



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Network Monitoring and Threat Detection In-Depth (Security 503)"  
at <http://www.giac.org/registration/gcia>

\*\*\* Northcutt, good work, solid process, shows what is possible with a firewall. 76 \*

## Practical for GIAC Certified Intrusion Analyst Certification

By Jeff Towry

April 21, 2000

### Detect 1 –

Apr 17 17:18:46 6560	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:46 6563	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:46 6564	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:46 6565	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:46 6566	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:46 6567	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:59 6560	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:59 6563	tcp	afiaibt.com	https	p.q.50.251
Apr 17 17:18:59 6564	tcp	afiaibt.com	https	p.q.50.251

**Active Targeting** – Yes, these packets are being sent to the outside address of our firewall.

**Intent** - 216.61.102.52 ARC Information Assurance Institute is doing a port scan on this address.

**Technique** – This attack seems to be script driven since the time between the packets is very small and the destination ports are wrapping and starting over. My first thought was someone went to a server that is constantly updating the browser screen with new information. The only thing odd about this is the fact that the destination port is wrapping and normally this increments continuously. So this may be a DOS attack against the firewall since it is targeting the outside interface of it.

**Severity** – Low since these packets were not getting through the firewall. If it continues then we will add this address to the access list on the outside router to keep the workload of processing the packet and logging it off the firewall.

## Detect 2 –

Apr 12 04:43:24 buster1 BUSTED: 04:43:24 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.1 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:25 buster1 BUSTED: 04:43:25 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.1 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:27 buster1 BUSTED: 04:43:27 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.1 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:33 buster1 BUSTED: 04:43:33 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.2 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:34 buster1 BUSTED: 04:43:34 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.2 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:36 buster1 BUSTED: 04:43:36 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.2 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:42 buster1 BUSTED: 04:43:42 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.3 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:44 buster1 BUSTED: 04:43:44 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.3 137 No\_DNS\_Name No\_Flags netbios-ns udp  
Apr 12 04:43:45 buster1 BUSTED: 04:43:45 207.214.144.126 64558 adsl-207-214-144-126.dsl.snfc21.pacbell.net p.q.60.3 137 No\_DNS\_Name No\_Flags netbios-ns udp

**Active Targeting** – Yes, these packets are being sent to an internal subnet behind the firewall..

**Intent** – To detect Windows based systems on this subnet.

**Technique** – This appears to be a Null scan of an internal subnet. The packets come in groups of 3 from the same source port of 64558 with no flags set. The only port it probes is 137 which is the Netbios name service.

**History** – No other activity was seen over the day. This is coming from a ISP customer The Source Group in San Francisco.

**Severity** – Low since these packets were not getting through the outside router. The outside router blocks all udp below 1023 coming in. A check of the firewall logs for the same time period showed no activity from this address.

## Detect 3 –

Apr 12 00:04:05 buster1 BUSTED: 00:03:54 202.154.4.145 2991 No\_DNS\_Name p.q.237.99 80 No\_DNS\_Name S www-http tcp  
Apr 12 00:04:05 buster1 BUSTED: 00:03:57 202.154.4.145 2991 No\_DNS\_Name p.q.237.99 80 No\_DNS\_Name S www-http tcp

Apr 12 00:04:05 buster1 BUSTED: 00:04:03 202.154.4.145 2991 No\_DNS\_Name  
 p.q.237.99 80 No\_DNS\_Name S www-http tcp  
 Apr 12 00:04:15 buster1 BUSTED: 00:04:15 202.154.4.145 2991 No\_DNS\_Name  
 p.q.237.99 80 No\_DNS\_Name S www-http tcp  
 Apr 12 00:04:39 buster1 BUSTED: 00:04:39 202.154.4.145 3027 No\_DNS\_Name  
 p.q.237.99 8080 No\_DNS\_Name S 8080 tcp  
 Apr 12 00:04:42 buster1 BUSTED: 00:04:42 202.154.4.145 3027 No\_DNS\_Name  
 p.q.237.99 8080 No\_DNS\_Name S 8080 tcp  
 Apr 12 00:04:48 buster1 BUSTED: 00:04:48 202.154.4.145 3027 No\_DNS\_Name  
 p.q.237.99 8080 No\_DNS\_Name S 8080 tcp  
 Apr 12 00:05:00 buster1 BUSTED: 00:05:00 202.154.4.145 3027 No\_DNS\_Name  
 p.q.237.99 8080 No\_DNS\_Name S 8080 tcp  
 Apr 12 00:05:24 buster1 BUSTED: 00:05:24 202.154.4.145 3071 No\_DNS\_Name  
 p.q.237.99 3128 No\_DNS\_Name S 3128 tcp  
 Apr 12 00:05:27 buster1 BUSTED: 00:05:27 202.154.4.145 3071 No\_DNS\_Name  
 p.q.237.99 3128 No\_DNS\_Name S 3128 tcp  
 Apr 12 00:05:33 buster1 BUSTED: 00:05:33 202.154.4.145 3071 No\_DNS\_Name  
 p.q.237.99 3128 No\_DNS\_Name S 3128 tcp  
 Apr 12 00:05:45 buster1 BUSTED: 00:05:45 202.154.4.145 3071 No\_DNS\_Name  
 p.q.237.99 3128 No\_DNS\_Name S 3128 tcp

