Global Information Assurance Certification Paper

*** Northcutt, good use of a process, accuracy is fine though I would look at 8 carefully. The project is nicely laid out and the writing is clear enough. Shawn mostly picked easy ones and there isn't much evidence of research, correlation, or history. 72 *

GCIA Practical Certification

10 Detects with analysis SANS 2000

Shawn Beatty

April 20, 2000

Detect #1

Mar 27 17:01:03.516 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port 53050->5556): Restricted Port: Protocol=TCP[SYN] Port 53050->5556 (received on interface x.x.x.x)
Mar 27 17:01:03.516 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host1[x.x.x.x1]: Protocol=TCP[SYN] Port 53051->512): Restricted Port: Protocol=TCP[SYN] Port 53051->512 (received on interface x.x.x.x)
Mar 27 17:01:03.521 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port 53052->5556): Restricted Port: Protocol=TCP[SYN] Port 53052->5556 (received on interface x.x.x.x)
Mar 27 17:01:03.522 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->host2[x.x.x.x2]: Protocol=TCP[SYN] Port 53053->512): Restricted Port: Protocol=TCP[SYN] Port 53053->512 (received on interface x.x.x.x)
Mar 27 17:01:03.528 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port 53054->5556): Restricted Port: Protocol=TCP[SYN] Port 53054->5556 (received on interface x.x.x.x)
Mar 27 17:01:03.528 host kernel: 226 IP packet dropped (www7.clever.net[209.235.11.254]->x.x.x.x3: Protocol=TCP[SYN] Port 53055->512): Restricted Port: Protocol=TCP[SYN] Port 53055->512 (received on interface x.x.x.x)

Trace Information:	Detect from GIAC website
Active Targeting:	Yes
Intent:	User is scanning for specific open ports on a network.
Analysis:	This trace indicates the user from clever.net is looking for a response from ports 512 and 5556. 512 is the exec port I am unsure what 5556 is but would guess it is a Trojan of some sort as it is an unassigned port and the scan is specifically searching for it. Scan is happening very fast and incrementing by one on ip addresses. User is not targeting specific machines so he does not know what machines are live on the network.

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality:	3	*Does not know specific machines but knows ip address range*
Lethality:	2	*Only scanning at present time*
System Countermeasures:	3	*Unknown on this network*
Network Countermeasures:	5	*Firewall has 512 and 5556 restricted*
Severity:	-3	

Detect #2

Mar 27 12:33:28 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:28 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:33 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:38 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:43 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:48 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:53 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:33:58 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:03 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111
Mar 27 12:34:08 myhost portsentry[178]: attackalert:
Connect from host: na-165-5.na.avantel.net.mx/148.245.165.5
to UDP port: 111

Trace Information:	Detect from GIAC website
Active Targeting:	Yes
Intent:	User is communicating to specific internal host on UDP 111 SUNRPC
Analysis:	User appears to be actively communicating with internal host on sunrpc port. Communication continues for 2 minutes in trace, unfortunately we do not have all handshake information for this event. More information would be needed to know if data is being transferred after connects but this trace gives reason to be very concerned!

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality:	5	*Targeting a specific machine on a specific port*
Lethality:	5	*User is connecting*
System Countermeasures:	3	*Unknown on this network*
Network Countermeasures:	0	*External host is connecting*
Severity:	7	

Detect #3

02:44:11.342642 212.106.196.111 > MY_NET.196: icmp: echo request
02:44:11.352642 212.106.196.111 > MY_NET.197: icmp: echo request
02:44:11.372642 212.106.196.111 > MY_NET.198: icmp: echo request
02:44:11.472642 212.106.196.111 > MY_NET.202: icmp: echo request
02:44:11.632642 212.106.196.111 > MY_NET.208: icmp: echo request
02:44:11.692642 212.106.196.111 > MY_NET.209: icmp: echo request
02:44:11.942642 212.106.196.111 > MY_NET.215: icmp: echo request
02:44:12.182642 212.106.196.111 > MY_NET.220: icmp: echo request
02:44:12.192642 212.106.196.111 > MY_NET.221: icmp: echo request
02:44:12.292642 212.106.196.111 > MY_NET.223: icmp: echo request
02:44:12.442642 212.106.196.111 > MY_NET.227: icmp: echo request
02:44:12.572642 212.106.196.111 > MY_NET.232: icmp: echo request
02:44:12.592642 212.106.196.111 > MY_NET.233: icmp: echo request
02:44:12.692642 212.106.196.111 > MY_NET.237: icmp: echo request
02:44:12.722642 212.106.196.111 > MY_NET.238: icmp: echo request
02:44:12.752642 212.106.196.111 > MY_NET.240: icmp: echo request
02:44:12.942642 212.106.196.111 > MY_NET.245: icmp: echo request
02:44:12.962642 212.106.196.111 > MY_NET.246: icmp: echo request
02:44:12.982642 212.106.196.111 > MY_NET.247: icmp: echo request
02:44:13.072642 212.106.196.111 > MY_NET.250: icmp: echo request

Trace Information: Detect from GIAC website
Active Targeting: Yes
Intent: ICMP Scan of network
Analysis: Simple ICMP scan user does not know network and is just in the process of recon. The attack is very fast as 20 hosts are scanned in 2 seconds. User later scanned same hosts again using different technique.

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality:	3	*Early recon effort user is grasping for straws*
Lethality:	3	
System Countermeasures:	3	*Unknown on this network*
Network Countermeasures:	3	*Firewall should be in place blocking incoming ICMP*
Severity:	0	*While the severity is not extreme we should keep an eye on this user and future attempts to access network*

Detect #4

[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.982810 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:21 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.983871 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:20 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.984192 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:19 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.984867 203.239.122.1:53 -> 2XX.X.15.1:53

```
TCP TTL:18 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.985163 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:17 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.985842 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:16 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.986131 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:15 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.986810 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:14 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.987100 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:13 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.987779 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:12 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.988070 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:11 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
[**] IDS198/SYN FIN Scan [**]03/23-21:25:56.988745 203.239.122.1:53 -> 2XX.X.15.1:53
TCP TTL:10 TOS:0x0 ID:39426 **SF**** Seq: 0x56D48C26 Ack: 0x2694742E Win: 0x404
```

Trace Information: Detect from GIAC website
Active Targeting: Yes
Intent: Network mapping
Analysis: User is mapping network using DNS server to find out where it is located on the network. Packets are crafted SYN/FIN and are identical with the exception of the time and TTL. User is attempting to bypass security in place by sending SYN/FIN packets.

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality: 3 *Early recon user mapping network*
Lethality: 3
System Countermeasures: 3 *Unknown on this network*
Network Countermeasures: 3 *Intrusion detection system in place*
Severity: 0 *While the severity is not extreme we should keep an eye on this user and future attempts to access network*

Detect #5

```
Mar 20 13:48:21.150739 212.217.21.232,2888 -> 10.1.8.55,31337 PR udp len 20 47
Mar 20 13:48:24.020806 212.217.21.232,3073 -> 10.1.8.55,6670 PR tcp len 20 48 -S
Mar 20 13:48:24.029734 212.217.21.232,3074 -> 10.1.8.55,1080 PR tcp len 20 48 -S
Mar 20 13:48:24.045835 212.217.21.232,3075 -> 10.1.8.55,20034 PR tcp len 20 48 -S
Mar 20 13:48:24.056012 212.217.21.232,3076 -> 10.1.8.55,5742 PR tcp len 20 48 -S
Mar 20 13:48:24.057198 212.217.21.232,3072 -> 10.1.8.55,12345 PR tcp len 20 48 -S
```

Trace Information: Detect from GIAC website
Active Targeting: Yes
Intent: Searching for Trojans to answer requests
Analysis: User is targeting a specific machine for all trojans they can think of! BackOrifice, DeepThroat, Socks, NetBus2, WinCrash, and NetBus. The concern being that the user has picked a certain machine to attempt to run the exploits at. Would monitor further activity from this network to see if he is attempting connections to other hosts.

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality: 5 *User attempting to run trojan exploits*

Lethality:	3	*Don't see return traffic from host but still do not like people looking*
System Countermeasures:	3	*Unknown on this network*
Network Countermeasures:	3	*Intrusion detection system in place*
Severity:	2	*Not gaining access to machine but we should be on alert with this user*

Detect #6

112385 19APR2000 13:00:41 reject 8875 10.92.x.x 208.184.216.223 tcp 87 1768
112389 19APR2000 13:00:42 reject 8875 10.92.x.x 208.184.216.223 tcp 87 1771
112404 19APR2000 13:00:49 reject 8875 10.92.x.x 208.184.216.223 tcp 87 1772
112407 19APR2000 13:00:50 reject 8875 10.92.x.x 208.184.216.223 tcp 87 1773
112433 19APR2000 13:01:00 reject 8875 10.92.x.x 208.184.216.223 tcp 87 1774
112441 19APR2000 13:01:02 reject 8875 10.92.x.x 208.184.216.223 tcp 87 1775
…snip!

Trace Information:	Checkpoint FW-1 Log internal
Active Targeting:	Yes
Intent:	Host trying to connect to machine on port 8875
Analysis:	We started seeing quite a few of these connect attempts from our internal network to 208.184.216.223 on port 8875 from our internal network. Our initial thought was we had a Trojan that spread through our internal network…we were somewhat correct! Napster (MP3 sharing software) is the culprit here. The software attempts to communicate back to a home server to broadcast what files a user has to share to other Napster users.

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality:	2	*User attempting to use software as intended, could be bandwidth issues*
Lethality:	2	*Not malicious code but against company policy*
System Countermeasures:	5	*SMS should pick software up on users PC*
Network Countermeasures:	5	*Firewall is blocking communication on this port*
Severity:	-6	

Detect #7

Feb 29 12:29:49 host1 portsentry[524]: attackalert:
Connect from host: 206.x.x.x/206.x.x.x to UDP port: 31337
Feb 29 12:29:49 host1 portsentry[524]: attackalert:
Connect from host: 206.x.x.x/206.x.x.x to UDP port: 31337
Feb 29 12:29:49 host2 portsentry[420]: attackalert:
Connect from host: 206.x.x.x/206.x.x.x to UDP port: 31337
Feb 29 12:32:40 host3 portsentry[16512]: attackalert:
Connect from host: 206.x.x.x/206.x.x.x to UDP port: 31337

Trace Information:	Detect from GIAC website
Active Targeting:	Yes
Intent:	Host attempting to connect via Back Orifice
Analysis:	Back Orifice connection internal to network.. Perhaps co-workers finding too much time to mess with one another?

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality:	5	*Running trojan*
Lethality:	5	*Connection has been completed*
System Countermeasures:	0	*Trojan is installed*

Network Countermeasures: 4 *Able to pick up the traffic*
Severity: 6

Detect #8

Feb 12 05:17:28.515591 172.16.0.1,26758 -> 10.11.6.255,7 PR udp len 20 1052
Feb 12 05:17:33.612045 172.16.0.1,3617 -> 10.11.6.255,7 PR udp len 20 1052
Feb 12 05:17:38.712856 172.16.0.1,20151 -> 10.11.6.255,7 PR udp len 20 1052
Feb 12 05:17:43.812900 172.16.0.1,16726 -> 10.11.6.255,7 PR udp len 20 1052
…snip!

Trace Information: Detect from GIAC website
Active Targeting: Yes
Intent: Denial of service
Analysis: Hacker is attempting to talk to echo port on broadcast address the hope here is that he generates enough chatter to disrupt the network.

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity
Criticality: 2
Lethality: 2
System Countermeasures: 3
Network Countermeasures: 5
Severity: -4

Detect #9

Jan 17 04:55:26 cc1014244-a kernel: securityalert: tcp if=ef0 from 207.17.13.54:1920 to 24.x.x.x on unserved port 98
Jan 17 09:03:42 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.6.113.66:4880 to 24.x.x.x on unserved port 1243
Jan 17 09:36:35 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.132.53.111:25316 to 24.x.x.x on unserved port 109
Jan 17 13:22:15 cc1014244-a kernel: securityalert: tcp if=ef0 from 152.202.84.242:3857 to 24.x.x.x on unserved port 1243
Jan 17 15:15:58 cc1014244-a kernel: securityalert: tcp if=ef0 from 207.13.193.100:4595 to 24.x.x.x on unserved port 98
Jan 17 17:22:26 cc1014244-a kernel: securityalert: tcp if=ef0 from 63.17.161.209:2315 to 24.x.x.x on unserved port 27374
Jan 17 17:32:42 cc1014244-a kernel: securityalert: tcp if=ef0 from 207.153.9.234:2366 to 24.x.x.x on unserved port 1524
Jan 17 21:51:38 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.5.104.187:4110 to 24.x.x.x on unserved port 27374
Jan 17 22:50:26 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.4.154.21:1199 to 24.x.x.x on unserved port 27374
Jan 17 23:01:18 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.4.160.187:830 to 24.x.x.x on unserved port 111

Trace Information: Detect from GIAC website
Active Targeting: Yes
Intent: Scanning for exploits

Analysis:	User from netops.com looking for exploits on this poor guy's machine. Linuxconf, POP2,SUNRPC, etc. Probably multiple hacks here as the time is spread out over the day and similar attempts are being made. My guess would be that 24.x.x.x is visiting in the dens of thieves and they are taking their shots at him!

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality:	3	*If one of the exploits is successful this machine is owned*
Lethality:	3	*Until we see connecting traffic*
System Countermeasures:	3	*Unknown at this point*
Network Countermeasures:	4	*Network alarms in place*
Severity:	-1	

Detect #10

Jan 12 10:39:50 border-router 50121: 7w6d: %SEC-6-IPACCESSLOGP: list 102 denied tcp 212.59.15.107(4472) -> 256.23.109.1(80), 1 packet
Jan 12 10:39:53 border-router 50122: 7w6d: %SEC-6-IPACCESSLOGP: list 102 denied tcp 212.59.15.107(4471) -> 256.23.109.1(8080), 1 packet
Jan 12 10:39:53 border-router 50123: 7w6d: %SEC-6-IPACCESSLOGP: list 102 denied tcp 212.59.15.107(4551) -> 256.23.109.41(8080), 1 packet
Jan 12 10:39:56 border-router 50124: 7w6d: %SEC-6-IPACCESSLOGP: list 102 denied tcp 212.59.15.107(4527) -> 256.23.109.29(8080), 1 packet

Trace Information:	Detect from GIAC website
Active Targeting:	Yes
Intent:	Scanning proxy servers.
Analysis:	Proxy scan from a dialup user at takas.lt. Router is stopping the scans so not a ton to be worried about here. Just watch the public lists and make sure these addresses are not added to the trophy lists!

Severity of trace

(Criticality + Lethality) - (System Countermeasures + Network Countermeasures) = Severity

Criticality:	2	*Proxy search*
Lethality:	1	*Not getting past routers*
System Countermeasures:	3	*Router ACL's blocking traffic*
Network Countermeasures:	5	*Router ACL's blocking traffic*
Severity:	-5	

Last Updated: May 28th, 2017

Upcoming Training

SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 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