Global Information Assurance Certification Paper

*** Northcutt, A great job, I really enjoyed reading it! Detect 1 and 3 were super special. We cover 3 in Judy's course, but never saw the 111:111 twist in the field so a 5 point bonus is in order for helping us to track a code branch. Thank you for bringing the traces to life. 93 *

Practical Exam for GIAC Intrusion Analyst Certification

Name: Marc E. Labram
Date: April 19, 2000

Introduction

This document contains an analysis of ten network traces to complete the practical part of the SANS GIAC Intrusion Detection Analyst Certification.

Note: IP addresses have been "sanitized" for privacy purposes.

Trace #1

Active Targeting:

Yes

History:

Yes. There have been previous scans from this particular Asian ISP. The System Administrator of goodguy-hacked.com noticed an unauthorized account called zippy on the machine.

Analysis:

This particular trace shows that they were scanning for an open UDP port 5135, the SGI Object Server. As you can see goodguy-a.com and goodguy-b.com answered back with a port unreachable, but open on goodguy-hacked.com

Intent:

The attacker was able to exploit a known hole in SGI's Object Server, which allows a remote user to add a local account.

The following is from the syslog on goodguy-hacked.com:

Apr 15 21:07:59 6C: goodguy-hacked.com telnetd[5020]: connect from some.edu
Apr 15 21:08:18 6E: goodguy-hacked.com login[5021]: ?@some.edu as zippy

Log file:

21:06:26.707866 badguy.com.26614 > goodguy-a.com.5135: udp 52
21:06:26.708960 badguy.com.26614 > goodguy-a.com.5135: udp 52
21:06:26.711804 goodguy-a.com > badguy.com: icmp: goodguy-a.com udp port 5135 unreachable
21:06:26.712748 goodguy-a.com > badguy.com: icmp: goodguy-a.com udp port 5135 unreachable
21:07:01.234448 badguy.com.26616 > goodguy-b.com.5135: udp 52
21:07:01.235528 badguy.com.26616 > goodguy-b.com.5135: udp 52
21:07:01.238380 goodguy-b.com > badguy.com: icmp: goodguy-b.com udp port 5135 unreachable
21:07:01.239430 goodguy-b.com > badguy.com: icmp: goodguy-b.com udp port 5135 unreachable
21:07:16.632941 badguy.com.26617 > goodguy-hacked.com.5135: udp 52
21:07:16.633974 badguy.com.26617 > goodguy-hacked.com.5135: udp 52
21:07:16.668785 goodguy-hacked.com.5135 > badguy.com.26617: udp 69
21:07:16.669475 goodguy-hacked.com.5135 > badguy.com.26617: udp 69
21:07:16.897641 badguy.com.26617 > goodguy-hacked.com.5135: udp 308
21:07:16.898367 badguy.com.26617 > goodguy-hacked.com.5135: udp 308
21:07:17.838778 goodguy-hacked.com.5135 > badguy.com.26617: udp 41
21:07:17.839684 goodguy-hacked.com.5135 > badguy.com.26617: udp 41

Trace #2

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

The intruder appears to be doing a network scan searching for subnet masks. The router 10.15.63.232 is unable to forward the IP datagram because of an access control list, so it replies to badguy.com with an ICMP admin prohibited error.

Intent:

The intruder is performing some initial reconnaissance of the network in preparation for future attacks.

Log file:

15:10:52.768400 badguy.com > 10.10.3.0: icmp: echo request
15:10:52.768403 badguy.com > 10.10.3.63: icmp: echo request

15:10:54.377316 badguy.com > 10.10.3.64: icmp: echo request
15:10:54.379635 badguy.com > 10.10.3.128: icmp: echo request
15:10:54.382354 badguy.com > 10.10.3.127: icmp: echo request
15:10:54.385908 badguy.com > 10.10.3.191: icmp: echo request
15:10:54.837281 badguy.com > 10.10.3.192: icmp: echo request
15:10:54.842209 badguy.com > 10.10.3.255: icmp: echo request
15:10:54.842211 badguy.com > 10.10.4.0: icmp: echo request
15:10:54.845473 badguy.com > 10.10.4.63: icmp: echo request
15:10:54.848996 badguy.com > 10.10.4.64: icmp: echo request
15:10:54.849431 badguy.com > 10.10.4.127: icmp: echo request
15:10:54.851292 badguy.com > 10.10.4.128: icmp: echo request
15:10:54.856367 badguy.com > 10.10.4.191: icmp: echo request
15:10:54.861662 badguy.com > 10.10.4.192: icmp: echo request
15:10:54.866796 badguy.com > 10.10.4.255: icmp: echo request
<SNIP>
15:11:00.243307 10.15.63.232 > badguy.com: icmp: host 10.10.3.64 unreachable - admin prohibited filter
15:11:00.246468 10.15.63.232 > badguy.com: icmp: host 10.10.3.128 unreachable - admin prohibited filter
15:11:00.250829 10.15.63.232 > badguy.com: icmp: host 10.10.4.63 unreachable - admin prohibited filter

Trace #3

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

Our Shadow console flagged this intruder, which performed a sequential scan of 64426 machines. Breaking out the session with tcpdump revealed the scan started with 10.10.0.1 and ended with 10.10.255.254. The intruder sent a packet to port 53 on each machine with the SYN flag set. Each of our name servers 10.10.1.1 and 10.10.1.4, responded with a SYN/ACK. The source port of 2666 and the 111:111(0) win 0 is the same as the IMAP scan signature. In addition, the signature is almost same on the RESET that the intruder sends back, except the sequence numbers are 112:112.

Intent:

It appears that they were scanning for DNS servers and trying to get the version of bind.

Log file:

```
06:03:32.807242 badguy.com.2666 > 10.10.0.1.53: S 111:111(0) win 0
06:03:32.866145 badguy.com.2666 > 10.10.0.4.53: S 111:111(0) win 0
06:03:32.866148 badguy.com.2666 > 10.10.0.5.53: S 111:111(0) win 0
06:03:32.866970 badguy.com.2666 > 10.10.0.2.53: S 111:111(0) win 0
06:03:32.866976 badguy.com.2666 > 10.10.0.3.53: S 111:111(0) win 0
06:03:32.866988 badguy.com.2666 > 10.10.0.9.53: S 111:111(0) win 0
06:03:32.866990 badguy.com.2666 > 10.10.0.7.53: S 111:111(0) win 0
06:03:32.866998 badguy.com.2666 > 10.10.0.6.53: S 111:111(0) win 0
06:03:32.867009 badguy.com.2666 > 10.10.0.8.53: S 111:111(0) win 0
<SNIP>
06:03:33.013354 badguy.com.2666 > 10.10.1.111.53: S 111:111(0) win 0
06:03:33.013356 badguy.com.2666 > 10.10.1.112.53: S 111:111(0) win 0
06:03:33.014269 10.10.1.1.53 > badguy.com.2666: S 700799081:700799081(0) ack 112 win 32768 <mss 4312> (DF)
06:03:33.014272 10.10.1.4.53 > badguy.com.2666: S 320076960:320076960(0) ack 112 win 32768 <mss 4312> (DF)
06:03:33.014704 badguy.com.2666 > 10.10.1.113.53: S 111:111(0) win 0
06:03:33.015167 badguy.com.2666 > 10.10.1.114.53: S 111:111(0) win 0
<SNIP>
06:03:33.095727 badguy.com.2666 > 10.10.1.199.53: S 111:111(0) win 0
06:03:33.095738 badguy.com.2666 > 10.10.1.200.53: S 111:111(0) win 0
06:03:33.127731 badguy.com.2666 > 10.10.1.1.53: R 112:112(0) win 0
06:03:33.127744 badguy.com.2666 > 10.10.1.4.53: R 112:112(0) win 0
06:03:33.144783 badguy.com.2666 > 10.10.1.201.53: S 111:111(0) win 0
06:03:33.146140 badguy.com.2666 > 10.10.1.204.53: S 111:111(0) win 0
<SNIP>
06:04:25.722527 badguy.com.2666 > 10.10.255.253.53: S 111:111(0) win 0
06:04:25.722540 badguy.com.2666 > 10.10.255.254.53: S 111:111(0) win 0
06:04:42.502170 badguy.com.1101 > 10.10.1.1.53: 16549+ TXT CHAOS)? VERSION.BIND. (30)
06:04:42.504336 10.10.1.1.53 > badguy.com.1101: 16549* 1/0/0 CHAOS) TXT  (63)
06:04:43.124673 badguy.com.1101 > 10.10.1.4.53: 34255+ TXT CHAOS)? VERSION.BIND. (30)
06:04:43.126981 10.10.1.4.53 > badguy.com.1101: 34255* 1/0/0 CHAOS) TXT  (63)
```

Trace #4

Active Targeting:

Yes

History:

Yes. We have had multiple scans with various source addresses from this country.

Analysis:

This one of our main web servers, so all ports except port 80 denied. The intruder tried several times to access ports 23 (telnet), 7 (echo), 13 (daytime), and 19 (chargen). The intruder sends a SYN to a closed port. The web server sends a RESET back to the intruder because the port is not available.

Intent:

The intruder could be scanning to check for a possible DOS attack on the server with ports 7 (echo), and 19 (chargen).

Log file:

09:07:18.692828 badguy.com.1048 > webserver.com.23: S 3108311:3108311(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:18.696782 webserver.com.23 > badguy.com.1048: R 0:0(0) ack 1 win 0 (DF)
09:07:19.943580 badguy.com.1048 > webserver.com.23: S 3108311:3108311(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:19.944466 webserver.com.23 > badguy.com.1048: R 0:0(0) ack 1 win 0 (DF)
09:07:21.213931 badguy.com.1048 > webserver.com.23: S 3108311:3108311(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:21.214436 webserver.com.23 > badguy.com.1048: R 0:0(0) ack 1 win 0 (DF)
09:07:31.130223 badguy.com.1049 > webserver.com.13: S 3121994:3121994(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:31.131204 webserver.com.13 > badguy.com.1049: R 0:0(0) ack 3121995 win 0 (DF)
09:07:32.438795 badguy.com.1049 > webserver.com.13: S 3121994:3121994(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:32.440865 webserver.com.13 > badguy.com.1049: R 0:0(0) ack 1 win 0 (DF)
09:07:33.691129 badguy.com.1049 > webserver.com.13: S 3121994:3121994(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:33.695140 webserver.com.13 > badguy.com.1049: R 0:0(0) ack 1 win 0 (DF)
09:07:34.942640 badguy.com.1049 > webserver.com.13: S 3121994:3121994(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:34.944211 webserver.com.13 > badguy.com.1049: R 0:0(0) ack 1 win 0 (DF)
09:07:42.157271 badguy.com.1050 > webserver.com.7: S 3133018:3133018(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:42.168457 webserver.com.7 > badguy.com.1050: R 0:0(0) ack 3133019 win 0 (DF)
09:07:43.450237 badguy.com.1050 > webserver.com.7: S 3133018:3133018(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:43.451208 webserver.com.7 > badguy.com.1050: R 0:0(0) ack 1 win 0 (DF)
09:07:44.720924 badguy.com.1050 > webserver.com.7: S 3133018:3133018(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:44.721429 webserver.com.7 > badguy.com.1050: R 0:0(0) ack 1 win 0 (DF)
09:07:45.971998 badguy.com.1050 > webserver.com.7: S 3133018:3133018(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:45.986077 webserver.com.7 > badguy.com.1050: R 0:0(0) ack 1 win 0 (DF)
09:07:53.663315 badguy.com.1051 > webserver.com.19: S 3144532:3144532(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:53.664271 webserver.com.19 > badguy.com.1051: R 0:0(0) ack 3144533 win 0 (DF)
09:07:54.984370 badguy.com.1051 > webserver.com.19: S 3144532:3144532(0) win 8192 <mss 536,nop,nop,sackOK> (DF)

09:07:55.011952 webserver.com.19 > badguy.com.1051: R 0:0(0) ack 1 win 0 (DF)
09:07:56.247915 badguy.com.1051 > webserver.com.19: S 3144532:3144532(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
09:07:56.255836 webserver.com.19 > badguy.com.1051: R 0:0(0) ack 1 win 0 (DF)

Trace #5

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

The intruder scanned the entire subnet searching for port 143 (IMAP). This is a scripted attack with sequential source port numbers. Also note the sequence numbers are incrementing by 512.

Intent:

The intruder is scanning port 143 (IMAP) for possible future exploit.

Log file:

02:27:16.877031 badguy.com.2345 > 10.10.167.255.143: S 1985478161:1985478673(0) win 32120 (DF)
02:27:16.877466 badguy.com.2346 > 10.10.167.254.143: S 1985478673:1985479185(0) win 32120 (DF)
02:27:16.878026 badguy.com.2347 > 10.10.167.253.143: S 1985479185:1985479697(0) win 32120 (DF)
02:27:16.878034 badguy.com.2348 > 10.10.167.252.143: S 1985479697:1985480209(0) win 32120 (DF)
02:27:16.878046 badguy.com.2349 > 10.10.167.251.143: S 1985480209:1985480721(0) win 32120 (DF)
02:27:16.878049 badguy.com.2350 > 10.10.167.250.143: S 1985480721:1985481233(0) win 32120 (DF)
02:27:16.878064 badguy.com.2351 > 10.10.167.249.143: S 1985481233:1985481745(0) win 32120 (DF)
02:27:16.878067 badguy.com.2352 > 10.10.167.248.143: S 1985481745:1985482257(0) win 32120 (DF)
02:27:16.878073 badguy.com.2353 > 10.10.167.247.143: S 1985482257:1985482769(0) win 32120 (DF)

Trace #6

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

Extremely fast random port scan of one of our web servers.

Intent:

The best guess is somebody scanning for known trojans.

Log file:

22:02:40.327446 reallyfast.badguy.com.4003 > scannedhost.com.140: S 1470426769:1470426769(0) win 512
22:02:40.328109 reallyfast.badguy.com.4004 > scannedhost.com.561: S 1478841816:1478841816(0) win 512
22:02:40.329491 reallyfast.badguy.com.4005 > scannedhost.com.518: S 1466588812:1466588812(0) win 512
22:02:40.344156 reallyfast.badguy.com.4006 > scannedhost.com.1080: S 1463019352:1463019352(0) win 512
22:02:40.344978 reallyfast.badguy.com.4007 > scannedhost.com.675: S 1471411072:1471411072(0) win 512
22:02:40.345341 reallyfast.badguy.com.4008 > scannedhost.com.346: S 1477485380:1477485380(0) win 512
22:02:40.346644 reallyfast.badguy.com.4009 > scannedhost.com.624: S 1475285370:1475285370(0) win 512
22:02:40.352437 reallyfast.badguy.com.4010 > scannedhost.com.1348: S 1473611889:1473611889(0) win 512
22:02:40.353792 reallyfast.badguy.com.4011 > scannedhost.com.2232: S 1477827117:1477827117(0) win 512
22:02:40.354671 reallyfast.badguy.com.4012 > scannedhost.com.1476: S 1478943892:1478943892(0) win 512
22:02:41.235218 reallyfast.badguy.com.4013 > scannedhost.com.734: S 1466745158:1466745158(0) win 512
22:02:41.273277 reallyfast.badguy.com.4015 > scannedhost.com.51: S 1468603373:1468603373(0) win 512
22:02:41.273732 reallyfast.badguy.com.4014 > scannedhost.com.10: S 1468461885:1468461885(0) win 512
22:02:41.274303 reallyfast.badguy.com.4018 > scannedhost.com.6715: S 1476079663:1476079663(0) win 512
22:02:41.275180 reallyfast.badguy.com.4016 > scannedhost.com.118: S 1467996519:1467996519(0) win 512
22:02:41.275183 reallyfast.badguy.com.4017 > scannedhost.com.3791: S 1478123006:1478123006(0) win 512
22:02:41.278777 reallyfast.badguy.com.4019 > scannedhost.com.846: S 1467893905:1467893905(0) win 512
22:02:41.294387 reallyfast.badguy.com.4020 > scannedhost.com.64: S 1468804363:1468804363(0) win 512
22:02:41.294390 reallyfast.badguy.com.4021 > scannedhost.com.904: S 1474836892:1474836892(0) win 512
22:02:41.295720 reallyfast.badguy.com.4022 > scannedhost.com.2632: S 1473029573:1473029573(0) win 512
22:02:41.295724 reallyfast.badguy.com.4023 > scannedhost.com.3476: S 1464576361:1464576361(0) win 512

Trace #7

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

Our Shadow sensor flagged on source port 31337 (the text in red). After breaking out the session with tcpdump, it was determined to be normal traffic. The source ports appear to be in a logical sequence 31161, 31198, and 31337. Each transaction followed the rules of a normal three-way handshake (text in green) and termination (text in blue).

Intent:

No malicious intent here, it was just normal traffic.

Log file:

21:18:17.414805 falsealarm.com.31161 > webserver.com.80: S 1452610498:1452610498(0) win 49152 <mss 1460>
21:18:17.415042 webserver.com.80 > falsealarm.com.31161: S 74901565:74901565(0) ack 1452610499 win 8760 <mss 1460> (DF)
21:18:17.482541 falsealarm.com.31161 > webserver.com.80: . ack 1 win 49152 (DF)
21:18:17.482586 falsealarm.com.31161 > webserver.com.80: P 1:471(470) ack 1 win 49152 (DF)
21:18:17.485099 webserver.com.80 > falsealarm.com.31161: P 1:315(314) ack 471 win 8290 (DF)
21:18:17.485503 webserver.com.80 > falsealarm.com.31161: F 315:315(0) ack 471 win 8290 (DF)
21:18:17.523503 falsealarm.com.31161 > webserver.com.80: . ack 1 win 49152 (DF)
21:18:17.545913 falsealarm.com.31161 > webserver.com.80: . ack 316 win 49152 (DF)
21:18:17.564629 falsealarm.com.31161 > webserver.com.80: F 471:471(0) ack 316 win 49152 (DF)
21:18:17.565527 webserver.com.80 > falsealarm.com.31161: . ack 472 win 8290 (DF)
21:18:18.071752 falsealarm.com.31198 > webserver.com.80: S 1457613698:1457613698(0) win 49152 <mss 1460>
21:18:18.072638 webserver.com.80 > falsealarm.com.31198: S 74901580:74901580(0) ack 1457613699 win 8760 <mss 1460> (DF)
21:18:18.131087 falsealarm.com.31198 > webserver.com.80: . ack 1 win 49152 (DF)
21:18:18.133891 falsealarm.com.31198 > webserver.com.80: P 1:487(486) ack 1 win 49152 (DF)
21:18:18.137346 webserver.com.80 > falsealarm.com.31198: . 1:1461(1460) ack 487 win 8274 (DF)
21:18:18.137581 webserver.com.80 > falsealarm.com.31198: P 1461:2776(1315) ack 487 win 8274 (DF)
21:18:18.137585 webserver.com.80 > falsealarm.com.31198: F 2776:2776(0) ack 487 win 8274 (DF)
21:18:18.168256 falsealarm.com.31198 > webserver.com.80: . ack 1 win 49152 (DF)
21:18:18.168697 falsealarm.com.31198 > webserver.com.80: . ack 1 win 49152 (DF)
21:18:18.202551 falsealarm.com.31198 > webserver.com.80: . ack 2777 win 49152 (DF)
21:18:18.246237 falsealarm.com.31198 > webserver.com.80: F 487:487(0) ack 2777 win 49152 (DF)
21:18:18.246974 webserver.com.80 > falsealarm.com.31198: . ack 488 win 8274 (DF)
21:18:21.690130 falsealarm.com.31337 > webserver.com.80: S 1476801098:1476801098(0) win 49152 <mss 1460>
21:18:21.691038 webserver.com.80 > falsealarm.com.31337: S 74901840:74901840(0) ack 1476801099 win 8760 <mss 1460> (DF)
21:18:21.752665 falsealarm.com.31337 > webserver.com.80: . ack 1 win 49152 (DF)

21:18:21.762823 falsealarm.com.31337 > webserver.com.80: P 1:401(400) ack 1 win 49152 (DF)
21:18:21.824932 webserver.com.80 > falsealarm.com.31337: P 1:320(319) ack 401 win 8360 (DF)
21:18:21.827033 webserver.com.80 > falsealarm.com.31337: FP 320:351(31) ack 401 win 8360 (DF)
21:18:21.880733 falsealarm.com.31337 > webserver.com.80: . ack 1 win 49152 (DF)
21:18:21.890458 falsealarm.com.31337 > webserver.com.80: . ack 352 win 49152 (DF)
21:18:21.915641 falsealarm.com.31337 > webserver.com.80: F 401:401(0) ack 352 win 49152 (DF)
21:18:21.916643 webserver.com.80 > falsealarm.com.31337: . ack 402 win 8360 (DF)

Trace #8

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

This is a NID log and the tcpdump session showing that a local user downloaded a password sniffer. After finding the owner of baduser.com address, it determined that it was someone in the Risk Assessment group. The result was he was downloading some "tools" for our test lab.

Intent:

No malicious intent, but was a good NID filter check exercise.

Log file:

=== Intruder Script from Stream File "000420.0907.1.stream.init" ===

IP Header from first packet:

Ethernet source : aa:0:0:0:bb:cc
Ethernet destination : dd:0:0:0:0:ee
Ethernet bytes : 102
Ethernet time : Thu Apr 20 09:07:34 2000
Network protocol : IP
Network source : 10.11.154.63 baduser.com
Network destination : 111.111.112.112 ftpsite.net
Network bytes : 88
Transport protocol : tcp

Transport bytes : 48
Application source : 2650
Application destination : 21
NIT total length : 122
NIT message length : 114

--- The stream script

RETR /Logging/pwdsniff.zip

=== End of Intruder Script from Stream File
"000420.0907.1.stream.init" ===

09:07:06.908333 baduser.com.2650 > ftpsite.net.21: S 192835:192835(0) win 8192 <mss 1460> (DF)
09:07:07.097373 ftpsite.net.21 > baduser.com.2650: S 343085852:343085852(0) ack 192836 win 8760 <mss 1460> (DF)
09:07:07.104263 baduser.com.2650 > ftpsite.net.21: . ack 1 win 8760 (DF)
09:07:07.317208 ftpsite.net.21 > baduser.com.2650: P 1:53(52) ack 1 win 8760 (DF)
09:07:07.323202 baduser.com.2650 > ftpsite.net.21: P 1:17(16) ack 53 win 8708 (DF)
09:07:07.543270 ftpsite.net.21 > baduser.com.2650: P 53:125(72) ack 17 win 8744 (DF)
09:07:07.560866 baduser.com.2650 > ftpsite.net.21: P 17:32(15) ack 125 win 8636 (DF)
09:07:07.773445 ftpsite.net.21 > baduser.com.2650: P 125:170(45) ack 32 win 8729 (DF)
09:07:07.778490 ftpsite.net.21 > baduser.com.2650: P 170:1630(1460) ack 32 win 8729 (DF)
09:07:07.778497 ftpsite.net.21 > baduser.com.2650: P 1630:1680(50) ack 32 win 8729 (DF)
09:07:07.785312 baduser.com.2650 > ftpsite.net.21: . ack 1630 win 8760 (DF)
09:07:07.983489 baduser.com.2650 > ftpsite.net.21: . ack 1680 win 8710 (DF)
09:07:08.017350 ftpsite.net.21 > baduser.com.2650: P 1680:1881(201) ack 32 win 8729 (DF)
09:07:08.023531 baduser.com.2650 > ftpsite.net.21: P 32:40(8) ack 1881 win 8509 (DF)
09:07:08.215659 ftpsite.net.21 > baduser.com.2650: P 1881:1903(22) ack 40 win 8721 (DF)
09:07:08.220496 baduser.com.2650 > ftpsite.net.21: P 40:46(6) ack 1903 win 8487 (DF)
09:07:08.423155 ftpsite.net.21 > baduser.com.2650: P 1903:1931(28) ack 46 win 8715 (DF)
09:07:08.429907 baduser.com.2650 > ftpsite.net.21: P 46:52(6) ack 1931 win 8459 (DF)
09:07:08.579776 ftpsite.net.21 > baduser.com.2650: P 1931:1981(50) ack 52 win 8709 (DF)
09:07:08.588890 baduser.com.2651 > ftpsite.net.3413: S 192847:192847(0) win 8192 <mss 1460> (DF)
09:07:08.737058 ftpsite.net.3413 > baduser.com.2651: S 343087491:343087491(0) ack 192848 win 8760 <mss 1460> (DF)
09:07:08.741178 baduser.com.2651 > ftpsite.net.3413: . ack 1 win 8760 (DF)
09:07:08.742080 baduser.com.2650 > ftpsite.net.21: P 52:60(8) ack 1981 win 8409 (DF)
09:07:08.870296 ftpsite.net.21 > baduser.com.2650: P 1981:2001(20) ack 60 win 8701 (DF)

09:07:08.876174 baduser.com.2650 > ftpsite.net.21: P 60:88(28) ack 2001 win 8389 (DF)
09:07:08.883266 ftpsite.net.3411 > baduser.com.2647: . 20441:21901(1460) ack 1 win 8760 (DF)
09:07:08.891111 baduser.com.2647 > ftpsite.net.3411: . ack 23361 win 8760 (DF)
09:07:09.046687 ftpsite.net.3411 > baduser.com.2647: . 23361:24821(1460) ack 1 win 8760 (DF)
09:07:09.053289 baduser.com.2647 > ftpsite.net.3411: . ack 24821 win 8760 (DF)
09:07:09.054134 ftpsite.net.3411 > baduser.com.2647: . 24821:26281(1460) ack 1 win 8760 (DF)
09:07:09.056049 ftpsite.net.21 > baduser.com.2650: P 2001:2013(12) ack 88 win 8673 (DF)
09:07:09.062372 baduser.com.2650 > ftpsite.net.21: P 88:116(28) ack 2013 win 8377 (DF)
09:07:09.175657 baduser.com.2647 > ftpsite.net.3411: . ack 26281 win 8760 (DF)
09:07:09.224928 ftpsite.net.3411 > baduser.com.2647: FP 26281:26990(709) ack 1 win 8760 (DF)
09:07:09.230626 baduser.com.2647 > ftpsite.net.3411: . ack 26991 win 8051 (DF)
09:07:09.231724 baduser.com.2647 > ftpsite.net.3411: F 1:1(0) ack 26991 win 8051 (DF)
09:07:09.239990 ftpsite.net.21 > baduser.com.2650: P 2013:2071(58) ack 116 win 8645 (DF)
09:07:09.247346 baduser.com.2650 > ftpsite.net.21: P 116:144(28) ack 2071 win 8319 (DF)
09:07:09.386640 ftpsite.net.21 > baduser.com.2644: P 2787:2811(24) ack 330 win 8431 (DF)
09:07:09.386654 ftpsite.net.3411 > baduser.com.2647: . ack 2 win 8760 (DF)
09:07:09.392453 baduser.com.2644 > ftpsite.net.21: F 330:330(0) ack 2811 win 7579 (DF)
09:07:09.406541 ftpsite.net.21 > baduser.com.2650: P 2071:2125(54) ack 144 win 8617 (DF)
09:07:09.459130 ftpsite.net.3413 > baduser.com.2651: . 1:1461(1460) ack 1 win 8760 (DF)
09:07:09.464723 ftpsite.net.3413 > baduser.com.2651: . 1461:2921(1460) ack 1 win 8760 (DF)
09:07:09.472877 baduser.com.2651 > ftpsite.net.3413: . ack 2921 win 8760 (DF)
09:07:09.573190 ftpsite.net.21 > baduser.com.2644: . ack 331 win 8431 (DF)
09:07:09.573747 ftpsite.net.21 > baduser.com.2644: F 2811:2811(0) ack 331 win 8431 (DF)
09:07:09.576733 baduser.com.2650 > ftpsite.net.21: . ack 2125 win 8265 (DF)
09:07:09.579004 baduser.com.2644 > ftpsite.net.21: . ack 2812 win 7579 (DF)

Trace #9

Active Targeting:

Yes

History:

Yes, there have been very large scans from this country in the past.

Analysis:

This is a port scan searching for open ports on the system. Scanner.com sends a SYN packet, victim.com responds with a RESET/ACK on the closed or unavailable ports. If the port was open, victim.com should send scanner.com a SYN/ACK to establish its part of the three-way handshake.

Intent:

Scanner.com is searching for open ports available on the system for possible future exploits.

Log file:

The following is a NID alert message:

ALERT: HEAVY level port scans detected on Fri Apr 21 12:49:04 2000
[Originating from scannerguy.com -> Last known target victim.com]

Corresponding tcpdump trace:

12:42:45.495456 scannerguy.com.1086 > victim.com.4: S 1948141:1948141(0) win 8192 <mss 1460> (DF)
12:42:45.496233 victim.com.4 > scannerguy.com.1086: R 0:0(0) ack 1948142 win 0 (DF)
12:42:45.549071 scannerguy.com.1087 > victim.com.5: S 1948180:1948180(0) win 8192 <mss 1460> (DF)
12:42:45.549843 victim.com.5 > scannerguy.com.1087: R 0:0(0) ack 1948181 win 0 (DF)
12:42:45.595573 scannerguy.com.1088 > victim.com.6: S 1948231:1948231(0) win 8192 <mss 1460> (DF)
12:42:45.600199 victim.com.6 > scannerguy.com.1088: R 0:0(0) ack 1948232 win 0 (DF)
12:42:45.709067 scannerguy.com.1089 > victim.com.7: S 1948344:1948344(0) win 8192 <mss 1460> (DF)
12:42:45.709970 victim.com.7 > scannerguy.com.1089: R 0:0(0) ack 1948345 win 0 (DF)
12:42:45.737922 scannerguy.com.1090 > victim.com.8: S 1948385:1948385(0) win 8192 <mss 1460> (DF)
12:42:45.738653 victim.com.8 > scannerguy.com.1090: R 0:0(0) ack 1948386 win 0 (DF)
12:42:45.815684 scannerguy.com.1091 > victim.com.9: S 1948446:1948446(0) win 8192 <mss 1460> (DF)
12:42:45.817794 victim.com.9 > scannerguy.com.1091: R 0:0(0) ack 1948447 win 0 (DF)
12:42:45.867849 scannerguy.com.1092 > victim.com.10: S 1948495:1948495(0) win 8192 <mss 1460> (DF)
12:42:45.868636 victim.com.10 > scannerguy.com.1092: R 0:0(0) ack 1948496 win 0 (DF)
12:42:45.895261 scannerguy.com.1093 > victim.com.11: S 1948539:1948539(0) win 8192 <mss 1460> (DF)
12:42:45.896148 victim.com.11 > scannerguy.com.1093: R 0:0(0) ack 1948540 win 0 (DF)
12:42:45.938215 scannerguy.com.1094 > victim.com.12: S 1948579:1948579(0) win 8192 <mss 1460> (DF)
12:42:45.939245 victim.com.12 > scannerguy.com.1094: R 0:0(0) ack 1948580 win 0 (DF)
12:42:46.101399 scannerguy.com.1096 > victim.com.14: S 1948739:1948739(0) win 8192 <mss 1460> (DF)
12:42:46.102088 victim.com.14 > scannerguy.com.1096: R 0:0(0) ack 1948740 win 0 (DF)
12:42:46.139085 scannerguy.com.1097 > victim.com.15: S 1948782:1948782(0) win 8192 <mss 1460> (DF)
12:42:46.143613 victim.com.15 > scannerguy.com.1097: R 0:0(0) ack 1948783 win 0 (DF)

12:42:46.268069 scannerguy.com.1098 > victim.com.16: S 1948910:1948910(0) win 8192 <mss 1460> (DF)
12:42:46.268858 victim.com.16 > scannerguy.com.1098: R 0:0(0) ack 1948911 win 0 (DF)
12:42:46.377366 scannerguy.com.1099 > victim.com.17: S 1949005:1949005(0) win 8192 <mss 1460> (DF)
12:42:46.378721 victim.com.17 > scannerguy.com.1099: R 0:0(0) ack 1949006 win 0 (DF)
12:42:46.446394 scannerguy.com.1101 > victim.com.19: S 1949091:1949091(0) win 8192 <mss 1460> (DF)
12:42:46.447384 victim.com.19 > scannerguy.com.1101: R 0:0(0) ack 1949092 win 0 (DF)
12:42:46.489427 scannerguy.com.1102 > victim.com.20: S 1949133:1949133(0) win 8192 <mss 1460> (DF)
12:42:46.489942 victim.com.20 > scannerguy.com.1102: R 0:0(0) ack 1949134 win 0 (DF)
<SNIP>

Trace #10

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

This site scanned our entire Class B network. The Technical Contact of the domain sent this in response to us inquiring about the scan:

```
Thanks for the notification.
We found the source of the probe.
It was from an internal machine, this port scan was accidental.  The probe
was intended to be run on our internal network.
If any other related issues come up please let us know.

Sorry for the mishap,
Technical Guy
```

Intent:

No malicious intent involved, it appears that it was an accidental scan of our network.

Log file:

```
PortScan Alert
Thursday, April 20, 2000 8:52 AM CDT
Port Scan detected.
Origination IP address : 12.13.14.14
Destination IP address : CLASS "B" NETWORK 10.10.
```

```
08:51:01.045522 scannerguy.com.41409 > victim.com.47: S 971212:971212(0) win 8192 <mss 1460> (DF)
08:51:01.045965 scannerguy.com.41410 > victim.com.48: S 971228:971228(0) win 8192 <mss 1460> (DF)
08:51:01.045977 scannerguy.com.41411 > victim.com.49: S 971244:971244(0) win 8192 <mss 1460> (DF)
08:51:01.045979 scannerguy.com.41412 > victim.com.50: S 971260:971260(0) win 8192 <mss 1460> (DF)
08:51:01.045992 scannerguy.com.41413 > victim.com.51: S 971276:971276(0) win 8192 <mss 1460> (DF)
08:51:01.046003 scannerguy.com.41414 > victim.com.52: S 971292:971292(0) win 8192 <mss 1460> (DF)
08:51:01.046461 scannerguy.com.41415 > victim.com.53: S 971308:971308(0) win 8192 <mss 1460> (DF)
08:51:01.046463 scannerguy.com.41416 > victim.com.54: S 971324:971324(0) win 8192 <mss 1460> (DF)
08:51:01.046477 scannerguy.com.41417 > victim.com.55: S 971340:971340(0) win 8192 <mss 1460> (DF)
08:51:01.046489 scannerguy.com.41418 > victim.com.56: S 971356:971356(0) win 8192 <mss 1460> (DF)
08:51:01.046491 scannerguy.com.41419 > victim.com.57: S 971372:971372(0) win 8192 <mss 1460> (DF)
08:51:01.046504 scannerguy.com.41420 > victim.com.58: S 971388:971388(0) win 8192 <mss 1460> (DF)
08:51:01.046518 scannerguy.com.41421 > victim.com.59: S 971404:971404(0) win 8192 <mss 1460> (DF)
08:51:01.047548 scannerguy.com.41422 > victim.com.60: S 971420:971420(0) win 8192 <mss 1460> (DF)
08:51:01.047561 scannerguy.com.41423 > victim.com.61: S 971436:971436(0) win 8192 <mss 1460> (DF)
08:51:01.047567 scannerguy.com.41424 > victim.com.62: S 971452:971452(0) win 8192 <mss 1460> (DF)
08:51:01.047580 scannerguy.com.41425 > victim.com.63: S 971468:971468(0) win 8192 <mss 1460> (DF)
08:51:01.047583 scannerguy.com.41426 > victim.com.64: S 971484:971484(0) win 8192 <mss 1460> (DF)
08:51:01.047740 scannerguy.com.41427 > victim.com.65: S 971500:971500(0) win 8192 <mss 1460> (DF)
08:51:01.047743 scannerguy.com.41428 > victim.com.66: S 971516:971516(0) win 8192 <mss 1460> (DF)
08:51:01.047760 scannerguy.com.41429 > victim.com.67: S 971532:971532(0) win 8192 <mss 1460> (DF)
08:51:01.048824 scannerguy.com.41430 > victim.com.68: S 971548:971548(0) win 8192 <mss 1460> (DF)
08:51:01.048829 scannerguy.com.41433 > victim.com.71: S 971596:971596(0) win 8192 <mss 1460> (DF)
08:51:01.055723 victim.com.47 > scannerguy.com.41409: R 0:0(0) ack 971213 win 0
08:51:01.056192 victim.com.48 > scannerguy.com.41410: R 0:0(0) ack 971229 win 0
08:51:01.057040 victim.com.49 > scannerguy.com.41411: R 0:0(0) ack 971245 win 0
08:51:01.057056 victim.com.50 > scannerguy.com.41412: R 0:0(0) ack 971261 win 0
08:51:01.057351 victim.com.51 > scannerguy.com.41413: R 0:0(0) ack 971277 win 0
08:51:01.058335 victim.com.52 > scannerguy.com.41414: R 0:0(0) ack 971293 win 0
08:51:01.058342 victim.com.54 > scannerguy.com.41416: R 0:0(0) ack 971325 win 0
08:51:01.059513 victim.com.55 > scannerguy.com.41417: R 0:0(0) ack 971341 win 0
08:51:01.060668 victim.com.56 > scannerguy.com.41418: R 0:0(0) ack 971357 win 0
08:51:01.060690 victim.com.57 > scannerguy.com.41419: R 0:0(0) ack 971373 win 0
08:51:01.060692 victim.com.58 > scannerguy.com.41420: R 0:0(0) ack 971389 win 0
08:51:01.065123 victim.com.59 > scannerguy.com.41421: R 0:0(0) ack 971405 win 0
08:51:01.065135 victim.com.60 > scannerguy.com.41422: R 0:0(0) ack 971421 win 0
08:51:01.065165 victim.com.61 > scannerguy.com.41423: R 0:0(0) ack 971437 win 0
08:51:01.065167 victim.com.62 > scannerguy.com.41424: R 0:0(0) ack 971453 win 0
```

```
08:51:01.065179 victim.com.63 > scannerguy.com.41425: R 0:0(0) ack 971469 win 0
08:51:01.065809 victim.com.64 > scannerguy.com.41426: R 0:0(0) ack 971485 win 0
08:51:01.065812 victim.com.65 > scannerguy.com.41427: R 0:0(0) ack 971501 win 0
08:51:01.066384 victim.com.66 > scannerguy.com.41428: R 0:0(0) ack 971517 win 0
08:51:01.068018 victim.com.67 > scannerguy.com.41429: R 0:0(0) ack 971533 win 0
08:51:01.068022 victim.com.68 > scannerguy.com.41430: R 0:0(0) ack 971549 win 0
08:51:01.068036 victim.com.71 > scannerguy.com.41433: R 0:0(0) ack 971597 win 0
```

Last Updated: May 25th, 2017

Upcoming Training

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 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 Baltimore Fall 2017	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, United Kingdom**	**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**
Community SANS Scottsdale SEC503	**Scottsdale, AZ**	**Oct 02, 2017 - Oct 07, 2017**	**Community SANS**
Community SANS Boston SEC503	**Boston, MA**	**Oct 09, 2017 - Oct 14, 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**