Global Information Assurance Certification Paper

*** Northcutt, fine job, accurate, concise, good use of a process. Love the evaluation of the windump against the firewall results. 83 *

Brian Betterton

Introduction

This document provides the "practical" portion of the GIAC Intrusion Detection Level 2 certification exam. Twelve detects, logged between April 12-23, are provided and analyzed. Ten were required, but I was having too much fun to stop. Interestingly, most of these detects were logged on my home DMZ network, outside my firewall. I have an "always-on" cable modem access to the Internet. The sheer number and type of these detects should encourage anyone with this type of home Internet access to install a firewall and perform Intrusion Detection (ID). These detects were logged either by my firewall or with tcpdump. If available, I provide both for correlation.

Analysis Methodology

The methodology used for each of these detects follow the "Simple Information Warfare Methodology" recommended by the SANS Institute during the SANS2000.

Existence: Identify the source
History: Identify their history
Techniques: Identify the techniques used
Targeting: Is there evidence of targeting?
Analysis: What is their intent? The analysis of the detect.

Severity Level

The methodology used for describing the severity level of these detects was recommended by the SANS Institute during the SANS2000. A measurement is required to provide guidance to determine which detects should receive priority over others. The higher the Severity Level, the more serious it is. The formula used is:

(Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a five-point scale that uses the following to help provide some quantitative measurement:

Critical

5	Firewall, Core Router
4	Mail Server
3	
2	Unix Desktop
1	MS-DOS Desktop

Lethal

5	Can gain root access over net
4	DOS attack causes total unavailability
3	User access via sniffed password
2	Confidentiality attack, e.g., null session
1	Attack is unlikely to succeed

System Countermeasures

5	Current OS, latest patches, hardened OS, tcp wrappers, tripwire
4	
3	OS not current, not patched, not hardened, tcp wrapper
2	
1	OS not current, not patched, not hardened

Network Countermeasures

5	Restrictive firewall, well maintained, no backdoors
4	Restrictive firewall, well maintained, some modem & ISDN external access
3	
2	Permissive firewall, poorly maintained, unknown quantities of modem & ISDN external access
1	No firewall

Detects

Detect 1:

Firewall Log:
04/13/2000 00:43:38.016 - TCP connection dropped - Source:24.9.201.189, 3936, WAN - Destination:my.firewall.net, 21, LAN - 'File Transfer (FTP)' - Rule 0

TCPDump:
00:45:35.324468 c817731-a.ankeny1.ia.home.com.3936 > my.firewall.net.ftp: S 3152835603:3152835603(0) win 32120 <mss 1460,sackOK,timestamp 126497[|tcp]> (DF)

Existence: The source, if not spoofed, comes from California, as this WHOIS indicates:

@Home Network (NETBLK-BB1-RDC1-IL-3)
425 Broadway
Redwood City, CA 94063
US

Netname: BB1-RDC1-IL-3
Netblock: 24.9.192.0 - 24.9.207.255

Coordinator:
Operations, Network (HOME-NOC-ARIN)
noc@NOC.HOME.NETabuse@corp.home.net
1-800-872-3595

Record last updated on 22-Jun-1999.
Database last updated on 24-Apr-2000 05:40:41 EDT.

History: None previously observed.

Techniques: This was a port scan for ftp. Since I was scanned only once, this was probably a network scan of many hosts, looking specifically for port 21. I can not be 100% sure of this since my tcpdump capture was looking specifically at traffic to and from my firewall, but this seems the most likely scenario.

Targeting: Not specifically. As this was most likely a scan of multiple hosts, looking for systems with ftp open, then my machine was not specifically targeted. During this first detect, I was filtering tcpdump on my firewall's IP as a destination host. I later changed my filtering to include it as both a source and destination. This is why no RST is seen from my firewall in this trace.

Analysis: This source attempted to see if ftp was available on my firewall, although probably several more hosts as well. As this was the focus of their scanning, the intruder probably has specific ftp vulnerabilities in mind, depending if they find Windows or unix

systems with ftp. They may be looking to break into the actual system or to use it as a potential "ftp-bounce" device to hide their further activities.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since ftp is not allowed either in or out through the firewall (5) and ftp is not a port open on any internal devices (5).

$$(5 + 1) – (5 + 5) = < 0$$

Detect 2:

Firewall Log:
04/09/2000 21:31:29.736 - TCP connection dropped - Source:24.112.107.239, 4326, WAN - Destination:my.firewall.net, 23, LAN - 'Telnet' - Rule 0

TCPDump:
21:28:27.323366 c647691-24.112.107.239.4326 > my.firewall.net.telnet: S 3152835603:3152835603(0) win 32120 <mss 1460,sackOK,timestamp 126497[|tcp]> (DF)

Existence: The source, if not spoofed, comes from Canada as this WHOIS indicates:

Rogers WAVE (NETBLK-ON-ROG-KTCH-1)
1 Mount Pleasant Road
Toronto, ON M4Y 2Y5
CA

Netname: ON-ROG-KTCH-1
Netblock: 24.112.104.0 - 24.112.107.255

Coordinator:
Network Security, Fraud (AD30-ARIN) abuse@rogers.home.net
416-935-4729

Record last updated on 04-Nov-1998.
Database last updated on 24-Apr-2000 05:40:41 EDT.

History: None previously observed.

Techniques: This was a port scan for telnet, similar to Detect 1, except a different destination port. Since I was scanned only once, this was probably a network scan of many hosts, looking specifically for telnet. I can not be 100% sure of this since my tcpdump capture was looking specifically at traffic to my firewall, but this seems the most likely scenario.

Targeting: Not specifically. This was most likely a scan of multiple hosts, looking for systems with telnet, so my machine was not targeted specifically.

