Global Information Assurance Certification Paper

*** Northcutt, well this is certainly one of the more interesting practicals that has been submitted! Thank you for describing your setup that was very helpful. What is your small class c network's subnet mask? This information may help unscramble detect 1. In the case of detect 2, could there be traffic that would stimulate the ident? Detect 7, is it possible someone is spoofing and using your address space to do it? With 8, there is a chance this is more related to mapping. Love the way you dumped the hex and were checking those TTL values! You are clearly on your way, keep practicing and reading other folk's analysis. 76 ***

GIAC Certification Practical
Ten detects with Analysis
By Garth Howe (Analyst Wannabe)

Notes about Network:

Although our network is a very small Class C net (25 hosts), for testing purposes we directly connect to two ISP's through two firewalls (NET.ONE.72.114 and NET.TWO.86.47), and two routers (NET.ONE.72.113 and NET.TWO.86.46). I utilized Windump on an NT 4.0 Workstation which connects to an ethernet hub, common to the two routers and firewalls. This allows me to capture all traffic moving in and out of our network. An unexpected find was the ability to capture traffic with neither a source, or destination address within our network. This appears to be due to one of our ISP links being a radio wave broadcast downlink, with their router at our location allowing us to not only see our traffic, but all downlink traffic!

Notes about Detects:

All of the detects were taken from our DMZ. Utilizing Windump I am building a library of filters and batch files to more efficiently parse through the massive amounts of data crossing the DMZ. I currently capture about two days of data at a time, and then work through it looking for anomalies. When suspicious traffic is found from a host, I then search the previous captures for historical data related to that host. My historical information is rather limited though with captures starting upon my return from SANS 2000.

Detect #1 (Sorry, bit of a long one)

. Telnet to "broadcast", then to two hosts, then to just the 118 host

02:26:26.054237 216.184.200.2.1491 > 255.255.255.255.23: S 2355437907:2355437907(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 49, id 49891)
02:26:26.063575 216.184.200.2.1493 > NET.ONE.72.114.23: S 2348034648:2348034648(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 49, id 49893)
02:26:26.066419 216.184.200.2.1494 > NET.ONE.72.115.23: S 2349529416:2349529416(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 49, id 49894)
.
02:26:26.082448 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 49, id 49897)
02:26:26.084565 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 48, id 49897)
02:26:26.085486 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 47, id 49897)
.
. TTL keeps decrementing one at a time
.
02:26:26.119798 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 23, id 49897)
.
. Let's hit the broadcast address again
.
02:26:26.121559 216.184.200.2.1506 > 255.255.255.255.23: S 2347454759:2347454759(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 49, id 49906)
.
. Now continue what we started
.
02:26:26.122323 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 22, id 49897)
.
.
02:26:26.155687 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 3, id 49897)
02:26:26.156608 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) (ttl 2, id 49897)
02:26:26.156846 216.184.200.2.1497 > NET.ONE.72.118.23: S 2355321387:2355321387(0) win 32120 <mss 1460,sackOK,timestamp 604795[|tcp]> (DF) [ttl 1] (id 49897)
.
. My router responds to the ttl of one
.
02:26:26.160501 NET.TWO.86.46 > 216.184.200.2: icmp: time exceeded in-transit (ttl 254, id 21)
.
. Now do a scan similar to the beginning of this trace, and then stop
.
02:26:29.034963 216.184.200.2.1491 > 255.255.255.255.23: S 2355437907:2355437907(0) win 32120 <mss 1460,sackOK,timestamp 605095[|tcp]> (DF) (ttl 49, id 50114)

02:26:29.037412 216.184.200.2.1494 > NET.ONE.72.115.23: S 2349529416:2349529416(0) win 32120 <mss 1460,sackOK,timestamp 605095[|tcp]> (DF) (ttl 49, id 50116)
02:26:29.044159 216.184.200.2.1493 > NET.ONE.72.114.23: S 2348034648:2348034648(0) win 32120 <mss 1460,sackOK,timestamp 605095[|tcp]> (DF) (ttl 49, id 50115)
02:26:29.062633 216.184.200.2.1499 > NET.ONE.72.120.23: S 2349099938:2349099938(0) win 32120 <mss 1460,sackOK,timestamp 605095[|tcp]> (DF) (ttl 49, id 50120)
02:26:29.091561 216.184.200.2.1506 > 255.255.255.255.23: S 2347454759:2347454759(0) win 32120 <mss 1460,sackOK,timestamp 605095[|tcp]> (DF) (ttl 49, id 50127)

