Global Information Assurance Certification Paper

Bob Older
SANS2000 IDIC practical.

These traces were detected between April1, and April 24, 2000 using SHADOW against network 205.245.X.X

(1)RCP server scan.
This attempt to map RCP across our class c IP block is narrow targeting, they know we are a class c. Critical high (5) because this includes our firewall/proxy server, DNS, mail server and www server. In itself RPC exploits are also in the 4-5 range of lethality, but, this is only a scan so I would drop to a 2. I can give my firewall and mail servers 4-5 and I still cling to CERN (never been hacked) for my www, so that and the wwws system protection gives it a 4-5 also. Over all, very low threat. 1 to 2
It has caused me to increase snaplen so I can see more of the payloads. Of concern is the narrow targeting and the source being a pool at the local ISP.

```
22:36:35:089768 r.p.c.scann.58193 > my.net.2.111: udp 94 (DF) [ttl 1]
22:36:35:109768 r.p.c.scann.58193 > my.net.3.111: udp 94 (DF) [ttl 1]
22:36:35:119768 r.p.c.scann.58193 > my.net.4.111: udp 94 (DF) [ttl 1]
22:36:35:149768 r.p.c.scann.58193 > my.net.5.111: udp 94 (DF) [ttl 1]
22:36:35:169768 r.p.c.scann.58193 > my.net.6.111: udp 94 (DF) [ttl 1]
..........
```

(2) SNMP attempt
Looking for a rise from SNMP, first on my firewall/proxy server, where Port Sentry only gives one chance and should have immediately made the IP a deny all. Came back about 45 minutes later and tried my www server. Color me targeted?? This should be high in the area of criticality and lethality (firewall/proxy server, looking for maybe passwords). Neither of the targets should have snmp running at all (last time I looked) and both run PortSentry and a Tripwire look-a-like, so I would even this out to a draw for criticality.

```
/usr/local/logger/site-loc/Apr11
16:44:38.314637 net.manager.2200 > my.fw.snmp: GetNextRequest(9)[|snmp]
17:32:06.574637 net.manager.2200 > my.www.snmp: GetNextRequest(9)[|snmp]
```

(3) port scan (blatant and audatious)
Maybe a later version of nmap to handle random sequence numbers. Three thousand or so SYNs to my fire wall in a couple of minutes pins down the targeting question.
High port numbers so maybe they have already found out that nearly all of the lower ports are out of service. Criticality is high when it's our firewall (5), severity is low for a port scan (2), system security is high, so this is a 1 or 2 severity.

```
16:20:44.276017 scan.isp.pool.6210 > my.fw.20261:
S 2501879446:2501879446(0) win 512
16:20:44.286017 scan.isp.pool.6211 > my.fw.20445:
S 3331318158:3331318158(0) win 512
16:20:44.286017 scan.isp.pool.6212 > my.fw.20973:
S 2134665597:2134665597(0) win 512
16:20:44.286017 scan.isp.pool.6214 > my.fw.20744:
S 2077628246:2077628246(0) win 512
..................
16:20:52.766017 scan.isp.pool.13334 > my.fw.20494:
S 1168059759:1168059759(0) win 512
16:20:52.766017 scan.isp.pool.13335 > my.fw.20979:
S 3089608399:3089608399(0) win 512
16:20:52.926017 scan.isp.pool.13336 > my.fw.20038:
S 4136320540:4136320540(0) win 512
16:20:52.926017 scan.isp.pool.13337 > my.fw.20980:
S 1485070582:1485070582(0) win 512
```

(4) DNS attack (sure hope I get credit for working through this false positive)
I was sure that I had a hot one here. Still have not extended snaplen, so I couldn't see the payload. These have numerous anomalies, repeating src ports, 3 SYN,

followed by 3 RESETS, then 3 more RESETS *with* ACKs to unrecorded sequence #s, repeating initial seq #s and very quick.! Couldn't see what they were doing, but,
this looked so juicy I failed to go back and look for more activity, just added it to the file of traces for the IDIC practical.

```
/usr/local/logger/site-loc/Apr18
10:19:43.036017 prober.isp.2300 > my.place.domain:
S 782526528:782526592(64) win 2048
10:19:43.036017 prober.isp.2301 > my.place.domain:
S 2114352503:2114352567(64) win 2048
10:19:43.036017 prober.isp.2302 > my.place.domain:
S 456943282:456943346(64) win 2048
10:19:43.126017 prober.isp.2302 > my.place.domain:
R 456943283:456943283(0) win 0
10:19:43.126017 prober.isp.2300 > my.place.domain:
R 782526529:782526529(0) win 0
10:19:43.126017 prober.isp.2301 > my.place.domain:
R 2114352504:2114352504(0) win 0
10:19:43.136017 prober.isp.2302 > my.place.domain:
R 456943283:456943283(0) ack 2250722881 win 2048
10:19:43.136017 prober.isp.2300 > my.place.domain:
R 782526529:782526529(0) ack
```