Analysis: This source attempted to see if telnet was available on my firewall, although probably several more hosts as well. Probing for systems with telnet is a common first step. Once they find a system, they will attempt to ascertain the system type. Some systems will provide this with a telnet banner, providing further information in this initial information gathering stage. Once a system type with telnet access is found, the intruder will attempt to take advantage of known vulnerabilities on that system.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since telnet is not allowed either in or out through the firewall (5) and telnet is not a port open on any internal devices (5).

$$(5 + 1) – (5 + 5) = < 0$$

Detect 3:

20:07:58.111221 212.204.216.151.63118 > my.firewall.net.5300: . win 2048
20:07:58.112097 212.204.216.151.63118 > my.firewall.net.2038: . win 2048
20:07:58.112967 212.204.216.151.63118 > my.firewall.net.348: . win 2048
20:07:58.113843 212.204.216.151.63118 > my.firewall.net.915: . win 2048
20:07:58.114722 212.204.216.151.63118 > my.firewall.net.798: . win 2048
20:07:58.115603 212.204.216.151.63118 > my.firewall.net.425: . win 2048
20:07:58.116477 212.204.216.151.63118 > my.firewall.net.1352: . win 2048
20:07:58.117395 212.204.216.151.63118 > my.firewall.net.2605: . win 2048
20:07:58.118279 212.204.216.151.63118 > my.firewall.net.308: . win 2048
20:07:58.119163 212.204.216.151.63118 > my.firewall.net.859: . win 2048
20:07:58.120080 212.204.216.151.63118 > my.firewall.net.7006: . win 2048
20:07:58.120994 212.204.216.151.63118 > my.firewall.net.1520: . win 2048
20:07:58.121871 212.204.216.151.63118 > my.firewall.net.535: . win 2048
20:07:58.122747 212.204.216.151.63118 > my.firewall.net.5193: . win 2048
20:07:58.123627 212.204.216.151.63118 > my.firewall.net.383: . win 2048
20:07:58.124510 212.204.216.151.63118 > my.firewall.net.1477: . win 2048
20:07:58.125384 212.204.216.151.63118 > my.firewall.net.443: . win 2048
20:07:58.126254 212.204.216.151.63118 > my.firewall.net.9876: . win 2048
20:07:58.127132 212.204.216.151.63118 > my.firewall.net.530: . win 2048
20:07:58.128004 212.204.216.151.63118 > my.firewall.net.659: . win 2048
20:07:58.128934 212.204.216.151.63118 > my.firewall.net.41: . win 2048
20:07:58.129815 212.204.216.151.63118 > my.firewall.net.206: . win 2048
20:07:58.130818 212.204.216.151.63118 > my.firewall.net.371: . win 2048
20:07:58.131690 212.204.216.151.63118 > my.firewall.net.2003: . win 2048
20:07:58.132570 212.204.216.151.63118 > my.firewall.net.1016: . win 2048
20:07:58.133456 212.204.216.151.63118 > my.firewall.net.510: . win 2048
20:07:58.134342 212.204.216.151.63118 > my.firewall.net.567: . win 2048
20:07:58.167773 my.firewall.net.5300 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.168675 my.firewall.net.2038 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.169581 my.firewall.net.348 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.170449 my.firewall.net.915 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.171338 my.firewall.net.798 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.172234 my.firewall.net.425 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.173130 my.firewall.net.1352 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.174016 my.firewall.net.2605 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.174979 my.firewall.net.308 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.175862 my.firewall.net.859 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.176737 my.firewall.net.7006 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.177628 my.firewall.net.1520 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.178537 my.firewall.net.535 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.179412 my.firewall.net.5193 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.180304 my.firewall.net.383 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.181193 my.firewall.net.1477 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.182090 my.firewall.net.443 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.182982 my.firewall.net.9876 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.183862 my.firewall.net.530 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.184790 my.firewall.net.659 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.185645 my.firewall.net.41 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.186549 my.firewall.net.206 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.187447 my.firewall.net.371 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.188334 my.firewall.net.2003 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0
20:07:58.189223 my.firewall.net.1016 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0

20:07:58.190166 my.firewall.net.510 > 212.204.216.151.63118: R 0:0(0) ack 0 win 0

additional trace skipped…then we see this interesting activity on ports 80 and 1354…

20:07:59.991914 212.204.216.151.63118 > my.firewall.net.80: . win 2048
20:08:00.370883 212.204.216.151.63119 > my.firewall.net.80: . win 2048
20:08:00.796363 212.204.216.151.63125 > my.firewall.net.80: SE 3102347426:3102347426(0) win 2048 <wscale 10,nop,mss 265,timestamp 1061109567[|tcp]>
20:08:00.797243 212.204.216.151.63126 > my.firewall.net.80: . win 2048 <wscale 10,nop,mss 265,timestamp 1061109567[|tcp]>
20:08:00.798097 212.204.216.151.63127 > my.firewall.net.80: SFP 3102347426:3102347426(0) win 2048 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567[|tcp]>
20:08:00.798948 212.204.216.151.63128 > my.firewall.net.80: . ack 0 win 2048 <wscale 10,nop,mss 265,timestamp 1061109567[|tcp]>
20:08:00.799806 212.204.216.151.63129 > my.firewall.net.1354: S 3102347426:3102347426(0) win 2048 <wscale 10,nop,mss 265,timestamp 1061109567[|tcp]>
20:08:00.800761 212.204.216.151.63130 > my.firewall.net.1354: . ack 0 win 2048 <wscale 10,nop,mss 265,timestamp 1061109567[|tcp]>
20:08:00.801614 212.204.216.151.63131 > my.firewall.net.1354: FP 3102347426:3102347426(0) win 2048 urg 0 <wscale 10,nop,mss 265,timestamp 1061109567[|tcp]>
20:08:00.802640 212.204.216.151.63118 > my.firewall.net.1354: udp 300
20:08:00.810505 my.firewall.net.80 > 212.204.216.151.63125: S 1348112897:1348112897(0) ack 3102347427 win 4096 <mss 1460>
20:08:00.811122 212.204.216.151.63125 > my.firewall.net.80: R 3102347427:3102347427(0) win 0
20:08:00.813452 my.firewall.net.80 > 212.204.216.151.63127: . ack 3102347428 win 4096
20:08:00.814081 212.204.216.151.63127 > my.firewall.net.80: R 3102347428:3102347428(0) win 0
20:08:00.814963 my.firewall.net.80 > 212.204.216.151.63128: R 0:0(0) win 4096
20:08:00.816255 my.firewall.net.1354 > 212.204.216.151.63129: R 0:0(0) ack 3102347427 win 0
20:08:00.817227 my.firewall.net.1354 > 212.204.216.151.63130: R 0:0(0) win 0
20:08:00.818227 my.firewall.net.1354 > 212.204.216.151.63131: R 0:0(0) ack 3102347426 win 0
20:08:00.819175 my.firewall.net > 212.204.216.151: icmp: my.firewall.net udp port 1354 unreachable
20:08:01.172519 212.204.216.151.63119 > my.firewall.net.80: S 3102347427:3102347427(0) win 2048
20:08:01.177209 my.firewall.net.80 > 212.204.216.151.63119: S 1348240897:1348240897(0) ack 3102347428 win 4096 <mss 1460>
20:08:01.177847 212.204.216.151.63119 > my.firewall.net.80: R 3102347428:3102347428(0) win 0
20:08:01.250806 212.204.216.151.63120 > my.firewall.net.80: S 3102347428:3102347428(0) win 2048
20:08:01.255225 my.firewall.net.80 > 212.204.216.151.63120: S 1348304897:1348304897(0) ack 3102347429 win 4096 <mss 1460>
20:08:01.255880 212.204.216.151.63120 > my.firewall.net.80: R 3102347429:3102347429(0) win 0
20:08:01.330876 212.204.216.151.63121 > my.firewall.net.80: S 3102347429:3102347429(0) win 2048
20:08:01.335256 my.firewall.net.80 > 212.204.216.151.63121: S 1348432897:1348432897(0) ack 3102347430 win 4096 <mss 1460>
20:08:01.335904 212.204.216.151.63121 > my.firewall.net.80: R 3102347430:3102347430(0) win 0
20:08:01.410846 212.204.216.151.63122 > my.firewall.net.80: S 3102347430:3102347430(0) win 2048
20:08:01.415248 my.firewall.net.80 > 212.204.216.151.63122: S 1348496897:1348496897(0) ack 3102347431 win 4096 <mss 1460>
20:08:01.415904 212.204.216.151.63122 > my.firewall.net.80: R 3102347431:3102347431(0) win 0
20:08:01.490832 212.204.216.151.63123 > my.firewall.net.80: S 3102347431:3102347431(0) win 2048
20:08:01.495271 my.firewall.net.80 > 212.204.216.151.63123: S 1348560897:1348560897(0) ack 3102347432 win 4096 <mss 1460>
20:08:01.495931 212.204.216.151.63123 > my.firewall.net.80: R 3102347432:3102347432(0) win 0
20:08:01.574627 212.204.216.151.63124 > my.firewall.net.80: S 3102347432:3102347432(0) win 2048
20:08:01.579168 my.firewall.net.80 > 212.204.216.151.63124: S 1348624897:1348624897(0) ack 3102347433 win 4096 <mss 1460>
20:08:01.579784 212.204.216.151.63124 > my.firewall.net.80: R 3102347433:3102347433(0) win 0

Existence: 212.204.216.151 is "hosted-by.widexs.nl"
European Regional Internet Registry/RIPE NCC (NET-RIPE-NCC-)
These addresses have been further assigned to European users.
Contact information can be found in the RIPE database, via the
WHOIS and TELNET servers at whois.ripe.net, and at
http://www.ripe.net/db/whois.html

Netname: RIPE-NCC-212
Netblock: 212.0.0.0 - 212.255.255.255
Maintainer: RIPE

Coordinator:
RIPE Network Coordination Centre (RIPE-NCC-ARIN) nicdb@RIPE.NET
+31 20 535 4444
Fax- - +31 20 535 4445

Domain System inverse mapping provided by:

NS.RIPE.NET	193.0.0.193
NS.EU.NET	192.16.202.11
AUTH03.NS.UU.NET	198.6.1.83
NS2.NIC.FR	192.93.0.4
SUNIC.SUNET.SE	192.36.125.2
MUNNARI.OZ.AU	128.250.1.21
NS.APNIC.NET	203.37.255.97

To search on arbitrary strings, see the Database page on
the RIPE NCC web-site at http://www.ripe.net/db/

Record last updated on 16-Oct-1998.
Database last updated on 24-Apr-2000 17:39:54 EDT.

History: None previously observed.

Techniques: This was a fast host port scan. Notice the same source port number 63118 during the majority of the scan. They also have used a null scan. A null scan turns off all flags. This type of scan is intended to go un-noticed by firewalls and packet filters looking for SYNs, and programs like Synlogger and Courtney. The scanner scanned over 1500 ports before scanning ports 80 and 1354. Notice that my firewall replied to these closed ports with a RST, as expected (refer to RFC 973).
The source ports then start incrementing as it begins to scan ports 80 and 1354. The scanning tool is probably nmap, as it appears that the further scan activity on ports 80 and 1354 may have been an effort at OS identification, using TCP/IP fingerprinting.

Targeting: Absolutely! This source has targeted my firewall specifically, scanning over 1500 ports and then trying to do an OS identification.

Analysis: The intruder is trying to determine the host type of my firewall and what open ports exist. Their next step might include trying specific known vulnerabilities against my firewall, assuming they can determine the type of system and what weaknesses it has.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5). They may have identified my firewall and have definitely targeted me, so I'm giving this a (3). They may be aware of vulnerabilities in this firewall that I'm not aware of.
HTTP was temporarily allowed through the firewall. (Time to turn this back off). The internal systems and network countermeasures are above average, but due to the unknown, I'll average the countermeasures. This may not rate a high severity level, but its worth performing some testing on the firewall myself to see what else they may have found.

$$(5 + 3) – (3 + 3) = 2$$

Solution: Turn off allowing HTTP on firewall…this was a temporary rule for a test. Research firewall vendor's bug list to verify it is up-to-date.

Detect 4:

04/10/2000 00:29:42.672 - TCP connection dropped - Source:208.232.120.196, 635, WAN - Destination:my.firewall.net, 111, LAN - 'Sun RPC'

Existence: 208.232.120.196 is coming from Florida, as this WHOIS shows:

Grupo Coripar (NETBLK-UU-208-232-120)
7007 NW 32nd Ave.
Miami, FL 33147
US

Netname: UU-208-232-120
Netblock: 208.232.120.0 - 208.232.120.255

Coordinator:
Barbery, Carlos (CB5314-ARIN) nomailbox@NOWHERE
(305) 696-4735

Record last updated on 12-Nov-1997.
Database last updated on 24-Apr-2000 05:40:41 EDT.

History: None previously observed.

Techniques: This is probably part of a network scan of many Internet systems, looking for SunRPC, port 111.

Targeting: Not really! This source is most likely scanning many Internet hosts.

Analysis: An intruder has attempted to access SunRPC. RPC is used on most unix systems and is a common way to build network applications. If the intruder had gained access to port 111, their next step would be to probe that port to see what RPC programs, and their respective ports, are running on the system. Again, this is a scan targeting unix systems.
There have been various RPC vulnerabilities posted, including tooltalkd overflow. A recent one is CERT CA-99-08-CMSD, which is a buffer overflow targeting the Calendar Manager service.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since port 111 port is not allowed either in or out through the firewall (5). However, I do run unix systems (4) on my home network.

$$(5 + 1) – (4 + 5) = < 0$$

Detect 5:

Firewall Log:
04/22/2000 03:28:40.736 TCP connection dropped
161.184.237.194, 2283, WAN my.firewall.net, 1080, LAN

TCPDump:
03:26:09.051444 edtn015942.hs.telusplanet.net.2283 > 24.48.181.221.1080: S 89635638:89635638(0) win 8192 <mss 1460> (DF)

Existence: Another Canada source:

Edmonton Telephones Corporation (NET-ED-TEL)
P.O. Box 20500
Edmonton, Alberta T2P 2R4
CA

Netname: ED-TEL
Netnumber: 161.184.0.0

Coordinator:
Ste 200, Fracmaster Tower (FTS1-ARIN) ip-admin@ab.tac.net
+1 403 503-3800

Domain System inverse mapping provided by:

CLGRPS01.AGT.NET 198.80.55.1
CLGRPS02.AGT.NET 198.161.156.1

Record last updated on 20-Dec-1999.
Database last updated on 24-Apr-2000 17:39:54 EDT.

History: None previously observed.

Techniques: This was a port scan, looking specifically for SOCKS, port 1080.

Targeting: Not specifically. As this was most likely a scan of multiple hosts, looking for systems with 1080 open, my machine was not targeted specifically.

Analysis: The intruder is trying to find systems that have SOCKs port 1080. SOCKs is a system that allows multiple internal systems to share a common Internet connection. A common Windows version, called WinGate (http://wingate.deerfield.com/) is an especially common target, since it allows almost any protocol to be tunneled through it. They may either be looking to hide their identity, by using a SOCKs system to proxy through, or they may be trying to gain internal access through a SOCKs system, since most are not particular about source and destination addresses.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since SOCKs port is not allowed either in or out through the firewall (5) and SOCKs is definitely not a port open on any internal devices (5).

$$(5 + 1) – (5 + 5) = < 0$$

Detect 6:

04/10/2000 09:17:06.352 - TCP connection dropped - Source:209.44.129.184, 58996, WAN - Destination:my.firewall.net, 8080, LAN - - Rule 0
04/10/2000 09:17:06.480 - TCP connection dropped - Source:209.44.129.184, 59115, WAN - Destination:my.firewall.net, 8080, LAN - - Rule 0

Existence: This source is from Houston, TX, assuming it's not spoofed:

NeoSoft, Inc. (NETBLK-NEO-CIDR-02)
1770 St. James Pl.
Suite 500
Houston, TX 77056

Netname: NEO-CIDR-02
Netblock: 209.44.128.0 - 209.44.255.255
Maintainer: NEO

Coordinator:
Smith, Andrew (AS187-ARIN) awsmith@neosoft.com
888-NEOSOFT 1-800-GET-NEOSoft (FAX) (713) 968-5801

Domain System inverse mapping provided by:

NS.NEO.NET 206.109.1.1
NS2.NEO.NET 206.109.7.65
GUMBO.NO.NEOSOFT.COM 206.27.160.245

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 17-Jul-1998.
Database last updated on 24-Apr-2000 05:40:41 EDT.

History: None previously observed.

Techniques: This was a port scan, looking specifically for port 8080. This is very similar to Detect 5

Targeting: Not specifically. As this was most likely a scan of multiple hosts, looking for systems with 8080 open, my machine was not specifically targeted.

Analysis: The intruder is probably trying to find systems that have WinGate port 8080. WinGate is a system that allows multiple internal systems to share a common Internet connection. WinGate http://wingate.deerfield.com/ is an especially common target, since it allows almost any protocol to be tunneled through it. They may either be looking to hide their identity, by using a WinGate system to proxy through. Or they may be trying to

gain internal access through a WinGate system, since most are not particular about source and destination addressess.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since 8080 port is not allowed either in or out through the firewall (5) and 8080 is definitely not a port open on any internal devices (5).

$$(5 + 1) – (5 + 5) = < 0$$

Detect 7:

```
14:52:00.140181 dub-tgn-edt-eth00.as.wcom.net.telnet > my.firewall.net.1053: . ack 141426 win 8191
14:52:00.140594 dub-tgn-edt-eth00.as.wcom.net.telnet > my.firewall.net.1053: P 0:1(1) ack 1 win 8192
14:52:00.141419 my.firewall.net.1053 > dub-tgn-edt-eth00.as.wcom.net.telnet: R 1:1(0) ack 3872972045 win 8191
14:52:00.142477 my.firewall.net.1053 > dub-tgn-edt-eth00.as.wcom.net.telnet: R 1:1(0) ack 3872972045 win 8192
14:52:00.457239 dub-tgn-edt-eth00.as.wcom.net.telnet > my.firewall.net.1053: R 421995251:421995251(0) win 256
14:52:01.268588 dub-tgn-edt-eth00.as.wcom.net.telnet > my.firewall.net.1053: R 421995251:421995251(0) win 256
14:52:03.243184 dub-tgn-edt-eth00.as.wcom.net.telnet > my.firewall.net.1053: R 421995251:421995251(0) win 256
14:52:06.096778 dub-tgn-edt-eth00.as.wcom.net.telnet > my.firewall.net.1053: R 421995251:421995251(0) win 256
14:52:12.559431 dub-tgn-edt-eth00.as.wcom.net.telnet > my.firewall.net.1053: R 421995251:421995251(0) win 256
```

Existence: This source appears to be from Ohio:

UUNET, an MCIWorldcom Company (NET-UUNET-HIL-BLK1)
5000 Britton Rd.
Hilliard, OH 43026
US

Netname: UUNET-HIL-BLK1
Netblock: 209.154.0.0 - 209.154.255.255
Maintainer: UUHI

Coordinator:
UUNET an MCI WorldCom Company (HC3-ORG-ARIN)
hostmaster@wcom.net
614/723-8128

Domain System inverse mapping provided by:

NS1.WCOM.NET	209.154.198.82
NS2.WCOM.NET	209.154.198.86

Record last updated on 02-Mar-2000.
Database last updated on 24-Apr-2000 05:40:41 EDT.

History: None previously observed.

Techniques: There was no initial SYN packet from this source to the firewall. This trace starts with an ACK packet, then follows with a PSH packet from the remote system. The firewall sends some RSTs, then the remote system sends RSTs. This was obviously not a normal TCP communication. The port was telnet, so it did catch my interest.

Targeting: Definitely sent to me! This source has targeted my firewall specifically, attempting telnet, or in the middle of a quasi-telnet connection.

Analysis: I'm fairly sure this is not anything to be concerned over. It appears that some packets in the middle of a legitimate telnet conversation came to my firewall. Both sides quickly RST. It may be that another machine, using the same IP address (ISP's DHCP gave out same address, or someone statically configured their system) as my firewall,

temporarily came on the network, initiated a telnet session to dub-tgn-edt-eth00.as.wcom.net, then packets got confused who to send to. This remote system, by the way, is running telnet on it.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1). Telnet is not allowed in or out through the firewall (5) and telnet is not a port open on any internal devices (5).

$$(5 + 1) – (5 + 5) = < 0$$

Detect 8:

```
20:36:18.457341 142.165.206.93 > my.firewall.net: (frag 30200:4@16)
20:36:18.458174 [|tcp] (frag 44435:16@0+)
20:36:18.458793 142.165.206.93 > my.firewall.net: (frag 44435:4@16)
20:36:18.459620 [|tcp] (frag 61893:16@0+)
20:36:18.460280 142.165.206.93 > my.firewall.net: (frag 61893:4@16)
20:36:18.461155 [|tcp] (frag 32278:16@0+)
20:36:18.461769 142.165.206.93 > my.firewall.net: (frag 32278:4@16)
20:36:18.462616 [|tcp] (frag 46861:16@0+)
20:36:18.463241 142.165.206.93 > my.firewall.net: (frag 46861:4@16)
20:36:18.464075 [|tcp] (frag 58982:16@0+)
20:36:18.464708 142.165.206.93 > my.firewall.net: (frag 58982:4@16)
20:36:18.770924 [|tcp] (frag 28341:16@0+)
20:36:18.771547 142.165.206.93 > my.firewall.net: (frag 28341:4@16)
20:36:18.772380 [|tcp] (frag 32659:16@0+)
20:36:18.773008 142.165.206.93 > my.firewall.net: (frag 32659:4@16)
20:36:18.773853 [|tcp] (frag 30200:16@0+)
20:36:18.774481 142.165.206.93 > my.firewall.net: (frag 30200:4@16)
20:36:18.775317 [|tcp] (frag 44435:16@0+)
20:36:18.775938 142.165.206.93 > my.firewall.net: (frag 44435:4@16)
20:36:18.776781 [|tcp] (frag 61893:16@0+)
20:36:18.777393 142.165.206.93 > my.firewall.net: (frag 61893:4@16)
20:36:18.778228 [|tcp] (frag 32278:16@0+)
20:36:18.778852 142.165.206.93 > my.firewall.net: (frag 32278:4@16)
20:36:18.779682 [|tcp] (frag 43677:16@0+)
20:36:18.780431 142.165.206.93 > my.firewall.net: (frag 43677:4@16)
20:36:18.781272 [|tcp] (frag 62586:16@0+)
20:36:18.781889 142.165.206.93 > my.firewall.net: (frag 62586:4@16)
20:36:18.782731 [|tcp] (frag 61703:16@0+)
20:36:18.783356 142.165.206.93 > my.firewall.net: (frag 61703:4@16)
```

Existence: Another source from Canada:

SaskTel (SASKTEL3)
2121 Saskatchewan Drive
Regina, SK S4P 3Y2
Canada

Netname: SASKTEL-B
Netnumber: 142.165.0.0
Maintainer: SASK

Coordinator:
Sasknet Administrator (SA30-ORG-ARIN) sasknet.admin@SASKTEL.SK.CA
(306) 777-2478
Fax- (306) 777-1624

Domain System inverse mapping provided by:

HARRIER.SASKNET.SK.CA 142.165.5.2
SPITFIRE.SASKNET.SK.CA 142.165.5.4

Record last updated on 25-Jun-1997.
Database last updated on 24-Apr-2000 17:39:54 EDT.

History: None previously observed.

Techniques: This was a host port scan using tiny fragments.

Targeting: Absolutely! This source has targeted my firewall specifically, null scanning using tiny fragmented packets. They are attempting to go unnoticed.

Analysis: The intruder is probably using nmap, running a null scan, such as in Detect 3. The difference here is they are also using tiny fragmented packets to try to elude notice. It worked in this case, as my firewall did not log these.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1). The firewall did not log these fragments, so I'll use an average value for network countermeasures.

$$(5 + 1) – (5 + 3) = < 0$$

Detect 9:

Firewall Log:
04/22/2000 06:05:02.608 TCP connection dropped
63.82.222.102, 1221, WAN > my.firewall.net, 30303, LAN

TCPDump:
06:02:32.627028 usr1-39.lipan.net.1221 > my.firewall.net.30303: S 39656629:39656629(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
06:02:32.631826 my.firewall.net.30303 > usr1-39.lipan.net.1221: R 0:0(0) ack 39656630 win 8192
06:02:33.284064 usr1-39.lipan.net.1221 > my.firewall.net.30303: S 39656629:39656629(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
06:02:33.286517 my.firewall.net.30303 > usr1-39.lipan.net.1221: R 0:0(0) ack 1 win 8192
06:02:33.917623 usr1-39.lipan.net.1221 > my.firewall.net.30303: S 39656629:39656629(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
06:02:33.920129 my.firewall.net.30303 > usr1-39.lipan.net.1221: R 0:0(0) ack 1 win 8192
06:02:34.606560 usr1-39.lipan.net.1221 > my.firewall.net.30303: S 39656629:39656629(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
06:02:34.608968 my.firewall.net.30303 > usr1-39.lipan.net.1221: R 0:0(0) ack 1 win 8192

Existence:

UUNET/ISP Alliance/L (NETBLK-UU-63-82-222)
6230 Shiloh Road
Alpharetta, GA 30009
US

Netname: UU-63-82-222
Netblock: 63.82.222.0 - 63.82.222.255

Coordinator:
Genovese, Rick (RG35-ARIN) genovese@ispalliance.net
(770) 888-8900 x2228

Record last updated on 27-Oct-1999.
Database last updated on 24-Apr-2000 05:40:41 EDT.

History: None previously observed.

Techniques: This was a very specific port scan on my firewall.

Targeting: Absolutely! This source has apparently targeted my firewall, trying to connect to port 30303 four times.

Analysis: The intruder is trying to connect to port 30303. They try four times, with about a half/second interval between attempts. Although there is no currently known trojan on port 30303, it seems like a conspicuous port number to try, especially 4 times. Some trojans do allow setting them to a particular port number.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since 30303 port is not allowed either in or out through the firewall (5), as evidenced by the RSTs from the firewall. I verified by using a netstat –a that no internal systems are listening on 30303

(5 + 1) – (4 + 5) = < 0

Detect 10:

```
20:15:24.781033 128.129.32.66.39197 > my.firewall.net.574: S 538976474:538976474(0) win 2048
20:15:24.781871 139.34.2.55.39197 > my.firewall.net.574: S 538976474:538976474(0) win 2048
20:15:24.782742 208.224.68.10.39197 > my.firewall.net.574: S 538976474:538976474(0) win 2048
20:15:24.783591 128.2.55.234.39197 > my.firewall.net.574: S 538976474:538976474(0) win 2048
20:15:24.784482 128.129.32.66.39197 > my.firewall.net.418: S 538976474:538976474(0) win 2048
20:15:24.785325 139.34.2.55.39197 > my.firewall.net.418: S 538976474:538976474(0) win 2048
20:15:24.786163 208.224.68.10.39197 > my.firewall.net.418: S 538976474:538976474(0) win 2048
20:15:24.786995 128.2.55.234.39197 > my.firewall.net.418: S 538976474:538976474(0) win 2048
20:15:24.787888 128.129.32.66.39197 > my.firewall.net.675: S 538976474:538976474(0) win 2048
20:15:24.788727 139.34.2.55.39197 > my.firewall.net.675: S 538976474:538976474(0) win 2048
20:15:24.789564 208.224.68.10.39197 > my.firewall.net.675: S 538976474:538976474(0) win 2048
20:15:24.796431 128.2.55.234.39197 > my.firewall.net.675: S 538976474:538976474(0) win 2048
20:15:24.797330 128.129.32.66.39197 > my.firewall.net.480: S 538976474:538976474(0) win 2048
20:15:24.798163 139.34.2.55.39197 > my.firewall.net.480: S 538976474:538976474(0) win 2048
20:15:24.799003 208.224.68.10.39197 > my.firewall.net.480: S 538976474:538976474(0) win 2048
20:15:24.799264 my.firewall.net.574 > 139.34.2.55.39197: R 0:0(0) ack 538976475 win 0
20:15:24.800468 128.2.55.234.39197 > my.firewall.net.480: S 538976474:538976474(0) win 2048
20:15:24.803323 my.firewall.net.418 > 139.34.2.55.39197: R 0:0(0) ack 538976475 win 0
20:15:24.807573 my.firewall.net.675 > 139.34.2.55.39197: R 0:0(0) ack 538976475 win 0
20:15:24.808364 128.129.32.66.39197 > my.firewall.net.587: S 538976474:538976474(0) win 2048
20:15:24.809197 139.34.2.55.39197 > my.firewall.net.587: S 538976474:538976474(0) win 2048
20:15:24.810063 208.224.68.10.39197 > my.firewall.net.587: S 538976474:538976474(0) win 2048
20:15:24.816433 128.2.55.234.39197 > my.firewall.net.587: S 538976474:538976474(0) win 2048
20:15:24.817325 128.129.32.66.39197 > my.firewall.net.447: S 538976474:538976474(0) win 2048
20:15:24.818157 139.34.2.55.39197 > my.firewall.net.447: S 538976474:538976474(0) win 2048
20:15:24.818993 208.224.68.10.39197 > my.firewall.net.447: S 538976474:538976474(0) win 2048
20:15:24.819832 128.2.55.234.39197 > my.firewall.net.447: S 538976474:538976474(0) win 2048
20:15:24.826597 my.firewall.net.480 > 139.34.2.55.39197: R 0:0(0) ack 538976475 win 0
20:15:24.827236 128.129.32.66.39197 > my.firewall.net.578: S 538976474:538976474(0) win 2048
20:15:24.828067 139.34.2.55.39197 > my.firewall.net.578: S 538976474:538976474(0) win 2048
20:15:24.828906 208.224.68.10.39197 > my.firewall.net.578: S 538976474:538976474(0) win 2048
20:15:24.829737 128.2.55.234.39197 > my.firewall.net.578: S 538976474:538976474(0) win 2048
```

Existence: These are spoofed addresses.

History: None previously observed.

Techniques: This was a host port scan. The scanning tool is probably nmap. They are using a SYN stealth scan and are masking themselves by spoofing a few additional source addresses. Notice however, all source addresses all use the same port 39197.

Targeting: Absolutely! This source has targeted my firewall specifically, and scanned several TCP ports using SYN stealth scanning.

Analysis: The intruder is trying to determine what open ports exist on my firewall. They may not yet realize it is a firewall, and may be assuming it's just an exposed system on a cable-modem. Their next step might include trying specific known vulnerabilities against my firewall, assuming they can determine the type of system and what weaknesses it has.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since 8080 port is not allowed either in or out through the firewall (5) and 8080 is definitely not a port open on any internal devices (5).

$$(5 + 1) – (5 + 5) = < 0$$

Detect 11:

```
10:54:11.223074 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9516 len 156
10:54:12.364037 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO
      cookie: 0000000000000000->0000000000000000 msgid: 00000000 [|isakmp]
10:54:15.173617 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9517 len 100
10:54:15.184818 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9518 len 156
10:54:15.193509 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9519 len 156
10:54:15.226040 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9520 len 156
10:54:23.170489 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9521 len 116
10:54:24.672359 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9522 len 116
10:54:26.174568 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9523 len 116
10:54:30.741818 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9524 len 116
10:54:32.240788 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9525 len 116
10:54:33.747941 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9526 len 116
10:54:39.760246 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9527 len 116
10:54:39.786321 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9528 len 100
10:54:39.824515 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9529 len 164
10:54:40.788519 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9530 len 100
10:54:40.879963 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9531 len 164
10:54:41.258646 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9532 len 116
10:54:41.290057 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9533 len 156
10:54:41.340957 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9534 len 156
10:54:42.757472 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9535 len 116
10:54:43.292761 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9536 len 100
10:54:43.301715 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9537 len 156
10:54:43.356068 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9538 len 164
10:54:43.381114 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9539 len 156
10:54:47.296656 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9540 len 100
10:54:47.308171 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9541 len 156
10:54:47.371903 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9542 len 164
10:54:47.372774 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9543 len 156
10:54:48.779602 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9544 len 116
10:54:50.285552 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9545 len 116
10:54:51.768254 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9546 len 116
10:54:55.295458 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9547 len 116
10:54:56.796867 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9548 len 116
10:54:57.787829 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9549 len 108
10:54:58.297814 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9550 len 116
10:54:59.278839 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9551 len 108
10:55:00.777480 esp 208.209.43.11 > my.firewall.net spi 0x00155077 seq 9552 len 108
10:55:17.455837 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO encrypted
      cookie: 620c6a3adb86f4d4->2759faf4908925a8 msgid: 9d428b70 [|isakmp]
10:55:17.567084 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO encrypted
      cookie: 620c6a3adb86f4d4->2759faf4908925a8 msgid: 40249a98 [|isakmp]
10:55:39.432727 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
      cookie: b99f4627d2d6dd9a->7d33423bee00786b msgid: 00000000 [|isakmp]
10:55:55.995698 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
      cookie: b99f4627d2d6dd9a->7d33423bee00786b msgid: 00000000 [|isakmp]
10:56:12.008829 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
      cookie: b99f4627d2d6dd9a->7d33423bee00786b msgid: 00000000 [|isakmp]
12:40:03.533562 esp 208.209.43.11 > my.firewall.net spi 0x001FE49F seq 11912 len 100
12:40:05.034645 esp 208.209.43.11 > my.firewall.net spi 0x001FE49F seq 11913 len 100
12:40:06.537095 esp 208.209.43.11 > my.firewall.net spi 0x001FE49F seq 11914 len 100
12:41:40.401753 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO
```

cookie: 0000000000000000->0000000000000000 msgid: 00000000 [|isakmp]
12:42:45.491355 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO
cookie: 0000000000000000->0000000000000000 msgid: 00000000 [|isakmp]
12:43:50.577511 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO
cookie: 0000000000000000->0000000000000000 msgid: 00000000 [|isakmp]
12:44:55.669160 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO encrypted
cookie: 8fada712031832ef->256964f7c63c4df3 msgid: a7b24ed2 [|isakmp]
12:44:55.779142 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO encrypted
cookie: 8fada712031832ef->256964f7c63c4df3 msgid: fb701e95 [|isakmp]
12:45:04.390444 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
cookie: 4ec9d3ec9d7897e2->48633334ac1a0ed7 msgid: 00000000 [|isakmp]
12:45:19.703060 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
cookie: 4ec9d3ec9d7897e2->48633334ac1a0ed7 msgid: 00000000 [|isakmp]
12:45:35.712158 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
cookie: 4ec9d3ec9d7897e2->48633334ac1a0ed7 msgid: 00000000 [|isakmp]
12:45:51.707580 208.209.43.11.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
cookie: 4ec9d3ec9d7897e2->48633334ac1a0ed7 msgid: 00000000 [|isakmp]

21:49:31.663511 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: 00000000 [|isakmp]
21:50:44.448129 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: 00000000 [|isakmp]
21:51:08.692562 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange QUICK_MODE encrypted
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: 8a427f5d [|isakmp]
21:51:25.264343 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange QUICK_MODE encrypted
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: 8a427f5d [|isakmp]
21:51:40.394453 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange QUICK_MODE encrypted
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: 8a427f5d [|isakmp]
21:51:56.786750 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange QUICK_MODE encrypted
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: 8a427f5d [|isakmp]
21:51:58.566870 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: 00000000 [|isakmp]
21:52:11.675605 esp isa-bl1ex.BayNetworks.COM > my.firewall.net spi 0x00103F23 seq 189 len 220
21:52:13.216698 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO encrypted
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: e5fa9bf1 [|isakmp]
21:52:13.447031 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange INFO encrypted
cookie: 89180ea83d89d8f8->e5b9a96d7f514772 msgid: b9494f16 [|isakmp]
21:53:25.178670 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
cookie: f3c1388f8e4ec2c7->1c4df7628fc9a5a8 msgid: 00000000 [|isakmp]
21:53:40.431743 isa-bl1ex.BayNetworks.COM.isakmp > my.firewall.net.isakmp: isakmp v1.0 exchange AGGRESSIVE
cookie: f3c1388f8e4ec2c7->1c4df7628fc9a5a8 msgid: 00000000 [|isakmp]

Existence:

Excel Switching Corporation (NETBLK-UU-208-209-43)
255 Independence Ave.
Hyannis, MA 02602
US

Netname: UU-208-209-43
Netblock: 208.209.43.0 - 208.209.43.255

Coordinator:
Billings, John A (JAB61-ARIN) jbillings@XL.COM
508 862-3333 (FAX) 508 862-3020

Record last updated on 09-Nov-1998.
Database last updated on 24-Apr-2000 05:40:41 EDT.

Wellfleet Communications, Inc. (NETBLK-WELLFLEET1)
12 DeAngelo Drive
Bedford, MA 01730-2204

Netname: WELLFLEET-CUST
Netblock: 192.32.5.0 - 192.32.253.0

Coordinator:
Kapica, Margaret (MK478-ARIN) mkapica@nortelnetworks.com
978-288-4555

Record last updated on 07-Apr-1997.
Database last updated on 24-Apr-2000 05:40:41 EDT.

History: None previously observed.

Techniques: This appears as though these two sources think an IPSec conversation is going on, though it is very one-sided. My firewall did stop and log the UDP 500 to UDP 500 attempts. The firewall did not log the ESP one-way packets, however.

Targeting: Absolutely! These two sources are definitely trying to talk IPSec with me.

Analysis: I wish I knew. I provided this 11th detect for interest. I do use an IPSec client on my laptop computer, but I do not connect to either of these two remote systems. Also, I was not even home with my laptop during all these logged activities.

Detect 12:

18:18:04.171709 129.125.130.218.3000 > my.firewall.net.53: S 3347845790:3347845790(0) win 32120 <mss 1460,sackOK,timestamp 40244027[|tcp]> (DF)
18:18:04.176384 my.firewall.net.53 > 129.125.130.218.3000: R 0:0(0) ack 3347845791 win 32120

Existence:

RUG University (NET-RUGNET)
Paddepoel-terrein
Landleven 1
Groningen
NETHERLANDS

Netname: RUGNET
Netnumber: 129.125.0.0

Coordinator:
Pattiapon, Magda (MP1092-ARIN) M.Pattiapon@RC.RUG.NL
+31 50 3633430

Domain System inverse mapping provided by:

MAILHOST.RUG.NL	129.125.4.6
RC.SERVICE.RUG.NL	129.125.4.13
NS1.SURFNET.NL	192.87.106.101

Record last updated on 02-Apr-1996.
Database last updated on 24-Apr-2000 17:39:54 EDT.

History: None previously observed.

Techniques: This was an attempt to see if the DNS TCP port 53 was open. This is not part of a name lookup, which is UDP port 53.

Targeting: Probably not. This may have been a network scan looking for open TCP port 53. The fact that it was a system in the Netherlands is also suspicious.

Analysis: The intruder is probably trying to find systems that allow a DNZ zone transfer. DNS servers not configured securely may give out more information than they should. Armed with a detailed DNS table, an intruder can begin a more extensive probing on those systems.

Severity Level: (Critical + Lethal) – (System Countermeasures + Net Countermeasures) = Severity Level

This is a firewall (5), but the attack is unlikely to succeed (1), since TCP 53 port is not allowed either in or out through the firewall (5), as evidenced by the RST from the firewall.

$$(5 + 1) – (4 + 5) = < 0$$

Last Updated: October 24th, 2017

Upcoming Training

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
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
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 Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 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
Las Vegas 2018 - SEC503: Intrusion Detection In-Depth	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201805,	May 02, 2018 - Jun 07, 2018	vLive
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
Community SANS Columbia SEC503	Columbia, MD	Aug 13, 2018 - Aug 18, 2018	Community SANS
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced