> (DF)
23:37:45.290907 > 192.168.1.1.4283 > 172.20.1.2.imap2: S
357305715:357305715(0)
win 32120 <mss 1460,sackOK,timestamp 2060926 0,nop,wscale 0> (DF)
23:37:45.370488 > 192.168.1.1.4294 > 172.20.1.2.imap2: S
360540033:360540033(0)
win 32120 <mss 1460,sackOK,timestamp 2060934 0,nop,wscale 0> (DF)
23:37:45.450410 > 192.168.1.1.4305 > 172.20.1.2.imap2: S
364959256:364959256(0)
win 32120 <mss 1460,sackOK,timestamp 2060942 0,nop,wscale 0> (DF)
.
.
.
```

Targeting

There is active targeting.

Techniques

From the timing, it looks to be an automated process – a burst of three with a pause and then a burst of three more to the same IP address. This scan went through the whole Class C address space looking for IMAP.

Intent

The intent was to map my subnet for any potential IMAP servers.

History

IMAP has known vulnerabilities. Since I was using a Check Point firewall at this site in SynDefender mode, every IP address showed up as having IMAP (response packets not shown here). This may have confused the instigator.

Severity

2

Resolution

I made sure there were no IMAP servers and double-checked the firewall rules.

4) RCMD Scan

```
23:37:02.198526 > 192.168.1.1.2461 > 172.20.1.2.login: S
325581924:325581924(0)
win 32120 <mss 1460,sackOK,timestamp 2056616 0,nop,wscale 0> (DF)
23:37:02.290556 > 192.168.1.1.2472 > 172.20.1.2.login: S
319543396:319543396(0)
win 32120 <mss 1460,sackOK,timestamp 2056626 0,nop,wscale 0> (DF)
23:37:02.370579 > 192.168.1.1.2483 > 172.20.1.2.login: S
315297417:315297417(0)
win 32120 <mss 1460,sackOK,timestamp 2056634 0,nop,wscale 0> (DF)
23:37:11.740227 > 192.168.1.1.3710 > 172.20.1.2.exec: S
325891805:325891805(0) w
in 32120 <mss 1460,sackOK,timestamp 2057571 0,nop,wscale 0> (DF)
23:37:11.819748 > 192.168.1.1.3721 > 172.20.1.2.exec: S
323866205:323866205(0) w
in 32120 <mss 1460,sackOK,timestamp 2057579 0,nop,wscale 0> (DF)
23:37:11.899774 > 192.168.1.1.3732 > 172.20.1.2.exec: S
331104906:331104906(0) w
in 32120 <mss 1460,sackOK,timestamp 2057587 0,nop,wscale 0> (DF)
23:37:16.060914 > 192.168.1.1.4275 > 172.20.1.2.shell: S
341695592:341695592(0)
win 32120 <mss 1460,sackOK,timestamp 2058003 0,nop,wscale 0> (DF)
23:37:16.140547 > 192.168.1.1.4286 > 172.20.1.2.shell: S
337484437:337484437(0)
win 32120 <mss 1460,sackOK,timestamp 2058011 0,nop,wscale 0> (DF)
23:37:16.234025 > 192.168.1.1.4297 > 172.20.1.2.shell: S
334568501:334568501(0)
win 32120 <mss 1460,sackOK,timestamp 2058020 0,nop,wscale 0> (DF)
.
.
.
```

Targeting
    There is active targeting.

Techniques
    From the timing, it looks to be an automated process looking for all of the r-commands on each host. I previously saw a potential NMAP scan on this subnet. After the hosts were found, this scan began.

Intent
    The intent was to map existing systems that may have the r-command ports open or in use.

History
    Known vulnerabilities in r-command utilities.

Severity
    3

Resolution

    This site does use UNIX systems. I verified the firewall rules. I double-checked each system to make sure no r-commands were allowed – especially from the outside.

5) FIN Scan

```
01:36:35.120109 > 192.168.1.1.52358 > 172.20.1.2.imap2: F 0:0(0) win
2048
01:36:35.220174 > 192.168.1.1.52359 > 172.20.1.2.imap2: F 0:0(0) win
2048
01:37:14.030110 > 192.168.1.1.52358 > 172.20.1.3.imap2: F 0:0(0) win
2048
01:37:14.170094 > 192.168.1.1.52359 > 172.20.1.3.imap2: F 0:0(0) win
2048
01:37:55.190110 > 192.168.1.1.52358 > 172.20.1.4.imap2: F 0:0(0) win
2048
01:37:55.320099 > 192.168.1.1.52359 > 172.20.1.4.imap2: F 0:0(0) win
2048
01:38:29.550113 > 192.168.1.1.52358 > 172.20.1.5.imap2: F 0:0(0) win
2048
01:38:29.660109 > 192.168.1.1.52359 > 172.20.1.5.imap2: F 0:0(0) win
2048
01:39:07.000128 > 192.168.1.1.52358 > 172.20.1.6.imap2: F 0:0(0) win
2048
01:39:07.140096 > 192.168.1.1.52359 > 172.20.1.6.imap2: F 0:0(0) win
2048
01:39:33.342581 > 192.168.1.1.52358 > 172.20.1.7.imap2: F 0:0(0) win
2048
01:40:00.240108 > 192.168.1.1.52358 > 172.20.1.9.imap2: F 0:0(0) win
2048
01:40:00.380112 > 192.168.1.1.52359 > 172.20.1.9.imap2: F 0:0(0) win
2048
01:40:43.210137 > 192.168.1.1.52358 > 172.20.1.10.imap2: F 0:0(0) win
2048
01:40:43.350096 > 192.168.1.1.52359 > 172.20.1.10.imap2: F 0:0(0) win
2048
```

Targeting
    There is active targeting.

Techniques
    From the timing, it looks to be an automated scan. This is a stealth FIN scan probably from NMAP. The destination port is IMAP, but I don't think this has anything to do with the mapping.

Intent
    The intent was to map my subnet with a stealth FIN scan – possibly to get past the firewall.

History
    Unknown.

Severity
    2

Resolution

    I added this to the list of source IPs to watch.

6) "not IP" – Ping Scan

```
00:11:53.626786 < arp who-has 192.168.1.1 tell 172.20.1.250
00:11:53.626869 > arp reply 192.168.1.1 (0:10:5a:c9:df:59) is-at
0:10:5a:c9:df:59 (8:0:2b:3d:25:7c)
00:11:53.627837 > arp who-has 172.20.1.2 tell 192.168.1.1
(0:10:5a:c9:df:59)
00:11:53.628066 > arp who-has 172.20.1.3 tell 192.168.1.1
(0:10:5a:c9:df:59)
00:11:53.628265 < arp reply 172.20.1.2 is-at 0:10:5a:9e:87:d7
(0:10:5a:c9:df:59)
00:11:53.628597 > arp who-has 172.20.1.4 tell 192.168.1.1
(0:10:5a:c9:df:59)
00:11:53.628643 < arp reply 172.20.1.3 is-at 0:10:5a:9e:87:d7
(0:10:5a:c9:df:59)
00:11:53.629045 > arp who-has 172.20.1.5 tell 192.168.1.1
(0:10:5a:c9:df:59)
00:11:53.629272 > arp who-has 172.20.1.6 tell 192.168.1.1
(0:10:5a:c9:df:59)
00:11:53.630189 < arp reply 172.20.1.4 is-at 0:10:5a:9e:87:d7
(0:10:5a:c9:df:59)
00:11:53.630439 < arp reply 172.20.1.5 is-at 0:10:5a:9e:87:d7
(0:10:5a:c9:df:59)
00:11:53.630598 < arp reply 172.20.1.6 is-at 0:10:5a:9e:87:d7
(0:10:5a:c9:df:59)
.
.
.
```

I had a very small network so I decided to change the default SHADOW filter to capture all traffic on the subnet. I saw this ping scan (via IP). I was curious what it looked like in the ARP protocol and the above is the result.

Targeting
    There is active targeting.

Techniques
    From the timing, it looks to be an automated process.

Intent
    The intent was to map my subnet with a ping scan.

History
    Unknown.

Severity
    2

Resolution

    I found that one of my fellow employees was using NMAP to scan this network for a vulnerability analysis for a customer. The customer was interested to know that this could be detected.

7) Port scan

```
00:11:55.745133 > 192.168.1.1.42223 > 172.20.1.2.400: FP 0:0(0) win
2048 urg 0
00:11:55.745371 > 192.168.1.1.42223 > 172.20.1.2.967: FP 0:0(0) win
2048 urg 0
00:11:55.764379 > 192.168.1.1.42223 > 172.20.1.2.425: FP 0:0(0) win
2048 urg 0
00:11:55.764611 > 192.168.1.1.42223 > 172.20.1.2.239: FP 0:0(0) win
2048 urg 0
00:11:55.764802 > 192.168.1.1.42223 > 172.20.1.2.2015: FP 0:0(0) win
2048 urg 0
00:11:55.764989 > 192.168.1.1.42223 > 172.20.1.2.675: FP 0:0(0) win
2048 urg 0
00:11:55.765174 > 192.168.1.1.42223 > 172.20.1.2.407: FP 0:0(0) win
2048 urg 0
00:11:55.765361 > 192.168.1.1.42223 > 172.20.1.2.9876: FP 0:0(0) win
2048 urg 0
00:11:55.765546 > 192.168.1.1.42223 > 172.20.1.2.651: FP 0:0(0) win
2048 urg 0
.
.
.
```

Targeting
    There is active targeting.

Techniques
    From the timing, it looks to be an automated process. This looks like NMAP. The source port stays the same. The destination port is somewhat random. The entire subnet was scanned in this manner. Also, many of the flags were set – FIN, PUSH, and URG.

Intent
    The intent was to map my subnet with a port scan on each IP address.

History
    NMAP is used quite often for this type of scan.

Severity
    3

Resolution

    I again added this IP address to my list of IPs to watch out for.

8) UDP Scan

```
00:23:50.536821 > 192.168.1.1.61749 > 172.20.1.251.604: udp 0
00:23:50.536821 > 192.168.1.1.61749 > 172.20.1.251.604: udp 0
00:23:50.537491 > 192.168.1.1.61749 > 172.20.1.251.431: udp 0
00:23:50.537491 > 192.168.1.1.61749 > 172.20.1.251.431: udp 0
00:23:50.538049 > 192.168.1.1.61749 > 172.20.1.251.214: udp 0
00:23:50.538049 > 192.168.1.1.61749 > 172.20.1.251.214: udp 0
00:23:50.538599 > 192.168.1.1.61749 > 172.20.1.251.1416: udp 0
00:23:50.538599 > 192.168.1.1.61749 > 172.20.1.251.1416: udp 0
.
.
.
```

Targeting
    There is active targeting.

Techniques
    From the timing, it looks to be an automated process. It is directed at a single host. Seems to be somewhat random port numbers, but no effort to hide source IP address.

Intent
    The intent was to scan this IP address for all open UDP ports.

History
    Unknown.

Severity
    1

Resolution

    I verified what UDP ports were in use. None were open on this system.

I ran out of detects on my customer networks (and got tired of lugging a PC around), so the remaining three detects are from the the GIAC site. I also didn't want to wait until the last day and prove Stephen correct about all of us procrastinators!

9) GIAC April 13 - pcAnywhere

```
Apr 11 21:59:17 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:3758 to 24.3.21.199 on unserved port 22
Apr 11 22:25:48 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:4007 to 24.3.21.199 on unserved port 22
Apr 11 22:26:18 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.21.225:4013 to 24.3.21.199 on unserved port 5632
```

Targeting

There is active targeting.

Techniques

Older versions of pcAnywhere used udp port 22 for its status. Newer versions use port 5632 and check the older port 22. This application - pcAnywhere - also will look for other pcAnywhere machines on the same subnet.

Intent

I think this is just the pcAnywhere application probing for other systems.

History

PcAnywhere is inherently dangerous.

Severity

2

Resolution

I would try and track down the source system.

10) GIAC April 11 – Trojan scan

```
Apr 6 19:44:05.798874 193.192.119.110,2435 -> 10.0.8.87,1243 PR tcp len
20 48 -S
Apr 6 19:44:05.799356 193.192.119.110,2436 -> 10.0.8.87,30100 PR tcp
len 20 48 -S
Apr 6 19:44:05.803185 193.192.119.110,2437 -> 10.0.8.87,54321 PR tcp
len 20 48 -S
Apr 6 19:44:05.829239 193.192.119.110,2438 -> 10.0.8.87,6670 PR tcp len
20 48 -S
Apr 6 19:44:05.829796 193.192.119.110,2439 -> 10.0.8.87,55555 PR tcp
len 20 48 -S
Apr 6 19:44:05.830331 193.192.119.110,2440 -> 10.0.8.87,1257 PR tcp len
20 48 -S
Apr 6 19:44:05.830749 193.192.119.110,2443 -> 10.0.8.87,6500 PR tcp len
20 48 -S
Apr 6 19:44:05.831771 193.192.119.110,2444 -> 10.0.8.87,21554 PR tcp
len 20 48 -S
Apr 6 19:44:05.835240 193.192.119.110,2446 -> 10.0.8.87,5742 PR tcp len
20 48 -S
Apr 6 19:44:05.835268 193.192.119.110,2447 -> 10.0.8.87,7307 PR tcp len
20 48 -S
Apr 6 19:44:05.870399 193.192.119.110,2448 -> 10.0.8.87,16969 PR tcp
len 20 48 -S
Apr 6 19:44:05.870428 193.192.119.110,2449 -> 10.0.8.87,1170 PR tcp len
20 48 -S
Apr 6 19:44:05.881925 193.192.119.110,2450 -> 10.0.8.87,20000 PR tcp
len 20 48 -S
Apr 6 19:44:05.893451 193.192.119.110,2451 -> 10.0.8.87,4950 PR tcp len
20 48 -S
Apr 6 19:44:05.905064 193.192.119.110,2452 -> 10.0.8.87,23456 PR tcp
len 20 48 -S
Apr 6 19:44:05.919541 193.192.119.110,2453 -> 10.0.8.87,1080 PR tcp len
20 48 -S
```

Targeting
    There is active targeting.

Techniques
    From the timing, it looks to be an automated process. This is a big scan for Trojans. I can't even find what some of them are. The Push and Reset flags are set.

Intent
    The intent was to scan this IP address for a list of known Trojans.

History
    Trojans are known to run on certain ports.

Severity
    3

Resolution

    I would verify that the ports are not in use and if they are what is using them.