Global Information Assurance Certification Paper

*** Northcutt, 70 *

Michael Whitson

All traces are from a Shadow system located in the DMZ. The IP's are obscured to protect the bad guys and of course our network.

Trace 1

```
18:11:27.604944 victim.COM > 10.0.1.0: icmp: echo request
18:11:27.604947 victim.COM > 10.0.2.0: icmp: echo request
18:11:27.604962 victim.COM > 10.0.1.255: icmp: echo request
18:11:27.604965 victim.COM > 10.0.0.255: icmp: echo request
18:11:27.605924 victim.COM > 10.0.2.255: icmp: echo request
18:11:27.619118 victim.COM > 10.0.3.255: icmp: echo request
18:11:27.629025 victim.COM > 10.0.3.0: icmp: echo request
18:11:27.633366 victim.COM > 10.0.4.0: icmp: echo request
18:11:27.635618 victim.COM > 10.0.4.255: icmp: echo request
[snip...]
```

Targeting: Yes
Technique: Smurf attack using ICMP echo to the broadcast address. Has to be a script, nobody can type that fast.

Intent: DOS or network mapping. Attempting to gather OS system information.
If the source is spoofed then the intent is to send all the echos back as a DOS to the victim. Regardless whether this is a DOS directed at the victim or a DOS directed at my network, the bad guy is network mapping.

Trace 2

```
03:00:07.962453 bad.guy.com > 10.0.156.34: icmp: time exceeded in-transit
03:00:31.586285 bad.guy.com > 11.0.43.196: icmp: time exceeded in-transit
03:00:35.639363 bad.guy.com > 10.0.199.107: icmp: time exceeded in-transit
03:00:38.053469 bad.guy.com > 10.0.49.107: icmp: time exceeded in-transit
03:01:06.940588 bad.guy.com > 10.0.241.87: icmp: time exceeded in-transit
03:01:18.406319 bad.guy.com > 11.0.161.74: icmp: time exceeded in-transit
03:02:28.811393 bad.guy.com > 10.0.198.205: icmp: time exceeded in-transit
03:04:05.962538 bad.guy.com > 10.0.251.2: icmp: time exceeded in-transit
03:04:29.460634 bad.guy.com > 10.0.220.32: icmp: time exceeded in-transit
[snip…]
```

Targeting: Yes
Technique: Script; As indicated by the time offset and the fact they were not targeting a specific system. There were no repeats on destination IP's.

Intent: Network mapping using ICMP or a DOS. "time exceeded in-transit" is another indication of a crafted packet. It is an attempt to force the destination to respond regardless of the return hops. It is also possible the packet is an attempt at a buffer overflow.

Trace 3

```
20:43:28.852597 real.bad.guy.com.1029 > 10.0.1.0.31337: udp 18
20:43:28.878855 real.bad.guy.com.1029 > 10.0.2.0.31337: udp 18
20:43:28.893558 real.bad.guy.com.1029 > 10.0.3.0.31337: udp 18
20:43:28.948124 real.bad.guy.com.1029 > 10.0.4.0.31337: udp 18
20:43:28.964402 real.bad.guy.com.1029 > 10.0.5.0.31337: udp 18
20:43:28.985077 real.bad.guy.com.1029 > 10.0.6.0.31337: udp 18
20:43:29.008443 real.bad.guy.com.1029 > 10.0.7.0.31337: udp 18
20:43:29.023662 real.bad.guy.com.1029 > 10.0.8.0.31337: udp 18
[snip..]
```

Targeting: Yes
Technique: Script; Very tight time stamp. Identical source, destination port (crafted packet) and the fact they walked the network.

Intent: Network mapping and/or probing for Back Orifice well known port 31337UDP.

Trace 4

```
01:03:31.209981 bad.guy.com > 11.0.76.134: icmp: host 13.0.251.7 unreachable
01:03:33.373299 bad.guy.com > 11.0.183.122: icmp: host 13.0.251.7 unreachable
01:03:37.608698 bad.guy.com > 10.0.226.183: icmp: host 13.0.251.7 unreachable
01:03:39.213816 bad.guy.com > 10.0.52.194: icmp: host 13.0.251.7 unreachable
01:03:41.914566 bad.guy.com > 10.0.28.247: icmp: host 13.0.251.7 unreachable
01:03:44.410353 bad.guy.com > 10.0.172.178: icmp: host 13.0.251.7 unreachable
01:03:46.072672 bad.guy.com > 11.0.37.64: icmp: host 13.0.251.7 unreachable
01:03:28.395904 bad.guy.com > 10.0.188.187: icmp: host 13.0.251.7 unreachable
[snip…]
```

Targeting: Yes
Technique: Script; Very tight time stamp. There were no repeats on IP's

Intent: Appears to be a ICMP Man in the middle DOS. The packet was crafted to fake the source address, the recipient of the pings my network responds to the victim (.251.7) with thousands of echo replies.

Trace 5

```
15:15:24.501984 bad.guy.com.56334 > 10.0.248.121.27953: R 0:0(0) ack 1668490570
win 0 [tos 0x8]
15:15:56.862132 bad.guy.com.63338 > 11.0.141.49.17118: R 0:0(0) ack 1202012792
win 0 [tos 0x8]
15:15:59.197126 bad.guy.com.63973 > 10.0.5.123.7553: R 0:0(0) ack 500988496 win 0
[tos 0x8]
15:15:59.668899 bad.guy.com.7959 > 10.0.219.74.61412: R 0:0(0) ack 2691813400 win
0 [tos 0x8]
15:16:00.202883 bad.guy.com.33647 > 10.0.107.16.16788: R 0:0(0) ack 2988721747
win 0 [tos 0x8]
```

```
15:16:01.235435 bad.guy.com.6650 > 10.0.209.7.50385: R 0:0(0) ack 3839255156 win
0 [tos 0x8]
[snip…]
```

Targeting: Yes
Technique: Script; High order port scan using Reset and ACK. The TOS 0x8 indicates this is an ICMP Echo packet.

Intent: Information gathering scan. If the destination host is unreachable and there is a poorly configured router. The router will return a destination unreachable. This allows the bad guy to determine what host/networks are alive, ie. *inverse* network mapping.

Trace 6

```
03:29:07.201667 bad.guy.com.3503 > 11.0.111.1.12345: S 5394851:5394851(0) win
8192 <mss 1460> (DF)
03:29:07.202989 bad.guy.com.3504 > 11.0.111.2.12345: S 5394859:5394859(0) win
8192 <mss 1460> (DF)
03:29:07.599746 bad.guy.com.3505 > 11.0.111.3.12345: S 5394868:5394868(0) win
8192 <mss 1460> (DF)
03:29:07.601079 bad.guy.com.3506 > 11.0.111.4.12345: S 5394877:5394877(0) win
8192 <mss 1460> (DF)
03:29:07.601970 bad.guy.com.3507 > 11.0.111.5.12345: S 5394886:5394886(0) win
8192 <mss 1460> (DF)
03:29:07.603363 bad.guy.com.3508 > 11.0.111.6.12345: S 5394895:5394895(0) win
8192 <mss 1460> (DF)
03:29:07.603790 bad.guy.com.3509 > 11.0.111.7.12345: S 5394904:5394904(0) win
8192 <mss 1460> (DF)
[snip…]
```

Targeting: Yes
Technique: Script; Very tight time stamp. Source port increments by 1, same destination port, scan using SYN not waiting on an acknowledgement.

Intent: At first glance I thought it was a SYN flood attack, because I initially just looked at the total frames. After breaking the session out I realized it was a network mapping script. Could be scanning for Trojan GabanBus, NetBus on Port 12345.

Trace 7

```
05:00:08.797154 bad.guy.com.137 > 11.0.240.16.137: udp 50
05:00:10.258720 bad.guy.com.137 > 11.0.240.16.137: udp 50
05:00:11.543462 bad.guy.com.137 > 11.0.240.16.137: udp 50
05:00:19.077541 bad.guy.com.137 > 11.0.240.17.137: udp 50
05:00:20.788179 bad.guy.com.137 > 11.0.240.17.137: udp 50
05:00:22.066490 bad.guy.com.137 > 11.0.240.17.137: udp 50
05:00:30.125840 bad.guy.com.137 > 11.0.240.18.137: udp 50
05:00:31.282795 bad.guy.com.137 > 11.0.240.18.137: udp 50
05:00:32.599139 bad.guy.com.137 > 11.0.240.18.137: udp 50
05:00:40.523803 bad.guy.com.137 > 11.0.240.19.137: udp 50
05:00:41.804436 bad.guy.com.137 > 11.0.240.19.137: udp 50
```

```
05:00:43.162177 bad.guy.com.137 > 11.0.240.19.137: udp 50
05:00:51.201630 bad.guy.com.137 > 11.0.240.20.137: udp 50
```

Targeting: Yes
Technique: Script; Tight time stamp. Source and destination ports do not increment. Possibly using tools provided by the NTRK.

Intent: UDP/137 is Netbios name request port scan. Information gathering scan, targeting Windows systems. Additional benefit for the bad guy, mapping the subnet.

Trace 8

```
13:03:41.747031 bad.guy.com.3435 > 11.0.46.255.143: S 823573491:823573491(0) win
32120  (DF)
13:03:41.747466 bad.guy.com.3436 > 11.0.46.254.143: S 813279596:813279596(0) win
32120  (DF)
13:03:41.748026 bad.guy.com.3437 > 11.0.46.253.143: S 821903209:821903209(0) win
32120  (DF)
13:03:41.748034 bad.guy.com.3438 > 11.0.46.252.143: S 821735312:821735312(0) win
32120  (DF)
13:03:41.748046 bad.guy.com.3439 > 11.0.46.251.143: S 814718829:814718829(0) win
32120  (DF)
13:03:41.748049 bad.guy.com.3440 > 11.0.46.250.143: S 818769977:818769977(0) win
32120  (DF)
13:03:41.748064 bad.guy.com.3441 > 11.0.46.249.143: S 811327015:811327015(0) win
32120  (DF)
13:03:41.748067 bad.guy.com.3442 > 11.0.46.248.143: S 818697783:818697783(0) win
32120  (DF)
13:03:41.748073 bad.guy.com.3443 > 11.0.46.247.143: S 823873246:823873246(0) win
32120  (DF)
[snip…]
```

Targeting: Yes
Technique: Script; Very tight time stamp. Source port increments by 1, destination port is constant. The loan SYS is a half open scan because a SYN/ACK is not returned to the originating host.

Intent: TCP/143 is the IMAP port, SYN Flood. The originator has spoofed the source of a nonexistent system. The return SYN/ACK is sent to the spoofed address. Now the destinations (my systems) are now in a SYN/RECV state. My systems are now committed to establishing a connection. The Bad Guy could exploit IMAP vulnerabilities.

Trace 9

```
20:38:47.050283 bad.guy.com.57932 > 11.0.0.255.80: . ack 0 win 1024
20:38:47.050291 bad.guy.com.57932 > 11.0.1.255.80: . ack 0 win 1024
20:38:47.052772 bad.guy.com.57932 > 11.0.2.255.80: . ack 0 win 1024
20:38:47.053498 bad.guy.com.57932 > 11.0.3.255.80: . ack 0 win 1024
20:38:47.053833 bad.guy.com.57932 > 11.0.4.255.80: . ack 0 win 1024
20:38:47.055802 bad.guy.com.57932 > 11.0.5.255.80: . ack 0 win 1024
```

```
20:38:47.057831 bad.guy.com.57932 > 11.0.6.255.80: . ack 0 win 1024
20:38:47.057846 bad.guy.com.57932 > 11.0.7.255.80: . ack 0 win 1024
20:38:47.079566 bad.guy.com.57932 > 11.0.9.255.80: . ack 0 win 1024
20:38:47.080023 bad.guy.com.57932 > 11.0.12.255.80: . ack 0 win 1024
20:38:47.080612 bad.guy.com.57932 > 11.0.13.255.80: . ack 0 win 1024
20:38:47.080619 bad.guy.com.57932 > 11.0.10.255.80: . ack 0 win 1024
20:38:47.082266 bad.guy.com.57932 > 11.0.8.255.80: . ack 0 win 1024
20:38:47.097504 bad.guy.com.57932 > 11.0.14.255.80: . ack 0 win 1024
[snip…]
```

Targeting: Yes
Technique: Script; Very tight time stamp. Source and destination port are constant but not the destination address..

Intent: Scanning for web servers port 80. By default many OS install Web Servers during the initial system installation. System owners either are unaware or overlook this application. The ACK is an indication of TCP/IP Stack Fingerprinting. The bad guy is scanning the Broadcast address of all the networks.

Trace 10

```
08:56:46.330769 bad.guy.com.13356 > 13.0.68.19.111: S 2105675008:2105675008 (0)
win 512
08:56:46.330929 bad.guy.com.13329 > 13.0.68.10.111: S 1283255785:1283255785 (0)
win 512
08:56:46.331419 bad.guy.com.13376 > 13.0.68.21.111: S 1093368475:1093368475 (0)
win 512
08:56:46.331747 bad.guy.com.13051 > 13.0.68.1.111: S 3429678225:3429678225 (0)
win 512
08:56:46.332607 bad.guy.com.13332 > 13.0.68.13.111: S 4149824266:4149824266 (0)
win 512
08:56:46.333058 bad.guy.com.13378 > 13.0.68.23.111: S 3619956806:3619956806 (0)
win 512
08:56:46.333222 bad.guy.com.13379 > 13.0.68.24.111: S 21823303:21823303 (0) win
512
08:56:46.333386 bad.guy.com.13190 > 13.0.68.5.111: S 2733884631:2733884631 (0)
win 512
[snip....]
```

Targeting: Yes
Technique: Script; Very tight time stamp. Slowly incrementing source port, destination port is constant.

Intent: TCP/UDP/111 is the SunRPC port. Information gathering, targeting UNIX system specifically looking for vulnerabilities on port 111. Additional benefit for the bad guy, mapping the subnet.
.