GIAC
CERTIFICATIONS

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 permited 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, nice job, got his own detects at least mostly, using a shadow system that has to be worth a ten point bonus :) (that is a joke for the humor impaired) Matt is using the I&W analysis process, coupled with severity this would be a near perfect score. I really liked the way he got detects that were outbound and even got to confront some people. There is a pattern I haven't seen before 3128 src to 3128 dst. 91 ***

10 Detects with analysis for

IDIC track Practical

Matthew Fearnow

Monday, April 3, 2000

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

The First 8 traces were detected on our own shadow system monitoring several "crown jewel" hosts and a few test lab machines. The last two traces were taken from the GIAC website.

Detect 1

18:30:03.968393 computer.edu.65535 > 192.168.1.180.53: S 3477602304:3477602304 (0) win 512
18:30:04.008493 computer.edu.65535 > 192.168.1.140.53: S 3477602304:3477602304 (0) win 512
18:30:04.034558 computer.edu.65535 > 192.168.1.145.53: S 3477602304:3477602304 (0) win 512

Active Targeting: Yes

History: No previous history

Technique: This appears to be a scripted network scan with minimal time difference, static source port and non-incrementing sequence numbers.

Intent: It appears that the source computer is scanning the network looking for a dns service to TCP port 53.

Detect 2

© SANS Institute 2000 - 2005 Author retains full rights.

20:01:04.968245 badguy.dsl.com.1838 > 192.168.1.140.98: S 1467928329:1467928329 (0) win 32
20:01:04.968391 badguy.dsl.com.1841 > 192.168.1.141.98: S 1461020383:1461020383 (0) win 32
20:01:05.016092 badguy.dsl.com.1864 > 192.168.1.165.98: S 1466732223:1466732223 (0) win 32
20:01:05.016167 badguy.dsl.com.1865 > 192.168.1.166.98: S 1468313730:1468313730 (0) win 32
20:01:05.041879 badguy.dsl.com.1876 > 192.168.1.177.98: S 1469208309:1469208309 (0) win 32
…
20:59:23.413165 badguy.dsl.com.683 > 192.168.1.140.111: udp 56
20:59:24.014912 badguy.dsl.com.685 > 192.168.1.166.111: udp 56
Active Targeting: Yes
History: No previous history
Technique: This appears to be a scripted network scan with minimal time difference.
Intent: It would appear that the source computer, at first is looking for TCP port 98, which is the Linux Conf port used for remote system administration. It gathers this information and then comes back nearly an hour later, to two computers that possibly responded earlier, it is now looking for the Port Mapper/Sun RPC service.

Detect 3
22:04:48.423754 somewhere.com.2860 > 192.168.1.180.53: S 2829929599:2829929599 (0) win 32120 (DF)
22:04:48.434826 somewhere.com.2846 > 192.168.1.166.53: S 2822289868:2822289868 (0) win 32120 (DF)
22:04:48.438452 somewhere.com.2869 > 192.168.1.189.53: S 2822386329:2822386329 (0) win 32120 (DF)
22:04:48.456862 somewhere.com.2808 > 192.168.1.141.53: S 2819685979:2819685979 (0) win 32120 (DF)
22:04:48.471707 somewhere.com.2819 > 192.168.1.140.53: S 2824373690:2824373690 (0) win 32120 (DF)
22:04:48.482901 somewhere.com.2857 > 192.168.1.177.53: S 2817499435:2817499435 (0) win 32120 (DF)
Active Targeting: Yes
History: No previous history.
Technique: This appears to be a scripted network scan with minimal time difference.
Intent: It would appear that the source computer is scanning the network attempting an active open of a connection. TCP port 53 is used for zone transfer and would allow the attacker to download a host table.

Detect 4
10:23:54.908896 192.168.1.165.7777 > 192.168.1.180.515: S 2290614272:2290614272 (0) win 16384
10:23:54.909387 192.168.1.165.7777 > 192.168.1.180.35: S 2290614273:2290614273 (0) win 16384
10:23:54.911087 192.168.1.165.7777 > 192.168.1.166.515: S 2290614274:2290614274 (0) win 16384
10:23:55.071445 192.168.1.165.7777 > 192.168.1.166.35: S 2290614275:2290614275 (0) win 16384
10:23:55.072271 192.168.1.165.7777 > 192.168.1.140.515: S 2290614276:2290614276 (0) win 16384
10:23:55.072602 192.168.1.165.7777 > 192.168.1.140.35: S 2290614277:2290614277 (0) win 16384
…
Active Targeting: Yes
History: No previous history but note this computer is a local test lab machine. After further investigation, we found no abnormal traffic before this going to or from this machine so we could safely assume that it had not been compromised. After confronting the user, this person indeed confessed to running an application to look for servers on the network.
Technique: This appears to be a scripted network scan with minimal time difference. Note, too, that the source

© SANS Institute 2000 - 2005 Author retains full rights.

port does not change throughout the scan.

Intent: The source computer is scanning the internal network for TCP port 515, which is the printer spooler port, and for TCP port 35. The only information I could find about port 35 is that it is used for any private printer server. The intent here is either to specifically look for printer services on servers or to get servers to answer back with a reset since they do not have that service running.

Detect 5

16:12:48.640443 proxy.scanner.com.3128 > 192.168.1.140.3128: SF 1638842970:1638842970 (0) win 1028
16:12:48.709812 proxy.scanner.com.3128 > 192.168.1.141.3128: SF 1638842970:1638842970 (0) win 1028
16:12:49.191528 proxy.scanner.com.3128 > 192.168.1.166.3128: SF 1337861729:1337861729 (0) win 1028
16:12:49.399577 proxy.scanner.com.3128 > 192.168.1.177.3128: SF 1337861729:1337861729 (0) win 1028
16:12:49.439757 proxy.scanner.com.3128 > 192.168.1.179.3128: SF 1337861729:1337861729 (0) win 1028

Active Targeting: Yes

History: No previous history.

Technique: This appears to be a scripted network scan with minimal time difference and static source port; sequence numbers change once during the scan but do not change with each packet. Note, too, that the both the SYN and FIN flags are set.

Intent: The source computer is scanning the network probably looking for hosts and hoping to get a reset back from the host. Also, note that the destination port is TCP 3128, which is what the squid proxy server runs on.

Detect 6

07:22:54.605159 dns.computer.jp.24193 > 192.168.1.140.143: S 4004110085:4004110085 (0) win 31744
07:22:54.696438 dns.computer.jp.24193 > 192.168.1.141.143: S 3543003608:3543003608 (0) win 31744
07:22:55.134305 dns.computer.jp.24193 > 192.168.1.177.143: S 3201027792:3201027792 (0) win 31744

Active Targeting: Yes

History: No previous history.

Technique: This appears to be a scripted network scan with minimal time difference and static source port.

Intent: The source computer is scanning the network for TCP port 143, which is the IMAP port. It is probably looking for a specific service to run a particular exploit.

Detect 7

01:47:07.331105 dialup.isp.net.10431 > 255.255.255.255.31337: udp 19
01:47:07.597435 dialup.isp.net.10431 > 192.168.1.140.31337: udp 19
01:47:07.655861 dialup.isp.net.10431 > 192.168.1.141.31337: udp 19
01:47:08.418523 dialup.isp.net.10431 > 192.168.1.177.31337: udp 19

Active Targeting: Yes

History: No previous history.

Technique: This appears to be a scripted network scan with minimal time difference and static source port. Note that the first packet is destined to address 255.255.255.255. This is probably to get answer back from all hosts on the network.

Intent: The source computer is scanning the network for UDP port 31337, which is most commonly related to Back Orifice.

© SANS Institute 2000 - 2005 Author retains full rights.

Detect 8

14:25:27.455559 192.168.1.176.9999 > x.x.181.255.53: 1205+ (45)
14:25:27.789605 192.168.1.176.9999 > x.x.213.255.53: 1205+ (45)
14:25:28.041413 192.168.1.176.9999 > x.x.246.255.53: 1205+ (45)
14:25:28.207602 192.168.1.176.9999 > x.x.244.255.53: 1205+ (45)
14:25:28.327880 192.168.1.176.9999 > x.x.149.255.53: 1205+ (45)
…

Active Targeting: Yes

History: No previous history but note this computer is a local test lab machine. After further investigation, we found no other suspicious activity to or from this computer. However, the individual denied any wrongdoing and this computers hard drive had been erased and operating system reinstalled hours after this detect.

Technique: This appears to be a scripted network scan with minimal time difference and static source port. Note that the user was scanning broadcast addresses on several internet class C's. This is probably to gain as many responses back as possible.

Intent: The source computer is scanning the networks for UDP port 53, probably to look for dns servers and to exploit them.

Detect 9

```
03/21-14:11:36.709202 212.238.134.99:27960 ->
MY.NET.10.119:27960 [**] Null scan! [**]
03/21-14:17:03.577695 212.238.134.99:27998 ->
MY.NET.10.119:27960 [**] Null scan! [**]
03/21-14:19:54.502156 212.238.134.99:27035 ->
MY.NET.10.119:3387 [**] Null scan! [**]
03/21-14:28:33.842668 212.238.134.99:9000 ->
MY.NET.10.119:9000 [**] Null scan! [**]
03/21-14:44:33.440931 212.238.134.99:21033 ->
MY.NET.10.119:2310 [**] Null scan! [**]
03/21-14:47:54.144549 212.238.134.99:27025 ->
MY.NET.10.119:2867 [**] Null scan! [**]
03/21-14:49:43.116595 212.238.134.99:27980 ->
MY.NET.10.119:27960 [**] Null scan! [**]
03/21-21:15:56.588060 194.217.188.53:27970 ->
MY.NET.98.133:27960 [**] SUNRPC highport access! [**]
03/21-21:17:31.168603 194.217.188.53:7788 ->
MY.NET.98.133:32771 [**] SYN-FIN scan! [**]
03/21-21:23:21.544496 194.217.188.53:27995 ->
MY.NET.98.133:10832 [**] Null scan! [**]
03/21-21:23:32.619598 194.217.188.53:7799 ->
MY.NET.98.133:2294 [**] Null scan! [**]
03/21-21:23:35.824415 194.217.188.53:27990 ->
MY.NET.98.133:27960 [**] Null scan! [**]
03/21-21:24:15.050650 194.217.188.21:27970 ->
MY.NET.98.130:29898 [**] Null scan! [**]
03/21-21:25:16.015794 194.217.188.53:27990 ->
MY.NET.98.133:27960
```

"In looking at this first it appears to be a scan. The first part of the trace may not be a script due to the time

© SANS Institute 2000 - 2005 Author retains full rights.

lapse, however, the second part could be a script. Possibly they are intentionally scanning for closed ports so that they get an rst back and then know that the host is alive.

Or this could be a scan for trinoo. Some versions of trinoo have been seen around this port range and they could perhaps be looking for a modified version of trinoo on this port.

Also the second part may either be spoofed or they may be trying to flood the system and here comes a packet from 194.217.188.21. This could be the real ip that is doing the scanning. "

The above mentioned was my first analysis on the trace. I would however like to add the format and a few more ideas.

Active Targeting: Yes
History: Unknown previous history.
Technique: Some low and slow approach.
Intent: I had read, I think in a report from someone on GIAC, that port 27960 was a standard port used for Quake III gaming. They could be trying to find that service running to find an exploit with QIII.

Detect 10

```
Mar 27 00:09:52 cc1014244-a kernel: securityalert: tcp if=ef0 from
209.235.11.254:50998 to 24.3.21.199 on unserved port 512
Mar 27 01:08:04 cc1014244-a kernel: securityalert: tcp if=ef0 from
24.40.35.215:2790 to 24.3.21.199 on unserved port 12345
Mar 27 08:18:19 cc1014244-a kernel: securityalert: tcp if=ef0 from
38.27.95.44:2756 to 24.3.21.199 on unserved port 1080

Mar 27 19:22:03 cc1014244-a kernel: securityalert: tcp if=ef0 from
38.26.9.97:4882 to 24.3.21.199 on unserved port 1080
Mar 27 20:29:59 cc1014244-a kernel: securityalert: tcp if=ef0 from
151.198.141.96:2660 to 24.3.21.199 on unserved port 27374

Mar 27 20:50:25 cc1014244-a kernel: securityalert: tcp if=ef0 from
151.198.141.96:2344 to 24.3.21.199 on unserved port 27374

Mar 27 20:57:48 cc1014244-a kernel: securityalert: tcp if=ef0 from
207.50.63.40:3537 to 24.3.21.199 on unserved port 1243

Mar 27 22:07:59 cc1014244-a kernel: securityalert: udp if=ef0 from
38.32.11.6:1044 to 24.3.21.199 on unserved port 31337
```

Active Targeting: Yes
History: Unknown previous history.
Technique: Very low and slow approach to network scanning.
Intent: The probable intent is to scan the network looking for various exploits. One that they are looking for is TCP port 512, which is rexec port for remote process execution. Another that they are searching for is TCP port 1080, which is for SOCKS proxy server. Yet others are TCP ports 27374 and 1243, which are used for various Trojans. All of this is directed towards 1 individual host. Either they thought they had something or they were just looking around.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	**Washington, DC**	**Jun 05, 2017 - Jun 12, 2017**	**Live Event**
SANS Houston 2017	**Houston, TX**	**Jun 05, 2017 - Jun 10, 2017**	**Live Event**
SANS Columbia, MD 2017	**Columbia, MD**	**Jun 26, 2017 - Jul 01, 2017**	**Live Event**
SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	**Washington, DC**	**Jul 24, 2017 - Jul 29, 2017**	**vLive**
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 Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 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 September 2017 - SEC503: Intrusion Detection In-Depth	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**vLive**
SANS Baltimore Fall 2017	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, United Kingdom**	**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 Boston SEC503	**Boston, MA**	**Oct 09, 2017 - Oct 14, 2017**	**Community SANS**
Community SANS Ottawa SEC503	**Ottawa, ON**	**Oct 16, 2017 - Oct 21, 2017**	**Community SANS**
SANS Seattle 2017	**Seattle, WA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS San Diego 2017	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**vLive**
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 OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**