Global Information Assurance Certification Paper

SANS PRACTICAL EXAM

For GIAC - Intrusion Detection Analyst

Prepared by: Michael Vars

Detect 1

May 29 19:43:41 morannon named [14021]: unapproved query from [203.149.232.6].3203 for "version.bind"
May 29 19:43:41 morannon named [14021]: unapproved query from [203.149.232.6].3237 for "version.bind"
May 29 19:43:41 morannon named [14021]: unapproved query from [203.149.232.6].3218 for "version.bind"
May 29 19:43:41 morannon named [14021]: unapproved query from [203.149.232.6].3374 for "version.bind"
May 29 19:43:41 morannon named [14021]: unapproved query from [203.149.232.6].3402 for "version.bind"
May 29 19:43:41 morannon named [14021]: unapproved query from [203.149.232.6].3245 for "version.bind"

Source of Trace:
http://www.sans.org/y2k/053100-1200.htm
Detect was generated by:
Psionic Portsentry
Probability the source address was spoofed:
Low – This is an example of reconnaissance work being done to find the version of BIND the victim is running. The current version of BIND is 8.22
Description of Attack:
An attacker may use DIG to query a name server for its version number. The attacker can obtain exploits known to affect the version of BIND that is being used and in turn use the exploit against it.
Attack Mechanism:
An Attacker finds the victims DNS sever via WHOIS. The Attacker can then try to transfer the zone files from the DNS server. The information an attacker can retrieve is the hosts and IP addresses within the victims zone files. Retrieving the victim's BIND version will make exploiting the DNS server easier for the attacker. This information is very valuable because it gives an attacker a "blueprint" of your hostnames and IP addresses.
Correlation:
This kind of attack is listed as one of the Top 10 Attacks by SANS. http://www.sans.org/topten.htm #1
DNS Vulnerabilities are listed at the CERT Advisory and CVE web sites:
http://www.cert.org/advisories/CA-99-14-bind.html
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=BIND

Evidence of active targeting:
This attack was directed at one host the DNS server.
Severity: (Critical + Lethal) – (System + Net Countermeasures)
(5+3)-(5+4) = -1
Defensive recommendations:
The system is blocking version queries. The site may want to block access to the DNS servers tcp/53 port to disable zone transfers on the Firewall. It is highly recommended to run the latest version of BIND with all patches. BIND updates and patches can be obtained from:
http://www.isc.org/products/BIND/bind8.html
Additional information:
BIND can be configured to not allow zone transfers to anyone. By putting the following statement in your BIND configuration file you can highly reduce the chance of an unauthorized zone transfers:
This command works on BIND 8.x `Options { allow-transfer { none; }; };` pg. 252 DNS & BIND Third Edition –O'Reilly & Associates, Paul Albitz & Cricket Liu
Online Documentation:
http://www.psionic.com/papers/dns/

Multiple Choice Question:

This trace is best described as the following:

a. DNS server scan
b. DNS buffer overflow
c. DNS zone transfer
d. DNS version query

Answer: **d**

Detect 2

---> Jun 20 04:00:39 Zion snort [9137]: spp_portscan:
-- > PORTSCAN DETECTED from 211.53.209.109
-- > Jun 20 04:00:39 211.53.209.109:2666 -> x.y.z.100:110 SYN **S*****
-- > Jun 20 04:00:39 211.53.209.109:2666 -> x.y.z.105:110 SYN **S*****
-- > Jun 20 04:00:39 211.53.209.109:2666 -> x.y.z.107:110 SYN **S*****
-- > Jun 20 04:00:39 211.53.209.109:2666 -> x.y.z.103:110 SYN **S*****
-- > Jun 20 04:00:47 zion snort[9137]: spp_portscan:
-- > portscan status from 211.53.209.109: 9 connections across 9 hosts:
-- > TCP(9), UDP(0)

Source of Trace:
http://www.sans.org/y2k/081200-1300.htm

Detect was generated by:
Snort IDS – http://www.snort.org
Probability the source address was spoofed:
Low – The packet looks crafted because the source port (2666) does not change. Reconnaissance may have already been done because the attacker is scanning only live hosts.
*** Another indication that a packet is crafted is to look for static sequence numbers.
Spoof info:
If you have the TTL time of the source address you can Traceroute that address to see if the TTL's match the ones found in the scan. If they are not close to the same value it is probable that the source address was spoofed.
Description of Attack:
The attack is a probe against multiple systems with a destination port of 110 (POP3).
Attack Mechanism:
Probes against POP3 servers are very common. The POP3 daemon runs with root privileges to handle multiple directories and mailboxes that are owned by the users of the mail system. Some versions of the software have vulnerabilities in the login process that may allow an attacker to compromise the system by using a buffer overflow. A buffer overflow attack may allow an attacker to mask commands send to the system that he/she could then execute with root privileges.
Correlation:
This kind of attack is listed as one of the Top 10 Attacks by SANS. http://www.sans.org/topten.htm #9
POP3 Vulnerabilities are listed at the CERT Advisory and CVE web sites:
http://www.cert.org/advisories/CA-97.09.imap_pop.html
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=pop3
Additional CVE Entries:
CVE-1999-0006, CVE-1999-0042, CVE-1999-0920, CVE-2000-0091
Evidence of active targeting:
This attack was directed at multiple hosts: x.y.z.100, x.y.z.105, x.y.z.107 and x.y.z.103
Severity: (Critical + Lethal) – (System + Net Countermeasures)
= -1
Defensive recommendations:
Since this mail system may be exposed to the Internet it highly susceptible to attacks. The vulnerabilities related to POP3 are dangerous because they may lead to a root compromise. Disable the POP3 and IMAP services from any system that is not an email server. Install latest patches.

Multiple Choice Question:

This trace is best described as the following:

a. A probe for Trojan Horse client
b. A probe for system running SQUID proxy.
c. A probe for POP3 server
d. Hack Attack denial of service attack

Answer: **c**

Detect 3

```
10:12:10.383619 194.204.206.60.21 > a.b.c.26.21:
  SF 904013986:904013986(0) win 1028
10:12:10.385202 194.204.206.60.21 > a.b.c.27.21:
  SF 904013986:904013986(0) win 1028
10:12:10.396730 194.204.206.60.21 > a.b.c.28.21:
  SF 904013986:904013986(0) win 1028
10:12:10.397749 194.204.206.60.21 > a.b.c.29.21:
  SF 1664236353:1664236353(0) win 1028
10:12:10.459859 194.204.206.60.21 > a.b.c.30.21:
  SF 1664236353:1664236353(0) win 1028
10:12:10.460876 194.204.206.60.21 > a.b.c.31.21:
  SF 1664236353:1664236353(0) win 1028
```

Source of Trace:
http://www.sans.org/y2k/080900.htm
Detect was generated by:
Tcpdump data
Probability the source address was spoofed:
Possible – The packet is crafted. The source port is the same as the destination port. The Sequence numbers change infrequently and the SYN/FIN flags are set.
Description of Attack:
The attack is a SYN/FIN scan against multiple systems looking for an ftp daemon to exploit.
Attack Mechanism:
Attacker probes a system stealthily by using SYN/FIN TCP flags in attempt to bypass Intrusion detection systems to see if they are running FTP services. An attacker can then run exploits against those services to compromise the system. There are known vulnerabilities for a very popular ftp daemon called WUftpd.
Correlation:
FTP Vulnerabilities are listed at the CERT Advisory and CVE web sites:
http://www.cert.org/advisories/CA-2000-13.html
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ftp
TCPdump Filter for SYN/FIN:
Tcp[13] & 0x3f=3
Evidence of active targeting:
This attack was directed at multiple hosts and for a particular service. (FTP)
Severity: (Critical + Lethal) – (System + Net Countermeasures)
= -1

Defensive recommendations:
The latest security patches and upgrades should be installed on all systems that need to run FTP services. If a system is not an FTP server, it is recommended to install SSH to use SFTP for secure file transfers. SSH provides encryption and authentication for Telnet and FTP.

Multiple Choice Question:

This trace is best described as the following:

a. A probe for IMAP servers
b. A probe for WINS servers
c. A probe for FTP servers
d. A probe for DNS servers

Answer: **c**

Detect 4

```
Jul 20 09:02:35 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
198.14.86.35/137 to aaa.bbb.14.198/137
Jul 20 09:02:35 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
198.14.86.35/137 to aaa.bbb.14.198/137
Jul 20 09:02:35 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
198.14.86.35/137 to aaa.bbb.14.198/137
Jul 20 09:03:36 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
198.14.86.35/137 to aaa.bbb.14.198/137
Jul 20 09:03:36 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
198.14.86.35/137 to aaa.bbb.14.198/137
Jul 20 09:03:36 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
198.14.86.35/137 to aaa.bbb.14.198/137
Jul 20 15:24:54 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
129.109.124.101/137 to aaa.bbb.109.129/137
Jul 20 15:43:07 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
129.109.124.101/137 to aaa.bbb.109.129/137
Jul 20 15:43:09 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
129.109.124.101/137 to aaa.bbb.109.129/137
Jul 20 18:36:18 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
200.10.95.201/137 to aaa.bbb.10.200/137
Jul 20 18:36:20 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
200.10.95.201/137 to aaa.bbb.10.200/137
Jul 20 18:36:21 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
200.10.95.201/137 to aaa.bbb.10.200/137
Jul 20 19:41:02 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
200.10.95.201/137 to aaa.bbb.10.200/137
Jul 20 19:41:02 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
200.10.95.201/137 to aaa.bbb.10.200/137
Jul 20 19:41:02 aaa.bbb.127.1 %PIX-2-106006:Deny inbound UDP from
200.10.95.201/137 to aaa.bbb.10.200/137
```

Source of Trace:
http://www.sans.org/y2k/072800.htm
Detect was generated by:
CISCO PIX Firewall (highlighted in yellow)
Probability the source address was spoofed:
High – Packet is definitely crafted. The first two octets of the source address match the last two octets of the destination address. Also the source port numbers do not change.
Description of Attack:
The attack is a scan from multiple spoofed addresses to multiple destination addresses with a destination port of 137. Netbios name service, which is used mostly by Microsoft machines, runs on port 137.
Attack Mechanism:
An Attacker probes a system from multiple spoofed addresses in attempt to evade possible detection. The probe is directed at the Microsoft Netbios service, which runs on port 137. Netbios service is prone to Denial of Service attacks. The "Netbios Name" DOS attack, is a popular exploit for port 137.
Correlation:
Netbios attacks are listed as one of the Top 10 Attacks by SANS. http://www.sans.org/topten.htm #7
Netbios Vulnerabilities are listed at the CERT Advisory and CVE web sites:
http://www.cert.org/vul_notes/VN-2000-03.html
http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Netbios
RFC Links:
http://www.ietf.org/rfc/rfc1001.txt?number=1001
http://www.ietf.org/rfc/rfc1002.txt?number=1002
Evidence of active targeting:
This attack was directed at multiple hosts for a particular service. Attacker also crafted these packets. This is shown by: • Destination and source ports are the same. (highlighted in red) • The first two octets of the source address match the last two octets of the destination address (highlighted in blue)
Severity: (critical + Lethal) – (System + Net Countermeasures)
= -2
Defensive recommendations:
Defenses are good. Attack is being stopped by Firewall.
Available Patches:
http://www.microsoft.com/technet/security/bulletin/ms00-047.asp
http://www.microsoft.com/technet/security/bulletin/fq00-047.asp

Multiple Choice Question:

This trace sample came from:

a. Cisco firewall Log
b. Snort Log
c. Router Log
d. Port Sentry Log

Answer: **a**

Detect 5

```
Jun 20 01:46:11 stealth portsentry [190]: attackalert: connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 12345
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 12345
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 12346
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 12346
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 20034
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 20034
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 31337
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 31337
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 40421
Jun 20 01:46:11 stealth portsentry [190]: attackalert: Connect from
host:
  195.clearwater-03-04rs.fl.dial-access.att.net/12.77.207.195 to TCP
port: 40421
```

Source of Trace:
http://www.sans.org/y2k/063000-1400.htm
Detect was generated by:
Psionic Portsentry (highlighted in the scan as blue)
Probability the source address was spoofed:

Low – Attacks come from an ATT dialup account located in Clearwater Florida shown in the scan as yellow.
Description of Attack:
The attack is a TCP scan for Multiple Trojan horses. The destination ports shown in the scan as red are well known Trojan horse ports. Port: 12345 = Netbus Trojan --runs on TCP Port: 12346 = Gaban Bus / Netbus Trojan --runs on TCP Port: 20034 = Netbus 2 Pro --runs on TCP Port 404211 = Masters Paradise --runs on TCP Port 31337 = Back Orifice --runs on UDP http://www.bo2k.com/
Attack Mechanism:
An Attacker probes a system for multiple Trojan Horse clients on ports known to serve this exploit. Trojans are used to remotely administer a system using software that connects to a client running on an infected system.
Correlation:
Trojan Horse Vulnerabilities are listed at the CERT Advisory and CVE web sites:
http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html
http://www.cert.org/vul_notes/VN-98.07.backorifice.html
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0660 (currently under review)
Evidence of active targeting:
• This attack was directed at well-known Trojan Ports.
Severity: (critical + Lethal) – (System + Net Countermeasures)
= -3
Defensive recommendations:
Defenses are good. Portsentry stops attack.
FYI:
Certain versions of BlackIce Defender and BlackIce Pro do not properly block against Back Orifice under certain settings.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-0562 (under review)

Multiple Choice Question:

This trace is scanning for what Trojan Horse:

a. SubSeven
b. Back Orifice
c. Blade Runner
d. Portal of Doom

Answer: **b**

Attack Evaluation

The following is actual reconnaissance done for this evaluation. The domain and IP addresses have been changed to hide identity.

DNS Reconnaissance

There are two common tools that can be used for obtaining information on a DNS server that are very useful and are probably installed on your system now. Although there are many more tools available, I wanted to show how reconnaissance can be done by anyone with a connection to the Internet and Windows NT.

Tools used:

Whois = Universal Domain name search tool

Nslookup = search Domain Name to IP address or IP address to Domain Name

The Whois tool can be found on a UNIX system or on a web site that offers the whois service online. For this example I will use a whois service from the website: http://www.network-tools.com.

The Nslookup tool is installed on most UNIX operating systems and it is also provided on Microsoft Windows NT and 2000.

The simple DNS reconnaissance we are going to show has two steps.

1. Gather Primary and Secondary DNS server addresses for target.edu.
2. Use the addresses we retrieved to try and execute a zone transfer from target.edu.

A transfer of targets zone file from DNS is a total listing of the domain names and their corresponding IP addresses. This information is invaluable to someone who wants to try to target your systems for an attack. Basically if you leave this vulnerability open an attacker will not have to map your network to exploit the hosts within it because you did most of this for him already.

Step 1.

Go to www.network-tools.com and do a www-whois for the domain target.edu. The following will be displayed.

```
Domain registry query for: target.edu:

Whois Server Version 1.1

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: TARGET.EDU
   Registrar: NETWORK SOLUTIONS, INC.
   Whois Server: whois.networksolutions.com
   Referral URL: www.networksolutions.com
   Name Server: NETOPS1.TARGET.EDU
   Name Server: NETOPS2.TARGET.EDU
```

Name Server: NS4.ISP.NET
Updated Date: 03-feb-2000

>>> Last update of whois database: Tue, 12 Aug 00 04:22:43 EDT <<<

Step 2.

Now that we have the primary and secondary DNS server addresses we can try to transfer the zone target.edu.

On Windows NT/2000:

- Go to: **`Start/Run`** type: **`cmd.`**
- At the DOS prompt type: **nslookup** `and hit enter.`
- Type**: server netops1.target.edu**

You should see the following:

> server netops1.target.edu
Default Server: netops1.target.edu
Address: 192.168.50.1

>(on this line type: **ls target.edu**)

The above command will list all the hostname and IP addresses within the target.edu zone file if the system is vulnerable.

Below is a cleaned zone transfer listing host and IP addresses for target.edu

d149.collegecampus	2H IN A	192.168.144.149
d151.collegecampus	2H IN A	192.168.144.151
d75.collegecampus	2H IN A	192.168.144.75
d152.collegecampus	2H IN A	192.168.144.152
d76.collegecampus	2H IN A	192.168.144.76
d153.collegecampus	2H IN A	192.168.144.153
d77.collegecampus	2H IN A	192.168.144.77
d154.collegecampus	2H IN A	192.168.144.154
d78.collegecampus	2H IN A	192.168.144.78
d80.collegecampus	2H IN A	192.168.144.80
d155.collegecampus	2H IN A	192.168.144.155
d79.collegecampus	2H IN A	192.168.144.79
d81.collegecampus	2H IN A	192.168.144.81
d156.collegecampus	2H IN A	192.168.144.156
d82.collegecampus	2H IN A	192.168.144.82
d157.collegecampus	2H IN A	192.168.144.157
d83.collegecampus	2H IN A	192.168.144.83

This evaluation shows how much info can be retrieved with just a few keystrokes. I have provided some defensive recommendations for BIND in the first network scan

listed in this practical. BIND attacks are listed as #1 on the SANS top ten attacks.

"Analyze This"

Source of Trace:
http://www.sans.org/giactc/snort/index.htm
Detect was generated by:
Snort data
Jun 20 01:08:38 207.236.40.20:54561 -> MY.NET.217.38:12345 SYN **S*****
Jun 20 01:08:37 207.236.40.20:54562 -> MY.NET.217.38:20034 SYN **S*****
Jun 20 01:08:38 207.236.40.20:54563 -> MY.NET.217.38:1243 SYN **S*****
Jun 20 01:08:37 207.236.40.20:54564 -> MY.NET.217.38:27374 SYN **S*****
Jun 20 01:08:38 207.236.40.20:54565 -> MY.NET.217.38:30100 SYN **S*****
Analysis
Jun 20 01:08:37
Attacker probes 217.38's ports for Trojan Horses that may have already been installed. Evidence of this can be seen in the destination port numbers. (12345, 20034, 1243, 27374) Attack started at 1:08am possibly to evade detection.
211.53.209.109:2666 - MY.NET.1.31:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.96:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.95:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.34:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.103:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.104:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.39:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.42:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.47:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.185:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.111:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.50:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.112:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.117:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.55:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.58:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.63:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.0:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.16:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.119:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.128:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.127:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.71:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.6:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.4:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.74:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.79:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.82:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.121:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.234:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.126:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.211:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.214:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.161:27374 SYN **S***** Jun 20

18:07:09 211.53.209.109:2666 - MY.NET.1.219:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.169:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.16:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.32:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.24:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.177:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.17:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.238:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.30:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.212:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.189:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.113:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.84:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.27:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.73:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.59:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.239:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.145:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.164:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.81:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.84:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.172:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.89:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.67:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.92:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.2.97:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.70:27374 SYN **S***** Jun 20 18:07:09 211.53.209.109:2666 - MY.NET.1.75:27374 SYN **S*****

Analysis

Attacker starts a network scan starting from my.net.1.5 to my.net.254.100. This scan goes on for four seconds, which seems like a very short amount of time to scan all of these hosts. The target port is 27374. The Subseven Trojan Horse is located on 27374.

Scan

Jun 20 20:02:28 24.23.36.24:1160 -> MY.NET.217.18:2729 NOACK 21SF*P** RESERVEDBITS
Jun 20 20:20:33 24.129.121.217:6699 -> MY.NET.217.158:2493 INVALIDACK 21*FRPAU RESERVEDBITS

Jun 20 20:27:17 24.23.36.24:1160 -> MY.NET.217.18:2729 NULL ********
Jun 20 20:33:57 24.9.56.208:4966 -> MY.NET.94.1:27374 SYN **S*****
Jun 20 20:33:57 24.9.56.208:4967 -> MY.NET.94.2:27374 SYN **S*****

Analysis

At 20:02:28, the IP address 24.23.36.24, starts into the trace and is sending null TCP flags to my.net.217.18 at a known Trojan port TCIM control. After this 24.23.36.24 starts scanning the network for SubSevan clients. Trace located below:

Jun 20 20:33:58 24.9.56.208:4990 - MY.NET.94.25:27374 SYN **S***** Jun 20 20:33:58 24.9.56.208:4991 - MY.NET.94.26:27374 SYN **S***** Jun 20 20:33:58 24.9.56.208:4993 - MY.NET.94.28:27374 SYN **S***** Jun 20 20:33:58 24.9.56.208:1035 - MY.NET.94.45:27374 SYN **S***** Jun 20 20:33:58 24.9.56.208:1036 - MY.NET.94.46:27374 SYN **S***** Jun 20 20:33:58 24.9.56.208:1040 - MY.NET.94.50:27374 SYN **S***** Jun 20 20:33:58 24.9.56.208:1043 - MY.NET.94.53:27374 SYN **S***** Jun 20 20:33:58 24.9.56.208:1044 - MY.NET.94.54:27374 SYN **S***** Jun 20 20:34:00 24.9.56.208:4985 - MY.NET.94.20:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:4999 - MY.NET.94.34:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:1051 - MY.NET.94.61:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:1065 - MY.NET.94.75:27374 SYN

S*** Jun 20 20:34:01 24.9.56.208:1067 - MY.NET.94.77:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:1068 - MY.NET.94.78:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:1069 - MY.NET.94.79:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:1083 - MY.NET.94.93:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:1086 - MY.NET.94.96:27374 SYN **S***** Jun 20 20:34:01 24.9.56.208:1088 - MY.NET.94.98:27374 SYN **S***** Jun 20 20:34:02 24.9.56.208:1100 - MY.NET.94.110:27374 SYN **S***** Jun 20 20:34:02 24.9.56.208:1102 - MY.NET.94.112:27374 SYN **S***** Jun 20 20:34:02 24.9.56.208:1103 - MY.NET.94.113:27374 SYN **S***** Jun 20 20:34:04 24.9.56.208:1088 - MY.NET.94.98:27374 SYN **S***** Jun 20 20:34:04 24.9.56.208:1098 - MY.NET.94.108:27374 SYN **S***** Jun 20 20:34:04 24.9.56.208:1108 - MY.NET.94.118:27374 SYN **S*****
Correlation:
FTP Vulnerabilities are listed at the CERT Advisory and CVE web sites:
http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html
Evidence of active targeting:
There seems to have been constant scans of the network and TCP and UDP scans.
Defensive recommendations:
Block all traffic going to unserved ports on the Firewall. To reduce the risk of Trojan exploits.

GCIA DC, Assignment 4

The information below was obtained from the web site: http://www.sans.org/giac.htm from the dates January 2000 to August 2000.

Top Ten Detects of Laurie@edu:

1. RPC / Portmapper
[**] RPC - portmap-request-mountd [**] 02/22-15:03:33.149576 212.25.118.45:633 -> x.x.x.x:111 UDP TTL:49 TOS:0x0 ID:5493 Len: 64 39 BE 43 FB 00 00 00 00 00 00 00 02 00 01 86 A0 9.C..... 00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 ..... 00 00 00 11 00 00 00 00 ..... [**] RPC - portmap-request-mountd [**] 02/22-15:03:38.142567 212.25.118.45:633 -> x.x.x.x:111 UDP TTL:49 TOS:0x0 ID:5531 Len: 64 39 BE 43 FB 00 00 00 00 00 00 00 02 00 01 86 A0 9.C.....

00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 01 86 A5 00 00 00 01 ..... 00 00 00 11 00 00 00 00 .....

Jul 5 10:43:50 203.197.144.142:111 -> a.b.e.47:111 SYNFIN **SF****
Jul 5 10:43:50 203.197.144.142:111 -> a.b.e.63:111 SYNFIN **SF****
Jul 5 10:43:50 203.197.144.142:111 -> a.b.e.68:111 SYNFIN **SF****
Jul 5 10:43:50 203.197.144.142:111 -> a.b.e.88:111 SYNFIN **SF****
Jul 5 10:43:50 203.197.144.142:111 -> a.b.e.91:111 SYNFIN **SF****
Jul 5 10:43:50 203.197.144.142:111 -> a.b.e.97:111 SYNFIN **SF****

Jun 20 04:15:41 dns1 snort[488133]: RPC Info Query:
210.145.109.162:910 -> z.y.w.34:111
Jun 20 04:16:13 dns2 snort[15799]: RPC Info Query:
210.145.109.162:943 -> z.y.w.66:111
Jun 20 04:16:44 dns3 snort[565]: RPC Info Query:
210.145.109.162:977 -> z.y.w.98:111
Jun 27 00:56:08 dns2 snort[336]: RPC Info Query:
210.145.109.162:791 -> z.y.w.66:111

2. DNS

Jul 25 06:30:34 200.241.187.2:4520 -> a.b.c.31:53 SYN **S*****
Jul 25 06:30:34 200.241.187.2:4522 -> a.b.c.33:53 SYN **S*****
Jul 25 06:30:34 200.241.187.2:4539 -> a.b.c.50:53 SYN **S*****
Jul 25 06:30:34 200.241.187.2:4540 -> a.b.c.51:53 SYN **S*****
Jul 25 06:30:34 200.241.187.2:4551 -> a.b.c.62:53 SYN **S*****
Jul 25 06:30:34 200.241.187.2:4714 -> a.b.c.225:53 SYN **S*****
Jul 25 06:30:36 200.241.187.2:4724 -> a.b.c.235:53 SYN **S*****

Jul 9 14:22:21 hostj snort[4594]: SCAN-SYN FIN:
193.173.174.119:53 -> z.y.x.66:53
Jul 9 14:22:12 hostm snort[15604]: spp_portscan:
PORTSCAN DETECTED from 193.173.174.119
Jul 9 14:22:12 hostm snort[15604]: SCAN-SYN FIN:
193.173.174.119:53 -> z.y.x.98:53
Jul 9 14:22:13 hostm snort[15604]: IDS277 - NAMED Iquery Probe:
193.173.174.119:1583 -> z.y.x.98:53
Jul 9 14:22:13 hostm snort[15604]: MISC-DNS-version-query:

