Global Information Assurance Certification Paper

*** Northcutt, solid analysis process, accuracy is fine, took a bunch of easy ones including a duplicate but that is OK, we are all learning. Did some source host reasearch, no attack research, didn't explain the trace formats, apparently took traces from somewhere other than his net and didn't attribute source. Clairity is excellent. Welcome to the club, keep at it! 74 *

GIAC Certified Intrusion Analyst (GCIA)
Practical
SANS 2000 Intrusion Detection Immersion Curriculum

Christopher M. Meinders

April 13, 2000

DETECT #1

Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33465 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33466 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33467 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33468 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33469 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33470 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33471 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33472 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33473 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33474 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33475 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33476 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33477 UDP
Mar 31 11:27:43 208.185.54.22:33161 -> a.b.c.34:33478 UDP

Existence: The source address in this detect is 208.185.54.22 (or someone claiming to be), which is assigned to Abovenet Communications, Inc in San Jose, CA. A reverse lookup provides the domain name speedera.com, which is registered, to Speedera Networks in Mountain View, CA
History: In my research on the Internet, I could not find any history of this source attempting connection to this or any other network.
Techniques: It appears as though the source address is very quickly scanning for an available connection to high-range UDP ports.
Intent: Although this initially appears to be a scan, due to the high numbered source and destination UDP ports and identical source ports, this is more than likely a traceroute; perhaps maybe even for load balancing.
Targeting: The source address is definitely targeting a.b.c.34. The traceroute could either be for troubleshooting network connectivity or for network mapping.
Analysis: This trace, though it appears to be a scan, is more than likely a non-malicious traceroute from 208.185.54.22 to a.b.c.34. However, consideration should be taken regarding the criticality of the destination that could possibly make it worth an attackers desire to map the Internet to this system. If the source address does not have reason to be tracerouting to the destination, action should be taken to block or monitor future access.

DETECT #2

Mar 31 05:08:28 myhost portsentry[172]: attackalert: Connect from host:
150.183.91.134/150.183.91.134 to TCP port: 111
Mar 31 10:36:38 myhost portsentry[173]: attackalert: Connect from host:
dgt048.cpunet.com.br/200.254.53.48 to UDP port: 111
Mar 31 10:38:36 myhost portsentry[173]: attackalert: Connect from host:
dgt048.cpunet.com.br/200.254.53.48 to UDP port: 111

Existence: Two source addresses in this detect. The first, 150.183.91.134, is registered to the Korea Institute of Science and Technology in Daejeon, Korea. The second, 200.254.53.48, which as the log shows and I have verified, is registered to a location in Brazil; the Brazilian Research Network.
History: In my research on the Internet, I could not find any other reports of these sources attempting connection to this or any other network.
Techniques: Based on the time between the connections, this does not appear to be a scripted scan.
Intent: Attempted connections to UDP port 111, commonly known for Sun Remote Procedure Calls.
Targeting: Destination address, though not specified, is targeted at a machine that is running portsentry.
Analysis: Only one connection from one of the sources and only two connections from the other. It appears that the source(s) are simply looking to exploit one of the many vulnerabilities available on port 111, although there is not enough information in this detect to determine which vulnerability the source(s) were looking for. I would recommend that future attempts for connections to UDP port 111, be closely monitored and/or blocked.

DETECT #3

Mar 31 12:34:44 myhost portsentry[173]: attackalert: Connect from host: user-33qs1hs.dialup.mindspring.com/199.174.6.60 to UDP port: 31337
Mar 31 12:35:10 myhost2 portsentry[8311]: attackalert: Connect from host: user-33qs1hs.dialup.mindspring.com/199.174.6.60 to UDP port: 31337

Existence: Claimed source address, 199.174.6.60, is registered to MindSpring Enterprises out of Atlanta, GA.
History: No other history of this source address attempting connections to this or any other network could be found.
Techniques: Time period between the two attempts in this trace is far enough apart to conclude that this was not an automated or scripted attempt.
Intent: Source address is attempting to connect to the default port for the Back Orifice trojan, UDP port 31337.
Targeting: Destination address, though not specified, is targeted at a machine running portsentry.
Analysis: Though this server may have software that is listening on this port, it is most likely a probe for the Back Orifice trojan. Infection with the Back Orifice trojan would lead to the source gaining complete control over the destination. Recommend continuing to monitor and/or block probes to UDP port 31337.

DETECT #4

```
03/28-11:17:55.595895 131.107.3.121:137 -> myhost:137
UDP TTL:51 TOS:0x0 ID:61040
Len: 58
CF CC 00 00 00 01 00 00 00 00 00 00 20 43 4B 41 ..... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 AAAAAAAAAAAAA..!
00 01 ..
03/28-11:17:55.600122 157.54.7.195:137 -> myhost:137
UDP TTL:51 TOS:0x0 ID:60784
Len: 58
CF CA 00 00 00 01 00 00 00 00 00 00 20 43 4B 41 ..... CKA
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAA
41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21 AAAAAAAAAAAAA..!
00 01 .
```

Existence: Source address, 131.107.3.121, registered to Microsoft Corporation in Redmond, WA. The hostname is mail5.microsoft.com so I would probably guess it's a mailserver.
History: I was unable to find additional evidence of this source address attempting connections.
Techniques: Two entries, one right after the other, occuring within the same second, signifies this was something automated.
Intent: The source address is attempting to connect on UDP port 137, with contents to query the destination for its NetBIOS information. The source port is also 137. This type of communication normally occurs internally on Microsoft Windows networks, however, attempts to connect from an unauthorized network machine could indicate someone looking for information it can use to exploit a system.
Targeting: The source address is targeting "myhost" on port 137. Based on this trace, I am unable to determine whether "myhost" is on the same network.
Analysis: Connection to UDP port 137 to discover the netbios information, if on the same network would not be considered malicious. For this case, I'll assume we're talking about a remote system being connected to. Since the source is (probably) a Microsoft mail server, we're probably seeing an automatic reply from the mailserver to "myhost", which had previously attempted to connect to it. Recommend monitoring, or even better, blocking, this port to prevent future requests.

DETECT #5

Mar 30 19:44:02 209-30-73-81.flash.net ASCEND: wan5 tcp a.b.c.80;27374
<- 24.29.78.48;1493 58 syn !pass (totcp-1)
Mar 30 19:44:02 209-30-73-81.flash.net ASCEND: wan6 tcp a.b.c.81;27374
<- 24.29.78.48;1494 58 syn !pass (totcp-1)
Mar 30 19:44:02 209-30-73-81.flash.net ASCEND: wan5 tcp a.b.c.82;27374
<- 24.29.78.48;1495 58 syn !pass (totcp-1)
Mar 30 19:44:02 209-30-73-81.flash.net ASCEND: wan6 tcp a.b.c.83;27374
<- 24.29.78.48;1496 58 syn !pass (totcp-1)
Mar 30 19:44:02 209-30-73-81.flash.net ASCEND: wan5 tcp a.b.c.95;27374
<- 24.29.78.48;1508 58 syn !pass (totcp-1)

Existence: The source address is 24.29.78.48, whose domain name is rr.com and registered to EXCALIBUR Group, A Time Warner Company out of Herndon, VA.
History: No other access attempts were discovered to originate from this source address.
Techniques: The timestamp and sequence numbers tell me this was a scripted scan. This if fairly fast considering we see five hits all within the same second.
Intent: The source address is scanning for systems listening on TCP port 27374, commonly known for the SubSeven 2.1 trojan.
Targeting: The source is definitely targeting machines on the a.b.c network.
Analysis: The source address is scanning for machines listening on TCP port 27374, to exploit the SubSeven 2.1 trojan, which could ultimately lead to complete control of a system. Recommend blocking all traffic destined for port 27374 and taking the necessary steps to ensure the destinations have not been compromised.

DETECT #6

Mar 30 21:17:18 209-30-73-81.flash.net ASCEND: wan5 udp a.b.c.80;137 <-
24.5.72.117;137 92 !pass (toudp-1)
Mar 30 21:17:27 209-30-73-81.flash.net ASCEND: wan5 udp a.b.c.81;137 <-
24.5.72.117;137 92 !pass (toudp-1)
Mar 30 21:17:36 209-30-73-81.flash.net ASCEND: wan6 udp a.b.c.82;137 <-
24.5.72.117;137 92 !pass (toudp-1)

Existence: Source address, 24.5.72.117, is identified as a home.com system registered out of Redwood City, CA.
History: No history of this source address could be located.
Techniques: Slow scripted scan or manual scan of UDP port 137, with source port also 137.
Intent: Source address is doing information gathering using NetBIOS to find out what services are available, probably for future malicious intent.
Targeting: The source is targeting three machines on the a.b.c network.
Analysis: The source address is clearly doing information gathering (nbtstat) in this trace. Information that can be gained about services running on these machines could be used to launch a specific attack in the future. NetBIOS traffic should not be allowed to enter the network from the Internet. Recommend blocking this traffic and looking for future activity from this source address.

DETECT #7

```
03/26-15:59:47.860982 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:47.898827 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:48.063184 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:48.224471 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:48.381950 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:48.534075 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:48.554078 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:48.704326 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:48.719580 132.241.80.10:25 -> MY.NET.253.24:35555
[**] GIAC 000218 VA-CIRT port 35555 [**]
03/26-15:59:53.701981 132.241.80.10:25 -> MY.NET.253.24:35555
```

Existence: The source address is 132.241.80.10, which is registered to a system at California State University out of Chico, California.
History: No other access attempts were discovered to originate from this source address.
Techniques: Ten attempts to access the same machine on the same port within one second signifies this as a scripted/automatic scan.
Intent: The source address is attempting to connect to port 35555.
Targeting: Attempt to connect to MY.NET.253.24 is clearly identified in this detect.
Analysis: Source address is attempting to connect to the destination on port 35555, which is the default port for the Trinoo trojan on a Microsoft Windows system. Recommend blocking this port and monitoring the source for future activity. Also should look at the destination system to ensure it has not been infected with this trojan.

DETECT #8

```
04/03-12:56:39.480862 216.160.38.58:750 -> a.b.c.98:111
UDP TTL:49 TOS:0x0 ID:47947
Len: 64 0B 3A 2F 6B 00 00 00 00 00 00 00 02 00 01 86 A0 .:/k.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
--------
04/03-12:56:39.550530 216.160.38.58:761 -> a.b.c.34:111
UDP TTL:49 TOS:0x0 ID:47954
Len: 64 7A 62 57 13 00 00 00 00 00 00 00 02 00 01 86 A0 zbW.....
00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....
00 00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 ....
00 00 00 11 00 00 00 00 ....
```

Existence: The source address is 216.160.38.58, with a domain name of dialupM58.mpls.uswest.net registered to USWest Communications in Minneapolis, MN.
History: No other history of this source address attempting connections to this or any other network could be found.
Techniques: Two connections to two different systems on the a.b.c network within one second signifies this is probably a scripted scan.
Intent: Source is attempting to locate machines listening on UDP port 111.
Targeting: Active targeting to two machines on the a.b.c. network
Analysis: Source address is attempting to query the portmap daemon, UDP port 111. The contents of the trace further indicate that the source is requesting information from the rpc.mountd service. Information provided by this query can be used to exploit the mountd service or buffer overflow some system versions. Recommend blocking access to port 111, unless authorized users use it, and continue to monitor source for future activity.

DETECT #9

Jan 17 12:09:42 host1 portsentry[740]: attackalert:
Connect from host: 209.35.124.3/209.35.124.3 to TCP port:
1080
Jan 17 12:09:42 host2 portsentry[337]: attackalert:
Connect from host: 209.35.124.3/209.35.124.3 to TCP port:
1080
Jan 17 12:09:42 host3 portsentry[13660]: attackalert:
Connect from host: 209.35.124.3/209.35.124.3 to TCP port:
1080

Existence: The source address, 209.35.124.3 is registered to Interland, Inc in Atlanta, Georgia.
History: No other evidence of activity from this source address could be found. Furthermore, I am *currently* unable to resolve a domain name or ping the source IP address.
Techniques: Automated scan. This detect shows three attempted connections within the same second.
Intent: Source is scanning for systems listening on TCP port 1080, socks.
Targeting: Although the destination is not identified, the source is targeting a machine that has portsentryrunning on it.
Analysis: Source address is either an IRC server verifying that the destination isn't using their system to chat anonymously or the source (what I'm more inclined to believe) is looking to see if the destination is running socks so that it can bounce traffic off of it. If the source is able to exploit the socks port, it can use the destination to be malicious to other machines on the Internet, appearing to be the system running socks.

Detect #10

Jan 18 08:36:16 border-router 683:
21:17:44: %SEC-6-IPACCESSLOGP: list 102 denied tcp 196.1.112.33(1801) -> x.x.109.132(80), 1 packet
Jan 18 08:37:14 border-router 685:
21:18:44: %SEC-6-IPACCESSLOGP: list 102 denied tcp 196.1.112.33(1850) -> x.x.109.132(8080), 1 packet
Jan 18 08:38:15 border-router 686:
21:19:44: %SEC-6-IPACCESSLOGP: list 102 denied tcp 196.1.112.33(1892) -> x.x.109.132(3128), 1 packet

Existence: The source address, 196.1.112.33 is registered to the Pan American Health Organization in Cuba.
History: No other history of activity from this source address could be found.
Techniques: Each entry is almost exactly one minute apart, therefore the traffic is being generated automatically.
Intent: Source address is scanning the system to see if it is listening on port 80, 8080, and 3128, common ports that are open on web proxy servers. Port 3128 is commonly used on Squid proxy servers.
Targeting: Source address is targeting x.x.109.132, which is behind the router from which this log was taken. The problem here is that the user of the source probably doesn't know it's sending out this traffic.
Analysis: The source address is infected with the Ring Zero Trojan which sends out requests to port 80, 8080, and 3128 (in that order) to randomly generated IP addresses. If it would have found a host listening on one of these ports, it would have sent the destination's IP address to a server that was collecting the IP addresses. Fortunately, this trace shows that the connections were denied by the router access list. Recommend contacting the source's registration point of contact and notify them of their infected machine and continue blocking/monitoring traffic destined for these ports.

Last Updated: October 18th, 2017

Upcoming Training

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 Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced