



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
"Intrusion Detection In-Depth (Security 503)"
at <http://www.giac.org/registration/gcia>

SANS Intrusion Detection Practical Exam
San Jose, May, 2000

John M. Dietrich
June 15, 2000

Detect # 1

672418	06/15/00	18:20:36	n allow	out	eth1	48	tcp	20	128
10.6.1.161		207.71.92.193	1065	443			syn (HTTPS)		
672448	06/15/00	18:20:50	n allow	out	eth1	48	tcp	20	128
10.6.1.161		207.71.92.193	1066	80			syn (HTTP)		
672518	06/15/00	18:20:50	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2155	21			syn (FTP)		
672658	06/15/00	18:20:54	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2155	21			syn (FTP)		
672738	06/15/00	18:20:59	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2155	21			syn FTP)		
672818	06/15/00	18:21:11	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2155	21			syn (FTP)		
673068	06/15/00	18:21:35	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2307	23			syn (telnet)		
673108	06/15/00	18:21:38	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2307	23			syn (telnet)		
673238	06/15/00	18:21:44	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2307	23			syn (telnet)		
673408	06/15/00	18:21:56	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2307	23			syn (telnet)		
673638	06/15/00	18:22:20	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2450	25			syn (default)		
673668	06/15/00	18:22:23	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2450	25			syn (default)		
673708	06/15/00	18:22:29	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2450	25			syn (default)		
673738	06/15/00	18:22:41	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2450	25			syn (default)		
673878	06/15/00	18:23:05	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2603	79			syn (default)		
673958	06/15/00	18:23:08	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2603	79			syn (default)		
674078	06/15/00	18:23:14	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2603	79			syn (default)		
674118	06/15/00	18:23:26	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2603	79			syn (default)		
674248	06/15/00	18:23:50	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2744	80			syn (HTTP)		
674278	06/15/00	18:23:53	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2744	80			syn (HTTP)		
674348	06/15/00	18:23:59	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2744	80			syn (HTTP)		
674508	06/15/00	18:24:11	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2744	80			syn (HTTP)		
674588	06/15/00	18:24:36	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2858	110			syn (default)		
674618	06/15/00	18:24:38	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2858	110			syn (default)		
674658	06/15/00	18:24:44	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2858	110			syn (default)		
674728	06/15/00	18:24:57	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	2858	110			syn (default)		
674928	06/15/00	18:25:21	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	3004	113			syn (default)		
674958	06/15/00	18:25:24	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	3004	113			syn (default)		
674998	06/15/00	18:25:30	n deny	in	eth0	44	tcp	20	117
207.71.92.221		38.150.x.x	3004	113			syn (default)		

675088	06/15/00	18:25:42	n deny	in	eth0	44	tcp	20	117
207.71.92.221	38.150.x.x	3004			113		syn (default)		
675348	06/15/00	18:25:56	n deny	in	eth0	78	udp	20	116
207.71.92.193	38.150.x.x	137			137		(default)		
675448	06/15/00	18:25:57	n deny	in	eth0	78	udp	20	116
207.71.92.193	38.150.x.x	137			137		(default)		
675508	06/15/00	18:25:58	n deny	in	eth0	78	udp	20	116
207.71.92.193	38.150.x.x	137			137		(default)		
675568	06/15/00	18:26:00	n deny	in	eth0	44	tcp	20	117
207.71.92.221	38.150.x.x	3109			139		syn (default)		
675688	06/15/00	18:26:03	n deny	in	eth0	44	tcp	20	117
207.71.92.221	38.150.x.x	3109			139		syn (default)		
1. Source of Trace		My Network							
2. Detect was generated by: (Explanation of fields)		WatchGuard Firewall Log – Date/Time/ Action/Interface/Proto/Src/Dst/SrcPort/DstPort/Details							
3. Probability the source address was spoofed.		Low – prober needs to get the results back to display them on a web page.							
4. Description of Attack		Internal user at 10.6.1.161 hits a web site that generates a response in the form of probes on 'well known' ports like SMTP, POP3, Telnet, FTP, Etc.							
5. Attack Mechanism		Server at 207.71.92.193 makes 4 attempts to contact the Firewall at 38.150.x.x on the 'well known' ports							
6. Correlations:		Visit the The ShieldsUP! Tests web site http://grc.com/default.htm by Steve Gibson, Gibson Research Corporation to confirm that it asks for your formal permission and requests 'our connection to your computer for the display of data that can be gained by anyone across the Internet'							
7. Evidence of active targeting		Definitely because the internal user initiates the request to be probed.							
8. Severity = (Critical + Lethal) – (System + Net Countermeasures)		(5+3)-(4+5)=-1							
9. Defensive recommendations		Firewall is configured to deny all inbound access.							
10. Multiple choice question		What indicates that the probes launched against this host were in response to a stimulus? A) Activity on port 137 B) An FTP session is established *C) An HTTP session is established D) There was no stimulus							

Detect # 2

```

Apr 22 00:25:58 cc1014244-a kernel: securityalert: udp if=ef0 from
24.3.123.2:1225 to 24.3.21.199 on unserved port 31337
Apr 22 07:16:29 cc1014244-a kernel: securityalert: tcp if=ef0 from
24.0.58.188:3604 to 24.3.21.199 on unserved port 27374
Apr 22 08:13:47 cc1014244-a kernel: securityalert: tcp if=ef0 from
24.65.6.142:1650 to 24.3.21.199 on unserved port 27374
Apr 22 08:49:13 cc1014244-a kernel: securityalert: tcp if=ef0 from
4.35.100.132:667 to 24.3.21.199 on unserved port 111
Apr 22 09:55:13 cc1014244-a kernel: securityalert: tcp if=ef0 from
24.1.36.229:1687 to 24.3.21.199 on unserved port 27374
Apr 22 12:24:44 cc1014244-a kernel: securityalert: tcp if=ef0 from
62.158.190.178:4837 to 24.3.21.199 on unserved port 1080
Apr 22 17:40:50 cc1014244-a kernel: securityalert: udp if=ef0 from
204.210.16.66:137 to 24.3.21.199 on unserved port 137
Apr 22 22:30:23 cc1014244-a kernel: securityalert: tcp if=ef0 from
171.218.13.132:2970 to 24.3.21.199 on unserved port 27374

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 4/25/00 http://www.sans.org/y2k/042500.htm
2. Detect was generated by: (Explanation of fields)	Server Date/Time/protocol/interface/src:port/dst/dst port
3. Probability the source address was spoofed.	Low – attacker needs to collect information he gathers
4. Description of Attack	Looking for SOCKS, Back Orifice, RPC, Quake Server, etc. – high ports hoping to find Trojans
5. Attack Mechanism	Probes are spread over the course of the day from different source addresses.
6. Correlations:	Covered in SANS San Jose 2000 classes 2.4 /2.5 – almost the same trace in Detects Analyzed 6/14/00 - Binette @home
7. Evidence of active targeting	Yes – More than one source IP looking for the same thing.
8. Severity = (Critical + Lethal) – (System + Net Countermeasures)	(4+4)-(4+4)=0
9. Defensive recommendations	Ensure you do not have services listening on ports you do not expect (Netstat – an) – Block incoming/outgoing packets destined to/from known Trojan ports like 31337
10. Multiple choice question	What BEST describes this trace? A) UDP port scan B) TCP port scan C) Back Orifice *D) Slow Scan

Detect # 3

```

02:26:31.574840 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30039:1480@0+)
02:26:31.574847 209.216.2.200 > morannon.kdi.com:
(frag 30041:48@2960)
02:26:31.583572 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30041:1480@0+)
02:26:31.583582 209.216.2.200 > morannon.kdi.com:
(frag 30044:48@2960)
02:26:31.591760 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30044:1480@0+)
02:26:31.591768 209.216.2.200 > morannon.kdi.com:
(frag 30046:48@2960)
02:26:31.600166 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30046:1480@0+)
02:26:31.600173 209.216.2.200 > morannon.kdi.com:
(frag 30048:48@2960)
02:26:31.609754 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30048:1480@0+)
02:26:31.609785 209.216.2.200 > morannon.kdi.com:
(frag 30050:48@2960)
02:26:31.618328 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30050:1480@0+)
02:26:31.618354 209.216.2.200 > morannon.kdi.com:
(frag 30052:48@2960)
02:26:31.626650 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30052:1480@0+)
02:26:31.626656 209.216.2.200 > morannon.kdi.com:
(frag 30054:48@2960)
02:26:31.635248 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30054:1480@0+)
02:26:31.635253 209.216.2.200 > morannon.kdi.com:
(frag 30056:48@2960)
02:26:31.643568 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30056:1480@0+)
02:26:31.643574 209.216.2.200 > morannon.kdi.com:
(frag 30058:48@2960)
02:26:31.652679 209.216.2.200 > morannon.kdi.com:
icmp: echo request (frag 30058:1480@0+)
02:26:31.652687 209.216.2.200 > morannon.kdi.com:
(frag 30060:48@2960)

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 3/29/00 http://www.sans.org/y2k/032900.htm
2. Detect was generated by: (Explanation of fields)	Tcpdump Time/ src/dst/
3. Probability the source address was spoofed.	Good chance source addr is spoofed as this is a denial of service.
4. Description of Attack	A Denial of Service attack
5. Attack Mechanism	Using fragmented icmp echo requests to rapidly flood one host
6. Correlations:	SANS 2000 text 2.4/2.5 page 255
7. Evidence of active targeting	Yes – a single host has been flooded.
8. Severity = (Critical + Lethal) – (System + Net Countermeasures)	(4+4)-(4+4)=0
9. Defensive recommendations	Configure Firewall to drop echo requests
10. Multiple choice question	This trace shows

- | | |
|--|--------------------------------------------------------------------------------------|
| | A) ping of death
B) teardrop
*C) Fragmented icmp DOS
D) icmp covert channel |
|--|--------------------------------------------------------------------------------------|

Detect # 4

```
05/01 00:05:50.677544 globcad-1.usnntc.savvis.net >
10.1.8.0: icmp: time exceeded in-transit (ttl 242, id 12846)
05/01 03:21:50.008103 garibaldi.ucaqld.com.au >
10.0.2.0: icmp: net h213-4-35.PD.infinito.it unreachable -
admin prohibited (ttl 42, id 41040)
05/01 05:15:27.116347 globcad-1.usnntc.savvis.net >
10.2.8.0: icmp: time exceeded in-transit (ttl 242, id 58225)
05/01 05:32:35.972887 globcad-1.usnntc.savvis.net >
10.0.3.0: icmp: time exceeded in-transit (ttl 242, id 42462)
05/01 10:26:36.898632 globcad-1.usnntc.savvis.net >
10.1.6.0: icmp: time exceeded in-transit (ttl 242, id 46417)
05/01 15:06:55.414884 globcad-1.usnntc.savvis.net >
10.2.8.0: icmp: time exceeded in-transit (ttl 242, id 23184)
05/01 15:08:43.113307 globcad-1.usnntc.savvis.net >
10.2.9.0: icmp: time exceeded in-transit (ttl 242, id 35139)
05/01 23:57:10.849683 globcad-1.usnntc.savvis.net >
10.1.9.0: icmp: time exceeded in-transit (ttl 242, id 39796)
05/02 00:53:26.544198 globcad-1.usnntc.savvis.net >
10.2.9.0: icmp: time exceeded in-transit (ttl 242, id 23982)
05/02 10:24:25.935155 globcad-1.usnntc.savvis.net >
10.1.9.0: icmp: time exceeded in-transit (ttl 242, id 41688)
05/02 16:56:32.665830 globcad-1.usnntc.savvis.net >
10.0.3.0: icmp: time exceeded in-transit (ttl 242, id 45818)
05/03 05:00:59.959806 globcad-1.usnntc.savvis.net >
10.1.9.0: icmp: time exceeded in-transit (ttl 242, id 43361)
05/03 07:09:50.339505 globcad-1.usnntc.savvis.net >
10.2.8.0: icmp: time exceeded in-transit (ttl 242, id 51021)
05/03 09:01:53.888791 globcad-1.usnntc.savvis.net >
10.2.11.0: icmp: time exceeded in-transit (ttl 242, id 13614)
05/03 12:49:54.378091 globcad-1.usnntc.savvis.net >
10.2.8.0: icmp: time exceeded in-transit (ttl 242, id 30752)
05/03 15:07:03.591869 globcad-1.usnntc.savvis.net >
10.1.9.0: icmp: time exceeded in-transit (ttl 242, id 30925)
05/03 19:54:15.449490 globcad-1.usnntc.savvis.net >
10.1.8.0: icmp: time exceeded in-transit (ttl 242, id 49273)
05/03 20:09:49.219705 globcad-1.usnntc.savvis.net >
10.1.6.0: icmp: time exceeded in-transit (ttl 242, id 22272)
05/03 21:30:03.791689 globcad-1.usnntc.savvis.net >
10.1.9.0: icmp: time exceeded in-transit (ttl 242, id 34729)
05/04 01:01:13.670002 globcad-1.usnntc.savvis.net >
10.2.11.0: icmp: time exceeded in-transit (ttl 242, id 4528)
05/04 01:36:23.094709 globcad-1.usnntc.savvis.net >
10.0.3.0: icmp: time exceeded in-transit (ttl 242, id 42827)
05/04 12:34:02.859002 globcad-1.usnntc.savvis.net >
10.1.8.0: icmp: time exceeded in-transit (ttl 242, id 38857)
05/04 13:24:18.447654 globcad-1.usnntc.savvis.net >
10.1.8.0: icmp: time exceeded in-transit (ttl 242, id 46784)
05/04 17:59:55.838341 globcad-1.usnntc.savvis.net >
10.1.6.0: icmp: time exceeded in-transit (ttl 242, id 49799)
```

```

05/04 22:31:59.036492 globcad-1.usnntc.savvis.net >
10.1.8.0: icmp: time exceeded in-transit (ttl 242, id 21173)
05/05 04:16:30.299315 globcad-1.usnntc.savvis.net >
10.1.8.0: icmp: time exceeded in-transit (ttl 242, id 23949)
05/05 05:08:04.484007 globcad-1.usnntc.savvis.net >
10.1.6.0: icmp: time exceeded in-transit (ttl 242, id 40354)
05/05 07:09:05.034362 globcad-1.usnntc.savvis.net >
10.1.6.0: icmp: time exceeded in-transit (ttl 242, id 56498)

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 5/8/00 - http://www.sans.org/y2k/050800.htm
2. Detect was generated by: (Explanation of fields)	Date/time/src/dst/protocol/
3. Probability the source address was spoofed.	Good chance src is spoofed 10.x.x.0 format
4. Description of Attack	Flood of time exceeded in-transit messages
5. Attack Mechanism	Not sure if it is just routers that are reporting TTL of 0
6. Correlations:	SANS 2000 text 2.1 page 5-26
7. Evidence of active targeting	Not likely
8. Severity= (Critical + Lethal) – (System + Net Countermeasures)	(5+4)-(4+4)=1
9. Defensive recommendations	Patch routers to latest OS / use ACLs
10. Multiple choice question	time exceeded in-transit means? *A)TTL has expired B) Ping has exceeded 1000 MS C) MTU is too small D) ARP was not successful

Detect # 5

```

05/03 20:16:35.148647 hastings.lib.ne.us.0 > .edu.pop2:
SF 790560768:790560768(0) win 512 (ttl 233, id 25092)
05/03 20:16:35.163158 hastings.lib.ne.us.0 > .edu.pop2:
SF 790560768:790560768(0) win 512 (ttl 233, id 29444)
05/04 05:58:16.469152 hastings.lib.ne.us.0 > .edu.pop2:
SF 2652962816:2652962816(0) win 512 (ttl 233, id 25092)
05/04 05:58:16.488035 hastings.lib.ne.us.0 > .edu.pop2:
SF 2652962816:2652962816(0) win 512 (ttl 233, id 29444)

