Global Information Assurance Certification Paper

*** Northcutt, a fine job, solid analysis process, could be more comprehensive, home field advantage of having her own traces, knowing her network well works for her and that is more than fair. No apologies needed for trace four, that is the way things are. 89 ***

Network Traces for GIAC Certification Exam
Carolyn Willey

Note about traces: I acquired all of the traces that I have included from our Shadow box, which is placed outside our firewall; all were seen within a three day period.

Trace #1

136.142.78.53 > my.dot.com.255
00:00:42.380000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:01:20.250000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:01:58.120000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:02:35.980000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:03:13.850000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:03:51.710000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:04:29.580000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:05:07.450000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:05:45.340000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:06:23.200000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:07:01.090000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:07:38.930000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:08:16.830000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:08:54.690000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:09:32.560000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:10:10.420000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)
00:10:48.300000 xxx.xxx.pitt.edu > my.dot.com.255: icmp: echo request (DF)

This was an interesting trace because it appeared in the hourly wrap up for every hour of the three days that I analyzed (as well as before and after those three days, upon further investigation).

Evidence of active targeting? Definitely. ICMP echo requests very regularly and for a sustained time period from this (spoofed) site.

Techniques? The offending site (not pitt.edu) was sending frequent icmp echo requests to our broadcast (.255) address. Upon further investigation, I realized (from this and other hourly wrap-ups of the same trace) that we were getting this pattern exactly once every 38

seconds. This attack was obviously scripted, for it to happen for that long and with that precise frequency.

History? This attack appeared consistently over a number of days.

Analysis - A "smurf" denial of service attack aimed at pitt.edu, with our site being used as the middle man. I found it very interesting that the attack was sustained for such a long period of time.

Trace

18:01:42.020000 Xxx.xxx.aol.com.1059 > fg14.my.dot.com.161: GetRequest(11)
18:01:43.040000 Xxx.xxx.aol.com.1059 > fg14.my.dot.com.161: GetRequest(11)
18:01:44.150000 Xxx.xxx.aol.com.1060 > fg14.my.dot.com.161: GetRequest(11)
18:01:45.080000 Xxx.xxx.aol.com.1060 > fg14.my.dot.com.161: GetRequest(11)
18:01:46.100000 Xxx.xxx.aol.com.1061 > fg14.my.dot.com.161: GetRequest(11)
18:01:47.130000 Xxx.xxx.aol.com.1061 > fg14.my.dot.com.161: GetRequest(11)
18:01:48.150000 Xxx.xxx.aol.com.1062 > fg14.my.dot.com.161: GetRequest(11)
18:01:49.160000 Xxx.xxx.aol.com.1062 > fg14.my.dot.com.161: GetRequest(11)
18:02:50.250000 Xxx.xxx.aol.com.1063 > fg14.my.dot.com.161: GetRequest(11)
18:02:51.260000 Xxx.xxx.aol.com.1063 > fg14.my.dot.com.161: GetRequest(11)
18:02:52.320000 Xxx.xxx.aol.com.1064 > fg14.my.dot.com.161: GetRequest(11)
18:02:53.270000 Xxx.xxx.aol.com.1064 > fg14.my.dot.com.161: GetRequest(11)
18:02:54.290000 Xxx.xxx.aol.com.1065 > fg14.my.dot.com.161: GetRequest(11)
18:02:55.290000 Xxx.xxx.aol.com.1065 > fg14.my.dot.com.161: GetRequest(11)
18:02:56.430000 Xxx.xxx.aol.com.1066 > fg14.my.dot.com.161: GetRequest(11)
18:02:57.320000 Xxx.xxx.aol.com.1066 > fg14.my.dot.com.161: GetRequest(11)

Evidence of active targeting? Yes, a string of SNMP traffic to a specific address on my network.

Technique? A series of crafted or scripted packets, about one per second, with the source port incrementing by one for every two packets that are sent.

Analysis – An AOL server doing "information gathering" from "customers" – note that the request was not directed at the broadcast address; rather a host on the network that is used by an employee at my company.

Trace #3

(Day 1)
38.200.145.120 > my.dot.com.255
21:37:42.150000 somehost.parklink.com > my.dot.com.255: icmp: echo request
21:37:43.140000 somehost.parklink.com > my.dot.com.255: icmp: echo request
(Day 2)
38.200.145.120 > my.dot.com.255

04:09:19.370000 somehost.parklink.com > my.dot.com.255: icmp: echo request
04:09:18.490000 somehost.parklink.com > my.dot.com.255: icmp: echo request
38.200.145.120 > my.dot.com.255
14:38:18.010000 somehost.parklink.com > my.dot.com.255: icmp: echo request
14:38:19.040000 somehost.parklink.com > my.dot.com.255: icmp: echo request
(Day 3)
38.200.145.120 > my.dot.com.255
04:09:19.370000 somehost.parklink.com > my.dot.com.255: icmp: echo request
04:09:18.490000 somehost.parklink.com > my.dot.com.255: icmp: echo request
38.200.145.120 > my.dot.com.255
14:38:18.010000 somehost.parklink.com > my.dot.com.255: icmp: echo request
14:38:19.040000 somehost.parklink.com > my.dot.com.255: icmp: echo request

Evidence of Active Targeting? Yes. ICMP echo requests to one of our broadcast addresses on several different occasions.

Techniques? Performed ICMP echo requests, two at a time, over a three day period to a broadcast address on our network. Time stamps for the transactions on days 2 and 3 were EXACTLY the same. Most likely scripted, possibly even cron'd, with output being captured by a file for later examination.

Analysis – a slow, stealthy scan of our network. Possibly part of a script which scanned multiple networks, and was activated by a cron job, a couple of times a day for a couple of days for recon purposes. Investigation of the source address suggests that its domain registrant is "Campuslink" in Ann Arbor, Michigan (the home of University of Michigan). Could this be a college "script kiddie" doing some recon in preparation for more fun-n-games on unsuspecting computers?

Trace #4

209.35.116.200 > my.dot.com.0
09:29:49.030000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:41:45.920000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:31:51.950000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:42:06.400000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:42:26.870000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:32:12.480000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:34:15.470000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:23:40.300000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:23:19.720000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request
09:37:40.170000 got.drunk.with.your.sister.and.had.wildteensex.com > my.dot.com.0: icmp: echo request

Note about source IP – I DID NOT MAKE IT UP. This is how it came in ☺ - not meant to offend.

Evidence of active targeting? Yes. This is but a sample of a pattern that occurred many times over a thirty minute time period, with our network as the destination.

Techniques? ICMP echo requests, at the rate of several per minute, over about a thirty minute period, to a possible broadcast address on our network.

Analysis – at first I thought this must just be a joke – someone generating traffic to give intrusion analysts a chuckle (considering the source IP). But then I got curious and actually tried going to the site – it actually exists! It appears to be a virtual hosting-type site that provides some other internet services as well (some that are quite questionable). This was apparently a smurf DOS attack against the "got.drunk.with. . ." site.

Trace #5

212.123.66.64 > my.dot.com.0
14:09:57.600000 mi1-572.tiscalinet.it > my.dot.com.0: icmp: echo request
14:10:01.560000 mi1-572.tiscalinet.it > my.dot.com.0: icmp: echo request
14:10:05.500000 mi1-572.tiscalinet.it > my.dot.com.0: icmp: echo request
14:10:09.440000 mi1-572.tiscalinet.it > my.dot.com.0: icmp: echo request
14:10:13.380000 mi1-572.tiscalinet.it > my.dot.com.0: icmp: echo request

212.216.166.190 > my.dot.com.0
14:49:02.890000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request
14:49:06.860000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request
14:49:10.760000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request
14:49:14.690000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request
14:49:18.650000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request

151.20.116.127 > my.dot.com.0
15:46:25.660000 ppp-20-116-127.libero.it > my.dot.com.0: icmp: echo request
15:50:06.270000 ppp-20-116-127.libero.it > my.dot.com.0: icmp: echo request
15:50:10.170000 ppp-20-116-127.libero.it > my.dot.com.0: icmp: echo request
15:50:14.100000 ppp-20-116-127.libero.it > my.dot.com.0: icmp: echo request
15:50:18.060000 ppp-20-116-127.libero.it > my.dot.com.0: icmp: echo request

212.216.166.190 > my.dot.com.0
15:04:21.320000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request
15:04:25.250000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request
15:04:29.200000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request
15:04:33.110000 a-rm23-63.tin.it > my.dot.com.0: icmp: echo request

Several separate traces are included here, but I grouped them together because I believe they might be related.

Evidence of active targeting? Yes. One of our possible broadcast addresses receiving ICMP echo requests continuously over a sustained time period by various internet hosts claiming to be in Italy.

Technique

ICMP echo requests, about every four seconds (this is a small sample of each trace), to an address that could possibly be a broadcast address (.0). Most likely scripted due to the frequency and duration of the requests.

History

These four traces were recorded on the same day, all within a one hour time period. Further investigation showed that we had recorded similar traces prior to and after these.

Analysis

Another "smurf" DOS attack, but unique from the others I've included because of the possibility that one attacker is attempting to wage DOS's on multiple sites in Italy. All of the "spoofed" source Ips were ".it" sites and closer review of the patterns shows that they are very similar to one another. Possibly a hacker (or hackers) attempting to cause widespread internet service interruptions of Italian sites.

Trace #6

xxx.xxx.5.157 > xxx.xxx.86.255

17:51:31.310000 xxx.xxx.5.157.40000 > my.dot.com.255.7: udp 64
7:51:31.660000 xxx.xxx.5.157.65083 > my.dot.com.255.7: udp 64
17:51:31.970000 xxx.xxx.5.157.46276 > my.dot.com.255.7: udp 64
17:51:51.770000 xxx.xxx.5.157.82 > my.dot.com.255.7: udp 64
17:51:52.120000 xxx.xxx.5.157.43176 > my.dot.com.255.7: udp 64
17:51:52.410000 xxx.xxx.5.157.55855 > my.dot.com.255.7: udp 64

Evidence of active targeting? Yes. Multiple UDP echo requests to a broadcast address on our network in a very short time frame.

Technique? Six udp echo requests to a broadcast address on our network. The first three are very close together (within a second) – the next three are also very close together, but occur about 20 seconds after the first three. All but one request originated from a very high-level port on the source. Why did one request originate from port 82?

Analysis – Network mapping using udp echo requests. The twenty seconds between the first set and second set would give the offender a chance to receive and digest any feedback between the two sets. Why would he perform three so close together, though? Must be scripted for them to happen so quickly.

Trace #7

152.174.83.64 > xxx.xxx.198.71
18:54:56.980000 xxx.xxx.aol.com.1035 > fg11.my.dot.com.389: S 445860:445860(0) win 8192 (DF) [tos 0x44]
18:54:59.890000 xxx.xxx.aol.com.1035 > fg11.my.dot.com.389: S 445860:445860(0) win 8192 (DF) [tos 0x44]
18:55:05.900000 xxx.xxx.aol.com.1035 > fg11.my.dot.com.389: S 445860:445860(0) win 8192 (DF) [tos 0x44]
18:55:18.020000 xxx.xxx.aol.com.1035 > fg11.my.dot.com.389: S 445860:445860(0) win 8192 (DF) [tos 0x44]
18:57:20.100000 xxx.xxx.aol.com.1042 > fg11.my.dot.com.389: S 588974:588974(0) win 8192 (DF) [tos 0x19]
18:57:23.160000 xxx.xxx.aol.com.1042 > fg11.my.dot.com.389: S 588974:588974(0) win 8192 (DF) [tos 0x19]
18:57:29.260000 xxx.xxx.aol.com.1042 > fg11.my.dot.com.389: S 588974:588974(0) win 8192 (DF) [tos 0x19]
18:57:41.480000 xxx.xxx.aol.com.1042 > fg11.my.dot.com.389: S 588974:588974(0) win 8192 (DF) [tos 0x19]
18:59:36.890000 xxx.xxx.aol.com.1050 > fg11.my.dot.com.389: S 725762:725762(0) win 8192 (DF) [tos 0x1e]
18:59:39.750000 xxx.xxx.aol.com.1050 > fg11.my.dot.com.389: S 725762:725762(0) win 8192 (DF) [tos 0x1e]

Evidence of active targeting? Several attempts by the same host to communicate with a host on our network, within a five minute time frame.

Technique? Several SYN packets sent from the source to the destination. SYN is apparently attempted four times with no response (see first four lines – same sequence # for all four, with increasing intervals [timeouts?] between tries – 3,6, and 13 seconds). SYN attempted again four times with no response (see second four lines – same sequence # for all four, with increasing intervals between tries – 3,6, and 12 seconds). SYN is attempted a third time, this time only twice (maybe received a SYN/ACK?). See the last two lines – same sequence # for each, with a three second interval in between. Notable difference between the three sets of SYNs is that the tos is different – 0x44, 0x19, and 0x1e.

Analysis - Assuming that the source IP is not spoofed and that AOL generated this traffic, I assume some kind of attempt to communicate with a customer's host, possibly for information gathering (especially considering the variation of tos). Although I am not familiar with which ports AOL uses for various "features," I assume this traffic could somehow be related to some of their "push" technology.

Trace #8

206.16.140.254 > my.dot.com.33
15:18:03.280000 ns1.parentcompany.com.42309 > raymac.my.dot.com.33447: udp 12 (DF) [ttl 1]
15:18:03.840000 ns1.parentcompany.com.42309 > raymac.my.dot.com.33448: udp 12 (DF)

History – The source IP is that of our parent company, which we have access to via VPN.

Analysis - The source IP of this traffic was that of a nameserver at our parent company. Considering that there is a ttl included in the first packet, this appears to be some sort of load balancing technique between our parent company and our internal servers which access the parent company via VPN.

Trace #9

62.136.120.214 > xxx.xxx.111.0
19:05:27.750000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.111.0: icmp: echo request
19:05:27.750000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.111.255: icmp: echo request
19:05:27.990000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.129.255: icmp: echo request
19:05:28.000000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.129.0: icmp: echo request
19:05:28.970000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.198.255: icmp: echo request
19:05:28.970000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.198.0: icmp: echo request
19:05:29.130000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.208.0: icmp: echo request
19:05:29.160000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.208.255: icmp: echo request
19:05:27.110000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.64.0: icmp: echo request
19:05:27.120000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.64.255: icmp: echo request
19:05:27.380000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.86.255: icmp: echo request
19:05:27.400000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.86.0: icmp: echo request
19:05:27.520000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.96.255: icmp: echo request
19:05:27.520000 modem-xx.some.dialup.pol.co.uk > xxx.xxx.96.0: icmp: echo request

Evidence of active targeting? Yes. A series of ICMP echo requests to broadcast addresses at seven different known subnets on our network, apparently from a .uk site.

Technique - ICMP echo requests, one each to port 0 and 255, on seven different known subnets. Traffic appears to be scripted, since it all occurs within a very short (two second) timeframe. Offender obviously has some knowledge of our network topology already, since he was able to target broadcast addresses on specific, valid subnets of our network.

Analysis - Smurf or network mapping?

Argument for network mapping – the offender obviously already knows something about our network topology, to be able to hit known subnets with such accuracy. Is this second sweep at the class "C" level, after getting feedback from an earlier sweep? Intelligence gathering from the UK?

Argument for Smurf – the rate of ICMP echo requests certainly suggests that a smurf DOS is possible here, with the pol.co.uk address being spoofed. But why would an attacker use our network in such a specific manner to wage a smurf attack on another site?

1. he was trying to cause a DOS to us as well?
2. he wanted traffic from our class "B" network to show up in the victim's network logs?

Trace #10

195.108.219.187 > my.dot.com.0
08:23:20.110000 www2.radio538.nl.41317 > my.dot.com.0.44602: udp 1024
08:23:20.120000 www2.radio538.nl > my.dot.com.0: icmp: echo request
08:23:24.070000 www2.radio538.nl.56035 > my.dot.com.0.36064: udp 1024
08:23:24.120000 www2.radio538.nl > my.dot.com.0: icmp: echo request
08:23:28.010000 www2.radio538.nl > my.dot.com.0: icmp: echo request
08:23:28.020000 www2.radio538.nl.38737 > my.dot.com.0.19382: udp 1024
08:23:31.960000 www2.radio538.nl > my.dot.com.0: icmp: echo request
08:23:31.980000 www2.radio538.nl.9775 > my.dot.com.0.50236: udp 1024
08:23:35.920000 www2.radio538.nl.4861 > my.dot.com.0.23538: udp 1024
08:23:35.930000 www2.radio538.nl > my.dot.com.0: icmp: echo request
08:23:39.810000 www2.radio538.nl > my.dot.com.0: icmp: echo request
08:23:39.810000 www2.radio538.nl.1339 > my.dot.com.0.25688: udp 1024
08:23:43.740000 www2.radio538.nl > my.dot.com.0: icmp: echo request
08:23:43.750000 www2.radio538.nl.41065 > my.dot.com.0.31470: udp 1024

Evidence of active targeting? Yes, a stream of udp traffic from the source to our local IP

Technique?

- A pattern of udp packets followed by one or two ICMP echo requests, every three or four seconds.
- All udp packets purport to have a 1024 byte payload.
- Both source and destination ports are very high-level (> 10,000) except for a couple of source ports (9775, 4861, 1339).
- The destination IP is my.dot.com.0
- Upon investigation of the source address, it appears to be an internet radio broadcast from the Netherlands

History

Saw a very similar pattern the following day from a different address. A portion of the trace is included here:

193.229.103.45 > my.dot.com.0
12:34:53.760000 m45m22hel.dial.kolumbus.fi.9870 > my.dot.com.0.57007: udp 1024
12:34:53.770000 m45m22hel.dial.kolumbus.fi > my.dot.com.0: icmp: echo request
12:34:57.640000 m45m22hel.dial.kolumbus.fi.16852 > my.dot.com.0.53117: udp 1024
12:34:57.650000 m45m22hel.dial.kolumbus.fi > my.dot.com.0: icmp: echo request
12:35:01.580000 m45m22hel.dial.kolumbus.fi > my.dot.com.0: icmp: echo request

2:35:01.590000 m45m22hel.dial.kolumbus.fi.62026 > my.dot.com.0.58811: udp 1024
12:35:05.540000 m45m22hel.dial.kolumbus.fi.14704 > my.dot.com.0.50409: udp 1024
12:35:05.560000 m45m22hel.dial.kolumbus.fi > my.dot.com.0: icmp: echo request
12:35:09.430000 m45m22hel.dial.kolumbus.fi > my.dot.com.0: icmp: echo request
12:35:09.790000 m45m22hel.dial.kolumbus.fi.58566 > my.dot.com.0.60551: udp 1024

The pattern of the two traces is almost identical, except for the second site is apparently in Finland. I was able to substantiate the first source address as valid using "whois"; however I was unable to find the second address.

Analysis - Upon first glance, I assumed that this was an audio/video application – possibly someone was listening to a broadcast from the Netherlands, especially since I was able to confirm that the first address in question is indeed an internet site that provides radio-like broadcasts. I noticed the use of high-numbered ports, although these port numbers were much higher than I would have expected to see for an audio application (6000-8000).

Conclusions

Unsure, although I have a couple of theories:

1. Network mapping meant to be disguised as a radio broadcast? Note the ICMP echo requests interleaved between the udp packets.
2. The source addresses are spoofed and the two incidents are two separate smurf DOS attempts against two different sites? Since the traces are so similar, maybe the DOS attempt originated from the same offender?
3. LOKI?
4. Is there any significance to the fact that most of the ports (source and dest) are very high level, with the exception of one or two in each trace? Could this have been some sort of decoy mechanism for a totally different attack? Possibly trojan ports?
5. A back door?

??????????????????????