*** Northcutt, I really enjoyed number 3 and 4 good sleuthing! Solid analysis process, good accuracy, clear writing, evidence of both source address research and pattern research. Nice job. I have seen the pattern in 6 before, it is in a binette @home detect in Jan 15 GIAC at least, but the research was still there. I'll tag this one at 90. *

Practical Exam for GIAC Intrusion Analyst Certification

Name:	Douglas Steinbaum
Date:	2000.04.13

Introduction

This document contains an analysis of ten network security device traces for the purpose of SANS GIAC Intrusion Detection Analyst Certification.

Note: In some cases, IP addresses and/or return addresses in mail headers have been “sanitized” for privacy purposes by changing them to fabricated values. The appearance in this document of an address is not intended to imply that a host that might reside at that actual address attempted any illegal or unauthorized activity.

Trace #1

Active Targeting:

Yes

History:

No previous activity from these source addresses is known.

Analysis:

The Gauntlet firewall log shows a series of connection attempts from a single source address in Italy to a single destination address. The destination address corresponds to the external NIC of our firewall. The destination ports are those of common UNIX services: 22 (secure shell), 69 (tftp), 143 (imap mail server), 1080 (socks), 6000 (X11), etc. The activity was most likely scripted considering how short the time intervals are between the connection attempts. Common exploits exist for the services being probed.

Intent:

The person responsible for the traffic was performing a port scan of our firewall. He/she was attempting to determine which exploitable services were running on our host. He/she was also likely searching for a socks server to use for relay purposes. Also, since they were scanning for X windows services, which do not normally run on firewalls, the person likely did not know much about our network and was performing early recon.

Log file:

```
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2454 to
1.2.3.4 on unserved port 22
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2457 to
1.2.3.4 on unserved port 42
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2459 to
1.2.3.4 on unserved port 69
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2465 to
1.2.3.4 on unserved port 143
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2466 to
1.2.3.4 on unserved port 1043
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2467 to
1.2.3.4 on unserved port 1080
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2468 to
1.2.3.4 on unserved port 1745
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2469 to
1.2.3.4 on unserved port 2301
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2470 to
1.2.3.4 on unserved port 5190
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2471 to
1.2.3.4 on unserved port 5191
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2472 to
1.2.3.4 on unserved port 5192
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2473 to
1.2.3.4 on unserved port 5193
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2474 to
1.2.3.4 on unserved port 5631
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2475 to
1.2.3.4 on unserved port 5632
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2476 to
1.2.3.4 on unserved port 5800
```

```
Feb 29 00:04:42 firewall vmunix: securityalert: tcp from 212.216.1.2:2477 to
1.2.3.4 on unserved port 5900
Feb 29 00:04:42 firewall vmunix: securityalert: packet denied by local screen:
TCP if=lan1 srcaddr=212.216.1.2 srcport=2478 dstaddr=1.2.3.4
dstport=6000
```

Trace #2

Active Targeting:

Yes.

History:

No previous activity from the source address is known.

Analysis:

This Firewall One log shows repeated attempts from a single external host to connect to multiple ports on our firewall box. A DNS lookup of the source address reveals that the activity is originating from what appears to be a commercial PPP account at an ISP. Because the timestamps of the connection attempts are so closely spaced, this was an automated port scan. The target ports are the following: 1080 (socks), 8081 (a proxy port), 3128 (squid proxy). Our firewall does not have any proxies running on it, so the activity was performed by someone unfamiliar with our network.

Intent:

The person responsible for the traffic in the trace was looking for proxies that they could use. They might have wanted to use proxies that they found to hide their identity when accessing other hosts at other sites. This is a common ploy used by hackers to hide their identity.

