Global Information Assurance Certification Paper

By Nathan Fain
June.16.00 2:30AM IDT
June.15.00 PST (so getting in this in JIT)

000000000000000000000000000000000000DesiredWidthOfDocument0000000000000000000000000000000000000

```
#############
# Detect.1  #
#############
   date        time     dst.port      src.ip        dest.ip    proto src.port other.info
"5Jun2000"  "16:37:08"  "27820"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 120"
"5Jun2000"  "16:37:38"  "27821"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 73"
"5Jun2000"  "16:38:28 "  "27822"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 120"
"5Jun2000"  "16:38:58"  "27820"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 73"
"5Jun2000"  "16:39:48"  "27822"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 120"
"5Jun200 0"  "16:40:18"  "27820"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 73"
"5Jun2000"  "16:46:18"  "27822"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 556"
"5Jun2000"  "16:47:39"  "27824"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 55   6"
"5Jun2000"  "16:48:58"  "27823"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 556"
"5Jun2000"  "16:49:48"  "27823"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 39"
"5Jun2000"  "16:50:19"  "27825"  "207.97.74.146"  "x.x.x.54"  "udp"  "10   32"  " len 556"
<snip>
"5Jun2000"  "23:22:49"  "49690"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 69"
"5Jun2000"  "23:22:59"  "49692"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 39"
"5Jun2000"  "23:24:09"  "49691"  "207.97.74.146"  "x.  x.x.54"  "udp"  "1032"  " len 69"
"5Jun2000"  "23:24:59"  "49691"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 39"
"5Jun2000"  "23:25:29"  "49693"  "207.97.74.146"  "x.x.x.54"  "udp"  "1032"  " len 69"
```

(1) Source of Trace:
A network th at I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall logs. The log was clipped for clarity but all lines have an incremental fashion for the destination port.

(3) Probability the source address was spoofed:
Low. Th e IP is apart of a Class C block of address that belongs to Verio/Clark.net, a large provider of Internet services (connectivity, web hosting) for businesses located within the US.

(4) Description of Attack:
Slow port scan. I noti ced that the source IP address has done this same scan several times in the past. One notable signature for this scan is the consistency of the source port though I am not sure which particular scanner or script uses this exact port.

Another interesting note is the "len" field. This number normally doesn't fluctuate but in this scan there are a few packets where the 'len' value varies. I'd like to see the payload of those packets but there is no current method set up for this on this network.

(5) Attack Mechanism:
Attacker seems to be scanning in an attempt to gather information about his target for a future attack. He/She is doing this at a relatively slow pace (one packet/30seconds) to tr y to disguise their packets amongst the other noise. However, the consistent source port and IP makes them stick out like sore thumb

(6) Correlations:
Port scanning is very common and often gives hint to future, possibly more serious, activity from this person.

(7) Evidence of Active Targeting:
This attack was targeted at our Firewall.

(8) Severity:
Criticality = 5 (firewall targeted)
Lethality = 2 (recon mission)
System C ountermeasures = 5 (all recent and applicable patches installed)
Network Countermeasures = 4 (firewall listens to no unauthenticated packets (unless for purpose of vpn authentication) sent to it directly)
THE VERDICT: -2 = (5+2) - (5+4)

(9) Defensive recommendations:
A: Inform the ISP of the users activity
B: block and drop all packets from outside the network destined for the Firewall
C: If attacker continues with this or other suspicious activity and IP is consistent, block the users up
(Note: All of the above actions have indeed been taken)

(10) Multiple Choice Question:

The above attack is characteristic of...
a) A DoS attack
b) A Port scan
c) A covert data channel (tunneling)
d) An attack to port 1032
Answer: b

##############
Detect.2
##############

date	time	dst.port	src.ip	dest.ip	proto	src.port	other.info
"4Jun2000"	"18:11:20"	"31789"	"2 12.102.0.152"	"x.x.x.51"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.54"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.62"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20 "	"31789"	"212.102.0.152"	"x.x.x.57"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.58"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.60"	"udp"	"31790"	" len 29"
"4Jun20 00"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.56"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.59"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.61"	"udp"	"31790"	" len 29"
"4Jun2000"	"18:11:20"	"31789"	"212.102.0.152"	"x.x.x.63"	"udp"	"31790"	" len 29"

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall log's

(3) Probability the source address was spoofed:
Very Low. Due to type of attack, in order to know of success the source IP must be valid and controlled by the attacker.

(4) Description of Attack:
This is an attempt to scan the entire x.x.x.x \26 network for possibl e "Hack -a-tack" Trojan installed on the network and listening on the 31789.

(5) Attack Mechanism:
The Hack -a-tack software has a built in scanner to scan for other trojaned machines.

Port 31790 serves as a transfer port while port 31789 the control.

(6) Correlations:

The Hack-a-tack Trojan (www.hack-a-tack.com) is well known and listed on many public Port and Trojan lists:
http://www.robertgraham.com/pubs/firewall-seen.html
http://www.wittys.com/files/all-ip-numbers.txt
http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html

(7) Evidence of Active Targeting:

This scan was not targeted at one particular machine and it is not clear if our network was the target for this scan or just apart of a much larger group of possible victim's scanned. Considering that the attacker doesn't seem to be trying to be at all stealthy it is likely that this is just a small view of a much larger scan for Trojaned machines on other networks.

(8) Severity:

```
Criticality = 5              (scan of both critical and not so critical systems)
Lethality = 3                (Successful attack (which this one was not) does not
                               normaly result in anything more than current user rights to
                              trojaned system)
System Countermeasures = 5   (no trojan installed on any of the IP's)
Network Countermeasures = 5  (restrictive firewall policy  which only allows specified
                              ports)
THE VERDICT:  -2 = (5+3)  - (5+5)
```

(9) Defensive recommendations:

A: Block all incoming and outgoing connections to or from ports 31790 or 31789
B: If consistent activity is seen from this IP contact the owner and inform them of the activity
C: If attacker continues with this or other suspicious activity and IP is consistent, block the users IP
D: proactively scan network for known b ackdoors
(Note: All of the above actions have indeed been taken)

(10) Multiple Choice Question:

The above attack is characteristic of...

a) An attempt to create network map
b) IP Frag DoS attack
c) Known trojan's s can
d) Attempt to crash machine with the '4Jun' bug

Answer: c

```
#############
# Detect.3  #
#############
   date        time     dst.port     src.ip           dest.ip    proto  src.port  other.info
"9Jun2000"  "14:07:44"  "nbname"  "192.0.0.1"         "x.x.x.51"  "udp"  "nbname"  " len 78"
"9Jun2000"  "14:07:44"  "nbname"  "207.221.192.161"  "x.x.x.51"  "udp"  "1030"    " len 78"
"9Jun2000"  "14:08:41"  "nbname"  "192.0.0.1"        "x.x.x.56"  "udp"  "nbname"  " len 78"
"9Jun2000"  "14:08:41"  "nb name"  "207.221.192.161"  "x.x.x.56"  "udp"  "1030"    " len 78"
"9Jun2000"  "14:09:02"  "nbname"  "207.221.192.161"  "x.x.x.58"  "udp"  "1030"    " len 78"
"9Jun2000"  "14:09:03"  "nbname"  "192.0.0.1"        "x.x.x.58"  "udp"  "nbname"  " len 78"
"9Jun2000"  "14:09:12"  "nbname"  "192.0.0.1"        "x.x.x.59"  "udp"  "nbname"  " len 78"
"9Jun2000"  "14:09:12"  "nbname"  "207.221.192.161"  "x.x.x.59"  "udp"  "1030"    " len 78"
"9Jun2000"  "14:09:23"  "nbname"  "192.0.0.1"        "x.x.x.60"  "udp"  "nbname   "  " len 78"
"9Jun2000"  "14:09:23"  "nbname"  "207.221.192.161"  "x.x.x.60"  "udp"  "1030"    " len 78"
```

```
"9Jun2000"  "14:09:34"  "nbname"  "192.0.0.1"        "x.x.x.61"  "udp"  "nbname"  " len 78"
"9Jun2000"  "14:09:34"  "nbname"  "207.221.192.161"  "x.x.x   .61"  "udp"  "1030"    " len 78"
"9Jun2000"  "14:09:45"  "nbname"  "192.0.0.1"        "x.x.x.62"  "udp"  "nbname"  " len 78"
"9Jun2000"  "14:09:45"  "nbname"  "207.221.192.161"  "x.x.x.62"  "udp"  "1030"    " len 78"
"9Jun2000"  "14:09:59"  "nbname"  "192.  0.0.1"        "x.x.x.63"  "udp"  "nbname"  " len 78"
"9Jun2000"  "14:09:59"  "nbname"  "207.221.192.161"  "x.x.x.63"  "udp"  "1030"    " len 78"
```

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall logs.

(3) Probability the source address was spoofed:
High. There are two IP addresses shown. 192.0.0.1 is for certain spoofed. 192.0.0.1 is an address within a one of the IANA reserved blocks (as reported by whois). 207 .221.192.161 I believe to be spoofed as it returned an echo -reply around the time of the scan. 207.221.192.161 belongs to Netcom/Mindspring, a very large generic internet services provider in the US.

(4) Description of Attack:
It look's like a script kiddy that just learned perl. I suspect that the initial request from 192.0.0.1 is generated by a DoS or scan script and the second is request from the attacker at his linux or unix terminal (perhaps also generated by a script). Do to the speed of the scan this seems like an attempt to cause massive havoc in the Internet using common DoS attack's against Windows and NetBIOS enabled machines. Though I'm not absolute on this fact, I believe the s econd request from the valid IP was just for verification and statistical purposes (to feed the ego). Another possibility is that the attacker is just trying to gather information about this network.

(5) Attack Mechanism:
After ch ecking the CVE database for possible leads on matching this pattern (spoofed ip then legit ip requests) to an exact script or tool used, I was unable to find any leads. I didn't find any public script that spoofs the IP of an outgoing packe t during a attack directed at a NetBIOS machine. I suspect that the script used is homegrown (from scratch or an edit of some other script). Also, because there is no IDS or sniffer setup on this network I could not get more infor mation about this attack (by looking at the data load).

(6) Correlations:
I've seen many different DoS attacks towards NetBIOS enable services/machines exposed over the past few years. It is likely that the above is attempt to cau se mass DoS havoc.

(7) Evidence of Active Targeting:
I don't believe this network is the focus of the attack. The attacker took no steps to hide themselves (sending requests at a fast pace). Instead, I believe that this networks IP's were apart of a larger pool of IP's on the attackers list to scan and/or attack.

