The Most Critical Internet Security Threats

CGI - One example

- htsearch of htdig – CVE-2000-0208

Snort Log:

```
[**] WEB-etc/passwd [**]
07/10-11:26:35.063544 195.96.98.222:12440 -> my.net.search.engine:80
TCP TTL:46 TOS:0x0 ID:34513  DF
*****PA* Seq: 0xC8F464C7   Ack: 0xC1F29A8F   Win: 0x2238
47 45 54 20 2F 63 67 69 2D 62 69 6E 2F 68 74 73  GET /cgi-bin/hts
65 61 72 63 68 3F 65 78 63 6C 75 64 65 3D 60 2F  earch?exclude=`/
65 74 63 2F 70 61 73 73 77 64 60 20 48 54 54 50  etc/passwd` HTTP
2F 31 2E 30 0D 0A 56 69 61 3A 20 31 2E 31 20 77  /1.0..Via: 1.1 w
77 77 2E 63 61 63 68 65 2E 63 61 73 65 6D 61 2E  ww.cache.casema.
6E 65 74 20 28 4E 65 74 43 61 63 68 65 20 34 2E  net (NetCache 4.
31 52 31 44 35 29 0D 0A 43 6F 6E 6E 65 63 74 69  1R1D5)..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A  on: Keep-Alive..
0D 0A                                            ..
```

Apache log:

```
A.B.C.D - - [10/Jul/2000:11:33:16 -0400] "GET /cgi-bin/
➥htsearch?exclude=%60/etc/passwd%60 HTTP/1.0" 200 1703 "-" "-"
```

One more example – Narrow Security Scanner

```
scanner.com - - [18/Apr/2000:23:25:57] "HEAD /scripts/convert.bas HTTP/1.0"     404
scanner.com - - [18/Apr/2000:23:25:57] "HEAD /cgi-bin/whois_raw.cgi HTTP/1.0"   404
scanner.com - - [18/Apr/2000:23:25:57] "HEAD /cgi-bin/nph-test-cgi HTTP/1.0"    404
                    ... cut for brevity ...
scanner.com - - [18/Apr/2000:23:26:14] "HEAD /_vti_pvt/administrators.
                                        ➥pwd HTTP/1.0"                          404
scanner.com - - [18/Apr/2000:23:26:50] "HEAD /cfdocs/expelval/sendmail.
                                        ➥cfm HTTP/1.0"                          404
scanner.com - - [18/Apr/2000:23:26:51] "HEAD /cfdocs/expelval/exprcalc.
                                        ➥cfm HTTP/1.0"                          404
scanner.com - - [18/Apr/2000:23:26:51] "HEAD /showfile.asp HTTP/1.0"             404
scanner.com - - [18/Apr/2000:23:26:52] "HEAD /cfdocs/expelval/
                                        ➥openfile.cfm HTTP/1.0"                 404
scanner.com - - [18/Apr/2000:23:26:55] "HEAD /ws_ftp.ini HTTP/1.0"               404
scanner.com - - [18/Apr/2000:23:26:55] "HEAD /cgi-dos/args.cmd HTTP/1.0"         404
scanner.com - - [18/Apr/2000:23:26:56] "HEAD /cgi-shl/win-c-sample.exe HTTP/
                                        ➥1.0"                                   404
scanner.com - - [18/Apr/2000:23:26:56] "HEAD /cgi-bin/passwd.txt HTTP/1.0"       404
scanner.com - - [18/Apr/2000:23:26:57] "HEAD /cgi-win/uploader.exe HTTP/1.0"     404
scanner.com - - [18/Apr/2000:23:26:57] "HEAD /...../autoexec.bat HTTP/1.0"       404
scanner.com - - [18/Apr/2000:23:26:59] "HEAD /cgi-bin/rwwwshell.pl HTTP/1.0"     404
scanner.com - - [18/Apr/2000:23:27:00] "HEAD /cgi-bin/unlg1.1 HTTP/1.0"          404
scanner.com - - [18/Apr/2000:23:27:00] "HEAD /.html/...../
                                        ➥autoexec.bat HTTP/1.0"                 404
                    ... cut for brevity ...
scanner.com - - [18/Apr/2000:23:27:12] "HEAD /cgi-bin/test.bat HTTP/1.0"         404
scanner.com - - [18/Apr/2000:23:27:13] "HEAD /cgi-bin/input.bat HTTP/1.0"        404
scanner.com - - [18/Apr/2000:23:27:13] "HEAD /cgi-bin/input2.bat HTTP/1.0"       404
scanner.com - - [18/Apr/2000:23:27:13] "HEAD /ssi/envout.bat HTTP/1.0"           404
scanner.com - - [18/Apr/2000:23:27:14] "HEAD /msadc/msadcs.dll HTTP/1.0"         404
scanner.com - - [18/Apr/2000:23:27:14] "HEAD /scripts/tools/newdsn.exe HTTP/
                                        ➥1.0"                                   404
scanner.com - - [18/Apr/2000:23:27:14] "HEAD /cgi-bin/get32.exe¦dir HTTP/1.0"    404
scanner.com - - [18/Apr/2000:23:27:15] "HEAD /cgi-bin/alibaba.pl¦dir HTTP/1.0"   404
scanner.com - - [18/Apr/2000:23:27:16] "HEAD /cgi-bin/tst.bat¦dir HTTP/1.0"      404
scanner.com - - [18/Apr/2000:23:27:16] "HEAD /publisher/ HTTP/1.0"               404
scanner.com - - [18/Apr/2000:23:27:18] "HEAD /.htaccess HTTP/1.0"                403
scanner.com - - [18/Apr/2000:23:27:19] "HEAD /.htpasswd HTTP/1.0"                404
scanner.com - - [18/Apr/2000:23:27:19] "HEAD /cgi-bin/Cgitest.exe HTTP/1.0"      404
scanner.com - - [18/Apr/2000:23:27:19] "HEAD NOTE: Your server has been
                                        ➥scanned for default vulnerabilities!
                                        ➥HTTP/1.0"                              400
```

Remote Procedure Call – rpc.cmsd

```
May 25 22:56:40 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 25 22:58:42 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 25 23:00:42 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 25 23:02:42 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 25 23:04:42 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 00:47:04 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 00:49:04 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 00:51:04 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 03:39:39 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 03:41:40 192.168.1.67 rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 03:43:40 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 15:31:17 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 15:32:07 fw inet: inetd shutdown succeeded
May 26 15:33:18 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 15:34:58 fw inet: inetd shutdown succeeded
May 26 15:35:19 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 15:36:37 fw inet: inetd shutdown succeeded
May 26 15:37:20 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 15:37:40 fw inet: inetd shutdown succeeded
```

Remote Procedure Call – rpc.cmsd

```
May 26 15:38:38 fw inet: inetd shutdown succeeded
May 26 15:39:21 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 15:40:27 fw inet: inetd shutdown succeeded
May 26 15:41:22 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 26 15:43:23 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
May 30 15:55:54 solaris rpc.cmsd: [ID 767094 daemon.error]
➥svc_reg(tcp) failed
```

CVE-1999-0696

One more example – rpc.statd

Snort output:

```
[**] IDS15 - RPC - portmap-request-status [**]
08/12-22:32:27.256042 SCANNER.OTHER.NET:783 -> NFS_SERVER.MY.NET:111
UDP TTL:64 TOS:0x0 ID:41021
Len: 64

[**] IDS181 - OVERFLOW-NOOP-X86 [**]
08/12-22:32:27.263002 SCANNER.OTHER.NET:862 -> NFS_SERVER.MY.NET:1011
UDP TTL:64 TOS:0x0 ID:64250
Len: 1120
```

CVE-1999-0018
CVE-1999-0019

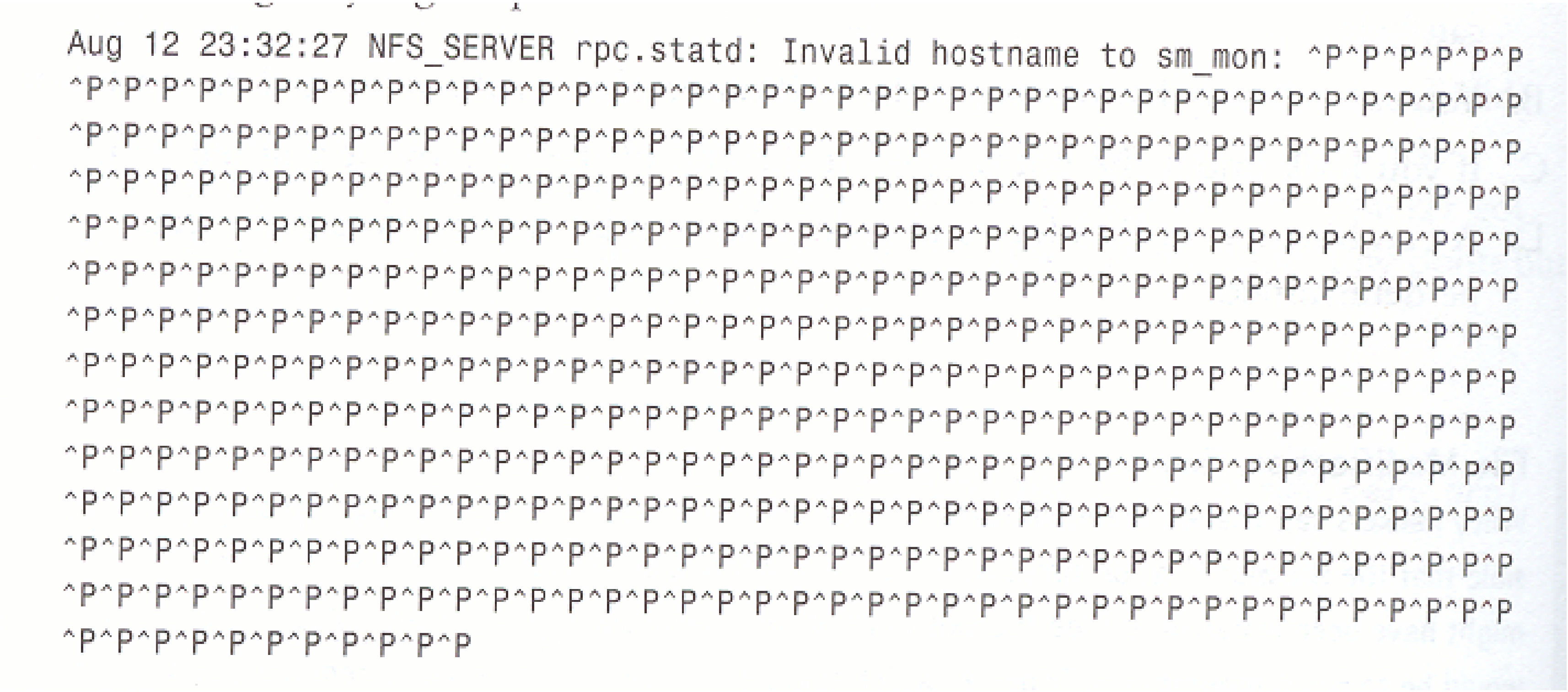
One more example – rpc.statd

TCPdump:

```
22:32:27.256028 SCANNER.OTHER.NET.783 > NFS_SERVER.MY.NET.sunrpc: udp 56
➥(ttl 64, id 41021)
22:32:27.257397 NFS_SERVER.MY.NET.sunrpc > SCANNER.OTHER.NET.783: udp 28
➥(ttl 64, id 49957)
22:32:27.262975 SCANNER.OTHER.NET.862 > NFS_SERVER.MY.NET.1011: udp 1112
➥(ttl 64, id 64250)
22:32:27.274461 NFS_SERVER.MY.NET.1011 > SCANNER.OTHER.NET.862: udp 32
➥(ttl 64, id 49958)
```

One more example – rpc.statd

Syslog data:



```
Aug 12 23:32:27 NFS_SERVER rpc.statd: Invalid hostname to sm_mon: ^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P^P
^P^P^P^P^P^P^P^P^P^P^P
```

One more example – rpc.statd

RPCinfo -p

```
program vers proto   port
 100000    2   tcp    111  portmapper
 100000    2   udp    111  portmapper
 100005    3   udp   1023  mountd
 100005    3   tcp   1023  mountd
```

…

sadmind and mountd Buffer Overflows

- sadmind:
  - CVE-1999-0977
  - Buffer overflow attack
  - Exploit source code available online
- mountd
  - CVE-1999-0002
  - Boundary Condition Error
  - Exploit source code available online

Imapd and Pop server

- Imapd and Pop Server Buffer Overflows
  - CVE-1999-0005: Imapd buffer overflow in its authenticate command
  - CVE-1999-0006
  - CVE-1999-0042
  - CVE-1999-0920
  - CVE-2000-0091

SNMP

- Can provide attackers a lot of information about the network and host configuration
- CVE-1999-0517
- CVE-1999-0516

Default SNMP Community Name

```
[**] SNMP public access [**]
05/29-16:58:21.047981 216.164.136.103:1029 -> 192.168.1.67:161 UDP TTL:49 TOS:
➥0x0 ID:11015
Len: 51
[**] SNMP public access [**]
05/29-16:58:23.034753 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11016
Len: 51
[**] SNMP public access [**]
05/29-16:58:25.029843 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11017
Len: 51
[**] SNMP public access [**]
05/29-16:58:27.003695 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11020
Len: 51
[**] SNMP public access [**]
05/29-16:58:29.047705 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11021
Len: 51
[**] SNMP public access [**]
05/29-16:58:31.042419 216.164.136.103:1029 -> 192.168.1.67:161
UDP TTL:49 TOS:0x0 ID:11023
Len: 51

dragon (Towards) 22:58:22
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 07 00 00 31 11 26 61 d8 a4 88 67 c7 ef 0f 43 E..G+...1.&a...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00                            .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:24
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
```

Default SNMP Community Name

```
45 00 00 47 2b 08 00 00 31 11 26 60 d8 a4 88 67 c7 ef 0f 43 E..G+...1.&`...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00                            .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:26
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 09 00 00 31 11 26 5f d8 a4 88 67 c7 ef 0f 43 E..G+...1.&_...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00                            .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:28
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 0c 00 00 31 11 26 5c d8 a4 88 67 c7 ef 0f 43 E..G+...1.&\...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00                            .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:30
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 0d 00 00 31 11 26 5b d8 a4 88 67 c7 ef 0f 43 E..G+...1.&[...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00                            .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
dragon (Towards) 22:58:32
SOURCE: 216.164.136.103 216-164-136-103.s103.tnt4.lnhva.md.dialup.rcn.com
DEST: 192.168.1.67 solaris.evilscan.com
45 00 00 47 2b 0f 00 00 31 11 26 59 d8 a4 88 67 c7 ef 0f 43 E..G+...1.&Y...g...C
04 05 00 a1 00 33 a2 95 30 29 02 01 00 04 06 70 75 62 6c 69 .....3..0).....publi
63 a0 1c 02 04 5e 11 07 42 02 01 00 02 01 00 30 0e 30 0c 06 c....^..B......0.0..
08 2b 06 01 02 01 01 01 00 05 00                            .+.........
EVENT1: [SNMP:PUBLIC] (udp,dp=161,sp=1029)
```

BIND Weakness

The following is Snort output data:

```
[**] IDS277 - NAMED Iquery Probe [**]
08/12-22:26:16.869305 SCANNER.OTHER.NET:1132 -> DNS_SERVER.MY.NET:53
UDP TTL:64 TOS:0x0 ID:48361
Len: 35

[**] MISC-DNS-version-query [**]
08/12-22:26:16.875718 SCANNER.OTHER.NET:1132 -> DNS_SERVER.MY.NET:53
UDP TTL:64 TOS:0x0 ID:48362
Len: 38

[**] IDS212 - MISC - DNS Zone Transfer [**]
08/12-22:26:17.102688 SCANNER.OTHER.NET:1200 -> DNS_SERVER.MY.NET:53
TCP TTL:64 TOS:0x0 ID:48366  DF
*****PA* Seq: 0x7663C408   Ack: 0x8DADD372   Win: 0x4470
```

BIND Weakness

The following is a TCPdump output of the same traffic:

```
22:26:16.869288 SCANNER.OTHER.NET.1132 > DNS_SERVER.MY.NET.domain:
➥12329 inv_q+ [b2&3=0x980] A? . (27) (ttl 64, id 48361)
22:26:16.875275 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1132:
➥12329 inv_q q: [4.3.2.1]. 1/0/0 . (42) (ttl 64, id 45177)
```

Continue on the next slide

BIND Weakness

```
22:26:16.875704 SCANNER.OTHER.NET.1132 > DNS_SERVER.MY.NET.domain:
➥13448+ [b2&3=0x180] (30) (ttl 64, id 48362)
22:26:17.059765 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1132:
➥13448* q: version.bind. 1/0/0  (63) (ttl 64, id 52055)

22:26:17.097466 SCANNER.OTHER.NET.1200 > DNS_SERVER.MY.NET.domain:
➥S 1986249733:1986249733(0) win 16384  (DF) (ttl 64, id 48363)
22:26:17.099362 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1200:
➥S 2376979313:2376979313(0) ack 1986249734 win 17520  (ttl 64, id 56245)
22:26:17.099770 SCANNER.OTHER.NET.1200 > DNS_SERVER.MY.NET.domain:
➥. ack 1 win 17520 (DF) (ttl 64, id 48364)
22:26:17.100400 SCANNER.OTHER.NET.1200 > DNS_SERVER.MY.NET.domain:
➥P 1:3(2) ack 1 win 17520 (DF) (ttl 64, id 48365)
22:26:17.102376 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1200:
➥. ack 3 win 17520 (ttl 64, id 56432)
22:26:17.102669 SCANNER.OTHER.NET.1200 > DNS_SERVER.MY.NET.domain:
➥P 3:30(27) ack 1 win 17520 (DF) (ttl 64, id 48366)
22:26:17.104083 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1200:
➥. ack 30 win 17520 (ttl 64, id 52126)
22:26:17.183542 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1200:
➥. 1:1461(1460) ack 30 win 17520 (ttl 64, id 62659)
22:26:17.184045 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1200:
➥P 1461:2049(588) ack 30 win 17520 (ttl 64, id 37419)
22:26:17.184943 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1200:
➥FP 2049:2342(293) ack 30 win 17520 (ttl 64, id 34864)
22:26:17.185066 SCANNER.OTHER.NET.1200 > DNS_SERVER.MY.NET.domain:
➥. ack 2343 win 15282 (DF) (ttl 64, id 48368)
22:26:17.211787 SCANNER.OTHER.NET.1200 > DNS_SERVER.MY.NET.domain:
➥F 30:30(0) ack 2343 win 17520 (DF) (ttl 64, id 48369)
22:26:17.213217 DNS_SERVER.MY.NET.domain > SCANNER.OTHER.NET.1200:
➥. ack 31 win 17520 (ttl 64, id 60072)
```

BIND Weakness

The following is the syslog record of these transactions:

```
Aug 12 22:26:15 DNS_SERVER named[19779]: XX /DNS_SERVER/DNS_SERVER/-A
Aug 12 22:26:15 DNS_SERVER named[19779]: XX /DNS_SERVER/version.bind/TXT
Aug 12 22:26:16 DNS_SERVER named[19779]: approved AXFR from
[SCANNER.OTHER.NET].1200 for "MY.NET"
Aug 12 22:26:16 DNS_SERVER named[19779]: XX /DNS_SERVER/MY.NET/AXFR
```