Then I made my daily trip to GIAC and read the analysis by Howard Kash on Type0 (Class 0) DNS and decided to look at this one more. Found pretty much the same
pattern he reported. SYNs to port 33434, 64 bytes, etc. Like Howard, I still don't like it, but it seems harmless.

```
10:01:11.910924 prober.isp.domain > my.place.33434:
2709 FormErr [0q] 0/0/0 (36) [ttl 1]
10:01:12.990924 prober.isp.domain > my.place.33434:
2710 FormErr [0q] 0/0/0 (36) [ttl 1]
10:45:12.500924 prober.isp.domain > my.place.domain: 2875*- 1/0/0 (66)
10:45:13.430924 prober.isp.domain > my.place.domain: 2879*- 1/0/0 (66)
```

(5) NetBus
NetBus Pro probing for trojans. It's my fire wall and Web server, so it's targeted. Fire wall is high criticality(5), NetBus is high criticality, but, since my firewall is UNIX,
no vulnerability. Severity -1

```
/usr/local/logger/site-loc/Apr11
16:38:52.450924 out.side.71.22.2123 > my.f1.20034: SF 297853618:297853618(0)
16:38:52.460924 out.side.71.22.2124 > my.f1.20034: SF 2483094037:2483094037(0)
16:38:52.510924 out.side.71.22.2125 > my.www.20034: SF 297853619:297853619(0)
16:38:52.460924 out.side.71.22.2126 > my.www.20034: SF 2483094038:2483094038(0)
```

(6) Low tech scan
Was rumaging thru firewall portsentry logs to compare to some of SHADOW's output and ran across this. It happened pretty fast in terms of portsentry logs, so was
easy to spot. Did not have SHADOW or tcpdump running, so I don't know how this would look in a tcpdump. We were targeted. It's a critical (5) anytime
someone scans the firewall. It's lethal (4) cause I can't see from this what it was that he was sending to the ports and he knows the ports that offer services. I have
good defenses (4-5) with only a few ports open and portsentry running. This one still comes out a plus in severity. (3-4)

```
955757508 - 04/01/2000 20:11:48 Host: d078.cconnect.net/205.244.106.78
Port: 21 TCP Blocked
955757508 - 04/01/2000 20:15:11 Host: d084.cconnect.net/205.244.106.84
Port: 23 TCP Blocked
955757508 - 04/01/2000 20:18:43 Host: d014.cconnect.net/205.244.106.14
Port: 53 TCP Blocked
955757508 - 04/01/2000 20:20:37 Host: d212.cconnect.net/205.244.106.212
Port: 111 TCP Blocked
955757508 - 04/01/2000 20:22:04 Host: d003.cconnect.net/205.244.106.03
```

```
Port: 143 TCP Blocked
955757508 - 04/01/2000 20:26:29 Host: e178.cconnect.net/205.244.107.178
Port: 512 TCP Blocked
955757508 - 04/01/2000 20:30:55 Host: d210.cconnect.net/205.244.106.210
Port: 513 TCP Blocked
```

