Global Information Assurance Certification Paper

*** Northcutt, good job, we have some analysis, research, correlations and so forth! 80 *

10 Network Detects for SANS Intrusion Analyst Certification

by

Geoffrey Young

I selected these examples from my files of network detects which I have had under investigation. These detects were deterred by our firewall, which logs and drops the packets, therefore I would put their Severity or Threat Level on the low side. However, if the firewall were not in place, most of these access attempts could have been very serious because of their nature - from mapping attempts to searching for trojans.

Example 1:

History: I noticed this source (147.46.46.169) accessing us over a period of time. This activity went on for a few weeks. It stopped two days after I escalated to our CERT group, and I haven't seen any activity from this site since that time.

Technique: This is a "Low and Slow" probe, probably manually done. The Whois lead us to Seoul National University Computer Center in KOREA, so this could be a 'student exercise'. The times are grouped throughout the day from just after midnight our time, to early morning and again in early evening.

Intent: Looks like an attempt to "stealth" map our network.

Targeting: Masquerading as telnet sessions to various hosts in our subnets, to random ports. Most are high ephemeral ports and I am not aware of any specific services on those ports. The only reserved port number scanned was port 18, which IANA lists as Message Send Protocol. Notice also the second attempt is to host zero(0), which would be a network broadcast type access, and can also be used to distinguish operating systems.

Analysis: It looks as though they are attempting to stealth map our site. Those hosts should not be originating telnets to us, so the possibility does not exist that these are "orphaned" telnet sessions that timed out (which I think they are supposed to look like -- source port 23 on the external site going to a "random" high port on our DMZ address). Oddly enough, two days after reporting this to our CERT, the probes stopped, and have not been seen again.

Oct 16 14:02:59 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.123 dstport=2415
Oct 16 16:33:43 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.0 dstport=7175
Oct 16 19:57:39 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.114 dstport=7543
Oct 18 10:20:46 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.12 dstport=4809
Oct 18 23:18:38 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.123 dstport=9232
Oct 22 21:56:09 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.47 dstport=7257
Oct 23 03:03:57 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.89 dstport=9966
Oct 24 06:21:25 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.28 dstport=5758
Oct 25 23:44:17 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.101 dstport=9077
Oct 27 00:37:15 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.67 dstport=7434
Oct 27 10:09:20 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.53 dstport=1083
Oct 29 17:47:46 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.67 dstport=9735
Oct 29 20:03:10 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.70 dstport=1658

Oct 29 20:03:10 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.70 dstport=1658
Oct 30 06:21:45 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.121 dstport=1529
Oct 30 23:06:46 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.104 dstport=7115
Oct 30 23:06:47 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.104 dstport=7115
Nov 1 01:07:11 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.32 dstport=7539
Nov 1 01:07:11 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.32 dstport=7539
Nov 1 07:56:47 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.11 dstport=8142
Nov 1 07:56:47 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.11 dstport=8142
Nov 1 08:16:07 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.46 dstport=7854
Nov 1 10:01:44 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.39 dstport=18
Nov 1 10:01:44 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.39 dstport=18
Nov 2 06:29:16 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.56 dstport=8740
Nov 2 08:45:48 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.36 dstport=6711
Nov 2 11:44:23 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.47 dstport=5132
Nov 2 11:44:23 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.47 dstport=5132
Nov 2 17:48:59 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.9 dstport=3635
Nov 2 22:54:19 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.122 dstport=8622
Nov 3 01:26:12 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.98 dstport=2215
Nov 3 09:42:30 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.19 dstport=5621
Nov 3 09:42:31 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.19 dstport=5621
Nov 3 21:20:46 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.66 dstport=4631
Nov 3 21:20:46 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.66 dstport=4631
Nov 4 01:33:05 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.21 dstport=409
Nov 4 03:02:37 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.126 dstport=2311
Nov 4 07:16:22 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.73 dstport=2920
Nov 4 07:16:22 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.73 dstport=2920
Nov 4 11:33:37 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.127 dstport=2424

Nov 4 12:01:35 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.64 dstport=4968
Nov 4 18:52:42 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.3 dstport=9321
Nov 4 18:52:42 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.251.3 dstport=9321
Nov 5 02:39:39 opsystem: securityalert: no match found in forward screen: TCP if=hme1 srcaddr=147.46.46.169 srcport=23 dstaddr=My.Site.254.68 dstport=4641

Example 2:

History: This is seemingly a one-time scan. Reviewing our history files I found no other access from this source.

Technique: A probe which increments through our network host range. This is probably a script because the timestamp is the same for each access.

Intent: Scan to try and locate Back Orifice

Targeting: This scan is aimed specifically at addresses that are advertised to the world; no attempt was made on any other hosts.

Analysis: This scan for Back Orifice came through an ISP, so I was unable to determine a specific originating host. When they received no response from our firewall, they probably moved on to an easier target. Note the same source port number (rather than incrementing) which further lends itself to being a script. Sequence numbers, ttl, and information of that nature would have been helpful in a clearer understanding of what was occurring.

```
Mar 18 21:30:56  opsystem: securityalert: udp from 613.210.128.161:1966 to Our.IP.Addr.94 on
unserved port 31337
Mar 18 21:30:56  opsystem: securityalert: udp from 613.210.128.161:1966 to Our.IP.Addr.95 on
unserved port 31337
Mar 18 21:30:56  opsystem: securityalert: udp from 613.210.128.161:1966 to Our.IP.Addr.96 on
unserved port 31337
```

Example 3:

History: This scan was first reported by our sister site; and the next day I had this one on my system. I began to be concerned that we were being targeted like this, to specific machines and to these ports with known vulnerabilities.

Technique: This is an automated scan based on the timestamp, which is targeting many of the "problem ports" of a Microsoft machine.

Intent: This looks like a vulnerability scan, possibly reconnaissance for a later attack.

Targeting: The scan targets ports 139 - Netbios (also used for the OOB attack), 80 - HTTP (probably CGI or other type probes), 110 - POP Mail, 143 - IMAP, 161 - SNMP, and 443 - SSL.

Analysis: On investigation, it was found that this is a service offered by Gibson Research Corp., where you go to their web site and request a scan of your machine. Someone in the organization elicited this response by clicking the Shield's Up product to be scanned. In this case it was foiled by our firewall, and we passed with flying colors. I am also happy to report Steve Gibson highly recommends personal firewalls. So it turned out this seems to be one of the White Hats this time.

```
Dec 14 06:38:17  opsystem: securityalert: tcp from 207.71.92.221:4634 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:38:18  opsystem: securityalert: tcp from 207.71.92.221:4634 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:38:18  opsystem: securityalert: tcp from 207.71.92.221:4634 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:38:19  opsystem: securityalert: tcp from 207.71.92.221:4634 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:38:51  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4659 dstaddr=aaa.bbb.ccc.194 dstport=80
Dec 14 06:38:54  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4659 dstaddr=aaa.bbb.ccc.194 dstport=80
Dec 14 06:39:00  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4659 dstaddr=aaa.bbb.ccc.194 dstport=80
Dec 14 06:39:12  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4659 dstaddr=aaa.bbb.ccc.194 dstport=80
Dec 14 06:39:36  opsystem: securityalert: tcp from 207.71.92.221:4689 to aaa.bbb.ccc.194 on
unserved port 110
Dec 14 06:39:38  opsystem: securityalert: tcp from 207.71.92.221:4689 to aaa.bbb.ccc.194 on
unserved port 110
Dec 14 06:39:38  opsystem: securityalert: tcp from 207.71.92.221:4694 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:39:40  opsystem: securityalert: tcp from 207.71.92.221:4698 to aaa.bbb.ccc.194 on
unserved port 143
Dec 14 06:39:40  opsystem: securityalert: tcp from 207.71.92.221:4698 to aaa.bbb.ccc.194 on
unserved port 143
Dec 14 06:39:41  opsystem: securityalert: tcp from 207.71.92.221:4698 to aaa.bbb.ccc.194 on
unserved port 143
```

```
Dec 14 06:39:42  opsystem: securityalert: tcp from 207.71.92.221:4698 to aaa.bbb.ccc.194 on
unserved port 143
Dec 14 06:39:42  opsystem: securityalert: tcp from 207.71.92.221:4702 to aaa.bbb.ccc.194 on
unserved port 161
Dec 14 06:39:42  opsystem: securityalert: tcp from 207.71.92.221:4702 to aaa.bbb.ccc.194 on
unserved port 161
Dec 14 06:39:43  opsystem: securityalert: tcp from 207.71.92.221:4702 to aaa.bbb.ccc.194 on
unserved port 161
Dec 14 06:39:44  opsystem: securityalert: tcp from 207.71.92.221:4702 to aaa.bbb.ccc.194 on
unserved port 161
Dec 14 06:39:44  opsystem: securityalert: tcp from 207.71.92.221:4705 to aaa.bbb.ccc.194 on
unserved port 443
Dec 14 06:39:44  opsystem: securityalert: tcp from 207.71.92.221:4705 to aaa.bbb.ccc.194 on
unserved port 443
Dec 14 06:39:45  opsystem: securityalert: tcp from 207.71.92.221:4705 to aaa.bbb.ccc.194 on
unserved port 443
Dec 14 06:39:45  opsystem: securityalert: tcp from 207.71.92.221:4705 to aaa.bbb.ccc.194 on
unserved port 443
Dec 14 06:41:24  opsystem: securityalert: tcp from 207.71.92.221:4787 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:41:25  opsystem: securityalert: tcp from 207.71.92.221:4787 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:41:26  opsystem: securityalert: tcp from 207.71.92.221:4787 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:41:26  opsystem: securityalert: tcp from 207.71.92.221:4787 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:42:28  opsystem: securityalert: tcp from 207.71.92.221:4851 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:42:28  opsystem: securityalert: tcp from 207.71.92.221:4851 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:42:30  opsystem: securityalert: tcp from 207.71.92.221:4851 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:42:49  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4866 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:42:52  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4866 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:42:58  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4866 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:43:01  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4874 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:43:04  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4874 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:43:10  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4866 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:43:10  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4874 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:43:22  opsystem: securityalert: packet denied by local screen: TCP if=hme1
srcaddr=207.71.92.221 srcport=4874 dstaddr=aaa.bbb.ccc.195 dstport=80
Dec 14 06:43:34  opsystem: securityalert: tcp from 207.71.92.221:4891 to aaa.bbb.ccc.195 on
unserved port 110
Dec 14 06:43:36  opsystem: securityalert: tcp from 207.71.92.221:4893 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:43:37  opsystem: securityalert: tcp from 207.71.92.221:4893 to aaa.bbb.ccc.195 on
unserved port 139
```

```
Dec 14 06:43:37  opsystem: securityalert: tcp from 207.71.92.221:4893 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:43:38  opsystem: securityalert: tcp from 207.71.92.221:4893 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:43:38  opsystem: securityalert: tcp from 207.71.92.221:4895 to aaa.bbb.ccc.195 on
unserved port 143
Dec 14 06:43:40  opsystem: securityalert: tcp from 207.71.92.221:4901 to aaa.bbb.ccc.195 on
unserved port 161
Dec 14 06:43:41  opsystem: securityalert: tcp from 207.71.92.221:4901 to aaa.bbb.ccc.195 on
unserved port 161
Dec 14 06:43:42  opsystem: securityalert: tcp from 207.71.92.221:4901 to aaa.bbb.ccc.195 on
unserved port 161
Dec 14 06:43:42  opsystem: securityalert: tcp from 207.71.92.221:4904 to aaa.bbb.ccc.195 on
unserved port 443
Dec 14 06:43:43  opsystem: securityalert: tcp from 207.71.92.221:4904 to aaa.bbb.ccc.195 on
unserved port 443
Dec 14 06:43:44  opsystem: securityalert: tcp from 207.71.92.221:4904 to aaa.bbb.ccc.195 on
unserved port 443
Dec 14 06:43:44  opsystem: securityalert: tcp from 207.71.92.221:4904 to aaa.bbb.ccc.195 on
unserved port 443
Dec 14 06:43:46  opsystem: securityalert: tcp from 207.71.92.221:4908 to aaa.bbb.ccc.195 on
unserved port 110
Dec 14 06:43:47  opsystem: securityalert: tcp from 207.71.92.221:4908 to aaa.bbb.ccc.195 on
unserved port 110
Dec 14 06:43:47  opsystem: securityalert: tcp from 207.71.92.221:4908 to aaa.bbb.ccc.195 on
unserved port 110
Dec 14 06:43:48  opsystem: securityalert: tcp from 207.71.92.221:4908 to aaa.bbb.ccc.195 on
unserved port 110
Dec 14 06:43:48  opsystem: securityalert: tcp from 207.71.92.221:4911 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:43:49  opsystem: securityalert: tcp from 207.71.92.221:4911 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:43:49  opsystem: securityalert: tcp from 207.71.92.221:4911 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:43:50  opsystem: securityalert: tcp from 207.71.92.221:4911 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:43:50  opsystem: securityalert: tcp from 207.71.92.221:4914 to aaa.bbb.ccc.195 on
unserved port 143
Dec 14 06:43:51  opsystem: securityalert: tcp from 207.71.92.221:4914 to aaa.bbb.ccc.195 on
unserved port 143
Dec 14 06:43:51  opsystem: securityalert: tcp from 207.71.92.221:4914 to aaa.bbb.ccc.195 on
unserved port 143
Dec 14 06:43:52  opsystem: securityalert: tcp from 207.71.92.221:4914 to aaa.bbb.ccc.195 on
unserved port 143
Dec 14 06:43:52  opsystem: securityalert: tcp from 207.71.92.221:4915 to aaa.bbb.ccc.195 on
unserved port 161
Dec 14 06:43:53  opsystem: securityalert: tcp from 207.71.92.221:4915 to aaa.bbb.ccc.195 on
unserved port 161
Dec 14 06:43:54  opsystem: securityalert: tcp from 207.71.92.221:4915 to aaa.bbb.ccc.195 on
unserved port 161
Dec 14 06:43:54  opsystem: securityalert: tcp from 207.71.92.221:4915 to aaa.bbb.ccc.195 on
unserved port 161
Dec 14 06:43:54  opsystem: securityalert: tcp from 207.71.92.221:4919 to aaa.bbb.ccc.195 on
unserved port 443
```

```
Dec 14 06:43:55  opsystem: securityalert: tcp from 207.71.92.221:4919 to aaa.bbb.ccc.195 on
unserved port 443
Dec 14 06:43:56  opsystem: securityalert: tcp from 207.71.92.221:4919 to aaa.bbb.ccc.195 on
unserved port 443
Dec 14 06:43:56  opsystem: securityalert: tcp from 207.71.92.221:4919 to aaa.bbb.ccc.195 on
unserved port 443
Dec 14 06:45:29  opsystem: securityalert: tcp from 207.71.92.221:4953 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:45:30  opsystem: securityalert: tcp from 207.71.92.221:4953 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:45:31  opsystem: securityalert: tcp from 207.71.92.221:4953 to aaa.bbb.ccc.194 on
unserved port 139
Dec 14 06:45:33  opsystem: securityalert: tcp from 207.71.92.221:4958 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:45:34  opsystem: securityalert: tcp from 207.71.92.221:4958 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:45:34  opsystem: securityalert: tcp from 207.71.92.221:4958 to aaa.bbb.ccc.195 on
unserved port 139
Dec 14 06:45:35  opsystem: securityalert: tcp from 207.71.92.221:4958 to aaa.bbb.ccc.195 on
unserved port 139
```