Log file:

```
Mar  3 18:38:13 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2265 to 1.2.3.4 on unserved port 1080
Mar  3 18:38:13 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2266 to 1.2.3.4 on unserved port 3128
Mar  3 18:38:13 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2269 to 1.2.3.4 on unserved port 8081
Mar  3 18:38:14 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2265 to 1.2.3.4 on unserved port 1080
Mar  3 18:38:14 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2266 to 1.2.3.4 on unserved port 3128
Mar  3 18:38:14 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2269 to 1.2.3.4 on unserved port 8081
Mar  3 18:38:15 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2265 to 1.2.3.4 on unserved port 1080
Mar  3 18:38:15 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2266 to 1.2.3.4 on unserved port 3128
Mar  3 18:38:15 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2269 to 1.2.3.4 on unserved port 8081
Mar  3 18:38:15 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2265 to 1.2.3.4 on unserved port 1080
Mar  3 18:38:15 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2266 to 1.2.3.4 on unserved port 3128
Mar  3 18:38:15 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:2269 to 1.2.3.4 on unserved port 8081
Mar  3 18:38:25 fw1 kernel: securityalert: packet forwarding denied: ICMP if=de0 srcaddr=209.133.1.2 dstaddr=10.0.2.35
Mar  3 18:50:04 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:3636 to 1.2.3.4 on unserved port 1080
Mar  3 18:50:04 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:3637 to 1.2.3.4 on unserved port 3128
Mar  3 18:50:05 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:3641 to 1.2.3.4 on unserved port 8081
Mar  3 18:50:05 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:3636 to 1.2.3.4 on unserved port 1080
Mar  3 18:50:05 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:3637 to 1.2.3.4 on unserved port 3128
Mar  3 18:50:05 fw1 kernel: securityalert: tcp if=de0 from 209.133.1.2:3641 to 1.2.3.4 on unserved port 8081
```

Trace #3

Active Targeting:

Yes.

History:

No previous activity from the source address is known.

Analysis:

The log below was in an email message automatically sent by a Gauntlet firewall to its administrator. The log includes an email that the firewall refused to forward/deliver. The log shows that the mail message's REPLY-TO field included shell commands that, if executed, would attempt to telnet into one of our computers. Researching the source IP address revealed that it belonged to an individual in our organization's security department who had just installed a vulnerability scanner tool.

Intent

The individual who sent the mail to the firewall was attempting to exploit a majordomo list server vulnerability that allows arbitrary commands to be run as a privileged user. Several days later, the person who generated the suspicious traffic was identified as someone working in our security department. He had been scanning various hosts in our organization for vulnerabilities with the intention of alerting owners of such vulnerabilities so they could be fixed. No malice was intended. However, this illustrates the importance of alerting system administrators in one's organization of scanning activity so that they do not mistake activities of the security personnel as attacks and escalate them needlessly.

Log file:

```
   ----- The following addresses have delivery notifications -----
majordomo  (unrecoverable error)

   ----- Transcript of session follows -----
550 majordomo... User unknown

   ----- Original message follows -----

Return-Path: <nobody@localhost.mydomain.com>
Received: by firewall.mydomain.com; id JAA13170; Tue, 3 Aug 1999 09:16:14 -0400 (EDT)
Date: Tue, 3 Aug 1999 09:16:14 -0400 (EDT)
From: <nobody@localhost.mydomain.coml>
Message-Id: <199908031316.JAA13170@mydomain.com>
Received: from bad-d00d.mydomain.com (4.3.2.1) by firewall.mydomain.com via smap (4.1)
                id xma013162; Tue, 3 Aug 99 09:16:09 -0400
To: majordomo@localhost.mydomain.com
Subject: Message for you
Reply-To: XX~.`telnet\${IFS}1.2.3.4\${IFS}4878`.q~/ad=AA/c=CC\\@ZZ.box.mydomain.com

lists
```

Trace #4

Active Targeting:

Yes.

History:

The security trace shown below was received at approximately the same time as that in Trace #3 (above). The source address of all suspicious activity in this trace resolves back to the canonical name of the host that originated the attack shown in Trace #3 (bad-d00d.mydomain.com). At the time we received this log, I did not realize that a person in our security department owned bad-d00d.mydomain.com and believed that box to have possibly been compromised.

Analysis:

The Gauntlet firewall log below shows attempts to connect to ports in the 6666-6669 range, which are typically used by IRC software. This is reconnaissance done most likely to determine if we had any non-secure IRC servers. The log also shows an attempt to connect to port 31337, also known as the “ELEET” port. Back Orifice servers, which are a popular and easy to use Trojan Horse, use this port by default to communicate with their handlers.

In the second part of the log, we see that numerous failed attempts were made to FTP through our FTP proxy. The person attempted several times to FTP as user “root” and as user “anonymous”. We do not have any publicly accessible FTP servers inside of this firewall, so the activity is very suspicious. Furthermore, since the timestamps of the failed FTP attempts are so closely spaced, this looks like an automated attack, rather than a caseof a user who accidentally typed an incorrect ftp server address while manually trying to access files legitimately on a server located elsewhere.

Since the source addresses of all of the traffic in the log below are the same, and since the source addresses in this trace match those of the previous trace (#3), this appears to be evidence of a determined hacker trying to compromise our systems.

Intent:

Eventually I learned that the “hacker” responsible for the traffic that generated the suspicious logs was an employee in our organization’s security department who had gotten a new “toy” – a copy of Cyber Cop Scanner. He was using this tool to find vulnerabilities in systems at our facility with the intention of alerting system administrators of these vulnerabilities so they could be fixed. No malice was intended. Again, this illustrates the importance of alerting system administrators in one’s organization of scanning activity before it occurs to prevent unnecessary escalation.

Log file:

```
Security Alerts
---------------
Aug  3 09:14:42 firewall vmunix: securityalert: tcp from 4.3.2.1:1615 to 1.2.3.4 on unserved port 6666
Aug  3 09:14:45 firewall vmunix: securityalert: tcp from 4.3.2.1:1619 to 1.2.3.4 on unserved port 6667
Aug  3 09:14:45 firewall vmunix: securityalert: tcp from 4.3.2.1:2012 to 1.2.3.4 on unserved port 6668
Aug  3 09:16:01 firewall vmunix: securityalert: tcp from 4.3.2.1:2953 to 1.2.3.4 on unserved port 31337


Possible Items of Interest
--------------------------
Aug  3 09:14:50 firewall authsrv[13071]: BADAUTH root (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:14:50 firewall authsrv[13072]: BADAUTH anonymous (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:14:50 firewall authsrv[13074]: BADAUTH ftp (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:31 firewall authsrv[13081]: BADAUTH anonymous (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:31 firewall authsrv[13080]: BADAUTH ftp (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:31 firewall authsrv[13082]: BADAUTH anonymous (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:32 firewall authsrv[13087]: BADAUTH ftp (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:32 firewall authsrv[13086]: BADAUTH anonymous (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:32 firewall authsrv[13088]: BADAUTH ftp (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:50 firewall authsrv[13097]: BADAUTH anonymous (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
Aug  3 09:15:50 firewall authsrv[13098]: BADAUTH anonymous (ftp-gw bad-d00d.mydomain.com/4.3.2.1)
```

Trace #5

Active Targeting:

Yes

History:

While I have seen NetBus probes before, I have not seen such a flurry of NetBus scans during the entire time I have had this firewall protecting my computer. (The firewall has been in operation for about 4 months.) The source addresses of the traffic are not familiar, either. So, this looks like a new incident unrelated to previous incidents.

Analysis:

