Global Information Assurance Certification Paper

These 10 traces were submitted by Gert Florijn for the practical examination following the IDS course curriculum attended at SANS2000, San Jose (Ca).

All IP addresses of my own systems are changed, using the 10.10.10.x notation.
The "erouter" is connected to the internet as access router.

Detect #1

```
Jun 6 20:05:47 erouter 4364729: *Jun 6 20:05:25: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(788) -> 10.10.10.45(53), 5 packets
Jun 6 20:35:48 erouter 4365544: *Jun 6 20:35:26: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(724) -> 10.10.10.45(53), 11 packets
Jun 6 21:05:50 erouter 4366251: *Jun 6 21:05:28: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(747) -> 10.10.10.45(53), 1 packet
Jun 6 21:06:22 erouter 4366263: *Jun 6 21:06:00: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(747) -> 10.10.10.45(53), 5 packets
Jun 6 21:21:34 erouter 4366618: *Jun 6 21:21:11: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(930) -> 10.10.10.45(53), 11 packets
Jun 6 21:36:22 erouter 4366975: *Jun 6 21:35:59: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(719) -> 10.10.10.45(53), 8 packets
Jun 6 21:50:48 erouter 4367351: *Jun 6 21:50:26: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(910) -> 10.10.10.45(53), 1 packet
Jun 6 21:51:11 erouter 4367363: *Jun 6 21:50:49: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(910) -> 10.10.10.45(53), 5 packets
Jun 6 22:06:30 erouter 4367724: *Jun 6 22:06:08: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(762) -> 10.10.10.45(53), 8 packets
Jun 6 22:21:29 erouter 4368076: *Jun 6 22:21:06: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(610) -> 10.10.10.45(53), 1 packet
Jun 6 22:22:13 erouter 4368086: *Jun 6 22:21:51: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(609) -> 10.10.10.45(53), 11 packets
Jun 6 22:36:19 erouter 4368450: *Jun 6 22:35:57: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(771) -> 10.10.10.45(53), 11 packets
Jun 6 22:36:20 erouter 4368451: *Jun 6 22:35:58: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(772) -> 10.10.10.45(53), 5 packets
Jun 6 22:51:39 erouter 4368806: *Jun 6 22:51:17: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(643) -> 10.10.10.45(53), 8 packets
Jun 6 22:51:41 erouter 4368807: *Jun 6 22:51:19: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(646) -> 10.10.10.45(53), 5 packets
Jun 6 23:06:31 erouter 4369161: *Jun 6 23:06:09: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(979) -> 10.10.10.45(53), 11 packets
Jun 6 23:06:39 erouter 4369162: *Jun 6 23:06:17: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(980) -> 10.10.10.45(53), 5 packets
Jun 6 23:21:33 erouter 4369488: *Jun 6 23:21:11: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(699) -> 10.10.10.45(53), 11 packets
Jun 6 23:21:36 erouter 4369489: *Jun 6 23:21:14: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(702) -> 10.10.10.45(53), 5 packets
Jun 6 23:36:29 erouter 4369806: *Jun 6 23:36:07: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(815) -> 10.10.10.45(53), 11 packets
Jun 6 23:36:31 erouter 4369807: *Jun 6 23:36:09: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(816) -> 10.10.10.45(53), 5 packets
Jun 6 23:51:12 erouter 4370128: *Jun 6 23:50:50: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(997) -> 10.10.10.45(53), 5 packets
Jun 6 23:51:16 erouter 4370131: *Jun 6 23:50:54: %SEC-6-IPACCESSLOGP: list 142 denied udp 12.15.170.193(996) -> 10.10.10.45(53), 8 packets
```

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	As long as the goal of this attack is uncertain, address spoofing is still an option. In case of misbehaviour of a DNS server, no address spoofing is used.	
Description of attack	Attack against DNS server port 53, reconnaissance. The signature is given by DNS requests coming from a source port < 1024. I keep the possibility of a bad configured DNS server open.	
Attack mechanism	Using low source port numbers for DNS queries. Probably looking for a weakness in the DNS server defence.	
Correlation	Mark Thyer (http://www.sans.org/y2k/practical/mark_thyer.doc)	
Active Targeting?	This kind of attack is coming from several servers, all over the world.	
Criticality	5	DNS server.
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-3	*Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)*
Defensive recommendations	Defences are fine. Attack was blocked by external router.	
Question	The intent of this attack is: a) Denial of Service b) Trying to get root access c) Information gathering d) Ordinary DNS queries Answer: C	
Notes	This attack is still going on and coming from different servers. No other requests are seen from those servers.	

Detect #2

```
Jun 5 10:40:17 erouter 4294686: *Jun 5 10:39:55: %SEC-6-IPACCESSLOGP: list 142 denied udp 212.4.5.34(62858) -> 10.10.10.44(33506), 1 packet
Jun 5 10:40:42 erouter 4294713: *Jun 5 10:40:20: %SEC-6-IPACCESSLOGP: list 142 denied udp 212.4.5.34(62858) -> 10.10.10.44(33511), 1 packet
Jun 5 10:40:52 erouter 4294722: *Jun 5 10:40:30: %SEC-6-IPACCESSLOGP: list 142 denied udp 212.4.5.34(62858) -> 10.10.10.44(33513), 1 packet
Jun 5 10:41:42 erouter 4294773: *Jun 5 10:41:20: %SEC-6-IPACCESSLOGP: list 142 denied udp 212.4.5.34(62858) -> 10.10.10.44(33523), 1 packet
Jun 5 10:43:47 erouter 4294882: *Jun 5 10:43:25: %SEC-6-IPACCESSLOGP: list 142 denied udp 165.117.52.185(34469) -> 10.10.10.44(33488), 1 packet
Jun 5 10:44:08 erouter 4294898: *Jun 5 10:43:46: %SEC-6-IPACCESSLOGP: list 142 denied udp 165.117.52.185(34469) -> 10.10.10.44(33495), 1 packet
Jun 5 10:44:57 erouter 4294939: *Jun 5 10:44:35: %SEC-6-IPACCESSLOGP: list 142 denied udp 165.117.52.185(34469) -> 10.10.10.44(33511), 1 packet
Jun 5 10:45:27 erouter 4294965: *Jun 5 10:45:05: %SEC-6-IPACCESSLOGP: list 142 denied udp 165.117.52.185(34469) -> 10.10.10.44(33521), 1 packet
```

Source of trace	Own network	
Detect is generated by	Cisco ACL loggi ng	
Address spoofing?	Not likely, responses are required to get the attack information.	
Description of attack	External network mapping, simultaneous traceroutes.	
Attack mechanism	By using multiple, almost simultaneous traceroutes from different source ad dresses, the attacker gains information about the external layers of the protected network.	
Correlation	This kind of attack is described in Staphan Northcutt's SANS 2000 class (Intrusion Detection Workshop, page 318)	
Active Targeting?	The attack is look ing for specific network entry points.	
Criticality	5	Core routers.
Lethality	2	No access possible.
System Countermeasures	5	Well-protected router.
Network Countermeasures	4	Restricted firewall connection.
Severity	-2	*Severity = (Criticality + Lethalit y) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. Attack was blocked by external router.	
Question	What is the best defence against simultaneous trace routes? a) Create as many as possible connections to the internet. b) Configure the routers so no response will be given to traceroutes c) Connect all providers to the same router. Answer: B	
Notes		

Detect #3

```
Jun 6 05:04:13 erouter 4329567: *Jun 6 05:03:51: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3427) -> 10.10.10.47(3000), 1 packet
Jun 6 05:04:14 erouter 4329568: *Jun 6 05:03:52: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3445) -> 10.10.10.47(7048), 1 packet
Jun 6 05:04:15 erouter 4329569: *Jun 6 05:03:53: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3402) -> 10.10.10.47(50), 1 packet
Jun 6 05:04:15 erouter 4329570: *Jun 6 05:03:54: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3429) -> 10.10.10.47(3080), 1 packet
Jun 6 05:04:17 erouter 4329571: *Jun 6 05:03:55: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3446) -> 10.10.10.47(7080), 1 packet
Jun 6 05:04:21 erouter 4329572: *Jun 6 05:03:59: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3400) -> 10.10.10.47(23), 1 packet
Jun 6 05:04:22 erouter 4329573: *Jun 6 05:04:00: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3423) -> 10.10.10.47(1234), 1 packet
Jun 6 05:04:23 erouter 4329574: *Jun 6 05:04:01: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3443) -> 10.10.10.47(6658), 1 packet
Jun 6 05:04:33 erouter 4329575: *Jun 6 05:04:11: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3400) -> 10.10.10.47(23), 1 packet
Jun 6 05:04:34 erouter 4329576: *Jun 6 05:04:12: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3425) -> 10.10.10.47(2146), 1 packet
Jun 6 05:04:35 erouter 4329577: *Jun 6 05:04:13: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3444) -> 10.10.10.47(7036), 1 packet
Jun 6 05:05:00 erouter 4329582: *Jun 6 05:04:38: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3448) -> 10.10.10.47(8000), 1 packet
Jun 6 05:05:01 erouter 4329583: *Jun 6 05:04:39: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3464) -> 10.10.10.47(8083), 1 packet
Jun 6 05:05:02 erouter 4329584: *Jun 6 05:04:40: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3480) -> 10.10.10.47(8973), 1 packet
Jun 6 05:05:03 erouter 4329585: *Jun 6 05:04:41: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3451) -> 10.10.10.47(8002), 1 packet
Jun 6 05:05:04 erouter 4329586: *Jun 6 05:04:42: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3467) -> 10.10.10.47(8086), 1 packet
Jun 6 05:05:05 erouter 4329587: *Jun 6 05:04:43: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3483) -> 10.10.10.47(9003), 1 packet
Jun 6 05:05:06 erouter 4329588: *Jun 6 05:04:44: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3499) -> 10.10.10.47(30101), 1 packet
Jun 6 05:05:09 erouter 4329589: *Jun 6 05:04:47: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3448) -> 10.10.10.47(8000), 1 packet
Jun 6 05:05:10 erouter 4329590: *Jun 6 05:04:48: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3465) -> 10.10.10.47(8084), 1 packet
Jun 6 05:05:11 erouter 4329591: *Jun 6 05:04:49: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3483) -> 10.10.10.47(9003), 1 packet
Jun 6 05:05:11 erouter 4329592: *Jun 6 05:04:50: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3497) -> 10.10.10.47(28800), 1 packet
Jun 6 05:05:21 erouter 4329595: *Jun 6 05:04:59: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3448) -> 10.10.10.47(8000), 1 packet
Jun 6 05:05:23 erouter 4329597: *Jun 6 05:05:01: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3480) -> 10.10.10.47(8973), 1 packet
Jun 6 05:05:24 erouter 4329598: *Jun 6 05:05:02: %SEC-6-IPACCESSLOGP: list 142 denied tcp 210.228.179.7(3496) -> 10.10.10.47(18765), 1 packet
```

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not likely, the responses ar e informative to the attacker.	
Description of attack	Port scan, probably looking for malicious code or trojans.	
Attack mechanism	The attacker tries to find a open port on a specific target system.	
Correlation	This is a well-known type of attack. See for instance the CERT reports. http://www.cert.org/summaries/CS_-99-01.html	
Active Targeting?	Only one specific target was scanned.	
Criticality	3	The target is a mx -failover host, only used for outg oing mail.
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-5	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recomm endations	Defences are fine. Attack was blocked by external router.	
Question	In this trace, the attack is best described by: a) Post scan b) Denial of service, by overloading a host. c) A search for malicious code or trojans d) Network scan Answer C	
Notes		

Detect #4

```
Jun 2 15:15:57 erouter 4238589: *Jun  2 15:15:37: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
Jun 2 15:16:03 erouter 4238594: *Jun  2 15:15:42: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
Jun 5 02:24:30 erouter 4283810: *Jun  5 02:24:08: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
Jun 5 16:42:21 erouter 4312788: *Jun  5 16:41:59: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
Jun 6 14:14:16 erouter 4349504: *Jun  6 14:13:54: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
Jun 6 22:20:57 erouter 4368067: *Jun  6 22:20:35: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
Jun 8 20:53:57 erouter 4458855: *Jun  8 20:53:34: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
Jun 8 20:54:17 erouter 4458862: *Jun  8 20:53:55: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 216.209.25.184 -> 10.10.10.255 (8/0), 1 packet
```

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not likely, response is required	
Description of attac k	Network mapping by pinging to the broadcast address	
Attack mechanism	Slow scan , to make it hard to detect.	
Correlation	Stealthy ping method is more and more common. This kind of attack is described in Staphan Northcutt's SANS 2000 class (Intrusion Detection Workshop, page 301)	
Active Targeting?	One specific network is the target.	
Criticality	3	External accessible network
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall c onnection.
Severity	-5	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. External router blocked the attack.	
Question	Why is this attack hard to detect by intrusion detection systems? a) Too few entries in the log files. b) Due to the slow scanning. c) No specific host is targeted. d) All of the above Answer B	
Notes		

Detect #5

```
Jun 5 21:18:12 erouter 4322338: *Jun  5 21:17:50: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.1 (8/0), 1 packet
Jun 5 21:18:13 erouter 4322340: *Jun  5 21:17:52: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.9 (8/0), 1 packet
Jun 5 21:18:14 erouter 4322342: *Jun  5 21:17:53: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.12 (8/0), 1 packet
Jun 5 21:18:16 erouter 4322343: *Jun  5 21:17:54: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.19 (8/0), 1 packet
Jun 5 21:18:17 erouter 4322345: *Jun  5 21:17:55: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.34 (8/0), 1 packet
Jun 5 21:18:18 erouter 4322348: *Jun  5 21:17:57: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.52 (8/0), 1 packet
Jun 5 21:18:20 erouter 4322350: *Jun  5 21:17:58: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.60 (8/0), 1 packet
Jun 5 21:18:21 erouter 4322353: *Jun  5 21:17:59: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.70 (8/0), 1 packet
Jun 5 21:18:22 erouter 4322354: *Jun  5 21:18:00: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.77 (8/0), 1 packet
Jun 5 21:18:23 erouter 4322356: *Jun  5 21:18:01: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.89 (8/0), 1 packet
Jun 5 21:18:24 erouter 4322358: *Jun  5 21:18:02: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.97 (8/0), 1 packet
Jun 5 21:18:25 erouter 4322360: *Jun  5 21:18:03: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.110 (8/0), 1 packet
Jun 5 21:18:26 erouter 4322362: *Jun  5 21:18:04: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.121 (8/0), 1 packet
Jun 5 21:18:27 erouter 4322364: *Jun  5 21:18:05: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.136 (8/0), 1 packet
Jun 5 21:18:28 erouter 4322366: *Jun  5 21:18:06: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.146 (8/0), 1 packet
Jun 5 21:18:29 erouter 4322368: *Jun  5 21:18:07: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.157 (8/0), 1 packet
Jun 5 21:18:30 erouter 4322370: *Jun  5 21:18:08: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.171 (8/0), 1 packet
Jun 5 21:18:31 erouter 4322372: *Jun  5 21:18:09: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.185 (8/0), 1 packet
Jun 5 21:18:32 erouter 4322373: *Jun  5 21:18:10: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.198 (8/0), 1 packet
Jun 5 21:18:33 erouter 4322375: *Jun  5 21:18:11: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.211 (8/0), 1 packet
Jun 5 21:18:34 erouter 4322377: *Jun  5 21:18:13: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.225 (8/0), 1 packet
Jun 5 21:18:36 erouter 4322379: *Jun  5 21:18:14: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.238 (8/0), 1 packet
Jun 5 21:18:37 erouter 4322381: *Jun  5 21:18:15: %SEC-6-IPACCESSLOGDP: list 142 denied icmp 194.134.15.181 -> 10.10.10.251 (8/0), 1 packet
```

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not very likely, responses are necessary for the attacker to gain information.	
Description of attack	Network mapping	
Attack mechanism	Using icmp echo requests to find hosts on a specific network.	
Correlation **Active Targeting?**	This is a very old type of information gathering. Most firewalls will block this type of attack, so I was surprised to find it. Probably a newby, ISP Euronet owns the I P address. It is a general scan of the network.	
Criticality	3	External network
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-5	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. Attack was blocked by external router.	
Question	This trace is best describes as: a) Port scan b) Portmapper exploit c) Scan for webservers on port 80 d) Network mapping Answer D	
Notes		

Detect #6

```
Jun 6 05:57:46 erouter 4330123: *Jun 6 05:57:24: %SEC-6-IPACCESSLOGP: list 142 denied tcp 166.48.242.62(53) -> 10.10.10.45(53), 1 packet
Jun 6 06:25:17 erouter 4330458: *Jun 6 06:24:54: %SEC-6-IPACCESSLOGP: list 142 denied tcp 166.48.242.62(53) -> 10.10.10.45(53), 1 packet
Jun 6 08:22:49 erouter 4332787: *Jun 6 08:22:27: %SEC-6-IPACCESSLOGP: list 142 denied tcp 166.48.242.62(53) -> 10.10.10.45(53), 1 packet
Jun 6 08:26:11 erouter 4332904: *Jun 6 08:25:49: %SEC-6-IPACCESSLOGP: list 142 denied tcp 166.48.242.62(53) -> 10.10.10.45(53), 3 packets
Jun 6 08:49:38 erouter 4333757: *Jun 6 08:49:16: %SEC-6-IPACCESSLOGP: list 142 denied tcp 166.48.242.62(53) -> 10.10.10.45(53), 1 packet
```

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not very likely, responses are needed by attacker.	
Description of attack	Attempt to unauthorised zone transfer.	
Attack mechanism	Zone transfer will give the attacker a lot of information about the network.	
Correlation	CERT Incident Note IN-98.02 http://www.cert.org/incident_notes/IN-98.02.html This incident note gives a lot of reasons to protect the DNS zone transfer.	
Active Targeting?	Target system is a DNS server indeed.	
Criticality	5	DNS server
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-3	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. Attack was blocked by external router.	
Question	Wind kind of attack is shown in the trace? a) Scan for DNS servers b) Zone transfer attempt c) DNS cache poisoning d) WINS attack Answer B	
Notes		

Detect #7

```
Jun 4 02:37:36 erouter 4268598: *Jun 4 02:37:14: %SEC-6-IPACCESSLOGP: list 142 denied tcp 213.46.26.45(3990) -> 10.10.10.37(80), 3 packets
Jun 4 02:38:15 erouter 4268604: *Jun 4 02:37:53: %SEC-6-IPACCESSLOGP: list 142 denied tcp 213.46.26.45(3992) -> 10.10.10.37(1080), 3 packets
Jun 4 02:38:20 erouter 4268607: *Jun 4 02:37:58: %SEC-6-IPACCESSLOGP: list 142 denied tcp 213.46.26.45(3993) -> 10.10.10.37(8000), 3 packets
```

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not very likely,	
Description of attack	Looking for proxy server.	
Attack mechanism	Try to connect to the well -known proxy ports.	
Correlation	Proxy servers have common ports.	
Active Targeting?	The attacke r is targeting a specific system	
Criticality	5	Proxy server used by internal users.
Lethality	3	User access
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-2	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. External router blocked the attack.	
Question	What type of attack is shown in the given trace? a) Unauthorised use of a proxy server b) Scan for potential proxy server s c) Information gathering d) None of the above Answer A	
Notes	The targeted server is indeed a proxy server for internal use.	

Detect #8

```
Jun 3 10:17:41 erouter 4258736: *Jun  3 10:17:20: %SEC-6-IPACCESSLOGP: list 142 denied tcp 208.59.14.66(111) -> 10.10.10.52(111), 1 packet
Jun 3 10:17:42 erouter 4258737: *Jun  3 10:17:21: %SEC-6-IPACCESSLOGP: list 142 denied tcp 208.59.14.66(111) -> 10.10.10.103(111), 1 packet
Jun 3 10:17:43 erouter 4258738: *Jun  3 10:17:22: %SEC-6-IPACCESSLOGP: list 142 denied tcp 208.59.14.66(111) -> 10.10.10.153(111), 1 packet
Jun 3 10:17:44 erouter 4258739: *Jun  3 10:17:23: %SEC-6-IPACCESSLOGP: list 142 denied tcp 208.59.14.66(111) -> 10.10.10.203(111), 1 packet
Jun 3 10:17:45 erouter 4258740: *Jun  3 10:17:24: %SEC-6-IPACCESSLOGP: list 142 denied tcp 208.59.14.66(111) -> 10.10.10.253(111), 1 packet
```

ource of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not very likely,	
Description of attack	Portmapper attack,	
Attack mechanism	Try to connect to the portmapper, to get information about specific rpc services, running on the target host.	
Correlation	On the CERT server is a clear incident note about this topic: http://www.cert.org/in cident_notes/IN -99-04.html	
Active Targeting?	Several systems on the same network are tested.	
Criticality	3	Several servers
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-5	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. Attack was blocked by external router.	
Question	The intent of this attack is: a) Information gathering b) Trying to get root access c) Denial of Service attack d) Port scan Answer A	
Notes		

Detect #9

Jun 2 21:08:39 erouter 4249657: *Jun 2 21:08:18: %SEC-6-IPACCESSLOGP: list 142 denied tcp 62.108.26.205(1524) -> 10.10.10.51(110), 2 packets
Jun 2 21:08:40 erouter 4249658: *Jun 2 21:08:19: %SEC-6-IPACCESSLOGP: list 142 denied tcp 62.108.26.205(1523) -> 10.10.10.51(111), 2 packets
Jun 2 21:08:41 erouter 4249659: *Jun 2 21:08:20: %SEC-6-IPACCESSLOGP: list 142 denied tcp 62.108.26.205(1526) -> 10.10.10.51(79), 2 packets
Jun 2 21:08:45 erouter 4249660: *Jun 2 21:08:24: %SEC-6-IPACCESSLOGP: list 142 denied tcp 62.108.26.205(1527) -> 10.10.10.51(53), 2 packets
Jun 2 21:08:46 erouter 4249661: *Jun 2 21:08:25: %SEC-6-IPACCESSLOGP: list 142 denied tcp 62.108.26.205(1525) -> 10.10.10.51(25), 2 packets
Jun 2 21:10:06 erouter 4249685: *Jun 2 21:09:45: %SEC-6-IPACCESSLOGP: list 142 denied tcp 62.108.26.205(1533) -> 10.10.10.51(1433), 2 packets
Jun 2 21:10:32 erouter 4249694: *Jun 2 21:10:11: %SEC-6-IPACCESSLOGP: list 142 denied tcp 62.108.26.205(1536) -> 10.10.10.51(1433), 2 packets

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not very likely, responses are required for attack	
Description of attack	Looking for vulnerabilities at a specific host.	
Attack mechanism	Testing specific tcp ports at a server with valuable contents. (Transaction server).	
Correlation	The used ports are well-defined and often used to get information about the target system.	
Active Targeting?	The attacker is attacking just one system.	
Criticality	5	Webserver
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-3	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. External router blocked attack.	
Question	Why is the attacker using only these ports? a) Stealth technique. b) These ports can give more information about the system c) Systems have to listen to these ports. d) All of the above Answer B	
Notes	I was in this one particularly because the server is used for financial transactions. See also the next detect.	

Detect #10

```
Jun 8 15:26:00 erouter 4445719: *Jun 8 15:25:37: %SEC-6-IPACCESSLOGNP: list 142 denied 54 195.86.251.112 -> 10.10.10.51, 1 packet
Jun 8 15:26:08 erouter 4445727: *Jun 8 15:25:47: %SEC-6-IPACCESSLOGNP: list 142 denied 54 195.86.251.112 -> 10.10.10.51, 1 packet
Jun 8 15:26:20 erouter 4445738: *Jun 8 15:25:58: %SEC-6-IPACCESSLOGNP: list 142 denied 54 195.86.251.112 -> 10.10.10.51, 1 packet
Jun 8 15:35:36 erouter 4446218: *Jun 8 15:35:14: %SEC-6-IPACCESSLOGNP: list 142 denied 54 195.86.251.112 -> 10.10.10.51, 1 packet
Jun 8 15:35:42 erouter 4446224: *Jun 8 15:35:20: %SEC-6-IPACCESSLOGNP: list 142 denied 54 195.86.251.112 -> 10.10.10.51, 1 packet
Jun 8 15:35:53 erouter 4446234: *Jun 8 15:35:30: %SEC-6-IPACCESSLOGNP: list 142 denied 54 195.86.251.112 -> 10.10.10.51, 1 packet
```

Source of trace	Own network	
Detect is generated by	Cisco ACL logging	
Address spoofing?	Not likely.	
Description of attack	Using odd IP protocol types to a particular host. a) Information gathering b) Denial of service attack	
Attack mechanism	Packets with an odd IP protocol number are used to test the targe t host.	
Correlation	I have never seen this one before. Protocol number 54 is used for NBMA Address Resolution Protocol (RFC 1735) http://freesoft.org/CIE/RFC/Orig/rfc1735.txt This RFC is only an experimental protocol, but the term Address Resolution, gives me the idea that some unwanted responses can go back, giving more information to the hacker.	
Active Targeting?	Only one system is targeted.	
Criticality	5	Transaction server
Lethality	2	No access possible.
System Countermeasures	5	Well-protected server.
Network Countermeasures	5	Restricted firewall connection.
Severity	-3	*Severity = (Criticality + Lethality) – (System + Network Countermeasures)*
Defensive recommendations	Defences are fine. External router blocked attack.	
Question	What kind of technique is used in the given trace? a) Sending packets with the same sequence number (54) b) Using an odd IP protocol c) Netbios scan d) None of the above Answer B	
Notes		