Global Information Assurance Certification Paper

*** Northcutt, accuracy appears to be fine. Clarity could use some work, I had to puzzle through many of these trying to figure out what was being said. A lot of work to present different types of traces has gone into this and this means this analyst has the skills to do the job! 78 *

IDIC - Intrusion Detection Practical Assignment

Student Name: Rick Genesi
Date: 4/11/2000

Methodology Enforcement (Used in practice for each detect below):

1] Identify Hostile Individuals & groups – Existence
2] Identify their History – History
3] Identify their Techniques – Techniques
4] Evidence of Intent – Intent
5] Evidence of Active Targeting – Targeting
6] Evaluate Information – Analysis & Severity Level

Notes: I wanted to use a number of methods to analyze network data and complete this assignment. My choice was to examine data from multiple firewall, Win dump, and ISS Real Secure logs to accomplish this task. I have also renamed many host described for security and sensitive nature of the data.

Other Tools Used: Ping, Neo trace (TraceRoute), Iana Web site (Port assignments)

Description: Detects #1, #2, and #3.Snapshots taken from a firewall log report.

Detect #1
Apr 5 06:53:48 firewall1.xxx.com unix: securityalert: no match found in local screen: UDP if=hme1 srcaddr=internal srcport=1015 dstaddr=127.0.0.1 dstport=111

Apr 5 06:54:42 firewall1.xxx.com unix: securityalert: no match found in local screen: UDP if=hme1 srcaddr=internal srcport=777 dstaddr=127.0.0.1 dstport=111

Apr 5 09:39:06 firewall1.xxx.com unix: securityalert: no match found in local screen: UDP if=hme1 srcaddr=internal srcport=784 dstaddr=127.0.0.1 dstport=111

Existence: It appears that the same host is making multiple attempts into this firewall, however I checked other Corp. firewall for similar events and found none.

History: The source address is a intranet address

Techniques: Destination address is the local loop back address

Intent: A multiling-http port call to a destination port SunRPC call

Targeting: Attempts are being taken to understand target

Analysis & Severity Level: No match found in local screen implies that firewall is not letting this host communication succeed outgoing, therefore severity level is low, however, situation or criticality needs attention.

Detect #2
Apr 5 09:20:12 firewall1.xxx.com unix: securityalert: source not allowed on interface: UDP if=hme0 srcaddr=nameserver srcport=53 dstaddr=nameserver1 dstport=53
Apr 5 09:37:55 firewall1.xxx.com unix: securityalert: source not allowed on interface: UDP if=hme0 srcaddr=nameserver srcport=53 dstaddr=nameserver1 dstport=53

Existence: It appears that the same host is making multiple attempts and is reporting into this firewall log. I did check other firewall logs and found nothing similar in substance.
History: The source address is a intranet name server address

Techniques: Destination address is also a nameserver1 address on the intranet.

Intent: One internal name server is attempting to query the other

Targeting: No targeting has been pinpointed

Analysis & Severity Level: Perhaps DNS configuration needs to be checked? Why is it that two name servers are attempting to complete a function but failed to do so based on rules filter in firewall? Severity level indication is low but my interest is peaked to discover more about the configuration.

Detect #3

Apr 5 09:06:40 firewall2.xxx.com unix: securityalert: packet denied by forward screen: ICMP if=hme1 srcaddr=internal2 dstaddr=dmz1
Apr 5 09:06:40 firewall2.xxx.com unix: securityalert: packet denied by forward screen: ICMP if=hme1 srcaddr=internal2 dstaddr=dmz2
Apr 5 09:06:40 firewall2.xxx.com unix: securityalert: packet denied by forward screen: ICMP if=hme1 srcaddr=internal2 dstaddr=dmz3
Apr 5 09:06:40 firewall2.xxx.com unix: securityalert: packet denied by forward screen: ICMP if=hme1 srcaddr=internal2 dstaddr=dmz4
Apr 5 09:06:40 firewall2.xxx.com unix: securityalert: packet denied by forward screen: ICMP if=hme1 srcaddr=internal2 dstaddr=dmz5

Existence: It appears that the same host is making multiple attempts

History: The source address is again a intranet or internal2 address

Techniques: Destination address seems to be focused toward hosts on 1 particular subnet

Intent: Attempts to see if nodes on given subnet are reachable

Targeting: Why would an inside machine be testing for reach ability of nodes outside the firewall. Specially if it was a firewall administrator. This person should already be aware that this is not possible unless testing firewall filter.

Analysis & Severity Level: The internal host is attempting to complete a ICMP ping command and is testing multiple host on the outside DMZ network. The attempts failed because ICMP packets are not permitted out of the intranet. Severity level classified as low because of the block, but I still need further analysis and study done in this case.

Description: Detects #4, #5, #6 were taken from a WINDUMP Log File

Detect #4

03:55:21.599161 destnode1 > host1: icmp: destnode1 udp port 653 unreachable
03:55:21.603654 host1.807 > destnode1.654: udp 80
03:55:21.603764 destnode1 > host1: icmp: destnode1L udp port 654 unreachable
03:55:21.608942 host1.807 > destnode1.655: udp 80
03:55:21.609036 destnode1 > host1: icmp: destnode1 udp port 655 unreachable
03:55:21.613908 host1.807 > destnode1.656: udp 80
03:55:21.614002 destnode1 > host1: icmp: destnode1 udp port 656 unreachable
03:55:21.621036 host1.50021 > destnode1.22: S 15148:15148(0) win 4096
03:55:21.621140 destnode1 > host1.50021: R 0:0(0) ack 15149 win 0
03:55:21.650500 arp who-has test tell test1
03:55:21.660544 host1.807 > destnode1.657: udp 80
03:55:21.660656 destnode1 > host1: icmp: destnode1 udp port 657 unreachable

Existence: It appears that the same host is making multiple attempts

History: The source address is again a intranet address

Techniques: Destination address seems to be focused toward a particular host called destnode1

Intent: Attempts to see if multiple udp ports are reachable on a particular host

Targeting: This particular host called destnode1 is being scanned

Analysis & Severity Level: This looks to be a precise udp port scan occurring. Being internal I would consider severity to be low, however, I would find out more about this scanning activity.

Detect #5

```
03:55:02.519877 nodea.1344 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.688494 nodea.1350 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.688811 nodea.1351 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.716826 nodea.1355 > beacon.161: GetRequest(9)[|snmp]
03:55:02.726232 nodea.1354 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.868300 nodea.1354 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.868377 nodea.1356 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.868919 nodea.1356 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.928179 nodea.1359 > beacon.161: GetNextRequest(9)[|snmp]
03:55:02.983043 nodea.1361 > beacon.161: GetNextRequest(9)[|snmp]
03:55:03.009538 nodea.1344 > beacon.161: GetNextRequest(9)[|snmp]
03:55:03.197083 nodea.1351 > beacon.161: GetNextRequest(9)[|snmp]
03:55:03.197860 nodea.1355 > beacon.161: GetRequest(9)[|snmp]
03:55:03.206375 nodea.1365 > beacon.69: 44 WRQ "/tmp/CyberCop.tftp.vulne" [|tftp]
03:55:03.245111 nodea.1350 > beacon.161: GetNextRequest(9)[|snmp]
03:55:03.373112 nodea.1367 > beacon.161: GetNextRequest(9)[|snmp]
03:55:03.639503 nodea.1370 beacon.161: GetNextRequest(9)[|snmp]
```

Existence: It appears that the same host called nodea is making multiple attempts

History: The source address is again an intranet address

Techniques: Destination address seems to be focused toward a host called beacon

Intent: Multiple attempts to see if snmp queries are successful

Targeting: A host is being targeted with a snmp type scan

Analysis & Severity Level: It looks to be a cyber cop scan perhaps checking for SNMP vulnerabilities by doing numerous get commands probably using common public community strings. Severity of scan I consider low because of it occurring internal to the firewall walls. I still need to trace down the source of the scan.

Detect #6

03:59:58.398928 USA.47026 > bert.139: **S** 4284125656:4284125656(0) win 4096
03:59:58.399050 bert.139 > USA.47026: **S** 3905713:3905713(0) **ack** 4284125657 win 8576 <mss 1456> (DF)
03:59:58.426030 USA.47026 > bert.139: **R** 4284125657:4284125657(0) win 0
03:59:58.446972 USA.59141 > bert.192: **S** 17395:17395(0) win 4096
03:59:58.447084 bert.192 > USA.59141: **R** 0:0(0) **ack** 17396 win 0

Existence: It appears that the same host called USA is making multiple attempts

History: The source address is again an intranet address

Techniques: Destination address seems to be focused toward a host called bert

Intent: Port 139 is a netbios-ssn session service port and port 192 is an osu-nms network monitoring port, looks to be random.

Targeting: Seems to be random ports on a particular host being targeted.

Analysis & Severity Level: It appears to be a typical signature of a TCP random port scan. By looking at the 3 way handshake signals half open type scanning. Severity level I still consider low because of internal source address completing the scanning.

Description: Detects #7 - #10 were taken from a ISS Real Secure Log File located on outside of intranet

Detect #7

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddressName
156702	07-Apr-00	SNMP_Suspicious_Get	17	3553	161	lookout	Seek1 (.254)
156703	07-Apr-00	SNMP_Suspicious_Get	17	3553	161	lookout	Seek1 (.254)
156704	07-Apr-00	SNMP_Suspicious_Get	17	3553	161	lookout	Seek1 (.254)

Existence: It appears that the same host is making multiple attempts

History: The source address is again a reachable intranet address. Also, the destination host address field (.254) are typically assigned by network administrators to network devices.

Techniques: Destination address seems to be a external device address on outside DMZ perimeter

Intent: Seems to be an attempt made through the firewall

Targeting: Why would a machine be attempting to communicate thru the firewall? Unless there is a miss configuration or misuse of the application being applied.
Analysis & Severity Level: A SNMP get request packet is being sent from a HP Openview management host to a device on the outside of the DMZ that its trying to manage. It is probably a network device because of the assigned host address convention used (last field .254) by the network administrators. Severity level perhaps considered medium, need to track trace to owners of management station.

Detect #8

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddressName
157512	07-Apr-00	Email_Turn	6	3432	25	guest	External mail relay
157513	07-Apr-00	Email_Turn	6	3432	25	guest	External mail relay
157514	07-Apr-00	Email_Turn	6	3432	25	guest	External mail relay

Existence: It appears that the same host is making multiple attempts

History: The source address appears to be coming from outside the perimeter of our intranet.

Techniques: The Guest is focused on destination address of our external mail relay box.

Intent: Some kind of mail / smtp function being performed

Targeting: No specific targeting other then a smtp request is seen.

Analysis & Severity Level: A smtp vulnerability may exist with specific older versions of smtp daemons. This older version allows an smtp email session to be turned around with no further security requests thru the same TCP connection. Severity would be considered low, however smtp version checks have to be made on mail server.

Detect #9

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddressName
165169	07-Apr-00	HTTP_DotDot	6	58050	80	proxy	216.77.148.35
ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddressName

165181	07-Apr-00	HTTP_DotDot	6	58741	80	proxy	216.77.148.35

Existence: It appears that the same host is making multiple attempts

History: The source address is a intranet address and appears to be the internal HTTP proxy server which is executing on someone's internal browser request.

Techniques: Destination address seems to be an external web site

Intent: Attempt to obtain sensitive server information

Targeting: Someone is accessing this outside web server from the inside via a HTTP proxy.

Analysis & Severity Level: A node is accessing a proxy server that in turn is requesting information of the destinations server directory structure. This vulnerability still exists in old ISS and NCSA web servers. The destination server should upgrade their web OS. Severity rated medium, knowing that pertinent system configuration could be compromised.

Detect #10

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPort	SourceAddressName	DestinationAddressName
610	06-Apr-00	Finger_Bomb	6	64938	79	Firewall1	208.156.27.21

Existence: It appears that this host is making an attempt

History: The source address is the address of the firewall box. Need to talk to the firewall folks to obtain logs to determine which inside address this request is initiated from.

Techniques: Destination address is someone's external web site. Perhaps a Russian language web site.

Intent: Attempts from source to use the finger command to the destination node

Targeting: The use of finger can be used as a denial of service attack by being able to redirect multiple finger packets to the destination device and consume its own cpu cycles.

Analysis & Severity Level: The destination could be vulnerable to a finger attack if it is running this finger daemon. Shutting down this process especially on a web server would be wise. Severity level in this case would be considered medium specially if your business web server were compromised!