(8) Severity:

Criticality = 3	(non discriminate scan against multiple IP's, most which having no thing listening and some that have servers listening)
Lethality = 3	(Had attack been successful, system halt would've been result)
System Countermeasure s = 5	(latest patches installed)
Network Countermeasures = 5	(restrictive firewall policy which only allows specified ports, NetBIOS is not specified)

THE VERDICT: -4 = (3+3) - (5+5)

(9) Defensive reco mmendations:
A: Block all incoming NetBIOS traffic to the network
B: Inform the ISP of the users activity
C: Setup IDS to become suspicious (cause alert) on any incoming NetBIOS (port 137 -139) traffic
(Note: All of the above actions but 'b' have indeed been taken)

(10) Multiple Choice Question:

Considering the source IP's of the packet stream...
a) This is a coordinated attack across multiple hosts
b) 192.0.0.1 shows packets from a tool on a compromised router while 207.221.192.161 is probably spoofed
c) 207.221.192.161 shows packets coming from the attacker's host while 192.0.0.1 is probably spoofed.
d) None of the Above
Answer: c

```
#############
# Detect.4  #
#############
   date        time     dst.port     src.ip       dest.ip     proto  src.port other.info
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.51"  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.54"  "udp   "  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.56"  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.57"  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.58  "  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.59"  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.60"  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x  .x.61"  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:10"  "28431"  "212.26.77.91"  "x.x.x.62"  "udp"  "28432"  " len 29"
"8Jun2000"  " 2:45:11"  "28431"  "212.26.77.91"  "x.x.x.63"  "udp"  "28432"  " len 29"
"9Jun2000"  " 0:30:03"  "28431"  "212.26.77.250"    "x.x.x.51"  "udp"  "28432"  " len 29"
  <snip>
"9Jun2000"  " 0:30:03"  "28431"  "212.26.77.250"  "x.x.x.63"  "udp"  "28432"  " len 29"
"9Jun2000"  " 1:29:56"  "28431"  "212.156.66.8"  "x.x.x.51"  "udp"  "28432"  " len 29"
  <snip>
"9Jun2000"  " 1:29:56"   "28431"  "212.156.66.8"  "x.x.x.63"  "udp"  "28432"  " len 29"
"9Jun2000"  " 3:30:39"  "28431"  "212.26.77.54"  "x.x.x.51"  "udp"  "28432"  " len 29"
  <snip>
"9Jun2000"  " 3:30:39"  "28431"  "212.26.77.54"  "x.x.x.63"  "udp"  "28432"  " len 29"
"10Jun2000"  " 0:46:17"  "28431"  "212.26.77.82"  "x.x.x.51"  "udp"  "28432"  " len 29"
  <snip>
"10Jun2000"  " 0:46:18"  "28431"  "212.26.77.82"  "x.x.x.58"  "udp"  "28432"  " len 29"
```

(1) Source of Trace:
A network that I monitor

(2) Detect was generate d by:
Checkpoint FW -1 firewall logs.

(3) Probability the source address was spoofed:
Low. I believe that the attacker is looking to get a response.
IP addressing info: 212.26.77.91, 212.26.77.250, 212.26.77.54, 212.26.77.82 = Saud i Arabia
"Saudi Arabia backbone and local registry address space"
While tremping through whois data I also noticed several referenced contacts from .gov.se addresses. Source IP's are probably remotely compromised hosts.

(4) Description of Attack:
The patterns shown with the above scans are an example of the Hack -a-tack Trojan scans mentioned earlier except the source and destination port have been changed.

(5) Attack Mechanism:
This is a typical ba ckdoor/trojan scan. It is my belief that this is a scan from a Hack-A-Tack Trojan client (which has a built in scanner for this exact purpose).

(6) Correlations:
While searching through many Internet sources I was unable to find much more than ot her people confirming that they too saw this suspicious activity. One other source agreed with the - Hack-A-Tack over different src/dst ports - theory:
http://www.securityfocus.com/templates/archive.pike?list=75&date=2000 -03-1&msg=1390.952607249@SURFnet.nl

(7) Evidence of Active Targeting:
Due to the fast rate of this scan, I believe that our IP's are apart of a large pool of IP's being scanned by the attacker.

(8) Severity:

Criticality = 3	(non discriminate scan against multiple IP's, most which having nothing listening and some that have servers listening)
Lethality = 3	(Successful attack (which this one was not) does not normally result in anything more than current user rights to trojaned system)
System Countermeasures = 5	(latest patches installed)
Network Countermeasures = 5	(restrictive firewall policy which only allows specified ports, NetBIOS is not specifi ed)

THE VERDICT: -4 = (3+3) - (5+5)

(9) Defensive recommendations:
A: Block all incoming traffic with destination port's above 1023 or block communication to/from port's 28431 and 28432.
B: Inform the sources Technical Cont act of the users activity
C: Confirm that Hack -a-tack and other Trojan's are not installed on the network.
(Note: All of the above actions have indeed been taken)

(10) Multiple Choice Question:

What is the above traffic most familiar with ?
a) A traceroute from a Unix client
b) DDoS attempt
c) Attempt to map Network Addressing structure
d) Scan for possible Hack -A-tack Trojan servers
Answer: d


```
#############
# Detect.5  #
#############
   date       time      dst.port     src.ip          dest.ip   proto  src.port other.info
"5Jun2000"  "10:12:50"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "12852"  " len 647"
"5Jun2000"  "10:14:01"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "14559"  " len 647"
"5Jun2000"  "10:15:33"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "11116"  " len 647"
"5Jun2000"  "10:18:29"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "19086"  " len 647"
"5Jun2000"  "10:23:11"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "26700"  " len 647"
"5Jun2000"  "10:27:00"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "13332"  " len 647"
"5Jun2000"  "10:31:59"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "25352"  " len 647"
```

```
"5Jun2000"  "10:36:58"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "10992"     " len 647"
"5Jun2000"  "10:38:08"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "19086"   " len 647"
"5Jun2000"  "10:46:24"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "18219"   " len 647"
"5Jun2000"  "10:46:59"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp   "  "17738"  " len 647"
"5Jun2000"  "10:48:59"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "19086"   " len 647"
"5Jun2000"  "10:54:08"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "11472"   " len 647"
"5Jun2000"  "10:59:22"  "6970"  "205.188.244.44"  "x.x.  x.54"  "udp"  "24964"  " len 647"
"5Jun2000"  "11:03:28"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "31710"   " len 647"
"5Jun2000"  "11:09:50"  "6970"  "205.188.244.44"  "x.x.x.54"  "udp"  "20822"   " len 647"
"5Jun2000"  "11:14:16"  "6970"  "205.188.244  .44"  "x.x.x.54"  "udp"  "8295"    " len 647"
"5Jun2000"  "11:37:23"  "6970"  "205.188.244.135" "x.x.x.54"  "udp"  "24484"   " len 647"
  <snip... cut 5 packets>
"5Jun2000"  "12:06:40"  "6970"  "205.188.244.135" "x.x.x.54"  "udp"  "9736"    " len 647"
"5Jun2000"  "12:09:41"  "6970"  "205.188.246.81"  "x.x.x.54"  "udp"  "21786"   " len 647"
  <snip... cut 18 packets>
"5Jun2000"  "17:51:44"  "6970"  "205.188.246.81"  "x.x.x.54"  "udp"  "21400"   " len 647"
"5Jun2000"  "17:55:01"  "6970"  "205.188.244.141" "x.x.x.5   4"  "udp"  "28535"  " len 647"
  <snip... cut 9 packets>
"5Jun2000"  "18:21:32"  "6970"  "205.188.244.141" "x.x.x.54"  "udp"  "25759"   " len 647"
"5Jun2000"  "18:25:11"  "6970"  "205.188.246.79"  "x.x.x.54"  "udp"  "23623"   " len 647"
  <snip... cut 7 pack ets>
"5Jun2000"  "18:53:14"  "6970"  "205.188.246.79"  "x.x.x.54"  "udp"  "27521"   " len 647"
```

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall logs. Groups of lines were cut from the log for clarity.

(3) Probability the source address was spoofed:
Low. Due to the connection oriented nature of this particular attack.

Note: A whole stream of sporadic behavior like that show above continue in the log's over a period of 3 days with a different IP each time.

The follow is a complete list of the IP's used and relevant whois data:
205.188.244.44, 205.188.244.135, 205.188.246.81, 205.188.244.141, 205.188.246.79 = AOL
AOL controls 205.188.x.x. There was another 16 log streams from other AOL addresses in this Class B range that were not show above.

(4) Description of Attack:
Three possible explanations for this detect:
1) This is a scan for the GateCrasher T rojan horse.
2) This is backwash from RealAudio/Video activity
3) This is a DoS attack against RealAudio/Video servers

So which is it?
1: while playing around with the GateCrasher trojan (to determine it's characteristics and capabilities, such as "does it have a built in scanner?")... I didn't see any characteristics that would cause such a large stream of requests.
2: Older versions of RealAudio/Video used ports 6970 -7170 for communication with RealAudio/Video servers. However, most of the source IP's return nothing from my fingerprinting attempts (`nmap -O') and no echo -reply so I doubt they are Audio or Video servers themselves. It is also possible that someone or a group of people think x.x.x.54 has a RealAudio/Video stream.
3: The DoS attacks that I have run across concerning RealAudio/Video do not directly relate to port 6970 except for maybe the pnserver exploit (see www.rootshell.com and CAN -1999-0271 at cve.mitre.org) or the ramgen exploit (http://www.securityfocus.com/bid/888). Both of these exploits use static source ports (unlike those in the detect).

My conclusion: Assume the worse but think realistically. Assume this was an attempted scan for GateCrasher even though the traffic looks more like external clients thinking x.x.x.54 is a RealAudio/Vide o server.

(5) Attack Mechanism:
Assuming this is a GateCrasher attack... GateCrasher uses 6969 but 6970 has also been found to be a common port used. The Trojan can be installed by opening a word document (e.g.: attached to an ema il) or plain executable. Upon installation it creates an executable called "explore.exe" and places a reference to itself in the Registry (the Run key) to startup at boot. Upon connection from client, client can do pretty much wha tever they want (within bounds of the permissions for the current logged in user).

(6) Correlations:
Both the SANS port list (http://www.sans.org/newlook/resources/IDFAQ/oddp orts.htm) and the popular Nyheter Trojan list (http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html) list 6970 as a common port for GateCrash a ctivity.

(7) Evidence of Active Targeting:
This attack was targeted at our Firewall.

(8) Severity:
Criticality = 5 (directed at firewall)
Lethality = 2 (GateCrash = 3, RealAudio DoS = 3, RealAudio streami ng = 0)
System Countermeasures = 5 (this (and all other) trojan's are not on this machine)
Network Countermeasures = 5 (firewall listens to no unauthenticated packets (unless for purpose of vpn authenti cation) sent to it directly)
THE VERDICT: -3 = (5+2) - (5+5)

(9) Defensive recommendations:
A: Block all incoming traffic to firewall from the outside
C: Scan network and be sure that the GateCrasher Trojan is not installed and che ck each machine for explore.exe in registry or startup folders
D: Setup a sniffer or IDS system (to save me 3 hours of my time by allowing me to look at more than just or more of the headers)
E: If RealAudio/Video server(s) exist on network, install valid patches found from Real Networks
(Note: All of the above actions excluding 'd' have indeed been taken, and there are no RealAudio/Video servers on this network)

(10) Multiple Choice Question:

The above attack is most characteristic of...
a) A DoS attack to the service running on port 6970
b) A reverse port scan
c) GateCrasher scan or connection request
d) A and C
Answer: D


```
#############
# Detect.6  #
#############
   date        time   dst.port  src.ip      dest.ip    proto  src.port other.info
"7Jun2000"  "10:41:24"  "98"  "127.0.0.1"  "x.x.x.51"  "tcp"  "16356"  " len 40"
"7Jun2000"  "10:41:24"  "98"  "127.0.0.1"  "x.x.x.54"  "tcp"  "16356"  " len 40"
"7Jun2000"  " 10:41:24"  "98"  "127.0.0.1"  "x.x.x.56"  "tcp"  "16356"  " len 40"
"7Jun2000"  "10:41:24"  "98"  "127.0.0.1"  "x.x.x.57"  "tcp"  "16356"  " len 40"
"7Jun2000"  "10:41:24"  "98"  "127.0.0.1"  "x.x.x.58"  "tcp"  "16356"  " len 40"
"7Jun2000"  "10:41:24"  "9 8"  "127.0.0.1"  "x.x.x.59"  "tcp"  "16356"  " len 40"
```

```
"7Jun2000"  "10:41:24"  "98"  "127.0.0.1"  "x.x.x.60"  "tcp"  "16356"  " len 40"
"7Jun2000"  "10:41:24"  "98"  "127.0.0.1"  "x.x.x.61"  "tcp"  "16356"  " len 40"
"7Jun2000"  "10:41:24"  "98"  "127.0.0.  1"  "x.x.x.62"  "tcp"  "16356"  " len 40"
"7Jun2000"  "10:41:24"  "98"  "127.0.0.1"  "x.x.x.63"  "tcp"  "16356"  " len 40"
```

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall logs.

(3) Probability the source address was spoofed:
High. 127.0.0.1 is not a valid network and Internet address. 127.0.0.1 is reserved and refers to the *localhost*.

(4) Description of Attack:
Example of a cracker taking a perfectly reasonab le exploit and totally bulaking it up. The intention of this attack seems to be 1) exploit the *theoretical* linuxconf buffer overflow (CAN -2000-0017). and 2) circumvent restrictions on port 98 only allowing access from localhost (127.0.0.1)

Whether the Linuxconf Buffer Overflow is real or not, these packets are being sent over TCP port 98 (as they should be for an http service) which connection oriented. This means that the destination would drop the packe t immediately (seeing that it is coming from ITSELF but from the Ethernet and not loopback interface). Of course, that is assuming that the Linux kernel is fully RFC complaint (sorry, I haven't trumped through the code to verify th is just yet).

Another reason that this attack will fail is that none of the IP's scanned belonged to linux machines. And, Linuxconf only runs on... well, Linux.

It is also possible that this is an attempted Linuxconf LANG value D oS attack discussed in the "Red Hat Linux 5.1 linuxconf bug" BugTraq thread. The same rules/problems already mentioned above apply to this attack as well.

(5) Attack Mechanism:
The code for this theoretical buffer overflow can be found in the message titled "(Possible) Linuxconf Remote Buffer Overflow Vulnerability" Dec 20 1999. It supposedly exploits a bounds checking problem with the way the http daemon for Linuxconf port/98 handles headers.

(6) Correlat ions:
This buffer overflow attack was mentioned in the SecurityFocus.com Incidents mailing list and later in Bugtraq. A good follow -up claiming that the exploit was theoretical was posted at:
http://lwn.net/1999/1223/a/linuxconfresponse.html
Exploit code FOR TESTING was posted in BugTraq message titled "(Possible) Linuxconf Remote Buffer Overflow Vulnerability" Dec 20 1999.

(7) Evidence of A ctive Targeting:
Considering the rate at which these packets were being sent I believe that the above IP range was just apart of a much large pool the attacker was scanning or attacking.

(8) Severity:

Criticality = 3	(non disc riminate scan against multiple IP's, most which having nothing listening and some that have servers listening)
Lethality = 5	(Linuxconf is a system config utility and common exploit could result in remote root access)
System Countermeasures = 5	(None of the listening machines run Linuxconf)
Network Countermeasures = 5	(Firewall blocks port anyway)

THE VERDICT: -2 = (3+5) - (5+5)

(9) Defensive recommendations:
a: Block all incoming traffic to firewall from the outside (for at least port 98)
d: Don't run Linuxconf on external machines!
(Note: All of the above actions have indeed been taken)

(10) Multiple Choice Question:

The above attack is most characteristic of...
a) a buffer overflow or DoS attempt directed at Linuxconf machines
b) "Land" DoS attack
c) Network map attempt (for all hosts with port 98 open)
d) Overlapping Fragmented packet's
Answer: a

Netbus

```
#############
# Detect.7  #
#############
   date        time     dst.port   src.ip          dest.ip    proto src.port other.info
"4Jun2000"  "23:24:40"  "12345"  "64.228.80.47"  "x.x.x.51"  "tcp"  "4716"  " len 48"
"4Jun2000"  "23:24:54"  "12345"  "64.228.80.47"  "x.x.x.54"  "tcp"  "4719"  " len 48"
"4Jun2000"  "23:25:06"  "12345"  "64.228.80.47"  "x.x.x.56"  "tcp"  "4721"  " len 48"
"4Jun2000"  "23:25:10"  "12345"  "64.228.80.47"  "x.x.x.57"  "tcp"  "4722"  " len 48"
"4Jun2000"  "23:25:15"  "12345"  "64.228.80.47"  "x.x.x.58"  "tcp"  "4723"  " len 48"
"4Jun2000"  "23:25:21"  "12345"  "64.228.80.47"  "x.x.x.59"  "tcp"  "4724"  " len 48"
"4Jun2000"  "23:25:26"  "12345"  "64.228.80.47"  "x.x.x.60"  "tcp"  "4725"  " len 48"
"4Jun2000"  "23:25:30"  "12345"  "64.228.80.47"  "x.x.x.61"  "tcp"  "4726"  " len 48"
"4Jun2000"  "23:25:35"  "12345"  "64.228.80.47"  "x.x.x.62"  "tcp"  "4727"  " len 48"
"4Jun2000"  "23:25:41"  "12345"  "64.228.80.47"  "x.x.x.63"  "tcp"  "4728"  " len 48"
```

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall logs.

(3) Probability the source address was spoofed:
Low, due to the type of attack and that 'src.ip' responds to icmp echo (ping) requests.

(4) Description of Attack:
Attacker is scanning entire network for the NetBus backdoor.

(5) Attack Mechanism:
If attacker were to find port 12345, 12346 or 20034 (NetBus ports) open he would probably try to connect to that port using the NetBus client. Of the backdoors for windows today, NetBus is amongst the most popular. If successfully installed the remote attacker connecting to a NetBus server will have the same permissions of the current logged in user.

(6) Correlations:
There are several port lists that point this NetBus port out (including the SANS list)

(7) Evidence of Active Targeting:
It is not clear if this was a scan of just our network or if our IP's were just apart of a larger pool being scanned. Plus, no real attempt to stealth the scan was made.

(8) Severity:

Criticality = 3 (non discriminate scan against multiple IP's, most which having nothing lis tening and some that have servers listening)

Lethality = 3 (Successful attack (which this one was not) does not normally result in anything more than current us er rights to trojaned system)

System Countermeasures = 5 (None of the listening machines have this (or any other) trojan)

Network Countermeasures = 5 (Firewall blocks po rt anyway)

THE VERDICT: -4 = (3+3) - (5+5)

(9) Defensive recommendations:

a: Block all incoming traffic to firewall from the outside (for at least port 12345, 12346 and 20034)

d: Regularly scan network and servers/workstati ons for open backdoors.

(Note: All of the above actions have indeed been taken)

(10) Multiple Choice Question:

The above attack is most characteristic of...

a) A scan for a well -known Backdoor
b) Reverse Network mapping attempt
c) DoS attack
d) none of the above

Answer: a


```
#############
# Detect.8  #
#############
   date        time     dst.port      src.ip         dest.ip    proto src.port other.info
"3Oct1999"  "20:30:09"  "telnet"  "130.161.149.95"  "x.x.x.62"     "tcp"  "24660"  " len 44"
"3Oct1999"  "20:30:12"  "telnet"  "130.161.149.95"  "x.x.x.54"  "tcp"  "24662"  " len 44"
"3Oct1999"  "20:31:42"  "telnet"  "130.161.149.95"  "x.x.x.62"  "tcp"  "24660"  " len 44"
"3Oct1999"  "20:31:45"  "telnet"  "130.161.149.9  5"  "x.x.x.54"  "tcp"  "24662"  " len 44"
"3Oct1999"  "20:33:18"  "telnet"  "130.161.149.95"  "x.x.x.62"  "tcp"  "24660"  " len 44"
"3Oct1999"  "20:33:18"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "866"  " len 44"
"3Oct1999"  "20:33:21"  "telnet"  "1 30.161.149.95"  "x.x.x.54"  "tcp"  "24662"  " len 44"
"3Oct1999"  "20:33:21"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "867"  " len 44"
"3Oct1999"  "20:33:33"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "868"  " len 44"
"3Oct1999"  "20:33:36"  "s unrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "869"  " len 44"
"3Oct1999"  "20:33:48"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "870"  " len 44"
"3Oct1999"  "20:33:51"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "871"  " len 44"
"3Oct1999"  "20:34 :03"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "872"  " len 44"
"3Oct1999"  "20:34:06"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "873"  " len 44"
"3Oct1999"  "20:34:18"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "874"  " len 44"
"3Oct1999"  "20:34:21"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "875"  " len 44"
"3Oct1999"  "20:34:33"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "876"  " len 44"
"3Oct1999"  "20:34:36"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "877"  " len 44"
"3Oct1999"  "20:34:48"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "878"  " len 44"
"3Oct1999"  "20:34:51"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "879"  " len 44"
"5Oct1999"  "10:10:50"  "telnet"  "130.161.149.95"  "x.x.x.62"  "tcp"  "3189"  " l   en 44"
"5Oct1999"  "10:11:02"  "telnet"  "130.161.149.95"  "x.x.x.54"  "tcp"  "3190"  " len 44"
"5Oct1999"  "10:12:23"  "telnet"  "130.161.149.95"  "x.x.x.62"  "tcp"  "3189"  " len 44"
"5Oct1999"  "10:12:35"  "telnet"  "130.161.149.95"  "x.x.x.54"  "tcp"     "3190"  " len 44"
"5Oct1999"  "10:13:59"  "telnet"  "130.161.149.95"  "x.x.x.62"  "tcp"  "3189"  " len 44"
"5Oct1999"  "10:13:59"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "734"  " len 44"
"5Oct1999"  "10:14:12"  "telnet"  "130.161.149.95"  "x.x.x.54  "  "tcp"  "3190"  " len 44"
"5Oct1999"  "10:14:12"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "736"  " len 44"
```

```
"5Oct1999"  "10:14:14"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "737"  " len 44"
"5Oct1999"  "10:14:27"  "sunrpc"  "130.161.149.95"    "x.x.x.54"  "tcp"  "739"  " len 44"
"5Oct1999"  "10:14:29"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "740"  " len 44"
"5Oct1999"  "10:14:41"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "742"  " len 44"
"5Oct1999"  "10:14:44"  "sunrpc"  "130.161.1  49.95"  "x.x.x.62"  "tcp"  "743"  " len 44"
"5Oct1999"  "10:14:56"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "745"  " len 44"
"5Oct1999"  "10:14:59"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "746"  " len 44"
"5Oct1999"  "10:15:12"  "sunrpc"  "1  30.161.149.95"  "x.x.x.54"  "tcp"  "747"  " len 44"
"5Oct1999"  "10:15:14"  "sunrpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "748"  " len 44"
"5Oct1999"  "10:15:26"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "749"  " len 44"
"5Oct1999"  "10:15:29"  "sun rpc"  "130.161.149.95"  "x.x.x.62"  "tcp"  "kerberos  -tcp"  " len 44"
"5Oct1999"  "10:15:41"  "sunrpc"  "130.161.149.95"  "x.x.x.54"  "tcp"  "751"  " len 44"
```

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkp oint FW-1 firewall logs.

(3) Probability the source address was spoofed:
Low. Though that depends on the type of attack. Note: the IP listed belongs to a University in the Netherlands and it responds to icmp echo (ping) requests.

(4) De scription of Attack:
This is most likely a recon. attempt against our network. It is not clear but I believe the attacker used another host to map IP's that are alive as he/she only sends these packets to the two IP's that are aliv e on my external network (meaning, they already knew which machines were up) because I didn't see any other requests from this or other similar IP's. It could also be possible that this is a direct attack on a rpc service but I dou bt it considering the intermixed telnet session requests. I believe that this is an attempt to grab login banners and rpcinfo for system finger printing.

(5) Attack Mechanism:
After finding an open rpc service the attacker would most like ly begin to attack this service. There are many well -known security problems with rpc oriented daemons (see #6). Or, if this is a simple scan for info than more activity could be possible from this attacker.

(6) Correlations:
I don't remember where or when I learned about rpc reconnaissance so I'd say that it is common knowledge (just try 'rpcinfo -p <server>' from any unix host). Beyond simple recon, there are many exploits and problems with rpc daemons tha t can give users remote access to the machine or be used for a type of DoS attack (CVE -1999-0168, http://xforce.iss.net/static/2308.php , Bugtrack: "(spoofed) RPC portmapper set/unset" Fri Nov 13 1998... and the list goes on and on) .

(7) Evidence of Active Targeting:
Both our firewall and our mail server were targeted.

(8) Severity:
```
Criticality = 5             (Directed at mail server and firewall)
Letha lity = 5               (well known root access exploits possible)
System Countermeasures = 5  (None of the listening machines have any rpc programs '.'
                             and latest patches installed)
Network Countermeasur es = 5 (Firewall blocks port anyway)
THE VERDICT: 0 = (5+5)  - (5+5)
```

(9) Defensive recommendations:
a: Block all incoming traffic to firewall from the outside (for at least port 111, 23 and any other rpc related ports)
d: As most r pc holes are old, you should have the proper patches already installed. If

not, install them.
(Note: All of the above actions have indeed been taken)

(10) Multiple Choice Question:

The above attack is most characteristic of...
a) An att empt to login to machine by brute forcing the username/passwd combo through telnet
b) Attempt to gather info about target using 'telnet' and 'rpcinfo'
c) a TCP SYN/ACK DoS attack
d) IP Fragmenting DoS attack
Answer: b

#############
Detect.9
#############
Note: '#.#.#' is attacker and 'x.x.x' is us (victim). This was done because the attacker is coming from a client at the same upstream provider as us.

date	time	dst.port	src.ip	dest.ip	proto	src.port	other.info
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.51"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.54"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.56"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.57"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.57"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.58"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.58"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.60"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.61"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.61"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.62"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.62"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14: 08"	"22"	"#.#.#.68"	"x.x.x.51"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632"	"#.#.#.68"	"x.x.x.63"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.54"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"5632 "	"#.#.#.68"	"x.x.x.59"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.56"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.60"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#. 68"	"x.x.x.63"	"udp"	"1075"	" len 30"
"23Dec1999"	"16:14:08"	"22"	"#.#.#.68"	"x.x.x.59"	"udp"	"1075"	" len 30"

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall logs.

(3) Probability the source address was spoofed:
Low - I believe that the attacker wishes to receive a response. Note: The source IP of this detect belongs to a government office in the same country (which shall remain nameless) as our ne twork.

(4) Description of Attack:
Port 22 and 5632 UDP are used by PCAnywhere (v8, a remote administration tool). This is possibly a scan for PCAnywhere. It is also possible that this is a DoS attack. Attack would be carried out by sending connection requests and stopping before it has a chance to fully finish the authentication process (see section 6). However, I imagine (I don't know exactly how PCAnywhere uses TCP) that the whole authentication process is done over

one port address, which is not what is going above (geeze, I wish I had a sniffer during this one).

(5) Attack Mechanism:
If the attacker finds a machine with these ports open what will come next is either a DoS attac k, exploit of an application bug or simple brute force attempt to login to PCAnwhere (see section 6).

(6) Correlations:
http://www.securityfocus.com/bid/1095 (possible DoS attack again st PCAnywhere)
http://www.securityfocus.com/bid/1093 (sniffing out usernames/passwords due to Weak Encryption Vulnerability)

(7) Evidence of Active Targeting:
Our external netw ork was targeted. Though, it is possible (due to the rate at which the attacker is sending the packets) that our IP's are apart of a larger pool being scanned.

(8) Severity:
Criticality = 3 (non discriminate scan against multi ple IP's, most which having nothing listening and some that have servers listening)
Lethality = 4 (Successful attack (which this one was not) does not normally result in user access and possibly more)
System Countermeasures = 5 (None of the listening machines have this, or any other, such program)
Network Countermeasures = 5 (Firewall blocks ports 22 and 5632 anyway)
THE VERDICT: -3 = (3+4) - (5+5)

(9) Defensive recommendations:
a: Block all incoming traffic to firewall from the outside (for at least port 22 and port 563)
d: Install proper p atches for PCAnywhere that are provided by Symantec
(Note: 'a' has been taken and we don't currently run PCAnywhere on any machines)

(10) Multiple Choice Question:

The above attack is most characteristic of...
a) attempt to find open port s for SSH
b) attempt to gain access through ssh by brute forcing the username and password
c) common exploit against the ftp data channel
d) attempt to find a PCAnywhere server
Answer: D


```
#############
# Detect.10 #
############ #
   date        time     dst.port      src.ip          dest.ip    proto  src.port other.info
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.54"  "tcp"  "65535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.56"  "tcp"  "6   5535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.57"  "tcp"  "65535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.58"  "tcp"  "65535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.  59"  "tcp"  "65535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.60"  "tcp"  "65535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.61"  "tcp"  "65535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208 .120"  "x.x.x.62"  "tcp"  "65535"  " len 40"
"15Feb2000"  " 3:29:42"  "imap"  "209.218.208.120"  "x.x.x.63"  "tcp"  "65535"  " len 40"
```

(1) Source of Trace:
A network that I monitor

(2) Detect was generated by:
Checkpoint FW -1 firewall lo gs.

(3) Probability the source address was spoofed:
High, due patterns seen from other sources (see #6).

(4) Description of Attack:
IMAP is a messaging/email protocol. Most of your modern and more popular mail servers now support at least IMAP, POP3 and SMTP. Over time many security problems have been found with different IMAP servers. I suspect the above attack is an attempt to gain root access by exploiting a well -known buffer overflow (see #6). Many others wh o watched this attack happen on their network noticed and claim that the source IP was spoofed. It is believed that the attacker may be running a sniffer on the Spoofed IP's network to continue communicating with the victim and sti ll be able to see the responses coming from the victim. The reason I attribute this detect to that attack is that the source port was also common amongst many attacks.

(5) Attack Mechanism:
Code to exploit this remote buffer overfl ow can be found at
http://www.securityfocus.com/bid/130
Bugtraq explains the problem as being in the IMAP Authentication type value sent during the initial connection.
"The value passed to the authenticate command is copied into a buffer of size 1024. The maximum size of this value, however, it 8192 characters. A failure to bound the read value to 1024 results in a buffer overflow." - BugTraq ID: 130

(6) Correlations:
http://www.cert.org/incident notes/IN -98-05.html
originally found out about this exploit through CERT. You'll find there some details on a possible buffer ove rflow attack to gain root access and a common patterns noticed. You can also check out the CVE entry for this exploit (CVE -1999-0005) or the mention on Bugtraq (http://www.securityfocus. com/bid/130).
http://cve.mitre.org/cgi -bin/cvekey.cgi?keyword=imap
A list of more IMAP related security vulnerabilities... a few of which could possibly apply to the de tect above.

(7) Evidence of Active Targeting:
Our external network was targeted. Though, it is possible (due to the rate at which the attacker is sending the packets) that our IP's are apart of a larger pool being scanned.

(8) Severity:
Criticality = 3 (non discriminate scan against multiple IP's, most which having nothing listening and some that have servers listening)
Lethality = 5 (could result in root on remote machine)
System Countermeasures = 5 (Our mail server happens to not be popular and doesn't support IMAP)
Network Countermeasures = 5 (Firewall blocks port anywa y)
THE VERDICT: -2 = (3+5) - (5+5)

(9) Defensive recommendations:
a: Consult the creator or vendor of the particular IMAP server software that you use and install the proper patches.
d: Block all IMAP communication on the f irewall
(Note: We have no IMAP servers on our network)

(10) Multiple Choice Question:

```
The above attack is most characteristic of...
        a) Possible IMAP exploit or DoS attack
        b) Port Scan
        c) Network map
        d) Port Scan an d network map
Answer: A
```