GIAC
CERTIFICATIONS

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 permited 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

*** Northcutt, very professional, concise, accurate, variety of sources, research includes resolution in several cases. There are pointers to attacks. 92 *

GIAC Certification Practical

10 Detects with Analyses

Viriya Upatising

April 24, 2000

I&W methodology

Submitted as practical for SANS 2000 written exam (March 25, 2000)

Background

The TCPDUMP program along with the NFR and the ISS RealSecure systems were used to collect data packets. The SNORT, NFR, ISS RealSecure and the TCPDUMP programs (with SHADOW filters and my own customized filters) were used to analyze the data. I'm working for an ISP operator in Thailand, three sensors were placed on our network segments outside the firewall. The data were collected during the April 10-24, 2000 period.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #1

```
23:13:36.321472 203.146.137.184.3622 > 203.146.43.178.1243: S 46171929:46171929(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:13:37.167007 203.146.137.184.3629 > 203.146.43.185.1243: S 46175895:46175895(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:13:37.250237 203.146.137.184.3638 > 203.146.43.194.1243: S 46175903:46175903(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:13:37.281959 203.146.137.184.3641 > 203.146.43.197.1243: S 46175906:46175906(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:13:40.131026 203.146.137.184.3638 > 203.146.43.194.1243: S 46175903:46175903(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:13:40.179359 203.146.137.184.3646 > 203.146.43.202.1243: S 46175911:46175911(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:26:07.974398 203.146.137.184.2489 > 203.146.70.128.1243: S 46926866:46926866(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:26:07.988969 203.146.137.184.2490 > 203.146.70.129.1243: S 46926867:46926867(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:26:08.003553 203.146.137.184.2491 > 203.146.70.130.1243: S 46926868:46926868(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:26:08.021246 203.146.137.184.2492 > 203.146.70.131.1243: S 46926869:46926869(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
23:26:08.021573 203.146.137.184.2493 > 203.146.70.132.1243: S 46926870:46926870(0) win 8192 <mss 536,nop,nop,sackOK> (DF)
```

Description

Actually, this traffic above is only a partial list of the scanning done by this IP address. This IP address probes our ten C-classes addresses (2437 IP addresses) during 23:13 - 23:36, 08:10-08:31, and 09:58-10:12. This IP address belongs to our pool of IP addresses that are given out to dialup customers. After an investigation, we have found that this dialup user account was hacked and we have already informed the customer about this matter. In addition, we have the hacker telephone number using the caller-id feature. Currently, the system administrator is getting in touch with the hacker regarding this activity.

Targeting: Yes
History: The hacked dialup customer account was used.
Techniques: Scanning for the TCP port 1243 using the half open scanning method (TCP Portscanning).
Intent: The host is scanning for either a SubSeven, a Backdoor-G, or a SubSeven Apocolypse trojan. (http://www.commodon.com/threat/threat-all.htm)
Analysis: This is a pretty fast and blatant attack, the hacker makes no attempt to hide the probe (2437 probes in short duration, and the probe contnued during the working hours). A program or a script was probably used to probe since the host port was incremented successively and the was quite fast. Since the probe was done quite carelessly, the hacker was probably a script-kiddie with no real expertise.
Severity: 3

Component	Score	Comments
Criticality:	2	users desktop are targeted
Lethality:	5	if found, SubSeven is pretty lethal - hacker can steal information and control the victim computer
System Countermeasures:	3	not all our customers will have updated patches
Network Countermeasures:	1	dialup users probably does not have a personal firewall
Severity:	3	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #2

```
Apr 20 08:05:22 203.146.131.146:3847 -> 203.146.93.15:21 SYN **S*****
Apr 20 08:05:23 203.146.131.146:3848 -> 203.146.93.15:80 SYN **S*****
Apr 20 08:05:23 203.146.131.146:3849 -> 203.146.93.16:21 SYN **S*****
Apr 20 08:05:23 203.146.131.146:3850 -> 203.146.93.16:80 SYN **S*****
Apr 20 08:05:23 203.146.131.146:3851 -> 203.146.93.17:80 SYN **S*****
Apr 20 08:05:23 203.146.131.146:3852 -> 203.146.93.18:21 SYN **S*****
Apr 20 08:05:23 203.146.131.146:3853 -> 203.146.93.18:80 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3856 -> 203.146.93.20:21 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3857 -> 203.146.93.20:80 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3858 -> 203.146.93.21:80 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3859 -> 203.146.93.22:21 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3860 -> 203.146.93.22:80 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3861 -> 203.146.93.23:21 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3862 -> 203.146.93.23:80 SYN **S*****
Apr 20 08:05:24 203.146.131.146:3863 -> 203.146.93.24:21 SYN **S*****
Apr 20 08:05:25 203.146.131.146:3864 -> 203.146.93.24:80 SYN **S*****
Apr 20 08:05:25 203.146.131.146:3865 -> 203.146.93.25:21 SYN **S*****
Apr 20 08:05:25 203.146.131.146:3866 -> 203.146.93.25:80 SYN **S*****
Apr 20 08:05:26 203.146.131.146:3874 -> 203.146.93.26:80 SYN **S*****
```

Description

Again, this IP address also belong to our pool of dialup IP addresses. The TCP Portscanning was done between 06:09-09:40 with 4740 TCP SYN packets were sent to 2000+ IP addresses.

Targeting: Yes
History: No previous history on this customer was kept
Techniques: Scanning for the TCP port 80 (Web server) and port 21 (FTP server) using the half open scanning method (TCP Portscanning).
Intent: The host is trying to find web and FTP servers on our networks.
Analysis: A program or a script was probably used to probe since the host port was incremented successively and the was quite fast. The intention was not clear, it could be a hacker who was trying to map our network or a customer who was trying to gather our network information.
Severity: 1

Component	Score	Comments
Criticality:	3	no clear target, just a blind sweeping
Lethality:	2	information gathering/confidentiality attack
System Countermeasures:	3	not all our customers will have updated patches
Network Countermeasures:	1	dialup users probably does not have a personal firewall
Severity:	1	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #3

```
[**] PING-ICMP Source Quench [**]
04/20-11:58:30.692022 203.155.136.134 -> 203.146.93.13
ICMP TTL:247 TOS:0x0 ID:12334
SOURCE QUENCH

[**] PING-ICMP Source Quench [**]
04/20-11:58:30.941345 203.155.136.134 -> 203.146.93.13
ICMP TTL:247 TOS:0x0 ID:12335  DF
SOURCE QUENCH

[**] PING-ICMP Source Quench [**]
04/20-11:58:31.397191 203.155.136.134 -> 203.146.93.13
ICMP TTL:247 TOS:0x0 ID:12336
SOURCE QUENCH

[**] PING-ICMP Source Quench [**]
04/20-11:58:31.707791 203.155.136.134 -> 203.146.93.13
ICMP TTL:247 TOS:0x0 ID:12337
SOURCE QUENCH
```

Description

This log was taken from the SNORT alert log that was generated using the 04052k.rules rule set. This alert was produced by the following rule:

alert icmp !$HOME_NET any <> $HOME_NET any (msg:"PING-ICMP Source Quench"; itype:4;)

The 203.146.93.13 is our Real audio/video server, when we check the source IP address (which is a dialup user from another ISP) we found that it response very slowly (i.e., ping response time between 2.6 – 4.5 seconds) as shown below.

```
traceroute to 203.155.136.134 (203.155.136.134), 30 hops max, 40 byte packets
 1  lir6-fl1-1-0.loxinfo.co.th (203.146.43.200)  0.505 ms  0.419 ms  0.431 ms
 2  203.146.68.186 (203.146.68.186)  1.961 ms  1.864 ms  1.784 ms
 3  ksc-pie.nectec.or.th (202.44.206.40)  2.6 ms  2.142 ms  4.397 ms
 4  r-l5.ksc.net.th (203.155.252.245)  11.672 ms  6.058 ms  7.184 ms
 5  ts-l5.ksc.net.th (203.155.33.205)  52.22 ms  13.275 ms  123.964 ms
 6  203.155.34.162 (203.155.34.162)  120.241 ms  48.01 ms  27.432 ms
 7  203.155.102.250 (203.155.102.250)  117.455 ms  83.262 ms  112.173 ms
 8  203.155.102.246 (203.155.102.246)  2463.78 ms  2682.16 ms  4386.61 ms
 9  203.155.136.134 (203.155.136.134)  4511.97 ms  2830.73 ms  2630.66 ms
```

A couple of hours later, we ping that IP address again and we have found that the response time is now much better (0.5 – 0.8 second).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
traceroute to 203.155.136.134 (203.155.136.134), 30 hops max, 40 byte packets
 1  lir6-fl l-1-0.loxinfo.co.th (203.146.43.200)  0.568 ms  0.425 ms  0.383 ms
 2  203.146.68.186 (203.146.68.186)  4.704 ms  2.876 ms  6.861 ms
 3  ksc-pie.nectec.or.th (202.44.206.40)  2.676 ms  2.337 ms  3.263 ms
 4  r-l5.ksc.net.th (203.155.252.253)  202.156 ms  185.07 ms  143.423 ms
 5  ts-l5.ksc.net.th (203.155.33.205)  220.051 ms  286.997 ms  376.887 ms
 6  203.155.34.162 (203.155.34.162)  326.168 ms  258.131 ms  286.103 ms
 7  203.155.102.250 (203.155.102.250)  356.48 ms  249.12 ms  339.036 ms
 8  203.155.102.246 (203.155.102.246)  506.849 ms  269.915 ms  405.735 ms
 9  203.155.136.134 (203.155.136.134)  459.928 ms  825.128 ms  470.303 ms
```

So in this case, the ICMP source quench is probably a real indication that the host 203.155.136.134 can't process the information quickly enough since at the time when we got the packet the PING response time on the host machine was really slow. We also have many similar detections of this type on various IP addresses (dialup users).

Targeting: Yes
History: No previous history on this customer was kept
Techniques: ICMP Source quenching technique was used.
Intent: To slow down the data tranfered rate of the server.
Analysis: This is probably not an attack but a genuine request for the server to slow down the data transfer rate.
Severity: -3

Component	Score	Comments
Criticality:	3	A Real Audio server
Lethality:	1	Unlikely to succeed, probably not an attack
System Countermeasures:	5	Modern OS with updated patches
Network Countermeasures:	2	Behind a permissive firewall
Severity:	-3	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #4

```
[**] Tiny Fragments - Possible Hostile Activity [**]
04/20-23:51:35.165669 202.183.198.76 -> 203.146.93.6
ICMP TTL:122 TOS:0x0 ID:45675  MF
Frag Offset: 0x0   Frag Size: 0x22

 [**] Tiny Fragments - Possible Hostile Activity [**]
04/20-20:14:41.081997 203.146.137.154 -> 203.146.93.6
ICMP TTL:124 TOS:0x0 ID:12806  MF
Frag Offset: 0x0   Frag Size: 0x22

[**] Tiny Fragments - Possible Hostile Activity [**]
04/20-20:14:41.321696 203.146.137.154 -> 203.146.93.6
ICMP TTL:124 TOS:0x0 ID:14598  MF
Frag Offset: 0x0   Frag Size: 0x22

[**] Tiny Fragments - Possible Hostile Activity [**]
04/20-20:14:41.513883 203.146.137.154 -> 203.146.93.6
ICMP TTL:124 TOS:0x0 ID:15622  MF
Frag Offset: 0x0   Frag Size: 0x22

[**] Tiny Fragments - Possible Hostile Activity [**]
04/20-20:14:41.673954 203.146.137.154 -> 203.146.93.6
ICMP TTL:124 TOS:0x0 ID:16134  MF
Frag Offset: 0x0   Frag Size: 0x22

[**] Tiny Fragments - Possible Hostile Activity [**]
04/20-20:15:27.548790 203.146.137.154 -> 203.146.93.6
ICMP TTL:124 TOS:0x0 ID:9737  MF
Frag Offset: 0x0   Frag Size: 0x22

[**] Tiny Fragments - Possible Hostile Activity [**]
04/20-20:15:30.606716 203.146.137.154 -> 203.146.93.6
ICMP TTL:124 TOS:0x0 ID:28681  MF
Frag Offset: 0x0   Frag Size: 0x22

[**] Tiny Fragments - Possible Hostile Activity [**]
04/20-20:16:00.787908 203.146.137.154 -> 203.146.93.6
ICMP TTL:124 TOS:0x0 ID:19467  MF
Frag Offset: 0x0   Frag Size: 0x22
```

Description

This log was taken from the SNORT alert log that was generated using the 04052k.rules rule set. We owned both IP addresses, the attacker is a dialup user. It's very unusual to have the fragment size 0x22 (34) bytes since most interfaces can handle much larger MTU than that so it's probably

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

not routers that do it. Notice that it's certainly not the protocol that was trying to discovery the maximum MTU size, since the fragment was fixed at 0x22 bytes. So this could be a crafted packet that attempt to bypass routers or intrusion detection systems.

Targeting: Yes
History: No previous history on this customer was kept
Techniques: ICMP fragmentation.
Intent: Information gathering.
Analysis: A program or a script was probably used to probe since probe speed was quite fast. It's probably an attempt to bypass the firewall or IDS. But I don't think it's caused by certain faulty routers otherwise we should be seeing this type of more packet regularly (since it's from the internal network).

Severity: -2

Component	Score	Comments
Criticality:	3	A non-critical server
Lethality:	2	information gathering/confidentiality attack
System Countermeasures:	5	The server has modern OS with updated patches
Network Countermeasures:	2	Permissive firewall
Severity:	-2	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #5

21/4/00 12:32:54	202.47.252.38	0	203.146.93.29	0	Smurf
21/4/00 13:13:02	202.47.252.46	0	203.146.93.29	0	Smurf

Description

This log was taken from the ISS RealSecure alert log. Currently, we are in the process of putting in the Egress filtering at our border routers and international gateways. We owned both IP addresses, this is the case where we have an dialup users attacking our server. Hopefully with our new Egress filters, we can block broadcast addresses at all border routers and can minimize the smurf attacks. We're blocking all invalid addresses from being routed as well as blocking certain broadcast addresses too.

Targeting: Yes
History: No previous history on this customer was kept
Techniques: Smurf.
Intent: Denial-of-service.
Analysis: This is a clear denial-of-service on the target host, trying to overwhelm to host file with ICMP traffic
Severity: 2

Component	Score	Comments
Criticality:	3	One of our non-critical server
Lethality:	2	Denial-of-Service (if enough packet was used)
System Countermeasures:	5	Modern OS with updated patches
Network Countermeasures:	2	Permissive firewall
Severity:	2	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #6

24/4/43	7:58:07	203.149.37.65	203.146.100.64	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.65	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.66	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.67	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.69	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.68	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.70	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.71	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.72	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.73	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.74	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.75	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.76	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.77	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.78	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.79	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.80	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.81	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.82	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.83	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.85	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.84	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.86	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.87	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.88	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.89	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.90	BackOrifice	COMMAND	Ping host
24/4/43	7:58:07	203.149.37.65	203.146.100.91	BackOrifice	COMMAND	Ping host

Description

This log was taken from the ISS RealSecure HIGH priority event log file. Here is the trace of this IP address :

```
traceroute to 203.149.37.65 (203.149.37.65), 30 hops max, 40 byte packets
 1  10.15.20.254 (10.15.20.254)  3.17 ms  3.28 ms  2.946 ms
 2  lir6-f11-1-0.loxinfo.co.th (203.146.43.200)  4.562 ms  2.307 ms  3.195 ms
 3  203.146.68.194 (203.146.68.194)  9.15 ms  8.691 ms  44.155 ms
 4  samart-pie.nectec.or.th (202.44.206.32)  36.188 ms  39.844 ms  41.995 ms
 5  SAMART-PIE-link-1M.samart.net.th (203.149.4.189)  20.097 ms telcom-digital-link-64k.samart.net.th (203.149.4.201)  29.196 ms  14.229 ms
 6  dialup5-65.samart.co.th (203.149.5.65)  22.307 ms  15.306 ms  10.169 ms
 7  e1-5.samart.co.th (203.149.33.8)  26.726 ms  19.199 ms  31.637 ms
 8  203.149.37.65 (203.149.37.65)  142.909 ms  143.678 ms  163.176 ms
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The IP address is from another ISP who was looking for the BackOrifice Trojan.

Targeting: Yes

History: No previous history on this customer was kept
Techniques: BO-ping from the BO client program.
Intent: Denial-of-service.
Analysis: A program (BO client) was probably used to probe since the probe speed was quite fast. The hack was trying to locate the BO infected hosts.
Severity: 3

Component	Score	Comments
Criticality:	3	no clear target, just a blind sweeping
Lethality:	5	If found, BO is very lethal – hackers can take over your computer
System Countermeasures:	3	not all our customers will have updated patches
Network Countermeasures:	2	dialup users probably does not have a personal firewall
Severity:	3	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #7

```
Apr 22 10:07:57 203.146.161.90:24225 -> 203.146.70.129:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24226 -> 203.146.70.131:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24227 -> 203.146.70.133:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24228 -> 203.146.70.135:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24231 -> 203.146.70.139:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24233 -> 203.146.70.141:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24235 -> 203.146.70.143:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24236 -> 203.146.70.145:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24238 -> 203.146.70.147:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24240 -> 203.146.70.155:27374 SYN **S*****
Apr 22 10:07:57 203.146.161.90:24242 -> 203.146.70.170:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21833 -> 203.146.70.183:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21834 -> 203.146.70.185:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21840 -> 203.146.70.181:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21844 -> 203.146.70.189:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21845 -> 203.146.70.190:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21847 -> 203.146.70.196:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21851 -> 203.146.70.198:27374 SYN **S*****
Apr 22 10:07:58 203.146.161.90:21853 -> 203.146.70.199:27374 SYN **S*****
```

Actually, this traffic above is only a partial list of the scanning done by this IP address. This IP address probes our two C-classes addresses (519 IP addresses) during 10:07-10:18. This IP address belongs to our pool of IP addresses that are given out to dialup customers. Currently, the system administrator is getting in touch with the hacker regarding this activity, we are trying to check whether the account was compromised or not.

Targeting: Yes
History: The dialup customer account with no previous history.
Techniques: Scanning for the TCP port 27374 using the half open scanning method (TCP Portscanning).
Intent: The host is scanning for a SubSeven trojan. (http://www.commodon.com/threat/threat-all.htm)
Analysis: This attack was very similar to the Detect #1 case where the host was targeting a SubSeven trojan. It's obviously a script too, if we look at the fast probe speed and the incremental nature of the TCP host port number
Severity: 3

Component	Score	Comments
Criticality:	2	users desktop are targeted
Lethality:	5	if found, SubSeven is pretty lethal - hacker can steal information and control the victim computer
System Countermeasures:	3	not all our customers will have updated patches
Network Countermeasures:	1	dialup users probably does not have a personal firewall
Severity:	3	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #8

Time: 10-Apr-2000 14:30:23
Source Addr: 203.155.247.19
Source Port: 0
Dest Addr: 203.146.43.55
Dest Port: 12345
TCP/UDP: TCP
TCP Flags:

Time: 10-Apr-2000 14:30:23
Source Addr: 203.146.43.55
Source Port: 12345
Dest Addr: 203.155.247.19
Dest Port: 0
TCP/UDP: TCP
TCP Flags: rst ack

Description

The above data was taken from the NFR log file. This was an attempt to discover whether IP 203.146.43.55 has a live port at 12345 (Netbus Trojan). In this case, if the port 12345 is live, the hacker won't get any response. If the port 12345 is dead, then the hacker will get a reply TCP/ packet with the RST, ACK flag set. This method is sometime used to do a port scanning through host inside a firewall or to avoid detection.

Targeting: Yes
History: No previous history on this customer was kept
Techniques: Non-SYN port scanning.
Intent: Find a Netbus Trojan on a target machine.
Analysis: A program or a script was probably used since this is a crafted packet (source port is 0 which was very unusual, no TCP flag set).
Severity: 1

Component	Score	Comments
Criticality:	3	Non-critical server
Lethality:	5	If found, the Netbus Trojan is lethal – hackers can take over infected host
System Countermeasures:	5	Modern OS with updated patches
Network Countermeasures:	2	Permissive firewall
Severity:	1	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Detect #9

23/4/43 14:54:25	0.0.0.0	203.146.93.8	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:28	0.0.0.0	203.146.93.13	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:29	0.0.0.0	203.146.93.61	SYNFlood	SPOOFEDS	203.146.104.119
23/4/43 14:54:29	0.0.0.0	203.146.93.62	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:29	0.0.0.0	203.146.93.63	SYNFlood	SPOOFEDS	203.146.138.2
23/4/43 14:54:29	0.0.0.0	203.146.93.64	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:29	0.0.0.0	203.146.93.72	SYNFlood	SPOOFEDS	203.146.137.171
23/4/43 14:54:29	0.0.0.0	203.146.93.73	SYNFlood	SPOOFEDS	202.183.225.11
23/4/43 14:54:29	0.0.0.0	203.146.93.74	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:29	0.0.0.0	203.146.93.75	SYNFlood	SPOOFEDS	203.146.138.2
23/4/43 14:54:29	0.0.0.0	203.146.93.76	SYNFlood	SPOOFEDS	203.146.104.119
23/4/43 14:54:29	0.0.0.0	203.146.93.112	SYNFlood	SPOOFEDS	202.183.225.26
23/4/43 14:54:32	0.0.0.0	203.146.93.68	SYNFlood	SPOOFEDS	202.183.225.26
23/4/43 14:54:32	0.0.0.0	203.146.93.70	SYNFlood	SPOOFEDS	203.146.138.112
23/4/43 14:54:32	0.0.0.0	203.146.93.66	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:32	0.0.0.0	203.146.93.65	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:32	0.0.0.0	203.146.93.69	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:32	0.0.0.0	203.146.93.67	SYNFlood	SPOOFEDS	202.183.225.21
23/4/43 14:54:32	0.0.0.0	203.146.93.84	SYNFlood	SPOOFEDS	203.146.138.112
23/4/43 14:54:36	0.0.0.0	203.146.93.34	SYNFlood	SPOOFEDS	203.146.161.2
23/4/43 14:54:36	0.0.0.0	203.146.93.47	SYNFlood	SPOOFEDS	203.146.161.2
23/4/43 14:54:37	0.0.0.0	203.146.93.199	SYNFlood	SPOOFEDS	203.146.137.204

Description

This log was taken from the ISS RealSecure HIGH event priority log file. Hackers were using a spoofed address 0.0.0.0 to attack servers with the SYN Flood method. We have rectified certain aspect of this problem by blocking reserved addresses. In addition, most of our servers were already patched to resist the SYNFlood attack

Targeting: Yes
History: No previous history on this customer was kept
Techniques: TCP SYNFlood attack.
Intent: Denial-of-service.
Analysis: A program or a script was probably used to probe since the probing was quite fast. Hackers were trying to do the denial-of-service attack to our servers.
Severity: 0

Component	Score	Comments

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Criticality:	3	Selected range of targets
Lethality:	4	Denial-of-service
System Countermeasures:	5	Modern OS with updated patches
Network Countermeasures:	2	Permissive firewall
Severity:	0	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002, Author retains full rights.

Detect #10

23/4/43 22:06:48	128.112.80.152	203.146.93.13	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.4	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.7	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.10	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.16	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.21	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.5	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.14	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.28	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.6	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.15	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.29	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.9	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.8	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.11	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.18	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.17	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.23	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.25	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.37	HTTP_TestCgi	URL	/cgi-bin/test-cgi/
23/4/43 22:06:48	128.112.80.152	203.146.93.38	HTTP_TestCgi	URL	/cgi-bin/test-cgi/

Description

This log was taken from the ISS RealSecure HIGH priority event logfile file. We tried to trace back to the host IP address, here is the traceroute result:

```
traceroute to 128.112.80.152 (128.112.80.152), 30 hops max, 40 byte packets
 1  10.15.20.254 (10.15.20.254)  2.391 ms  1.814 ms  1.089 ms
 2  lir6-fl1-1-0.loxinfo.co.th (203.146.43.200)  2.621 ms  1.84 ms  2.968 ms
 3  lir-spl.loxinfo.net (203.146.64.130)  5.568 ms  2.334 ms  2.955 ms
 4  gip-stock-5-s8-0-6.gip.net (204.59.165.57)  270.716 ms  293.875 ms  297.916 ms
 5  sl-bb10-stk-2-1.sprintlink.net (144.232.4.129)  375.8 ms  390.173 ms  309.367 ms
 6  sl-bb10-ana-6-1.sprintlink.net (144.232.8.90)  224.603 ms  207.489 ms  211.285 ms
 7  pos9-2-155M.lax-bb5.cerf.net (134.24.32.241)  375.717 ms  447.015 ms  494.951 ms
 8  pos4-0-622M.lax-bb4.cerf.net (134.24.32.13)  335.972 ms  362.227 ms  570.589 ms
 9  so1-0-0-622M.dfw-bb2.cerf.net (134.24.29.78)  275.477 ms  372.399 ms  409.056 ms
10  so1-3-0-622M.chi-bb5.cerf.net (134.24.46.82)  346.518 ms  373.824 ms  353.837 ms
11  pos1-0-622M.nyc-bb8.cerf.net (134.24.32.214)  458.897 ms  451.077 ms  441.101 ms
12  pos12-0-0-155M.nyc-bb2.cerf.net (134.24.32.222)  443.448 ms  300.977 ms  498.635 ms
13  princeton-gw.nyc-bb2.cerf.net (134.24.131.6)  445.042 ms  531.366 ms  503.538 ms
14  vgate1.Princeton.EDU (128.112.60.1)  499.049 ms  482.106 ms  641.28 ms
15  *
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

We are probably blocked at the firewall from tracing any further. For vulnerable Web servers, the “test-cgi” security hole allows hacker to arbitrary list remote file in the server.

When we check our TCPDUMP log, we can see a similar behavior as follows:

```
22:06:53.633751 fugue.csbmb.Princeton.EDU.11750 > vweb2.loxinfo.co.th.www: S 1337735200:1337735200(0) win 49152 <mss 1460>
22:06:53.633754 fugue.csbmb.Princeton.EDU.11747 > 203.146.11.129.www: S 1337536800:1337536800(0) win 49152 <mss 1460>
22:06:53.633788 fugue.csbmb.Princeton.EDU.11751 > my.i-kool.com.www: S 1337794400:1337794400(0) win 49152 <mss 1460>
22:06:53.633914 fugue.csbmb.Princeton.EDU.11754 > 203.146.11.136.www: S 1337998400:1337998400(0) win 49152 <mss 1460>
22:06:53.634242 fugue.csbmb.Princeton.EDU.11755 > 203.146.11.137.www: S 1338056000:1338056000(0) win 49152 <mss 1460>
22:06:53.634447 fugue.csbmb.Princeton.EDU.11764 > 203.146.11.146.www: S 1338625600:1338625600(0) win 49152 <mss 1460>
22:06:53.634569 fugue.csbmb.Princeton.EDU.11765 > 203.146.11.147.www: S 1338701600:1338701600(0) win 49152 <mss 1460>
22:06:53.636965 my.i-kool.com.www > fugue.csbmb.Princeton.EDU.11751: S 2353895647:2353895647(0) ack 1337794401 win 32120 <mss 1460> (DF)
22:06:53.643784 fugue.csbmb.Princeton.EDU.11746 > 203.146.11.128.www: S 1337479200:1337479200(0) win 49152 <mss 1460>
22:06:53.643947 fugue.csbmb.Princeton.EDU.11749 > vweb1.loxinfo.co.th.www: S 1337679200:1337679200(0) win 49152 <mss 1460>
22:06:53.644234 fugue.csbmb.Princeton.EDU.11753 > 203.146.11.135.www: S 1337925600:1337925600(0) win 49152 <mss 1460>
22:06:53.644440 fugue.csbmb.Princeton.EDU.11763 > 203.146.11.145.www: S 1338572800:1338572800(0) win 49152 <mss 1460>
22:06:53.645903 vweb1.loxinfo.co.th.www > fugue.csbmb.Princeton.EDU.11749: R 0:0(0) ack 1337679201 win 0
22:06:53.648986 fugue.csbmb.Princeton.EDU.11748 > vweb0.loxinfo.co.th.www: S 1337607200:1337607200(0) win 49152 <mss 1460>
22:06:53.649149 fugue.csbmb.Princeton.EDU.11752 > 203.146.11.134.www: S 1337868000:1337868000(0) win 49152 <mss 1460>
22:06:53.649356 fugue.csbmb.Princeton.EDU.11762 > 203.146.11.144.www: S 1338498400:1338498400(0) win 49152 <mss 1460>
22:06:53.649643 fugue.csbmb.Princeton.EDU.11766 > 203.146.11.148.www: S 1338762400:1338762400(0) win 49152 <mss 1460>
22:06:53.650481 vweb0.loxinfo.co.th.www > fugue.csbmb.Princeton.EDU.11748: S 2699986351:2699986351(0) ack 1337607201 win 32120 <mss 1460> (DF)
22:06:53.965077 fugue.csbmb.Princeton.EDU.11751 > my.i-kool.com.www: . ack 1 win 2920 (DF)
22:06:53.967492 fugue.csbmb.Princeton.EDU.11750 > vweb2.loxinfo.co.th.www: . ack 3602173860 win 2920 (DF)
22:06:53.968360 fugue.csbmb.Princeton.EDU.11751 > my.i-kool.com.www: P 1:50(49) ack 1 win 32767 (DF)
22:06:53.968863 my.i-kool.com.www > fugue.csbmb.Princeton.EDU.11751: . ack 50 win 32120 (DF)
```

With the TCPDUMP output, you can see pretty clearly that the host is trying to scan Web servers. Once it found the Web server then it started to implement the “test-cgi” attack.

Targeting: Yes
History: No previous history on this host was kept
Techniques: “test-cgi” web attack.
Intent: Unauthorized server access .
Analysis: A program or a script was probably used to probe since the probe speed was quite fast. The intention was quite clear, the hacker was trying to hack your Web server through the “test-cgi” hole.

Severity: 0

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Component	Score	Comments
Criticality:	3	no clear target, just a blind sweeping
Lethality:	2	information gathering/confidentiality attack
System Countermeasures:	3	not all our customers will have updated patches
Network Countermeasures:	2	permissive firewall
Severity:	0	(Criticality + Lethality) - (System + Net Countermeasures)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Zurich 2017	Zurich, Switzerland	May 15, 2017 - May 20, 2017	Live Event
Mentor Session - SEC503	Oceanside, CA	May 29, 2017 - Jun 29, 2017	Mentor
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
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 Fall 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 September 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 16, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego Fall 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced