Global Information Assurance Certification Paper

Frederick A. Kolbrener
IDIC-1, SANS 2000, Orlando, FL

***, Northcutt, a great read, bummer about number 7, takes this out of the 90s, but wow, I know I wouldn't mess with Fred's net! Solid analysis, clarity and the gift to bring the traces to life. The first three had me clapping! 87 *

Fred Kolbrener

IDIC Analysis Assignment

This is an analysis of eleven sets of data related to intrusion attempts on both a dial-up ISP connection which is protected by BlackICE firewall and detects posted to the GIAC site. BlackICE Defender (BID) is a personal firewall that also functions as an intrusion detection system. Each time a non-allowed event occurs, a record is produced and, if possible, evidence files are created. It is also possible for the program to fully log all packets entering or leaving the computer. However, I have found that this latter logging process slows down the detection and warning parts of the program tremendously. Unfortunately, the program does not include a handy means of reading either the evidence logs or the packet logs. This is a disadvantage as it would be advantageous to analyze them using another tool such as WINdump (TCPDump for Windows). A packet reader has been used to examine some packet logs, but this analysis has proved to be tedious with the current tool I have located. The BlackICE firewall was installed on January 26, 2000. Data has been collected continuously, but because this is a dial-up connection, there are not that many detections from this computer.

This data is submitted in fulfillment of the requirements of the Intrusion Detection Immersion Curriculum held at SANS 2000 in Orlando, FL, March 21-25, 2000..

+

1. **PCAnywhere probes**. The first event occurred on April 1, 2000 just after 12 Noon. BlackICE Defender (BID) reported an intrusion attempt as shown below. The time shown as posted to the attack log is GMT or UFT time which was 5 hours ahead of Eastern Standard Time. The data was originally recorded as a comma delimited ASCII file that was subsequently imported into Excel for analysis. An explanation of the entry is as follows:

Severity as assigned by BID: 19 (Scale runs from 1 to 99)
Date/Time (GMT) [YYYY-MM-DD hh:mm:ss]: 2000-04-01 17:14:08
Event Type (BID Code): 2001507
Event Name: PCAnywhere ping
IP Address of source computer: 207.172.73.49
NetBIOS name of source computer: ROADRUNNER
IP of Target computer: 207.172.73.41

Frederick A. Kolbrener
IDIC-1, SANS 2000, Orlando, FL

Port(s) on targeted computer: 22 & 5632
Number of "sub-events": 2

19 2000-04-01 17:14:08 2001507 PCAnywhere ping 207.172.73.49 207.172.73.41 port=22|5632 2

Concurrently, this attacked computer was running WINDUMP (version 2.02 beta) and was recording standard length (68) byte packet headers of all incoming and outgoing traffic. (No filtering of events was in place at that time.) The WINDUMP output file was queried for all events with a source computer of 207.172.73.49. The following list was produced:

12:11:47.311800 207.172.73.49.3123 > 207.172.73.41.5632: udp 2
12:11:47.321198 207.172.73.49.3123 > 207.172.73.41.22: udp 2
12:11:48.520847 207.172.73.49.137 > 207.172.73.41.1598: udp 283

Reviewing the first two lines of data, we see one side of the conversation, receipt of data. The first two lines indicate that the prober is using his ethereal port 3123 to send pings probes for computers running PC anywhere (port 22 or 5632). The fact that the source port does not increment and the probes are very fast supports the use of an unidentified tool to do this probing.

Listing showing MAC addresses (dial-up modem) and size of the UDP packets:

12:11:47.311800 20:53:52:43:0:0 44:45:53:54:0:0 ip 44: 207.172.73.49.3123 207.172.73.41.5632: udp 2
12:11:47.321198 20:53:52:43:0:0 44:45:53:54:0:0 ip 44: 207.172.73.49.3123 > 207.172.73.41.22: udp 2
12:11:48.520847 20:53:52:43:0:0 44:45:53:54:0:0 ip 325: 207.172.73.49.137 > 207.172.73.41.1598: udp 283

The third line is a response to a NetBIOS request launched by BID to which the prober's computer answered with the computer name, and other information. This shows the prober was assigned an address by DHCP on the same network dial-up segment as the probed computer (207.172.72).

IP: 207.172.73.49
DNS: 207-172-73-49.s49.tnt1.man.va.dialup.rcn.com
Node: ROADRUNNER
NetBIOS: SMELLY
Group: ACME

HEX DUMP from WINdump confirms the probe in UDP packets (protocol 0x11):

```
12:11:47.311800 207.172.73.49.3123 > 207.172.73.41.5632: udp 2
                        4500 001e 8b7d 0000 7f11 7e9e cfac 4931
                        cfac 4929 0c33 1600 000a 5da2 4e51
12:11:47.321198 207.172.73.49.3123 > 207.172.73.41.22: udp 2
                        4500 001e 8c7d 0000 7f11 7d9e cfac 4931
                        cfac 4929 0c33 0016 000a 738c 4e51
12:11:48.520847 207.172.73.49.137 > 207.172.73.41.1598: udp 283
                        4500 0137 c97d 0000 7f11 3f85 cfac 4931
                        cfac 4929 0089 063e 0123 4a4d 80b0 8400
                        0000 0001 0000 0000 2043 4b41 4141 4141
                        4141 4141 4141
```

On Sunday, April 2, a second event was recorded as below (from a computer named DEFAULT). Two pings of port 22 were recorded. The source was a different computer as evidenced by the different NetBIOS name and also the different mode of the ping. Only port 22 was targeted.

```
19      2000-04-03 01:10:25     2001507     PCAnywhere ping   207.172.73.166     DEFAULT     207.172.73.134
        port=22     2
```

Since these initial pings, additional pings apparently from other computers have been recorded. Note that the NetBIOS names are different and there is a lack of consistency in the probing. Sometimes there is a single port probed and sometimes two are probed. From reading about PCAnywhere, I have found that it apparently uses port 22 for initial contact, and may then switch to port 5632 (default) for data transfer, although it can be set to use any port the user desires.

```
19      2000-04-15 20:36:30     2001507     PCAnywhere ping   207.172.73.127     207-172-73-127.s127.tnt1.
        man.va.dialup.rcn.com   207.172.73.188      port= 22|5632           2
19      2000-04-16 03:55:21           2001507     PCAnywhere ping   207.172.73.108     FASTCOMPUTER
        207.172.73.187      port= 22|5632           2
```

ANALYSIS:

Was I targeted? Yes, the IP address was targeted by a probe; however, since the ISP's DHCP assigns an address each time we establish a connection to the ISP, this particular computer was not ***specifically*** targeted.
Were we at risk? NO, this particular computer 1) does not run PCAnywhere, and 2) sits behind a firewall that filters out attacks
Were the probes hostile: Yes. There is and was no valid reason for these events to have occurred. Interesting also is the fact that this probing is taking place on my ISP's own network (207.172.73.XXX) from another ISP user, not from an outside source. The intrusions have all been reported to the ISP. One possible explanation still needs to be followed up. It has been proposed that PCAnywhere , when installed on a computer, may ping the local network looking for other copies of itself each time it is able to connect to a network. Testing to this hypothesis is planned for the future when I can get the program to test with.

+

2. **Program misconfiguration**. The next series of detects were recorded in the first few days after BlackICE Defender was installed.. At first, they appeared to be UDP port probes from another network computer; however, on closer examination, they were determined to be due to: 1) a lack of experience with the data recorded by the IDS portion of the firewall on my part, and; 2) a need to configure the firewall to allow Network Time Service data replies back into the firewall.

59	2000-01-26 19:38:53	2003502	UDP port probe	207.172.73.197	207-172-73-197.s197.tnt1.man.va.dialup.rcn.com	198.189.18.5	port=123	1
59	2000-01-26 19:42:43	2003502	UDP port probe	207.172.73.197	207-172-73-197.s197.tnt1.man.va.dialup.rcn.com	128.102.16.10	port=123	1
19	2000-01-28 03:59:39	2000101	Trace route	207.172.74.100	207-172-74-100.s100.tnt2.man.va.dialup.rcn.com	207.172.73.197	count=3	1
19	2000-01-29 03:21:54	2000101	Trace route	207.172.73.47	207-172-73-47.s47.tnt1.man.va.dialup.rcn.com	210.212.218.34	count=3	2
59	2000-01-29 18:36:22	2003502	UDP port probe	207.172.74.164	207-172-74-164.s164.tnt2.man.va.dialup.rcn.com	192.203.230.10	port=123	1
59	2000-02-06 15:41:45	2003502	UDP port probe	207.172.73.46	207-172-73-46.s46.tnt1.man.va.dialup.rcn.com	128.102.16.10	port=123	2
19	2000-02-03 03:47:21	2000101	Trace route	207.172.104.25	207-172-104-25.s279.tnt1.man.va.dialup.rcn.com	128.18.100.11	count=3	1
39	2000-02-03 03:47:21	,2000102	Echo storm	207.172.104.25	207-172-104-25.s279.tnt1.man.va.dialup.rcn.com	128.18.100.11	count=20	1

(The monitored computer uses a program that checks the internet for the correct time and updates the computer's clock.. The program makes use of the standard port 123 to effect this transfer of time data. Since I had not been running a firewall prior to the installation of the firewall, I was not aware of the manner in which the program operated and no need to reconfigure it or any other program to make sure it ran correctly.)

Analysis: Was I targeted? Yes, the attempts to get into my port 123 were aimed at my computer.
Was the intent hostile? No.   Timing: Does not apply to this analysis.
Was I at risk: No. Requested time data could not get into the firewall and generated a false positive.

The trace routes were launched by me in a misguided attempt to determine why the IDS portion of BlackICE (BID) was recording potentially hostile activity. The result was that the trace route itself was recorded by BID and appeared hostile. Based on this series of recorded activity, I modified the firewall 'ini' file to open port 123 for incoming time data. The problem has not recurred.   The IDS portion of BlackICE revealed a need for reconfiguration for normal operations.