Example 4:

History: This is an odd detect because of the 127.0.0.100 source address. It occurred over a couple of days. We have had several RFC 1918 source address probes; so we asked our upstream ISP to block them at their router.

Technique: I believe this is a crafted packet, based on the anomalies in the various fields in the packet.

Intent: The intent is not clear. Using unroutable addresses should not gain any information - unless source routing is used to return to an "owned" machine. This is not a Denial of Service (DoS).

Targeting: This came to our web gateway which is load balanced, but only one address appears.

Analysis: Because this was so odd I set up a tcp trace routine. Fortunately, it lasted for a while and was able to obtain the following information.
This could possibly be an intermittent problem with our router or host, but I don't think so because of the MAC address and the decremented TTL. Other notable features are that the sequence number remained constant for 7 packets then switched to a new number. The source port showed the same pattern. The time to live was 48 seconds/hops (and 248 for the tcp portion in the ip header) - this does not correspond to our machine. Because of internal restrictions I could not traceroute to it to count the hops.
The ICMP message was ICMP Destination unreachable (Bad host) The packet size was a constant 70 bytes. I was able to telnet to port 25 of the mailserver indicated in the packet.

```
Feb 15 09:56:49  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 09:56:49  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 09:56:57  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 09:57:10  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 09:57:32  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 09:58:18  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 09:59:14  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 21:04:30  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 21:04:30  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 21:04:38  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 21:04:50  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 21:05:13  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
```

```
Feb 15 21:05:53  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
Feb 15 21:06:55  opsystem: securityalert: packet denied by local screen: ICMP if=hme1
srcaddr=127.0.0.100 dstaddr=aaa.bbb.ccc.196
```

This continued and I was able to get a tcp trace of it the next day:

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 1 arrived at 15:33:23.53
ETHER:  Packet size = 70 bytes
ETHER:  Destination = MAC:Address,OpSys
ETHER:  Source      = 0:90:b7:21:cc:8,
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 56 bytes
IP:   Identification = 54524
IP:   Flags = 0x0
IP:         .0.. .... = may fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 48 seconds/hops
IP:   Protocol = 1 (ICMP)
IP:   Header checksum = e6d9
IP:   Source address = 127.0.0.100, 127.0.0.100
IP:   Destination address = aaa.bbb.ccc.196, machine1
IP:   No options
IP:
ICMP:  ----- ICMP Header -----
ICMP:
ICMP:  Type = 3 (Destination unreachable)
ICMP:  Code = 1 (Bad host)
ICMP:  Checksum = 23d5
ICMP:
ICMP:  [ subject header follows ]
ICMP:
ICMP:IP:   ----- IP Header -----
ICMP:IP:
ICMP:IP:   Version = 4
ICMP:IP:   Header length = 20 bytes
ICMP:IP:   Type of service = 0x00
ICMP:IP:         xxx. .... = 0 (precedence)
ICMP:IP:         ...0 .... = normal delay
ICMP:IP:         .... 0... = normal throughput
ICMP:IP:         .... .0.. = normal reliability
ICMP:IP:   Total length = 44 bytes
```

```
ICMP:IP:   Identification = 31869
ICMP:IP:   Flags = 0x4
ICMP:IP:        .1.. .... = do not fragment
ICMP:IP:        ..0. .... = last fragment
ICMP:IP:   Fragment offset = 0 bytes
ICMP:IP:   Time to live = 238 seconds/hops
ICMP:IP:   Protocol = 6 (TCP)
ICMP:IP:   Header checksum = 1c92
ICMP:IP:   Source address = aaa.bbb.ccc.196, machine1
ICMP:IP:   Destination address = 271.130.210.154, mail.somestatefair.org
ICMP:IP:   No options
ICMP:IP:
ICMP:TCP:  ----- TCP Header -----
ICMP:TCP:
ICMP:TCP:  Source port = 61059
ICMP:TCP:  Destination port = 25 (SMTP)
ICMP:TCP:  Sequence number = 106554419
ICMP:TCP:  Acknowledgement number = 0
ICMP:TCP:  Data offset = 0 bytes
ICMP:TCP:  Flags = 0x00
ICMP:TCP:        ..0. .... = No urgent pointer
ICMP:TCP:        ...0 .... = No acknowledgement
ICMP:TCP:        .... 0... = No push
ICMP:TCP:        .... .0.. = No reset
ICMP:TCP:        .... ..0. = No Syn
ICMP:TCP:        .... ...0 = No Fin
ICMP:TCP:  Window = 0
ICMP:TCP:  Checksum = 0x1000
ICMP:TCP:  Urgent pointer = 0
ICMP:TCP:  No options
ICMP:TCP:
ICMP:SMTP:  ----- SMTP:   -----
ICMP:SMTP:
ICMP:SMTP:  ""
ICMP:SMTP:


ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 2 arrived at 15:33:23.54
ETHER:  Packet size = 70 bytes
ETHER:  Destination = MAC:Address,OpSys
ETHER:  Source      = 0:90:b7:21:cc:8,
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 56 bytes
```

```
IP:   Identification = 54780
IP:   Flags = 0x0
IP:         .0.. .... = may fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 48 seconds/hops
IP:   Protocol = 1 (ICMP)
IP:   Header checksum = e5d9
IP:   Source address = 127.0.0.100, 127.0.0.100
IP:   Destination address = aaa.bbb.ccc.196, machine1
IP:   No options
IP:
ICMP:  ----- ICMP Header -----
ICMP:
ICMP:  Type = 3 (Destination unreachable)
ICMP:  Code = 1 (Bad host)
ICMP:  Checksum = 23d5
ICMP:
ICMP:  [ subject header follows ]
ICMP:
ICMP:IP:   ----- IP Header -----
ICMP:IP:
ICMP:IP:   Version = 4
ICMP:IP:   Header length = 20 bytes
ICMP:IP:   Type of service = 0x00
ICMP:IP:         xxx. .... = 0 (precedence)
ICMP:IP:         ...0 .... = normal delay
ICMP:IP:         .... 0... = normal throughput
ICMP:IP:         .... .0.. = normal reliability
ICMP:IP:   Total length = 44 bytes
ICMP:IP:   Identification = 31870
ICMP:IP:   Flags = 0x4
ICMP:IP:         .1.. .... = do not fragment
ICMP:IP:         ..0. .... = last fragment
ICMP:IP:   Fragment offset = 0 bytes
ICMP:IP:   Time to live = 238 seconds/hops
ICMP:IP:   Protocol = 6 (TCP)
ICMP:IP:   Header checksum = 1c91
ICMP:IP:   Source address = aaa.bbb.ccc.196, machine1
ICMP:IP:   Destination address = 271.130.210.154, mail.somestatefair.org
ICMP:IP:   No options
ICMP:IP:
ICMP:TCP:  ----- TCP Header -----
ICMP:TCP:
ICMP:TCP:  Source port = 61059
ICMP:TCP:  Destination port = 25 (SMTP)
ICMP:TCP:  Sequence number = 106554419
ICMP:TCP:  Acknowledgement number = 0
ICMP:TCP:  Data offset = 0 bytes
ICMP:TCP:  Flags = 0x00
ICMP:TCP:         ..0. .... = No urgent pointer
ICMP:TCP:         ...0 .... = No acknowledgement
ICMP:TCP:         .... 0... = No push
ICMP:TCP:         .... .0.. = No reset
ICMP:TCP:         .... ..0. = No Syn
```

```
ICMP:TCP:       .... ...0 = No Fin
ICMP:TCP:  Window = 0
ICMP:TCP:  Checksum = 0x1000
ICMP:TCP:  Urgent pointer = 0
ICMP:TCP:  No options
ICMP:TCP:
ICMP:SMTP:  ----- SMTP:   -----
ICMP:SMTP:
ICMP:SMTP:  ""
ICMP:SMTP:


ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 3 arrived at 15:33:33.63
ETHER:  Packet size = 70 bytes
ETHER:  Destination = MAC:Address,OpSys
ETHER:  Source      = 0:90:b7:21:cc:8,
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 56 bytes
IP:   Identification = 57852
IP:   Flags = 0x0
IP:         .0.. .... = may fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 48 seconds/hops
IP:   Protocol = 1 (ICMP)
IP:   Header checksum = d9d9
IP:   Source address = 127.0.0.100, 127.0.0.100
IP:   Destination address = aaa.bbb.ccc.196, machine1
IP:   No options
IP:
ICMP:  ----- ICMP Header -----
ICMP:
ICMP:  Type = 3 (Destination unreachable)
ICMP:  Code = 1 (Bad host)
ICMP:  Checksum = 23d5
ICMP:
ICMP:  [ subject header follows ]
ICMP:
ICMP:IP:   ----- IP Header -----
ICMP:IP:
ICMP:IP:   Version = 4
ICMP:IP:   Header length = 20 bytes
ICMP:IP:   Type of service = 0x00
```

```
ICMP:IP:        xxx. .... = 0 (precedence)
ICMP:IP:        ...0 .... = normal delay
ICMP:IP:        .... 0... = normal throughput
ICMP:IP:        .... .0.. = normal reliability
ICMP:IP:   Total length = 44 bytes
ICMP:IP:   Identification = 31871
ICMP:IP:   Flags = 0x4
ICMP:IP:        .1.. .... = do not fragment
ICMP:IP:        ..0. .... = last fragment
ICMP:IP:   Fragment offset = 0 bytes
ICMP:IP:   Time to live = 238 seconds/hops
ICMP:IP:   Protocol = 6 (TCP)
ICMP:IP:   Header checksum = 1c90
ICMP:IP:   Source address = aaa.bbb.ccc.196, machine1
ICMP:IP:   Destination address = 271.130.210.154, mail.somestatefair.org
ICMP:IP:   No options
ICMP:IP:
ICMP:TCP:  ----- TCP Header -----
ICMP:TCP:
ICMP:TCP:  Source port = 61059
ICMP:TCP:  Destination port = 25 (SMTP)
ICMP:TCP:  Sequence number = 106554419
ICMP:TCP:  Acknowledgement number = 0
ICMP:TCP:  Data offset = 0 bytes
ICMP:TCP:  Flags = 0x00
ICMP:TCP:        ..0. .... = No urgent pointer
ICMP:TCP:        ...0 .... = No acknowledgement
ICMP:TCP:        .... 0... = No push
ICMP:TCP:        .... .0.. = No reset
ICMP:TCP:        .... ..0. = No Syn
ICMP:TCP:        .... ...0 = No Fin
ICMP:TCP:  Window = 0
ICMP:TCP:  Checksum = 0x1000
ICMP:TCP:  Urgent pointer = 0
ICMP:TCP:  No options
ICMP:TCP:
ICMP:SMTP:  ----- SMTP:   -----
ICMP:SMTP:
ICMP:SMTP:  ""
ICMP:SMTP:


ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 4 arrived at 15:33:40.70
ETHER:  Packet size = 70 bytes
ETHER:  Destination = MAC:Address,OpSys
ETHER:  Source      = 0:90:b7:21:cc:8,
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
```

```
IP:       xxx. .... = 0 (precedence)
IP:       ...0 .... = normal delay
IP:       .... 0... = normal throughput
IP:       .... .0.. = normal reliability
IP:   Total length = 56 bytes
IP:   Identification = 60668
IP:   Flags = 0x0
IP:       .0.. .... = may fragment
IP:       ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 48 seconds/hops
IP:   Protocol = 1 (ICMP)
IP:   Header checksum = ced9
IP:   Source address = 127.0.0.100, 127.0.0.100
IP:   Destination address = aaa.bbb.ccc.196, machine1
IP:   No options
IP:
ICMP:  ----- ICMP Header -----
ICMP:
ICMP:  Type = 3 (Destination unreachable)
ICMP:  Code = 1 (Bad host)
ICMP:  Checksum = 23d5
ICMP:
ICMP:  [ subject header follows ]
ICMP:
ICMP:IP:   ----- IP Header -----
ICMP:IP:
ICMP:IP:   Version = 4
ICMP:IP:   Header length = 20 bytes
ICMP:IP:   Type of service = 0x00
ICMP:IP:       xxx. .... = 0 (precedence)
ICMP:IP:       ...0 .... = normal delay
ICMP:IP:       .... 0... = normal throughput
ICMP:IP:       .... .0.. = normal reliability
ICMP:IP:   Total length = 44 bytes
ICMP:IP:   Identification = 31872
ICMP:IP:   Flags = 0x4
ICMP:IP:       .1.. .... = do not fragment
ICMP:IP:       ..0. .... = last fragment
ICMP:IP:   Fragment offset = 0 bytes
ICMP:IP:   Time to live = 238 seconds/hops
ICMP:IP:   Protocol = 6 (TCP)
ICMP:IP:   Header checksum = 1c8f
ICMP:IP:   Source address = aaa.bbb.ccc.196, machine1
ICMP:IP:   Destination address = 271.130.210.154, mail.somestatefair.org
ICMP:IP:   No options
ICMP:IP:
ICMP:TCP:  ----- TCP Header -----
ICMP:TCP:
ICMP:TCP:  Source port = 61059
ICMP:TCP:  Destination port = 25 (SMTP)
ICMP:TCP:  Sequence number = 106554419
ICMP:TCP:  Acknowledgement number = 0
ICMP:TCP:  Data offset = 0 bytes
ICMP:TCP:  Flags = 0x00
```

```
ICMP:TCP:       ..0. .... = No urgent pointer
ICMP:TCP:       ...0 .... = No acknowledgement
ICMP:TCP:       .... 0... = No push
ICMP:TCP:       .... .0.. = No reset
ICMP:TCP:       .... ..0. = No Syn
ICMP:TCP:       .... ...0 = No Fin
ICMP:TCP:  Window = 0
ICMP:TCP:  Checksum = 0x1000
ICMP:TCP:  Urgent pointer = 0
ICMP:TCP:  No options
ICMP:TCP:
ICMP:SMTP:  ----- SMTP:   -----
ICMP:SMTP:
ICMP:SMTP:  ""
ICMP:SMTP:


ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 5 arrived at 15:34:7.89
ETHER:  Packet size = 70 bytes
ETHER:  Destination = MAC:Address,OpSys
ETHER:  Source      = 0:90:b7:21:cc:8,
ETHER:  Ethertype = 0800 (IP)
ETHER:
IP:   ----- IP Header -----
IP:
IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:         xxx. .... = 0 (precedence)
IP:         ...0 .... = normal delay
IP:         .... 0... = normal throughput
IP:         .... .0.. = normal reliability
IP:   Total length = 56 bytes
IP:   Identification = 7933
IP:   Flags = 0x0
IP:         .0.. .... = may fragment
IP:         ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 48 seconds/hops
IP:   Protocol = 1 (ICMP)
IP:   Header checksum = 9cd9
IP:   Source address = 127.0.0.100, 127.0.0.100
IP:   Destination address = aaa.bbb.ccc.196, machine1
IP:   No options
IP:
ICMP:  ----- ICMP Header -----
ICMP:
ICMP:  Type = 3 (Destination unreachable)
ICMP:  Code = 1 (Bad host)
ICMP:  Checksum = 23d5
ICMP:
ICMP:  [ subject header follows ]
ICMP:
```

```
ICMP:IP:   ----- IP Header -----
ICMP:IP:
ICMP:IP:   Version = 4
ICMP:IP:   Header length = 20 bytes
ICMP:IP:   Type of service = 0x00
ICMP:IP:         xxx. .... = 0 (precedence)
ICMP:IP:         ...0 .... = normal delay
ICMP:IP:         .... 0... = normal throughput
ICMP:IP:         .... .0.. = normal reliability
ICMP:IP:   Total length = 44 bytes
ICMP:IP:   Identification = 31873
ICMP:IP:   Flags = 0x4
ICMP:IP:         .1.. .... = do not fragment
ICMP:IP:         ..0. .... = last fragment
ICMP:IP:   Fragment offset = 0 bytes
ICMP:IP:   Time to live = 238 seconds/hops
ICMP:IP:   Protocol = 6 (TCP)
ICMP:IP:   Header checksum = 1c8e
ICMP:IP:   Source address = aaa.bbb.ccc.196, machine1
ICMP:IP:   Destination address = 271.130.210.154, mail.somestatefair.org
ICMP:IP:   No options
ICMP:IP:
ICMP:TCP:  ----- TCP Header -----
ICMP:TCP:
ICMP:TCP:  Source port = 61059
ICMP:TCP:  Destination port = 25 (SMTP)
ICMP:TCP:  Sequence number = 106554419
ICMP:TCP:  Acknowledgement number = 0
ICMP:TCP:  Data offset = 0 bytes
ICMP:TCP:  Flags = 0x00
ICMP:TCP:        ..0. .... = No urgent pointer
ICMP:TCP:        ...0 .... = No acknowledgement
ICMP:TCP:        .... 0... = No push
ICMP:TCP:        .... .0.. = No reset
ICMP:TCP:        .... ..0. = No Syn
ICMP:TCP:        .... ...0 = No Fin
ICMP:TCP:  Window = 0
ICMP:TCP:  Checksum = 0x1000
ICMP:TCP:  Urgent pointer = 0
ICMP:TCP:  No options
ICMP:TCP:
ICMP:SMTP:  ----- SMTP:  -----
ICMP:SMTP:
ICMP:SMTP:  ""
ICMP:SMTP:
```

And so on for 70 packets…

Example 5:

History: These packets continued for a while before we tracked it down.

Technique: This did not make sense, it took place day and night, always to the same machine and the same port - 1500, which is VLSI License Manager according to IANA port assignments.

Intent: I could not figure out what someone was trying to accomplish hitting the same machine and port day after day, but not hard enough to be a denial of service.

Targeting: This was always to the same port on the same host.

Analysis: I checked around our system because it was hitting the internal NIC of our firewall, then our router for packet forwarding, both of which were denied by the firewall and router rules. We tracked it to a test machine with multiple NIC's. A routine was misconfigured and this was corrected following our inquiry. We have met the enemy and he is us.

```
Dec  1 16:34:37  opsystem: securityalert: tcp from 172.1X2.834.66:33142 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:34:37  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:34:41  opsystem: securityalert: tcp from 172.1X2.834.66:33142 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:34:41  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:34:47  opsystem: securityalert: tcp from 172.1X2.834.66:33142 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:34:47  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:35:00  opsystem: securityalert: tcp from 172.1X2.834.66:33142 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:35:00  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:35:26  opsystem: securityalert: tcp from 172.1X2.834.66:33142 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:35:26  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:36:17  opsystem: securityalert: tcp from 172.1X2.834.66:33142 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:36:17  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:57:58  opsystem: securityalert: tcp from 172.1X2.834.66:33144 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:57:58  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:58:02  opsystem: securityalert: tcp from 172.1X2.834.66:33144 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:58:02  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:58:08  opsystem: securityalert: tcp from 172.1X2.834.66:33144 to 152.11b.q??.62 on
unserved port 1500
```

```
Dec  1 16:58:08  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:58:21  opsystem: securityalert: tcp from 172.1X2.834.66:33144 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:58:21  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:58:47  opsystem: securityalert: tcp from 172.1X2.834.66:33144 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:58:47  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
Dec  1 16:59:38  opsystem: securityalert: tcp from 172.1X2.834.66:33144 to 152.11b.q??.62 on
unserved port 1500
Dec  1 16:59:38  opsystem: securityalert: packet forwarding denied: ICMP if=le0
srcaddr=152.171.321.1 dstaddr=152.11b.q??.62
```

Example 6:

History: I received this from one of our sister sites during the "Millenium" period.

Technique: An automated scan based on the timestamps.

Intent: Looking for vulnerable services on the host, and possibly others based on the missing packets.

Targeting: Source is targeting klogin, netbios-ssn, ScheduleAgent (a trojan), socks, sunrpc, xwindows, kshell, finger, imap, telnet, and POP Mail services.

Analysis: This is a probe specifically looking for vulnerable ports. Another question might be what happened to the packets 1816 through 1819? Since it came from Buenos Aires, we went on high alert for any further developments.

```
Jan  6 20:56:42  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1807 to 132.200.32.33
on unserved port 543
Jan  6 20:56:42  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1809 to 132.200.32.33
on unserved port 139
Jan  6 20:56:42  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1811 to 132.200.32.33
on unserved port 6667
Jan  6 20:56:42  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1812 to 132.200.32.33
on unserved port 1080
Jan  6 20:56:42  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1813 to 132.200.32.33
on unserved port 111
Jan  6 20:56:42  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1814 to 132.200.32.33
on unserved port 6000
Jan  6 20:56:42  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1815 to 132.200.32.33
on unserved port 544
Jan  6 20:56:43  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1820 to 132.200.32.33
on unserved port 79
Jan  6 20:56:43  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1821 to 132.200.32.33
on unserved port 143
Jan  6 20:56:43  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1822 to 132.200.32.33
on unserved port 23
Jan  6 20:56:43  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1823 to 132.200.32.33
on unserved port 110
Jan  6 20:56:43  opsystem: securityalert: tcp if=qfe0 from 209.13.235.7:1824 to 132.200.32.33
on unserved port 109
```

Example 7:

History: This seems like a one-time scan, no other history from this source. SecuritiTeam lists the Remote vulnerability in POP2 Daemon as being The POP2 daemon component of imap version 4.4 and earlier (including earlier RedHat releases), is vulnerable to a remote attack that enables users to gain shell access as user "nobody". There was also an old pop2 buffer overflow listed on the ISOC website that could be a problem as well.

Technique: It is probably a script based on the timestamps scanning hosts for POP-2 Mail.

Intent: Find POP-2 mail servers.

Targeting: Specific to port 109.

Analysis: This came from the University of Southern California, so is probably a student. Although with later developments it could possibly have been related to the DDoS which happened later since many were based on compromised University machines.

```
Feb 21 13:21:19  opsystem: securityalert: tcp from 128.125.52.50:9175 to ccc.bbb.aaa.194 on
unserved port 109
Feb 21 13:21:19  opsystem: securityalert: tcp from 128.125.52.50:9190 to ccc.bbb.aaa.195 on
unserved port 109
Feb 21 13:21:19  opsystem: securityalert: tcp from 128.125.52.50:9260 to ccc.bbb.aaa.196 on
unserved port 109
```

Example 8:

History: This is a scan interleaved between two hosts on our system, looking for trojans.

Technique: Automated scan of specific trojan ports on these machines lasting only about a minute.

Intent: This specifically targets trojan ports, looking for compromised systems. I also noticed an attempt to port 1999, which is the Cisco login access attempt, as well as a trojan.

Targeting: This person seems to be trying to scan for a number of different trojans BackOrifice, WinCrash, PhaseZero/StealthSpy, Millenium... This is based on the list of ports used by trojans at www.simovits.com.

Analysis: This scanner looks as though it is specifically designed to search for trojans. When I related that to our other sites, one wrote back seemingly in disbelief that such a scanner existed. After about a 15 minute search on the internet, I had three that claimed to do exactly that and stopped there. Like Stephen said - they share.
This occurred at about about 3 am our time but since there is a 14 hour time difference in Japan it would be about 5pm local time - school's out.

```
Nov 22 03:09:14  opsystem: securityalert: udp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 31337
Nov 22 03:09:21  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 5742
Nov 22 03:09:22  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 5742
Nov 22 03:09:33  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 2583
Nov 22 03:09:59  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 2140
Nov 22 03:10:09  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1001
Nov 22 03:10:10  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1001
Nov 22 03:10:14  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 30303
Nov 22 03:10:26  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 21554
Nov 22 03:10:28  opsystem: securityalert: udp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 31337
Nov 22 03:09:14  opsystem: securityalert: udp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 31337
Nov 22 03:09:21  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 5742
Nov 22 03:10:35  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 5742
Nov 22 03:09:22  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 5742
Nov 22 03:09:33  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 2583
```

```
Nov 22 03:10:47  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 2583
Nov 22 03:11:14  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 2140
Nov 22 03:09:59  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 2140
Nov 22 03:11:23  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 1001
Nov 22 03:10:09  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1001
Nov 22 03:10:10  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1001
Nov 22 03:11:28  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 30303
Nov 22 03:10:14  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 30303
Nov 22 03:11:40  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 21554
Nov 22 03:10:26  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 21554
Nov 22 03:10:26  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 21554
Nov 22 03:11:45  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 20001
Nov 22 03:10:31  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 20001
Nov 22 03:10:32  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 20001
Nov 22 03:10:37  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 31
Nov 22 03:11:51  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 31
Nov 22 03:11:54  opsystem: securityalert: udp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 2801
Nov 22 03:10:40  opsystem: securityalert: udp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 2801
Nov 22 03:10:45  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1999
Nov 22 03:11:59  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 1999
Nov 22 03:12:03  opsystem: securityalert: udp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 31336
Nov 22 03:10:49  opsystem: securityalert: udp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 31336
Nov 22 03:10:53  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 23456
Nov 22 03:12:07  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 23456
Nov 22 03:12:13  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 6969
Nov 22 03:10:59  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 6969
Nov 22 03:12:19  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 20034
```

