Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Intrusion Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia
*** 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

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>15:37:52.678810</td>
<td>host1.probe.com</td>
<td>1.dest.com</td>
<td>icmp</td>
<td>echo request</td>
</tr>
<tr>
<td>15:37:52.678946</td>
<td>host1.probe.com</td>
<td>3.dest.com</td>
<td>icmp</td>
<td>echo request</td>
</tr>
<tr>
<td>15:37:52.679016</td>
<td>host1.probe.com</td>
<td>4.dest.com</td>
<td>icmp</td>
<td>echo request</td>
</tr>
<tr>
<td>15:37:52.679181</td>
<td>host1.probe.com</td>
<td>5.dest.com</td>
<td>icmp</td>
<td>echo request</td>
</tr>
<tr>
<td>15:37:52.679371</td>
<td>5.dest.com</td>
<td>209.37.106.25</td>
<td>icmp</td>
<td>echo reply</td>
</tr>
<tr>
<td>15:37:52.679563</td>
<td>3.dest.com</td>
<td>host1.probe.com</td>
<td>icmp</td>
<td>echo reply</td>
</tr>
<tr>
<td>15:37:52.679633</td>
<td>4.dest.com</td>
<td>host1.probe.com</td>
<td>icmp</td>
<td>echo reply</td>
</tr>
<tr>
<td>15:37:52.679765</td>
<td>5.dest.com</td>
<td>host1.probe.com</td>
<td>icmp</td>
<td>echo request</td>
</tr>
<tr>
<td>15:37:52.679989</td>
<td>7.dest.com</td>
<td>host1.probe.com</td>
<td>icmp</td>
<td>echo reply</td>
</tr>
<tr>
<td>15:37:52.681185</td>
<td>host1.probe.com</td>
<td>25.dest.com</td>
<td>icmp</td>
<td>echo request</td>
</tr>
<tr>
<td>15:37:52.681381</td>
<td>25.dest.com</td>
<td>host1.probe.com</td>
<td>icmp</td>
<td>echo reply</td>
</tr>
<tr>
<td>15:37:52.698257</td>
<td>1.dest.com</td>
<td>host1.probe.com</td>
<td>icmp</td>
<td>echo reply</td>
</tr>
<tr>
<td>15:37:52.698451</td>
<td>host1.probe.com</td>
<td>26.dest.com</td>
<td>icmp</td>
<td>echo request</td>
</tr>
<tr>
<td>15:37:52.698625</td>
<td>host1.probe.com</td>
<td>26.dest.com</td>
<td>icmp</td>
<td>echo reply</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:12:28.612659</td>
<td>host1.probe.com.4764</td>
<td>5.dest.com</td>
<td>TCP</td>
<td>4764</td>
<td>870</td>
</tr>
<tr>
<td>09:12:28.692076</td>
<td>host1.probe.com.4765</td>
<td>5.dest.com</td>
<td>TCP</td>
<td>4765</td>
<td>1460</td>
</tr>
<tr>
<td>09:12:29.692226</td>
<td>host1.probe.com.4766</td>
<td>5.dest.com</td>
<td>TCP</td>
<td>4766</td>
<td>491</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Time</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:56:13.044382</td>
<td>host1.probe.com.61445</td>
<td>5.dest.com</td>
<td>UDP</td>
<td>61445</td>
<td>729</td>
</tr>
<tr>
<td>08:56:13.044452</td>
<td>host1.probe.com.61445</td>
<td>5.dest.com</td>
<td>UDP</td>
<td>61445</td>
<td>961</td>
</tr>
</tbody>
</table>

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)
11:47:00.389590 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)
11:47:00.403464 3.dest.com.2893 > tr7-007.source.se.ftp-data: . 197101:19856)
11:47:00.483021 3.dest.com.2893 > tr7-007.source.se.ftp-data: . 200021:20148)
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


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


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

<table>
<thead>
<tr>
<th>Date</th>
<th>prot</th>
<th>source host</th>
<th>srcprt</th>
<th>destination host</th>
<th>dstprt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 14 08:45:02</td>
<td>tcp</td>
<td>5.6.7.8</td>
<td>1086</td>
<td>firewall.mydomain.com</td>
<td>8080</td>
</tr>
<tr>
<td>Apr 14 08:47:02</td>
<td>tcp</td>
<td>5.6.7.8</td>
<td>1087</td>
<td>firewall.mydomain.com</td>
<td>8080</td>
</tr>
<tr>
<td>Apr 14 08:49:05</td>
<td>tcp</td>
<td>5.6.7.8</td>
<td>1086</td>
<td>firewall.mydomain.com</td>
<td>8080</td>
</tr>
<tr>
<td>Apr 14 08:51:05</td>
<td>tcp</td>
<td>5.6.7.8</td>
<td>1087</td>
<td>firewall.mydomain.com</td>
<td>8080</td>
</tr>
<tr>
<td>Apr 14 08:53:11</td>
<td>tcp</td>
<td>5.6.7.8</td>
<td>1087</td>
<td>firewall.mydomain.com</td>
<td>8080</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Date</th>
<th>prot</th>
<th>source host</th>
<th>srcprt</th>
<th>destination host</th>
<th>dstprt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 13 07:36:16</td>
<td>udp</td>
<td>1.2.3.4</td>
<td>2879</td>
<td>firewall.mydomain.com</td>
<td>snmp</td>
</tr>
<tr>
<td>Apr 13 07:36:22</td>
<td>udp</td>
<td>1.2.3.4</td>
<td>2879</td>
<td>firewall.mydomain.com</td>
<td>snmp</td>
</tr>
<tr>
<td>Apr 13 08:07:09</td>
<td>udp</td>
<td>1.2.3.4</td>
<td>2879</td>
<td>firewall.mydomain.com</td>
<td>snmp</td>
</tr>
<tr>
<td>Apr 13 08:07:15</td>
<td>udp</td>
<td>1.2.3.4</td>
<td>2879</td>
<td>firewall.mydomain.com</td>
<td>snmp</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Date</th>
<th>prot</th>
<th>source host</th>
<th>srcprt</th>
<th>destination host</th>
<th>dstprt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 12 09:58:34</td>
<td>tcp</td>
<td>172.10.253.10</td>
<td>1274</td>
<td>irc.some.net</td>
<td>6667</td>
</tr>
<tr>
<td>Apr 12 09:58:40</td>
<td>tcp</td>
<td>172.10.253.10</td>
<td>1274</td>
<td>irc.some.net</td>
<td>6667</td>
</tr>
<tr>
<td>Apr 12 09:58:52</td>
<td>tcp</td>
<td>172.10.253.10</td>
<td>1277</td>
<td>irc.some.net</td>
<td>6667</td>
</tr>
<tr>
<td>Apr 12 09:59:31</td>
<td>tcp</td>
<td>172.10.253.10</td>
<td>1277</td>
<td>irc.some.net</td>
<td>6667</td>
</tr>
<tr>
<td>Apr 12 09:59:34</td>
<td>tcp</td>
<td>172.10.253.10</td>
<td>1277</td>
<td>irc.some.net</td>
<td>6667</td>
</tr>
<tr>
<td>Apr 12 09:59:40</td>
<td>tcp</td>
<td>172.10.253.10</td>
<td>1277</td>
<td>irc.some.net</td>
<td>6667</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Date</th>
<th>prot</th>
<th>source host</th>
<th>srcprt</th>
<th>destination host</th>
<th>dstprt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 19 19:06:33</td>
<td>udp</td>
<td>172.10.253.10</td>
<td>1029</td>
<td>x.icq.yyy.com</td>
<td>4000</td>
</tr>
<tr>
<td>Apr 19 19:06:43</td>
<td>udp</td>
<td>172.10.253.10</td>
<td>1029</td>
<td>x.icq.yyy.com</td>
<td>4000</td>
</tr>
<tr>
<td>Apr 19 19:07:03</td>
<td>udp</td>
<td>172.10.253.10</td>
<td>1029</td>
<td>x.icq.yyy.com</td>
<td>4000</td>
</tr>
<tr>
<td>Apr 19 19:07:13</td>
<td>udp</td>
<td>172.10.253.10</td>
<td>1029</td>
<td>x.icq.yyy.com</td>
<td>4000</td>
</tr>
<tr>
<td>Apr 19 19:07:23</td>
<td>udp</td>
<td>172.10.253.10</td>
<td>1029</td>
<td>x.icq.yyy.com</td>
<td>4000</td>
</tr>
<tr>
<td>Apr 19 19:07:33</td>
<td>udp</td>
<td>172.10.253.10</td>
<td>1029</td>
<td>x.icq.yyy.com</td>
<td>4000</td>
</tr>
</tbody>
</table>

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.
# Upcoming Training

<table>
<thead>
<tr>
<th>Training</th>
<th>Location</th>
<th>Dates</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 11, 2020 - May 16, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - SEC503: Intrusion Detection In-Depth</td>
<td>United Arab Emirates</td>
<td>May 28, 2020 - Jul 06, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANSFIRE 2020</td>
<td>DC</td>
<td>Jun 13, 2020 - Jun 20, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Rocky Mountain Summer 2020</td>
<td>CO</td>
<td>Jul 20, 2020 - Jul 25, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>Live Online - SEC503: Intrusion Detection In-Depth</td>
<td>United Arab Emirates</td>
<td>Jul 29, 2020 - Sep 04, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>Instructor-Led Training</td>
<td>Aug 3 ET</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS vLive - SEC503: Intrusion Detection In-Depth</td>
<td>SEC503 - 202008,</td>
<td>Aug 10, 2020 - Sep 16, 2020</td>
<td>vLive</td>
</tr>
<tr>
<td>SANS Essentials Live Online 2020</td>
<td>Australia</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA - Reston Fall 2020</td>
<td>Reston, VA</td>
<td>Sep 28, 2020 - Oct 03, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>