Global Information Assurance Certification Paper

*** Northcutt, smile, last I heard IRC was TCP (trace 1) and 4 could be load balancing but that is a nit. Other than that I like the report, especially the research done into the vulnerabilities, that will help this student to defend her nets, a few references and URLs would have been fantastic. Mostly clear writing. Analysis process would benefit from some rigor. 79 *

Practical Exam Submission:
Lisa Swain-Morris
SANS 2000

Origins of Traces : GIAC Web Site

```
02:18:30.295451 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
02:18:30.301084 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
02:18:30.306508 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
02:18:30.312112 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
02:18:30.317681 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
02:18:30.323070 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024

[Snip more packets]

02:18:31.100991 morannon.kdi.com > 209.216.2.200: icmp:
morannon.kdi.com udp port ircd unreachable [tos 0xc0]
02:18:31.106472 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
02:18:31.111972 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
02:18:31.117526 209.216.2.200.4164 > morannon.kdi.com.ircd: udp 1024
```

wc -l reveals 28808 lines of the above upd packets to port 6667 in an approx. 3 minute time span.

Analysis: This trace seems to indicate that 209.216.2.200 are irc scanning of morannon.kdi.com.ircd. looking to see if port 6667 is open. May even be a covert channel to hide data in the UDP packet sized to 1024.The timing indicates a scripted reconnaissance effort. morannon.kdi.com responds back with ircd port unreachable.
Severity level =High
Active Targeting = Yes
Vulnerabilty : IRC servers up to ver 8.21 contain vulnerability for DOS
Also IRC Buffer overflow allows execution of arbitrary code on the users systems via DCC Chat.

Detect 2

```
 02:26:31.574847 209.216.2.200 > morannon.kdi.com:
(frag 30041:48@2960)
02:26:31.583572 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30041:1480@0+)
02:26:31.583582 209.216.2.200 > morannon.kdi.com:
(frag 30044:48@2960)
02:26:31.591760 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30044:1480@0+)
02:26:31.591768 209.216.2.200 > morannon.kdi.com:
(frag 30046:48@2960)
02:26:31.600166 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30046:1480@0+)
02:26:31.600173 209.216.2.200 > morannon.kdi.com:
```

(frag 30048:48@2960)
02:26:31.609754 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30048:1480@0+)
02:26:31.609785 209.216.2.200 > morannon.kdi.com:
(frag 30050:48@2960)

Analysis: The first thing I noticed in the above trace is that the order of which the fragmented packets arrive, it appears that the first frag (frag offset 0) in the transmission comes in after the packet with the offset set (2960). Also there is a gap in the offset values. This appears to be a crafted ICMP packet possibly attempting a DOS by sending the offset fragment first in addition to the gap between offsets or could it be just poorly written code. The time values indicate a fast send.

Severity level = Medium
Targeted Scan = Yes
Vulnerabilty : miscrafted fragment offsets are sent to confuse packet re-assembly in TCP/IP stacks possibly to crash them.

Detect 3

Apr 3 22:03:34 cm-208-138-199-120 kernel: Packet logs:
input DENY eth0 PROTO=17 24.148.10.100:1073 208.138.199.120:137
L=78 S=0x00 I=37635 F=0x0000 T=118 (#7)
Apr 3 22:03:39 cm-208-138-199-120 kernel: Packet log:
input DENY eth0 PROTO=17 24.148.10.100:1073 208.138.199.120:137
L=78 S=0x00 I=38147 F=0x0000 T=118 (#7)
Apr 3 22:03:54 cm-208-138-199-120 kernel: Packet log:
input DENY eth0 PROTO=17 24.148.10.100:1073 208.138.199.120:137
L=78 S=0x00 I=38403 F=0x0000 T=118 (#7)

Analysis: The firewall logs seems to indicate a denial to allow an UDP packet for NetBios for printing/browsing or pass through validation. (dest port 137) NetBios/SMB are used for Windows "Files and Print Sharing" as well as Samba. End Users sharing their hard disk on the port are probably the most common vulnerability on the Internet. Recently there have been attempts for worms to propagate on this port.
The packet description appears to indicate a crafted packet the source IP and especially the port number is the same from 22:03:34 until 22:04:54. This is a good indication the firewall is doing its job of port blocking. NetBios services should come in over TCP/IP.
Severity Level = High
Targeted Scan = Yes
Vulnerabilty : Scans at this port tapered off the end of 1999, now attempts at this port have picked up again. Several VBS worms have appeared to attempt to copy themselves on this port. Also attempts to connect remotely to NetBios filesharing without user-name and password allows an attacker to view listing of shares

---

Detect 4

Apr 4 00:16:12 212.62.17.145:39805 -> 92.168.247.34:33439 UDP
Apr 4 00:16:12 212.62.17.145:39805 -> 192.168.247.34:33440 UDP
Apr 4 00:16:12 212.62.17.145:39805 -> 192.168.247.34:33441 UDP
Apr 4 00:16:12 212.62.17.145:39805 -> 192.168.247.34:33442 UDP
Apr 4 00:16:13 212.62.17.145:39805 -> 192.168.247.34:33443 UDP
Apr 4 00:16:13 212.62.17.145:39805 -> 192.168.247.34:33444 UDP

Analysis:UDP Port Scan Crafted packet walking down UDP port on host 192.168.247.34 ports 33440 thru 33444 Indicative of a trace route.
Severity Level: = Med (crafted packet the source port never changes)
Targeted Scan = Yes
Vulnerabilty : Common Network Utility.

Detect 5

Apr 5 20:13:50 gatekeeper portsentry[1776]: attackalert:
UDP scan from host: router.nastec.com.au/150.101.8.1 to UDP port: 161
Apr 5 20:13:50 gatekeeper portsentry[1776]: attackalert:
Host 150.101.8.1 has been blocked via wrappers with string: "ALL: 150.101.8.1"
Apr 5 20:13:50 gatekeeper portsentry[1776]: attackalert:
UDP scan from host: router.nastec.com.au/150.101.8.1 to UDP port: 161

Analysis:
UDP port scan from host 150.101.8.1 to SNMP port 161.
This trace also shows that the gatekeeper has good access rules in place to prevent access to port 161.
Severity Level: Low (packet was not allowed)
Targeted Attack = Yes
Vulnerabilty :Port 161 is a common port that intruders probe for.
SNMP allows for remote management of devices.
All the configuration and performance information is stored in a database that can be retrieved via SNMP. Also Windows machines running HP JetDirect remote management software uses SNMP, and this could also indicate misconfigured machines.

Detect 6

Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from
216.77.245.249:2606 to 24.3.21.199 on unserved port 1243
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from
216.77.245.249:2607 to 24.3.21.199 on unserved port 12345
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from
216.77.245.249:2608 to 24.3.21.199 on unserved port 20034
Apr 8 01:37:56 cc1014244-a kernel: securityalert: tcp if=ef0 from
216.77.245.249:2609 to 24.3.21.199 on unserved port 27374

Analysis: Trojan probe from source 216.77.245.249. probably looking to see if 24.3.21.199 has been compromised with the following trojans, Sub-7 Voodoo Doll, Netbus 2 and Sub-7 ver 2.1.
Severity Level = High
Target Scan = Yes
Vulnerabilty : Well known compromises due to Trojan implantation.

Detect 7

Apr 9 05:43:03 cc1014244-a kernel: securityalert: tcp if=ef0 from
208.232.120.196:623 to 24.3.21.199 on unserved port 111
Analysis:Scan to see if port mapper is listening.
Severity Level = High
Targeted Scan = Yes (even though a detect is made several packets later from different destination could indicate distributed scan)
Vulnerabilty : Portmapper contains known vulnerabilities such as it will allow remote users to register/unregister services on a remote host by way of forging UDP packets

---

Detect 8

Apr 9 05:48:02 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:3592 to 24.3.21.199 on unserved port 5632
Apr 9 05:48:02 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:3592 to 24.3.21.199 on unserved port 22
Apr 9 05:49:33 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:3595 to 24.3.21.199 on unserved port 5632
Apr 9 05:49:33 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:3595 to 24.3.21.199 on unserved port 22
Apr 9 06:06:43 cc1014244-a kernel: securityalert: udp if=ef0 from 24.3.21.225:1081 to 24.3.21.199 on unserved port 5632

Analysis: UDP packets directed at this port along with port 5632 indicate a scan for PCAnywhere.
Severity Level = High
Targeted Scan = Yes
Vulnerabilty : PCAnywhere versions 8 & P contain a DOS where an attacker can terminate/cancel the connection before being prompted to log in causing the service to crash.

Detect 9

Apr 12 12:17:48.205477 194.98.128.15,4557 -> 10.1.6.30,98 PR tcp len 20 60 –S
Apr 12 12:17:48.206080 194.98.128.15,4547 -> 10.1.6.20,98 PR tcp len 20 60 -S
Apr 12 12:17:48.206686 194.98.128.15,4550 -> 10.1.6.23,98 PR tcp len 20 60 -S
Apr 12 12:17:48.207292 194.98.128.15,4569 -> 10.1.6.42,98 PR tcp len 20 60 -S
Apr 12 12:17:48.207894 194.98.128.15,4570 -> 10.1.6.43,98 PR tcp len 20 60 –S

Analysis: This trace indicates a port scan for linuxconf on several hosts, from one source. Not a script because the port numbers change on source.
Targeted Scan = Yes
Severity = High
Vulnerabilty : The utility “linuxconf” provide easy administration of Unix boxes. It includes a web-enabled interface at port 98 through an integrated HTTP server. It has a number of security issues. Some versions are setuid root, trust the local network, create world-accessible files in /tmp, and a buffer overflow in the LANG environment variable. Also because it contains an integrated web server, it may be vulnerable to many of the typical HTTP exploits(buffer overruns, directory traversal using ../…,etc0

Detect 10

Apr 12 15:27:12.874453 159.148.165.250,1613 -> 10.0.0.7,53 PR udp len 20 55
Apr 12 15:27:12.875545 159.148.165.250,1609 -> 10.0.0.9,53 PR udp len 20 55
Apr 12 15:27:13.149663 159.148.165.250,1615 -> 10.0.0.6,53 PR udp len 20 55
Apr 12 15:27:13.491630 159.148.165.250,1745 -> 10.0.0.5,53 PR udp len 20 55

Analysis: A port scan for DNS
Targeted Scan = Yes (Notice the private IP address of destination)
Severity = High
Vulnerabilty : This may be an attempt to spoof DNS or even hide other traffic since port 53 is frequently neither filtered nor logged by firewalls.

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 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