The scan below comes from a SonicWall firewall protecting a home computer connected to a cable modem. The home computer's address is 24.10.X.Y (the last two octets are not shown for privacy purposes). The scan shows several dozen probes to port 12345, which is the port on which the NetBus Trojan Horse listens. The scans ostensibly come from a multitude of source addresses. Normally, when probing systems for the presence of NetBus or another Trojan Horse, the attacker must use his/her real source address so that he/she can receive responses from the compromised machines. However, the log shows that the NetBus probes occurred numerous times over a short period of time, and occurred somewhat regularly - approximately once every 10 or 20 minutes. In the past, I have not observed such a large number of NetBus probes of this firewall. This sudden burst of probes is anomalous. Doing DNS lookups of the source addresses, I found that those which can be resolved are for hosts all around the world – some addresses correspond to a dialup account for an ISP in Sweden, some correspond to a Canadian ISP, some correspond to various dialup accounts with different ISPs in California, and one corresponds to a host in Argentina. Obviously, it too much of a coincidence that people in these diverse places all of a sudden decided to do a NetBus probe of my firewall over a short period of time. Based on the fact that the probes appear to be related since they occurred together over a short period of time, I am concluding that the same party initiated them all. However, for a NetBus probe to be of any value to a hacker, he/she must be able to receive responses from the probed computer. This requires that one of the two conditions hold: (1) The hacker uses his/her true source address when constructing the scan packets; (2) The hacker can sniff the responses produced by the victim computer that is being probed. Neither condition seemed possible until I remembered that cable modem customers in an apartment building or a small community all share the same broadcast media (the coax cable TV line) for their communications. Since this probed firewall is connected to the Internet by means of a cable modem in a large apartment complex, the explanation seems clear: The attacker's computer is connected to the same LAN as my computer. It is quite probable that he/she is located in the same apartment building as I, too.

Since the firewall is protecting the computer, the NetBus probes are fairly harmless. However, this incident made me realize that my "private" computer communications are likely visible to other cable ISP customers in my apartment complex.

Intent:

The person producing the traffic visible in the firewall log is most likely intent on completely compromising my home computer.

Log file:

```
04/04/2000 11:50:58.880 - NetBus Attack Dropped - Source:211.32.196.81, 1148, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 12:08:53.368 - NetBus Attack Dropped - Source:212.151.128.43, 1314, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 12:12:39.848 - NetBus Attack Dropped - Source:212.151.138.112, 1288, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 12:16:09.800 - NetBus Attack Dropped - Source:208.167.233.110, 1503, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 12:32:50.864 - NetBus Attack Dropped - Source:210.127.71.203, 1416, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 12:51:49.256 - NetBus Attack Dropped - Source:211.50.125.19, 1384, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 13:10:17.480 - NetBus Attack Dropped - Source:212.151.122.33, 1541, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 13:25:00.432 - NetBus Attack Dropped - Source:213.1.73.176, 1208, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 13:35:25.480 - NetBus Attack Dropped - Source:203.80.212.154, 1167, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 13:35:28.512 - ICMP packet dropped - Source:137.39.23.209, 3, WAN - Destination:24.10.X.Y, 3, LAN - 'Dest Unreachable' - Rule 0
04/04/2000 13:36:57.784 - NetBus Attack Dropped - Source:211.44.30.155, 2121, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 13:47:37.000 - NetBus Attack Dropped - Source:24.222.43.48, 1864, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 14:22:41.000 - NetBus Attack Dropped - Source:166.72.150.4, 2783, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 14:36:05.592 - NetBus Attack Dropped - Source:63.27.35.253, 2100, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 14:41:32.240 - NetBus Attack Dropped - Source:148.235.8.3, 1817, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 14:46:31.672 - NetBus Attack Dropped - Source:210.217.61.51, 1206, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 14:54:18.240 - NetBus Attack Dropped - Source:210.183.31.139, 1390, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 15:13:08.832 - NetBus Attack Dropped - Source:211.40.192.207, 4674, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 15:27:28.688 - NetBus Attack Dropped - Source:62.137.97.173, 2610, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 15:33:50.128 - NetBus Attack Dropped - Source:213.1.94.160, 2501, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 15:59:24.672 - NetBus Attack Dropped - Source:212.151.128.118, 1201, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 16:59:21.096 - NetBus Attack Dropped - Source:211.48.237.174, 1106, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 18:01:56.720 - NetBus Attack Dropped - Source:24.2.31.36, 2306, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 19:58:06.464 - UDP packet dropped - Source:24.5.80.34, 53, WAN - Destination:24.10.X.Y, 10316, LAN - - Rule 0
04/04/2000 19:58:11.432 - UDP packet dropped - Source:24.5.80.33, 53, WAN - Destination:24.10.X.Y, 10244, LAN - - Rule 0
04/04/2000 21:19:03.704 - ICMP packet dropped - Source:24.15.134.141, 8, WAN - Destination:24.10.X.Y, 8, LAN - 'Ping' - Rule 0
```

```
04/04/2000 21:22:32.224 - NetBus Attack Dropped - Source:24.232.18.163, 3595, WAN - Destination:24.10.X.Y, 12345, LAN - -
04/04/2000 23:31:21.576 - NetBus Attack Dropped - Source:63.22.12.223, 2479, WAN - Destination:24.10.226.124, 12345, LAN - -
```

Trace #6

History:

On 2000.04.12, I observed an unusual probe to UDP port 28431 in my SonicWall firewall log. I checked my older log records, and discovered a probe to this same unusual port had occurred on 2000.04.03. The two probes have different source addresses. The older probe originated from a host on the AOL domain; the newer probe originated from Saudi Arabia. A reverse DNS lookup of the older probe's hostname revealed the rather unusual name "ABD5ED29.ipt.aol.com". Thinking that this might be geographically close to the second probe's origin (Saudi Arabia), I did a trace-route to ABD5ED29.ipt.aol.com. The trace-route indicated that this host is located in VA, USA. I am not sure whether the two probes are related. They may not have been initiated by the same party; but, they likely were initiated for the same purpose.

Active Targeting:

Yes.

Analysis:

The second SonicWall trace below show a probe from 195.229.229.83 (the host is cac083.emirates.net.ae), located in Saudi Arabia. The probe was performed only once, and targeted UDP port 28431. This probe is identical to one made earlier by 171.213.237.41 (this is the AOL host mentioned above). I did a netstat of the computer the external host attempted to probe, and determined that the computer was not listening on UDP 28431. So, the prober likely was not targeting my computer specifically; they were likely targeting my computer along with numerous others in its address space. So, I conclude that these probes are likely part of a massive sweep search of random computers for a Trojan Horse.

Searching the web yielded a reference to probes of UDP port 28431:

http://www.securityfocus.com/templates/archive.pike?list=75&date=1999-12-22&msg=30487.946046116@shore.net

The individual at the URL above detected a probe to UDP port 28431 on his host, which is located in the Eastern United States, as is mine. His probe packet had a different source address; however, his and one of my source addresses originated in Saudi Arabia, which is very intriguing. This could be evidence of a new type of Trojan Horse making its rounds across the 'Net.

Intent:

The intent is not completely clear. However, it seems likely that a new Trojan Horse is being distributed, and people are attempting to detect its presence on multiple hosts.

Log file:

```
First probe:
04/03/2000 19:04:22.528 - UDP packet dropped - Source:171.213.237.41, 28432, WAN - Destination:24.10.X.Y, 28431, LAN - - Rule 0

Second probe:
04/12/2000 00:55:49.608 -  UDP packet dropped -  Source:195.229.229.83, 28432, WAN -  Destination:24.10.X.Y, 28431, LAN -   -  Rule 0
```

Trace #7

Active Targeting:

Yes.

History:

No previous activity from the source address 62.36.157.170 has previously been observed. However, similar activity to that shown in the log file below has been observed for source addresses 24.5.A.B. and 24.0.94.130.

Analysis:

The firewall log file shows a series of connection attempts to my host, 24.10.X.Y. The first two entries in the log show UDP traffic from a DNS server. These two entries are similar to numerous other occurrences observed in the past. The source of the packets is the DNS that serves hosts behind the firewall. The most likely scenario for the firewall blocking these two connection attempts is as follows: A client behind the firewall opened a connection through the firewall to talk to the DNS. The firewall updated its state table to expect a response from the DNS to the client computer. But, the DNS took too long to respond to the client, so the stateful firewall cleared the entry in its state table that would have allowed a response to come back from the DNS to the requesting client. When the DNS finally did send a response, the firewall did not know it was part of an earlier connection, so it blocked it. This traffic is therefore benign and simply indicative of a slow DNS.

The connection attempts to port 119 (news) are also similar to previously observed activity. A DNS lookup of the source address shows that the traffic all originates from the ISP, and are simply routine scans by the ISP to ensure that unauthorized news servers are not connected to their network.

Buried within the news port probes is a connection attempt to port 21, the FTP command port. There is no FTP server running behind the firewall, so this activity is suspicious. A DNS lookup of the source address indicates the traffic originated from a dialup account in Spain. This activity could simply be the result of someone mis-typing an address when attempting to open a connection to a legitimate ftp server somewhere else. It could also be evidence of someone probing my host to determine if it is running an ftp server.

Intent:

The DNS traffic is part of normal network activity and can be ignored.

The news traffic is part of an ongoing probe by my ISP to determine whether any of its customers are running unauthorized news servers. These probes are benign and can be ignored.

The FTP connection attempt could simply be accidental. However, it also could be an attempt to determine if my host is running an FTP server. FTP servers are not always securely configured or properly patched, and are often vulnerable to attacks that can be used to gain access to the computer. So, it is possible that the prober was attempting to compromise my computer. Another possible explanation is that the prober was looking for an ftp server that allows anonymous users to store data so that he/she could use it as a repository for various files such as “warez” material.

Log file:

```
SonicWALL Log (part 1) dumped to email at 04/11/2000 20:12:58.752
04/02/2000 01:07:27.880 - Log successfully sent via email
04/02/2000 12:22:14.336 - UDP packet dropped - Source:24.5.A.B, 53, WAN - Destination:24.10.X.Y, 12170, LAN - - Rule 0
04/02/2000 13:22:35.336 - UDP packet dropped - Source:24.5.A.B, 53, WAN - Destination:24.10.X.Y, 12172, LAN - - Rule 0
04/02/2000 14:01:13.448 - TCP connection dropped - Source:24.0.94.130, 43434, WAN - Destination:24.10.X.Y, 119, LAN - 'News (NNTP)' - Rule 0
04/02/2000 14:01:37.176 - TCP connection dropped - Source:24.0.94.130, 59776, WAN - Destination:24.10.X.Y, 119, LAN - 'News (NNTP)' - Rule 0
04/02/2000 15:11:43.112 - TCP connection dropped - Source:62.36.157.170, 1849, WAN - Destination:24.10.X.Y, 21, LAN - 'File Transfer (FTP)' - Rule 0
04/02/2000 18:39:12.064 - TCP connection dropped - Source:24.0.94.130, 37794, WAN - Destination:24.10.X.Y, 119, LAN - 'News (NNTP)' - Rule 0
04/02/2000 18:39:28.528 - TCP connection dropped - Source:24.0.94.130, 48716, WAN - Destination:24.10.X.Y, 119, LAN - 'News (NNTP)' - Rule 0
04/02/2000 23:30:07.128 - TCP connection dropped - Source:24.0.94.130, 38793, WAN - Destination:24.10.X.Y, 119, LAN - 'News (NNTP)' - Rule 0
04/02/2000 23:30:28.368 - TCP connection dropped - Source:24.0.94.130, 50463, WAN - Destination:24.10.X.Y, 119, LAN - 'News (NNTP)' - Rule 0
```

Trace #8

Active Targeting:

Yes.

History:

No previous activity from the source address is known.

Analysis:

In this log entry, we see a connection attempt from a commercial website (the actual IP address was sanitized) to a client computer's identd service (port 113). Identd, when requested, will provide the name of the currently logged-in user to the requesting machine. Queries to the ident port of a client often occur when the attempts to connect to a server that is running TCP-Wrappers. TCP-Wrappers, depending on its configuration, may do an ident query to determine who initiated a connection and/or to determine if address spoofing is occurring.

This probe was most likely an automated response by a TCP-Wrappers daemon running on a commercial website accessed by a client host.

Intent:

This probe was most likely automatically initiated by the commercial web server for the purpose of blocking connection attempts from clients with spoofed source addresses. The probe is thus most likely benign. Note, however, that it is not a good idea to advertise one's username, as doing so makes it easier for others to break into one's computer (if the username is known, then only the password, as opposed to the password plus the username, must be guessed). So, it is good practice to block ident requests.

Trace Content:

```
04/06/2000 01:29:38.464 - TCP connection dropped - Source:a.b.c.d, 26830, WAN - Destination:24.10.X.Y, 113, LAN - 'Authentication' - Rule 0
```

Trace #9

Active Targeting:

Yes.

History:

No previous connection attempts from source address shown in the trace have been detected. No previous connection attempts with a source port of 3133 have been detected.

Analysis:

The SonicWall firewall trace shows four closely spaced connection attempts from the same source to port 80 of the firewall. Since no hosts behind the firewall are running a web server, this traffic is suspicious. Inspection of the traffic reveals that all four connection attempts have the same source port: 3133. This is anomalous behavior, since source ports should be different for each connection attempt originating from a given host. This indicates that the four connection attempts were likely made using crafted packets. It is interesting to note that the number used for the source port, 3133, has the same value as the first four digits of the popular "ELEET" port (31337) used by Back Orifice. Also interesting to note is that a WHOIS query of the source address indicates that the address is owned by a company in the Republic of Belarus.

Intent:

The party responsible for generating the traffic that resulted in the trace below was likely attempting to find web servers for exploitation. Unfortunately, the firewall log does not include details about the packets' payloads. It is likely that the payloads included HTTP GET commands designed to take advantage of one of the many existing web server vulnerabilities. Since no web servers have ever existed behind the firewall that was probed, it is clear that the prober was unfamiliar with my network and was probing random blocks of IP address space to find vulnerable systems.

Log file:

```
03/12/2000 14:10:17.032 -   TCP connection dropped -   Source:193.232.248.199, 3133, WAN -   Destination:24.10.X.Y, 80, LAN -   'Web (HTTP)' -   Rule 0
03/12/2000 14:10:17.832 -   TCP connection dropped -   Source:193.232.248.199, 3133, WAN -   Destination:24.10.X.Y, 80, LAN -   'Web (HTTP)' -   Rule 0
03/12/2000 14:10:18.736 -   TCP connection dropped -   Source:193.232.248.199, 3133, WAN -   Destination:24.10.X.Y, 80, LAN -   'Web (HTTP)' -   Rule 0
03/12/2000 14:10:19.560 -   TCP connection dropped -   Source:193.232.248.199, 3133, WAN -   Destination:24.10.X.Y, 80, LAN -   'Web (HTTP)' -   Rule 0
```

Trace #10

Active Targeting:

Yes.

History:

This alert appeared numerous times initially after installation of the IDS.

Analysis:

A NetRanger IDS was configured to monitor traffic passing through a firewall. The IDS was installed inside of the firewall and a stock signature configuration was used. Shortly after installation, the NetRanger generated a series of level 4 (i.e., serious) alerts of type 3010, indicating a "TCP High Port Sweep" had occurred. This alert indicated that a series of TCP connections had been made to sequential ports of a single host on the protected network. Since the alert icon shown in the IDS' GUI did not reveal much, I examined the raw log files.

The NetRanger's raw log files showed that in each case, the offending connection's source port was 80 and its source address was that of the inner interface of the firewall. The destination address of the connection was a Windows workstation located inside of the firewall. These connections are highlighted below. The context of the highlighted alerts reveals that just before the alert triggered, the Windows workstation made a series of connections to a web server outsideof the firewall. The source port numbers used by the workstation to access the web had been increasing sequentially. Thus, the web server was replying back to a series of sequentially increasing ports on the workstation. This caused the NetRanger to alarm. This is a false alarm.

Intent:

This was a false alarm. The NetRanger should be tuned by disabling alert 3010 to prevent this false alarm in the future.

Log file:

Note 1: Address 1.2.3.4 corresponds to the Windows workstation inside of our firewall.
Note 2: Address 2.4.6.8 corresponds to the inside interface of the firewall that is the default gateway for host 1.2.3.4.

```
4,1002136,2000/04/06,12:03:33,2000/04/06,12:03:33,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1559,80,0.0.0.0,75473680
4,1002137,2000/04/06,12:04:10,2000/04/06,12:04:10,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1560,80,0.0.0.0,75510557
4,1002138,2000/04/06,12:04:10,2000/04/06,12:04:10,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1561,80,0.0.0.0,75510558
4,1002139,2000/04/06,12:04:10,2000/04/06,12:04:10,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1562,80,0.0.0.0,75510563
4,1002140,2000/04/06,12:04:21,2000/04/06,12:04:21,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1563,80,0.0.0.0,75521400
4,1002141,2000/04/06,12:04:24,2000/04/06,12:04:24,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1564,80,0.0.0.0,75524362
4,1002142,2000/04/06,12:04:33,2000/04/06,12:04:33,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1565,80,0.0.0.0,75533180
4,1002143,2000/04/06,12:05:02,2000/04/06,12:05:02,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1566,80,0.0.0.0,75561860
4,1002144,2000/04/06,12:05:09,2000/04/06,12:05:09,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1567,80,0.0.0.0,75569793
4,1002145,2000/04/06,12:05:29,2000/04/06,12:05:29,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1568,80,0.0.0.0,75589646
4,1002146,2000/04/06,12:05:36,2000/04/06,12:05:36,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1569,80,0.0.0.0,75596126
4,1002147,2000/04/06,12:05:36,2000/04/06,12:05:36,10008,10,5000,IN,IN,4,3010,0,TCP/IP,2.4.6.8,1.2.3.4,80,1569,0.0.0.0,
4,1002148,2000/04/06,12:05:39,2000/04/06,12:05:39,10008,10,5000,IN,OUT,2,3000,80,TCP/IP,132.250.89.112,132.250.89.204,35228,80,0.0.0.0,1339698
4,1002149,2000/04/06,12:06:05,2000/04/06,12:06:05,10008,10,5000,IN,OUT,2,3000,80,TCP/IP,132.250.89.112,132.250.89.204,35230,80,0.0.0.0,1467789
4,1002150,2000/04/06,12:06:16,2000/04/06,12:06:16,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1570,80,0.0.0.0,75636243
4,1002151,2000/04/06,12:06:16,2000/04/06,12:06:16,10008,10,5000,IN,IN,4,3010,0,TCP/IP,2.4.6.8,1.2.3.4,80,1570,0.0.0.0,
4,1002152,2000/04/06,12:06:19,2000/04/06,12:06:19,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1571,80,0.0.0.0,75638892
4,1002153,2000/04/06,12:06:28,2000/04/06,12:06:28,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1572,80,0.0.0.0,75648358
4,1002154,2000/04/06,12:06:36,2000/04/06,12:06:36,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1573,80,0.0.0.0,75656027
4,1002155,2000/04/06,12:06:37,2000/04/06,12:06:37,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1574,80,0.0.0.0,75657293
4,1002156,2000/04/06,12:06:54,2000/04/06,12:06:54,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1575,80,0.0.0.0,75674088
4,1002157,2000/04/06,12:07:02,2000/04/06,12:07:02,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1576,80,0.0.0.0,75682382
4,1002158,2000/04/06,12:07:39,2000/04/06,12:07:39,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1577,80,0.0.0.0,75719567
4,1002159,2000/04/06,12:07:40,2000/04/06,12:07:40,10008,10,5000,IN,IN,4,3010,0,TCP/IP,2.4.6.8,1.2.3.4,80,1577,0.0.0.0,
4,1002160,2000/04/06,12:07:42,2000/04/06,12:07:42,10008,10,5000,IN,IN,2,3000,80,TCP/IP,1.2.3.4,2.4.6.8,1578,80,0.0.0.0,75721981
```