(7)BackOrifice
This came across in the wee hours of the morning, did not scan the whole class c, but bracketed our major servers. Targeted , but all are UNIX boxes, so should no be vulnerable to backorifice. Criticality high, lethality is 1. System defences are good, so I consider severity to be 0 or less.

```
/usr/local/logger/site-loc/Apr13
02:24:33:089518 find.trojans.31284 > my.place.unused.31337: udp 21 (DF)
02:24:33:109518 find.trojans.31284 > my.place.unused.31337: udp 21 (DF)
02:24:33:239518 find.trojans.31284 > my.place.fw.31337: udp 21 (DF)
02:24:33:449518 find.trojans.31284 > my.place.fw.31337: udp 21 (DF)
02:24:33:719518 find.trojans.31284 > my.place.www.31337: udp 21 (DF)
02:24:34:149518 find.trojans.31284 > my.place.www.31337: udp 21 (DF)
02:24:34:209518 find.trojans.31284 > my.place.dns.31337: udp 21 (DF)
02:24:34:379518 find.trojans.31284 > my.place.dns.31337: udp 21 (DF)
02:24:34:549518 find.trojans.31284 > my.place.unused.31337: udp 21 (DF)
02:24:34:809518 find.trojans.31284 > my.place.unused.31337: udp 21 (DF)
02:24:34:989518 find.trojans.31284 > my.place.unused.31337: udp 21 (DF)
02:24:35:029518 find.trojans.31284 > my.place.unused.31337: udp 21 (DF)
```

(8) Frags ICMP with a fragmented packet. SHADOW showed no other fragments following this packet. Same source follows with udp packets to RCP and Syslog ports, with a packet size of 5!! Trying to overwrite the stack? All three came from the same source and look like they are trying to get information or Dos. Criticality is 5, lethality 3. System defense is 5 and network is not much, maybe a .25 for my ISPs router. This one is a 4 and should be investigated quickly.

```
13:25:51.674766 frager.net > fw1.proxy: icmp: echo request (frag 15461:1480@0+)
13:25:51.794766 frager.net.1132 > fw1.proxy.111: udp 5
13:25:51.844766 frager.net.1134 > fw1.proxy.514: udp 5
```

(9) HTTP SNMP probe
Just poking about to see if what comes back? These fast scans hit our DNS server on 80 and 161, then a couple of pings. At any rate no one should be trying to connect to my DNS on either of these ports. Criticality of 5 for DNS but 1 for lethality because ports are closed. Our dirty side boxes are very well protected and rate at least a 5, so I'll give this a 1 for severity.

```
01:07:00.492856 prob.net.6.200.60805 > d.n.s.box.80: . ack 0 win 3072
01:07:00.492856 d.n.s.box.80 > prob.net.6.200.60805: R 0:0(0) win 0
01:07:00.582856 prob.net.6.200.1114 > d.n.s.box.161:
S 1264694000:1264694000(0) win 512
01:07:00.582856 d.n.s.box.161 > prob.net.6.200.1114: R 0:0(0)
ack 1264694001 win 0
01:07:31.592856 prob.net.6.200 > d.n.s.box: icmp: echo request
01:09:31.592856 prob.net.6.200 > d.n.s.box: icmp: echo request
```

(10) SYN scan
Fast, quasi random SYN scan of high and low tcp ports. This is targeted against my proxy server so it is a criticality 5, scanning is 2 for lethal. There were about 30 hits in the scan. Very limited ports are open on the FW and port sentry should have put this IP into deny on the second hit. I give my system defense a 5 , so this is a 1 or 2 for severity.

```
18:25:49.914766 syn.scanner.5756 > fw.proxy.1: S 4390:4390(0) win 512
18:25:49.914766 syn.scanner.5756 > fw.proxy.1025: S 4391:4391(0) win 512
.............................
18:25:49.924766 syn.scanner.5756 > fw.proxy.1080: S 4393:4393(0) win 512
18:25:49.944766 syn.scanner.5756 > fw.proxy.111: S 4397:4397(0) win 512
18:25:49.954766 syn.scanner.5756 > fw.proxy.103: S 4399:4399(0) win 512
```

```
.............................
18:25:49.974766 syn.scanner.5756 > fw.proxy.138: S 4406:4406(0) win 512
18:25:49.974766 syn.scanner.5756 > fw.proxy.139: S 4407:4407(0) win 512
18:25:50.004766 syn.scanner.5756 > fw.proxy.143: S 4408:4408(0)win 512
18:25:50.904766 syn.scanner.5756 > fw.proxy.23: S 4417:4417(0) win 512
.............................
18:25:50.914766 syn.scanner.5756 > fw.proxy.4444: S 4421:4421(0) win 512
18:25:50.914766 syn.scanner.5756 > fw.proxy.512: S 4422:4422(0) win 512
18:25:50.944766 syn.scanner.5756 > fw.proxy.530: S 4428:4428(0) win 512
.............................
18:25:50.954766 syn.scanner.5756 > fw.proxy.6667: S 4431:4431(0) win 512
```