Global Information Assurance Certification Paper

*** Northcutt, this was done with windump. I am astounded at some of these detects, full points for home field advantage, accuracy is really good, six and nine have aspects that I have never seen before so he gets that bonus. I will give this one a draft grade of 95 and the panel can make any adjustments. 95 ***

10 Detects for SANS GIAC Intrusion Analyst Certification

Tony P. Adams

April 8, 2000

Attended:
SANS 2000 in Orlando, Florida
March 21 – 25, 2000

Detect #1

29-Mar-00 12:50:44 63.73.208.143.7687 > A.B.C.245.138: udp 1
29-Mar-00 12:50:44 63.73.208.143.7688 > A.B.C.245.139: udp 1
29-Mar-00 12:50:44 63.73.208.143.7689 > A.B.C.245.140: udp 1
29-Mar-00 12:50:44 63.73.208.143.7690 > A.B.C.245.141: udp 1
....
29-Mar-00 12:50:44 63.73.208.143.7767 > A.B.C.245.218: udp 1
29-Mar-00 12:50:44 63.73.208.143.7768 > A.B.C.245.219: udp 1
29-Mar-00 12:50:44 63.73.208.143.7769 > A.B.C.245.220: udp 1
29-Mar-00 12:50:44 63.73.208.143.7770 > A.B.C.245.221: udp 1

Trace Information: This trace was captured on our DMZ
Active Targeting: Yes
History: None previously
Technique: An automated high speed UPD port scan targeted at a single host.
Analysis: This is a host scan to determine what UPD ports are open on the targeted machine. The originator of the scan does not appear to be attempting to hide his identity, unless this is being run through a compromised machine. Upon tracing back the IP address we were able to determine that it belonged to a cable modem user with Prestige.net.
Threat: While the scan is maybe for malicious purposes it would be a LOW risk. The low risk is due to the system being up-to-date on patches and only allowing HTTP connections.

Detect #2

30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.53: F 15341:15341(0) win 4096
30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.54: F 15341:15341(0) win 4096
30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.55: F 15341:15341(0) win 4096
30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.56: F 15341:15341(0) win 4096
30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.57: F 15341:15341(0) win 4096
30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.58: F 15341:15341(0) win 4096
30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.59: F 15341:15341(0) win 4096
30-Mar-00 21:42:48 63.73.208.143.24925 > A.B.C.245.60: F 15341:15341(0) win 4096

Trace Information: This trace was captured on our DMZ.
Active Targeting: Yes
History: Had a UPD port scan from this same IP address 33 hours earlier
Technique: An automated high speed Fin TCP port scan. Notice the source port and sequence numbers do not change throughout the scan.
Analysis: This is a host scan to determine what TCP ports are open on the machine. The scanner is sending packets with the FIN bit flag set in an attempt to have RESET responses from open/listening TCP ports. The originator of the scan does not appear to be attempting to hide his identity, unless this is being run through a compromised machine. Upon tracing back the IP address we were able to determine that it belonged to a cable modem user with Prestige.net. Due to the time space from the earlier scan it could be possible the individual is port scanning a large range of IP address. Upon reviewing this scan we forwarded the logs to Prestige.net administrators and are awaiting a response.
Threat: While the scan maybe for malicious purposes it would be a MEDIUM risk. The risk being that the scanner should locate the open port 80, which there are numerous known exploits.

Detect #3

13:52:45 38.2.99.101.9513 > A.B.C.245.9999:
13:53:38 38.2.99.101.9522 > A.B.C.245.31337:
13:54:39 38.2.99.101.9524 > A.B.C.245.23:
13:55:22 38.2.99.101.9525 > A.B.C.245.12345:
13:56:31 38.2.99.101.9527 > A.B.C.245.20034:
13:58:25 38.2.99.101.9529 > A.B.C.246.9999:
13:59:36 38.2.99.101.9533 > A.B.C.246.31337:
14:00:33 38.2.99.101.9537 > A.B.C.246.23:
14:01:12 38.2.99.101.9538 > A.B.C.246.12345:
14:02:22 38.2.99.101.9542 > A.B.C.246.20034:

Trace Information: This trace was captured on our DMZ
Active Targeting: Yes
History: None previously
Technique: A network scan targeting Trojan/backdoor ports. Averages about 1 minute between scans but source ports don't jump very much.
Analysis: This is an attempt to locate commonly known Trojans/Backdoors, such as Back Orifice and Netbus. Looking at the time of each probe, I am not sure if a manual or an automated process is being run against a range of IP addresses. The reason for this indecision is that the probes on the systems I can monitor are approximately 1 minute apart from each other. If this were a stealth type attack the times would be further apart, or if this was an automated scan of a couple of machines the times would most likely be closer together. However, the source ports are close together indicating the machine is not very busy or the source port is being manipulated. It does not appear the attacker is attempting to hide his address unless it is using a compromised machine. The IP address being used belongs to PSI.net, probably part of a dial-in pool.
Threat: This scan would be a MEDIUM risk, due to its malicious purposes. Each machine in the DMZ is up-to-date on security and software patches, as well as anti-virus software. The anti-virus software detects most Trojan related applications/files. The machines in the DMZ do not have access to the internal network.

Detect #4

14:46:28 proxy.scan.com.3128 > X.Y.Z.230.3128: SF 1337861729:1337861729 (0) win 1028
14:46:28 proxy.scan.com.3128 > X.Y.Z.231.3128: SF 1337861729:1337861729 (0) win 1028
14:46:28 proxy.scan.com.3128 > X.Y.Z.232.3128: SF 1337861729:1337861729 (0) win 1028
14:46:28 proxy.scan.com.3128 > X.Y.Z.233.3128: SF 1337861729:1337861729 (0) win 1028
14:46:28 proxy.scan.com.3128 > X.Y.Z.234.3128: SF 1337861729:1337861729 (0) win 1028

Trace Information: This trace was captured on a corporate division DMZ.
Active Targeting: Yes
History: None previously
Technique: An automated high-speed network scan, targeting port 3128. Notice that source port and sequence numbers do not change during the scan. The SYN and FIN flags set, which are anomalous, along with a destination port of 3128.
Analysis: This is an attempt to determine what host on a specified range of addresses will respond with open port 3128. Port 3128 is commonly probed for squid proxy. By locating a available proxy the individual can redirect services so that it looks like attacks/intrusions are coming from your site.
Threat: This scan would constitute a LOW risk to this network. Squid proxy is not used on these machines, which helps make this a manageable risk.

Detect #5

03-Apr-00 13:48:31 38.222.85.2.20000 > A.B.C.2.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]
03-Apr-00 13:48:31 38.222.85.2.20000 > A.B.C.3.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]
03-Apr-00 13:48:31 38.222.85.2.20000 > A.B.C.4.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]
03-Apr-00 13:48:31 38.222.85.2.20000 > A.B.C.5.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]
03-Apr-00 13:48:32 38.222.85.2.20000 > A.B.C.6.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]
03-Apr-00 13:48:32 38.222.85.2.20000 > A.B.C.7.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]
03-Apr-00 13:48:32 38.222.85.2.20000 > A.B.C.8.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]
03-Apr-00 13:48:32 38.222.85.2.20000 > A.B.C.9.111: S 105148:105148(0) win 8192 <mss 1460> (DF) [tos 0x10]

Trace Information: This trace was captured on our DMZ.
Active Targeting: Yes
History: None previously
Technique: An automated high-speed network scan, targeting port 111. Notice that source port, sequence numbers, and destination port do not change during the scan.
Analysis: This is an attempt to determine what host on a specified range of addresses will respond with open port 111. Port 111 is commonly probed for portmapper. With Port 111 numerous vulnerabilities exist that could allow a remote attacker to trick the service into executing arbitrary commands on the system with root privileges. The IP address being used belongs to PSI.net, probably part of a dial-in pool.
Threat: This scan is a LOW risk to this network, due to the machines being scanned are windows machines.

Detect #6

04-Apr-00 13:52:08.767368 38.222.85.2 > A.B.C.8: icmp: echo request (frag 42:512@0+)
04-Apr-00 13:52:08.768019 38.222.85.2 > A.B.C.8: (frag 42:512@512+)
04-Apr-00 13:52:08.768549 38.222.85.2 > A.B.C.8: (frag 42:512@1024+)
04-Apr-00 13:52:08.768980 38.222.85.2 > A.B.C.8: (frag 42:512@1536+)
04-Apr-00 13:52:08.769275 38.222.85.2 > A.B.C.8: (frag 42:512@2048+)
04-Apr-00 13:52:08.769504 38.222.85.2 > A.B.C.8: (frag 42:512@2560+)
04-Apr-00 13:52:08.769732 38.222.85.2 > A.B.C.8: (frag 42:512@3072+)
04-Apr-00 13:52:08.769959 38.222.85.2 > A.B.C.8: (frag 42:512@3584+)
04-Apr-00 13:52:08.770411 38.222.85.2 > A.B.C.8: (frag 42:5@4096)
04-Apr-00 13:52:08.779000 38.222.85.2 > A.B.C.8: icmp: echo request

Trace Information: This trace was captured on our DMZ.
Active Targeting: Yes
History: This IP address did a scan of our IP address range for host with open port 111 (portmapper) 24 hours earlier.
Technique: Direct attempt at a denial of service attack, by sending fragmented ping packets.
Analysis: This is a deliberate attempt to take this machine offline. The attacker is sending fragmented ping packets, which some TCP stacks can not properly handle. The attack can cause a machine to hang thus the denial of service. This could be a form of the "Ping of Death". The IP address being used belongs to PSI.net, probably part of a dial-in pool.
Threat: This would constitute a HIGH threat due to the deliberate attempt to take the system offline.

Detect #7

13:42:35 38.5.20.12 > A.B.C.0: icmp: echo request
13:42:35 38.5.20.12 > A.B.C.255: icmp: echo request
13:45:19 38.5.20.12 > A.B.C.8: icmp: time stamp request
13:45:19 38.5.20.12 > A.B.C.8: icmp: address mask request
13:45:19 38.5.20.12 > A.B.C.11: icmp: time stamp request
13:45:19 38.5.20.12 > A.B.C.11: icmp: address mask request

Trace Information: This trace was captured on our DMZ.
Active Targeting: Yes
History: None previously
Technique: Using ICMP to attempt to map out our network. First, a broadcast to .0 and .255 to gain information on the operating system used. Secondly, a time stamp and address mask request.
Analysis: This is an intelligence-gathering scan to determine the structure of our network. An initial ICMP broadcast was sent on both the old BSD and windows broadcast address. This can help provide information on the type of operating systems being used. Then it was followed by an address mask request, which could provide more information about the structure of our network. The scanner also did a time stamp request, which can provide additional intelligence to the scanner. The IP address being used belongs to PSI.net, probably part of a dial-in pool.
Threat: This scan would be a MEDIUM risk. In this case the scanner was able to get the information requested. Since that time this has become a LOW risk for steps have been taken to resolve these vulnerabilities.

Detect #8

21:45:29.180479 host20-245.58516 > host20-243.39741: udp 0 (frag 54751:36@0+)
21:45:29.262189 truncated-ip - 3 bytes missing!host20-245 > host20-243.: (frag 54751:4@24)

23:22:40.749511 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.751140 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.752601 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.754091 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.755541 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.757033 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.758484 host20-245.58516 > host20-243. 39741: udp 28 (frag 57138:36@0+)
23:22:40.759978 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.761433 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.762918 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.765484 host20-245.58516 > host20-243. 39741: udp 28 (frag 57138:36@0+)
23:22:40.767044 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.768504 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.769993 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.771442 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.772931 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.774380 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.775870 host20-245 > host20-243: (frag 57138:3@32)
23:22:40.777318 host20-245.58516 > host20-243.39741: udp 28 (frag 57138:36@0+)
23:22:40.778816 host20-245 > host20-243: (frag 57138:3@32)

Trace Information: This trace was captured on my home cable modem.
Active Targeting: Yes
History: None previously
Technique: Attacker is sending two fragmented packets with pathological offsets. Then a different series of two fragmented packets with pathological offsets is repeatedly sent. Notice the source port, destination port, and fragment ID do not change throughout either scan.
Analysis: This is an attempted Denial of Service attack against the host. The first attack is referred to as a Teardrop attack. The attack uses fragmented IP packets with a negative offset in an attempt to disable the host. Less than two hours later, a different set of fragmented packets with a negative offset was repeatedly sent to the same host. This attack appears to be a variation of the original Teardrop attack, possible Teardrop #2. Both of these attacks can potentially work because TCP does not handle negative math well.
Threat: There would be a HIGH risk associated with this scan. If this attack is successful the system will not be available for service until after a system reboot.

Detect #9

04:36:21 one.nosy.guy.154.137 > A.B.C.1.137: udp 50 (ttl 109, id 46551)
04:36:22 one.nosy.guy.154.137 > A.B.C.1.137: udp 50 (ttl 109, id 46676)
04:36:24 one.nosy.guy.154.137 > A.B.C.1.137: udp 50 (ttl 109, id 46801)
04:36:25 one.nosy.guy.154.137 > A.B.C.2.137: udp 50 (ttl 109, id 46926)
04:36:27 one.nosy.guy.154.137 > A.B.C.2.137: udp 50 (ttl 109, id 47051)
04:36:28 one.nosy.guy.154.137 > A.B.C.2.137: udp 50 (ttl 109, id 47176)
04:36:30 one.nosy.guy.154.137 > A.B.C.3.137: udp 50 (ttl 109, id 47301)
04:36:32 one.nosy.guy.154.137 > A.B.C.3.137: udp 50 (ttl 109, id 47426)
04:36:33 one.nosy.guy.154.137 > A.B.C.3.137: udp 50 (ttl 109, id 47551)
….
04:39:11 one.nosy.guy.154.137 > A.B.C.49.137: udp 50 (ttl 109, id 64551)
04:39:12 one.nosy.guy.154.137 > A.B.C.49.137: udp 50 (ttl 109, id 64676)
04:39:14 one.nosy.guy.154.137 > A.B.C.49.137: udp 50 (ttl 109, id 64926)
04:39:15 one.nosy.guy.154.137 > A.B.C.50.137: udp 50 (ttl 109, id 65051)
04:39:17 one.nosy.guy.154.137 > A.B.C.50.137: udp 50 (ttl 109, id 65176)
04:39:18 one.nosy.guy.154.137 > A.B.C.50.137: udp 50 (ttl 109, id 65301)
04:39:20 one.nosy.guy.154.137 > A.B.C.51.137: udp 50 (ttl 109, id 65426)
04:39:21 one.nosy.guy.154.137 > A.B.C.51.137: udp 50 (ttl 109, id 65551)
04:39:23 one.nosy.guy.154.137 > A.B.C.51.137: udp 50 (ttl 109, id 65676)

Trace Information: This trace was captured on our DMZ.
Active Targeting: Yes
History: None previously
Technique: Automated network scan where three UDP packets are being sent to each address. The UDP TTL value seems to be manipulated as does the ID, which increments by 125 each time. Source and destination ports are 137, which is Netbios –Name Service on Windows machines.
Analysis: This appears to be a network scan that is attempting to identify Windows machines. The UDP TTL value seems to have been manipulated. A traceroute would set the value between 126 and 130 for a non-windows machine. The ID increments by 125, which indicates these may have been manipulated as well. This scan could be a Netbios Name Query scan, though the source port is consistently 137. The scan could also be an attempt to determine additional information about a Windows machine such as unprotected shares or information about accounts on the system
Threat: This scan would constitute a LOW threat, due to the fact that associated ports 137-139 are blocked at the firewall.

Detect 10

19:20:45 COMPETITOR.5423 > A.B.C.2.80: S 154909:154909(0) win 8192 <mss 1460> (DF) [tos 0x10]
19:20:45 COMPETITOR.5424 > A.B.C.3.80: S 154948:154948(0) win 8192 <mss 1460> (DF) [tos 0x10]
19:20:45 COMPETITOR.5425 > A.B.C.4.80: S 154950:154950(0) win 8192 <mss 1460> (DF) [tos 0x10]
19:20.45 COMPETITOR.5426 > A.B.C.5.80: S 154957:154957(0) win 8192 <mss 1460> (DF) [tos 0x10]
19:20:45 COMPETITOR.5427 > A.B.C.6.80: S 154967:154967(0) win 8192 <mss 1460> (DF) [tos 0x10]
19:20:45 COMPETITOR.5428 > A.B.C.7.80: S 154971:154971(0) win 8192 <mss 1460> (DF) [tos 0x10]
19:20:45 COMPETITOR.5429 > A.B.C.8.80: S 154972:154972(0) win 8192 <mss 1460> (DF) [tos 0x10]
19:20:45 COMPETITOR.5430 > A.B.C.9.80: S 154975:154975(0) win 8192 <mss 1460> (DF) [tos 0x10]

Trace Information: This trace was captured on our DMZ.
Active Targeting: Yes
History: None previously
Technique: Rapid automated scan of network addresses targeting port 80.
Analysis: This is a network scan to determine if any systems will respond with an open port 80 (http). Originally, thought was this was someone looking for a web server to attempt known vulnerabilities. A lot of "out of the box" web servers contain default applications and code that can be easily exploited. Also, cgi-bin scripts are another opportunity for exploitation. However, after researching the IP address of the attacker it was found to be from a pool belonging to one of our biggest competitors. It is now believed they where trying to locate additional web servers to obtain additional information on our company. However, we will not rule out the exploitation possibility.
Threat: This scan would be a LOW-MEDIUM risk. The reason for this is that the only web server available in that range of addresses is our known public site, which is up-to-date on software and patches. However, if the pages where modified without permission company integrity could be damaged. This machine only contains public information with read only permissions. This machine does not have a connection into our corporate network.

Last Updated: May 23rd, 2017

Upcoming Training

Mentor Session - SEC503	**Oceanside, CA**	**May 29, 2017 - Jun 29, 2017**	**Mentor**
Security Operations Center Summit & Training	**Washington, DC**	**Jun 05, 2017 - Jun 12, 2017**	**Live Event**
SANS Houston 2017	**Houston, TX**	**Jun 05, 2017 - Jun 10, 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**
SANS Baltimore Fall 2017	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Baltimore September 2017 - SEC503: Intrusion Detection In-Depth	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**vLive**
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 Ottawa SEC503	**Ottawa, ON**	**Oct 16, 2017 - Oct 21, 2017**	**Community SANS**
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**vLive**
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**
SIEM & Tactical Analytics Summit & Training	**Scottsdale, AZ**	**Nov 28, 2017 - Dec 05, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**