Global Information Assurance Certification Paper

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

*** Name added by Northcutt, good show getting your own traces, that is excellent and you seem to know your firewall and network very well! Trace 10 is very intriguing. Little more effort researching your ports would be good, could be some more analysis on severity. 75 ***

Shawn Frederickson

I grabbed these traces from our Checkpoint Firewall-1 server. Since these are from my company's internal network, I cleaned up the traces to remove any sensitive internal networking information. In all the following traces, the 172.26.x.x network refers to our internal hosts and the 192.168.x.x network refers to the external hosts.

Trace 1

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
14:37:07	Firewall-1	reject	33453	192.168.100.60	172.26.10.223	udp	62039
14:37:12	Firewall-1	reject	33454	192.168.100.60	172.26.10.223	udp	62039
14:37:17	Firewall-1	reject	33455	192.168.100.60	172.26.10.223	udp	62039
14:37:22	Firewall-1	reject	33456	192.168.100.60	172.26.10.223	udp	62039

This trace shows that someone was a little interested in our network. This indicates a traceroute from 192.168.100.60 to one of our internal servers (denoted by the UDP destination ports above 33000). Fortunately this was blocked by our firewall policy since we do not allow any external source to traceroute into our network, but the external host probably found out what the IP address was of our external perimeter router. This means he at least as a starting point into our network. The intent seems to be that the external host was trying to map the route into a specific server (this was the only attempt in a 4 hour period). I categorize this as low severity since the attempt was unsuccessful.

Trace 2

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
14:35:36	Firewall-1	reject	6998	192.168.185.10	172.26.10.15	tcp	1725
14:36:31	Firewall-1	reject	6998	192.168.185.10	172.26.10.15	tcp	1733
14:36:42	Firewall-1	reject	6998	192.168.185.10	172.26.10.15	tcp	1734
14:39:09	Firewall-1	reject	6998	192.168.185.10	172.26.10.15	tcp	1750
14:41:02	Firewall-1	reject	6999	192.168.185.10	172.26.10.15	tcp	1761
14:44:48	Firewall-1	reject	6999	192.168.185.10	172.26.10.15	tcp	1780
14:55:31	Firewall-1	reject	6999	192.168.185.10	172.26.10.15	tcp	1824
15:05:08	Firewall-1	reject	6999	192.168.185.10	172.26.10.15	tcp	1892

This trace shows that someone seemed to be looking at one specific host on 2 ports. My first thought was that they were possibly scanning for a trojan on one of these ports, but I hadn't heard of any well-known trojan on tcp-6998 or tcp-6999. This appears to be manual scanning, not automated because the timestamps aren't really close together. Also, this would appear not to be a very busy server as there is not a lot of gap in the source port numbers. I found it interesting that they were trying to access a test server, so I called the application support group that administers the server. It would seem that one of our divisions was trying to sign on a new customer for electronic data interchange. It would also seem that our EDI application listens on port 6998 and 6999. So in retrospect, this was not an intrusion detect, it just proves that our testing division and our firewall division do not communicate very well.

Trace 3

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
23:57:24	Firewall-1	accept		192.168.100.105	172.26.100.1	icmp	
23:57:25	Firewall-1	accept		192.168.100.105	172.26.100.2	icmp	
23:57:26	Firewall-1	accept		192.168.100.105	172.26.100.3	icmp	
23:57:36	Firewall-1	accept		192.168.100.105	172.26.100.4	icmp	
23:57:36	Firewall-1	accept		192.168.100.105	172.26.100.5	icmp	
23:57:37	Firewall-1	accept		192.168.100.105	172.26.100.6	icmp	
23:58:19	Firewall-1	accept		192.168.100.105	172.26.100.7	icmp	
23:58:19	Firewall-1	accept		192.168.100.105	172.26.100.8	icmp	
23:58:19	Firewall-1	accept		192.168.100.105	172.26.100.9	icmp	
23:58:21	Firewall-1	accept		192.168.100.105	172.26.100.10	icmp	
0:30:26	Firewall-1	accept		192.168.100.105	172.26.100.11	icmp	
0:30:28	Firewall-1	accept		192.168.100.105	172.26.100.12	icmp	
0:30:29	Firewall-1	accept		192.168.100.105	172.26.100.13	icmp	
0:30:39	Firewall-1	accept		192.168.100.105	172.26.100.14	icmp	
0:30:39	Firewall-1	accept		192.168.100.105	172.26.100.15	icmp	
0:30:40	Firewall-1	accept		192.168.100.105	172.26.100.16	icmp	
0:31:22	Firewall-1	accept		192.168.100.105	172.26.100.17	icmp	
0:31:22	Firewall-1	accept		192.168.100.105	172.26.100.18	icmp	
0:31:22	Firewall-1	accept		192.168.100.105	172.26.100.19	icmp	
0:31:24	Firewall-1	accept		192.168.100.105	172.26.100.20	icmp	

This trace shows that someone was interested in which hosts were alive on our network. This seems to be a ping scan of several different IP addresses on one of our subnets. This also appears to be an automated script of some kind since the time stamps are very close together. I did find it interesting that there are a couple noticeable time gaps (between 23:58 and 0:30 and again between 0:30 and 0:31). This could be caused by a couple of things. It's possible that the automated script failed at some point, or it's possible that this was not the only subnet that was being scanned. Possibly between 23:58 and 0:30 the intruder decided to scan another subnet that we were not monitoring. This is not a very severe detect because the intruder did not receive any responses back. Even though we will accept inbound icmp traffic, we deny outbound icmp traffic.

Trace 4

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
0:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
1:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
2:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
3:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
4:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
5:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
6:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
7:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	
8:19:55	Firewall-1	accept		192.168.230.13	172.26.160.55	icmp	

This trace shows an attempt to ping a specific internal host. This appears to be very automated since the timestamps are exactly 1 hour apart. This appears to be some sort of heartbeat type automation. Probably checking every hour to see if a specific server is up. The odd thing here is that this shouldn't do the external source any good since we do not allow outbound ping replies. Unless I'm missing something the external host would not receive any responses to this heartbeat traffic and in fact I don't see any in the firewall logs. I don't find this very serious since this is the only traffic I found on the firewall log from this external source.

Trace 5

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
10:02:32	Firewall-1	reject	smtp	192.168.175.9	172.26.104.175	tcp	1174
10:02:35	Firewall-1	reject	smtp	192.168.175.75	172.26.104.175	tcp	3217
10:04:05	Firewall-1	reject	smtp	192.168.175.180	172.26.104.175	tcp	1088
10:06:15	Firewall-1	reject	smtp	192.168.175.10	172.26.104.175	tcp	1208
10:23:04	Firewall-1	reject	smtp	192.168.175.250	172.26.104.175	tcp	1026
10:23:18	Firewall-1	reject	smtp	192.168.175.90	172.26.104.175	tcp	1691
10:27:17	Firewall-1	reject	smtp	192.168.175.45	172.26.104.175	tcp	1227
10:30:00	Firewall-1	reject	smtp	192.168.175.12	172.26.104.175	tcp	1110
10:30:20	Firewall-1	reject	smtp	192.168.175.108	172.26.104.175	tcp	3250
10:31:56	Firewall-1	reject	smtp	192.168.175.176	172.26.104.175	tcp	1240
10:34:53	Firewall-1	reject	smtp	192.168.175.202	172.26.104.175	tcp	3274

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

This trace appears to be a search for sendmail ports open on our internal network. This traffic is coming from several hosts on an external subnet. It seems that someone wants to get to one of our production application servers. They are trying to break through our defenses from several different hosts, but the attacks are all launched from the same external subnet. This traffic was blocked by our firewall so the severity of this is fairly low.

Trace 6

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
9:13:31	Firewall-1	reject	1503	192.168.109.79	172.26.122.11	tcp	1575
9:15:33	Firewall-1	reject	1503	192.168.109.79	172.26.122.12	tcp	1579
9:20:56	Firewall-1	reject	1503	192.168.109.79	172.26.122.13	tcp	1592
9:21:00	Firewall-1	reject	1503	192.168.109.79	172.26.122.14	tcp	1593
9:23:32	Firewall-1	reject	1503	192.168.109.79	172.26.122.15	tcp	1601
9:23:42	Firewall-1	reject	1503	192.168.109.79	172.26.122.16	tcp	1603

I found this trace interesting. It appears to be a search of our network for an open tcp port of 1503. I can't think of any application that would normally run on port 1503 so this is probably a search for a trojan (but I don't know of one that uses port 1503). Fortunately the firewall policy rejects this traffic. This is the first time I have noticed this IP address show up in our logs (and I looked back for the last week). This doesn't appear to be automated since the timestamps aren't very close together. I put the severity of this as fairly low. The traffic is rejected by the firewall and seems to just be scanning our network for a specific port. I think it would be interesting to look at some other organization's IDS to see if they monitored this traffic as well.

Trace 7

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
11:18:46	Firewall-1	drop	33441	192.168.100.10	172.26.100.5	udp	60941
11:18:51	Firewall-1	drop	33442	192.168.100.10	172.26.100.5	udp	60941
11:18:56	Firewall-1	drop	33443	192.168.100.10	172.26.100.5	udp	60941
11:19:01	Firewall-1	drop	33444	192.168.100.10	172.26.100.5	udp	60941
11:19:06	Firewall-1	drop	33445	192.168.100.10	172.26.100.5	udp	60941
11:19:11	Firewall-1	drop	33446	192.168.100.10	172.26.100.5	udp	60941
11:19:16	Firewall-1	drop	33447	192.168.100.10	172.26.100.5	udp	60941
11:19:37	Firewall-1	drop	33441	192.168.100.10	172.26.26.10	udp	60987
11:19:42	Firewall-1	drop	33442	192.168.100.10	172.26.26.10	udp	60987
11:19:47	Firewall-1	drop	33443	192.168.100.10	172.26.26.10	udp	60987
11:19:52	Firewall-1	drop	33444	192.168.100.10	172.26.26.10	udp	60987
11:19:57	Firewall-1	drop	33445	192.168.100.10	172.26.26.10	udp	60987
11:20:15	Firewall-1	drop	33444	192.168.100.10	172.100.15	udp	61009
11:20:20	Firewall-1	drop	33445	192.168.100.10	172.100.15	udp	61009
11:20:25	Firewall-1	drop	33446	192.168.100.10	172.100.15	udp	61009
11:20:30	Firewall-1	drop	33447	192.168.100.10	172.100.15	udp	61009

This trace implies a traceroute to 3 of our internal servers. This is similar to one of the previous traces I have submitted above, with one major exception. The Source IP address is assigned to one of our external AS5300 dial-in access servers. We provide remote dial-in access to some of our customers to use our web based application. The servers targeted are 2 production servers and one test server. But there is no reason for someone to run a traceroute once they are dialed in to our system. There is no way for me to track whether this was one of our clients trying the traceroute or if someone else dialed in to our network that was not authorized. No responses were sent back to the external address since we do not allow traceroute through the firewall and hence the packets were dropped. However, I consider this a moderately serious detect since this is a dial-in to our production systems that is not password protected. So, now we need to go and try to lock down our AS5300 access servers with some sort of authentication.

Trace 8

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
11:11:11	Firewall-1	reject	80	192.168.59.9	172.26.100.5	tcp	1111
11:11:12	Firewall-1	reject	23	192.168.59.9	172.26.100.5	tcp	1111
11:11:12	Firewall-1	reject	8001	192.168.59.9	172.26.100.5	tcp	1111
11:11:12	Firewall-1	reject	8080	192.168.59.9	172.26.100.5	tcp	1111
11:11:18	Firewall-1	reject	755	192.168.59.9	172.26.100.5	tcp	1111
11:11:19	Firewall-1	reject	1409	192.168.59.9	172.26.100.5	tcp	1111
11:11:21	Firewall-1	reject	1604	192.168.59.9	172.26.100.5	tcp	1111
11:11:22	Firewall-1	reject	9200	192.168.59.9	172.26.100.5	tcp	1111

This trace shows a port scan on one of our internal hosts. The intruder is looking at some well-known ports (http, telnet) and some other more obscure ports. He is probably just trying to see if there are any open ports on our system, but this could also be a scan for trojans. This seems to be an automated attack due to the close timestamps. Also, if you notice the source port never changes from 1111. This shows that this is not a naturally occurring transaction. This is most likely a crafted packet. Since we lock our firewall down and this traffic is rejected, I don't see this as a very severe threat. We have the defenses in place to defend this port scan.

Trace 9

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
10:47:18	Firewall-1	reject	5632	192.168.100.8	172.26.155.174	udp	1755
10:47:36	Firewall-1	reject	5632	192.168.100.8	172.26.155.174	udp	1756

This trace shows an external source trying to reach a specific port (udp-5632) on a specific internal host. Based on the destination port, this looks like someone trying to access PC-Anywhere. It is known for communicating on port 5632. The firewall rejected this based on our security policy. I would classify this as a medium severity because the machine that they attempted to access was a production NT server. It looks like the intruder knew that this server was running NT and not Unix. Based on this information it is probably a good idea to look back through the logs for the past few days to see if there was any time of recon and info gathering traffic to this server.

Trace 10

Time	Origin	Action	Dest. Port	Source IP	Dest. IP	Protocol	Source Port
9:12:51	Firewall-1	reject	sunrpc-udp	192.168.155.22	172.26.190.50	udp	1060
9:12:51	Firewall-1	reject	3714	192.168.155.22	172.26.190.50	udp	1061
9:13:27	Firewall-1	reject	sunrpc-udp	192.168.155.22	172.26.190.50	udp	1068
9:13:27	Firewall-1	reject	3716	192.168.155.22	172.26.190.50	udp	1069

Submitted by: Shawn Frederickson
shawn_frederickson@amsinc.com

This trace shows an external source trying to access a some higher UDP ports (one of the rpc) on a specific unix server. It appears that the sunrpc and 3714/16 traffic comes in at almost exactly the same time. This trace bothers me somewhat because of the activity type. I am relieved that the firewall rejected this traffic, but it looks like someone is trying to gain access to one of our development unix servers.

Last Updated: July 24th, 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 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 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