+

3. **Gaming "Attack"**. The activity listed below occurred one evening over a prolonged period. The BlackICE essentially appeared to be going wild with events being recorded each few seconds. The "attack" began at about 10:11 PM EST went on until 10:42 PM EST with 39 separate attempts at unauthorized entry into the computer. BlackICE responded with NetBIOS probes back to each address and gleaned the Netbios names shown in the lines. All the activity was aimed at one port – 2346. I had no service running on that port that I knew about. (I have replaced my IP address with MYCOMP to fit the data on one line.)

```
39 2000-03-04 03:11:28 2003502 UDP port probe 216.67.4.223 OEMCOMPUTER MY-IP port=2346 2
39 2000-03-04 03:11:28 2003502 UDP port probe 63.26.174.65 1Cust.uu.net, MY-IP port=2346 2
39 2000-03-04 03:11:33 2003502 UDP port probe 24.67.162.167 QWERT, MY-IP port=2346 2
39 2000-03-04 03:11:50 2003502 UDP port probe 216.179.3.140 dialin.bestweb.net MY-IP port=2346 2
39 2000-03-04 03:12:05 2003502 UDP port probe 24.16.57.4 C749526-A MY-IP port=2346 2
39 2000-03-04 03:12:55 2003502 UDP port probe 24.141.120.115 CO291878-A MY-IP port=2346 2
39 2000-03-04 03:12:55 2003502 UDP port probe 161.184.231.96 ISUTTON-1 MY-IP port=2346 2
39 2000-03-04 03:12:55 2003502 UDP port probe 24.141.145.25 co513175.home.com MY-IP port=2346 2
39 2000-03-04 03:12:56 2003502 UDP port probe 24.6.179.176 cx440614-b.vbch1.va.home.com MY-IP port=2346 2
39 2000-03-04 03:13:02 2003502 UDP port probe 216.227.152.75 dialup-b-55.mint.net MY-IP port=2346 2
39 2000-03-04 03:13:35 2003502 UDP port probe 216.68.176.240 PAVILION, MY-IP port=2346 2
39 2000-03-04 03:13:41 2003502 UDP port probe 195.54.80.25 web.webnnet.dk, MY-IP port=2346 2
39 2000-03-04 03:14:12 2003502 UDP port probe 209.177.1.27 TJ'S COMPUTER, MY-IP port=2346 2
39 2000-03-04 03:14:12 2003502 UDP port probe 141.151.22.17 MENGEL MY-IP port=2346 2
39 2000-03-04 03:14:37 2003502 UDP port probe 208.190.61.25 CHIENG MY-IP port=2346 2
39 2000-03-04 03:14:45 2003502 UDP port probe 24.14.198.115 cx6468.ct.home.com, MY-IP port=2346 2
```

```
39 2000-03-04 03:14:53 2003502 UDP port probe 199.44.199.134 OEMCOMPUTER, MY-IP port=2346 2
39 2000-03-04 03:15:33 2003502 UDP port probe 209.179.246.66 pool0576.earthlink.net MY-IP port=2346 2
39 2000-03-04 03:15:33 2003502 UDP port probe 24.2.77.185 CC1016440-A MY-IP port=2346,4
39 2000-03-04 03:15:45 2003502 UDP port probe 63.17.37.204 HOMEGR0WN MY-IP port=2346 2
39 2000-03-04 03:15:58 2003502 UDP port probe 207.199.1.16 APHEXAPP1 MY-IP port=2346,4
39 2000-03-04 03:15:58 2003502 UDP port probe 195.226.100.178 stu1ir11.tesion.net MY-IP port=2346 2
39 2000-03-04 03:16:29 2003502 UDP port probe 24.64.143.149 CS221859-A MY-IP port=2346 2
39 2000-03-04 03:16:57 2003502 UDP port probe 207.158.191.11 SHANECOL MY-IP port=2346,4
39 2000-03-04 03:16:59 2003502 UDP port probe 208.32.160.175 BUBBA, MY-IP port=2346 2
39 2000-03-04 03:17:46 2003502 UDP port probe 199.174.210.60 ROLANDTI MY-IP port=2346 2
39 2000-03-04 03:17:49 2003502 UDP port probe 216.62.118.3 FRED MY-IP port=2346 2
39 2000-03-04 03:18:08 2003502 UDP port probe 24.11.21.198 c613158.la.home.com MY-IP port=2346 2
39 2000-03-04 03:18:20 2003502 UDP port probe 24.72.24.121 ip121.net247224.cr.sk.ca MY-IP port=2346 2
39 2000-03-04 03:19:05 2003502 UDP port probe 210.236.133.35 SIGE MY-IP port=2346 2
39 2000-03-04 03:21:15 2003502 UDP port probe 205.244.188.32 BRIAN2 MY-IP port=2346,12
39 2000-03-04 03:23:22 2003502 UDP port probe 24.14.234.176        MY-IP port=2346 2
39 2000-03-04 03:24:05 2003502 UDP port probe 24.213.54.10, 054hgt010.bresnanlink.net, MY-IP port=2346 2
39 2000-03-04 03:25:36 2003502 UDP port probe 206.133.171.159, ROYANDERSON, MY-IP port=2346 2
39 2000-03-04 03:26:23 2003502 UDP port probe 24.161.233.85, 4GTAZ, MY-IP port=2346 2
39 2000-03-04 03:26:30 2003502 UDP port probe 206.150.169.93, JOSHKUFA, MY-IP port=2346 2
39 2000-03-04 03:29:37 2003502 UDP port probe 63.200.49.155, adsl-pacbell.net, MY-IP port=2346 2
39 2000-03-04 03:42:51 2003502 UDP port probe 63.16.249.202, JASON, MY-IP port=2346 2
```

Two thoughts came into mind at first, either I was being scanned by many people who were all working together (conspiracy theory) or a single attacker was spoofing addresses to gain either gain entrance to my computer or create a denial of service attack against me. Actually neither one really seemed to hold water. It did not seem probable that so many real people would gang up on my constantly changing DHCP-assigned dial-up connection. However, one person spoofing addresses seemed plausible, but still improbable. I printed out my results and took them to work to discuss with co-workers who ran BlackICE. One person suggested a search of Deja.com for the specific port involved. This yielded the answer to the "attack". Messages (one shown below) were found making reference to the use of port 2346 for the game 'Rogue Spear'. When the "attack is analyzed in the light of this message, an explanation emerges. Since my Internet connection is a dial-up, I get a new IP address from DHCP each time I connect. I called in and received a connection that had been used by a multi-user computer game that was hosted by a person using my ISP. When he lost his connection, the many game players all tried to reconnect (unsuccessfully) to the host computer giving the appearance of an "attack.."

Message follows:
****

Frederick A. Kolbrener
IDIC-1, SANS 2000, Orlando, FL

Subject:
IPCHAINS and Rogue Spear
Date:
03/05/2000
Author:
Adam Pearse <apearse@yahoo.com>

Hello all, I am trying to host a rogue spear game which operates on port 2346, 2347, and 2348 on tcp and udp on an internal (private) network which is connected to a Redhat 6.1 box configured with ipchains for basic nat functionality. My problem is that no one can connect to my game. Does anyone know how to configure ipchains to allow connections into my hosted game? This is what I have for connectivity from the Internet to my box when I am hosting ...

ipchains -A input -j REDIRECT -i eth0 -d 192.168.0.129 2346 -p tcp ipchains -A input -j REDIRECT -i eth0 -d 192.168.0.129 2347 -p tcp ipchains -A input -j REDIRECT -i eth0 -d 192.168.0.129 2348 -p tcp ipchains -A input -j REDIRECT -i eth0 -d 192.168.0.129 2346 -p udp ipchains -A input -j REDIRECT -i eth0 -d 192.168.0.129 2347 -p udp ipchains -A input -j REDIRECT -i eth0 -d 192.168.0.129 2348 -p udp

ANALYSIS: Was I targeted? Yes

Was the intent hostile? No. A computer acting as host for a multi-user computer game "Rogue Spear" lost a connection which I got when I dialed into my ISP. Other computers tried to reconnect to the game host unsuccessfully. No further activity involving this port has been seen.

Was I at risk? No. The port was blocked and I don't run the software on my machine.

Timing: The timing would suggest that had this been a real scan of many computers from a single computer, it would have had to have been automated if it was covering all the available ports. The signature of the "tool" would have been suggested by the fact that two UDP probes were conducted each time. Examination of the UDP packets shows the other computer sent a UDP message of '/status/'.

There is another disturbing part of this event -I intentionally left the list intact although it is a little tedious. What is apparent is that there are MANY Windows-based computers which are connecting to the internet which do not have their NetBIOS service unbound from the TCP/IP adapter for either dialup or even worse, for always-on cable (At Home) and DSL connections. This is a serious vulnerability that provides a very fertile area for persons who want to set up Distributed Denial of Service (DDOS) attack tools.

+

4. **Another Internet Gaming "Attack"**. This activity occurred two weeks after the first "gaming attack" and consisted of attempts to connect to 27015 by several different computers. Based on the previous experience with the Rogue Spear game connection attempts, this one proved fairly easy to spot. Port 27105 did not match any expected ports for services or any known Trojan or exploit. A check of Deja.com led to several messages posted regarding the game, "Half-Life" which can be run on a server as a multi-player game. I have not seen this activity since the first time, and believe that the same situation as occurred in number 3 happened. A game server lost its connection ot my ISP and I got it when I dialed in. Two extracts of messages from Deja.com follow – they refer to ports 27015 and 27016 used with the game, Half-Life. Data from BlackICE is (from left to right) severity rating, date and time in GMT, BID event code, type event, source computer, NetBIOS name of attacker, attacked IP, port targeted, and number of probes/events. As before, BID was able to extract a NetBIOS name from most of the computers indicating that many users are not protected from probes into their computers. Each set of UDP packets contained the words: "details" and "players"

```
39 2000-03-19 04:18:07 2003502 UDP port probe 24.94.233.98 MIKE 207.172.73.4 port=27015,2
39 2000-03-19 04:27:43 2003502 UDP port probe 194.251.249.48 qizmo.edome.net 207.172.73.4 port=27015,2
39 2000-03-19 05:09:19 2003502 UDP port probe 169.254.67.15     207.172.73.4 port=27015,2
39 2000-03-19 05:09:19 2003502 UDP port probe 206.58.105.210 SILICONNET 207.172.73.4 port=27015,2
39 2000-03-19 05:26:13 2003502 UDP port probe 24.188.33.68 PAVILION 207.172.73.4 port=27015,5
39 2000-03-19 05:28:50 2003502 UDP port probe 24.6.238.164 CC69739-A 207.172.73.4 port=27015,5
39 2000-03-19 05:32:56 2003502 UDP port probe 194.216.235.27 DOMINION 207.172.73.4 port=27015,5
39 2000-03-19 05:58:23 2003502 UDP port probe 150.243.176.0 eickhorst.truman.edu 207.172.73.4 port=27015,5
```

Extract of first message
****

I'm trying to run a half life server behind a firewall, and am running the following portfw rules

```
/usr/sbin/ipmasqadm portfw -f
/usr/sbin/ipmasqadm portfw -a -P tcp -L 24.114.71.49 27015 -R 10.0.0.2 27015
echo -n "HL TCP, "
/usr/sbin/ipmasqadm portfw -a -P udp -L 24.114.71.49 27015 -R 10.0.0.2 27015
echo -n "HL UDP, "
```

****

Extract of second message

When I create a dedicated Cstrike server on Internet I cannot join my own server.

I get an "could not obtain WON authentification" (sic) error. My buds can join but I can't, allthough (sic) server has port 27016 and client 27015.
****

ANALYSIS: Was I targeted? Yes. Was the intent hostile? No. A computer which had been acting as a gaming host for the game "Half-Life" lost a dial-up connection to my ISP and I was given that connection when I signed onto the ISP. Timing analysis does not apply to this sequence of attempts to connect to the computer. No further action was required by me. Was I at risk? No. The port was blocked and I don't run the software on my machine.

+

5. **Trojan Port Probes/Pings.** BID has recorded attempts to locate Trojan Horse programs when I have been on line. Obviously, there are many people out there who try to locate computers into which they may peek or seek to control. Listed below are attempts that have been logged by BID. Data from BlackICE is (from left to right) severity rating, date and time in GMT, BID event code, type event, source computer, NetBIOS name of attacker, attacked IP, port targeted, and number of probes/events.

a. **SubSeven and SubSeven 2.1**

59 2000-02-22 01:30:19 2003105 SubSeven port probe 152.204.106.90 207.172.75.185 port=1243&name=Fho+7 4
59 2000-02-10 03:55:46 2003102 TCP port probe 207.172.243.253 FROM MD on rcn.com 207.172.73.249 port=27374 16
59 2000-02-10 03:57:20 2003102 TCP port probe 194.251.251.197 user-sjk2-197.dial.inet.fi 207.172.73.249 port=27374 8
59 2000-03-04 03:31:29 2003105 SubSeven port probe 62.6.83.223 host62-6-83-223.btinternet.com 207.172.73.247 port=1243|27374&name=Fho+7 10

These SubSeven probes have been seen both from U.S.-based and off-shore (Finland) computers. They were blocked by the firewall. It is interesting to note that each has originated from an apparently different site and the number of attempts to make contact with the Trojan has been 4, 8, 10, and 16. Coupled with the different alleged sources, this would support a conclusion that four different persons tied to determine if a SubSeven Trojan was installed.

b. **NetBus Port Probe**

59 2000-03-03 02:56:38,2003103, NetBus port probe 207.172.75.144 FROM MD on rcn.com 207.172.73.2 port=12345&name=ArgOhf 4

This probe originated from a dial-up connection on my own ISP's network. Four attempts were made to gain access to the computer. At this time, packet logging was not on and no details of the individual probes are available. This is the only NetBus Trojan probe over the past 3 months. Because it is from a dial-up connection and BID did not succeed in getting data from the source computer, it is not possible to tell if this computer has executed other probes.

c. **Back Orifice ping**

59 2000-03-18 03:54:05 2001506 Back Orifice ping 216.210.34.246 - 207.172.73.43
type=PING(1)&passwd=0x7A69&length=18&xid=0x0&iport=0x0413&vport=0x7A69 1

This probe originated from a Canadian connection on Total.net. A single scan was made of this address. At that time, packet logging was not on so no details of the individual probes are available. This is the only Back Orifice probe over the past 3 months. It is not possible to tell if this computer has executed other probes on this site. My best guess is that the entire range of RCN.COM addresses was scanned for BackOrifice.

d. **Hack a' Tack probe**

59 2000-04-23 04:47:29, 2003501, UDP trojan horse probe, 207.172.33.154, COMPUTER, 207.172.73.147
port=31789&name=Unpx'n'Gnpx, 2

This single probe originated from another dial-up connection on my ISP's network this weekend. The computer name "COMPUTER" has not been seen in probes before, but it is entirely possible that the scanner changes the name of the computer as he executes different scans and probes.
BID gathered the following data about this computer: Node: COMPUTER, Group: WORKGROUP, NetBIOS: ASHISH,
MAC: 444553540000 – the MAC address is consistent with other dial-up computer connections I have seen.

ANALYSIS for all Trojan Probes: Was I targeted? Yes. Was the intent hostile? Yes. The only reason for a computer to scan other computers for installed Trojan Horses is for the purpose of gaining unauthorized access to the scanned computers. Timing analysis does not apply to this sequence of attempts to connect to the computer. Was I at risk? No. The ports were blocked and I don't have any of the Trojans installed. Each of the intrusion attempts has been reported to the proper ISP; however, there is usually no feedback from the ISP's with action they take.

+

6. **Proxy Port Probe:** This single proxy port probe was seen on February 22, 2000. I could be part of a larger port scan for Ring Zero, but the characteristic scan of ports 80, and 3128 are not present. It is more likely just a scan of computers on the RCN.COM network looking for open proxies. Two rapid probes were made. The specific data for the scans was not collected in greater detail. BID was not able to get a computer NetBIOS name for this computer.

59 2000-02-22 03:04:58 2003104 Proxy port probe 204.0.112.135   207.172.75.185 port=8080 2

ANALYSIS: Was I targeted? Yes. Was the intent hostile? Yes. The only reason for a computer to scan other computers for open proxy ports is to gain unauthorized access to the scanned computers. Timing analysis does not apply to this sequence of attempts to connect to the computer. Was I at risk? No. There was no risk to my computer since the proxy is not used and the firewall is in place.

+

7. **Port Scan**: This is a series of detects posted on GIAC that was made on April 3, 2000 by Abovenet Communications, Inc., San Jose CA, USA. Unfortunately, there is not a lot of data available on the timing involved, but the entire string of port scans occurred at 08:49:22 and covered 14 ascending ports on the machine from 33512 through 33525. All the scans originated from a single port on the scanning computer, 33161, which is indicative of an automated tool using crafted packages. If the scans had been done manually, the timing would have been more spread out and one could expect the source ports to increment. These do not. All scans were directed toward a single machine that indicates that an attempt was being made to locate an open port on that computer.

```
Apr 3 08:49:22 dns1 snort[4415]: spp_portscan:
PORTSCAN DETECTED from 208.185.54.22
Apr 3 08:49:28 dns1 snort[4415]: spp_portscan: portscan status
from 208.185.54.22: 14 connections across 1 hosts: TCP(0), UDP(14)
Apr 3 08:49:34 dns1 snort[4415]: spp_portscan: End of portscan
from 208.185.54.22
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33512 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33513 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33514 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33515 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33516 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33517 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33518 UDP
```

Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33519 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33520 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33521 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33522 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33523 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33524 UDP
Apr 3 08:49:22 208.185.54.22:33161 -> a.b.c.34:33525 UDP

ANALYSIS: Was the machine targeted? Yes. Was the intent hostile? Yes. The only reason for a computer to scan all the ports on another computer is to locate an open port to gain unauthorized access to the scanned computers. Timing analysis as above shows an automated tool as this was a very fast scan. The level of risk to this computer can't be judged based on the available data.

+

8. **Port Scan from China Posted to GIAC on 4/14/2000:** A port scan originating from China was posted to GIAC. No specific data on the system scanned was posted, nor was any indication on how the scanned system responded to the scan. The list of scans is actually three separate scans that occurred on April 12, 2000 within ten seconds. (Lines have been added to separate the three scans.) Due to the speed of the scans, it appears that some sort of automated tool was used. The pattern of the first scan is different from the following two scans. Except for port 7306, which is part of the first and third scans, standard known ports were scanned on each of the scan series. The second and third scans are very similar in structure. The first seems almost random in that the order of the ports is mixed. The source ports increment in the expected manner in the first scan, but in the second and third scans, they have been randomized time wise, but interestingly, each source port is PAIRED with its destination port in all three. This may provide a signature to this tool and this attacker. One almost gets the impression that the scanner was experimenting with different configurations of the tool. Due to the speed and closeness of the scans, this configuration decision probably would have been reached before the scan was launched.

Detect 8: Portscan from China Telecom. 4/14

Apr 12 03:10:05.941443 202.104.51.5,3785 -> 10.0.1.1,139 PR tcp len 20 44 -S
Apr 12 03:10:05.950328 202.104.51.5,3786 -> 10.0.1.1,1080 PR tcp len 20 44 -S
Apr 12 03:10:05.953418 202.104.51.5,3787 -> 10.0.1.1,7306 PR tcp len 20 44 -S
Apr 12 03:10:05.982185 202.104.51.5,3789 -> 10.0.1.1,110 PR tcp len 20 44 -S
Apr 12 03:10:05.985099 202.104.51.5,3790 -> 10.0.1.1,23 PR tcp len 20 44 -S

Apr 12 03:10:05.996190 202.104.51.5,3791 -> 10.0.1.1,21 PR tcp len 20 44 -S
Apr 12 03:10:05.996989 202.104.51.5,3792 -> 10.0.1.1,53 PR tcp len 20 44 -S
Apr 12 03:10:09.091565 202.104.51.5,3785 -> 10.0.1.1,139 PR tcp len 20 44 -S
Apr 12 03:10:09.098754 202.104.51.5,3792 -> 10.0.1.1,53 PR tcp len 20 44 -S
Apr 12 03:10:09.100331 202.104.51.5,3791 -> 10.0.1.1,21 PR tcp len 20 44 -S
Apr 12 03:10:09.107214 202.104.51.5,3789 -> 10.0.1.1,110 PR tcp len 20 44 -S
Apr 12 03:10:09.119768 202.104.51.5,3790 -> 10.0.1.1,23 PR tcp len 20 44 -S
Apr 12 03:10:09.131320 202.104.51.5,3786 -> 10.0.1.1,1080 PR tcp len 20 44 -S
Apr 12 03:10:15.366805 202.104.51.5,3787 ->10.0.1.1,7306 PR tcp len 20 44 -S
Apr 12 03:10:15.385775 202.104.51.5,3785 -> 10.0.1.1,139 PR tcp len 20 44 -S
Apr 12 03:10:15.415514 202.104.51.5,3792 -> 10.0.1.1,53 PR tcp len 20 44 -S
Apr 12 03:10:15.416053 202.104.51.5,3791 -> 10.0.1.1,21 PR tcp len 20 44 -S
Apr 12 03:10:15.418977 202.104.51.5,3789 -> 10.0.1.1,110 PR tcp len 20 44 -S
Apr 12 03:10:15.420989 202.104.51.5,3790 -> 10.0.1.1,23 PR tcp len 20 44 -S
Apr 12 03:10:15.429610 202.104.51.5,3786 -> 10.0.1.1,1080 PR tcp len 20 44 -S

ANALYSIS: Was the machine targeted? Yes. Was the intent hostile? Yes. The only reason for a computer to scan known service ports on another computer is to locate an open port in order to gain unauthorized access to the scanned computer. Timing analysis as above shows an automated tool as this was a very fast scan. The level of risk to this computer can't be judged based on the available data. It is not clear from the posted data if there was a firewall in place or the IDS tool with which this was recorded.

+

9. **Multiple Trojan Horse Scans:** Multiple Trojan Horse scans from GIAC post of 4/11/2000. This list of detects apparently was recorded in a college/university environment and shows a concerted attempt to break into one machine. This appears to be a very fast port scan using SYN packets. We do not know if a firewall was blocking these packets or not, but assume that this was recorded by a firewall as traffic that was blocked. Since we have only one side of the traffic (packets received) it is not known how many of these packets really were answered by the targeted system. The source ports are incrementing on a regular sequential basis and from the timing of the packets, it is apparent that this is an automated scan using some tool. Source ports 2441 and 2442 were apparently dropped by the data collection program and are missing. One entire scan takes place in about one second and then we see the beginning of another one. Scanning for various Trojans (and games) is interspersed with other random ports which are used by legitimate programs. In the list of dst ports are: 54321 – Back Orifice 2K; 666 – Satanz Backdoor and Doom; 1011 - Doly ver. 1 &2; 20034 – NetBus; and more. It is apparent that the scanner is seeking to find an open port to try an exploit of some kind or set up the

machine for use as a base for cracking other sites. If the ports were active on the machine, it reasonable to expect they would answer with a SYN-ACK packet.

```
Apr 6 19:44:05.798874 193.192.119.110,2435 -> 10.0.8.87,1243 PR tcp len 20 48 -S
Apr 6 19:44:05.799356 193.192.119.110,2436 -> 10.0.8.87,30100 PR tcp len 20 48 -S
Apr 6 19:44:05.803185 193.192.119.110,2437 -> 10.0.8.87,54321 PR tcp len 20 48 -S
Apr 6 19:44:05.829239 193.192.119.110,2438 -> 10.0.8.87,6670 PR tcp len 20 48 -S
Apr 6 19:44:05.829796 193.192.119.110,2439 -> 10.0.8.87,55555 PR tcp len 20 48 -S
Apr 6 19:44:05.830331 193.192.119.110,2440 -> 10.0.8.87,1257 PR tcp len 20 48 -S
Apr 6 19:44:05.830749 193.192.119.110,2443 -> 10.0.8.87,6500 PR tcp len 20 48 -S
Apr 6 19:44:05.831771 193.192.119.110,2444 -> 10.0.8.87,21554 PR tcp len 20 48 -S
Apr 6 19:44:05.835240 193.192.119.110,2446 -> 10.0.8.87,5742 PR tcp len 20 48 -S
Apr 6 19:44:05.835268 193.192.119.110,2447 -> 10.0.8.87,7307 PR tcp len 20 48 -S
Apr 6 19:44:05.870399 193.192.119.110,2448 -> 10.0.8.87,16969 PR tcp len 20 48 -S
Apr 6 19:44:05.870428 193.192.119.110,2449 -> 10.0.8.87,1170 PR tcp len 20 48 -S
Apr 6 19:44:05.881925 193.192.119.110,2450 -> 10.0.8.87,20000 PR tcp len 20 48 -S
Apr 6 19:44:05.893451 193.192.119.110,2451 -> 10.0.8.87,4950 PR tcp len 20 48 -S
Apr 6 19:44:05.905064 193.192.119.110,2452 -> 10.0.8.87,23456 PR tcp len 20 48 -S
Apr 6 19:44:05.919541 193.192.119.110,2453 -> 10.0.8.87,1080 PR tcp len 20 48 -S
Apr 6 19:44:05.919871 193.192.119.110,2454 -> 10.0.8.87,666 PR tcp len 20 48 -S
Apr 6 19:44:05.920495 193.192.119.110,2455 -> 10.0.8.87,5400 PR tcp len 20 48 -S
Apr 6 19:44:05.921098 193.192.119.110,2456 -> 10.0.8.87,1011 PR tcp len 20 48 -S
Apr 6 19:44:08.885068 193.192.119.110,2434 -> 10.0.8.87,20034 PR tcp len 20 48 -S
```

ANALYSIS: Was the machine targeted? Yes. Was the intent hostile? Yes. The only reason for a computer to scan known service ports and to try to find Trojans installed on another computer is to locate an open port to gain unauthorized access to the scanned computer. Timing analysis as above shows an automated tool as this was a very fast scan. The speed and the starting source port may constitute a signature that could be used to recognize this tool. The level of risk to this computer can't be judged based on the available data. It is not clear from the posted data if there was a firewall in place or the tool with which this was recorded.

+

10. **DNS Portscan:** This scan was listed on the GIAC site as a DNS probe from the Roadrunner network in VA. It is a SNORT listing of detects. Since SNORT is not yet ported to NT, the detection computer was either a UNIX or LINUX machine. The detect consists of a series of very fast SYN scans of a subnet attempting to connect to a DNS server port. It is not known if any of these machines was in fact a DNS server. One packet arrived out of sequence one second after the first series of scans. Based on the timing of the scan, it is apparent this was an automated tool, but the source ports do not increment by one as might be expected. This may be caused by the scanner performing an interleaved scan in an attempt to hide the full extent of his activities.

Road Runner Group, Herndon VA, USA DNS probe

```
Apr 11 05:32:59 hosth snort[87556]: spp_portscan: PORTSCAN DETECTED from 24.27.209.180
Apr 11 05:33:05 hosth snort[87556]: spp_portscan: portscan status from 24.27.209.180: 18 connections
across 18 hosts: TCP(18), UDP(0)
Apr 11 05:33:12 hosth snort[87556]: spp_portscan: portscan status from 24.27.209.180: 35 connections
across 35 hosts: TCP(35), UDP(0)
Apr 11 05:33:18 hosth snort[87556]: spp_portscan: End of portscan from 24.27.209.180
--------
Apr 11 05:32:59 24.27.209.180:1482 -> a.b.c.19:53 SYN **S*****
Apr 11 05:32:59 24.27.209.180:1489 -> a.b.c.26:53 SYN **S*****
Apr 11 05:32:59 24.27.209.180:1496 -> a.b.c.33:53 SYN **S*****
Apr 11 05:32:59 24.27.209.180:1514 -> a.b.c.51:53 SYN **S*****
Apr 11 05:32:59 24.27.209.180:1525 -> a.b.c.62:53 SYN **S*****
Apr 11 05:33:02 24.27.209.180:1546 -> a.b.c.83:53 SYN **S*****
Apr 11 05:32:59 24.27.209.180:1684 -> a.b.c.221:53 SYN **S*****
Apr 11 05:32:59 24.27.209.180:1695 -> a.b.c.232:53 SYN **S*****
Apr 11 05:32:59 24.27.209.180:1698 -> a.b.c.235:53 SYN **S*****
Apr 11 05:33:02 24.27.209.180:1652 -> a.b.c.189:53 SYN **S*****
```

ANALYSIS: Was the machine targeted? Yes. Was the intent hostile? Most likely, yes. While computers might scan a subnet looking for an open DNS port for legitimate reasons, there appears to be little reason for this series of scans to have occurred. The real reason is probably to map the network by locating a DNS server and attempting a DNS transfer once located. Timing analysis as above shows an automated tool as this was a very fast scan. The port increment spaces may indicate an interleaved scan of multiple

subnets simultaneously. The level of risk to this computer can't be judged based on the available data; however, it is probably low due to the fact that routine monitoring is in place. The monitoring tool was SNORT.

+

11. **Program configuration error:** There is no trace to support this analysis – one is constructed to illustrate the event. In the course of first using BlackICE Defender, I enabled packet logging to see what data was collected. Packet logs were limited to 1,400 kb (or 1.4 Mb). I thought little of the setting until I noticed one day that a packet log had closed at about 3:30 PM when I was not at home. Since I use a dial-up connection, it meant that there was a chance that my computer was communicating with the Internet without permission. An anti-virus scan with the latest signatures failed to find any Trojans that were then known and detectable by the AV program on the machine or other machines on my home network (3 machines). I decided that I would have to read the packet logs and located a shareware encoded scanner packet reader. The reader essentially showed the following (reconstructed):

```
date  15:15:32  10.0.0.3:port  >  10.0.0.2:6588
date  15:16:02  10.0.0.3:port  >  10.0.0.2:6588
date  15:16:32  10.0.0.3:port  >  10.0.0.2:6588
date  15:17:02  10.0.0.3:port  >  10.0.0.2:6588
date  15:17:32  10.0.0.3:port  >  10.0.0.2:6588
date  15:18:02  10.0.0.3:port  >  10.0.0.2:6588
date  15:18:32  10.0.0.3:port  >  10.0.0.2:6588
date  15:19:02  10.0.0.3:port  >  10.0.0.2:6588
```

The reader also showed that all packets were UDP and carried the same information. I knew that I ran a proxy server on one machine (10.0.0.2) and it was for one and only one program's use, a distributed computing tool from http://www.distributed.net/ working on a cryptographic problem. This machine had no direct connection to the Internet by modem as the other two computer had – thus the proxy. When I consulted the log of the program running on the third computer (10.0.0.3) I fond that it had exhausted its input buffer and was trying to get more work from the host server for the project. The problem was that I was not there to make a connection for it. Had BlackICE not been running in packet logging mode, this error in program configuration would not have shown up in the packet logs. None of the activity was logged as hostile; it was the unexpected closing of a packet log that revealed this problem.

ANALYSIS: Was the machine targeted? No. Was the intent hostile? No. A program was misconfigured and did not behave as expected. Was I at Risk? No. A program was simply misconfigured.