**Active Targeting** – Yes, these packets are being sent to an address behind the firewall.

**Intent** – This PC's have been infected with the Ring 0 trojan and are looking for the existence of proxy servers.

**Technique** – This is the standard Ring 0 probe looking on ports 80, 8080, 3128.

**History** – We see this all day long from different networks to multiple addresses.

**Severity** – Low since these packets were not getting through the outside router. .

**Detect 4** –

Apr 7 06:45:51 buster1 BUSTED: 06:44:31 171.209.75.173 1843 No\_DNS\_Name  
 p.q.50.1 53 ns1.my.dom S domain tcp  
 Apr 7 06:47:11 buster1 BUSTED: 06:44:34 171.209.75.173 1843 No\_DNS\_Name  
 p.q.50.1 53 ns1.my.dom S domain tcp  
 Apr 7 06:50:14 buster1 BUSTED: 06:48:53 171.209.75.173 2466 No\_DNS\_Name  
 p.q.50.2 53 ns2.my.dom S domain tcp  
 Apr 7 06:51:34 buster1 BUSTED: 06:48:56 171.209.75.173 2466 No\_DNS\_Name  
 p.q.50.2 53 ns2.my.dom S domain tcp  
 Apr 7 06:52:54 buster1 BUSTED: 06:50:14 171.209.75.173 2647 No\_DNS\_Name  
 p.q.50.1 53 ns1.my.dom S domain tcp

Apr 7 06:58:51 buster1 BUSTED: 06:57:31 171.209.75.173 3762 No\_DNS\_Name  
p.q.50.1 53 ns1.my.dom S domain tcp  
Apr 7 07:00:13 buster1 BUSTED: 06:58:53 171.209.75.173 3950 No\_DNS\_Name  
p.q.50.1 53 ns1.my.dom S domain tcp  
Apr 7 07:01:33 buster1 BUSTED: 06:58:56 171.209.75.173 3950 No\_DNS\_Name  
p.q.50.1 53 ns1.my.dom S domain tcp

**Active Targeting** – Yes.

**Intent** – Trying to pull zones.

**Technique** – Trying to initiate a zone transfer every 1-2 minutes.

**History** – These addresses mapped to the AOL domain. So these are probably just dialup users.

**Severity** – Low since these packets were not getting through outside router. The router is setup to only allow from our secondaries.

**Detect 5** –

Apr 12 08:05:16 buster1 BUSTED: 08:05:16 156.46.8.135 1348 mars.capital-  
internet.net p.q.50.251 113 host.my.dom S auth tcp  
Apr 12 08:05:19 buster1 BUSTED: 08:05:19 156.46.8.135 1348 mars.capital-  
internet.net p.q.50.251 113 host.my.dom S auth tcp  
Apr 12 08:05:25 buster1 BUSTED: 08:05:25 156.46.8.135 1348 mars.capital-  
internet.net p.q.50.251 113 host.my.dom S auth tcp

**Active Targeting** – Yes.

**Intent** – This series of packets was doing a scan to see if port 113 was open on the firewall.

**Technique** – This appears to be automated with a backoff timer that doubles.

**History** – No other activity was seen over the day. This is coming from a ISP customer in Milwaukee, WI.

**Severity** – Low since these packets were not getting through the router.

**Detect 6** –

Mar 31 18:52:28 buster1 BUSTED: 18:52:19 24.16.51.74 No\_Src\_Port c1054142-a.smateo1.sfba.home.com 131.63.0.3 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping  
Mar 31 18:52:28 buster1 BUSTED: 18:52:19 24.16.51.74 No\_Src\_Port c1054142-a.smateo1.sfba.home.com 131.63.0.4 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping  
Mar 31 18:52:28 buster1 BUSTED: 18:52:19 24.16.51.74 No\_Src\_Port c1054142-a.smateo1.sfba.home.com 131.63.0.5 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping  
Mar 31 18:52:28 buster1 BUSTED: 18:52:19 24.16.51.74 No\_Src\_Port c1054142-a.smateo1.sfba.home.com 131.63.1.3 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping  
Mar 31 18:52:28 buster1 BUSTED: 18:52:19 24.16.51.74 No\_Src\_Port c1054142-a.smateo1.sfba.home.com 131.63.1.4 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping  
Mar 31 18:52:28 buster1 BUSTED: 18:52:19 24.16.51.74 No\_Src\_Port c1054142-a.smateo1.sfba.home.com 131.63.1.5 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping

**Active Targeting** – Yes.

**Intent** – This host appears to be trying to determine which hosts are alive on our network.

**Technique** – Fast ping probe.

**History** – More activity was seen over the next few days. The activity ceased finally with no other traffic from this network coming to ours.

**Severity** – Low since these packets were not getting through the router and we silently discard them.

**Detect 7** –

Apr 12 18:06:53 buster1 BUSTED: 18:06:32 193.216.116.247 No\_Src\_Port mp-116-247.daxnet.no p.q.0.255 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping  
Apr 12 18:06:53 buster1 BUSTED: 18:06:32 193.216.116.247 No\_Src\_Port mp-116-247.daxnet.no p.q.255.0 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping  
Apr 12 18:06:53 buster1 BUSTED: 18:06:32 193.216.116.247 No\_Src\_Port mp-116-247.daxnet.no p.q.255.255 No\_Dst\_Port No\_DNS\_Name No\_Flags Echo\_Request ping

**Active Targeting** – Yes.

**Intent** – Network mapping but to the broadcast addresses on our networks.

**Technique** – Fast ping probe to the broadcast addresses.

**History** – No other activity was seen over the day from this network address space.

**Severity** – Low since these packets were not getting through the router and we silently discard them.

**Detect 8** –

Apr 12 07:56:19 buster1 BUSTED: 07:56:18 206.137.100.2 21130  
netva01.wangfed.com p.q.139.27 1601 No\_DNS\_Name S 1601 tcp  
Apr 12 08:10:52 buster1 BUSTED: 08:10:52 206.137.100.2 25956  
netva01.wangfed.com p.q.139.27 1601 No\_DNS\_Name S 1601 tcp  
Apr 12 08:21:51 buster1 BUSTED: 08:21:51 206.137.100.2 30193  
netva01.wangfed.com p.q.139.27 1601 No\_DNS\_Name S 1601 tcp

**Active Targeting** – Yes.

**Intent** – Someone trying to connect to a sql server on the host.

**History**– We get a lot of traffic from wangfed.com so we went to firewall logs and found this to be valid traffic.

**Severity** – Low since these packets were going to a host that was open for testing by these contractors.

**Detect 9** –

10:37:45.931756 p.q.244.65.3996 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.931891 p.q.244.65.3996 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.936792 p.q.244.65.5599 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.936973 p.q.244.65.5599 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.943580 p.q.244.65.5600 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.943729 p.q.244.65.5600 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.948406 p.q.244.65.5601 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.948604 p.q.244.65.5601 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.953926 p.q.244.65.5603 > p.q.242.4.161: C=AFLAN  
GetRequest(18) [|snmp]  
10:37:45.954050 p.q.244.65.5603 > p.q.242.4.161: C=AFLAN

GetRequest (18) [|snmp]

**Active Targeting** – Yes.

**Intent** – Initially the thought was we had found someone with too much free time on their hands and had downloaded some of the DOS tools off the web.

**Technique** – DOS attack on one of our internal routers.

**History** – These packets were picked up after someone noticed that SNMP Get Request counters were significantly higher for this one router. It turned out to be misconfigured HPOV software on a test machine.

**Severity** – Low since these packets were not getting outside the core of the network and going to the outside of the network.

**Detect 10** –

```
04:30:37.784998 p.q.244.179 > p.q.235.172: (frag 15770:1480@53280+)
04:30:37.786230 p.q.244.179 > p.q.235.172: (frag 15770:1480@54760+)
04:30:37.787461 p.q.244.179 > p.q.235.172: (frag 15770:1480@56240+)
04:30:37.788694 p.q.244.179 > p.q.235.172: (frag 15770:1480@57720+)
04:30:37.789923 p.q.244.179 > p.q.235.172: (frag 15770:1480@59200+)
04:30:37.791161 p.q.244.179 > p.q.235.172: (frag 15770:1480@60680+)
04:30:37.792388 p.q.244.179 > p.q.235.172: (frag 15770:1480@62160+)
04:30:37.793622 p.q.244.179 > p.q.235.172: (frag 15770:1480@63640+)
04:30:37.793964 p.q.244.179 > p.q.235.172: (frag 15770:546@65120)
```

**Active Targeting** – Yes.

**Intent** – Denial of service attack from the inside.

**Technique** – Ping of death.

**History** – Upon researching the attack found it was the PC Security shop was doing scans of the network to find people that were reloading their own PC's and not putting the service packs back on with the latest security fixes.

**Severity** – Low since it was a controlled test and was being run after hours.