Global Information Assurance Certification Paper

SANS GIAC Certified Intrusion Analyst
Level 2 Practical Analysis

*** Northcutt, thanks for the extra research, that is quite helpful! Good use of an analysis process, clear, concise and accurate. 85 *

Name: **Jay Howie**

Date: **April 25 2000**
Submitted as the practical portion to accompany the SANS 2000 written exam taken (03/25/2000).

The traces used throughout this practical come from various sources (lab environment, home firewall, and the GIAC web site). The intent was to try to broaden my ability to examine different trace and log formats.

The I&W methodology is used to determine severity throughout the analysis process.

Severity will be determined using the following formula:

$$\text{Severity} = \frac{\text{(Criticality + Lethality)}}{\text{(System Countermeasures + Network Countermeasures)}}$$

Each area is measured on a scale of 0 (not severe) to 5 (very severe).

Criticality: Importance of targeted machine.
Lethality: Amount of potential damage inflicted if targeted machine gets compromised.
System Countermeasures: Host based defenses in place to prevent such an attack.
Network Countermeasures: Network based defenses in place to prevent such attack.

Analysis – 1 TCP PORT SCAN (Test Lab)

```
Apr 06 05:32:03 test.net unix: securityalert: tcp if=hme0 from source1:61232 to 206.116.94.75 on unserved port 21
Apr 06 05:32:03 test.net unix: securityalert: tcp if=hme0 from source1:61233 to 206.116.94.75 on unserved port 23
Apr 06 05:32:03 test.net unix: securityalert: tcp if=hme0 from source1:61234 to 206.116.94.75 on unserved port 150
Apr 06 05:32:04 test.net unix: securityalert: tcp if=hme0 from source1:61235 to 206.116.94.75 on unserved port 111
Apr 06 05:32:04 test.net unix: securityalert: tcp if=hme0 from source1:61236 to 206.116.94.75 on unserved port 1462
Apr 06 05:32:04 test.net unix: securityalert: tcp if=hme0 from source1:61237 to 206.116.94.75 on unserved port 159
```

Evidence of Active Targeting: Yes

History: Conducted in a lab environment.

Existence: Same source IP address seen throughout trace. This source IP address is one from my lab environment.

Technique: TCP Port Scan using the nmap tool. Very quick and powerful scanning tool easily available on the Internet.

Evidence of Intent: Information Gathering / Reconnaissance.

Analysis:

- Automated attack.
- Very quick, very little time between connection attempts.
- No spoofing of the source IP address.
- In this analysis, nmap was used to try to discover open TCP ports on a single system.
- The tool nmap, is a very powerful scanning tool with lots of configuration options; it is easily available on the Internet.
- One single source IP address used throughout going against one destination IP address.
- For more information regarding nmap check out: http://www.insecure.org/nmap

Severity:

(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 4) – (4 + 4) = 1

Criticality:	Targeted system.
Lethality:	Information could be used to mount an attack on open ports.
System Countermeasure:	Operating system running latest and greatest patch levels.
Network Countermeasure:	Firewall protecting internal network in lab environment.

Analysis – 2 ICMP ECHO REQUEST MAPPING (Test Lab)

```
11:13:23.615604 source1> x.x.x.255: icmp: echo request
11:13:23.618760 source1> x.x.x.0: icmp: echo request
11:13:23.626882 source1> x.x.x.255: icmp: echo request
11:13:23.641389 source1> x.x.x.0: icmp: echo request
11:13:23.657316 source1> x.x.x.255: icmp: echo request
11:13:24.679453 source1> x.x.x.0: icmp: echo request
11:13:24.682628 source1> x.x.x.255: icmp: echo request
11:13:24.689459 source1> x.x.x.0: icmp: echo request
```

Evidence of Active Targeting: Yes

History: Conducted in a lab environment.

Existence: Same source IP address. The source IP address is one from my lab environment.

Technique: Very quick scan. Looks like a script. In fact, nmap was used to create and send the ICMP packets.

Evidence of Intent: Information Gathering / Reconnaissance.

Analysis:

- Automated attack.
- Very quick, not much time between attempts.
- Tool can be used to map active hosts on a network.
- ICMP echo requests could be sent to each IP address in a network sequentially but this would take longer than the approach demonstrated above.
- Should not allow these types of packet into your network, should block at router or perimeter firewall. Disable these broadcasts.
- Source IP cannot be spoofed so they can receive the ICMP echo replies.
- For more information regarding nmap check out: http://www.insecure.org/nmap

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 4) – (4+4) = 1

Criticality:	Targeted network.
Lethality:	Information could be used to mount an attack on open ports.
System Countermeasure:	Operating systems running latest and greatest patch levels.
Network Countermeasure:	Firewall protecting network in lab environment.

Analysis – 3 SYN-FIN SCAN (GIAC Web Site)

```
Mar 4 17:30:28.902226 128.16.160.1,0 -> 10.0.1.1,109 PR tcp len 20 40 -SF
Mar 4 17:30:33.809050 128.16.160.1,0 -> 10.0.2.1,109 PR tcp len 20 40 -SF
Mar 4 17:30:38.907983 128.16.160.1,0 -> 10.0.3.1,109 PR tcp len 20 40 -SF
Mar 4 17:52:09.113368 128.16.160.1,0 -> 10.0.1.2,109 PR tcp len 20 40 -SF
Mar 4 17:52:14.214796 128.16.160.1,0 -> 10.0.2.2,109 PR tcp len 20 40 -SF
Mar 4 17:52:19.324670 128.16.160.1,0 -> 10.0.3.2,109 PR tcp len 20 40 -SF
Mar 4 18:13:44.425532 128.16.160.1,0 -> 10.0.0.3,109 PR tcp len 20 40 -SF
Mar 4 18:13:49.522489 128.16.160.1,0 -> 10.0.1.3,109 PR tcp len 20 40 -SF
Mar 4 18:13:54.606478 128.16.160.1,0 -> 10.0.2.3,109 PR tcp len 20 40 -SF
Mar 4 18:13:59.710369 128.16.160.1,0 -> 10.0.3.3,109 PR tcp len 20 40 -SF
Mar 4 18:35:24.989013 128.16.160.1,0 -> 10.0.0.4,109 PR tcp len 20 40 -SF
Mar 4 18:35:29.975789 128.16.160.1,0 -> 10.0.1.4,109 PR tcp len 20 40 -SF
Mar 4 18:35:34.998380 128.16.160.1,0 -> 10.0.2.4,109 PR tcp len 20 40 -SF
```

Evidence of Active Targeting: Yes

History: Trace taken from GIAC web site, no history was given.

Existence: Source port is the same throughout the trace. The source IP address (128.16.160.1) resolves to: sleipnir1.cs.ucl.ac.uk.

Technique: Use of a SYN-FIN scan with the source port 0. This scan is very slow and is trying to determine which machines have POP2 running. SYN FIN is not a legal TCP flag setting. The source port of 0 says to me that these packets are crafted. There is a sequence to this scan. It appears to be scanning hosts in 4 different class C subnets at the same time. It checks the x.x.0.1 before moving to x.x.1.1, x.x.2.1, x.x.3.1. Once it has completed this iteration it goes through each of the 4 subnets incrementing the final octet. This is definitely scripted.

Evidence of Intent: Information Gathering / Reconnaissance.

Analysis:

- Automated attack.
- Slow.
- Scripted, very sequential in nature (looking at 4 different class C subnets at the same time.
- Source IP address is the same throughout the trace.
- No spoofing of source address.
- Source port is 0, crafted packets.
- Attempt to map out machines that will respond to POP2 requests.
- Using non-legal SYN-FIN TCP flags, to perhaps bypass Firewall.
- Looking to get RST messages back to determine port availability.

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 4) – (4 + 4) = 1

Criticality:	Targeted networks.
Lethality:	Information could be used to mount an attack on open ports.
System Countermeasure:	OS should be running the latest patch levels.
Network Countermeasure:	Firewalls may be able to filter this out.

Analysis – 4 SUBSEVEN TROJAN SCAN (Home Linux FW)

```
Apr 04 07:26:14 riggs kernel: Packet log: input - eth0 PROTO=6 24.114.117.105:22619 x.x.x.x:27374 L=48 S=0x00
I=15306 F=0x4000 T=106
Apr 04 07:26:14 riggs kernel: Packet log: input - eth0 PROTO=6 24.114.117.105:22619 x.x.x.x:27374 L=48 S=0x00
I=28362 F=0x4000 T=106
Apr 04 07:33:42 riggs kernel: Packet log: input - eth0 PROTO=6 24.114.117.105:22619 x.x.x.x:27374 L=48 S=0x00
I=28362 F=0x4000 T=106
```

Evidence of Active Targeting: Yes

History: Found this in my ipchains log on my firewall at home. My home firewall protects me from the @HOME network. I have been seeing tons of SubSeven Trojan scans lately.

Existence: The source IP address (24.114.117.105) was resolved to cr288071-a.ym1.on.wave.home.com. These are coming from all different sources. Most of which are likely from script-kiddies. Good thing I have a firewall protecting my home machine from all of this stuff. It is scary to think that there are lots of people running systems without any protection at all.

Technique: Attackers are likely using a script to send packets to the SubSeven port 27374. The scan is coming from the same source IP address targeting one single destination IP address. The scan is also happening very quickly, two attempts logged at the exact same time. One other attempt came shortly after the first 2. I wonder why? – Perhaps the attacker made a modification to a script he/she was running.

Evidence of Intent: This is an attempt to attain remote administration of the destination machine.

Analysis:

- SYN packets directed at a single host.
- Attacker looking for a SYN-ACK to be returned.
- Short duration in time between attempts.
- TCP port 27374 is known as the SubSeven Trojan listening port.
- For more information on the SubSeven Trojan check out: http://english.sub7help.de/

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 5) – (4 + 4) = 2

Criticality:	Targeted against my machine on the @HOME network.
Lethality:	Attempted connection to a malicious Trojan.
System Countermeasure:	Firewall being targeted and it is patched up to latest and greatest rev levels. Systems behind this firewall have virus scanning software installed and signatures are updated frequently.
Network Countermeasure:	Firewall protects home network.

Analysis – 5 DEEP THROAT / THE INVASOR TROJAN (Home Linux FW)

Apr 04 17:04:13 riggs kernel: Packet log: input - eth0 PROTO=17 24.114.117.227:60000 x.x.x.x:2140 L=30 S=0x00 I=2320 F=0x0000 T=50
Apr 11 17:26:31 riggs kernel: Packet log: input - eth0 PROTO=17 24.114.117.227:60000 x.x.x.x:2140 L=30 S=0x00 I=2320 F=0x0000 T=50
Apr 13 19:44:53 riggs kernel: Packet log: input - eth0 PROTO=17 24.114.117.227:60000 x.x.x.x:2140 L=30 S=0x00 I=2320 F=0x0000 T=50

Evidence of Active Targeting: Yes

History: Found this in my ipchains log on my firewall at home. My home firewall protects me from the @HOME network.

Existence: The source IP address (24.114.117.227) resolved to cr792654-a.ym1.on.wave.home.com. It was determined that the source IP was someone from the @HOME network.

Technique: Attackers are sending packets to port 2140 to try to get a response. I found 3 different entries for this attempt coming in the evenings from the same source IP address.

Evidence of Intent: To gain remote administration of targeted machine.

Analysis:

- Looking for the Deep Throat or Invasor Trojan.
- Connection attempt to TCP 2140.
- Same source IP address used in 3 different attempts.
- Most likely a script.
- Run in the early evening.
- GUESS – Scan being performed by a script –kiddie after he/she is done school for the day.

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 5) – (4 + 4) = 2

Criticality:	Targeted against my machine on the @HOME network.
Lethality:	Attempted connection to a malicious Trojan.
System Countermeasure:	Firewall machine is being targeted and it is patched up to latest and greatest rev levels. Systems behind this firewall have virus scanning software installed and signatures are updated frequently.
Network Countermeasure:	Firewall protects home network.

.

Analysis - 6 TCP FIN SCAN (Test Lab)

```
10:22:29.617452 source1.62322 > source2.530: F 0:0(0) win 4096
10:22:29.617570 source1.62322 > source2.208: F 0:0(0) win 4096
10:22:29.617654 source1.62322 > source2.7003: F 0:0(0) win 4096
10:22:29.617690 source1.62322 > source2.5004: F 0:0(0) win 4096
10:22:29.617754 source162322 > source2.1380: F 0:0(0) win 4096
10:22:29.617789 source1.62322 > source2.204: F 0:0(0) win 4096
10:22:29.617852 source1.62322 > source2.960: F 0:0(0) win 4096
10:22:29.617893 source1.62322 > source2.10082: F 0:0(0) win 4096
```

Evidence of Active Targeting: Yes

History: Conducted in a lab environment.