```
Nov 22 03:11:05  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 20034
Nov 22 03:11:11  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 555
Nov 22 03:12:25  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 555
Nov 22 03:12:31  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 1509
Nov 22 03:11:17  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1509
Nov 22 03:12:36  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 11000
Nov 22 03:11:22  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 11000
Nov 22 03:11:23  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 11000
Nov 22 03:12:42  opsystem: securityalert: tcp if=hme1 from 210.149.71.110:1195 to
nnn.xxx.118.035 on unserved port 1514
Nov 22 03:11:28  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1514
Nov 22 03:11:29  opsystem: securityalert: tcp from 210.149.71.110:1194 to nnn.xxx.118.034 on
unserved port 1514
```

Example 9:

History: A recent port scan.

Technique: This is a scan that looks for vulnerable ports.

Intent: Once ports are found with specific vulnerabilities, then the attacker can use those to either compromise or deny service to that machine. If compromised, the machine can be used to attack other machines on the network, either internally or back out on the internet.

Targeting: Port 7 - echo, 110 - POP Mail, 37 - time, 143 - IMAP, 161 - SNMP, and 80 - HTTP.

Analysis: This probe is looking for open ports that have known vulnerabilities. This was the only probe noted, so since the firewall dropped and logged the accesses, the prober probably went on to an easier target.

Apr 3 15:26:41 opsystem: securityalert: tcp from 208.184.134.95:3402 to nnn.xxx.118.034 on unserved port 7
Apr 3 15:26:42 opsystem: securityalert: tcp from 208.184.134.95:3402 to nnn.xxx.118.034 on unserved port 7
Apr 3 15:26:42 opsystem: securityalert: tcp from 208.184.134.95:3402 to nnn.xxx.118.034 on unserved port 7
Apr 3 15:26:43 opsystem: securityalert: tcp from 208.184.134.95:3411 to nnn.xxx.118.034 on unserved port 110
Apr 3 15:26:43 opsystem: securityalert: tcp from 208.184.134.95:3402 to nnn.xxx.118.034 on unserved port 7
Apr 3 15:26:43 opsystem: securityalert: tcp from 208.184.134.95:3411 to nnn.xxx.118.034 on unserved port 110
Apr 3 15:26:44 opsystem: securityalert: tcp from 208.184.134.95:3411 to nnn.xxx.118.034 on unserved port 110
Apr 3 15:26:44 opsystem: securityalert: tcp from 208.184.134.95:3419 to nnn.xxx.118.034 on unserved port 37
Apr 3 15:26:44 opsystem: securityalert: packet denied by local screen: TCP if=hme0 srcaddr=208.184.134.95 srcport=3422 dstaddr=nnn.xxx.118.034 dstport=80
Apr 3 15:26:45 opsystem: securityalert: tcp from 208.184.134.95:3411 to nnn.xxx.118.034 on unserved port 110
Apr 3 15:26:45 opsystem: securityalert: tcp from 208.184.134.95:3419 to nnn.xxx.118.034 on unserved port 37
Apr 3 15:26:45 opsystem: securityalert: tcp from 208.184.134.95:3424 to nnn.xxx.118.034 on unserved port 143
Apr 3 15:26:45 opsystem: securityalert: tcp from 208.184.134.95:3419 to nnn.xxx.118.034 on unserved port 37
Apr 3 15:26:46 opsystem: securityalert: tcp from 208.184.134.95:3424 to nnn.xxx.118.034 on unserved port 143
Apr 3 15:26:46 opsystem: securityalert: tcp from 208.184.134.95:3419 to nnn.xxx.118.034 on unserved port 37
Apr 3 15:26:46 opsystem: securityalert: udp from 208.184.134.95:3426 to nnn.xxx.118.034 on unserved port 161
Apr 3 15:26:46 opsystem: securityalert: tcp from 208.184.134.95:3424 to nnn.xxx.118.034 on unserved port 143
Apr 3 15:26:47 opsystem: securityalert: tcp from 208.184.134.95:3424 to nnn.xxx.118.034 on unserved port 143
Apr 3 15:26:48 opsystem: securityalert: packet denied by local screen: TCP if=hme0 srcaddr=208.184.134.95 srcport=3422 dstaddr=nnn.xxx.118.034 dstport=80

Example 10:

History: This was recently picked up because of the source / destination anomaly, and the destination port is listed as a trojan port.

Technique: An automated probe, based on the close timestamps, the destination port is 3024, which could be the WinCrash trojan according to www.simovits.com/nyheter9902.html.

Intent: This could be looking for a machine compromised with the WinCrash server installed.

Targeting: Port 3024.

Analysis: This is either a probe, or a misconfigured application. It is questionable only because it went against the same machine and port 24 times in 7 seconds. On the other hand, I know of no reason why the source's type of business (an engine and tranny shop per ARIN) located in mid-USA would be contacting us for any legitimate reason. No further detects, but this is on the "open" list.

According to a user manual I located, WinCrash Probe is a remote control program written by M@niac_Teen and Terminal Crasher at hallofjustice.org. It has many of the capabilities of BackOrifice using a similar client server connection.

```
Apr 12 08:21:06  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:06  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:07  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:07  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:07  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:07  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:08  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:08  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:08  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:08  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:09  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:09  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:10  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:10  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:10  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
```

```
Apr 12 08:21:10  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:11  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:11  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:11  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:12  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:12  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:12  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:12  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
Apr 12 08:21:13  opsystem: securityalert: udp from 12.633.234.2:3024 to ccc.bbb.aaa.214 on
unserved port 3024
```