Active Targeting? Very definitely, targeted at the few IP's in our DMZ

History The specific hosts targeted would indicate that some reconnaissance work had been done previously, but I have no record of this

Technique With 54 packets sent in a second this is a scripted scan, "smells" like a DOS attack

Analysis The detect starts with what might be considered a network mapping technique, looking for a response to the first part of the TCP handshake. Then one specific host (.118) is hit 48 times with a SYN to the Telnet port, indicating a Denial of Service (DOS) attack. But if the point is to cause a DOS on host 118, why would you bother decrementing the TTL, like some crazy reverse Unix Traceroute? Then we pretty much repeat the first network mapping attempt again. There may be a simple explanation for this behaviour, but I don't know what it is

A little further information. A Traceroute back to the source IP indicates that the initial TTL of 49 makes sense. The starting TTL was likely 64, and our site is about 15 hops away, so the Source is not likely spoofed. The IP belongs to a Host at an ISP, so this could be a shell account, hijacked host, maybe a relay?

Threat Low. The unknown nature of this probe makes my heart rate this a "medium", but my brain indicates this is just another form of network probe, and I should relax

---

Detect #2

02:37:44.339206 206.172.130.72.1170 > NET.ONE.72.114.113: S 1578995:1578995(0) win 8192 <mss 1460> (DF) (ttl 112, id 40452)
02:37:44.340553 NET.ONE.72.114.113 > 206.172.130.72.1170: S 1969865729:1969865729(0) ack 1578996 win 16384 <mss 512> (ttl 60, id 61954)
02:37:44.569223 206.172.130.72.1170 > NET.ONE.72.114.113: . ack 1 win 8192 (DF) (ttl 112, id 40708)
02:37:44.603747 NET.ONE.72.114.113 > 206.172.130.72.1170: F 1:1(0) ack 1 win 16384 (ttl 60, id 61959)
02:37:44.889865 206.172.130.72.1170 > NET.ONE.72.114.113: . ack 2 win 8192 (DF) (ttl 112, id 40964)
02:37:48.636034 206.172.130.72.1170 > NET.ONE.72.114.113: F 1:1(0) ack 2 win 8192 (DF) (ttl 112, id 41476)

02:37:48.636323 NET.ONE.72.114.113 > 206.172.130.72.1170: . ack 2 win 16384 (ttl 60, id 61961)

Active Targeting?	Definitely, one specific host
History	This occurred eleven minutes after Detect #1, to one of the same hosts
Technique	Very stealthy, connect to one host, and get out
Analysis	Eleven minutes after Detect #1, someone using a dialup account on a different ISP, connects to the Identd (port 113) port of a host scanned in the previous detect. Doing a Traceroute indicated the source host was about 17 hops away. Adding this to the TTL of 112 on the arriving packets, we get 129. More likely the starting TTL was 128, so the source address is probably legitimate and not spoofed. This appears to be a stealthy information gathering attempt, which seems odd given the very noisey one in Detect #1. Maybe it is a GIAC student trying out some tools ☺
Threat	Low, well at least I will call it low to minimize my blood pressure. Although I did not see any further activity in the following nights, I may need to refine my filters to pull the information out of the background noise. If this person has the ability to utilize multiple hosts, he/she may be hiding further activity

---

Detect #3 (nice short one)

02:32:50.971093 207.75.164.81.109 > NET.TWO.86.47.109: SF 163551692:163551692(0) win 1028 (ttl 26, id 39426)

02:32:50.989155 207.75.164.81.110 > NET.TWO.86.47.110: SF 163551692:163551692(0) win 1028 (ttl 26, id 39426)

Active Targeting?	Very definitely, targeted at one of our firewalls
History	This occurred in between Detect #1 and Detect #2, but from a third completely different IP address, and aimed at a completely different host. They appear to have known the exact host they were looking for, so reconnaissance must have occurred in the past.
Technique	A single SYN-FIN packet to each of the POP ports on one of our firewalls. An attempt to be extremely stealthy, minimizing the number of probes, along with the SF attempt to avoid logging

Analysis This appears to be an attempt to look for open ports on our firewall, as part of an overall mission to survey our hosts. It occurs at 2:32 am in the morning, in between two other suspicious detects (#1 and #2), but against a different host. The use of a third completely different source host indicates that this person is wary of too much probing being traced back to the same address. Detects 1 and 2 had a source address at ISP's, while this one comes from a host at a .EDU consortium claiming to be developing "revolutionary Internet applications".

Threat Low. I'll stay with "low" until I can refine my filters, and see if I can pull out more activity from this person on other nights. This could be minor probing, or it could be part of a much larger scan.

Detect #4

15:45:48.174679 194.217.120.89.6112 > NET.TWO.86.47.6112: SFRP 2053970:2055422(1452) ack 0 win 4864 <[bad opt]> (DF) (ttl 47, id 193)

Active Targeting? Yes, single packet, aimed at our firewall

History Since they fired off a single packet at my firewall, I assume they did some reconnaissance ahead of time. There was no record of activity from this IP address in the five days before.

Technique Using a stealthy technique, with a single packet full of bad options

Analysis A single packet with SYN/FIN/RESET/PUSH and ACK all set, and directed from source port 6112 to destination port 6112. This could be an application trying to do Fingerprinting to determine the OS on this host, or perhaps an attempt to confuse the Operating System as part of a DOS. In either case, why would this be aimed at port 6112, as they stood next to no chance that this would be an open port? Perhaps this after school haxor, using the latest tool he acquired to produce a manufactured packet, does not know how to change the destination port yet ☺.

Threat Low. This wannabe is going to have to try a lot harder

---

Detect #5

10:47:55.625044 216.209.191.99.2457 > NET.TWO.86.47.8080: S 1314144:1314144(0) win 8192 <mss 1414,nop,nop,sackOK> (DF) (ttl 115, id 28033)

10:47:58.596944 216.209.191.99.2457 > NET.TWO.86.47.8080: S 1314144:1314144(0) win 8192 <mss 1414,nop,nop,sackOK> (DF) (ttl 115, id 52865)

Active Targeting? Very definitely, two datagrams targeted at one host

History No previous contact seen with this host in the previous five days

Technique Simple test for an open port 8080 on our firewall

Analysis This person is likely looking for a host running Wingate. Wingate apparently has a default configuration which has a proxy running on port 8080. This would allow someone to use this Wingate host to make them anonymous when connecting to other sites. What bothers me is that they are not scanning our range of addresses looking for Wingate, but that they targeted one specific IP address, one of our firewalls. This would indicate that they had previously mapped our network. The source IP address is a dial up port at a Canadian ISP.

Threat Low, very low. Someone looking for a Wingate host is of no threat to my network

---

Detect #6

02:55:35.758800 NET.TWO.86.46 > 216.208.80.173: icmp: NET.TWO.86.46 udp port 2140 unreachable (ttl 254, id 90)

4500 0038 005a 0000 fe01 64b1 d80d 562e
d8d0 50ad 0303 8502 0000 0000 4500 001e
92ed 0000 1411 bc28 d8d0 50ad d80d 562e
ea60 085c 000a

02:55:35.821370 216.208.80.173.60000 > NET.TWO.86.47.2140: udp 2 (ttl 20, id 37869)

4500 001e 93ed 0000 1411 bb27 d8d0 50ad
d80d 562f ea60 085c 000a 8532 3030 0000
0000 0000 0000 0000 0000 0000 0000

Active Targeting? Definitely, targeted two specific hosts

History No previous contact seen with this host in the previous five days

Technique Looking for a trojan, Deep Throat installed on port 2140

Analysis In looking through my captures I am always particularly interested in late night activity, as we do not operate a 24 hour shop. This capture caught my attention for two reasons, first being a source port of 60000. The odds of a UDP datagram at 2:55 am having such a high and even source port are pretty unlikely. Looking further I

found that destination port 2140 is commonly used for the trojans Deep Throat and The Invasor. Looking for further information I found an article on GIAC by Matt Scarborough about the Deep Throat trojan. He describes ports 60000 and 2140 being the most common UDP pair of ports. Bingo! My detect exactly. Having some information about my network they first looked for Deep Throat on my router, which responded with a Port Unreachable, and then on my Firewall which wisely remained silent.

A further note, the UDP datagram includes two bytes of data 0x3030, which is ASCII zero and zero. Apparently Deep Throat can be configured to contact an ICQ user. Is this two bytes of data a way of passing the ICQ Identification Number, and 0x3030 is just the default when you get your copy of Deep Throat?

Threat Low, just another person looking for a trojan installed by someone else that they can utilize

---

Detect #7

11:12:12.128597 172.31.0.122.8080 > NET.TWO.86.47.3263: . ack 1732172668 win 33304 <nop,nop,timestamp 153069260 1847232> (DF) (ttl 243, id 31720)

11:12:12.128752 NET.TWO.86.47.3263 > 172.31.0.122.8080: R 1732172668:1732172668(0) win 0 (ttl 64, id 62867)
11:12:12.129336 NET.TWO.86.47.3263 > 172.31.0.122.8080: R 1732172668:1732172668(0) win 0 (ttl 64, id 62867)

Active Targeting? Definitely

History No previous contact seen with this host in the previous five days

Technique May be an extremely slow, stealthy network mapping

Analysis The foreign host sends the third part of the three-way TCP handshake to my firewall, the problem being that there is no evidence of the first two parts of the handshake ever occurring. The firewall, knowing that this is an invalid ACK, responds by sending a RESET back to the foreign host. This could be a technique to map our network, while making the datagram appear to be just erroneous. It is a successful method as many other techniques have received the "silent treatment" from our firewall, but this one worked well in getting a response.

Threat Low. Everyday there is someone mapping our network, it is just a fact of life

Detect #8

07:57:16.225104 207.127.234.146 > 255.255.255.255: icmp: echo request (ttl 239, id 1750)
10:45:14.807939 207.127.234.146 > 255.255.255.255: icmp: echo request (ttl 239, id 1862)

Active Targeting?	Not my specific hosts, but my net
History	No previous contact seen with this host in the previous five days
Technique	PING sent to broadcast address, likely as part of a Denial of Service attack
Analysis	PINGing a broadcast address is typically an attempt to get a large number of hosts to respond with a Echo Reply back to the (spoofed) Source address. It is interesting to note that these two datagrams are separated by almost three hours. This might suggest that I am indeed seeing a very small slice of a much larger DOS attack.
Threat	Low.

Detect #9

23:40:04.007927 4.48.149.55.31790 > 255.255.255.255.31789: udp 1 (ttl 112, id 64572)
23:40:04.101725 4.48.149.55.31790 > 255.255.255.255.31789: udp 1 (ttl 112, id 2877)

Active Targeting?	Not my specific hosts, but my net
History	No previous contact seen with this host in the previous eight days
Technique	Scanning a broadcast address looking for Hack-A-Tack trojan
Analysis	Robert Grahams FAQ on Firewalls describes the Hack-A-Tack Trojan, and these characteristics match what I am seeing. It has a built in scanner which operates on port 31790, and port 31789 is the Control connection. The Source address is a PPP connection at an ISP, so likely it is someone who has intentionally loaded the Hack-A-Tack client and is searching for hosts with the Hack-A-Tack Server loaded.

Threat Low, just someone fishing for a Trojan

Detect #10

14:43:12.484025 209.144.217.20.53 > NET.TWO.86.47.53: SF 1562698825:1562698825(0) win 1028 (ttl 30, id 39426)

Active Targeting? Yes, aimed right at my firewall

History No previous contact seen with this host in the previous eight days

Technique Stealthy SYN-FIN scan looking for DNS server

Analysis This appears to be an attempt to scan for a DNS server, while not attracting any attention. First they are trying to evade detection by sending a single datagram. Secondly they have set the SYN-FIN flags to avoid logging by a firewall. It may also be a scan to look for a host, any host, and they have used port 53 as it is also a port which is commonly not logged by firewalls (so I am told).

Threat Low