Global Information Assurance Certification Paper

*** NORTHCUTT, THIS WAS A FUN READ. I REALLY ENJOYED THE SENSE OF ADVENTURE IN THE TRACES. THERE ARE SOME PROBLEMS WITH ACCURACY, 11 IS PROBABLY LINUXCONF, 5 IS PROBABLY THE RESULT OF SPOOFING, A COUPLE OTHERS, WITHOUT HIGHER FIDELITY I DUNNO. BUT STILL FUN, STILL A GOOD EXAMPLE OF WHAT CAN BE DONE WITH FIREWALL LOGS. 76 *

GCIA

(GIAC CERTIFIED INTRUSION ANALYSTS)

PRACTICAL DETECT SUBMISSIONS TO GIAC

(GLOBAL INCIDENT ANALYSIS CENTER)

SCOTT N. MARTIN

APRIL 20, 2000

Because of the nature of the company I work for and the work I do, it's quite easy to come up with 10 original detects. The following are some excerpts from the last 16 hours of firewall logs. Naturally, I have only included parts of each detect, as together they would contain over 92,000 lines of log information. If you would like to obtain the entire detect, please contact me.

Please note that our IP addresses have been changed although external IP addresses and the time/date information is accurate (all times GMT). This allows for coordination with other companies/facilities on analysis.

DETECT #1 – 3 MINUTES AND 3 SECONDS

LOG EXCERPT:

Ref. #	Date	Time	Inter.	Origin	Type	Action	Port	Source	Destination	Protocol
52	18-Apr-00	23:54:41	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp
231	18-Apr-00	23:55:13	hme2	A.B.C.1	log	drop	38293	165.243.249.79	Y.Z.112.18	udp
908	18-Apr-00	23:57:43	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp
1046	18-Apr-00	23:58:15	hme2	A.B.C.1	log	drop	38293	165.243.249.79	Y.Z.112.18	udp
1787	19-Apr-00	0:00:44	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp
<snip>										
194550	19-Apr-00	11:16:17	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp
195112	19-Apr-00	11:19:19	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp
195748	19-Apr-00	11:22:22	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp
196362	19-Apr-00	11:25:24	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp
197069	19-Apr-00	11:28:27	hme2	A.B.C.1	log	drop	38293	165.243.249.12	Y.Z.112.18	udp

TARGETING:

YES

EXISTENCE:

The source IP address from an ISP in Seoul. The target IP address is assigned to a development system that is also in Seoul.

HISTORY:

No previous history of inappropriate activity from the source or the target IP addresses known.

TECHNIQUES:

Regular udp connections only on port 38293 to the target IP address. The packets were interleaved at 3 minute and 2 or 3 second intervals without end. At 8:29:33 (GMT) one of the source systems stops (not included in the log excerpt).

ANALYSIS:

Connecting with the admins of the development system in Seoul, yielded some answers to this activity. The product under development will be requesting updates from production servers in the future. This system (Y.Z.112.18) has been setup as the testing update server. The connections seen here are (as suspected) from our developers accidentally leaving their test configurations active on their systems when connecting to their personal ISP.

INTENT/THREAT ASSESSMENT:

The short answer: Low Threat. The port is blocked by firewall connection and the connections are/were from the authorized users of the target system.

DETECT #2 – WHAT ARE THEY DOING?

LOG EXCERPT:

Ref. #	Date	Time	Inter.	Origin	Type	Action	Port	Source	Destination	Protocol
44	18-Apr-00	23:54:40	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
579	18-Apr-00	23:56:40	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
1156	18-Apr-00	23:58:40	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
1752	19-Apr-00	0:00:40	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
2399	19-Apr-00	0:02:40	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
3050	19-Apr-00	0:04:40	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
<snip>										
231958	19-Apr-00	13:47:43	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
232479	19-Apr-00	13:49:43	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
233036	19-Apr-00	13:51:43	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
233495	19-Apr-00	13:53:43	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
234041	19-Apr-00	13:55:43	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
234573	19-Apr-00	13:57:43	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp
235142	19-Apr-00	13:59:43	hme2	A.B.C.1	log	drop	2301	X.Y.Z.40	255.255.255.255	udp

TARGETING:

NO Active Targeting – These packets were being broadcast (255.255.255.255). Normally, this would lower the priority of this particular detect however, there were other reasons that necessitated a follow-up.