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 5/8/00 -
--------------------	------------------------------------------------------------------

	http://www.sans.org/y2k/050800.htm
2. Detect was generated by: (Explanation of fields)	Date/time/src/dest/flags/sequence#
3. Probability the source address was spoofed.	Not likely as attacker needs to collect information
4. Description of Attack	syn-fin scan.
5. Attack Mechanism	Uses non-normal Syn-Fin flags to avoid detection – hitting POP2 (old) port. Source port is 0! Sequence # is the same.
6. Correlations:	SANS 2000 text 2.1 page 6-25
7. Evidence of active targeting	Yes - same attack returns on a different day to same dest.
8. Severity = (Critical + Lethal) – (System + Net Countermeasures)	(4+4)-(3+4)=1
9. Defensive recommendations	Do not run POP2 / filter source ports of 0.
10. Multiple choice question	The above trace is 'normal' in what respect? A) Source port is 0 B) Sequence # is the same C) Syn/Fin flags are set *D) POP2 port is specified

Detect # 6

```

May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1153
to 204.245.8.48.98 seq 18B51F50, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1154
to 204.245.8.49.98 seq 1820D26B, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1155
to 204.245.8.50.98 seq 183A49DA, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1156
to 204.245.8.51.98 seq 183D4A45, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1157
to 204.245.8.52.98 seq 18195E9A, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1158
to 204.245.8.53.98 seq 18342524, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1159
to 204.245.8.54.98 seq 18BD1155, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1160
to 204.245.8.55.98 seq 1841994B, ack 0x0, win 32120, SYN
May 23 03:48:52 pyramid 26 deny: TCP from 193.129.252.129.1161
to 204.245.8.56.98 seq 17F4FD5A, ack 0x0, win 32120, SYN
May 23 03:48:55 pyramid 26 deny: TCP from 193.129.252.129.1168
to 204.245.8.63.98 seq 1897887C, ack 0x0, win 32120, SYN

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 5/26/00 - http://www.sans.org/y2k/052600-1130.htm
2. Detect was generated by: (Explanation of fields)	Date/time/action/src/dest/
3. Probability the source address was spoofed.	Low – attacker needs the information .
4. Description of Attack	Linuxconf - .
5. Attack Mechanism	Scan all hosts for Linuxconf to reveal how OS is configured – running as root!
6. Correlations:	SANS 2000 text 2.4/2.5 page 159 Started after Nov 1999
7. Evidence of active targeting	Not targeted – scanning all machines on subnet.
8. Severity = (Critical + Lethal) – (System + Net Countermeasures)	(5+5)-(4+4)=2
9. Defensive recommendations	Configure Linux properly.

10. Multiple choice question	Linuxconf is what? A) Installer for Linux B) Removes the Linux OS *C) Configures Linux D) Virus for Linux
------------------------------	------------------------------------------------------------------------------------------------------------------------------

Detect # 7	
Mar 15 13:08:05.516720	209.4.162.239,2317 -> 10.0.3.24,1080 PR tcp len 20 64 -S
Mar 15 13:08:08.189768	209.4.162.239,2317 -> 10.0.3.24,1080 PR tcp len 20 64 -S
Mar 15 13:08:14.377628	209.4.162.239,2317 -> 10.0.3.24,1080 PR tcp len 20 64 -S
Mar 15 13:08:27.450134	209.4.162.239,2317 -> 10.0.3.24,1080 PR tcp len 20 64 -S
Mar 15 13:08:53.226587	209.4.162.239,3120 -> 10.0.3.24,8080 PR tcp len 20 64 -S
Mar 15 13:08:56.573158	209.4.162.239,3120 -> 10.0.3.24,8080 PR tcp len 20 64 -S
Mar 15 13:09:02.913774	209.4.162.239,3120 -> 10.0.3.24,8080 PR tcp len 20 64 -S
Mar 15 13:09:15.707667	209.4.162.239,3120 -> 10.0.3.24,8080 PR tcp len 20 64 -S
Mar 15 13:09:41.473938	209.4.162.239,4025 -> 10.0.3.24,3128 PR tcp len 20 64 -S
Mar 15 13:09:44.883563	209.4.162.239,4025 -> 10.0.3.24,3128 PR tcp len 20 64 -S
Mar 15 13:09:50.878854	209.4.162.239,4025 -> 10.0.3.24,3128 PR tcp len 20 64 -S
Mar 15 13:10:03.624947	209.4.162.239,4025 -> 10.0.3.24,3128 PR tcp len 20 64 -S
Mar 15 13:10:29.296657	209.4.162.239,4905 -> 10.0.3.24,80 PR tcp len 20 64 -S
Mar 15 13:10:32.541328	209.4.162.239,4905 -> 10.0.3.24,80 PR tcp len 20 64 -S
Mar 15 13:10:38.696486	209.4.162.239,4905 -> 10.0.3.24,80 PR tcp len 20 64 -S
Mar 15 13:10:51.725926	209.4.162.239,4905 -> 10.0.3.24,80 PR tcp len 20 64 -S
1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 3/17/00 http://www.sans.org/y2k/031700.htm
2. Detect was generated by: (Explanation of fields)	Date/time/src/dest/port/protocol
3. Probability the source address was spoofed.	Low – attacker needs to have information returned to him.
4. Description of Attack	Looking for Web related services (Squid/Proxy/Web). Maybe RingZero
5. Attack Mechanism	Attempt to connect on port of interest.
6. Correlations:	http://www.sans.org/newlook/resources/ringzero.htm
7. Evidence of active targeting	Yes same host is targeted for many services.
8. Severity = (Critical + Lethal) – (System + Net Countermeasures)	(5+4)-(4+5)=0
9. Defensive recommendations	Limit OUTBOUND traffic for ports 80, 8080, and 3128 block inbound if not used.
10. Multiple choice question	Port 3128 is used for? *A) Squid proxy B) Netscape proxy C) Microsoft proxy D) Novell proxy

Detect # 8

```

Mar 9 20:48:05 dns2 snort[20879]:
SNMP access, public: 206.109.62.1:2466 -> x.x.x.a:161
-----
[**] SNMP access, public [**]
03/09-20:48:05.262616 206.109.62.1:2466 -> x.x.x.a:161
UDP TTL:111 TOS:0x0 ID:58322
Len: 63
30 35 02 01 00 04 06 70 75 62 6C 69 63 A1 28 02 05.....public.(.
04 38 CA 42 B0 02 01 00 02 01 00 30 1A 30 0B 06 .8.B.....0.0..
07 2B 06 01 02 01 01 02 05 00 30 0B 06 07 2B 06 .+.....0...+.
01 02 01 01 01 05 00 .....

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 3/15/00 - http://www.sans.org/y2k/031500.htm
2. Detect was generated by: (Explanation of fields)	Snort Date/time/src/dst
3. Probability the source address was spoofed.	Small since attacker needs the information
4. Description of Attack	Retrieve information from Public string and beyond.
5. Attack Mechanism	Query the Public string
6. Correlations:	SANS 2000 text 2.4/2.5 page 169
7. Evidence of active targeting	No – will try many hosts
8. Severity= (Critical + Lethal) – (System + Net Countermeasures)	(4+3)-(4+5)=-2
9. Defensive recommendations	Do not allow the world to query Public strings – change defaults
10. Multiple choice question	SNMP is? A) used to test connectivity B) used to send mail *C) used as a management tool D) used to encrypt packets