Existence: Same source IP address (source1) and same destination address (source2).

Technique: This is a FIN host scan of just one particular host. The source port is remaining the same for the entire scan (62322).

Evidence of Intent: The host is scanning one particular host looking for a certain response/non-response.

Analysis:

- Automated attack.
- Very fast.
- Source port remains the same throughout the trace.
- One host targeted.
- FIN scan allows the attacker to detect closed ports on a target by listening for RESET-ACK response packets (see FRC 793).
- Open ports should not respond to the FIN packets.

Severity:

Severity: (criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 4) – (4 + 4) = 1

Criticality: Targeted system.
Lethality: Information could be used to mount an attack on open ports.
System Countermeasure: Operating system running latest and greatest patch levels.
Network Countermeasure: Firewall protecting system in lab environment.

Analysis – 7 TROJAN & WELL KNOWN EXPLOITABLE PORT SCAN (GIAC Web Site)

Apr 18 23:52:52 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.0.110.68:1684 to 24.3.21.199 on unserved port 27374
Apr 19 00:24:57 cc1014244-a kernel: securityalert: tcp if=ef0 from 212.188.132.101:1736 to 24.3.21.199 on unserved port 12345
Apr 19 07:31:10 cc1014244-a kernel: securityalert: udp if=ef0 from 24.188.240.136:137 to 24.3.21.199 on unserved port 137
Apr 18 04:41:48 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:3053 to 24.3.21.199 on unserved port 22
Apr 14 01:04:58 cc1014244-a kernel: securityalert: tcp if=ef0 from 63.77.199.123:3690 to 24.3.21.199 on unserved port 111

Evidence of Active Targeting: Yes

History: From the GIAC web site.

Existence: Many different sources. There is an ever increasing trend of Trojan scans on the Internet. Lots of scripts available that make this easy to perform.

24.0.110.68	– c865570-a.grapid1.mi.home.com
212.188.132.101	- SCREAMING-NET UK ISP
24.188.240.136	– d240-136.hntnny.optonline.net
24.3.21.225	– cc731456-b.hwrd1.md.home.com
63.77.199.123	-- acs-63-77-199-123.zbzoom.net

Technique: Looking for the existence of Trojans listening and/or for other well known exploitable listening ports. This trace does not demonstrate an automated attack. This appears to be just a sampling of a log file showing multiple attempts from various sources to connect to a single destination machine IP address on potentially dangerous ports.

Evidence of Intent: Attempting to find a system open to remote administration via Trojans, or responding with well-known exploitable ports available for system compromise.

Analysis:

- More and more common.
- Subseven (TCP 27374/1243), netbus 12345, netbios name sevice (TCP 137), portmapper (TCP 111), PCAnywhere (UDP 22)
- Attacker looking to get SYN-ACK returned for one of these ports.
- Source addresses are all valid Internet addresses and do not appear to be spoofed.
- For more information on Trojans check out: http://newdata.box.sk/maniac/trojans.txt
- For more information on the well-known port exploits check out: http://www.cert.org/

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 5) – (4 + 4) = 2

Criticality:	Targeted machine.
Lethality:	Attempted connection to a malicious Trojan.
System Countermeasure:	Make sure virus protection software installed and signatures are up-to-date.
Network Countermeasure:	Firewalls should not allow this traffic to enter into network. IDS should send real time alerts on attempts outside the firewall and anything that is able to pass through. Look for machines to respond, this is a clear indication to serious problems.

Analysis – 8 Linuxconf (GIAC Web Site)

Apr 19 22:37:06 cc1014244-a kernel: securityalert: tcp if=ef0 from 24.1.86.154:1198 to 24.3.21.199 on unserved port 98

Evidence of Active Targeting: Yes

History: No history from the GIAC web site reported.

Existence: Performed nslookup on the IP address 24.1.86.154 and it was resolved to an @Home user c685583-a.pinol1.sfba.home.com

Technique: This is a scan targeting the TCP port 98 which is known to be used by the linuxconf administration utility.

Evidence of Intent: To remotely administer the system via the linuxconf administration tool.

Analysis:

- Trace shows attacker looking for TCP port 98 (linuxconf) response.
- Linuxconf is an administration system (GUI) for the Linux operating system

Linuxconf runs as root therefore if compromised, the attacker could potentially gain root access.

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 5) – (4 + 4) = 2

Criticality:	Targeted machine.
Lethality:	Attempted connection to a malicious Trojan.
System Countermeasure:	Make sure linuxconf, has been configured correctly.
Network Countermeasure:	Proper configuration and deployment of firewall technology and IDS may help prevent this from happening or at least being unknown.

From Port	Date - Time (CST)	From	To	To Port	EventName Information
1746	4/17/00 11:20:06AM	200.42.140.45	163.186.32.92	31337	BackOrifice COMMAN Ping host
1746	4/17/00 11:20:06AM	200.42.140.45	163.186.32.91	31337	BackOrifice COMMAN Ping host
1746	4/17/00 11:20:06AM	200.42.140.45	163.186.32.93	31337	BackOrifice COMMAN Ping host

Evidence of Active Targeting: Yes

History: No previous history given.

Existence: Source IP address (200.42.140.45) resolves to host140045.datamarkets.com.ar

Technique: Using a script to find out if any machines on the 163.186.32.x network are listening on the BackOrifce port. Scan is very quick and looks automated. The scan is also targeting a class C subnet network at the same time.

Evidence of Intent: The source computer is scanning the network for UDP port 31337, which is most commonly related to BackOrifice. This is an attempt to gain remote administration to any machines on this network that my have the BackOrifice Trojan installed.

Analysis:

- Automated.
- Very quick, scanning multiple machines at the same time.
- Most likely a script being used to scan an entire network.
- Can give attacker remote access to compromised machines.
- For more information regarding BackOrifice check out: http://www.cultdeadcow.com/tools/bo.html

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 5) – (4 + 4) = 2

Criticality:	Targeted Class C network.
Lethality:	Attempted connection to a malicious Trojan port.
System Countermeasure:	Make sure virus scanning software is installed and virus signatures are kept up to date.
Network Countermeasure:	Have Firewalls block incoming requests and any outgoing connections. Have an IDS system both on the outside and inside of the firewall providing real time notification of any successful attempts or for any suspicious connections originating from internal machines.

```
Apr 8 11:05:48 192.116.7.35:2434 -> a.b.e.52:53 UDP
Apr 8 11:05:48 192.116.7.35:2825 -> a.b.e.58:53 UDP
Apr 8 11:05:49 192.116.7.35:2973 -> a.b.e.63:53 UDP
 ...
Apr 8 11:05:51 192.116.7.35:2184 -> a.b.e.201:53 UDP
Apr 8 11:05:55 192.116.7.35:4141 -> a.b.e.176:53 UDP
Apr 8 11:05:55 192.116.7.35:3800 -> a.b.e.135:53 UDP
Apr 8 11:05:55 192.116.7.35:3367 -> a.b.e.216:53 UDP
```

Evidence of Active Targeting: Yes

History: Taken from the GIAC web site. No prior history given.

Existence: Source IP address resoled to: linux.bethlehembiblecollege.edu

Technique: The attacker will send UPD port 53 packets to a range of IP addresses or an entire subnet in hopes of determining the IP address of machines running a DNS server. This is an automated attack generated by a script, which makes mapping very quick.

Evidence of Intent: Information Gathering / Reconnaissance.

Analysis:

- Automated attack.
- Very quick.
- Uses UDP port 53.
- Closed ports respond with ICMP port unreachable messages.
- Open ports do not respond at all.
- By nature UDP is unreliable.
- The tool nmap has the ability to perform this kind of scan.
- Depending upon DNS server configurations, it may be possible to gain info from a zone transfer.

Severity:
(criticality + lethality) – (system countermeasure + network countermeasure)
(5 + 4) – (4 + 4) = 1

Criticality:	Targeted network.
Lethality:	Information could be used to mount an attack.
System Countermeasure:	Make sure DNS servers have been configured correctly and running the latest and greatest patches.
Network Countermeasure:	Implement firewalls that are configured correctly to not allow DNS mapping, and IDS to give real time alerts if this traffic is being seen.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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
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
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
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