Global Information Assurance Certification Paper

SNAP Level One Certification Practical

Intrusion Detection: 10 Detects with Analyses

Carl F. Endorf

April 12, 2000

Scan 1

10:28:06.049920 207.207.3.158.1027 > 172.16.3.14.34716: udp 546
10:30:19.967384 207.207.3.158.1032 > 172.16.3.14.34716: udp 546
….
10:48:50.597404 207.207.3.158.1103 > 172.16.3.14.34716: udp 546
10:52:36.613724 207.207.3.158.1097 > 172.16.3.14.34716: udp 546

Source: GIAC

History: Not known

Techniques: UDP scan

Intent: To find what UDP services are available on the host.

Targeting: YES

Analysis: Appears that these packets have an unusually large payload attached to them. Static source port. Timed a few minutes a part. Appears to be a slow and low manual UDP port scan to 172.16.3.14

Scan 2

23:32:07.006546 20x.xxx.162.156.64322> 20x.xxx.145.118.53: S 1808832000: 1808832000 (0) win 512
23:32:07.007256 20x.xxx.162.156.64322> 20x.xxx.145.122.53: S 1808832000: 1808832000 (0) win 512
23:32:07.007326 20x.xxx.162.156.64322> 20x.xxx.145.123.53: S 1808832000: 1808832000 (0) win 512
23:32:07.007344 20x.xxx.162.156.64322> 20x.xxx.145.139.53: S 1808832000: 1808832000 (0) win 512
23:32:07.008210 20x.xxx.162.156.64322> 20x.xxx.145.141.53: S 1808832000: 1808832000 (0) win 512
23:32:07.008254 20x.xxx.162.156.64322> 20x.xxx.145.146.53: S 1808832000: 1808832000 (0) win 512
23:32:07.008341 20x.xxx.162.156.64322> 20x.xxx.145.149.53: S 1808832000: 1808832000 (0) win 512
……..

Source: Windump

History: None known.

Techniques: This appears to be a network scan. The sequence numbers do not change and it all happens in a small amount of time.

Intent: Yes, scan for DNS on port 53

Targeting: Yes

Analysis: Appears that someone has crafted packets for a DNS scan of port 53, due to high speed probably some sort of script.

Scan 3

```
2Apr2000 13:11:21 208.53.30.146 3921 > x.x.x.32 445 tcp
2Apr2000 13:11:21 208.53.30.146 3922 > x.x.x.32 139 tcp
2Apr2000 13:11:42 208.53.30.146 3923 > x.x.x.33 445 tcp
2Apr2000 13:11:42 208.53.30.146 3924 > x.x.x.33 139 tcp
2Apr2000 13:12:03 208.53.30.146 3925 > x.x.x.34 445 tcp
2Apr2000 13:12:03 208.53.30.146 3926 > x.x.x.34 139 tcp
```

History: None known

Techniques: TCP port scan.

Intent: Yes

Targeting: YES

Analysis: Source unreachable, static source IP, scanning same network and ports sequentially indicates that this is a definite port scan. The time difference between each scan may suggest a scripted attack as they are all apart by 21 seconds exactly.

Scan 4

```
 Mar 29 18:39:31 morton kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3224 xxx.xxx.xxx.201:23 L=44 S=0x00 I=32765 F=0x4000 T=43 SYN

Mar 29 18:39:31 pooky kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3230 xxx.xxx.xxx.204:23 L=44 S=0x00 I=32778 F=0x4000 T=43

Mar 29 18:39:31 www kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3231 xxx.xxx.xxx.205:23 L=44 S=0x00 I=32782 F=0x4000 T=43 SYN

Mar 29 18:39:33 morton kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3224 xxx.xxx.xxx.201:23 L=44 S=0x00 I=33116 F=0x4000 T=43 SYN

Mar 29 18:39:34 pooky kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3230 xxx.xxx.xxx.204:23 L=44 S=0x00 I=33123 F=0x4000 T=43

Mar 29 18:39:34 www kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3231 xxx.xxx.xxx.205:23 L=44 S=0x00 I=33124 F=0x4000 T=43 SYN

Mar 29 18:39:40 morton kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3224 xxx.xxx.xxx.201:23 L=44 S=0x00 I=33833 F=0x4000 T=43 SYN

Mar 29 18:39:40 pooky kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3230 xxx.xxx.xxx.204:23 L=44 S=0x00 I=33841 F=0x4000 T=43

Mar 29 18:39:40 www kernel: Packet log: input DENY eth0 PROTO=6
212.32.167.56:3231 xxx.xxx.xxx.205:23 L=44 S=0x00 I=33842 F=0x4000 T=43 SYN
```

Source: GIAC

History: Not Known

Techniques: Telnet attempts

Intent: To see if they can telnet into the system

Targeting: YES

Analysis: Someone making an attempt to Telnet into this system on port 23, trying consecutive hosts. I guess you could call it a telnet scan to see what boxes are vulnerable.

Scan 5

16:25:26.235	IP-x.x.x.x:10 :4B:FE:DA:B8	61521	IP-10.xx.1.2 :50:04:8C:C8:99	423	IP UDP	64	
16:25:26.235	IP-x.x.x.x:10 :4B:FE:DA:B8	61521	IP-10.xx.1.2 :50:04:8C:C8:99	410	IP UDP	64	
16:25:26.235	IP-10.xx.1.2 :50:04:8C:C8:99		IP-x.x.x.x:10 :4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: x.x.x.x
16:25:26.235	IP-10.xx.1.2 :50:04:8C:C8:99		IP-x.x.x.x:10 :4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: x.x.x.x
16:25:26.235	IP-10.xx.1.2 :50:04:8C:C8:99		IP-x.x.x.x:10 :4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: x.x.x.x
16:25:26.235	IP-x.x.x.x:10:4B:FE:DA:B8	61521	IP-10.xx.1.2 :50:04:8C:C8:99	484	IP UDP	64	
16:25:26.235	IP-x.x.x.x:10:4B:FE:DA:B8	61521	IP-10.xx.1.2 :50:04:8C:C8:99	432	IP UDP	64	
16:25:26.235	IP-x.x.x.x:10:4B:FE:DA:B8	61521	IP-10.xx.1.2 :50:04:8C:C8:99	548	IP UDP	64	
16:25:26.235	IP-10.xx.1.2 :50:04:8C:C8:99		IP-x.x.x.x:10 :4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: x.x.x.x:10
16:25:26.236	IP-10.xx.1.2 :50:04:8C:C8:99		IP-x.x.x.x:10 :4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: x.x.x.x:10
16:25:26.236	IP-x.x.x.x:10:4B:FE:DA:B8	61521	IP-10.xx.1.2 :50:04:8C:C8:99	454	IP UDP	64	
16:25:26.236	IP-10.xx.1.2 :50:04:8C:C8:99		IP-x.x.x.x:10 :4B:FE:DA:B8		ICMP DUnr	74	Port unreachable: x.x.x.x:10

History: None

Techniques: UDP Port scan

Intent: Yes

Targeting: Yes

Analysis: This attack is trying to connect and do a UDP scan and getting a port unreachable ICMP. The attacker is using high port 61521.

Scan 6

24.148.17.23 11 0408 1E61 13K 24-148-17-23.NA.21STCENTURY.NET
24.218.179.25 11 0613 1E61 10K H0050BAD1ECB2.NE.MEDIAONE.NET
62.155.190.215 11 040E 1E61 29K P3E9BBED7.DIP0.T-IPCONNECT.DE
151.189.139.148 11 0BC9 1E61 21K PP.139.148.FRA.GERMANYNET.DE
166.49.44.28 11 4552 1B40 10K RBN3.WASHINGTONEAST.CW.NET
194.251.249.169 11 1518 0BE1 22K VESIKAUHU.TMT.TELE.FI
199.239.30.62 11 5306 1B3A 10K *VERIO.NET
206.190.43.26 11 043B 1B3B 10K *.BROADCAST.COM
206.253.222.226 11 3E82 1B3A 10K *.PNAP.NET
206.253.222.226 11 3E82 1B3A 16K *.PNAP.NET
207.115.62.45 11 0000 0538 10K VIDEO.PSEUDO.COM
207.115.62.45 11 0000 0000 19K VIDEO.PSEUDO.COM
209.185.245.7 11 36B2 1B3E 15K *.EXODUS.NET
209.185.245.7 11 36B2 1B3E 18K *.EXODUS.NET
209.246.41.140 11 288A 1B3A 11K *.LEVEL3.NET
210.94.0.147 11 0000 0000 16K *.HANAROTEL.NET
210.94.0.147 11 0000 0000 22K *.HANAROTEL.NET

210.94.0.147 11 0000 0000 11K *.HANAROTEL.NET
211.40.176.205 11 5D43 1B3A 34K *.BORA.NET
211.40.176.197 11 5BD8 1B3A 46K *.BORA.NET
213.171.129.135 11 08AB 1E61 29K *.SUPERWEB.NL
216.2.9.4 11 6D62 078E 12K RADIUS2.CITYISP.NET
216.63.218.84 11 05F8 1E61 25K ADSL-216-63-218-84.DSL.CRCHTX.SWBELL.NET
216.78.216.47 11 045B 1E61 19K ADSL-78-216-47.RDU.BELLSOUTH.NET
216.78.216.47 11 0414 1E61 21K ADSL-78-216-47.RDU.BELLSOUTH.NET

Source=GIAC

History: Unknown

Techniques: UDP flood

Intent: Yes

Targeting: Yes

Analysis: Large volumes of UDP packets coming from several sites to many hosts on the network, flooding UDP port 11. Malicious intent. DOS attack if successful.

Scan 7

Mar 29 21:48:34 209-30-73-81.flash.net ASCEND: wan2 tcp 09.30.73.81;12345 <- 211.45.208.151;3647 62 syn !pass (totcp-1)
Mar 29 21:48:39 209-30-73-81.flash.net ASCEND: wan3 tcp 209.30.73.82;12345 <- 211.45.208.151;3648 62 syn !pass (totcp-1)
Mar 29 21:48:44 209-30-73-81.flash.net ASCEND: wan3 tcp 209.30.73.83;12345 <- 211.45.208.151;3649 62 syn !pass (totcp-1)
Mar 29 21:48:49 209-30-73-81.flash.net ASCEND: wan3 tcp 209.30.73.84;12345 <- 211.45.208.151;3650 62 syn !pass (totcp-1)
Mar 29 21:48:54 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.85;12345 <- 211.45.208.151;3651 62 syn !pass (totcp-1)
Mar 29 21:48:59 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.86;12345 <- 211.45.208.151;3652 62 syn !pass (totcp-1)
Mar 29 21:49:04 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.87;12345 <- 211.45.208.151;3653 62 syn !pass (totcp-1)
Mar 29 21:49:09 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.88;12345 <- 211.45.208.151;3654 62 syn !pass (totcp-1)
Mar 29 21:49:14 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.89;12345 <- 211.45.208.151;3655 62 syn !pass (totcp-1)
Mar 29 21:49:19 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.90;12345 <- 211.45.208.151;3656 62 syn !pass (totcp-1)
Mar 29 21:49:24 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.91;12345 <- 211.45.208.151;3657 62 syn !pass (totcp-1)
Mar 29 21:49:29 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.92;12345 <- 211.45.208.151;3658 62 syn !pass (totcp-1)
Mar 29 21:49:34 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.93;12345 <- 211.45.208.151;3659 62 syn !pass (totcp-1)
Mar 29 21:49:40 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.94;12345 <- 211.45.208.151;3660 62 syn !pass (totcp-1)
Mar 29 21:49:45 209-30-73-81.flash.net ASCEND: wan2 tcp 209.30.73.95;12345 <- 211.45.208.151;3661 62 syn !pass (totcp-1)

Source=GIAC

History: Unknown

Techniques: TCP scan

Intent: Yes

Targeting: Yes

Analysis: TCP scan of consecutive ports all originating from same source IP. Source is all coming from same port 12345 which is flag.

Scan 8

03/30/2000 02:23:12 PM 192.XX8.8X.6 7521 > www.warpradio.com 6770 :UDP
03/30/2000 02:23:12 PM www.warpradio.com 7521 > 205.xxx.2x8.7 6770 :UDP
03/30/2000 02:23:12 PM 192.XX8.8X.6 7521 > www.warpradio.com 6770 :UDP

03/30/2000 02:23:12 PM 192.XX8.8X.6 7521 > www.warpradio.com 6770 :UDP
03/30/2000 02:23:12 PM 192.XX8.8X.6 7521 > www.warpradio.com 6770 :UDP
03/30/2000 02:23:12 PM 192.XX8.8X.6 7521 > www.warpradio.com 6770 :UDP
03/30/2000 02:23:12 PM www.warpradio.com 7521 > 205.xxx.2x8.7 6770 :UDP
03/30/2000 02:23:12 PM www.warpradio.com 7521 > 205.xxx.2x8.7 6770 :UDP

History: Seen and detected many times

Techniques: None, False Positive.

Intent: No

Targeting: No

Analysis: Set off alert as a UDP port scan, but was just some audio application coming across.

Scan 9

[2x9.xx.166.41] [2x9.xx.166.41] 60 0:00:00.000 0.000.000 03/30/2000 02:23:12 PM TCP: D=1592 S=80 SYN

[2x9.xx.166.41] [2x9.xx.166.41] 60 0:00:00.000 0.000.178 03/30/2000 02:23:12 PM TCP: D=1592 S=80 SYN

[2x9.xx.166.41] [2x9.xx.166.41] 60 0:00:00.000 0.000.108 03/30/2000 02:23:13 PM TCP: D=1592 S=80 SYN

History: Unknown

Techniques: Land attack attempt

Intent: Yes

Targeting: Yes

Analysis: This was an attempt at a Land attack that was caught at our firewall and not let through. Malicious intent, but unsuccessful.

Scan 10

Feb 22 15:01:39 dns1 telnetd[385244]:
refused connect from 212.25.118.45
Feb 22 15:01:45 dns1 ftpd[384361]:
refused connect from 212.25.118.45
Feb 22 15:01:54 dns1 portsentry[172871]: attackalert:

Connect from host: 212.25.118.45/212.25.118.45 to TCP port: 143

Feb 22 15:01:34 dns3 in.telnetd[22400]:
refused connect from 212.25.118.45
Feb 22 15:01:41 dns3 in.ftpd[22401]:
refused connect from 212.25.118.45
Feb 22 15:01:51 dns3 portsentry[301]: attackalert:
Connect from host: 212.25.118.45/212.25.118.45 to TCP port: 143

Source=GIAC

History: Unknown

Techniques: Blatant attempts to get unauthorized access to system.

Intent: Yes

Targeting: Yes

Analysis: 212.25.118.45 is trying, unsuccessfully to Telnet and Ftp into this system.

Last Updated: July 22nd, 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
SANS Seattle 2017	Seattle, WA	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
SANS San Diego 2017	San Diego, CA	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