



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Intrusion Detection In-Depth (Security 503)"
at <http://www.giac.org/registration/gcia>

- [Detect #1](#)
- [Detect #2](#)
- [Detect #3](#)
- [Detect #4](#)
- [Detect #5](#)
- [Assignment #2](#)
- [Assignment #3](#)

Assignment #1 – Five Network Scans

Detect #1 (named iquery attempt)

```
[**] DNS named iquery attempt [**]  
03/14-22:16:11.061618 seeker.net:2693 -> my.dns.com:53  
UDP TTL:45 TOS:0x0 ID:1794 IpLen:20 DgmLen:493  
Len: 473  
25 15 09 80 00 00 00 01 00 00 00 00 3E 41 41 41 %.....>AAA  
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA  
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA  
41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAAAAAAAAAAAA  
41 41 41 41 41 41 41 41 41 41 41 41 3E 42 42 42 AAAAAAAAAAAA>BBBB  
42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 BBBB BBBB BBBB BBBB  
42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 BBBB BBBB BBBB BBBB  
42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 BBBB BBBB BBBB BBBB  
42 42 42 42 42 42 42 42 42 42 3E 43 43 43 43 BBBB BBBB >CCCC  
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC  
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC  
43 43 43 43 43 43 43 43 43 43 43 43 43 43 43 CCCCCCCCCCCCCCCC  
43 43 43 43 43 43 43 43 43 43 3E 00 01 02 03 04 05 CCCCCCCC>.....  
06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 .....  
16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 ..... !"#$$%  
26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 &'()*+,-./012345  
36 37 38 39 3A 3B 3C 3D 3E 45 45 45 45 45 45 45 6789;,<=>EEEEEEE  
45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 EEEEEEEEEEEEEEEEE  
45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 EEEEEEEEEEEEEEEEE  
45 45 45 45 45 45 45 45 45 45 45 45 45 45 45 EEEEEEEEEEEEEEEEE  
45 45 45 45 45 45 3E 46 46 46 46 46 46 46 46 46 EEEEEEE>FFFFFFF  
46 46 46 46 46 46 46 46 46 46 46 46 46 46 46 FFFFFFFFFFFFFFFFF  
46 46 46 46 46 46 46 46 46 46 46 46 46 46 46 FFFFFFFFFFFFFFFFF  
46 46 46 46 46 46 46 46 46 46 46 46 46 46 46 FFFFFFFFFFFFFFFFF  
46 46 46 46 46 46 3D 47 47 47 47 47 47 47 47 47 FFFFFF=GGGGGGGGG  
47 47 47 47 47 47 47 47 47 47 47 47 47 47 47 GGGGGGGGGGGGGGGGG  
47 47 47 47 47 47 47 47 47 47 47 47 47 47 47 GGGGGGGGGGGGGGGGG  
47 47 47 47 47 47 47 47 47 47 47 47 47 47 47 GGGGGGGGGGGGGGGGG  
47 47 47 47 00 00 01 00 01 00 00 00 01 00 FF BF GGGG.....
```

=====
=====

The Log Format:

Meaning	Snort information
Snort signature	[**] DNS named iquery attempt [**]
Date/Time group	03/14-22:16:11.061618
Source Address and port (2693)	seeker.net:2693
Direction operator	->
Destination Address and port (53)	my.dns.com:53
Protocol and Time to Live (TTL)	UDP TTL:45
Type of Service (TOS)	TOS:0x0
Packet ID in binary	ID:1794
IP header length	IpLen:20
Total length	DgmLen:493
UDP length	Len: 473

1. Source of trace.

My network.

2. Detect was generated by:

Detect was generated by Snort Intrusion Detection System, Version 1.7.

Snort rule:

```
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"DNS named iquery attempt"; content:"|0980 0000 0001 0000 0000|"; offset: 2; depth : 16; reference:arachnids,277; reference:cve,CVE-1999-009; reference:bugtraq,134;)
```

explain the log format

3. Probability the source address was spoofed:

Probably not spoofed. Spoofing the address would be defeating the purpose to see response.

4. Description of attack:

The attacker is trying to determine if a name server supports IQUERY (Inverse Query).

5. Attack Mechanism:

IP address **seeker.net** is trying to determine if the name server, **my.dns.com**, supports IQUERY.

This signature often indicates a pre-attack probe used to locate vulnerable servers running named. With Inverse Query Buffer Overrun in BIND 4.9 and BIND 8 Releases attacker can gain root-level access to name server.

6. Correlation:

The following links have additional information:

<http://www.whitehats.com/info/IDS277>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0009>

<http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D134>

<http://www.insecure.org/spl0its/bind.multiple.vuln.html>

7. Evidence of active targeting:

The source IP address **iquery.net** targeted IP address **my.dns.com**

8. Severity:

(System Criticality + Attack Lethality) – (System Countermeasures + Network Countermeasures) = Severity

$(5 + 3) - (5+2) = 1$

System Criticality: 5 - DNS server

Attack Lethality: 3 - Pre-attack probe

System Countermeasures: 5 - Modern operating system, all patches

Network Countermeasures: 2 - Firewall in place, but traffic is allowed to target

9. Defensive recommendation:

"Upgrading to the latest version of bind, available at: <http://www.isc.org/bind.html> will eliminate this vulnerability.

CERT advisory CA-98.05.bind_problems.html details individual vendor responses. It also provides information about specific vendor patches."

(<http://www.securityfocus.com/frames/?content=/vdb/bottom.html%3Fvid%3D134>).

10. Multiple choice test question:

Which service is on port 53?

- A SMTP
- B WWW
- C FTP
- D DNS

On the Internet, there are mail servers that are miss-configured and are an open relay. This means that unscrupulous people can send bulk unsolicited junk e-mail through those relays and bombard other sites.

6. Correlation:

<http://www.whitehats.com/info/IDS249>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0512>

7. Evidence of active targeting:

The **seeker.relaying.net** targeted **my.smtp.com** and packets, from the dump, are responses from **my.smtp.com**.

8. Severity:

(System Criticality + Attack Lethality) - (System Countermeasures + Network Countermeasures) = Severity

$$(4 + 1) - (5 + 2) = -2$$

System Criticality: 4 - SMTP server
Attack Lethality: 1 - Attack is unlikely to succeed
System Countermeasures: 5 - Modern operating system, all patches
Network Countermeasures: 2 - Firewall in place, but traffic is allowed to target

9. Defensive recommendation:

"This behavior indicates the successful blocking of an attempt at relaying email through an internal email server." (ids249)

10. Multiple choice test question:

What is signature of the "SMTP relaying denied"

- A FLAGS SYN, PSH
- B CONTENT "550"
- C FLAGS ACK, PSH CONTENT "5.7.1", DEPTH "70"
- D DEPTH "7"

Answer C

Detect #3 (False Positive - transmitting data via HTTP) - (Back)

```
[**] DDOS mstream client to handler [**]  
03/14-13:51:25.235058 www.server.net:80 -> my.ws.com:12754  
TCP TTL:117 TOS:0x0 ID:1009 IpLen:20 DgmLen:141 DF  
***AP*** Seq: 0xE70F58F Ack: 0x1645CAEE Win: 0x2058 TcpLen: 20  
72 3E 0D 0A 09 09 3C 54 52 3E 0D 0A 09 09 3C 54 r>....<TR>....<T
```

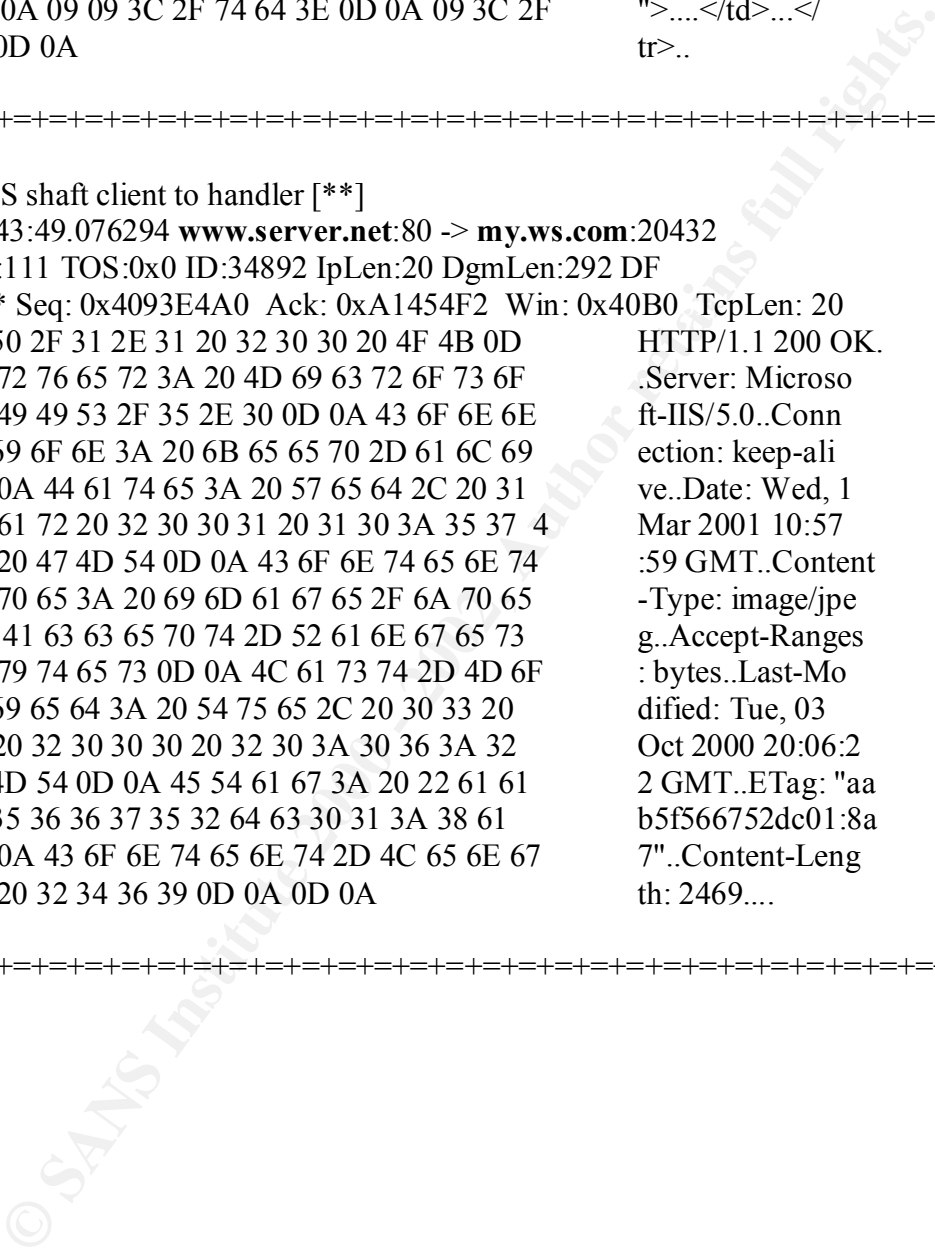
SANS Intrusion Detection & Analysis Certification
New Orleans January 28 - February 2, 2001

```
44 20 43 4F 4C 53 50 41 4E 3D 22 33 22 20 41 4C      D COLSPAN="3" AL
49 47 4E 3D 22 43 45 4E 54 45 52 22 3E 0D 0A 09      IGN="CENTER">...
09 09 3C 68 72 20 77 69 64 74 68 3D 22 31 30 30      ..<hr width="100
25 22 20 61 6C 69 67 6E 3D 22 63 65 6E 74 65 72      %" align="center
22 3E 0D 0A 09 09 3C 2F 74 64 3E 0D 0A 09 3C 2F      ">....</td>...</
74 72 3E 0D 0A                                          tr>..
```

=====
=====

```
[**] DDOS shaft client to handler [**]
03/14-13:43:49.076294 www.server.net:80 -> my.ws.com:20432
TCP TTL:111 TOS:0x0 ID:34892 IpLen:20 DgmLen:292 DF
***AP*** Seq: 0x4093E4A0 Ack: 0xA1454F2 Win: 0x40B0 TcpLen: 20
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D      HTTP/1.1 200 OK.
0A 53 65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F      .Server: Microso
66 74 2D 49 49 53 2F 35 2E 30 0D 0A 43 6F 6E 6E      ft-IIS/5.0..Conn
65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69      ection: keep-ali
76 65 0D 0A 44 61 74 65 3A 20 57 65 64 2C 20 31      ve..Date: Wed, 1
34 20 4D 61 72 20 32 30 30 31 20 31 30 3A 35 37 4   Mar 2001 10:57
3A 35 39 20 47 4D 54 0D 0A 43 6F 6E 74 65 6E 74      :59 GMT..Content
2D 54 79 70 65 3A 20 69 6D 61 67 65 2F 6A 70 65      -Type: image/jpe
67 0D 0A 41 63 63 65 70 74 2D 52 61 6E 67 65 73      g..Accept-Ranges
3A 20 62 79 74 65 73 0D 0A 4C 61 73 74 2D 4D 6F      : bytes..Last-Mo
64 69 66 69 65 64 3A 20 54 75 65 2C 20 30 33 20      dified: Tue, 03
4F 63 74 20 32 30 30 30 20 32 30 3A 30 36 3A 32      Oct 2000 20:06:2
32 20 47 4D 54 0D 0A 45 54 61 67 3A 20 22 61 61      2 GMT..ETag: "aa
62 35 66 35 36 36 37 35 32 64 63 30 31 3A 38 61      b5f566752dc01:8a
37 22 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67      7"..Content-Leng
74 68 3A 20 32 34 36 39 0D 0A 0D 0A                  th: 2469....
```

=====
=====



The Log Format:

Meaning	Snort information
Snort signature	[**] DDOS mstream client to handler [**]
Date/Time group	03/14-13:51:25.235058
Source Address and port (80)	www.server.net:80
Direction operator	->
Destination Address and port (12754)	my.ws.com:12754
Protocol and Time to Live (TTL)	TCP TTL:117
Type of Service (TOS)	TOS:0x0
Packet ID in binary	ID:1009
IP header length	IpLen:20
Total length	DgmLen:141
Don't Fragment Flag	DF
TCP flags set	***AP***
Sequence # in Hex	Seq: 0xE70F58F
Acknowledgement # in Hex	Ack: 0x1645CAEE
Windows size in Hex	Win: 0x2058
TCP header length	TcpLen: 20

1. Source of trace.

My network

2. Detect was generated by:

Detect was generated by Snort Intrusion Detection System, Version 1.7.

Snort rule:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 12754 (msg:"DDOS mstream client to handler"; content: ">"; flags: A+; reference:cve,CAN-2000-0138;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 20432 (msg:"DDOS shaft client to handler"; flags: A+; reference:arachnids,254;)
```

3. Probability the source address was spoofed:

Probably not spoofed.

4. Description of attack:

N/A

5. Attack Mechanism:

N/A

6. Correlation:

The following links have additional information about Distributed Denial of Service (DDOS) attacks "mstream client to handler" and " shaft client to handler":

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0138>

<http://xforce.iss.net/alerts/advise48.php>

<http://marc.theaimsgroup.com/?l=bugtraq&m=95715370208598&w=2>

<http://marc.theaimsgroup.com/?l=bugtraq&m=95722093124322&w=2>

<http://www.whitehats.com/info/IDS254>

http://www.securiteam.com/windowsntfocus/Microsoft_IIS_shtml_exe_path_disclosure_vulnerability.html

7. Evidence of active targeting:

N/A

8. Severity:

(System Criticality + Attack Lethality) – (System Countermeasures + Network Countermeasures) = Severity

$(x + x) - (x + x) = x$

System Criticality:

Attack Lethality:

System Countermeasures:

Network Countermeasures:

9. Defensive recommendation:

N/A

10. Multiple choice question:

This log was generated by which IDS:

A Shadow

B Snort

C Real Secure

D Net Ranger

Answer B

Detect #4 (WEB-FRONTPAGE shtml.exe) - ([Back](#))

[**] WEB-FRONTPAGE shtml.exe [**]

03/20-11:52:34.076724 192.168.100.101:57426 -> my.web.com:80

6. Correlation:

The following links have additional information:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0413>

<http://www.securityfocus.com/bid/1174>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2000-0709>

<http://www.securityfocus.com/bid/1608>

7. Evidence of active targeting:

The source IP address **192.168.100.101** targeted **my.web.com**.

8. Severity:

(System Criticality + Attack Lethality) - (System Countermeasures + Network Countermeasures) = Severity

$$(4 + 2) - (2 + 2) = 2$$

System Criticality: 4 - Web server

Attack Lethality: 2 - Pre attack probe

System Countermeasures: 2 - Target is not patched

Network Countermeasures: 2 - Firewall in place, but traffic is allowed to target

9. Defensive recommendation:

"Microsoft will be addressing this issue with version 1.2 of Frontpage Server Extensions 2000." (bid 1174)

10. Multiple choice test question:

Which item is a signature of a " WEB-FRONTPAGE shtml.exe " attack:

A /_vti_/html.exe

B /_vti_bin/shtml.exe

C /_vti_bin/http.exe

D /_bin/shttp.exe

Answer B

Detect #5 (False Positive - miss-configured Tivoli/IBM TME 10 agent) - ([Back](#))

portscan.log

Mar 11 20:58:01 192.168.100.100:13991 -> 17.32.184.68:13991 UDP

Mar 11 20:58:02 192.168.100.100:13991 -> 17.32.225.4:13991 UDP

Mar 11 20:58:03 192.168.100.100:13991 -> 17.32.125.132:13991 UDP

Mar 11 20:58:04 192.168.100.100:13991 -> 17.32.241.196:13991 UDP

SANS Intrusion Detection & Analysis Certification
New Orleans January 28 - February 2, 2001

Mar 11 20:58:04 192.168.100.100:13991 -> 17.32.16.228:13991 UDP
Mar 11 20:58:05 192.168.100.100:13991 -> 17.32.156.4:13991 UDP
Mar 11 20:58:06 192.168.100.100:13991 -> 17.32.229.4:13991 UDP

alert

[**] spp_portscan: portscan status from 192.168.6.202: 7 connections across 7 hosts:
TCP(0), UDP(7) [**]
03/11-20:58:08.684813

Cisco Secure PIX firewall

106011: Deny inbound (No xlate) udp src xxx: 192.168.100.100/13991 dst
xxx:17.32.115.196/13991
106011: Deny inbound (No xlate) udp src xxx: 192.168.100.100/13991 dst
xxx:17.32.157.196/13991

The log format:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v50/pix55em/pixemsgs.htm#40403

1. Source of trace.

My network.

2. Detect was generated by:

Detect was generated by Snort Intrusion Detection System, Version 1.7.
Cisco Secure PIX firewall. (explain the format)

3. Probability the source address was spoofed:

Probably not spoofed

4. Description of attack:

IP address 192.168.100.100 scanned IP addresses on port 13991.

5. Attack Mechanism:

N/A

6. Correlation:

The following correlating data is included (from Sniffer Pro), providing a complete UDP packet.

DLC: ----- DLC Header -----

SANS Intrusion Detection & Analysis Certification
New Orleans January 28 - February 2, 2001

DLC:
DLC: Frame 1 arrived at 14:45:32.0000; frame size is 60 (003C hex) bytes.
DLC: Destination = Station Cisco107AC10
DLC: Source = Station 00105AE795F6
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. = routine
IP: ...0 ... = normal delay
IP: 0... = normal throughput
IP: 0.. = normal reliability
IP: Total length = 31 bytes
IP: Identification = 21878
IP: Flags = 0X
IP: .0.. = may fragment
IP: ..0. = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 64 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 5B01 (correct)
IP: Source address = [192.168.100.100]
IP: Destination address = [17.32.241.196]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 13991
UDP: Destination port = 13991
UDP: Length = 11
UDP: Checksum = 4732 (correct)
UDP: [3 byte(s) of data]
UDP:
ADDR HEX ASCII
0000: 00 00 0c 07 ac 10 00 10 5a e7 95 f6 08 00 45 00 |!Xn6...
0010: 00 1f 55 76 00 00 40 11 5b 01 xx xx xx xx xx xx |\$.{y...
0020: xx xx 36 a7 36 a7 00 0b 47 32 81 00 00 00 00 00 | 1D.x.x....a....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |

7. Evidence of active targeting:

N/A

8. Severity:

(System Criticality + Attack Lethality) – (System Countermeasures + Network Countermeasures) = Severity

$$(x + x) - (x + x) = x$$

System Criticality:

Attack Lethality:
System Countermeasures:
Network Countermeasures:

9. Defensive recommendation:

Do right configuration.

10. Multiple choice question:

106011: Deny inbound (No xlate) udp src xxx:192.168.100.100/13991 dst
xxx:17.32.115.196/13991

This log was generated by:

- A Check Point FW1
- B Cisco Secure PIX firewall
- C Cisco Secure IDS
- D Shadow

Answer B

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

Assignment 2 –Evaluate and attack – (Back)

1. Source of the Attack - thong.pl - automated multi dos attack tool

<http://www.hack.co.za/html/index.january.html>

According to the (1), " Thong-th-thong-th-thong.pl AKA thong.pl is a PERL script which automates several attacks against various Cisco products.

To be specific:

12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability"

2. Description of Attack

2.1 Exploits Details

Name: Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability

CVE: CAN-2001-0080 (under review) (2)

Operating System: Cisco Catalyst 6000, 5000, or 4000 switches

Brief Description: Cisco switches allow remote attackers to cause a denial of service by connecting to the SSH service with a non-SSH client, which generates a protocol mismatch error.

Name: Cisco 675 Web Administration Denial of Service Vulnerability

BUGTRAQ id: 2012

Operating System: Cisco DSL Router 677.0, Cisco DSL Router 675.0

Brief Description: "If the Cisco 675 DSL Router has the Web Administration Interface enabled, a remote attacker could telnet to the router and issue a simple malformed HTTP GET request. Once connected via telnet to the Web Administration Interface, issuing the command GET ?\n\n will crash the telnet session as well as the router, requiring it be power cycled before resuming normal operation." (3)

Name: Cisco Catalyst 3500 XL Remote Arbitrary Command

CVE: CAN-2000-0945 (under review) (4)

Operating System: Cisco Catalyst 3500 XL switches

Brief Description: Web configuration interface for Catalyst 3500 XL switches allows remote attackers to execute arbitrary commands without authentication via URL containing the /exec/ directory.

Name: Cisco IOS Software HTTP Request DoS Vulnerability

CVE: CVE-2000-0984 (5)

Operating System: Cisco IOS 12.0 through 12.1

Brief Description: HTTP server in Cisco IOS 12.0 through 12.1 allows local users to cause a denial of service (crash and reload) via URL containing a "?" string.

2.2 How to use the exploit

To start PERL script, the following command can be used:

```
# ./thong.pl -h <host>
```

Then, you can choose one of the next options:

DATE VULNERABILITY

1. 12-13-00 - Cisco Catalyst ssh Protocol Mismatch DoS Vulnerability
2. 11-28-00 - Cisco 675 Web Administration Denial of Service Vulnerability
3. 10-26-00 - Cisco Catalyst 3500 XL Remote Arbitrary Command
4. 10-25-00 - Cisco IOS Software HTTP Request DoS Vulnerability

Enter Option:

2.3 Source code

The source code can be found at (1) and the lines below come from thong.pl:

```
sub computeOption
{
  if ($menu_opt == "1"){ $PORT = 22; $STRING = "this ain't SSH";}
  elsif ($menu_opt == "2"){ $PORT = 80; $STRING = "GET ? HTTP/1.0\n\n";}
  elsif ($menu_opt == "3"){ $PORT = 80; three();}
  elsif ($menu_opt == "4"){ $PORT = 80; $STRING = "GET /error?/ HTTP/1.0\n\n";}
  else {print "Select a real option!\n"; menu();}
}

sub three
{
  print "Enter file to read or enter D for default (/show/config/cr): ";
  $key = <STDIN>;
  chomp ($key);
  print "\nGetting $key...";

  if (($key eq "D") || ($key eq "d"))
  {
    print "\nGetting /show/config/cr...\n";
    $STRING = "GET /exec/show/config/cr HTTP/1.0\n\n";
  }
  else
  {
    print "\nGetting $key...\n";
    $STRING = "GET /exec$key HTTP/1.0\n\n";
  }
}
```


}

3. Trace of the Attack

I used Sniffer Pro from Network Associates and I have done trace for Cisco IOS Software HTTP Request DoS Vulnerability.

First the three way handshake, SYN, SYN-ACK, ACK:

1 [attacker] [http-server] 74 TCP: D=80 S=1130 **SYN** SEQ=3676262050 LEN=0
WIN=32120

2 [http-server] [attacker] 60 TCP: D=1130 S=80 **SYN ACK**=3676262051
SEQ=3588378044 LEN=0 WIN=4128

3 [attacker] [http-server] 60 TCP: D=80 S=1130 **ACK**=3588378045 WIN=32120

Attacker sends a HTTP request:

----- Frame 4 -----

...

TCP: ----- TCP header -----

TCP:

TCP: Source port = 1130

TCP: Destination port = 80 (WWW-HTTP)

TCP: Sequence number = 3676262051

TCP: Next expected Seq number= 3676262074

TCP: Acknowledgment number = 3588378045

TCP: Data offset = 20 bytes

TCP: Flags = 18

TCP: ..0. = (No urgent pointer)

TCP: ...1 = Acknowledgment

TCP: 1... = Push

TCP:0.. = (No reset)

TCP:0. = (No SYN)

TCP:0 = (No FIN)

TCP: Window = 32120

TCP: Checksum = 45D2 (correct)

TCP: No TCP options

TCP: [23 Bytes of data]

TCP:

HTTP: ----- Hypertext Transfer Protocol -----

HTTP:

HTTP: Line 1: GET /error?/ HTTP/1.0

HTTP: Line 2:

HTTP:

Detecting the attack

I wrote the Snort rule:

Assignment #3 – Analyze This Scenario – (Back)

1. Scenario

"Your organization has been asked to provide a bid for security services to GIAC Enterprises, an e-business startup that sells electronic fortune cookie sayings. You have been provided with one month's worth of data from a Snort system with a fairly standard rulebase. From time to time, the power has failed or the disk was full so you do not have data for all days. Your task is to analyze the data. Be especially alert for signs of compromised systems or network problems and produce an analysis report." (1)

2. Snort Snarf output of the alert files

Signature	# Alerts	# Sources	# Destinations
site exec - Possible wu-ftpd exploit - GIAC000623	1	1	1
SITE EXEC - Possible wu-ftpd exploit - GIAC000623	1	1	1
STATDX UDP attack	1	1	1
Happy 99 Virus	1	1	1
Probably NMAP fingerprint attempt	8	5	6
External RPC call	59	15	25
Back Orifice	63	9	60
TCP SMTP source Port traffic	100	5	88
Broadcast Ping to subnet 70	151	23	1
connect to 515 from inside	159	10	98
SUNRPC highport access	204	25	19
SMB Name Wildcard	515	93	171
Russia Dynamo - SANS Flash 28-jul-00	546	2	2
NMAP TCP ping!	558	47	156
SNMP public access	591	20	7
Queso fingerprint	710	52	72
Null scan!	824	525	171
Attempt Sun RPC high port access	2041	16	22
Win Gate 1080 Attempt	2202	466	565
Watch list 000222 NET - NCFC	2401	31	19
Connect to 515 from outside	4237	9	2876
Tiny Fragments - Possible Hostile Activity	5339	26	12
DNS udp DoS attack described on unisog	16146	8	6
SYN - FIN scan!	51192	37	27067
Watchlist 000220 IL - ISDNNET-990517	104507	46	100

Table 1

3. Top 5 alert signatures of 25 identified signatures

3.1 Watchlist 000220 IL - ISDNNET-990517

Watchlist 000220 IL - ISDNNET-990517	46 sources	100 destinations
--------------------------------------	------------	------------------

Top Source Hosts

#	Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	212.179.79.2	48786	48786	41	41
2	212.179.27.111	37604	37604	1	1
3	212.179.95.5	4563	4563	4	4
4	212.179.77.20	2353	2353	2	2
5	212.179.44.105	1517	1517	1	1

Top Destination Hosts

#	Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	MY.NET.201.222	37604	37609	1	6
2	MY.NET.220.126	25182	25183	1	2
3	MY.NET.225.234	9309	9314	1	4
4	MY.NET.202.94	5181	5253	4	20
5	MY.NET.229.114	5080	5082	1	3

Detailed analyze of the summary field (SnortSnarf) shows that only one signature is present for all five Top Source Hosts and it is Watchlist 000220 IL - ISDNNET-990517 and all 46 source hosts traffic comes from Israel. For example IP address 212.179.79.2 has the next information from RIPE Whois Database:

```
Inetnum:      212.179.79.0 - 212.179.79.63
netname:      CREOSCITEX
descr:        CREOSCITEX-SIFRA
country:      IL
admin-c:      ZV140-RIPE
tech-c:       NP469-RIPE
status:       ASSIGNED PA
notify:       hostmaster@isdn.net.il
changed:      hostmaster@isdn.net.il 20001109
source:       RIPE
```

Top Destination Hosts shows most targeted hosts on MY.NET, for this attack, and all of them have at least one scanning signature, for example "SYN-FIN scan!". The lines below come from Snort. "Null scan!", in the first line, indicates the scanning of the port 6699 on MY.NET.201.222. After scanning came traffic to MY.NET.201.22 on the same port.

01/02-16:16:47.594317 [**] Null scan! [**] 213.96.7.214:60860 ->
MY.NET.201.222:6688

...

01/04-02:54:06.872039 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.27.111:1778 -> MY.NET.201.222:6688

01/04-02:54:07.917555 [**] Watchlist 000220 IL-ISDNNET-990517 [**]
212.179.27.111:1778 -> MY.NET.201.222:6688

...

I have found the rapport of similar traffic on (2) and comment was: "In this case, a large portion of it looks like gnutella related activity." "Gnutella is the protocol that allows those with a Gnutella client to distribute files." (3) For more information on Gnutella, take a look at (3) or (4). There are some security risks to use gnutella, for example:

- no restrictions possible on unauthorized sharing of files,
- not anonymous,
- ability to see what other people are searching for on the network,
- distributed nature of servant makes it difficult to block access to GnutellaNet, '
- ability to change the port you use makes it difficult to block access to GnutellaNet,
- ability to define your own internal network with a single exit point to the rest of the internet makes it difficult to block access to GnutellaNet

7 different signatures are present for IP address MY.NET.202.94 as a destination:

- 2 instances of Null scan!,
- 3 instances of SYN-FIN scan!,
- 3 instances of BackOrifice,
- 4 instances of Attempt Sun RPC high port access,
- 6 instances of SUNRPC highport access,
- 54 instances of WinGate 1080 Attempt,
- 5181 instances of Watchlist 000220 IL - ISDNNET-990517.

Lines above show many strange actions on the IP address MY.NET.202.94 and it will require further review.

3.2 SYN - FIN scan!

Event description: "A TCP probe was sent with the SYN+FIN flags set in the header. This traffic does not occur naturally and indicates an intentional probe, likely as a part of single-packet OS detection." (6)

SYN - FIN scan!	37 sources	27067 destinations
-----------------	------------	--------------------

SANS Intrusion Detection & Analysis Certification
New Orleans January 28 - February 2, 2001

Top Source Hosts

#	Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	211.34.40.1	17604	17604	17604	17604
2	195.56.182.206	9878	9878	9878	9878
3	194.234.48.26	8565	8565	8565	8565
4	147.8.182.157	4096	4096	4096	4096
5	194.204.334.131	3052	3052	3052	3052

Top Destination Hosts

#	Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	MY.NET.253.11	19	294	17	24
2	MY.NET.21.15	8	8	8	8
3	MY.NET.5.125	7	7	7	7
4	MY.NET.11.212	7	8	7	8
5	MY.NET.223.255	6	6	6	6

Snort rule:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN SYN
FIN";flags:SF;reference:arachnids,198;)
```

The number of 27067 destinations shows that MY.NET has been seriously scanned. Most scanned ports were 21, 109 and 53. The lines below show one example of SYN-FIN scan on port 21.

```
12/12-06:11:20.503923 132.68.37.141:21 -> MY.NET.4.249:21
12/12-06:11:20.763860 132.68.37.141:21 -> MY.NET.5.7:21
12/12-06:11:20.784158 132.68.37.141:21 -> MY.NET.5.8:21
12/12-06:11:20.864150 132.68.37.141:21 -> MY.NET.5.12:21
12/12-06:11:20.884078 132.68.37.141:21 -> MY.NET.5.13:21
```

3.3 DNS udp DoS attack described on unisog

DNS udp DoS attack described on unisog	8 sources	16 destinations
--	-----------	-----------------

Top Source Hosts

#	Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	209.67.50.203	16132	16132	3	3
2	209.67.50.253	4	4	1	1
3	209.67.50.85	3	3	2	2
4	209.67.50.209	2	2	2	2
5	209.67.50.241	2	2	1	1

Top Destination Hosts

#	Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	MY.NET.1.8	3148	3219	17	31
2	MY.NET.1.10	1264	1279	14	22
3	MY.NET.217.162	727	733	1	6
4	MY.NET.60.11	168	1456	2	140
5	MY.NET.1.9	8	16	5	10

I'll point that some of the Tiny Fragments - Possible Hostile Activity took place at same time as DNS udp DoS attack and it shows the lines below.

01/06-19:14:50.459957 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:8660
-> MY.NET.1.3:53

01/06-19:14:50.511252 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:5889
-> MY.NET.1.3:53

01/06-19:14:50.672602 [**] Tiny Fragments - Possible Hostile Activity [**] 202.205.5.10 ->
MY.NET.1.8

01/06-19:14:50.672647 [**] Tiny Fragments - Possible Hostile Activity [**] 202.205.5.10 ->
MY.NET.1.8

01/06-19:14:50.702372 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:29297
-> MY.NET.1.4:53

01/06-19:14:51.027301 [**] DNS udp DoS attack described on unisog [**] 209.67.50.203:13164
-> MY.NET.1.4:53

It will require further review.

3.5 Connect to 515 from outside

Port 515/tcp uses to access to printer service ports and printing service is called LPRng. According to CVE-2000-0917 "Format string vulnerability in use_syslog() function in LPRng 3.6.24 allows remote attackers to execute arbitrary commands."

Connect to 515 from outside	9 sources	2876 destinations
-----------------------------	-----------	-------------------

Top Source Hosts

#	Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	141.211.176.99	2236	2236	2195	2195
2	216.119.15.88	1273	1273	4	4
3	209.217.166.69	713	713	710	710
4	192.118.36.9	7	7	1	1
5	64.46.70.175	4	4	1	1

Top Destination Hosts

#	Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	MY.NET.100.209	405	405	1	1
2	MY.NET.99.104	403	406	1	4
3	MY.NET.130.86	259	260	2	3
4	MY.NET.214.166	209	211	3	5
5	MY.NET.20.1	7	10	1	4

The number of 2876 destinations shows that MY.NET has been scanned on port 515 and the first four destinations IP addresses, from table above, require further investigation.

Snort rules, which can detect LPRng exploits:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 515 (msg:"EXPLOIT LPRng overflow";
flags: A+; content: "/43 07 89 5B 08 8D 4B 08 89 43 0C B0 0B CD 80 31 C0 FE C0 CD 80 E8
94 FF FF FF 2F 62 69 6E 2F 73 68 0A/"; reference:bugtraq,1712;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 515 (msg:"EXPLOIT redhat 7.0 lpr
overflow"; flags: A+; content:"|58 58 58 58 25 2E 31 37 32 75 25 33 30 30 24 6E|";)
```

Snort records:

```
[**] connect to 515 from outside [**] 141.211.176.99:4683 -> MY.NET.71.56:515
[**] connect to 515 from outside [**] 141.211.176.99:4719 -> MY.NET.71.90:515
[**] connect to 515 from outside [**] 141.211.176.99:4732 -> MY.NET.71.103:515
[**] connect to 515 from outside [**] 141.211.176.99:4873 -> MY.NET.71.244:515
[**] connect to 515 from outside [**] 141.211.176.99:1714 -> MY.NET.75.35:515
```

4. Other Alerts of Interest

4.1 SNMP public access

The Simple Network Management Protocol (SNMP) is used for monitoring routers, switches and other network elements (UDP port 161). For authentication, SNMP is using community strings. Default SNMP community strings, set to "public" and "private", are frequently used. SNMP public access is one of the Top Ten Internet Security Threats. (8)

SNMP public access	20 sources	7 destinations
--------------------	------------	----------------

Top Source Hosts

#	Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	128.46.156.231	161	161	3	3
2	MY.NET.97.244	74	74	1	1
3	MY.NET.162.201	71	71	1	1
4	MY.NET.97.155	60	60	1	1
5	MY.NET.98.134	40	40	1	1

Top Destination Hosts

#	Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	MY.NET.101.192	316	374	14	15
2	MY.NET.100.99	104	106	1	3
3	MY.NET.50.154	94	94	3	3
4	MY.NET.100.143	36	37	1	2
5	MY.NET.100.206	21	22	1	2

Snort rule:

```
alert udp any any -> $HOME_NET 161 (msg: "SNMP public access"; content:"public");
```

IP address targeted three computers on MY.NET (MY.NET.100.99, MY.NET.100.143 and MY.NET.100.206) and the next lines shows some Snort records.

```
...  
01/12-09:56:42.477347 [**] SNMP public access [**] 128.46.156.231:2159 ->  
MY.NET.100.206:161  
01/12-09:56:43.001464 [**] SNMP public access [**] 128.46.156.231:2163 ->  
MY.NET.100.143:161  
01/12-09:56:48.423324 [**] SNMP public access [**] 128.46.156.231:2168 ->  
MY.NET.100.99:161  
01/12-09:56:50.337560 [**] SNMP public access [**] 128.46.156.231:2171 ->  
MY.NET.100.99:161  
01/12-09:56:53.542213 [**] SNMP public access [**] 128.46.156.231:2173 ->  
MY.NET.100.99:161  
...
```

For this alert, there are 20 sources and 7 destinations and it's something odd. It must be opposite, i.e. more destinations than sources and it means there are always more network elements than network management stations.

It will require further investigation.

4.2 Russia Dynamo - SANS Flash 28-jul-00

The SANS Institute wrote:

"SANS Flash Report: Trojans Sending More Data To Russia
July 28, 2000, 6:20 pm, EDT

This is preliminary information. The GIAC (Global Incident Analysis Center) has received several submissions showing large amounts of data being sent, illegitimately, from Windows 98 machines to a Russian IP address (194.87.6.X). The cause is most probably a Trojan, but whatever it is, it is moving fast."

SANS Intrusion Detection & Analysis Certification
New Orleans January 28 - February 2, 2001

Top Source Hosts

#	Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	MY.NET.205.138	442	442	1	1
2	194.87.6.38	104	104	1	1

Top Destination Hosts

#	Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	194.87.6.38	442	442	1	1
2	MY.NET.205.138	104	108	1	1

The lines below come from Snort and we can see traffic in both directions.

...

```
12/08-16:08:54.086006 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 ->
MY.NET.205.138:6699
12/08-16:08:56.777675 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:08:57.590220 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:08:59.189855 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 ->
MY.NET.205.138:6699
12/08-16:08:59.672791 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:00.315359 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 ->
MY.NET.205.138:6699
12/08-16:09:01.419429 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:01.419771 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:01.900908 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:01.901472 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:02.217496 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 ->
MY.NET.205.138:6699
12/08-16:09:03.692655 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:05.164572 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:14.532328 [**] Russia Dynamo - SANS Flash 28-jul-00 [**] 194.87.6.38:2478 ->
MY.NET.205.138:6699
12/08-16:09:18.221557 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
12/08-16:09:20.714259 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478
```

12/08-16:09:24.108584 [**] Russia Dynamo - SANS Flash 28-jul-00 [**]
MY.NET.205.138:6699 -> 194.87.6.38:2478

...

It is an evidence that computer MY.NET.205.138 was probably infected with Trojan.

4.3 Broadcast Ping to subnet 70

Event description: "ICMP messages to broadcast addresses are allowed, allowing for a Smurf attack that can cause a denial of service." (9)

Top Source Hosts

#	Sources	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	213.154.131.131	52	52	1	1
2	194.102.93.101	26	26	1	1
3	193.231.220.91	17	17	1	1
4	193.231.220.137	12	12	1	1
5	193.231.220.238	8	8	1	1

Top Destination Hosts

#	Destinations	# Alerts (sig)	# Alerts (total)	# Srcs (sig)	# Srcs (total)
1	MY.NET.70.255	151	153	23	25

Detailed analyze of the summary field (SnortSnarf) shows that 2 different signatures are present for MY.NET.70.255 as a destination:

- 2 instances of SYN-FIN scan!
- 151 instances of Broadcast Ping to subnet 70.

I don't know addressing scheme and all net masks on MY.NET. If MY.NET.70.255 is a broadcast address, this net possibly would be used as a smurf amplifier. If not, MY.NET.70.255 requires further investigation. For example, Loki traffic, which is using for covering the tracks, looks like ICMP traffic.

4.4 Back Orifice

Back orifice is well known backdoor, with many versions. Old Back Orifice port was UDP 31337, but today Back Orifice hasn't default port.

All alerts under this headline require further investigation.

4.5 Attempt Sun RPC high port access, SUNRPC highport access and External RPC call

"Sun's Remote Procedure Call (RPC) protocol [Sun Microsystems, 1988, 1990} underlies many of the new services. Unfortunately, many of these services represent potential security problems " (10)

Remote Procedure Calls is, also, one of the Top Ten Internet Security Threats. (8)

All alerts under this headline require further investigation.

Conclusion

From the Table 1, we can see many signatures and they can cover one attack scenario, i.e. reconnaissance, penetration and denial of service.

MY.NET scanned heavily and the most popular scan was "SYN - FIN scan".

There are many signs that traffic on MY.NET was probably gnutella related.

On MY.NET, there are many examples of strange traffic, like Tiny Fragments, Connect to 515 from outside and inside, SNMP public access, RPC traffic. It will require further investigation.

Russia Dynamo - SANS Flash 28-jul-00 is one example that MY.NET has computer infected probably with "Trojans Sending More Data To Russia".

"DNS udp DoS attack described on unisog" and "Broadcast Ping to subnet 70" are examples of Denial of Service attacks on MY.NET.

Resources and References

- (1) http://www.sans.org/giactc/GCIA_assignment.htm#7
- (2) <http://www.sans.org/y2k/052000.htm>
- (3) <http://www.gnutella.co.uk/about/>
- (4) <http://gnutella.nerdherd.net/tutorial.htm>
- (5) <http://www.whitehats.com/info/IDS198>
- (6) <http://www.theorygroup.com/Archive/Unisog/2001/msg00067.html>
- (7) www.cs.technion.ac.il/Labs/Lccn/projects/spring98/firewall1/public_html/details.html
- (8) <http://www.sans.org/topten.htm>
- (9) <http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0513>
- (10) (Firewalls and Internet Security, Repelling the Wily Hacker, William R. Cheswick, Steven M. Belovin, Addison - Wesley Publishing Company)

Upcoming Training

Click Here to
{Get CERTIFIED!}



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
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Ottawa SEC503	Ottawa, ON	Oct 16, 2017 - Oct 21, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC503: Intrusion Detection In-Depth	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS 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 Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 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 London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	Tysons, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS Baltimore Spring 2018	Baltimore, MD	Apr 21, 2018 - Apr 28, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced