Global Information Assurance Certification Paper

*** Northcutt, late, pass
Vincent L. Stigall, Sr.

DETECT #1

While reviewing the drop and reject traffic in my FW log I discovered this lone entry. I further examined the FW log all entries from the src address to dst but there was only this one entry. I searched through the days sensor files but only found two entries that correlate to my FW log

Firewall 1 log:
25Apr2000 16:01:37 hme0 reject service 43144 src 207.211.106.42 dst my.net.169.105 protocol tcp rule 24 s_port http len 40

Tcpdump output:
16:01:34.748639 my.net.169.105.43144 > 207.211.106.40.80: S 1911485137:1911485137(0) win 8760 <mss 1460> (DF) (ttl 253, id 36643)
16:01:34.823723 207.211.106.40.80 > my.net.169.105.43144: S 3579061942:3579061942(0) ack 1911485138 win 8760 <mss 1460> (DF) (ttl 244, id 44957)
16:01:34.824697 my.net.169.105.43144 > 207.211.106.40.80: . ack 1 win 8760 (DF) (ttl 253, id 36644)
16:01:34.849585 my.net.169.105.43144 > 207.211.106.40.80: P 1:389(388) ack 1 win 8760 (DF) (ttl 253, id 36645)
16:01:34.951044 207.211.106.40.80 > my.net.169.105.43144: . ack 389 win 8760 (DF) (ttl 244, id 44958)
16:01:34.951734 207.211.106.40.80 > my.net.169.105.43144: F 411:411(0) ack 389 win 8760 (DF) (ttl 244, id 44960)
16:01:34.954390 207.211.106.40.80 > my.net.169.105.43144: P 1:411(410) ack 389 win 8760 (DF) (ttl 244, id 44959)
16:01:34.955407 my.net.169.105.43144 > 207.211.106.40.80: . ack 411 win 8760 (DF) (ttl 253, id 36646)
16:01:35.028405 my.net.169.105.43144 > 207.211.106.40.80: F 389:389(0) ack 411 win 8760 (DF) (ttl 253, id 36647)
16:01:35.123823 207.211.106.40.80 > my.net.169.105.43144: . ack 390 win 8760 (DF) (ttl 244, id 44961)
16:01:36.945028 207.211.106.42.80 > my.net.169.105.43144: F 3579062353:3579062353(0) ack 1911485527 win 8760 (DF) (ttl 244, id 44962)
16:01:36.946945 my.net.169.105.43144 > 207.211.106.42.80: R 1911485527:1911485527(0) win 0 (DF) (ttl 60, id 24029)

Description:
Possible FIN scan. I scanned all of the sensor logs for the day and this is the only traffic that was listed for net 207.211.106.

Technique:
I believe that this is a crafted packet because:
a) a FIN/ACK was received without any stimulus
b) a new host on network 207.211.106 sent traffic to the same dst port that a previous session had just closed
c) the packet sequence number used in the FIN and the ACK is out of sequence
d) Though host 207.211.106.42 does answer on port 80. The page simply states:

"You Have Reached An AdForce AdServer."
"To Visit The AdForce Home Page Please Joto http://www.adforce.com. "

Intent:

It is possible that this is a low & slow scan. I have placed a filter for this entry on my analysis system so that I can watch for any other occurrence and hopefully gain more information.

Severity:
Low

DETECT #2

This is a trace from my sensor log on April 21, 2000.

19:16:22.927431 207.181.246.14.4293 > my.external.rtr.50.sunrpc: S 1985804865:1985804865(0) win 32120 <mss 1460,sackOK,timestamp 162062478[|tcp]> (DF)
19:16:22.936663 207.181.246.14.4295 > my.external.rtr.52.sunrpc: S 1983773279:1983773279(0) win 32120 <mss 1460,sackOK,timestamp 162062478[|tcp]> (DF)
19:16:22.936742 207.181.246.14.4296 > my.external.rtr.53.sunrpc: S 1985307383:1985307383(0) win 32120 <mss 1460,sackOK,timestamp 162062478[|tcp]> (DF)
19:16:22.942868 207.181.246.14.4297 > my.external.rtr.54.sunrpc: S 1979441641:1979441641(0) win 32120 <mss 1460,sackOK,timestamp 162062478[|tcp]> (DF)
19:16:22.946844 207.181.246.14.4298 > my.external.rtr.55.sunrpc: S 1974595391:1974595391(0) win 32120 <mss 1460,sackOK,timestamp 162062478[|tcp]> (DF)
19:16:22.970589 207.181.246.14.4303 > my.external.rtr.60.sunrpc: S 1975375573:1975375573(0) win 32120 <mss 1460,sackOK,timestamp 162062478[|tcp]> (DF)
19:16:25.713476 207.181.246.14.4296 > my.external.rtr.53.sunrpc: S 1985307383:1985307383(0) win 32120 <mss 1460,sackOK,timestamp 162062778[|tcp]> (DF)

Description:
This is a port mapper scan that was directed at the ip address of my external router. The source IP address is not spoofed.

Technique:
This was an automated scan and the packets are crafted. Note that the destination address increments by one each time, but on packet #7 the destination, source port, and packet sequence number are the same a packet #3,. There is a three second lapse in time between packet #6 and packet #7. Also note that the packet sequence numbers decrement instead of incrementing.

Intent:
Information gathering. To locate hosts answering on port 111.

Severity:
Low. We do not run RPC on hosts in our DMZ. Our Firewall blocks external connection requests to our internal network from unknown hosts.

DETECT #3

This detect is from my sensor logs for April 23,2000

19:20:13.288617 207.181.51.210.2666 > my.net.159.172.111: S 111:111(0) win 0 (ttl 228, id 23808)
19:20:13.300485 207.181.51.210.2666 > my.net.159.175.111: S 111:111(0) win 0 (ttl 228, id 10243)
19:20:13.304454 207.181.51.210.2666 > my.net.159.200.111: S 111:111(0) win 0 (ttl 228, id 11266)
19:20:13.306457 207.181.51.210.2666 > my.net.160.28.111: S 111:111(0) win 0 (ttl 228, id 29697)
19:20:13.312400 207.181.51.210.2666 > my.net.160.35.111: S 111:111(0) win 0 (ttl 228, id 8192)
19:20:13.316373 207.181.51.210.2666 > my.net.160.37.111: S 111:111(0) win 0 (ttl 228, id 28672)
19:20:13.324293 207.181.51.210.2666 > my.net.160.38.111: S 111:111(0) win 0 (ttl 228, id 44035)

19:20:13.336160 207.181.51.210.2666 > my.net.160.40.111: S 111:111(0) win 0 (ttl 228, id 46594)
19:20:13.342105 207.181.51.210.2666 > my.net.160.60.111: S 111:111(0) win 0 (ttl 228, id 55044)
19:20:13.342172 207.181.51.210.2666 > my.net.160.158.111: S 111:111(0) win 0 (ttl 228, id 52226)
19:20:13.348070 207.181.51.210.2666 > my.net.160.161.111: S 111:111(0) win 0 (ttl 228, id 39681)
19:20:13.352043 207.181.51.210.2666 > my.net.160.164.111: S 111:111(0) win 0 (ttl 228, id 49922)
---------- cut for brevity ----------
19:20:14.487472 207.181.51.210.2666 > my.net.178.222.111: S 111:111(0) win 0 (ttl 228, id 47873)
19:20:14.493417 207.181.51.210.2666 > my.net.178.223.111: S 111:111(0) win 0 (ttl 228, id 45568)
19:20:14.495418 207.181.51.210.2666 > my.net.178.221.111: S 111:111(0) win 0 (ttl 228, id 35585)
19:20:14.503336 207.181.51.210.2666 > my.net.178.224.111: S 111:111(0) win 0 (ttl 228, id 2819)
19:20:14.509783 207.181.51.210.2666 > my.net.178.225.111: S 111:111(0) win 0 (ttl 228, id 5888)
19:20:14.513697 207.181.51.210.2666 > my.net.178.226.111: S 111:111(0) win 0 (ttl 228, id 36098)
19:20:14.533463 207.181.51.210.2666 > my.net.178.227.111: S 111:111(0) win 0 (ttl 228, id 38146)
19:20:14.545329 207.181.51.210.2666 > my.net.178.239.111: S 111:111(0) win 0 (ttl 228, id 28672)
19:20:14.546033 207.181.51.210.2666 > my.net.178.241.111: S 111:111(0) win 0 (ttl 228, id 37632)
19:20:14.902654 207.181.51.210.2666 > my.net.186.57.111: S 111:111(0) win 0 (ttl 228, id 59906)
19:20:14.904653 207.181.51.210.2666 > my.net.186.59.111: S 111:111(0) win 0 (ttl 228, id 24835)
19:20:14.908644 207.181.51.210.2666 > my.net.186.62.111: S 111:111(0) win 0 (ttl 228, id 10243)
19:20:14.916947 207.181.51.210.2666 > my.net.186.64.111: S 111:111(0) win 0 (ttl 228, id 37123)
19:20:14.923280 207.181.51.210.2666 > my.net.186.65.111: S 111:111(0) win 0 (ttl 228, id 53760)
19:20:14.926453 207.181.51.210.2666 > my.net.186.70.111: S 111:111(0) win 0 (ttl 228, id 49152)
19:20:14.935593 207.181.51.210.2666 > my.net.186.168.111: S 111:111(0) win 0 (ttl 228, id 12802)

Description:
Another Port mapper Scan searching for hosts that answer on port 111.

Technique:
This was an automated scan. Unlike the scan in detect #2 this scan is very easy to detect. The src port stays the same, the sequence numbers stay the same and ironically are the same as the dst port, the packet id's are random but would have been more sequential if it were normal traffic.

Intent:
To locate hosts answering on port 111. The fact that the scan was targeted at ip's that are not currently being used on my network could indicate that the attacker may be looking for IP's to spoof in preparation to lunch a SYN Flood DOS attack.

Severity:
Medium. This attacker apparently already has some knowledge of our network because the scan was targeted ip's that are not in use right now. It will be useful to watch for more traffic on these addresses for a while.

DETECT #4

This detect is from my sensor logs for April 23,2000

06:17:57.111832 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 55, id 56741)
06:17:57.112488 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 54, id 56741)

06:17:57.117812 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 53, id 56741)
06:17:57.118309 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 52, id 56741)
06:17:57.123849 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 51, id 56741)
06:17:57.124310 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 50, id 56741)

---------- 44 packets cut for brevity ----------

06:17:57.247297 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 6, id 56741)
06:17:57.252379 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 5, id 56741)
06:17:57.252829 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 4, id 56741)
06:17:57.258441 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 3, id 56741)
06:17:57.259172 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) (ttl 2, id 56741)
06:17:57.264432 216.216.189.114.4948 > my net.74.0.53: S 1150000457:1150000457(0) win 32120 <mss 1460,sackOK,timestamp 1265199090[|tcp]> (DF) [ttl 1] (id 56741)

Description:
This appears to be a DOS attempt against 216.216.189.114. The source IP is probably spoofed. The reason I believe that this is possibly a DOS is because SYN packet was sent to port 53 of the broadcast address of my my.net.74 class C.

Technique:
The packet is definitely crafted because the src port, packet sequence number, and packet id number are the same. The ttl value decrements by 1 for each subsequent packet.

Intent:
Malicious. Because the packets were sent to the broadcast address this effect would be that every host on that particular network, except the DNS host of course, would return a port unreachable to the source.

Severity:
Low. Our firewall blocks all inbound connections that are not explicitly allowed.

DETECT #5

This detect is from my FW logs for Apri1 18, 2000

ID	Date	Time	I-face	Action	Source	SrcPrt	Dest	DstPort	Protocol
27378	18Apr2000	7:24:37	hme0	reject	206.251.19.88	2811	my.dns.svr	33434	udp
27382	18Apr2000	7:24:38	hme0	reject	206.251.19.88	2812	my.dns.svr	33434	udp
27383	18Apr2000	7:24:39	hme0	reject	206.251.19.88	2813	my.dns.svr	33434	udp
27385	18Apr2000	7:24:40	hme0	reject	206.251.19.88	2814	my.dns.svr	33434	udp
27390	18Apr2000	7:24:42	hme0	reject	206.251.19.88	2815	my.dns.svr	33434	udp
27431	18Apr2000	7:24:58	hme0	reject	216.33.87.8	2711	my.dns.svr	33434	udp
27432	18Apr2000	7:24:59	hme0	reject	216.33.87.8	2712	my.dns.svr	33434	udp

```
27434  18Apr2000 7:25:00  hme0  reject  216.33.87.8     2713  my.dns.svr 33434  udp
27437  18Apr2000 7:25:02  hme0  reject  216.33.87.8     2714  my.dns.svr 33434  udp
27439  18Apr2000 7:25:03  hme0  reject  216.33.87.8     2715  my.dns.svr 33434  udp
27524  18Apr2000 7:25:29  hme0  reject  216.33.87.9     2811  my.dns.svr 33434  udp
27525  18Apr2000 7:25:30  hme0  reject  216.33.87.9     2812  my.dns.svr 33434  udp
27526  18Apr2000 7:25:31  hme0  reject  216.33.87.9     2813  my.dns.svr 33434  udp
27531  18Apr2000 7:25:32  hme0  reject  216.33.87.9     2814  my.dns.svr 33434  udp
27534  18Apr2000 7:25:33  hme0  reject  216.33.87.9     2815  my.dns.svr 33434  udp
27558  18Apr2000 7:25:47  hme0  reject  206.251.19.89   2811 my.dns.svr 33434  udp
27559  18Apr2000 7:25:48  hme0  reject  206.251.19.89   2812 my.dns.svr 33434  udp
27560  18Apr2000 7:25:49  hme0  reject  206.251.19.89   2813 my.dns.svr 33434  udp
27562  18Apr2000 7:25:50  hme0  reject  206.251.19.89   2814 my.dns.svr 33434  udp
27565  18Apr2000 7:25:51  hme0  reject  206.251.19.89   2815 my.dns.svr 33434  udp
27571  18Apr2000 7:25:56  hme0  reject  209.67.29.9     2809 my.dns.svr 33434  udp
27573  18Apr2000 7:25:58  hme0  reject  209.67.29.9     2810 my.dns.svr 33434  udp
27578  18Apr2000 7:25:59  hme0  reject  209.67.29.9     2811 my.dns.svr 33434  udp
27581  18Apr2000 7:26:00  hme0  reject  209.67.29.9     2812 my.dns.svr 33434  udp
31616  18Apr2000 7:40:42  hme0  reject  206.251.19.89   2811 my.dns.svr 33434  udp
31618  18Apr2000 7:40:43  hme0  reject  206.251.19.89   2812 my.dns.svr 33434  udp
31620  18Apr2000 7:40:44  hme0  reject  206.251.19.89   2813 my.dns.svr 33434  udp
31624  18Apr2000 7:40:45  hme0  reject  206.251.19.89   2814 my.dns.svr 33434  udp
31626  18Apr2000 7:40:46  hme0  reject  206.251.19.89   2815 my.dns.svr 33434  udp
```

Description:
This is a prime example of load balancing by online content hosting sites. In this case the packets were generated by an online newspaper that is well known nationally.

Technique:
Five trace routes to the same target host are generated from web servers located in different demographic regions for the purpose of gathering response time statistics. These statistics would then be used to determine which site would provide the best response time to the site visitor.

Intent:
The intent here is not malicious. The trace routes will allow the src hosts to gather timing data to determine which location offers the best response time.

Severity:
N/A

DETECT #6

This detect was gathered from my sensor logs on April 22, 2000

07:24:18.957229 206.245.152.my.net > my.NAT.addr.002.31337: S 650069655:650069655(0) ack 81087302 win 34752 <nop,nop,timestamp 298789520 0,nop,[|tcp]> (DF)
07:24:19.010934 206.245.152.my.net > my.NAT.addr.002.31337: . ack 489 win 34752 <nop,nop,timestamp 298789526 774988> (DF)
07:24:19.046584 206.245.152.my.net > my.NAT.addr.002.31337: P 1:135(134) ack 489 win 34752 <nop,nop,timestamp 298789529 774988> (DF)

07:24:19.051109 206.245.152.my.net > my.NAT.addr.002.31337: P 135:890(755) ack 489 win 34752 <nop,nop,timestamp 298789529 774988> (DF)
07:24:19.090605 206.245.152.my.net > my.NAT.addr.002.31337: F 890:890(0) ack 489 win 34752 <nop,nop,timestamp 298789534 774989> (DF)
07:24:20.148005 206.245.152.my.net > my.NAT.addr.002.31337: . ack 490 win 34752 <nop,nop,timestamp 298789639 775000> (DF)

Description:
At first glance it looks like a connection had been established to the Back Orifice trojan. In actuality this is a legitimate connection. My FW NAT's any outbound private address to the same IP and uses port numbers to correlate the NAT'd.

Technique:
N/A

Intent:
Non-Hostile. Legitimate traffic.

Severity:
N/A

DETECT #7

This detect was taken from my sensor logs on April 24, 2000. I was scanning for udp traffic to broadcast ports.

22:37:51.877015 194.65.174.5.31790 > my.net.159.255.31789: udp 1 (ttl 113, id 29110)
22:38:00.601743 194.65.174.5.31790 > my.net.167.255.31789: udp 1 (ttl 113, id 30654)
22:38:02.827659 194.65.174.5.31790 > my.net.169.255.31789: udp 1 (ttl 113, id 31168)
22:38:12.457330 194.65.174.5.31790 > my.net.178.255.31789: udp 1 (ttl 113, id 31433)
22:38:21.252944 194.65.174.5.31790 > my.net.186.255.31789: udp 1 (ttl 113, id 31697)

Description:
This appears to be a trojan scan for Hack'a'Tack.

Technique:
This packet is definitely crafted. The source port is constant in all five packets. The traffic is targeted at port 31789 on the broadcast address of several of our networks. Port 31789 is one of the known ports for the Trojan Hack'a'Tack. Also, the udp length is another indicator that this is a malicious packet because the minimum udp length is 8 and this scan shows a length of 1.

Intent:
Malicious. The initiator's intent is probably to locate a host that has been compromised with the Hack'a'Tack trojan.

Severity:
Low. Our firewall blocks all inbound connections that are not explicitly allowed.

DETECT #8

This detect also shook out while I was scanning for udp traffic to broadcast ports on sensor logs on April 24, 2000.

14:37:07.808696 63.77.65.26.11675 > my.net.167.255.41524: udp 50 (ttl 117, id 58566)
14:37:07.810750 63.77.65.26.11681 > my.net.159.255.41524: udp 50 (ttl 117, id 60614)
14:40:12.014931 63.77.65.26.11694 > my.net.167.255.41524: udp 148 (ttl 117, id 13824)
14:40:12.023977 63.77.65.26.11700 > my.net.159.255.41524: udp 148 (ttl 117, id 15872)

15:30:55.319407 63.77.65.26.12085 > my.net.167.255.41524: udp 50 (ttl 117, id 39954)
15:30:55.324223 63.77.65.26.12091 > my.net.159.255.41524: udp 50 (ttl 117, id 42002)
15:33:58.387213 63.77.65.26.12101 > my.net.167.255.41524: udp 148 (ttl 117, id 13824)
15:33:58.397395 63.77.65.26.12107 > my.net.159.255.41524: udp 148 (ttl 117, id 15872)

Description:
According to information that I found at http://mlarchive.ima.com/firewalls/1999/2082.html, this could quite possibly a modified smurf attack. By using UDP the protection afforded by blocking ICMP echo requests can be circumvented.

Technique:
UDP Packets for port 41524 are sent to the broadcast address to a high port, in this case 41524, which will cause an ICMP unreachable message to be returned.

Intent:
Network mapping. Only live hosts will respond with an ICMP unreachable message.

Severity:
Low.

DETECT #9

This detect is from my sensor logs for April 25, 2000 and April 26, 2000

**** 04/25/2000

14:37:47.887967 194.217.122.153.30975 > my.net.167.2.49172: SFRP 2030026772:2030028224(1452) ack 2030026772 win 49172 urg 49172 <[bad opt]> (DF) (ttl 51, id 15043)

14:37:52.215384 194.217.122.153.30975 > my.net.167.2.49400: SFRP 2030027000:2030028452(1452) ack 2030027000 win 49400 urg 49400 <[bad opt]> (DF) (ttl 51, id 15508)

14:44:02.441919 195.173.28.91.30975 > my.net.167.2.50628: SFRP 2030028228:2030029676(1448) ack 2030028228 win 50628 urg 50628 <[bad opt]> (DF) (ttl 51, id 44762)

**** 04/26/2000
06:44:34.950674 194.247.64.133.30975 > my.net.167.129.16404: SFRP [bad hdr length] (DF) (ttl 241, id 22910)
06:44:41.794702 194.247.64.133.30975 > my.net.167.129.16404: SFRP [bad hdr length] (DF) (ttl 241, id 23023)

06:44:42.610010 194.247.64.133.30975 > my.net.167.129.32788: SFRP [bad hdr length] (DF) (ttl 241, id 23028)
07:18:03.624425 194.217.242.35.30975 > my.net.167.129.32788: SFRP [bad hdr length] (DF) (ttl 243, id 24253)
07:18:17.138867 194.217.242.35.30975 > my.net.167.129.32788: SFRP [bad hdr length] (DF) (ttl 243, id 24449)
13:42:30.540683 195.173.136.17.30975 > my.net.178.22.32800: SFRP 2030010400:2030010404(4) ack 2030010400 win 32800 urg 32800 <[bad opt]> (ttl 242, id 8904)
13:51:12.558102 195.173.136.17.30975 > my.net.178.22.1476: SFRP 2029979076:2029980524(1448) ack 2029979076 win 1476 urg 1476 <[bad opt]> (DF) (ttl 242, id 3795)
13:53:40.338718 195.173.136.17.30975 > my.net.178.22.33232: SFRP 2030010832:2030011267(435) ack 2030010832 win 33232 urg 33232 <[bad opt]> (DF) (ttl 242, id 374)

Description:
Being a beginner in Intrusion Detection I first thought that I was on to something really good! While searching for correlating data/info I found the msg from Lloyd Vancil at www.csclub.stthomas.edu/~bugtraq/1998/msg01276.html. After performing a trace route on the source addresses I discovered that the packets were from demon.net.

Technique:
Munged packet.

Intent:
Non-Hostile.

Severity:
N/A

DETECT #10

This detect is from my April 24, 2000 sensor logs

07:56:54.132287 my.net.159.197.1029 > 207.217.77.82.53: 1+ (29) (ttl 126, id 18432)
07:56:54.156108 my.net.159.197.1031 > 207.217.77.82.53: 2+ (36) (ttl 126, id 18944)
07:56:54.219533 207.217.77.82.53 > my.net.159.197.1029: 1 7/4/4 . (299) (ttl 241, id 52057)
07:56:54.221719 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1029 unreachable (ttl 126, id 19456)
07:56:54.248254 207.217.77.82.53 > my.net.159.197.1031: 2* 7/4/4 . (297) (ttl 241, id 52058)
07:57:09.131354 my.net.159.197.1033 > 207.217.77.82.53: 1+ (29) (ttl 126, id 19968)
07:57:09.138127 my.net.159.197.1035 > 207.217.77.82.53: 2+ (36) (ttl 126, id 20480)
07:57:09.221305 207.217.77.82.53 > my.net.159.197.1033: 1 7/4/4 . (299) (ttl 241, id 52059)
07:57:09.221597 207.217.77.82.53 > my.net.159.197.1035: 2* 7/4/4 . (297) (ttl 241, id 52060)
07:57:09.224017 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1033 unreachable (ttl 126, id 20992)
07:57:09.224456 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1035 unreachable (ttl 126, id 21248)
07:57:25.753835 my.net.159.197.1037 > 207.217.77.82.53: 1+ (37) (ttl 126, id 21504)
07:57:25.834676 207.217.77.82.53 > my.net.167.129.53: 19360 (37) (ttl 241, id 18141)
07:57:25.837314 my.net.167.129.53 > 207.217.77.82.53: 19360* 1/4/4 . (217) (DF) (ttl 253, id 33845)
07:57:25.918495 207.217.77.82.53 > my.net.159.197.1037: 1* 1/4/4 . (217) (ttl 241, id 52061)

07:57:25.923844 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1037 unreachable (ttl 126, id 22528)
07:57:26.914991 my.net.159.197.1040 > 207.217.77.82.53: 1+ (29) (ttl 126, id 24832)
07:57:26.921224 my.net.159.197.1042 > 207.217.77.82.53: 2+ (36) (ttl 126, id 25344)
07:57:26.925300 my.net.159.197.1044 > 207.217.77.82.53: 1+ (37) (ttl 126, id 25856)
07:57:26.997128 207.217.77.82.53 > my.net.159.197.1040: 1 7/4/4 . (299) (ttl 241, id 52062)
07:57:26.998761 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1040 unreachable (ttl 126, id 30208)
07:57:27.003399 207.217.77.82.53 > my.net.159.197.1042: 2* 7/4/4 . (297) (ttl 241, id 52063)
07:57:27.005029 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1042 unreachable (ttl 126, id 30720)
07:57:46.733860 my.net.159.197.1048 > 207.217.77.82.53: 1+ (29) (ttl 126, id 42752)
07:57:46.739180 my.net.159.197.1050 > 207.217.77.82.53: 2+ (36) (ttl 126, id 43264)
07:57:46.816555 207.217.77.82.53 > my.net.159.197.1048: 1 7/4/4 . (299) (ttl 241, id 52065)
07:57:46.818220 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1048 unreachable (ttl 126, id 43776)
07:57:46.820712 207.217.77.82.53 > my.net.159.197.1050: 2* 7/4/4 . (297) (ttl 241, id 52066)
07:57:46.822346 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 1050 unreachable (ttl 126, id 44032)

********** cut for brevity **********
16:56:19.325967 207.217.77.82.53 > my.net.159.197.4587: 1 7/4/4 . (299) (ttl 241, id 45946)
16:56:19.327712 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 4587 unreachable (ttl 126, id 13142)
16:56:19.332099 207.217.77.82.53 > my.net.159.197.4589: 2* 7/4/4 . (297) (ttl 241, id 45947)
16:56:19.333740 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 4589 unreachable (ttl 126, id 13398)
16:56:39.254787 my.net.159.197.4591 > 207.217.77.82.53: 1+ (29) (ttl 126, id 14166)
16:56:39.261075 my.net.159.197.4593 > 207.217.77.82.53: 2+ (36) (ttl 126, id 14678)
16:56:39.341295 207.217.77.82.53 > my.net.159.197.4591: 1 7/4/4 . (299) (ttl 241, id 45948)
16:56:39.343147 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 4591 unreachable (ttl 126, id 15190)
16:56:39.345619 207.217.77.82.53 > my.net.159.197.4593: 2* 7/4/4 . (297) (ttl 241, id 45949)
16:56:39.347286 my.net.159.197 > 207.217.77.82: icmp: my.net.159.197 udp port 4593 unreachable (ttl 126, id 15446)
20:46:32.188570 207.217.77.82.53 > my.net.167.103.53: 54306 (30) (ttl 241, id 25977)
20:46:32.191828 my.net.167.103.53 > 207.217.77.82.53: 54306 2/6/6 (332) (DF) (ttl 253, id 53023)
21:04:20.282449 207.217.77.82.53 > my.net.159.197.137: 12 7/4/4 . (299) (ttl 241, id 45461)
21:04:21.770938 207.217.77.82.53 > my.net.159.197.137: 12 7/4/4 . (299) (ttl 241, id 45462)
21:04:23.405470 207.217.77.82.53 > my.net.159.197.137: 12 7/4/4 . (299) (ttl 241, id 45463)
21:04:24.859634 207.217.77.82.53 > my.net.167.103.53: 23486 (38) (ttl 241, id 50041)
21:04:24.862314 my.net.167.103.53 > 207.217.77.82.53: 23486 NXDomain* 0/1/0 (97) (DF) (ttl 253, id 11451)
21:04:24.944639 207.217.77.82.53 > my.net.159.197.137: 12 NXDomain* 0/1/0 (97) (ttl 241, id 45464)
21:04:26.269968 207.217.77.82.53 > my.net.159.197.137: 12 NXDomain 0/1/0 (97) (ttl 241, id 45465)
21:04:27.764631 207.217.77.82.53 > my.net.159.197.137: 12 NXDomain 0/1/0 (97) (ttl 241, id 45466)

Description:
This detect is a UDP port scan against my.net.159.197. These packets are definitely crafted. Apparently this host is quite interesting to the scanner because these scans continued 4 days later. Sometimes to the same port, sometimes to ports that returned ICMP unreachable messages. The scanner also performed quite a few queries against our DNS server for other host and websites in our domain.

Technique:

Utilizing src port 53 the scanner sent packets crafted to look like responses to DNS queries to my.net.159.197. Available ports sent no response while closed ports generated an ICMP unreachable message. Thereby providing an accurate map of available ports based on ports that did not respond with an ICMP unreachable message.

Intent:
Information gathering.

Severity:
Medium. The reason the severity on this is medium is because I can't find any inbound entries in my FW log for this detect. The only entries in the log are the outbound ICMP packets. This detect has uncovered a vulnerability that needs to be secured.