Detect # 9

```

Feb 21 01:05:06 aeon icmplogd: ping
from bannister.globalcenter.net [208.48.114.124]
Feb 24 17:04:57 bishop-rock icmplogd: ping
from atrel2.hp.com [156.153.255.202]
Feb 24 17:04:57 bishop-rock icmplogd: ping
from atrel1.hp.com [156.153.255.210]
Feb 24 17:18:52 bishop-rock icmplogd: ping
from atrel1.hp.com [156.153.255.210]

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 2/28/00
--------------------	------------------------------------------------------------------------

	http://www.sans.org/y2k/022800.htm
2. Detect was generated by: (Explanation of fields)	Date/time/dest/service/src
3. Probability the source address was spoofed.	Low – prober needs the information
4. Description of Attack	load-balancing. technique.
5. Attack Mechanism	Send pings to same host from 2 different sources at the same time to calculate the optimum path.
6. Correlations:	SANS 2000 text 2.4/2.5 page 318
7. Evidence of active targeting	Yes – 2 sources hit the same target at the same time.
8. Severity=(Critical + Lethal) – (System + Net Countermeasures)	(3+3)-(4+5)=-3
9. Defensive recommendations	Monitor traffic to contact offending party
10. Multiple choice question	This trace is? A) A denial of service *B) A load balancing technique C) A port mapping D) A fragmentation attack

Detect # 10

```
Feb 25 19:42:26 host1 proftpd[2435] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - local : 1.2.3.4:21
Feb 25 19:42:26 host1 proftpd[2435] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - remote : 24.128.77.138:4294
Feb 25 19:42:30 host1 proftpd[2435] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
FTP session closed.
Feb 25 19:49:17 host1 proftpd[2477] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - local : 1.2.3.4:21
Feb 25 19:49:17 host1 proftpd[2477] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - remote : 24.128.77.138:2166
Feb 25 19:49:18 host1 proftpd[2477] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
FTP session closed.
Feb 25 20:56:47 host1 proftpd[2619] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - local : 1.2.3.4:21
Feb 25 20:56:47 host1 proftpd[2619] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - remote : 24.128.77.138:1426
Feb 25 20:56:47 host1 proftpd[2619] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
FTP session closed.
Feb 25 21:47:59 host1 proftpd[2729] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - local : 1.2.3.4:21
Feb 25 21:47:59 host1 proftpd[2729] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - remote : 24.128.77.138:2277
```

```

Feb 25 21:48:00 host1 proftpd[2729] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
FTP session closed.
Feb 26 20:16:14 host1 proftpd[7018] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - local : 1.2.3.4:21
Feb 26 20:16:14 host1 proftpd[7018] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
connected - remote : 24.128.77.138:2838
Feb 26 20:16:38 host1 proftpd[7018] host1
(h00801935e177.ne.mediaone.net[24.128.77.138]):
FTP session closed.

```

1. Source of Trace	GIAC Archive of Activity and Reports – Detects Analyzed 2/29/00 http://www.sans.org/y2k/022900.htm
2. Detect was generated by: (Explanation of fields)	Server Date/time/client/server
3. Probability the source address was spoofed.	Low – session gets established.
4. Description of Attack	Ftp probes
5. Attack Mechanism	Many connections to the server in a very short time.
6. Correlations:	SANS 2000 text 2.1 page 6-19
7. Evidence of active targeting	Yes – multiple connections to the same host
8. Severity = (Critical + Lethal) – (System + Net Countermeasures)	(5+4)-(4+5)=0
9. Defensive recommendations	Do not allow anonymous FTP
10. Multiple choice question	FTP uses what 2 ports? A) 21&25 B) 23&21 C) 23&20 *D)20&21

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC503: Intrusion Detection In-Depth	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS vLive - SEC503: Intrusion Detection In-Depth	SEC503 - 201709,	Sep 11, 2017 - Oct 18, 2017	vLive
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Baltimore Fall 2017 - SEC503: Intrusion Detection In-Depth	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Scottsdale SEC503	Scottsdale, AZ	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Pensacola SEC503	Pensacola, FL	Nov 27, 2017 - Dec 02, 2017	Community SANS
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZ	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced