Global Information Assurance Certification Paper

***** Northcutt, 70**

Trace #1: Slow distributed broadcast ICMP scan

Packet filter rules on DMZ router dropped ICMP echo-request packets before reaching internal workstations. A single echo request from a number of ISP's over the course of several days may indicate a low level mapping of a large address space with the target address here (masked to be 256.256.201.255) being one of many target networks being mapped. The mechanism appears to be use of the directed boradcast address intending that the devices on the target network will reply to provide further target detail.

As no users were using the network at the early morning/late night hours of some of the scan, there is no appearance that web browsing or similar client activity was actively provoking all the probes. Also, the slow and distributed-source, repetitive scan suggests that the effort is intentional and coordinated.

```
Mar 22 05:44:34: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 195.54.67.70 -> 207.86.201.255 (8/0), 1 packet
Mar 22 14:36:35: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 159.226.40.136 -> 207.86.201.255 (8/0), 1 packet

Mar 23 11:21:39: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.91.164.44 -> 207.86.201.255 (8/0), 1 packet
Mar 23 15:53:19: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 151.21.74.122 -> 207.86.201.255 (8/0), 1 packet
Mar 23 18:57:33: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.78.157.37 -> 207.86.201.255 (8/0), 1 packet
Mar 23 19:39:16: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 209.202.45.143 -> 207.86.201.255 (8/0), 1 packet
Mar 23 19:44:48: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 209.202.45.143 -> 207.86.201.255 (8/0), 1 packet
Mar 23 23:14:56: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 38.27.152.5 -> 207.86.201.255 (8/0), 1 packet

Mar 24 07:15:12: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.216.233.107 -> 207.86.201.255 (8/0), 1 packet

Mar 25 02:04:28: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.216.184.16 -> 207.86.201.255 (8/0), 1 packet
Mar 25 07:20:05: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 151.21.78.145 -> 207.86.201.255 (8/0), 1 packet
Mar 25 07:40:42: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 151.21.78.145 -> 207.86.201.255 (8/0), 1 packet
Mar 25 09:18:45: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 151.20.107.40 -> 207.86.201.255 (8/0), 1 packet
Mar 25 20:30:27: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 213.1.136.245 -> 207.86.201.255 (8/0), 1 packet
Mar 25 23:36:09: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.216.238.190 -> 207.86.201.255 (8/0), 1 packet

Mar 26 15:36:59: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.139.160.90 -> 207.86.201.255 (8/0), 1 packet
Mar 26 23:27:36: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.78.157.37 -> 207.86.201.255 (8/0), 1 packet

Mar 27 02:01:30: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.216.169.106 -> 256.256.201.255 (8/0), 1 packet
Mar 27 03:55:18: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 210.104.180.1 -> 256.256.201.255 (8/0), 1 packet
Mar 27 04:00:41: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 210.104.180.1 -> 256.256.201.255 (8/0), 1 packet
```

Trace #2: Targeted host scan (524/tcp)

This late-night scan of two subnets of hosts in the class-C address range has distinct markings of being very specifically targeted. The scanner appears to have gathered intelligence through DNS lookups as demonstrated by scans targeted at hosts in the .16-.31 range and .192-.255 range. The packets are crafted programmatically as indicated by a single tcp packet sent to each host rather than the normal IP stack behavior of several retries before halting the connection attempt.

No prior or following scans have been noted from this address space in the prior or following days around the event. A partial log follows with targeted addresses (256.256.201.x) masked.

```
*Mar 19 00:06:55: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(40286) -> 256.256.201.192(524), 1 packet
*Mar 19 00:07:10: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(41030) -> 256.256.201.192(524), 1 packet
*Mar 19 00:07:20: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(42099) -> 256.256.201.192(524), 1 packet
*Mar 19 00:07:31: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(39359) -> 256.256.201.193(524), 1 packet
*Mar 19 00:07:45: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(41129) -> 256.256.201.193(524), 1 packet
*Mar 19 00:07:56: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(42249) -> 256.256.201.193(524), 1 packet
*Mar 19 00:08:06: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(41106) -> 256.256.201.194(524), 1 packet
*Mar 19 00:08:21: %SEC-6-IPACCESSLOGP: list 100 denied tcp 209.44.16.110(39267) -> 256.256.201.194(524), 1 packet
```

Trace #3: Targeted host scan (137/udp)

A scan from xxxxxxxx made apparently searching for Windows machines on the network. The scan sends only two packets attempting to intiate a connection and moves rapidly through the hosts, pausing about 12 seconds between each host before continuing. The scan for hosts .192-.254 is completed in under one hour.

A partial trace is included below with IP target IP addresses (256.256.201.x) masked.

```
Mar 27 12:57:15: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.242(137), 2 packets
Mar 27 12:57:27: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.243(137), 2 packets
Mar 27 12:57:40: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.251(137), 1 packet
Mar 27 12:57:52: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.244(137), 2 packets
Mar 27 12:57:55: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.246(137), 2 packets
Mar 27 12:58:16: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.248(137), 2 packets
Mar 27 12:58:27: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.249(137), 2 packets
Mar 27 13:01:44: %SEC-6-IPACCESSLOGP: list 152 denied udp 200.200.200.120(137) -> 256.256.201.250(137), 2 packets
```

Trace #4: Targeted high-port Trojan attempt (1497/udp)

This scan is looking for an unknown service on a proxy server at the .17 address. Since the proxy act makes normal web requests, it is uncertain whether the attacker is aware that it is a firewall being attacked. The logs are generated from a packet-filtering router before the firewall preventing non-ESTablished traffic from outside the network to the firewall address. While the attacker is attempting to use well-known port 80 (HTTP) to perhaps bypass security filters, this was still trapped at the outer router rather than the host.

The target application (1497/tcp) may be a new trojan port or an obscure application.

```
Mar 28 08:47:41: %SEC-6-IPACCESSLOGP: list 100 denied tcp 10.2.7.240(80) -> 256.256.201.17(1497), 6 packets
Mar 28 08:48:01: %SEC-6-IPACCESSLOGP: list 100 denied tcp 10.2.7.240(80) -> 256.256.201.17(1497), 1 packet
Mar 28 08:53:59: %SEC-6-IPACCESSLOGP: list 100 denied tcp 10.2.7.240(80) -> 256.256.201.17(1497), 2 packets
Mar 28 08:58:59: %SEC-6-IPACCESSLOGP: list 100 denied tcp 10.2.7.240(80) -> 256.256.201.17(1497), 3 packets
Mar 28 09:03:59: %SEC-6-IPACCESSLOGP: list 100 denied tcp 10.2.7.240(80) -> 256.256.201.17(1497), 2 packets
Mar 28 09:05:27: %SEC-6-IPACCESSLOGP: list 100 denied tcp 10.2.7.240(80) -> 256.256.201.17(1497), 1 packet
```

Trace #5: Attempted access to intranet web server

An intranet server was set up at the target site in the DMZ (a bad design) and the name placed in the external DNS for simplicity of administration (poor choice). The attacker attempted to repeatedly access the server using some type of scanning tool. Of interest in this connection attempt is the use twice of a given high-port number for the originating port, separated by several minutes. Also, each return visit using a new source port is delayed by a period of time. It appears that the attacker has a very long time-out (six minutes) for their program and that they may be scanning a programatic list of targets. Scanning was abandoned in a few hours.

24.92.0.0/14 is in an address block owned by a large cable company. Attacker is probably using a cable modem host.

```
Apr  3 10:10:52: %SEC-6-IPACCESSLOGP: list 100 denied tcp 24.94.117.31(61017) -> 256.256.201.23(80), 1 packet
Apr  3 10:11:13: %SEC-6-IPACCESSLOGP: list 100 denied tcp 24.94.117.31(61019) -> 256.256.201.23(80), 1 packet
Apr  3 10:16:15: %SEC-6-IPACCESSLOGP: list 100 denied tcp 24.94.117.31(61017) -> 256.256.201.23(80), 2 packets
Apr  3 10:18:33: %SEC-6-IPACCESSLOGP: list 100 denied tcp 24.94.117.31(61250) -> 256.256.201.23(80), 1 packet
Apr  3 10:24:15: %SEC-6-IPACCESSLOGP: list 100 denied tcp 24.94.117.31(61250) -> 256.256.201.23(80), 1 packet
Apr  3 11:31:54: %SEC-6-IPACCESSLOGP: list 100 denied tcp 24.94.117.31(61147) -> 256.256.201.23(80), 1 packet
Apr  3 11:37:18: %SEC-6-IPACCESSLOGP: list 100 denied tcp 24.94.117.31(61147) -> 256.256.201.23(80), 2 packets
```

Trace #6: One-shot attempt

This is a very unusual entry found on two routers (inner and outer packet-screening routers). The source host has be noticed in the logs as a web site that pings the source host (a proxy firewall on a different address) when visited. As such, this is not significant traffic; however, this single connect attempt to an unusual high port at an address where no host has been located in two years was spotted. It is possbile that other attempts (slow scan) have been made and not discovered in logs.

256.256.201.18 is the inner router interface. There is no host at .249. The attacker is sourced from a ISP in Massachusetts (216.243.0.0/18).

```
(Inner router) Apr  4 22:08:52: %SEC-6-IPACCESSLOGP: list fmDMZ denied tcp 216.243.8.224(44370) ->
256.256.201.249(2315), 1 packet
(Outer router) Apr  4 22:08:52: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 256.256.201.18 -> 216.243.8.224 (3/13), 1
packet
```

Trace #7: Targeted host scan (137/udp)

A scan from xxxxxxxx made apparently searching for Windows machines on the network. This scan differs both in source address and success of having the udp packets cross the Internet without being lost. I appears that the same approach is taken (two packets on each attempt), but about one third of the packets are being lost before being blocked and logged at the outer router. The scan moves very rapidly through the hosts, pausing only five seconds between each host before continuing. The scan for hosts .2-.254 is completed in twenty-six minutes.

A partial trace is included below.

```
Apr  6 09:50:32: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.2(137), 1 packet
Apr  6 09:50:38: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.3(137), 1 packet
Apr  6 09:50:42: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.4(137), 1 packet
Apr  6 09:50:45: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.5(137), 1 packet
```

```
Apr  6 09:50:50: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.6(137), 1 packet
Apr  6 09:50:55: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.7(137), 1 packet
Apr  6 09:50:59: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.8(137), 1 packet
Apr  6 09:51:04: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.2(137), 2 packets
Apr  6 09:51:10: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.3(137), 1 packet
Apr  6 09:51:15: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.4(137), 1 packet
Apr  6 09:51:18: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.5(137), 2 packets
Apr  6 09:51:24: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.7(137), 2 packets
Apr  6 09:51:31: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.8(137), 2 packets
Apr  6 09:51:37: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.9(137), 1 packet
```

Trace #8: Attempted access to Internet web server

An Internet web server with a single page was set up at the target site in the DMZ. The attacker(s) attempted to repeatedly access the server using well known Windows attacks against 137/udp. Several interesting elements were identified: the use of fake addresses (172.24.33.144) to confuse tracing the attack, the use of several different attack source hosts, and the use of an unusual low source port (perhaps a mistake in the use of a Unix attacking source host).

```
Apr  6 09:52:58: %SEC-6-IPACCESSLOGP: list 152 denied udp 209.183.128.200(137) -> 256.256.201.27(137), 2 packets
Apr  6 09:52:59: %SEC-6-IPACCESSLOGP: list 152 denied udp 172.24.33.144(137) -> 256.256.201.27(137), 1 packet
Apr  6 19:02:46: %SEC-6-IPACCESSLOGP: list 152 denied udp 203.108.97.59(137) -> 256.256.201.27(137), 1 packet
Apr  6 19:08:09: %SEC-6-IPACCESSLOGP: list 152 denied udp 203.108.97.59(137) -> 256.256.201.27(137), 5 packets
Apr  6 22:18:04: %SEC-6-IPACCESSLOGP: list 152 denied udp 203.108.239.189(137) -> 256.256.201.27(137), 1 packet
Apr  6 22:23:15: %SEC-6-IPACCESSLOGP: list 152 denied udp 203.108.239.189(657) -> 256.256.201.27(137), 2 packets
```

Trace #9: Smurf attack (recurring)

Over several days a pair of ICMP echo requests were sent against the target network (masked here as 256.256.201.0/24). Packet filters on the Internet router prevented the ICMP packet from being processed and expanded, thus the attack failed. While the times are scattered, they all are attempting to use the target network as the amplifier and mostly cluster around early morning and late evening times in the Americas. No other entries from the selected victim networks are found in the target logs.

Complete listing of Smurf attempts for April 1-15 are listed below.

```
Apr 11 00:32:41: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 24.28.161.247 -> 256.256.201.255 (8/0), 1 packet
Apr 11 00:38:11: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 24.28.161.247 -> 256.256.201.255 (8/0), 1 packet
Apr 11 11:23:34: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.216.238.178 -> 256.256.201.255 (8/0), 1 packet
Apr 11 23:13:55: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.64.45.180 -> 256.256.201.255 (8/0), 1 packet
Apr 12 05:11:47: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 4.3.163.184 -> 256.256.201.255 (8/0), 1 packet
Apr 12 21:36:41: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 151.27.130.228 -> 256.256.201.255 (8/0), 1 packet
Apr 13 10:23:22: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 63.65.84.73 -> 256.256.201.255 (8/0), 1 packet
Apr 13 22:31:48: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.139.143.111 -> 256.256.201.255 (8/0), 1 packet
Apr 14 06:47:36: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 202.188.8.221 -> 256.256.201.255 (8/0), 1 packet
Apr 14 09:43:42: %SEC-6-IPACCESSLOGDP: list 100 denied icmp 212.216.236.23 -> 256.256.201.255 (8/0), 1 packet
```

Trace #10: Limited host scan for 98/tcp

Early on April 10 this small collection of packet rejections appeared in the target system logs. The 98/tcp is not an obvious service for abuse, and the addresses chosen are not in use. The attempts are only seconds apart and no other attempts to access 98/tcp are recorded in at the site in the period April 1-15. This is most likely a random attempt to communicate to a Trojan or a scattered host scan with an unusual port number. No other traffic is noted from the source network.

```
Apr 10 04:29:32: %SEC-6-IPACCESSLOGP: list 100 denied tcp 210.217.24.1(1901) -> 256.256.201.16(98), 1 packet
Apr 10 04:29:32: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 256.256.201.17 -> 210.217.24.1 (3/13), 1 packet
Apr 10 04:29:35: %SEC-6-IPACCESSLOGP: list 100 denied tcp 210.217.24.1(1903) -> 256.256.201.18(98), 1 packet
Apr 10 04:29:35: %SEC-6-IPACCESSLOGDP: list 102 denied icmp 256.256.201.17 -> 210.217.24.1 (3/13), 1 packet
Apr 10 04:29:36: %SEC-6-IPACCESSLOGP: list 100 denied tcp 210.217.24.1(2130) -> 256.256.201.245(98), 1 packet
```