193.173.174.119:1583 -> z.y.x.98:53

Aug 4 22:38:06 hostma Connection attempt to
UDP z.y.x.28:53 from 24.15.0.21:1205
Aug 4 22:38:07 hostma snort[2517]: MISC-DNS-version-query:
24.15.0.21:1205 -> z.y.x.28:53
Aug 4 22:58:03 hostma Connection attempt to TCP z.y.x.28:53
from 24.13.199.150:1437
Aug 4 22:58:06 hostma Connection attempt to TCP z.y.x.28:53
from 24.13.199.150:1437
Aug 4 22:38:10 hostma snort[2517]: MISC-DNS-version-query:
24.15.0.21:1205 -> z.y.x.241:53

3. FTP Connection Attempts

Jul 30 06:49:19 hosth inetd[45649]: refused connection
from 203.233.199.252, service ftpd (tcp)
Jul 30 06:49:19 hostmv /kernel: Connection attempt
to TCP a.b.f.167:21 from 203.233.199.252:2284
Jul 30 06:50:09 hostda in.ftpd[18574]:
refused connect from 203.233.199.252
Jul 30 06:50:09 hostdo in.ftpd[28904]:
refused connect from 203.233.199.252

Jul 18 22:47:52 hostz ftpd[28908]: refused connect from 149.112.77.46
Jul 18 22:54:29 hosts ftpd[29936]: refused connect from 149.112.77.46
Jul 18 23:04:33 hostba in.ftpd[15324]: refused connect from 149.112.77.46
Jul 19 02:32:35 hostki in.ftpd[7983]: refused connect from 149.112.77.46

Jul 15 20:29:17 hostda in.ftpd[8752]:
refused connect from r43h109.res.gatech.edu
Jul 15 20:29:59 hostdo in.ftpd[6976]:
refused connect from r43h109.res.gatech.edu
Jul 15 20:30:12 hosth inetd[8095]:
refused connection from r43h109.res.gatech.edu, service ftpd (tcp)
Jul 15 20:30:58 hostma ftpd[3063]:
connect from r43h109.res.gatech.edu
Jul 15 20:32:59 hostl proftpd[7049] hostl
(r43h109.res.gatech.edu[128.61.43.109]): connected - local : a.b.c.159:21

4. Telnet Connection Attempts

Jul 25 15:07:49 hostmf /kernel: Connection attempt to
TCP a.b.f.167:23 from 210.104.214.125:4148
Jul 25 15:08:21 hostl in.telnetd[29528]: [ID 947420 daemon.warning]
refused connect from 210.104.214.125
Jul 25 15:08:22 hostci in.telnetd[19119]:
refused connect from 210.104.214.125
Jul 25 15:08:23 hostda in.telnetd[9032]:
refused connect from 210.104.214.125

Jul 12 00:43:59 hosty telnetd[19105]:
refused connect from ppp30.doylestown.pil.net
Jul 12 00:45:32 hostj in.telnetd[14719]:
refused connect from ppp30.doylestown.pil.net
Jul 12 00:47:14 hostm in.telnetd[26216]:
refused connect from ppp30.doylestown.pil.net

Jun 27 20:33:38, Jun 27 23:10:05
Jun 28 21:46:31 dns3 in.telnetd[2788]: refused connect from server.hatada.to
Jun 28 23:40:13 dns3 in.telnetd[3021]: refused connect from server.hatada.to
Jun 28 23:40:20 dns1 telnetd[189993]: refused connect from server.hatada.to

5. FTP Scans

Aug 3 08:18:14 hosty snort[87735]: SCAN-SYN FIN:
212.177.241.85:21 -> z.y.w.34:21
Aug 3 08:18:58 hosty snort[87735]: SCAN-SYN FIN:
212.177.241.85:21 -> z.y.w.34:21

[**] SCAN-SYN FIN [**]
08/03-12:15:03.430616 206.78.1.18:21 -> z.y.w.34:21
TCP TTL:26 TOS:0x0 ID:39426
SF** Seq: 0x6D1EAE3E Ack: 0x617F3500 Win: 0x404
Aug 3 12:15:03 hostmi snort[314]: SCAN-SYN FIN:
206.78.1.18:21 -> z.y.w.98:21

[**] SCAN-SYN FIN [**]
08/03-12:15:03.408903 206.78.1.18:21 -> z.y.w.98:21
TCP TTL:27 TOS:0x0 ID:39426
SF** Seq: 0x6D1EAE3E Ack: 0x617F3500 Win: 0x404
00 00 00 00 00 00 .....

[**] SCAN-SYN FIN [**]
07/29-13:06:26.989665 208.50.27.150:21 -> z.y.w.98:21
TCP TTL:26 TOS:0x0 ID:39426
SF** Seq: 0x34670B6B Ack: 0x443576B5 Win: 0x404
00 00 00 00 00 00 .....

[**] SCAN-SYN FIN [**]
07/29-17:50:47.555089 208.50.27.150:21 -> z.y.w.98:21
TCP TTL:26 TOS:0x0 ID:39426
SF** Seq: 0x1CF4E7EC Ack: 0x426F167F Win: 0x404
00 00 00 00 00 00 .....

6. Telnet Scans

[**] SCAN-SYN FIN [**]
07/29-12:57:20.204213 212.160.132.58:23 -> z.y.w.66:23
TCP TTL:23 TOS:0x0 ID:39426
SF** Seq: 0x63260566 Ack: 0x27E158F6 Win: 0x404
00 00 00 00 00 00 .....

Jul 29 12:57:21 hostmi snort[15604]: SCAN-SYN FIN:
212.160.132.58:23 -> z.y.w.98:23

Jul 25 15:08:20 210.104.214.125:3249 -> a.b.c.33:23 SYN **S*****
Jul 25 15:08:20 210.104.214.125:3317 -> a.b.c.101:23 SYN **S*****
Jul 25 15:08:20 210.104.214.125:3333 -> a.b.c.117:23 SYN **S*****
Jul 25 15:08:20 210.104.214.125:3337 -> a.b.c.121:23 SYN **S*****

Jul 17 13:09:03 hostka snort[20224]: IDS027 - SCAN-FIN:
213.8.203.144:47850 -> a.b.e.48:23
Jul 17 13:09:04 hostka snort[20224]: IDS027 - SCAN-FIN:
213.8.203.144:47850 -> a.b.e.66:23

Jul 17 13:09:05 hostka snort[20224]: IDS027 - SCAN-FIN:
213.8.203.144:47850 -> a.b.e.79:23
Jul 17 13:09:05 hostka snort[20224]: IDS027 - SCAN-FIN:

7. WinGate Scans

Aug 9 02:02:02 hostma snort[2517]: MISC-WinGate-1080-Attempt:
151.197.10.114:3198 -> z.y.x.14:1080
Aug 9 02:02:13 hostma snort[2517]: MISC-WinGate-1080-Attempt:
151.197.10.114:3212 -> z.y.x.28:1080
Aug 9 02:02:13 hostma portsentry[11406]: attackalert:
Connect from host: adsl-151-197-10-114.bellatlantic.net/151.197.10.114
to TCP port: 1080
Aug 9 02:04:57 hostma snort[2517]: MISC-WinGate-1080-Attempt:
151.197.10.114:3373 -> z.y.x.189:1080

[**] MISC-WinGate-1080-Attempt [**]
08/06-23:19:04.473803 206.172.149.24:3155 -> z.y.w.98:1080
tcp TTL:49 TOS:0x0 ID:46331 DF
S*** Seq: 0xE2B16909 Ack: 0x0 Win: 0x3EBC
TCP Options => MSS: 1460 SackOK TS: 1058273 0 NOP WS: 0
Aug 6 23:19:05 hosty snort[87735]: MISC-WinGate-1080-Attempt:
206.172.149.24:3156 -> z.y.w.34:1080
Aug 6 23:19:05 hosty portsentry[594]: attackalert: Connect from host:
ppp11791.qc.bellglobal.com/206.172.149.24 to TCP port: 1080

Jul 26 22:26:23 hostka snort[20224]: MISC-WinGate-8080-Attempt:
194.87.6.201:3344 -> a.b.c.32:8080

[**] MISC-WinGate-8080-Attempt [**]
07/26-22:26:23.341264 194.87.6.201:3344 -> 128.173.12.32:8080
TCP TTL:110 TOS:0x0 ID:43466 DF
S*** Seq: 0x405DB1 Ack: 0x0 Win: 0x2000
TCP Options => MSS: 536 NOP NOP SackOK
+++++

8. Finger Probes

Jul 26 10:17:01 hostmi snort[15604]: FINGER-ProbeNull:

130.64.1.16:3315 -> z.y.w.98:79
Jul 26 10:17:01 hostmi portsentry[301]: attackalert:
Connect from host: emerald.tufts.edu/130.64.1.16 to TCP port: 79

[**] FINGER-ProbeNull [**]
07/24-21:06:39.416067 216.32.78.34:4378 -> z.y.w.66:79
TCP TTL:112 TOS:0x0 ID:22532 DF
*****PA* Seq: 0x1DA30D2 Ack: 0xF845A4EA Win: 0x2238
79 61 6F 0D 0A 00 yao...

Jun 19 23:05:26 dns1 portsentry[278053]: attackalert:
Connect from host: grace.isc.rit.edu/129.21.3.102 to TCP port: 79
Jun 19 23:05:26 dns1 snort[488133]: FINGER-ProbeNull:
129.21.3.102:2491 -> z.y.w.34:79

9. Ingres Scans and Attempts

Jul 7 18:17:49 210.222.31.100:1524 -> z.y.w.98:1524 SYNFIN **SF****
Jul 7 18:17:53 210.222.31.100:2595 -> z.y.w.98:1524 SYN **S*****
Jul 7 18:17:59 210.222.31.100:2601 -> z.y.w.98:1524 SYN **S*****

[**] default Backdoor access! [**]
06/05-07:54:30.017891 196.36.119.102:20 -> 192.168.0.12:1524
TCP TTL:124 TOS:0x10 ID:9051 DF
S*** Seq: 0x4551E8 Ack: 0x0 Win: 0x2000
TCP Options => MSS: 1460

Feb 21 14:26:16 milo portsentry[301]: attackalert:
Connect from host: 247-35.siteleader.net/207.211.35.247
to TCP port: 1524
Feb 21 14:26:16 yardbird portsentry[172871]: attackalert:
Connect from host: 247-35.siteleader.net/207.211.35.247
to TCP port: 1524

10. POP2 Scans

Jul 29 17:52:22 hostmi snort[15604]: SCAN-SYN FIN:
212.177.241.139:109 -> z.y.w.98:109
Jul 29 17:52:30 hostmi snort[15604]: SCAN-SYN FIN:

212.177.241.139:109 -> z.y.w.98:109 Jul 29 17:53:14 hostmi snort[15604]: SCAN-SYN FIN: 212.177.241.139:109 -> z.y.w.98:109
Jul 5 10:43:50 212.210.111.68:109 -> a.b.c.19:109 SYNFIN **SF**** Jul 5 10:43:50 212.210.111.68:109 -> a.b.c.32:109 SYNFIN **SF**** Jul 5 10:43:50 212.210.111.68:109 -> a.b.c.33:109 SYNFIN **SF**** Jul 5 10:43:50 212.210.111.68:109 -> a.b.c.62:109 SYNFIN **SF****
Jun 27 18:40:26 139.92.51.119:109 -> z.y.w.98:109 SYNFIN **SF**** Jun 27 18:41:03 139.92.51.119:109 -> z.y.w.98:109 SYNFIN **SF**** Jun 27 18:42:05 139.92.51.119:21 -> z.y.w.98:21 SYNFIN **SF**** Jun 27 18:43:48 139.92.51.119:109 -> z.y.w.98:109 SYNFIN **SF****

Top Ten Attacker Address Families:

1. Korean Education Network, Korea
203.232
203.230
2. @Home Network Netname: RDC1-MI-7 Netblock: 24.15.0.0 - 24.15.15.255
3. Japan Network Information Center, Japan
210.164.
210.189.
4. Exodus Commnications Inc. (NETBLK-ECI-7) 1605 Wyatt Dr. Santa Clara, CA 95054US US Netname: ECI-7 Netblock: 216.32.0.0 - 216.35.255.255
5. AOL, Reston VA, USA
AC8CF850.ipt.aol.com
62.125.10.102
6. Bell Atlantic (NETBLK-BELL-ATLANTIC1)

1880 Campus Commons Drive Reston, VA 20191 Netname: BELL-ATLANTIC1 Netblock: 151.196.0.0 - 151.205.0.0
7. Information Sciences Institute University of Southern California 4676 Admiralty Way, Suite 330 Marina del Rey, CA 90292-6695 US Netname: RESERVED-2 Netblock: 2.0.0.0 - 2.255.255.255
8. UUNET Technologies, Inc. (NETBLK-NETBLK-UUNET97DU) 3060 Williams Drive, Suite 601 Fairfax, va 22031 US Netname: NETBLK-UUNET97DU Netblock: 63.0.0.0 - 63.53.255.255
9. Worldlinx (NETBLK-WORLDLINX-6-B) WorldLinx Telecommunications Inc. 160 Elgin St. Floor 12, CA Netname: WORLDLINX-6-B Netblock: 206.172.62.0 - 206.172.223.0
10. I-2000 INC (NET-I2000-INC) 88 BEECHWOOD AVE EDISON, NY 08837 US Netname: SPRINT-CF29BF Netblock: 207.41.160.0 - 207.41.191.0

ISP Load Balancing Detects

The listed detects below are most likely caused from a load balancing device like F5 Big IP or Cisco Local Director. The device will run traceroutes to find the fastest route to a particular server. Evidence of the traceroutes is shown by the port attempts to port 33434.
May 10 10:56:31 dns2 snort[1323]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.66:33434 May 10 14:00:30 dns2 snort[1323]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.66:33434 May 10 14:09:40 dns2 snort[1323]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.66:33434

May 10 14:09:43 dns2 snort[1323]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.66:33434 May 10 13:51:31 dns3 snort[3439]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.98:33434 May 11 01:48:03 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.34:33434 May 10 15:50:35 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.34:33434 May 10 15:50:36 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.34:33434 May 10 15:50:38 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.34:33434 May 10 16:30:48 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.34:33434 May 10 16:01:29 dns2 snort[1323]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.66:33434 May 10 16:53:11 dns3 snort[3439]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.98:33434 May 10 16:54:01 dns3 snort[3439]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.98:33434 May 10 16:56:06 dns3 snort[3439]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.98:33434 May 10 20:25:20 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> 198.82.247.34:33434
14:11:54.879357 167.8.29.52.53 > my.firewall.com.33434: 2713 FormErr [0q] q: . 0/0/0 (36) [ttl 1] (id 2713) 14:11:55.053428 167.8.29.52.53 > my.firewall.com.33434: 2714 FormErr [0q] q: . 0/0/0 (36) (ttl 2, id 2714)
May 10 15:50:35 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> z.y.w.34:33434 May 10 15:50:36 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> z.y.w.34:33434 May 10 15:50:38 dns1 snort[51901]: IDS115 - MISC-Traceroute-UDP: 167.8.29.52:53 -> z.y.w.34:33434

Last Updated: July 23rd, 2017

Upcoming Training

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