EXISTENCE:

The source IP address is from a former competitor. This would have previously been classified as a potentially hostile source, but détente's a great thing (see history).

HISTORY:

No previous history of inappropriate activity from the source IP address is known. This was, however, originating from the IP address of a company that was previously a competitor and has just acquired our competing product (we've adjusted our focus).

TECHNIQUES:

Traffic indicates, noisy, voluminous, regular (every 2 minutes), UDP packets. From one IP address on one port (2301) only. Very specific traffic, but non-specific delivery.

ANALYSIS:

Upon further research, I identified UDP port 2301 as a port that is used for the "Compaq Insight Management" web agents. This service is enabled by default on NT systems if installed (typically using the Smart Start CD) and can/should be disabled if the system is open to the Internet.

INTENT/THREAT ASSESSMENT:

The short answer: Minimal Threat.
Detail: This was broadcast traffic from an identifiable IP address. It is undirected and visible to any system on the Internet able to receive it. All existing firewall policies drop this traffic. While we're certainly not the Internet Police, casually connecting with the other company's IT department revealed that the system was a development system and had, indeed, accidentally activated this service.

DETECT #3 – DO THEY THINK THIS IS A CONNECTED WORLD?

LOG EXCERPT:

Ref. #	Date	Time	Inter.	Origin	Type	Action	Port	Source	Destination	Protocol
224750	19-Apr-00	13:22:09	hme2	A.B.C.1	log	drop	nbname	208.46.190.14	Y.Z.70.26	udp
225586	19-Apr-00	13:24:09	hme2	A.B.C.1	log	drop	nbname	208.46.190.14	Y.Z.70.26	udp
225844	19-Apr-00	13:24:38	hme2	A.B.C.1	log	drop	http	208.46.190.14	Y.Z.151.22	tcp
226511	19-Apr-00	13:26:05	hme2	A.B.C.1	log	drop	http	208.46.190.14	Y.Z.151.22	tcp
226536	19-Apr-00	13:26:09	hme2	A.B.C.1	log	drop	nbname	208.46.190.14	Y.Z.70.26	udp
<snip>										
233470	19-Apr-00	13:53:36	hme2	A.B.C.1	log	drop	nbname	208.46.190.14	Y.Z.3.9	udp
233598	19-Apr-00	13:54:08	hme2	A.B.C.1	log	drop	nbname	208.46.190.14	Y.Z.70.26	udp
233887	19-Apr-00	13:55:11	hme2	A.B.C.1	log	drop	http	208.46.190.14	Y.Z.151.22	tcp
234170	19-Apr-00	13:56:08	hme2	A.B.C.1	log	drop	nbname	208.46.190.14	Y.Z.70.26	udp
234428	19-Apr-00	13:57:10	hme2	A.B.C.1	log	drop	nbname	208.46.190.14	Y.Z.3.9	udp

TARGETING:

YES – These packets are directed at internal web servers and primary domain controllers.

EXISTENCE:

The Source network is a small (Class C) network that belongs to Qwest.

HISTORY:

No previous history of inappropriate activity from this source IP address known.

TECHNIQUES:

Regular connection attempts every 2 minutes on the nbname port for an extended period of time with intermixed http connection attempts at seemingly random intervals. None of these ports/IP addresses are/should be accessible externally.

ANALYSIS:

These target ports and IP address are typically used by internal NT/MS2000 systems for network connectivity. The source IP address is that of an ISP.

INTENT/THREAT ASSESSMENT:

The short answer: Minimal threat. I suspect that this traffic is generated by an employee's laptop system when connected to their personal ISP (along with Detect #2, this is starting to indicate a trend).

DETECT #4 – MANY MAIL PROBLEMS

LOG EXCERPT:

Ref.#	Date	Time	Intf.	Origin	Type	Action	Port	Source	Destination	Protocol
10261	19-Apr-00	0:29:57	hme2	A.B.C.1	log	drop	http	anchor-post-30.mail.demon.net	A.B.C.176	tcp
10264	19-Apr-00	0:29:58	hme2	A.B.C.1	log	drop	28800	anchor-post-30.mail.demon.net	A.B.C.176	tcp
10268	19-Apr-00	0:29:59	hme2	A.B.C.1	log	drop	16715	anchor-post-30.mail.demon.net	A.B.C.176	tcp
10274	19-Apr-00	0:30:00	hme2	A.B.C.1	log	drop	http	anchor-post-30.mail.demon.net	A.B.C.176	tcp
<snip>										
11545	19-Apr-00	0:34:29	hme2	A.B.C.1	log	drop	http	deliver-5.tiptree.jobserve.com	A.B.C.176	tcp
11957	19-Apr-00	0:35:55	hme2	A.B.C.1	log	drop	51680	deliver-5.tiptree.jobserve.com	A.B.C.176	tcp
12039	19-Apr-00	0:36:19	hme2	A.B.C.1	log	drop	45933	deliver-5.tiptree.jobserve.com	A.B.C.176	tcp
12104	19-Apr-00	0:36:33	hme2	A.B.C.1	log	drop	2336	deliver-5.tiptree.jobserve.com	A.B.C.176	tcp
<snip>										
20203	19-Apr-00	1:04:52	hme2	A.B.C.1	log	drop	6346	deliver-5.tiptree.jobserve.com	A.B.C.176	tcp
20320	19-Apr-00	1:05:14	hme2	A.B.C.1	log	drop	28810	deliver-5.tiptree.jobserve.com	A.B.C.176	tcp
20661	19-Apr-00	1:06:30	hme2	A.B.C.1	log	drop	2628	deliver-5.tiptree.jobserve.com	A.B.C.176	tcp
28356	19-Apr-00	1:33:55	hme2	A.B.C.1	log	drop	37125	....dsl.snfc21.pacbell.net	A.B.C.176	tcp
28756	19-Apr-00	1:35:08	hme2	A.B.C.1	log	drop	37125	....dsl.snfc21.pacbell.net	A.B.C.176	tcp

TARGETING:

YES -- All packets are targeting one specific system -- our primary mail gateway.

EXISTENCE:

Review of the entire log revealed that these packets originated from 5 different IP addresses. Four of these were in the UK (from two different networks) and the last one was from the West Coast of the US.

HISTORY:

No previous history of inappropriate activity from these source IP addresses known.

TECHNIQUES:

Clearly directed from mail servers to our primary mail server. Uses a variety of seemingly random ports, but frequently tries port 80 (http). Scans were in serial (not parallel) from these systems although the ports were not repeated (except http and 27005). The first four systems scans were separated by less than 2 minutes. The last system scan (from a totally different network) was separated by about 25 minutes. Again, ports were NOT duplicated by **any** of these systems (with the exception of ports 80 and 27005).

ANALYSIS:

This indicates the use of several systems and networks to do a coordinated, comprehensive system scan of our primary mail gateway. Since this traffic was NOT seen to other systems, (such as our secondary mail server), and they apparently originated from other mail related systems, one possibility would be that this scan was an attempt to scout our system for vulnerabilities to specifically compromise our e-mail infrastructure. Another possibility would be that this is a “verification” service that check’s mail relays for blacklist purposes although the distributed nature of this detect opposes this.

INTENT/THREAT ASSESSMENT:

Short Answer: Moderate to High Threat.
Detail: Although these systems are individually protected as well as behind a firewall, this was a VERY specific, and well coordinated attack. This alert definitely requires follow-up.

DETECT #5 – I HATE YOU, YOUR SERVER MUST DIE.

LOG EXCERPT:

Ref.#	Date	Time	Interf.	Origin	Type	Action	Port	Source	Destination	Protocol
2470	19-Apr-00	0:02:51	hme2	A.B.C.1	log	drop	16536	irc.nethead.com	Y.Z.158.116	tcp
2471	19-Apr-00	0:02:52	hme2	A.B.C.1	log	drop	51211	irc.nethead.com	Y.Z.146.72	tcp
2476	19-Apr-00	0:02:52	hme2	A.B.C.1	log	drop	14669	irc.nethead.com	Y.Z.129.117	tcp
2488	19-Apr-00	0:02:54	hme2	A.B.C.1	log	drop	30552	irc.nethead.com	Y.Z.203.75	tcp
<snip>										
7166	19-Apr-00	0:18:45	hme2	A.B.C.1	log	drop	42202	irc.nethead.com	Y.Z.120.111	tcp
7218	19-Apr-00	0:18:55	hme2	A.B.C.1	log	drop	42127	irc.nethead.com	Y.Z.115.33	tcp
7242	19-Apr-00	0:18:58	hme2	A.B.C.1	log	drop	17976	irc.nethead.com	Y.Z.108.31	tcp
7266	19-Apr-00	0:19:03	hme2	A.B.C.1	log	drop	18322	irc.nethead.com	Y.Z.85.18	tcp
7297	19-Apr-00	0:19:12	hme2	A.B.C.1	log	drop	62232	irc.nethead.com	Y.Z.112.90	tcp
115538	19-Apr-00	5:10:53	hme2	A.B.C.1	log	drop	56341	irc.nethead.com	Y.Z.243.59	tcp
115898	19-Apr-00	5:12:29	hme2	A.B.C.1	log	drop	56341	irc.nethead.com	Y.Z.243.59	tcp
115899	19-Apr-00	5:12:30	hme2	A.B.C.1	log	drop	12979	irc.nethead.com	Y.Z.59.83	tcp
115923	19-Apr-00	5:12:34	hme2	A.B.C.1	log	drop	41216	irc.nethead.com	Y.Z.105.54	tcp
115974	19-Apr-00	5:12:48	hme2	A.B.C.1	log	drop	57973	irc.nethead.com	Y.Z.167.137	tcp
115988	19-Apr-00	5:12:49	hme2	A.B.C.1	log	drop	16979	irc.nethead.com	Y.Z.17.247	tcp

…

TARGETING:
YES

EXISTENCE:
The source IP address belongs to an ISP in Seattle. They're a hosting facility.

HISTORY:
No previous history of inappropriate activity from the source IP address is known.

TECHNIQUES:
Slow, deliberate, packets ranging over our entire class B network and over a variety of ports. There is no pattern readily noticeable.

ANALYSIS:
This is typical of several network-mapping programs available including NMAP. This is possibly a scouting scan in preparation for a directed attack. Upon contact with the ISP, they have indicated that they are receiving numerous complaints regarding this system. It appears that these packets are being spoofed for personality conflict reasons (I hate you, so your server must die). Capturing any additional raw packets (not just Firewall logs) would help further analysis.

INTENT/THREAT ASSESSMENT:
Short Answer: Moderate Threat.
Detail: These systems and these networks are protected by a firewall, and the owners of the network have indicated an … unhappy history with this system. This is NOT a low risk, however as it still presents a potentially successful network mapping mission.

DETECT #6 – ANOTHER ONE!?

LOG EXCERPT:

Ref. #	Date	Time	Inter.	Origin	Type	Action	Port	Source	Destination	Protocol
8	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	54666	212.108.4.152	Y.Z.196.118	tcp
13	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	30629	212.108.4.152	Y.Z.161.120	tcp
17	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	19664	212.108.4.152	Y.Z.104.27	tcp
42	18-Apr-00	23:54:39	hme2	A.B.C.1	log	drop	23751	212.108.4.152	Y.Z.102.125	tcp
99	18-Apr-00	23:54:50	hme2	A.B.C.1	log	drop	31532	212.108.4.152	Y.Z.54.97	tcp
180	18-Apr-00	23:55:04	hme2	A.B.C.1	log	drop	48953	212.108.4.152	Y.Z.230.39	tcp
497	18-Apr-00	23:56:21	hme2	A.B.C.1	log	drop	25361	212.108.4.152	Y.Z.56.97	tcp
506	18-Apr-00	23:56:25	hme2	A.B.C.1	log	drop	8889	212.108.4.152	Y.Z.150.72	tcp
613	18-Apr-00	23:56:46	hme2	A.B.C.1	log	drop	45736	212.108.4.152	Y.Z.54.21	tcp
624	18-Apr-00	23:56:48	hme2	A.B.C.1	log	drop	41492	212.108.4.152	Y.Z.34.120	tcp
692	18-Apr-00	23:57:00	hme2	A.B.C.1	log	drop	65376	212.108.4.152	Y.Z.135.16	tcp
1084	18-Apr-00	23:58:24	hme2	A.B.C.1	log	drop	gopher	212.108.4.152	A.B.C.19	tcp
1112	18-Apr-00	23:58:31	hme2	A.B.C.1	log	drop	1004	212.108.4.152	Y.Z.200.80	tcp

TARGETING:

YES – These packets are specifically directed at our Class C and Class B networks.

EXISTENCE:

This IP address is one of a class C registered to “Comned Networks B.V.” (Netherlands).

HISTORY:

No previous history of inappropriate activity from the source IP address is known.

TECHNIQUES:

Very distributed/randomized scan of multiple ports and multiple IP addresses with no specific pattern discernable. This scan is extremely similar to Detect #5

ANALYSIS:

This is typical of several network-mapping programs available including NMAP. One indicator that this is a specifically targeted scan is our public address range being included in this scan. This is possibly a scouting session in preparation for a directed attack. As with Detect #5, there is also the possibility that these packets are being spoofed for denial of service attack purposes.

INTENT/THREAT ASSESSMENT:

Short Answer: Moderate to High Threat.
Detail: These systems and these networks are protected by a firewall, however, this is an deliberate scouting scan. This will require follow up with the owners of this IP address. As with Detect #5, capturing any additional raw packets (not just Firewall logs) would help further analysis.

DETECT #7 – UT-OH, WHAT'S ON PORT 27015?

LOG EXCERPT:

Ref#	Date	Time	Int.	Origin	Type	Act.	Port	Source	Destination	Protocol
7	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...dialup.earthlink.net	Y.Z.30.75	udp
9	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...tx.home.com	Y.Z.30.75	udp
10	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...bolivar.wilkshire.net	Y.Z.30.75	udp
14	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...mn.home.com	Y.Z.30.75	udp
16	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...ipt.aol.com	Y.Z.30.75	udp
19	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...stny.rr.com	Y.Z.30.75	udp
20	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...splitrock.net	Y.Z.30.75	udp
23	18-Apr-00	23:54:37	hme2	A.B.C.1	log	drop	27015	...saturn.bbn.com	Y.Z.30.75	udp
25	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...tampabay.rr.com	Y.Z.30.75	udp
26	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...sdf.bellsouth.net	Y.Z.30.75	udp
29	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...abo.wanadoo.fr	Y.Z.30.75	udp
30	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...49.152.87	Y.Z.30.75	udp
31	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...ipt.aol.com	Y.Z.30.75	udp
32	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...res.iastate.edu	Y.Z.30.75	udp
33	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...adsl.bellglobal.com	Y.Z.30.75	udp
34	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...RipNET.com	Y.Z.30.75	udp
38	18-Apr-00	23:54:38	hme2	A.B.C.1	log	drop	27015	...nconnect.net	Y.Z.30.75	udp

TARGETING:

YES

EXISTENCE:

The Source IP addresses are WAY too numerous to begin research. There are dozens of hosts and dozens of ISP's included in this detect. The Source IP address is internal and unreachable from any external networks.

HISTORY:

No previous history of inappropriate activity from the source IP address nor the destination address is known.

TECHNIQUES:

An immense number of UDP connection attempts. All on a single port (27015) and all to a single IP address, but from literally hundreds of different Source addresses.

ANALYSIS:

My first thought was some form of denial of service or trojan – this was, however, improbable since the Destination IP address is unreachable on ANY ports/protocols by external systems. Contact with the system administrator revealed that this system was set up as an "Halflife" server and was publicly advertised on a master game server as a multi-player system. The result was that hundreds of players were attempting to reach this server because of its "killer" ping time. Too bad it wasn't accessible. Most amusing – reminds me of ping.symantec.com.

INTENT/THREAT ASSESSMENT:

Low Threat. The system was shut down and the public listing removed.

DETECT #8 – NETGAZER? DON'T THEY MEAN NETSCANNER?

LOG EXCERPT:

Ref.#	Date	Time	Int.	Origin	Type	Act.	Port	Source	Destination	Protocol
17766	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1100	...netgazer.com.ph	X.Y.Z.22	tcp
17767	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1101	...netgazer.com.ph	X.Y.Z.22	tcp
17768	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1102	...netgazer.com.ph	X.Y.Z.22	tcp
17769	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	xaudio	...netgazer.com.ph	X.Y.Z.22	tcp
17771	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1104	...netgazer.com.ph	X.Y.Z.22	tcp
17772	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1105	...netgazer.com.ph	X.Y.Z.22	tcp
17773	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1106	...netgazer.com.ph	X.Y.Z.22	tcp
17774	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1107	...netgazer.com.ph	X.Y.Z.22	tcp
17775	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1108	...netgazer.com.ph	X.Y.Z.22	tcp
17777	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1109	...netgazer.com.ph	X.Y.Z.22	tcp
17779	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1110	...netgazer.com.ph	X.Y.Z.22	tcp
17780	19-Apr-00	0:56:56	hme2	A.B.C.1	log	drop	1111	...netgazer.com.ph	X.Y.Z.22	tcp
17782	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1112	...netgazer.com.ph	X.Y.Z.22	tcp
17783	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1113	...netgazer.com.ph	X.Y.Z.22	tcp
17784	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1114	...netgazer.com.ph	X.Y.Z.22	tcp
17785	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1115	...netgazer.com.ph	X.Y.Z.22	tcp
17786	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1116	...netgazer.com.ph	X.Y.Z.22	tcp
17788	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1117	...netgazer.com.ph	X.Y.Z.22	tcp
17789	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1118	...netgazer.com.ph	X.Y.Z.22	tcp
17790	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1119	...netgazer.com.ph	X.Y.Z.22	tcp
17791	19-Apr-00	0:56:57	hme2	A.B.C.1	log	drop	1120	...netgazer.com.ph	X.Y.Z.22	tcp

TARGETING:

YES

EXISTENCE:

This IP address belongs to an ISP in the Philippines. Most likely handed out to a dialup customer.

HISTORY:

No previous history of inappropriate activity from the source IP address is known.

TECHNIQUES:

Very fast, sequential port-scan of one specific system. Definitely not using the standard TCP stack to submit/receive packets as there are >10 packets per second.

ANALYSIS:

Since this scan was only directed at one system (a web server), this was likely a post scan to determine A) what type of system is it, B) Are there any hidden web/ftp/other servers, or C) What can be exploited on the system.

INTENT/THREAT ASSESSMENT:

The short answer: Low to Moderate Threat. This system and this network are firewall protected, however, this is a deliberate system scan.

DETECT #9 – SWBELL, ISN'T THAT SWELL.

LOG EXCERPT:

Ref.#	Date	Time	Inter.	Origin	Type	Action	Port	Source	Destination	Protocol
10326	19-Apr-00	0:30:10	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.1	udp
10371	19-Apr-00	0:30:22	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.2	udp
10440	19-Apr-00	0:30:35	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.3	udp
10503	19-Apr-00	0:30:44	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.4	udp
10580	19-Apr-00	0:31:01	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.5	udp
<snip>										
23744	19-Apr-00	1:17:48	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.251	udp
23783	19-Apr-00	1:17:57	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.252	udp
23822	19-Apr-00	1:18:06	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.253	udp
23860	19-Apr-00	1:18:15	hme2	A.B.C.1	log	drop	nbname	...dsl.rcsntx.swbell.net	Y.Z.200.254	udp

TARGETING:

YES

EXISTENCE:

The Source IP address is (as long as it's not spoofed) is obviously from a dsl account of Southwest Bell's Internet Services.

HISTORY:

No previous history of inappropriate activity from the source IP address is known.

TECHNIQUES:

Very deliberate, moderate speed, sequential scan of one specific Class C subnet. This is also only on the nbname port.

ANALYSIS:

This is detect is typical of a Legion scan. This person is either scanning for Windows system shares (then potentially hoping to exploit them) or has made a really bad guess on choosing a port to do a general scan with. Either way, this is an obvious host scan of a complete Class C subnet.

INTENT/THREAT ASSESSMENT:

The short answer: Moderate Threat. Although these systems are firewall protected, this is a potential prelude to some form of directed intrusion attempt.

DETECT #10 – PORT SCAN? WE DON'T NEED NO STINKIN' PORT SCAN.

LOG EXCERPT:

Ref. #	Date	Time	Inter.	Origin	Type	Action	Port	Source	Destination	Protocol
22456	19-Apr-00	1:13:04	hme2	A.B.C.1	log	drop	33465	200.225.26.177	A.B.C.100	udp
22481	19-Apr-00	1:13:09	hme2	A.B.C.1	log	drop	33466	200.225.26.177	A.B.C.100	udp
22508	19-Apr-00	1:13:14	hme2	A.B.C.1	log	drop	33467	200.225.26.177	A.B.C.100	udp
22525	19-Apr-00	1:13:19	hme2	A.B.C.1	log	drop	33468	200.225.26.177	A.B.C.100	udp
22557	19-Apr-00	1:13:24	hme2	A.B.C.1	log	drop	33469	200.225.26.177	A.B.C.100	udp
23687	19-Apr-00	1:17:34	hme2	A.B.C.1	log	drop	33519	200.225.26.177	A.B.C.100	udp
23708	19-Apr-00	1:17:39	hme2	A.B.C.1	log	drop	33520	200.225.26.177	A.B.C.100	udp
23727	19-Apr-00	1:17:44	hme2	A.B.C.1	log	drop	33521	200.225.26.177	A.B.C.100	udp
23748	19-Apr-00	1:17:48	hme2	A.B.C.1	log	drop	33522	200.225.26.177	A.B.C.100	udp
23766	19-Apr-00	1:17:54	hme2	A.B.C.1	log	drop	33523	200.225.26.177	A.B.C.100	udp
23786	19-Apr-00	1:17:59	hme2	A.B.C.1	log	drop	33524	200.225.26.177	A.B.C.100	udp

TARGETING:
YES

EXISTENCE:
Single IP address in Brazil.

HISTORY:
No previous history of inappropriate activity from the source IP address is known.

TECHNIQUES:
Similar to Detect #9 in that this is a very deliberate, moderate speed, sequential scan. This Detect, however, is sequentially scanning each port of a single system.

ANALYSIS:
Further research indicated that this was the ONLY system scanned by this Source IP address that day. This is very similar to Detect #8. Since this is also a publicly accessed web server system, it is likely that this person was, again, attempting to determine A) what type of system is it, B) are there any hidden web/ftp/other servers, and/or C) what can be exploited on the system.

INTENT/THREAT ASSESSMENT:
The short answer: Low to Moderate Threat. This system and this network is protected by a firewall, however, this is a deliberate system scan.

DETECT #11 – ONE MORE FOR THE FUN OF IT!

LOG EXCERPT:

Ref. #	Date	Time	Inter.	Origin	Type	Action	Port	Source	Destination	Protocol
29744	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.80	tcp
29745	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.92	tcp
29746	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.93	tcp
29747	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.81	tcp
29748	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.94	tcp
29749	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.82	tcp
29750	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.95	tcp
29751	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.83	tcp
29752	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.96	tcp
29753	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.84	tcp
29754	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.97	tcp
29755	19-Apr-00	1:38:39	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.0.90	tcp
<snip>										
63861	19-Apr-00	1:43:04	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.255.239	tcp
63862	19-Apr-00	1:43:04	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.255.240	tcp
63863	19-Apr-00	1:43:04	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.255.241	tcp
63864	19-Apr-00	1:43:04	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.255.242	tcp
63865	19-Apr-00	1:43:04	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.255.243	tcp
63866	19-Apr-00	1:43:04	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.255.244	tcp
63867	19-Apr-00	1:43:04	hme2	A.B.C.1	log	drop	98	210.205.121.47	Y.Z.255.245	tcp

TARGETING:

YES

EXISTENCE:

This IP address belongs to a Korean organization called “ULINELAIM”

HISTORY:

No previous history of inappropriate activity from the source IP address is known.

TECHNIQUES:

VERY fast, very obvious complete Class B network host scan. An interesting point about this scan is that the port of choice is port 98 (tacnews).

ANALYSIS:

After flagging this scan, a co-worker of mine indicated that he’d also heard of these scans recently in military circles as well. MS Exchange servers run their X.400 connections on port 98 (and some UNIX systems run RPC commands through port 98 as well). Exchange servers are probably more common and frequently configured to use X.400 connections. Since Exchange can also have web based functions (and those require IIS), this would be an excellent way to identify potential IIS servers for future exploitation.

INTENT/THREAT ASSESSMENT:

The short answer: Moderate Threat.
Details: While this scan was (presumably) unsuccessful because of the firewall protection, this was a complete network scan as well as representing a upcoming intrusion attempt. This one definitely requires a nastygram to be delivered to the IP address owner.

Last Updated: May 28th, 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 Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 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 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