Global Information Assurance Certification Paper

*** Northcutt, trace 4 is fun and may have been worth the price of admission into the course for all I know. Nice work! 80 *

GCIA Certification Practical
Dan Strom
Submitted April 21, 2000

Attended
SANS2000
Orlando, FL
March 21-25, 2000

Context
Out connection to the Internet is through an application level firewall. The DMZ contains a web server, a RealAudio server, and two workstations. Although I am awaiting the hardware necessary to run a network intrusion detection system, many of these detects were extracted by putting a sacrificial Linux box in the DMZ and capturing packets via tcpdump with various filters applied. Believe me, without the capabilities to easily sift through the data, it is difficult to arrive at useful information! In addition to the Linux box with tcpdump, I also provide some detects as they appear in various forms on the corporate firewall.

The data has been sanitized to protect the innocent.

Detect #1 – Network Mapping via icmp

```
15:37:52.678810 host1.probe.com > 1.dest.com: icmp: echo request
15:37:52.678946 host1.probe.com > 3.dest.com: icmp: echo request
15:37:52.679016 host1.probe.com > 4.dest.com: icmp: echo request
15:37:52.679181 host1.probe.com > 5.dest.com: icmp: echo request
15:37:52.679371 5.dest.com > 209.37.106.251: icmp: echo reply
15:37:52.679563 3.dest.com > host1.probe.com: icmp: echo reply
15:37:52.679633 4.dest.com > host1.probe.com: icmp: echo reply
15:37:52.679765 host1.probe.com > 7.dest.com: icmp: echo request
15:37:52.679989 7.dest.com > host1.probe.com: icmp: echo reply
15:37:52.681185 host1.probe.com > 25.dest.com: icmp: echo request
15:37:52.681381 25.dest.com > host1.probe.com: icmp: echo reply
15:37:52.698257 1.dest.com > host1.probe.com: icmp: echo reply
15:37:55.747451 host1.probe.com > 26.dest.com: icmp: echo request
15:37:55.750229 26.dest.com > host1.probe.com: icmp: echo reply
```

Analysis:
In a very short period of time, several *icmp echo requests* were sent to individual computers on the dest.com network. This scan appears to be scripted considering the short time intervals between *icmp echo requests*. Severity – Low.

Active targeting:
Yes.

History:
I have seen prior evidence of a ping scan on the DMZ subnet, but not from this same source.

Intent:
It appears that the host1.probe.com computer is attempting to determine what computers exist in the subnet.

Trace #2 – TCP Port Scan

```
09:12:28.612659 host1.probe.com.4764 > 5.dest.com.870: S 1156769396:115)
09:12:28.692076 host1.probe.com.4765 > 5.dest.com.1460: S 1155630805:11)
09:12:28.692148 host1.probe.com.4766 > 5.dest.com.491: S 1150039151:115)
09:12:29.692226 host1.probe.com.4767 > 5.dest.com.1222: S 1156115262:11)
09:12:28.692310 host1.probe.com.4768 > 5.dest.com.16: S 1156335994:1156)
09:12:28.771867 host1.probe.com.4769 > 5.dest.com.1460: S 1155700593:11)
09:12:30.771942 host1.probe.com.4770 > 5.dest.com.491: S 1154127674:115)
09:12:30.772025 host1.probe.com.4771 > 5.dest.com.1222: S 1151739618:11)
09:12:33.772104 host1.probe.com.4772 > 5.dest.com.16: S 1143172211:1143)
09:12:34.851872 host1.probe.com.4773 > 5.dest.com.1460: S 1143144273:11)
09:12:34.851949 host1.probe.com.4774 > 5.dest.com.491: S 1152128871:115)
09:12:34.852027 host1.probe.com.4775 > 5.dest.com.1222: S 1157970287:11)
09:12:34.852108 host1.probe.com.4776 > 5.dest.com.16: S 1150730027:1150)
```

Analysis:

The tcpdump log shows that several SYN packets were sent to the 5.dest.com computer over the course of a few seconds. These SYN packets were to different destination ports. The probing host (host1.probe.com) seems to be primarily devoted to this task, as the source ports are nearly incremental. The destination ports have been randomized in a simple attempt at masking the scan. Note that this is a scan of tcp ports. The probes also have a small amount of delay included between bursts. If this is an attempt at masking the probes, it failed. Severity – Low.

Active targeting:

Yes

History:

This same source address was seen over the course of two days, each time returning to do a tcp or udp port scan of different ports.

Intent:

This seems to be a precursor to a full-fledged intrusion or compromise attempt. The intent would be to know what services are running on the 5.dest.com host to then target specific exploits against the 5.dest.com computer.

Trace #3 – UDP Port Scan

```
08:56:13.044382 host1.probe.com.61445 > 5.dest.com.729: udp 0
08:56:13.044452 host1.probe.com.61445 > 5.dest.com.961: udp 0
08:56:13.044520 host1.probe.com.61445 > 5.dest.com.1446: udp 0
08:56:13.044590 host1.probe.com.61445 > 5.dest.com.1386: udp 0
08:56:13.044662 host1.probe.com.61445 > 5.dest.com.787: udp 0
08:56:13.044728 host1.probe.com.61445 > 5.dest.com.313: udp 0
08:56:13.044805 host1.probe.com.61445 > 5.dest.com.550: udp 0
```

Analysis:

Specifically note that the UDP packets have a length of zero and are being sent to random ports on the 5.dest.com host. The source port of host1.probe.com remains the same. The packets are being sent rapidly. Similar to trace #2 (above), this appears to be a simple, scripted scan for listening udp ports. Severity – Low.

Active targeting:

Host 5.dest.com is definitely being targeted.

History:

This same source address was seen over the course of two days, each time returning to do a tcp or udp port scan of different ports.

Intent:

See previous trace.

Trace #4 – Unauthorized access

```
11:47:00.309553 3.dest.com.2893 > tr7-007.source.se.ftp-data: . 192721:19418)
11:47:00.333017 p3E9EDF6C.source.de.1317 > 3.dest.com.ftp-data: . a)
11:47:00.333573 3.dest.com.ftp-data > p3E9EDF6C.source.de.1317: . 4)
11:47:00.334075 3.dest.com.ftp-data > p3E9EDF6C.source.de.1317: . 4)
11:47:00.389590 tr7-007.source.se.ftp-data > 3.dest.com.2893: . ack 188341 w)
11:47:00.390921 3.dest.com.3.2893 > tr7-007.source.se.ftp-data: . 194181:19564)
11:47:00.392165 3.dest.com.3.2893 > tr7-007.source.se.ftp-data: . 195641:19710)
11:47:00.402143 tr7-007.source.se.ftp-data > 3.dest.com.2893: . ack 191261 w)
11:47:00.403464 3.dest.com.2893 > tr7-007.source.se.ftp-data: . 197101:19856)
11:47:00.404714 3.dest.com.2893 > tr7-007.source.se.ftp-data: . 198561:20002)
11:47:00.481692 tr7-007.source.se.ftp-data > 3.dest.com.2893: . ack 194181 w)
11:47:00.483021 3.dest.com.2893 > tr7-007.source.se.ftp-data: . 200021:20148)
11:47:00.484256 3.dest.com.2893 > tr7-007.source.se.ftp-data: . 201481:20294)
11:47:00.500989 artech-nat.source.fr.1335 > 3.dest.com.ftp-data: . a)
11:47:00.531646 p3E9EDF6C.source.de.1317 > 3.dest.com.ftp-data: . a)
11:47:00.532218 3.dest.com.ftp-data > p3E9EDF6C.source.de.1317: . 4)
11:47:00.532715 3.dest.com.ftp-data > p3E9EDF6C.source.de.1317: . 4)
11:47:00.567239 tr7-007.source.se.ftp-data > 3.dest.com.2893: . ack 197101 w
```

Analysis:

This trace shows the results of unauthorized access to an ftp server in our DMZ. Connections have been established from domains in France, Germany, and Japan. Data is flowing on tcp port 20. The data transfers are quite large.

Active targeting:

Yes

History:

Upon reviewing the logs from the firewall and 3.dest.com, it seems that this access had been occurring for about 10 days. During this time ftp connections were established from at least 10 countries other than the U.S. and from many educational institutions within the U.S. This was not an exploitation of an obscure vulnerability, but instead was the result of careless server administration. Anonymous ftp had been enabled on a web server for a specific one-time use and never disabled. The lesson learned here is that regardless of the time spent on looking for and eliminating exposures, we should never forget the basic principles of network security. Steps were taken immediately to shut down ftp services and further review basic security on the server.

Intent:

The folks from around the world were using this server as a storage location for pirated software and music. The severity level of this intrusion is HIGH due to the legal liability it presents.

Trace #5 – Attempted NetBios connection

```
22:23:18.919039 one.badguy.com.137 > firewall.mydomain.com.137: udp 50
22:23:20.417181 one.badguy.com.137 > firewall.mydomain.com.137: udp 50
22:23:21.915642 one.badguy.com.137 > firewall.mydomain.com.137: udp 50
```

Analysis:

This is interesting. Our corporate firewall had three NetBios NameService requests. Each request contained 50 bytes of data. These interval between these packets is around one second. This frequency seems to indicate the traffic was scripted. Our firewall does not listen on udp or tcp ports 137-140, so the packet was dropped. The source host is from a dial-up ISP, and I have not seen any traffic from that specific address since. I am continuing to monitor traffic for ports 137-140 from this domain. The severity is low.

Active targeting:

Yes

History:

No previous activity from the source address is known.

Intent:

The individual sending this traffic appears to want to exploit a NetBios vulnerability.

Trace #6 – OS Identification

```
15:59:34.277811 host.badguy.com.45584 > 3.dest.com.ftp: SFP 1530734600:>
```

Analysis:

In the midst of what appeared to be a legitimate ftp session, an anomalous packet appears. It is sent to port 21 and has the SYN, FIN, and PSH flags all set - an invalid combination.

Active targeting:

Yes

History:

No previous activity like this is known. However, since the capture of this packet, I have seen the SFP flags set on attempted connections to 3.dest.com on other tcp ports from this same source.

Intent:

Many times invalid flag combinations are used for operating system identification. That is a reasonable assumption of the intent here. If this is an os id attempt, then the severity is medium, as it could portend other things to come.

Trace #7 – Port 8080

Date	prot	source host	srcprt	destination host	dstprt
Apr 14 08:45:02	tcp	5.6.7.8	1086	firewall.mydomain.com	8080
Apr 14 08:47:02	tcp	5.6.7.8	1087	firewall.mydomain.com	8080
Apr 14 08:49:05	tcp	5.6.7.8	1086	firewall.mydomain.com	8080
Apr 14 08:51:05	tcp	5.6.7.8	1087	firewall.mydomain.com	8080
Apr 14 08:53:11	tcp	5.6.7.8	1087	firewall.mydomain.com	8080

Analysis:

This is from our corporate firewall. The 5.6.7.8 host is attempting a connection to port 8080 on our firewall. Port 8080 is often used as an alternative to port 80 for http. The attempts are being made at two second intervals. This would tend to indicate that this is a scripted probe. The firewall does not respond to port 8080, thus the severity is low.

Active targeting:

Yes

History:

None previously detected from this host. Since this was detected, there has been one similar probe from a different source host targeting a different destination host on our DMZ.

Intent:

The intent probably is to search out a publicly accessible proxy server.

Trace #8 – SNMP probes

Date	prot	source host	srcprt	destination host	dstprt
Apr 13 07:36:16	udp	1.2.3.4	2879	firewall.mydomain.com	snmp
Apr 13 07:36:22	udp	1.2.3.4	2879	firewall.mydomain.com	snmp
Apr 13 08:07:09	udp	1.2.3.4	2879	firewall.mydomain.com	snmp
Apr 13 08:07:15	udp	1.2.3.4	2879	firewall.mydomain.com	snmp

Analysis:

This is a log from our corporate firewall. Someone at 1.2.3.4 was trying to get it to give up information via SNMP. The firewall does not provide SNMP information, thus the severity is low.

Active targeting:

Yes

History:

None previously detected from this host. Since this data was captured, I have not seen any further SNMP attempts from this source.

Intent:

The intent of this SNMP probe appears to gather information about the firewall.

Trace #9 - IRC

Date	prot	source host	srcprt	destination host	dstprt
Apr 12 09:58:34	tcp	172.10.253.10	1274	irc.some.net	6667
Apr 12 09:58:40	tcp	172.10.253.10	1274	irc.some.net	6667
Apr 12 09:58:52	tcp	172.10.253.10	1274	irc.some.net	6667
Apr 12 09:59:31	tcp	172.10.253.10	1277	irc.some.net	6667
Apr 12 09:59:34	tcp	172.10.253.10	1277	irc.some.net	6667
Apr 12 09:59:40	tcp	172.10.253.10	1277	irc.some.net	6667

Analysis:

This is a log from our corporate firewall. This detect indicates a host on our internal network attempting to make a connection to an IRC server on port 6667. We do not have a business need for IRC. The firewall does not allow IRC and effectively blocked the connection attempt. The severity is low.

Active targeting:

Yes

History:

IRC attempts have been seen before from this and other computers on our internal networks.

Intent:

The intent was to play and was not malicious.

Trace #10 - ICQ

Date	prot	source host	srcprt	destination host	dstprt
Apr 19 19:06:33	udp	172.10.253.10	1029	x.icq.yyy.com	4000
Apr 19 19:06:43	udp	172.10.253.10	1029	x.icq.yyy.com	4000
Apr 19 19:06:53	udp	172.10.253.10	1029	x.icq.yyy.com	4000
Apr 19 19:07:03	udp	172.10.253.10	1029	x.icq.yyy.com	4000
Apr 19 19:07:13	udp	172.10.253.10	1029	x.icq.yyy.com	4000
Apr 19 19:07:23	udp	172.10.253.10	1029	x.icq.yyy.com	4000
Apr 19 19:07:33	udp	172.10.253.10	1029	x.icq.yyy.com	4000

Analysis:

This is a log from our corporate firewall. The detect is showing an attempt to connect to host x.icq.yyy.com on port 4000. Port 4000 is commonly used for Terabase (per ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers) as well as ICQ. In this situation, the destination host name is x.icq.yyy.com. In reviewing the traffic from 172.10.253.10 and after reviewing the applications on 172.10.253.10, the traffic is being generated by an unsuccessful attempt to connect to an ICQ server. The firewall does not allow ICQ traffic and effectively blocked the connection attempt. The severity is low.

Active targeting:

Yes

History:

ICQ traffic has been observed previously from this and other source hosts.

Intent:

The intent is not malicious.

Last Updated: July 27th, 2017

Upcoming Training

SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced