Global Information Assurance Certification Paper

Practical Assignment for GCIA Certification
Submitted by: James L. Benanti

I. Network Detects

Detect One

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:07.798832 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:57547  DF
**S***** Seq: 0x9DBE8C   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:07.798898 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9144  DF
**S***A* Seq: 0x83DE8D9E   Ack: 0x9DBE8D   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:07.799432 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:57803  DF
******A* Seq: 0x9DBE8D   Ack: 0x83DE8D9F   Win: 0x2238

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:07.800281 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:58059  DF
*****PA* Seq: 0x9DBE8D   Ack: 0x83DE8D9F   Win: 0x2238
00 72 6F 6F 74 00 2D 66 72 6F 6F 74 00 76 74 31  .root.-froot.vt1
30 30 2F 39 36 30 30 00                          00/9600.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:07.800356 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9145  DF
******A* Seq: 0x83DE8D9F   Ack: 0x9DBEA5   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:07.815556 192.168.1.162:1088 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:9146
Len: 52
69 29 01 00 00 01 00 00 00 00 00 00 03 31 32 39  i)...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.820466 192.168.1.162:1088 -> 129.250.35.250:53
UDP TTL:64 TOS:0x0 ID:9147
Len: 52
69 29 01 00 00 01 00 00 00 00 00 00 03 31 32 39  i)...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.846667 129.250.35.250:53 -> 192.168.1.162:1088
UDP TTL:245 TOS:0x0 ID:10695  DF
Len: 134
69 29 81 83 00 01 00 00 00 01 00 00 03 31 32 39  i)...........129
```

```
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 03 31 36 38  dr.arpa......168
03 31 39 32 07 49 4E 2D 41 44 44 52 04 41 52 50  .192.IN-ADDR.ARP
41 00 00 06 00 01 00 00 16 80 00 32 09 62 6C 61  A.........2.bla
63 6B 68 6F 6C 65 03 69 73 69 03 65 64 75 00 08  ckhole.isi.edu..
62 6D 61 6E 6E 69 6E 67 C0 56 01 30 BE DA 00 00  bmanning.V.0....
2A 30 00 00 03 84 00 09 3A 80 00 01 51 80        *0.....:...Q.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.852633 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9148  DF
*****PA* Seq: 0x83DE8D9F   Ack: 0x9DBEA5   Win: 0x7D78
00                                .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.855780 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:17356  DF
****R*** Seq: 0x9DBEA5   Ack: 0xCAF0F4   Win: 0x0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.948317 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:17612  DF
**S***** Seq: 0x9DBE92   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.948398 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9149  DF
**S***A* Seq: 0x842D20D8   Ack: 0x9DBE93   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.948949 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:17868  DF
******A* Seq: 0x9DBE93   Ack: 0x842D20D9   Win: 0x2238

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.949749 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:18124  DF
*****PA* Seq: 0x9DBE93   Ack: 0x842D20D9   Win: 0x2238
00 72 6F 6F 74 00 2D 66 72 6F 6F 74 00 76 74 31  .root.-froot.vt1
30 30 2F 39 36 30 30 00                  00/9600.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.949808 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9150  DF
******A* Seq: 0x842D20D9   Ack: 0x9DBEAB   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:12.966186 192.168.1.162:1088 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:9151
Len: 52
BC E5 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:17.970460 192.168.1.162:1088 -> 129.250.35.250:53
UDP TTL:64 TOS:0x0 ID:9152
Len: 52
BC E5 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:17.997780 129.250.35.250:53 -> 192.168.1.162:1088
UDP TTL:245 TOS:0x0 ID:10696  DF
Len: 134
BC E5 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 03 31 36 38  dr.arpa......168
03 31 39 32 07 49 4E 2D 41 44 44 52 04 41 52 50  .192.IN-ADDR.ARP
41 00 00 06 00 01 00 00 16 7B 00 32 09 62 6C 61  A........{.2.bla
63 6B 68 6F 6C 65 03 69 73 69 03 65 64 75 00 08  ckhole.isi.edu..
62 6D 61 6E 6E 69 6E 67 C0 56 01 30 BE DA 00 00  bmanning.V.0....
2A 30 00 00 03 84 00 09 3A 80 00 01 51 80        *0......:...Q.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.004075 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9153  DF
*****PA* Seq: 0x842D20D9   Ack: 0x9DBEAB   Win: 0x7D78
00                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.006579 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:43724  DF
****R*** Seq: 0x9DBEAB   Ack: 0xCB0E47   Win: 0x0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.108145 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:43980  DF
**S***** Seq: 0x9DBE9B   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.108231 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9154  DF
**S***A* Seq: 0x847BDC71   Ack: 0x9DBE9C   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.108742 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:44236  DF
******A* Seq: 0x9DBE9C   Ack: 0x847BDC72   Win: 0x2238

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.109660 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:44492  DF
*****PA* Seq: 0x9DBE9C   Ack: 0x847BDC72   Win: 0x2238
00 72 6F 6F 74 00 2D 66 72 6F 6F 74 00 76 74 31  .root.-froot.vt1
30 30 2F 39 36 30 30 00                          00/9600.
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.109729 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9155  DF
******A* Seq: 0x847BDC72   Ack: 0x9DBEB4   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:18.126593 192.168.1.162:1088 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:9156
Len: 52
EC C0 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:20.935261 192.168.2.10:53 -> 192.168.1.162:1088
UDP TTL:127 TOS:0x0 ID:28469
Len: 52
69 29 81 82 00 01 00 00 00 00 00 00 03 31 32 39  i)...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:23.662956 192.168.2.10:53 -> 192.168.1.162:1088
UDP TTL:127 TOS:0x0 ID:30005
Len: 52
BC E5 81 82 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:23.663472 192.168.1.162:1088 -> 129.250.35.250:53
UDP TTL:64 TOS:0x0 ID:9157
Len: 52
EC C0 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:23.697397 129.250.35.250:53 -> 192.168.1.162:1088
UDP TTL:245 TOS:0x0 ID:10697  DF
Len: 134
EC C0 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 03 31 36 38  dr.arpa......168
03 31 39 32 07 49 4E 2D 41 44 44 52 04 41 52 50  .192.IN-ADDR.ARP
41 00 00 06 00 01 00 00 16 75 00 32 09 62 6C 61  A........u.2.bla
63 6B 68 6F 6C 65 03 69 73 69 03 65 64 75 00 08  ckhole.isi.edu..
62 6D 61 6E 6E 69 6E 67 C0 56 01 30 BE DA 00 00  bmanning.V.0....
2A 30 00 00 03 84 00 09 3A 80 00 01 51 80        *0......:...Q.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:23.703415 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9158  DF
*****PA* Seq: 0x847BDC72   Ack: 0x9DBEB4   Win: 0x7D78
00                                               .
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:23.706564 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:34253  DF
****R*** Seq: 0x9DBEB4   Ack: 0xCB4EF4   Win: 0x0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:24.100759 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:34509  DF
**S***** Seq: 0x9DBEA5   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:24.100841 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9159  DF
**S***A* Seq: 0x84D74D15   Ack: 0x9DBEA6   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:24.101358 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:34765  DF
******A* Seq: 0x9DBEA6   Ack: 0x84D74D16   Win: 0x2238

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:24.102271 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:35021  DF
*****PA* Seq: 0x9DBEA6   Ack: 0x84D74D16   Win: 0x2238
00 72 6F 6F 74 00 2D 66 72 6F 6F 74 00 76 74 31  .root.-froot.vt1
30 30 2F 39 36 30 30 00                          00/9600.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:24.102336 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9160  DF
******A* Seq: 0x84D74D16   Ack: 0x9DBEBE   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:24.117382 192.168.1.162:1088 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:9161
Len: 52
B0 49 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .I...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.120468 192.168.1.162:1088 -> 129.250.35.250:53
UDP TTL:64 TOS:0x0 ID:9162
Len: 52
B0 49 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .I...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.153910 129.250.35.250:53 -> 192.168.1.162:1088
UDP TTL:245 TOS:0x0 ID:10698  DF
Len: 134
B0 49 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .I...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
```

```
64 72 04 61 72 70 61 00 00 0C 00 01 03 31 36 38  dr.arpa......168
03 31 39 32 07 49 4E 2D 41 44 44 52 04 41 52 50  .192.IN-ADDR.ARP
41 00 00 06 00 01 00 00 16 70 00 32 09 62 6C 61  A........p.2.bla
63 6B 68 6F 6C 65 03 69 73 69 03 65 64 75 00 08  ckhole.isi.edu..
62 6D 61 6E 6E 69 6E 67 C0 56 01 30 BE DA 00 00  bmanning.V.0....
2A 30 00 00 03 84 00 09 3A 80 00 01 51 80        *0......:...Q.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.160119 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9163  DF
*****PA* Seq: 0x84D74D16   Ack: 0x9DBEBE   Win: 0x7D78
00                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.162921 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:28110  DF
****R*** Seq: 0x9DBEBE   Ack: 0xCB8A0E   Win: 0x0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.255557 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:28366  DF
**S***** Seq: 0x9DBEB3   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.255629 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9164  DF
**S***A* Seq: 0x8525F4F8   Ack: 0x9DBEB4   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.256113 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:28622  DF
******A* Seq: 0x9DBEB4   Ack: 0x8525F4F9   Win: 0x2238

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.257025 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:28878  DF
*****PA* Seq: 0x9DBEB4   Ack: 0x8525F4F9   Win: 0x2238
00 72 6F 6F 74 00 2D 66 72 6F 6F 74 00 76 74 31  .root.-froot.vt1
30 30 2F 39 36 30 30 00                          00/9600.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.257093 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9165  DF
******A* Seq: 0x8525F4F9   Ack: 0x9DBECC   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:29.273861 192.168.1.162:1088 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:9166
Len: 52
2D 31 01 00 00 01 00 00 00 00 00 00 03 31 32 39  -1...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
09/01-16:01:31.750560 192.168.2.10:53 -> 192.168.1.162:1088
UDP TTL:127 TOS:0x0 ID:41525
Len: 52
EC C0 81 82 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.760459 192.168.1.162:1088 -> 129.250.35.250:53
UDP TTL:64 TOS:0x0 ID:9167
Len: 52
2D 31 01 00 00 01 00 00 00 00 00 00 03 31 32 39  -1...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.801463 129.250.35.250:53 -> 192.168.1.162:1088
UDP TTL:245 TOS:0x0 ID:10699  DF
Len: 134
2D 31 81 83 00 01 00 00 00 01 00 00 03 31 32 39  -1...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 03 31 36 38  dr.arpa......168
03 31 39 32 07 49 4E 2D 41 44 44 52 04 41 52 50  .192.IN-ADDR.ARP
41 00 00 06 00 01 00 00 16 6A 00 32 09 62 6C 61  A........j.2.bla
63 6B 68 6F 6C 65 03 69 73 69 03 65 64 75 00 08  ckhole.isi.edu..
62 6D 61 6E 6E 69 6E 67 C0 56 01 30 BE DA 00 00  bmanning.V.0....
2A 30 00 00 03 84 00 09 3A 80 00 01 51 80        *0......:...Q.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.807557 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9168  DF
*****PA* Seq: 0x8525F4F9   Ack: 0x9DBECC   Win: 0x7D78
00                                .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.810722 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:62670  DF
****R*** Seq: 0x9DBECC   Ack: 0xCBAEC3   Win: 0x0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.903039 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:62926  DF
**S***** Seq: 0x9DBEC7   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.903120 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9169  DF
**S***A* Seq: 0x857C217A   Ack: 0x9DBEC8   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.903640 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:63182  DF
******A* Seq: 0x9DBEC8   Ack: 0x857C217B   Win: 0x2238
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.904597 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:63438  DF
*****PA* Seq: 0x9DBEC8   Ack: 0x857C217B   Win: 0x2238
00 72 6F 6F 74 00 2D 66 72 6F 6F 74 00 76 74 31  .root.-froot.vt1
30 30 2F 39 36 30 30 00                          00/9600.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.904663 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:9170  DF
******A* Seq: 0x857C217B   Ack: 0x9DBEE0   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:34.921205 192.168.1.162:1088 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:9171
Len: 52
0C BC 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:38.781238 192.168.2.10:53 -> 192.168.1.162:1088
UDP TTL:127 TOS:0x0 ID:59701
Len: 52
B0 49 81 82 00 01 00 00 00 00 00 00 03 31 32 39  .I...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:39.790457 192.168.1.162:1088 -> 129.250.35.250:53
UDP TTL:64 TOS:0x0 ID:9172
Len: 52
0C BC 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:39.816468 129.250.35.250:53 -> 192.168.1.162:1088
UDP TTL:245 TOS:0x0 ID:10704  DF
Len: 134
0C BC 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 03 31 36 38  dr.arpa......168
03 31 39 32 07 49 4E 2D 41 44 44 52 04 41 52 50  .192.IN-ADDR.ARP
41 00 00 06 00 01 00 00 16 65 00 32 09 62 6C 61  A........e.2.bla
63 6B 68 6F 6C 65 03 69 73 69 03 65 64 75 00 08  ckhole.isi.edu..
62 6D 61 6E 6E 69 6E 67 C0 56 01 30 BE DA 00 00  bmanning.V.0....
2A 30 00 00 03 84 00 09 3A 80 00 01 51 80        *0......:...Q.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:39.822446 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9173  DF
*****PA* Seq: 0x857C217B   Ack: 0x9DBEE0   Win: 0x7D78
00                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
09/01-16:01:39.826564 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9174  DF
*****PAU Seq: 0x857C217C   Ack: 0x9DBEE0   Win: 0x7D78
80                                .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:39.830033 192.168.1.162:513 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x10 ID:9175  DF
***F**A* Seq: 0x857C217D   Ack: 0x9DBEE0   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:39.830517 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:24271  DF
******A* Seq: 0x9DBEE0   Ack: 0x857C217E   Win: 0x2237

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:39.831111 192.168.1.129:1023 -> 192.168.1.162:513
TCP TTL:128 TOS:0x0 ID:24527  DF
****R*** Seq: 0x9DBEE0   Ack: 0x857C217E   Win: 0x0
```

Source of Trace:
This trace was generated using NetSonar to attack a victim Linux workstation on my lab LAN. My lab LAN has RFC1918 addressing and hide NAT is used to enable legal routing on the Internet. The attacker is 192.168.1.129 and the victim is 192.168.1.162 (these will be referenced as "attacker" and "victim" throughout the rest of this document). The lab's LAN is connected to the internet via a DSL router and a CheckPoint VPN-1 firewall serves as perimeter protection.

Detect was generated by:
Running Cisco's NetSonar vulnerability testing software on a Windows 98 workstation. The victim was a Red Hat Linux v6.2 workstation running Snort v1.6.3 with the 08/29/2000 rule set. The rule set (as well as the Snort software itself) was downloaded from the Snort Web page (www.snort.org) and contains 818 rules which are used to define attack patterns which trigger alerts.

The Snort output is formatted as follows:
[**] Detect Messages [**] (this will identify a signature match from the above mentioned rule set)
Date mm/dd-hh:mm:ss.decimal First.IP.Address -> (dataflow direction) Second.IP.Address
Decode of header info (Protocol – TCP/UDP/ICMP) flags if any, ID's ETC.[Protocol dependent]

Data in HEX Data in ASCII

Probability the source address was spoofed:
Very low. This attack will not work without first completing the three-way handshake to a specific host. The attacker would need to be able to see system responses and prompts to continue the attack. The attacker is probably using a system at someone else's site that has already been "rooted" or a system which is going to be "thrown away" from which to launch the attack.

Description of attack:
The rlogin daemon of some AIX and Linux systems allow an attacker to gain remote root access without having to specify a password. By specifying the "-froot" option to the rlogin command, vulnerable systems will immediately drop the remote user into a root shell. This vulnerability affects some Linux and AIX 3.x systems. Please reference the Cert Advisory *CA-94.09.bin.login.vulnerability* or *CVE-1999-0113* for futher discussion.

Attack mechanism:
The attack works by first completing the three-way handshake to port 513 which is the well-known remote login port (rlogind) for AIX, BSD and Linux. A packet is then pushed to the victim host containing the "root –froot" string in its data field as the username and option to rlogind.

The trace then shows the target host doing an inverse address lookup to gain the identity of the attacking host – typical protocol behavior which I sometimes reject at the firewall to increase connection response – using the well-known dns port 53. A failed inverse lookup will not reset the connection or kill the attack.

After the lookup is attempted, the victim host sends an ACK to the attacker to continue the connection. At this point, the attack is completed and the attacker has access to the host. In this trace, the attacker simply sends a reset to tear-down the connection.

A hostile attacker, after successfully running this exploit and gaining root access to the victim may then undertake several courses of action including but not limited to:

- creating new users/passwords for his/her own use
- creating hidden directories for "warez" use
- copying the /etc/password file to his own machine
- cleaning up logs of his activities
- installing back doors and trojans

The attacker may even repair the vulnerability to ensure that other attackers cannot also exploit it.

The URLs mentioned above, give instructions on how to repair the vulnerability. The issue here, may be in trying to determine just what the attacker did to the victim host. This could be simple if a mechanism such as Tripwire was regularly used to check and take a snapshot of the host , not so simple if regular backups of the system were made, and nearly impossible in the absence of either of these. A last resort would be to disconnect the host from your network (not power it down) and then do a total off-line rebuild and patch of the host. Be sure to repair the vulnerability and check for additional ones before putting the machine back into production.

Correlations:
This vulnerability was detected and known as early as March of 1994 as seen in the Bugtraq archives at http://geek-girl.com/bugtraq/1994_3/0100.html. References to it are also available at the CERT and CVE sites using the URLs mentioned above.

Evidence of Active Targeting:

This attack is definitely targeted at a specific host. Probability is high that at this point recon. work was already done and the attacker has identified the host as having an Operating System that is known to be vulnerable to this attack.

Severity:

Criticality: 2 due to the fact that the victim host is a Linux desktop system and does not provide critical services to the network.

Lethality: 5 due to the fact that the attacker can gain root to the victim host and may be able to do this across the network using trust relationships.

System Countermeasures: 4 due to the fact that this is a modern OS, however some patching and configuation will be necessary to bring it up-to-date and secure it.

Network Countermeasures: 4 due to the fact that a permissive firewall is in place and the host is monitored

by Snort IDS. This vulnerability, although detected, is still not stopped.
(2+5) – (4+4) = -1

Defensive Recommendation:

Network countermeasures can be increased by configuring the VPN-1 firewall to allow only trusted hosts access to specific hosts on the network using the rlogin service port. System countermeasures can be increased by applying the configuration changes outlined in the CERT advisory mentioned in the URL above.

Possible Multiple Choice Question:

Why does the trace include packets generated by an inverse name lookup?

a. This is network traffic that coincidentally occurred during the event
b. This is typical of a connection oriented protocol attempting to build trust relationships by identifying the source host
c. The source host needs to identify the destination host before a connection can occur
d. The destination host needs to identify the source host before a connection can occur

Answer: b

Detect Two

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.391388 192.168.1.129:2947 -> 192.168.1.162:6000
TCP TTL:128 TOS:0x0 ID:31951  DF
**S***** Seq: 0x9DBED8   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.391453 192.168.1.162:6000 -> 192.168.1.129:2947
TCP TTL:64 TOS:0x0 ID:9176  DF
**S***A* Seq: 0x859B4456   Ack: 0x9DBED9   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.391934 192.168.1.129:2947 -> 192.168.1.162:6000
TCP TTL:128 TOS:0x0 ID:32207  DF
******A* Seq: 0x9DBED9   Ack: 0x859B4457   Win: 0x2238

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.393360 192.168.1.129:2947 -> 192.168.1.162:6000
TCP TTL:128 TOS:0x0 ID:32463  DF
*****PA* Seq: 0x9DBED9   Ack: 0x859B4457   Win: 0x2238
42 00 00 0B 00 00 00 00 00 00 00 00             B...........

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.393405 192.168.1.162:6000 -> 192.168.1.129:2947
TCP TTL:64 TOS:0x0 ID:9177  DF
******A* Seq: 0x859B4457   Ack: 0x9DBEE5   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.393771 192.168.1.162:6000 -> 192.168.1.129:2947
TCP TTL:64 TOS:0x0 ID:9178  DF
*****PA* Seq: 0x859B4457   Ack: 0x9DBEE5   Win: 0x7D78
00 2D 00 0B 00 00 00 0C 43 6C 69 65 6E 74 20 69  .-......Client i
73 20 6E 6F 74 20 61 75 74 68 6F 72 69 7A 65 64  s not authorized
20 74 6F 20 63 6F 6E 6E 65 63 74 20 74 6F 20 53   to connect to S
65 72 76 65 72 D5 39 08                          erver.9.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.393816 192.168.1.162:6000 -> 192.168.1.129:2947
TCP TTL:64 TOS:0x0 ID:9179  DF
***F**A* Seq: 0x859B448F   Ack: 0x9DBEE5   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.394374 192.168.1.129:2947 -> 192.168.1.162:6000
TCP TTL:128 TOS:0x0 ID:32719  DF
******A* Seq: 0x9DBEE5   Ack: 0x859B4490   Win: 0x2200

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:41.395445 192.168.1.129:2947 -> 192.168.1.162:6000
TCP TTL:128 TOS:0x0 ID:32975  DF
***F**A* Seq: 0x9DBEE5   Ack: 0x859B4490   Win: 0x2200

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

09/01-16:01:41.395472 192.168.1.162:6000 -> 192.168.1.129:2947
TCP TTL:64 TOS:0x0 ID:9180 DF
******A* Seq: 0x859B4490 Ack: 0x9DBEE6 Win: 0x7D78

Source of Trace:
This trace was generated using NetSonar to attack a victim Linux workstation on my lab LAN. My lab LAN has RFC1918 addressing and hide NAT is used to enable legal routing on the Internet. The attacker is 192.168.1.129 and the victim is 192.168.1.162 (these will be referenced as "attacker" and "victim" throughout the rest of this document). The lab's LAN is connected to the internet via a DSL router and a CheckPoint VPN-1 firewall serves as perimeter protection.

Detect was generated by:
Running Cisco's NetSonar vulnerability testing software on a Windows 98 workstation. The victim was a Red Hat Linux v6.2 workstation running Snort v1.6.3 with the 08/29/2000 rule set. The rule set (as well as the Snort software itself) was downloaded from the Snort Web page (www.snort.org) and contains 818 rules which are used to define attack patterns which trigger alerts.

The Snort output is formatted as follows:
[**] Detect Messages [**] (this will identify a signature match from the above mentioned rule set)
Date mm/dd-hh:mm:ss.decimal First.IP.Address -> (dataflow direction) Second.IP.Address
Decode of header info (Protocol – TCP/UDP/ICMP) flags if any, ID's ETC.[Protocol dependent]

Data in HEX Data in ASCII

Probability the source address was spoofed:
Very low. This attack will not work without first completing the three-way handshake to a specific host. The attacker would need to be able to see system responses and prompts to continue the attack. The attacker is probably using a system at someone else's site that has already been "rooted" or a system which is going to be "thrown away" from which to launch the attack.

Description of attack:
This is an attack against port 6000, which is the TCP and UDP port used for the XWINDOWS system. The specific attack is known as *xwin xhost+*. This vulnerability is used to determine if an X server has been configured to allow connections from any host or restricted to only the local host. Please reference CVE-1999-0526 or http://www.uwsg.indiana.edu/usail/external/recommended/Xsecure.html for further discussion.

Attack mechanism:
The attack works by completing the three-way handshake on port 6000 and then testing if the X server is configured to allow connections from any host.

The handshake is necessary because attempting to start an Xwindow on a host that runs no X server will simply hang the calling process. So, if the handshake is good, then the attacker knows that the X server is running, on port 6000, and that the exploit can be continued.

A "B" is sent from the attacker to the victim – to date, I have not figured out exactly why a "B" is used. I think that any character can be used since this attack is testing to see if the X server allows connections from untrusted hosts.

The victim then sends "Client is not authorized to connect to Server" in response to the attacker. This means that the X server was configured to restrict X window connections to the local host only. This is a good move from a security standpoint and serves to thwart the attack.

Correlations:
This vulnerability was detected and known as early as March of 1996 as seen in the URLs listed above.

Evidence of Active Targeting:
This attack is definitely targeted at a specific host. Probability is high that at this point recon. work was already done and the attacker has identified the host as having an Operating System that is known to be vulnerable to this attack.

Severity:
Criticality: 2 due to the fact that the victim host is a Linux desktop system and does not provide critical services to the network.

Lethality: 3 due to the fact that the attacker has only identified a vulnerability at this point. A username/password combination would have to sniffed or learned in order to log on and gain access to the system.

System Countermeasures: 5 due to the fact that this is a modern OS and configuation has been done to thwart this exploit at the victim.

Network Countermeasures: 4 due to the fact that a permissive firewall is in place and the host is monitored by Snort IDS. This vulnerability, although detected, is still not stopped by network countermeasures.
(2+3) – (5+4) = -4

Defensive Recommendation

Network countermeasures can be increased by configuring the VPN-1 firewall to allow only trusted hosts access to specific hosts on the network using the X Window System service port (if this is required then those selected hosts will need to be reconfigured to allow X Window connections from all hosts). System countermeasures are in place and correct allowing only local host access.

Multiple Choice Test Question

This attack relies heavily on successful completion of the three-way handshake because

a. A complete tcp connection must be completed prior to attempting the exploit
b. Attempting the exploit against a host that is not running an X server will hang the attacking host
c. It is not necessary and only done for reasons of consistency

Answer: b

Detect Three

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.934677 192.168.1.129:2945 -> 192.168.1.162:79
TCP TTL:128 TOS:0x0 ID:1739  DF
**S***** Seq: 0x9DBE70   Ack: 0x0   Win: 0x2000
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.934744 192.168.1.162:79 -> 192.168.1.129:2945
TCP TTL:64 TOS:0x0 ID:9136  DF
**S***A* Seq: 0x82E23F6E   Ack: 0x9DBE71   Win: 0x7D78
TCP Options => MSS: 1460

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.935285 192.168.1.129:2945 -> 192.168.1.162:79
TCP TTL:128 TOS:0x0 ID:1995  DF
******A* Seq: 0x9DBE71   Ack: 0x82E23F6F   Win: 0x2238

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.936189 192.168.1.129:2945 -> 192.168.1.162:79
TCP TTL:128 TOS:0x0 ID:2251  DF
*****PA* Seq: 0x9DBE71   Ack: 0x82E23F6F   Win: 0x2238
7C 2F 62 69 6E 2F 69 64 0A                      |/bin/id.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.936252 192.168.1.162:79 -> 192.168.1.129:2945
TCP TTL:64 TOS:0x0 ID:9137  DF
******A* Seq: 0x82E23F6F   Ack: 0x9DBE7A   Win: 0x7D78

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.954158 192.168.1.162:79 -> 192.168.1.129:2945
TCP TTL:64 TOS:0x0 ID:9138  DF
*****PA* Seq: 0x82E23F6F   Ack: 0x9DBE7A   Win: 0x7D78
66                                              f

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.954775 192.168.1.162:79 -> 192.168.1.129:2945
TCP TTL:64 TOS:0x0 ID:9139  DF
***F*PA* Seq: 0x82E23F70   Ack: 0x9DBE7A   Win: 0x7D78
69 6E 67 65 72 3A 20 7C 2F 62 69 6E 2F 69 64 3A  inger: |/bin/id:
20 6E 6F 20 73 75 63 68 20 75 73 65 72 2E 0D 0A   no such user...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.955328 192.168.1.129:2945 -> 192.168.1.162:79
TCP TTL:128 TOS:0x0 ID:2507  DF
******A* Seq: 0x9DBE7A   Ack: 0x82E23F91   Win: 0x2217

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/01-16:01:01.956270 192.168.1.129:2945 -> 192.168.1.162:79
TCP TTL:128 TOS:0x0 ID:2763  DF
****R*** Seq: 0x9DBE7A   Ack: 0x82E23F91   Win: 0x0
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Source of Trace:
This trace was generated using NetSonar to attack a victim Linux workstation on my lab LAN. My lab LAN has RFC1918 addressing and hide NAT is used to enable legal routing on the Internet. The attacker is 192.168.1.129 and the victim is 192.168.1.162 (these will be referenced as "attacker" and "victim" throughout the rest of this document). The lab's LAN is connected to the internet via a DSL router and a CheckPoint VPN-1 firewall serves as perimeter protection.

Detect was generated by:
Running Cisco's NetSonar vulnerability testing software on a Windows 98 workstation. The victim was a Red Hat Linux v6.2 workstation running Snort v1.6.3 with the 08/29/2000 rule set. The rule set (as well as the Snort software itself) was downloaded from the Snort Web page (www.snort.org) and contains 818 rules which are used to define attack patterns which trigger alerts.

The Snort output is formatted as follows:
[**] Detect Messages [**] (this will identify a signature match from the above mentioned rule set)
Date mm/dd-hh:mm:ss.decimal First.IP.Address -> (dataflow direction) Second.IP.Address
Decode of header info (Protocol – TCP/UDP/ICMP) flags if any, ID's ETC.[Protocol dependent]

Data in HEX Data in ASCII

Probability the source address was spoofed:
Very low. This attack will not work without first completing the three-way handshake to a specific host. The attacker would need to be able to see system responses and prompts to continue the attack. The attacker is probably using a system at someone else's site that has already been "rooted" or a system which is going to be "thrown away" from which to launch the attack.

Description of attack:
This attack is targeted at port 79 which is the well-known port for the finger service. Finger can give an attacker information, such as login accounts and trusted hosts. This attack is done as an information gathering exercise designed to return usernames and trust information to the attacker.

Attack Mechanism:
The attack is started by first completing the three-way handshake to establish that the finger service port is listening and to create a connection. The attacker then sends a packet containing the text "|/bin/id". This text contains the pipe command character "|" that instructs Unix and Linux machines to redirect output to some destination other than the standard output device. In this attack the output of the finger service will be sent to a file called *id* in the */bin* directory.

The victim sends an ACK and then sends two packets containing the reply to the finger service request as "finger: |/bin/id: no such user". So, in this trace, the attacker gained no user information, but does now know that the finger service is running.

This attack can be extremely useful to an attacker when you consider how the finger service works. First, it reads and interprets the /etc/password file giving the login ID, comment field, home location, and login command issued. Next the /var/run/utmp file is checked and if the user is logged on it displays for how long, on which terminal, and from where. Then it checks to see if the user has any mail waiting to be read. Next, it looks for a .plan file in the users home directory which contains information that the user wants displayed when he is looked up. The finger service will give quite a bit of public information and care should be taken to control what information is displayed. An administrator may wish to disable the service or install one that only gives limited information.

Correlations:
This vulnerability has been known for some time and can be seen as early as March, 1997 at http://xforce.iss.net/static/48.php . It can also be referenced at the CVE site by entering CVE-1999-0612.

Evidence of Active Targeting:
This attack is definitely targeted at a specific host. Probability is high that at this point some recon. work was already done and the attacker has identified the host as having an Operating System that is known to be vulnerable to this attack. This attack is a continuation of the recon. process since it is designed to return user and trust data back to the attacker. It is also aimed at a target using Linux or Unix since these are the operating systems that run the finger service.

Severity:
Criticality: 2 due to the fact that the victim host is a Linux desktop system and does not provide critical services to the network.

Lethality: 2 the attacker was unable to gain user names. Even if user names and trusts were given, he must still go through a brute force password crack to gain access to the system. Therefore I view this as more of a breach in confidentiality.

System Countermeasures: 5 due to the fact that this is a modern OS and configuation has been done to thwart this exploit at the victim by using a finger daemon that only gives limited (no) information.

Network Countermeasures: 4 due to the fact that a permissive firewall is in place and the host is monitored by Snort IDS. This vulnerability, although detected, is still not stopped by network countermeasures.
(2+2) – (5+4) = -5

Defensive Recommendation:
Network countermeasures can be increased by configuring the VPN-1 firewall to drop or reject inbound external traffic using port 79. This would block all finger requests from outside hosts to the internal network. Desktop systems can also be configured to disable the finger service or to install a finger daemon that limits the information provided (such as the victim in the above traces).

Multiple Choice Test Question:
In the traces above, the attacker uses the "|" character for what purpose?

a. To pipe output to a file
b. The listening service requires the character as part of its command syntax
c. To conceal the fact that the command is coming from an external source
d. To exploit a known vulnerability in the listening service

Answer: a

Detect Four

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.518660 192.168.1.129:2565 -> 192.168.1.162:98
TCP TTL:64 TOS:0x0 ID:1872  DF
**S***** Seq: 0x89E00EAB   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47462 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.518716 192.168.1.162:98 -> 192.168.1.129:2565
TCP TTL:64 TOS:0x0 ID:3735  DF
**S***A* Seq: 0x73A92C37   Ack: 0x89E00EAC   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173553 47462 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.519251 192.168.1.129:2565 -> 192.168.1.162:98
TCP TTL:64 TOS:0x0 ID:1873  DF
******A* Seq: 0x89E00EAC   Ack: 0x73A92C38   Win: 0x7D78
TCP Options => NOP NOP TS: 47462 173553

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.520440 192.168.1.129:2565 -> 192.168.1.162:98
TCP TTL:64 TOS:0x0 ID:1874  DF
*****PA* Seq: 0x89E00EAC   Ack: 0x73A92C38   Win: 0x7D78
TCP Options => NOP NOP TS: 47462 173553
47 45 54 20 2F 20 48 54 54 50 2F 31 2E 31 0D 0A  GET / HTTP/1.1..
0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.520484 192.168.1.162:98 -> 192.168.1.129:2565
TCP TTL:64 TOS:0x0 ID:3736  DF
******A* Seq: 0x73A92C38   Ack: 0x89E00EBE   Win: 0x7D78
TCP Options => NOP NOP TS: 173553 47462

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.520856 192.168.1.162:98 -> 192.168.1.129:2565
TCP TTL:64 TOS:0x0 ID:3737  DF
*****PA* Seq: 0x73A92C38   Ack: 0x89E00EBE   Win: 0x7D78
TCP Options => NOP NOP TS: 173554 47462
35 30 30 20 61 63 63 65 73 73 20 64 65 6E 69 65  500 access denie
64 3A 20 43 68 65 63 6B 20 6E 65 74 77 6F 72 6B  d: Check network
69 6E 67 2F 6C 69 6E 75 78 63 6F 6E 66 20 6E 65  ing/linuxconf ne
74 77 6F 72 6B 20 61 63 63 65 73 73 0D 0A        twork access..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.520904 192.168.1.162:98 -> 192.168.1.129:2565
TCP TTL:64 TOS:0x0 ID:3738  DF
***F**A* Seq: 0x73A92C76   Ack: 0x89E00EBE   Win: 0x7D78
TCP Options => NOP NOP TS: 173554 47462

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.521438 192.168.1.129:2565 -> 192.168.1.162:98
TCP TTL:64 TOS:0x0 ID:1875  DF
******A* Seq: 0x89E00EBE   Ack: 0x73A92C76   Win: 0x7D78
TCP Options => NOP NOP TS: 47462 173554
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.521515 192.168.1.129:2565 -> 192.168.1.162:98
TCP TTL:64 TOS:0x0 ID:1876  DF
******A* Seq: 0x89E00EBE   Ack: 0x73A92C77   Win: 0x7D78
TCP Options => NOP NOP TS: 47462 173554

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.521985 192.168.1.129:2565 -> 192.168.1.162:98
TCP TTL:64 TOS:0x0 ID:1877  DF
***F**A* Seq: 0x89E00EBE   Ack: 0x73A92C77   Win: 0x7D78
TCP Options => NOP NOP TS: 47462 173554

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.522017 192.168.1.162:98 -> 192.168.1.129:2565
TCP TTL:64 TOS:0x0 ID:3739  DF
******A* Seq: 0x73A92C77   Ack: 0x89E00EBF   Win: 0x7D78
TCP Options => NOP NOP TS: 173554 47462
```

Source of Trace:
This trace was generated using Nessus to attack a victim Linux workstation on my lab LAN. My lab LAN has RFC1918 addressing and hide NAT is used to enable legal routing on the Internet. The attacker is 192.168.1.129 and the victim is 192.168.1.162 (these will be referenced as “attacker” and “victim” throughout the rest of this document). The lab’s LAN is connected to the internet via a DSL router and a CheckPoint VPN-1 firewall serves as perimeter protection.

Detect was generated by:
This detect was generated by running the Nessus (www.nessus.org) vulnerability testing software on a Red Hat Linux v6.1 workstation. The victim was a Red Hat Linux v6.2 workstation running Snort v1.6.3 with the 08/29/2000 rule set. The rule set (as well as the Snort software itself) was downloaded from the Snort Web page (www.snort.org) and contains 818 rules which are used to define attack patterns which trigger alerts.

The Snort output is formatted as follows:
[**] Detect Messages [**] (this will identify a signature match from the above mentioned rule set)
Date mm/dd-hh:mm:ss.decimal First.IP.Address -> (dataflow direction) Second.IP.Address
Decode of header info (Protocol – TCP/UDP/ICMP) flags if any, ID’s ETC.[Protocol dependent]

Data in HEX Data in ASCII

Probability the source address was spoofed:
Very low. This attack will not work without first completing the three-way handshake to a specific host. The attacker would need to be able to see system responses and prompts to continue the attack. The attacker is probably using a system at someone else’s site that has already been “rooted” or a system which is going to be “thrown away” from which to launch the attack.

Description of attack:
This attack is directed against the Linux Configuration utility (linuxconf) which uses the well-known port 98. Linuxconf is an Xwindows-based GUI configuration tool for Linux system administration. This utility is known to contain various buffer overflows and access to it should not be allowed via a network connection.

Attack Mechanism:
This attack starts by completing a connection (three-way handshake) to TCP port 98. After this is completed, the command “GET / HTTP/1.1” is issued to the victim. The GET command is attempting to test the victim’s handling of HTTP headers. In this case, the victim’s response is “access denied: Check networking/linuxconf network access” indicating that the linuxconf utility has been configured to not allow

connection to this port via the network. Had access been allowed, the exploit would then continue on to issue an excessively long URL statement in an attempt to cause a buffer overflow and gain root access to the victim host.

Correlations:
This vulnerability has been known for some time and can be seen as early as March, 1997 at http://xforce.iss.net/static/48.php . It can also be referenced at the CVE site by entering CVE-1999-0612.

Evidence of Active Targeting:
This attack is definitely targeted at a specific host. Probability is high that at this point some recon. work was already done and the attacker has identified the host as having an Operating System that is known to be vulnerable to this attack. This attack is a continuation of the recon. process since it is designed to return user and trust data back to the attacker. It is also aimed at a target using Linux or Unix since these are the operating systems that run the finger service.

Severity:
Criticality: 2 due to the fact that the victim host is a Linux desktop system and does not provide critical services to the network.

Lethality: 2 the attacker was unable to gain user names. Even if user names and trusts were given, he must still go through a brute force password crack to gain access to the system. Therefore I view this as more of a breach in confidentiality.

System Countermeasures: 5 due to the fact that this is a modern OS and configuation has been done to thwart this exploit at the victim by using a finger daemon that only gives limited (no) information.

Network Countermeasures: 4 due to the fact that a permissive firewall is in place and the host is monitored by Snort IDS. This vulnerability, although detected, is still not stopped by network countermeasures.
(2+2) – (5+4) = -5

Defensive Recommendation:
Network countermeasures can be increased by configuring the VPN-1 firewall to drop or reject inbound external traffic using port 79. This would block all finger requests from outside hosts to the internal network. Desktop systems can also be configured to disable the finger service or to install a finger daemon that limits the information provided (such as the victim in the above traces).

Multiple Choice Test Question:
In the traces above, the attacker uses the "|" character for what purpose?

e. To pipe output to a file
f. The listening service requires the character as part of its command syntax
g. To conceal the fact that the command is coming from an external source
h. To exploit a known vulnerability in the listening service

Answer: a

II. Evaluate An Attack

Attack Tool Description

Nessus (www.nessus.org) vulnerability testing software was used to generate this attack. Nessus is a free network security scanner used to evaluate a network's defensive state against malicious activity. Nessus uses *plugins* – code modules that are downloaded and added to the base program – to add new vulnerability tests to keep the product as up-to-date as possible. One interesting thing about Nessus is that it will not merely attempt to use well-known ports for testing, but will attempt to locate the service regardless of what port it is running on. Nessus also disregards software version numbers and will attempt to run the exploit if a service is found to be running irregardless of the version of that service.

Attack Description

The particular plugin used in this attack is called "*rsh on finger output"* which attempts to gain restricted shell access, via the rsh port, using information returned to it via finger output. However, before attempting the finger queery, it tries to use well-known user id's for backdoors and Trojans, that typically use the rsh port, to gain access to the system.

So why use the restricted shell? The restricted shell is designed to *restrict* a user's capabilities by disallowing certain capabilities that the standard shell allows. The list of disallowed actions is very short:

- Cannot change directory (cd)
- Cannot change PATH or SHELL variables
- Cannot specify a path to a command
- Cannot redirect output (> and >>)
- Cannot exec programs

In Unix/Linux, commands for a restricted user are contained in /usr/rbin. The commands in this directory can simply be copied from /usr/bin into /usr/rbin and care needs to be taken when choosing the commands you allow restricted users to use. You would not want to give access to the shell, a compiler, or chmod as these may be used to bypass the restricted shell. So, the attacker is attempting to gain access in the hopes that he can then exploit a poorly configured restricted shell.

The r utilities also depend upon IP addresses for authentication to build trust relationships which is a dangerous concept. Trusted hosts are defined in two different files: /etc/hosts.equiv and .rhosts . This explains the inverse address lookups throughout the following trace. Linux is looking to equate a host name with the IP address in order to test for a trust relationship.

If a host name is listed in the /etc/hosts.equiv file and the user's name appears in the /etc/passwd file, then the user is allowed to use the rlogin or rsh without providing a password. There is a single wildcard character that can be used in the /etc/hosts.equiv file, the "+". If the /etc/hosts.equiv file contains only the "+" then all hosts are trusted. Many Sun systems were delivered in this configuration. Care should be taken to check the /etc/hosts.equiv file for the "+" and to remove it if it exists.

This attack cannot be done with a spoofed source address since the attacker needs to be able to create a connection (complete the three-way handshake) and receive responses back from the victim host. The attacker must also have already done some initial network mapping and OS fingerprinting since this attack is going to be aimed at a Unix or Linux system.

This is also an attack that, in order to thwart detection, could be done "low and slow" (not as it appears in the following trace). The exploit could also be done from different source hosts at different times – again, in an effort to be stealthy.

An attacker, if successful, would be able to gain remote shell access and begin to hack the system. The level of this attack depends on the hostility of the attacker as well as the privileges granted him upon successful login to the system.

In terms of prevention, perimeter devices and firewalls may be configured to disallow this type of traffic into the internal network. Also, the host system should be configured to remove "r" utilities if they're not necessary.

Attack Code

Following is the Nessus plug-in code that executes this attack with my comments in blue:

```
Nessus attempts to determine which port is running the rsh service. If the function cannot determine
the port, the well-known port is used… function login(port, name)
{
 soc = open_priv_sock_tcp(dport:port);

Here, the packet is crafted and sent to the victim…
 if(soc)
 {
  s1 = raw_string(0);
  s2 = name + raw_string(0) + name + raw_string(0) + "id" + raw_string(0);

  send(socket:soc, data:s1);
  send(socket:soc, data:s2);

Pattern matching is done to determine if a login was successful. If so, a message is sent to the
Nessus log along with a solution to repair the vulnerability…
  a = recv(socket:soc, length:1024);
  a = recv(socket:soc, length:1024);
  if(ereg(string:a, pattern:"^uid.*$"))
  {
   data = "It was possible to log into this host using the account '" + name +
              "' !" + string("\n") + "Either it is passwordless or the file " +
              "~/.rhosts is not configured properly." + string("\n") +
              "Here is the output of the command 'id' : " + string("\n") + string("\n") + a + string("\n")
+
              "Solution : remove ~/.rhosts or set a password" + string("\n") +
              "Risk factor : High";
   security_hole(port:port, data:data);
  }
  close(soc);
 }
}

This function determines which port is listening for rsh. If none is found, the well-known port is
used…
port = get_kb_item("Services/rsh");
if(!port)port = 514;
if(!get_port_state(port))exit(0);

Call the login function to test root and well-known backdoor and trojan user id's…
login(port:port, name:"root");
```

```
#
# these will most likely find backdoor rather
# than real unconfigured systems
#
login(port:port, name:"toor");
login(port:port, name:"bin");
login(port:port, name:"daemon");
login(port:port, name:"operator");
login(port:port, name:"nobody");
login(port:port, name:"adm");
login(port:port, name:"ftp");
login(port:port, name:"postgres");
login(port:port, name:"gdm");
```

Now the attempt is made at a finger queery…

Look for the finger service on any port, if none is found, use the well-known port 79…

```
finger_port = get_kb_item("Services/finger");
if(!finger_port)finger_port = 79;
```

If no finger port was found, exit the routine…

```
if(!get_port_state(finger_port))exit(0);
```

Call the function to send the finger packets…

```
finger = open_sock_tcp(finger_port);
send(socket:finger, data:string("\r\n"));
r = recv_line(socket:finger, length:1024);
```

Loop to attempt login using returned finger info, if any…

```
if(!r)exit(0);
r = recv_line(socket:finger, length:1024);

tested = " root toor bin daemon operator nobody adm ftp postgres gdm ";

while(r)
{
 s = strstr(r," ");
 r = r - s;
 pat = ".* " + r + " .*";

 if(!ereg(string:tested, pattern:pat))
 {
 tested = tested + " " + r + " ";
 login(name:r, port:port);
 }
 r = recv_line(socket:finger, length:1024);
}

close(finger);
```

Below is the trace I captured of this attack with my comments in blue…

Here's your basic three-way handshake to tcp port 514, the well-known port for rshd…

=+

09/08-08:23:29.578099 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1884 DF
S*** Seq: 0x8A0BA64E Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47468 0 NOP WS: 0

=+
09/08-08:23:29.578146 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3740 DF
S*A* Seq: 0x73D869A2 Ack: 0x8A0BA64F Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173559 47468 NOP WS: 0

=+
09/08-08:23:29.578632 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1885 DF
******A* Seq: 0x8A0BA64F Ack: 0x73D869A3 Win: 0x7D78
TCP Options => NOP NOP TS: 47468 173559

=+
09/08-08:23:29.580755 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1886 DF
*****PA* Seq: 0x8A0BA64F Ack: 0x73D869A3 Win: 0x7D78
TCP Options => NOP NOP TS: 47468 173559
00 .

=+
09/08-08:23:29.580827 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3741 DF
******A* Seq: 0x73D869A3 Ack: 0x8A0BA650 Win: 0x7D78
TCP Options => NOP NOP TS: 173560 47468

The first attempt at trying the "root" user id…
=+
09/08-08:23:29.581295 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1887 DF
*****PA* Seq: 0x8A0BA650 Ack: 0x73D869A3 Win: 0x7D78
TCP Options => NOP NOP TS: 47468 173560
72 6F 6F 74 00 72 6F 6F 74 00 69 64 00 root.root.id.

=+
09/08-08:23:29.590766 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3742 DF
******A* Seq: 0x73D869A3 Ack: 0x8A0BA65D Win: 0x7D78
TCP Options => NOP NOP TS: 173561 47468

Here's an inverse address lookup in an attempt to equate an IP address with a host name to allow a check for trusted hosts…
=+
09/08-08:23:29.594362 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3743
Len: 52
DF 93 01 00 00 01 00 00 00 00 00 00 03 31 32 39 129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64 .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 dr.arpa.....

Can't resolve the address so we go to the "black hole"…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.596265 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:63828
Len: 114
DF 93 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 72 00 32 09 62 6C 61 63 6B 68 6F  ....Pr.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 76                    ....:....v
```

The Linux system denies permission since no trust can be built, and also because there's no user id/password match in the etc/passwd file since the attack does not supply passwords…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.717168 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3744  DF
*****PA* Seq: 0x73D869A3   Ack: 0x8A0BA65D   Win: 0x7D78
TCP Options => NOP NOP TS: 173573 47468
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.718150 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1902  DF
******A* Seq: 0x8A0BA65D   Ack: 0x73D869B7   Win: 0x7D78
TCP Options => NOP NOP TS: 47482 173573
```

This connection is closed…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.720191 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3745  DF
***F**A* Seq: 0x73D869B7   Ack: 0x8A0BA65D   Win: 0x7D78
TCP Options => NOP NOP TS: 173573 47482

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.720689 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1903  DF
******A* Seq: 0x8A0BA65D   Ack: 0x73D869B8   Win: 0x7D78
TCP Options => NOP NOP TS: 47482 173573

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.722700 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1904  DF
***F**A* Seq: 0x8A0BA65D   Ack: 0x73D869B8   Win: 0x7D78
TCP Options => NOP NOP TS: 47482 173573

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.723306 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3746  DF
******A* Seq: 0x73D869B8   Ack: 0x8A0BA65E   Win: 0x7D78
TCP Options => NOP NOP TS: 173574 47482
```

Another three-way handshake to open the conection over which the attack will attempt to use backdoor/trojan user ids. Done in the hope that the system has previously been hacked and a backdoor/trojan was planted. This same pattern repeats while the attack tries 9 user id's…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.723494 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1905  DF
**S***** Seq: 0x8A435F83   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47482 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.723542 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3747  DF
**S***A* Seq: 0x73D5C8B1   Ack: 0x8A435F84   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173574 47482 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.724025 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1906  DF
******A* Seq: 0x8A435F84   Ack: 0x73D5C8B2   Win: 0x7D78
TCP Options => NOP NOP TS: 47482 173574

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.725938 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1907  DF
*****PA* Seq: 0x8A435F84   Ack: 0x73D5C8B2   Win: 0x7D78
TCP Options => NOP NOP TS: 47482 173574
00                                                .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.726002 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3748  DF
******A* Seq: 0x73D5C8B2   Ack: 0x8A435F85   Win: 0x7D78
TCP Options => NOP NOP TS: 173574 47482
```

First, it tries “toor”…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.731352 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1910  DF
*****PA* Seq: 0x8A435F85   Ack: 0x73D5C8B2   Win: 0x7D78
TCP Options => NOP NOP TS: 47483 173574
74 6F 6F 72 00 74 6F 6F 72 00 69 64 00          toor.toor.id.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.740761 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3749  DF
******A* Seq: 0x73D5C8B2   Ack: 0x8A435F92   Win: 0x7D78
TCP Options => NOP NOP TS: 173576 47483

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.741197 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3750
Len: 52
9D 51 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .Q...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.742269 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:64084
```

```
Len: 114
9D 51 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .Q...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:....u

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.745626 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3751  DF
*****PA* Seq: 0x73D5C8B2   Ack: 0x8A435F92   Win: 0x7D78
TCP Options => NOP NOP TS: 173576 47483
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.746040 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3752  DF
***F**A* Seq: 0x73D5C8C6   Ack: 0x8A435F92   Win: 0x7D78
TCP Options => NOP NOP TS: 173576 47483

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.746219 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1913  DF
******A* Seq: 0x8A435F92   Ack: 0x73D5C8C6   Win: 0x7D78
TCP Options => NOP NOP TS: 47485 173576

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.746888 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1914  DF
******A* Seq: 0x8A435F92   Ack: 0x73D5C8C7   Win: 0x7D78
TCP Options => NOP NOP TS: 47485 173576

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.752292 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1915  DF
***F**A* Seq: 0x8A435F92   Ack: 0x73D5C8C7   Win: 0x7D78
TCP Options => NOP NOP TS: 47485 173576

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.752343 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3753  DF
******A* Seq: 0x73D5C8C7   Ack: 0x8A435F93   Win: 0x7D78
TCP Options => NOP NOP TS: 173577 47485

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.753541 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1916  DF
**S***** Seq: 0x8A0E53A2   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47485 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.753586 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3754  DF
```

```
**S***A* Seq: 0x73DA5DB8   Ack: 0x8A0E53A3   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173577 47485 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.754018 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1917  DF
******A* Seq: 0x8A0E53A3   Ack: 0x73DA5DB9   Win: 0x7D78
TCP Options => NOP NOP TS: 47485 173577

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.755989 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1918  DF
*****PA* Seq: 0x8A0E53A3   Ack: 0x73DA5DB9   Win: 0x7D78
TCP Options => NOP NOP TS: 47485 173577
00                                              .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.756058 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3755  DF
******A* Seq: 0x73DA5DB9   Ack: 0x8A0E53A4   Win: 0x7D78
TCP Options => NOP NOP TS: 173577 47485
```

Next, it tries "bin"…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.758082 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1919  DF
*****PA* Seq: 0x8A0E53A4   Ack: 0x73DA5DB9   Win: 0x7D78
TCP Options => NOP NOP TS: 47486 173577
62 69 6E 00 62 69 6E 00 69 64 00                bin.bin.id.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.761641 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3756  DF
******A* Seq: 0x73DA5DB9   Ack: 0x8A0E53AF   Win: 0x7D78
TCP Options => NOP NOP TS: 173578 47486

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.772044 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3757
Len: 52
65 47 01 00 00 01 00 00 00 00 00 00 03 31 32 39  eG...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.773028 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:64340
Len: 114
65 47 81 83 00 01 00 00 00 01 00 00 03 31 32 39  eG...........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:....u
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.784062 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3758  DF
*****PA* Seq: 0x73DA5DB9   Ack: 0x8A0E53AF   Win: 0x7D78
TCP Options => NOP NOP TS: 173580 47486
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.784598 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1922  DF
******A* Seq: 0x8A0E53AF   Ack: 0x73DA5DCD   Win: 0x7D78
TCP Options => NOP NOP TS: 47488 173580

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.784836 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3759  DF
***F**A* Seq: 0x73DA5DCD   Ack: 0x8A0E53AF   Win: 0x7D78
TCP Options => NOP NOP TS: 173580 47488

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.785313 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1923  DF
******A* Seq: 0x8A0E53AF   Ack: 0x73DA5DCE   Win: 0x7D78
TCP Options => NOP NOP TS: 47488 173580

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.789858 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1926  DF
***F**A* Seq: 0x8A0E53AF   Ack: 0x73DA5DCE   Win: 0x7D78
TCP Options => NOP NOP TS: 47489 173580

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.789900 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3760  DF
******A* Seq: 0x73DA5DCE   Ack: 0x8A0E53B0   Win: 0x7D78
TCP Options => NOP NOP TS: 173580 47489

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.791111 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1927  DF
**S***** Seq: 0x8A0EE68A   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47489 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.791162 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3761  DF
**S***A* Seq: 0x73DC51CE   Ack: 0x8A0EE68B   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173581 47489 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.791588 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1928  DF
******A* Seq: 0x8A0EE68B   Ack: 0x73DC51CF   Win: 0x7D78
TCP Options => NOP NOP TS: 47489 173581
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.793558 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1929  DF
*****PA* Seq: 0x8A0EE68B   Ack: 0x73DC51CF   Win: 0x7D78
TCP Options => NOP NOP TS: 47489 173581
00                                         .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.793629 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3762  DF
******A* Seq: 0x73DC51CF   Ack: 0x8A0EE68C   Win: 0x7D78
TCP Options => NOP NOP TS: 173581 47489
```

Trying “daemon”…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.794159 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1930  DF
*****PA* Seq: 0x8A0EE68C   Ack: 0x73DC51CF   Win: 0x7D78
TCP Options => NOP NOP TS: 47489 173581
64 61 65 6D 6F 6E 00 64 61 65 6D 6F 6E 00 69 64  daemon.daemon.id
00                                         .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.801607 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3763  DF
******A* Seq: 0x73DC51CF   Ack: 0x8A0EE69D   Win: 0x7D78
TCP Options => NOP NOP TS: 173582 47489

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.809599 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3764
Len: 52
96 DA 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.810581 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:64596
Len: 114
96 DA 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:....u

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.820332 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3765  DF
*****PA* Seq: 0x73DC51CF   Ack: 0x8A0EE69D   Win: 0x7D78
TCP Options => NOP NOP TS: 173583 47489
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.821262 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1932  DF
******A* Seq: 0x8A0EE69D   Ack: 0x73DC51E3   Win: 0x7D78
TCP Options => NOP NOP TS: 47492 173583

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.822629 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3766  DF
***F**A* Seq: 0x73DC51E3   Ack: 0x8A0EE69D   Win: 0x7D78
TCP Options => NOP NOP TS: 173584 47492

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.823088 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1933  DF
******A* Seq: 0x8A0EE69D   Ack: 0x73DC51E4   Win: 0x7D78
TCP Options => NOP NOP TS: 47492 173584

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.824380 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1934  DF
***F**A* Seq: 0x8A0EE69D   Ack: 0x73DC51E4   Win: 0x7D78
TCP Options => NOP NOP TS: 47492 173584

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.824408 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3767  DF
******A* Seq: 0x73DC51E4   Ack: 0x8A0EE69E   Win: 0x7D78
TCP Options => NOP NOP TS: 173584 47492

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.825715 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1935  DF
**S***** Seq: 0x8A0F6C9B   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47492 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.825762 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3768  DF
**S***A* Seq: 0x73DE45E4   Ack: 0x8A0F6C9C   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173584 47492 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.826194 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1936  DF
******A* Seq: 0x8A0F6C9C   Ack: 0x73DE45E5   Win: 0x7D78
TCP Options => NOP NOP TS: 47493 173584

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.828163 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1937  DF
*****PA* Seq: 0x8A0F6C9C   Ack: 0x73DE45E5   Win: 0x7D78
TCP Options => NOP NOP TS: 47493 173584
00                                        .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
09/08-08:23:29.828239 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3769  DF
******A* Seq: 0x73DE45E5   Ack: 0x8A0F6C9D   Win: 0x7D78
TCP Options => NOP NOP TS: 173584 47493
```

User is “operator”…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.828707 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1938  DF
*****PA* Seq: 0x8A0F6C9D   Ack: 0x73DE45E5   Win: 0x7D78
TCP Options => NOP NOP TS: 47493 173584
6F 70 65 72 61 74 6F 72 00 6F 70 65 72 61 74 6F  operator.operato
72 00 69 64 00                                   r.id.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.830751 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3770  DF
******A* Seq: 0x73DE45E5   Ack: 0x8A0F6CB2   Win: 0x7D78
TCP Options => NOP NOP TS: 173585 47493

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.844493 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3771
Len: 52
01 7E 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .~..........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.845554 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:64852
Len: 114
01 7E 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .~..........129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:....u

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.855642 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3772  DF
*****PA* Seq: 0x73DE45E5   Ack: 0x8A0F6CB2   Win: 0x7D78
TCP Options => NOP NOP TS: 173587 47493
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.856653 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1939  DF
******A* Seq: 0x8A0F6CB2   Ack: 0x73DE45F9   Win: 0x7D78
TCP Options => NOP NOP TS: 47496 173587

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.857796 192.168.1.162:514 -> 192.168.1.129:1023
```

TCP TTL:64 TOS:0x0 ID:3773 DF
***F**A* Seq: 0x73DE45F9 Ack: 0x8A0F6CB2 Win: 0x7D78
TCP Options => NOP NOP TS: 173587 47496

=+
09/08-08:23:29.858241 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1940 DF
******A* Seq: 0x8A0F6CB2 Ack: 0x73DE45FA Win: 0x7D78
TCP Options => NOP NOP TS: 47496 173587

=+
09/08-08:23:29.859686 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1941 DF
***F**A* Seq: 0x8A0F6CB2 Ack: 0x73DE45FA Win: 0x7D78
TCP Options => NOP NOP TS: 47496 173587

=+
09/08-08:23:29.859718 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3774 DF
******A* Seq: 0x73DE45FA Ack: 0x8A0F6CB3 Win: 0x7D78
TCP Options => NOP NOP TS: 173587 47496

=+
09/08-08:23:29.861009 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1942 DF
S*** Seq: 0x8A0FF630 Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47496 0 NOP WS: 0

=+
09/08-08:23:29.861077 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3775 DF
S*A* Seq: 0x73E039FA Ack: 0x8A0FF631 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173588 47496 NOP WS: 0

=+
09/08-08:23:29.861552 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1943 DF
******A* Seq: 0x8A0FF631 Ack: 0x73E039FB Win: 0x7D78
TCP Options => NOP NOP TS: 47496 173588

=+
09/08-08:23:29.863459 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1944 DF
*****PA* Seq: 0x8A0FF631 Ack: 0x73E039FB Win: 0x7D78
TCP Options => NOP NOP TS: 47496 173588
00 .

=+
09/08-08:23:29.863532 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3776 DF
******A* Seq: 0x73E039FB Ack: 0x8A0FF632 Win: 0x7D78
TCP Options => NOP NOP TS: 173588 47496

User id is "nobody"…
=+
09/08-08:23:29.864002 192.168.1.129:1023 -> 192.168.1.162:514

```
TCP TTL:64 TOS:0x0 ID:1945  DF
*****PA* Seq: 0x8A0FF632   Ack: 0x73E039FB   Win: 0x7D78
TCP Options => NOP NOP TS: 47496 173588
6E 6F 62 6F 64 79 00 6E 6F 62 6F 64 79 00 69 64  nobody.nobody.id
00                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.871637 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3777  DF
******A* Seq: 0x73E039FB   Ack: 0x8A0FF643   Win: 0x7D78
TCP Options => NOP NOP TS: 173589 47496

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.879782 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3778
Len: 52
B8 A2 01 00 00 01 00 00 00 00 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.880788 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:65108
Len: 114
B8 A2 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:.....u

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.890851 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3779  DF
*****PA* Seq: 0x73E039FB   Ack: 0x8A0FF643   Win: 0x7D78
TCP Options => NOP NOP TS: 173591 47496
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.891950 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1946  DF
******A* Seq: 0x8A0FF643   Ack: 0x73E03A0F   Win: 0x7D78
TCP Options => NOP NOP TS: 47499 173591

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.892810 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3780  DF
***F**A* Seq: 0x73E03A0F   Ack: 0x8A0FF643   Win: 0x7D78
TCP Options => NOP NOP TS: 173591 47499

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.893255 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1947  DF
******A* Seq: 0x8A0FF643   Ack: 0x73E03A10   Win: 0x7D78
```

```
TCP Options => NOP NOP TS: 47499 173591

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.894722 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1948  DF
***F**A* Seq: 0x8A0FF643   Ack: 0x73E03A10   Win: 0x7D78
TCP Options => NOP NOP TS: 47499 173591

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.896636 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3781  DF
******A* Seq: 0x73E03A10   Ack: 0x8A0FF644   Win: 0x7D78
TCP Options => NOP NOP TS: 173591 47499

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.895927 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1949  DF
**S***** Seq: 0x8A45FFED   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47499 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.897136 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3782  DF
**S***A* Seq: 0x73D7BCC7   Ack: 0x8A45FFEE   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173591 47499 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.898081 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1950  DF
******A* Seq: 0x8A45FFEE   Ack: 0x73D7BCC8   Win: 0x7D78
TCP Options => NOP NOP TS: 47500 173591

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.899529 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1951  DF
*****PA* Seq: 0x8A45FFEE   Ack: 0x73D7BCC8   Win: 0x7D78
TCP Options => NOP NOP TS: 47500 173591
00                              .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.899575 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3783  DF
******A* Seq: 0x73D7BCC8   Ack: 0x8A45FFEF   Win: 0x7D78
TCP Options => NOP NOP TS: 173591 47500
```

Now the attack tries “adm”…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.900023 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1952  DF
*****PA* Seq: 0x8A45FFEF   Ack: 0x73D7BCC8   Win: 0x7D78
TCP Options => NOP NOP TS: 47500 173591
61 64 6D 00 61 64 6D 00 69 64 00             adm.adm.id.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.900744 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3784  DF
```

```
******A* Seq: 0x73D7BCC8   Ack: 0x8A45FFFA   Win: 0x7D78
TCP Options => NOP NOP TS: 173592 47500

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.917192 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3785
Len: 52
2A 90 01 00 00 01 00 00 00 00 00 00 03 31 32 39  *............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.918189 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:65364
Len: 114
2A 90 81 83 00 01 00 00 00 01 00 00 03 31 32 39  *............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:....u

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.928516 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3786  DF
*****PA* Seq: 0x73D7BCC8   Ack: 0x8A45FFFA   Win: 0x7D78
TCP Options => NOP NOP TS: 173594 47500
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.929536 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1953  DF
******A* Seq: 0x8A45FFFA   Ack: 0x73D7BCDC   Win: 0x7D78
TCP Options => NOP NOP TS: 47503 173594

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.930407 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3787  DF
***F**A* Seq: 0x73D7BCDC   Ack: 0x8A45FFFA   Win: 0x7D78
TCP Options => NOP NOP TS: 173594 47503

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.930873 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1954  DF
******A* Seq: 0x8A45FFFA   Ack: 0x73D7BCDD   Win: 0x7D78
TCP Options => NOP NOP TS: 47503 173594

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.932293 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1955  DF
***F**A* Seq: 0x8A45FFFA   Ack: 0x73D7BCDD   Win: 0x7D78
TCP Options => NOP NOP TS: 47503 173594

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

09/08-08:23:29.932343 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3788 DF
******A* Seq: 0x73D7BCDD Ack: 0x8A45FFFB Win: 0x7D78
TCP Options => NOP NOP TS: 173595 47503

=+
09/08-08:23:29.933624 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1956 DF
S*** Seq: 0x8A11118F Ack: 0x0 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47503 0 NOP WS: 0

=+
09/08-08:23:29.933683 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3789 DF
S*A* Seq: 0x73E22E10 Ack: 0x8A111190 Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173595 47503 NOP WS: 0

=+
09/08-08:23:29.934134 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1957 DF
******A* Seq: 0x8A111190 Ack: 0x73E22E11 Win: 0x7D78
TCP Options => NOP NOP TS: 47503 173595

=+
09/08-08:23:29.935915 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1958 DF
*****PA* Seq: 0x8A111190 Ack: 0x73E22E11 Win: 0x7D78
TCP Options => NOP NOP TS: 47503 173595
00 .

=+
09/08-08:23:29.935985 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3790 DF
******A* Seq: 0x73E22E11 Ack: 0x8A111191 Win: 0x7D78
TCP Options => NOP NOP TS: 173595 47503
"ftp"…
=+
09/08-08:23:29.937518 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1959 DF
*****PA* Seq: 0x8A111191 Ack: 0x73E22E11 Win: 0x7D78
TCP Options => NOP NOP TS: 47504 173595
66 74 70 00 66 74 70 00 69 64 00 ftp.ftp.id.

=+
09/08-08:23:29.940761 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3791 DF
******A* Seq: 0x73E22E11 Ack: 0x8A11119C Win: 0x7D78
TCP Options => NOP NOP TS: 173596 47504

=+
09/08-08:23:29.952643 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3792
Len: 52
A7 13 01 00 00 01 00 00 00 00 00 00 03 31 32 39 129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64 .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 dr.arpa.....

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:29.953669 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:85
Len: 114
A7 13 81 83 00 01 00 00 00 01 00 00 03 31 32 39  .............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:....u

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.024666 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3793  DF
*****PA* Seq: 0x73E22E11   Ack: 0x8A11119C   Win: 0x7D78
TCP Options => NOP NOP TS: 173604 47504
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.025655 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1960  DF
******A* Seq: 0x8A11119C   Ack: 0x73E22E25   Win: 0x7D78
TCP Options => NOP NOP TS: 47512 173604

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.026791 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3794  DF
***F**A* Seq: 0x73E22E25   Ack: 0x8A11119C   Win: 0x7D78
TCP Options => NOP NOP TS: 173604 47512

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.027267 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1961  DF
******A* Seq: 0x8A11119C   Ack: 0x73E22E26   Win: 0x7D78
TCP Options => NOP NOP TS: 47513 173604

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.028292 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1962  DF
***F**A* Seq: 0x8A11119C   Ack: 0x73E22E26   Win: 0x7D78
TCP Options => NOP NOP TS: 47513 173604

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.028747 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3795  DF
******A* Seq: 0x73E22E26   Ack: 0x8A11119D   Win: 0x7D78
TCP Options => NOP NOP TS: 173604 47513

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.029648 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1963  DF
**S***** Seq: 0x8A48095F   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47513 0 NOP WS: 0
```

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.030114 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3796  DF
**S***A* Seq: 0x73D9B0DD   Ack: 0x8A480960   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173604 47513 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.030589 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1964  DF
******A* Seq: 0x8A480960   Ack: 0x73D9B0DE   Win: 0x7D78
TCP Options => NOP NOP TS: 47513 173604

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.032383 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1965  DF
*****PA* Seq: 0x8A480960   Ack: 0x73D9B0DE   Win: 0x7D78
TCP Options => NOP NOP TS: 47513 173604
00                                              .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.032455 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3797  DF
******A* Seq: 0x73D9B0DE   Ack: 0x8A480961   Win: 0x7D78
TCP Options => NOP NOP TS: 173605 47513
```

Now try “postgres”…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.032930 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1966  DF
*****PA* Seq: 0x8A480961   Ack: 0x73D9B0DE   Win: 0x7D78
TCP Options => NOP NOP TS: 47513 173605
70 6F 73 74 67 72 65 73 00 70 6F 73 74 67 72 65  postgres.postgre
73 00 69 64 00                                   s.id.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.040755 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3798  DF
******A* Seq: 0x73D9B0DE   Ack: 0x8A480976   Win: 0x7D78
TCP Options => NOP NOP TS: 173606 47513

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.048735 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3799
Len: 52
6A FA 01 00 00 01 00 00 00 00 00 00 03 31 32 39  j............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.049779 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:341
Len: 114
6A FA 81 83 00 01 00 00 00 01 00 00 03 31 32 39  j............129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64  .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06  dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F  ....Pq.2.blackho
```

```
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E  le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00  ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75                    ....:....u

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.052700 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3800  DF
*****PA* Seq: 0x73D9B0DE   Ack: 0x8A480976   Win: 0x7D78
TCP Options => NOP NOP TS: 173607 47513
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.053703 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1967  DF
******A* Seq: 0x8A480976   Ack: 0x73D9B0F2   Win: 0x7D78
TCP Options => NOP NOP TS: 47515 173607

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.054820 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3801  DF
***F**A* Seq: 0x73D9B0F2   Ack: 0x8A480976   Win: 0x7D78
TCP Options => NOP NOP TS: 173607 47515

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.055290 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1968  DF
******A* Seq: 0x8A480976   Ack: 0x73D9B0F3   Win: 0x7D78
TCP Options => NOP NOP TS: 47515 173607

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.056789 192.168.1.129:1022 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1969  DF
***F**A* Seq: 0x8A480976   Ack: 0x73D9B0F3   Win: 0x7D78
TCP Options => NOP NOP TS: 47516 173607

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.056822 192.168.1.162:514 -> 192.168.1.129:1022
TCP TTL:64 TOS:0x0 ID:3802  DF
******A* Seq: 0x73D9B0F3   Ack: 0x8A480977   Win: 0x7D78
TCP Options => NOP NOP TS: 173607 47516

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.058153 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1970  DF
**S***** Seq: 0x8A12F7D2   Ack: 0x0   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 47516 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.058199 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3803  DF
**S***A* Seq: 0x73E42226   Ack: 0x8A12F7D3   Win: 0x7D78
TCP Options => MSS: 1460 SackOK TS: 173607 47516 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.058633 192.168.1.129:1023 -> 192.168.1.162:514
```

TCP TTL:64 TOS:0x0 ID:1971 DF
******A* Seq: 0x8A12F7D3 Ack: 0x73E42227 Win: 0x7D78
TCP Options => NOP NOP TS: 47516 173607

=+
09/08-08:23:30.060407 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1972 DF
*****PA* Seq: 0x8A12F7D3 Ack: 0x73E42227 Win: 0x7D78
TCP Options => NOP NOP TS: 47516 173607
00 .

=+
09/08-08:23:30.060476 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3804 DF
******A* Seq: 0x73E42227 Ack: 0x8A12F7D4 Win: 0x7D78
TCP Options => NOP NOP TS: 173607 47516

"gdm"…
=+
09/08-08:23:30.060955 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1973 DF
*****PA* Seq: 0x8A12F7D4 Ack: 0x73E42227 Win: 0x7D78
TCP Options => NOP NOP TS: 47516 173607
67 64 6D 00 67 64 6D 00 69 64 00 gdm.gdm.id.

=+
09/08-08:23:30.070766 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3805 DF
******A* Seq: 0x73E42227 Ack: 0x8A12F7DF Win: 0x7D78
TCP Options => NOP NOP TS: 173609 47516

=+
09/08-08:23:30.076931 192.168.1.162:1027 -> 192.168.2.10:53
UDP TTL:64 TOS:0x0 ID:3806
Len: 52
F8 D4 01 00 00 01 00 00 00 00 00 00 03 31 32 39 129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64 .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 dr.arpa.....

=+
09/08-08:23:30.077936 192.168.2.10:53 -> 192.168.1.162:1027
UDP TTL:127 TOS:0x0 ID:597
Len: 114
F8 D4 81 83 00 01 00 00 00 01 00 00 03 31 32 39 129
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64 .1.168.192.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 C0 12 00 06 dr.arpa.........
00 01 00 01 50 71 00 32 09 62 6C 61 63 6B 68 6F Pq.2.blackho
6C 65 03 69 73 69 03 65 64 75 00 08 62 6D 61 6E le.isi.edu..bman
6E 69 6E 67 C0 42 01 30 BE DA 00 00 2A 30 00 00 ning.B.0....*0..
03 84 00 09 3A 80 00 00 02 75 ....:....u

=+
09/08-08:23:30.082375 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3807 DF
*****PA* Seq: 0x73E42227 Ack: 0x8A12F7DF Win: 0x7D78
TCP Options => NOP NOP TS: 173610 47516

```
01 50 65 72 6D 69 73 73 69 6F 6E 20 64 65 6E 69  .Permission deni
65 64 2E 0A                                      ed..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.082883 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1974  DF
******A* Seq: 0x8A12F7DF   Ack: 0x73E4223B   Win: 0x7D78
TCP Options => NOP NOP TS: 47518 173610

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.083107 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3808  DF
***F**A* Seq: 0x73E4223B   Ack: 0x8A12F7DF   Win: 0x7D78
TCP Options => NOP NOP TS: 173610 47518

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.083592 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1975  DF
******A* Seq: 0x8A12F7DF   Ack: 0x73E4223C   Win: 0x7D78
TCP Options => NOP NOP TS: 47518 173610

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.085149 192.168.1.129:1023 -> 192.168.1.162:514
TCP TTL:64 TOS:0x0 ID:1976  DF
***F**A* Seq: 0x8A12F7DF   Ack: 0x73E4223C   Win: 0x7D78
TCP Options => NOP NOP TS: 47518 173610

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.085348 192.168.1.162:514 -> 192.168.1.129:1023
TCP TTL:64 TOS:0x0 ID:3809  DF
******A* Seq: 0x73E4223C   Ack: 0x8A12F7E0   Win: 0x7D78
TCP Options => NOP NOP TS: 173610 47518
```

Now the finger port is used to try and get user information…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.088917 192.168.1.129:2566 -> 192.168.1.162:79
TCP TTL:64 TOS:0x0 ID:1979 DF
*****PA* Seq: 0x8A2A8E46   Ack: 0x7437CDF4   Win: 0x7D78
TCP Options => NOP NOP TS: 47519 173610
0D 0A                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.088967 192.168.1.162:79 -> 192.168.1.129:2566
TCP TTL:64 TOS:0x0 ID:3811  DF
******A* Seq: 0x7437CDF4   Ack: 0x8A2A8E48   Win: 0x7D78
TCP Options => NOP NOP TS: 173610 47519
```

User information is returned for the "root" process that is currently logged in. This, of course, is the process running the snort utility…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.197320 192.168.1.162:79 -> 192.168.1.129:2566
TCP TTL:64 TOS:0x0 ID:3812  DF
*****PA* Seq: 0x7437CDF4   Ack: 0x8A2A8E48   Win: 0x7D78
TCP Options => NOP NOP TS: 173621 47519
4C 6F 67 69 6E 20 20 20 20 20 4E 61 6D 65 20 20  Login     Name
20 20 20 20 20 54 74 79 20 20 20 20 20 20 49 64       Tty      Id
```

```
6C 65 20 20 4C 6F 67 69 6E 20 54 69 6D 65 20 20  le  Login Time
20 4F 66 66 69 63 65 20 20 20 20 20 4F 66 66 69   Office     Offi
63 65 20 50 68 6F 6E 65 0D 0A 72 6F 6F 74 20 20  ce Phone..root
20 20 20 20 72 6F 6F 74 20 20 20 20 20 20 2A 3A      root      *:
30 20 20 20 20 20 20 20 20 20 20 20 20 20 53 65  0             Se
70 20 20 38 20 30 37 3A 35 35 0D 0A              p  8 07:55..
```

The connection is closed…

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.197809 192.168.1.162:79 -> 192.168.1.129:2566
TCP TTL:64 TOS:0x0 ID:3813  DF
***F**A* Seq: 0x7437CE70   Ack: 0x8A2A8E48   Win: 0x7D78
TCP Options => NOP NOP TS: 173621 47519

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.198046 192.168.1.129:2566 -> 192.168.1.162:79
TCP TTL:64 TOS:0x0 ID:1980  DF
******A* Seq: 0x8A2A8E48   Ack: 0x7437CE70   Win: 0x7D78
TCP Options => NOP NOP TS: 47530 173621

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.198283 192.168.1.129:2566 -> 192.168.1.162:79
TCP TTL:64 TOS:0x0 ID:1981  DF
******A* Seq: 0x8A2A8E48   Ack: 0x7437CE71   Win: 0x7D78
TCP Options => NOP NOP TS: 47530 173621

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.202665 192.168.1.129:2566 -> 192.168.1.162:79
TCP TTL:64 TOS:0x0 ID:1982  DF
***F**A* Seq: 0x8A2A8E48   Ack: 0x7437CE71   Win: 0x7D78
TCP Options => NOP NOP TS: 47530 173621

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
09/08-08:23:30.202702 192.168.1.162:79 -> 192.168.1.129:2566
TCP TTL:64 TOS:0x0 ID:3814  DF
******A* Seq: 0x7437CE71   Ack: 0x8A2A8E49   Win: 0x7D78
TCP Options => NOP NOP TS: 173622 47530
```

III. "Analyze This" Scenario

The following analysis was done using an incomplete set of data. The "Snort" intrusion detection software package was used to collect information for only a few days. Throughout the duration of the scanning, the system was not functioning at all times which can be attributed to disk storage, power, and other issues. These parameters should be kept in mind when reading this assessment which should be viewed as an overview of the state of your network's security.

The results of this analysis focus on one fundamental point: this network is very interesting to outside parties and a permanent, managed, 24/7/365 IDS system should be put in place to completely monitor security events.

MY.NET.1.3

The host located at MY.NET.1.3 appears to have been compromised. It has launched scans against other hosts on MY.NET searching for exploitable vulnerabilities. This host represents a serious risk to your network's security which should be addressed immediately.

This machine should be disconnected from MY.NET (at the Ethernet port – do not power off) regardless of the services it provides. Losing these services will be a small price to pay as opposed to the risk presented. Analysis should then be done to determine who and how this machine was compromised. Backup all user directories (/home) reformat the disks and reinstall the operating system. Add known and trusted users as new, harden the operating system as much as possible, and place the host back into the network.

MY.NET.70.121
This host seems to have taken part in a Denial-of-Service type attack against MY.NET. On August 8th between 6:30 PM and 6:39 PM, over 22,000 "PING-ICMP Destination Unreachable" alerts were generated with this host as either the source or the destination.

MY.NET.70.121 as Destination (Pinger)	
63.205.40.169	212.204.188.51
4.54.47.148	209.86.165.105
24.4.52.197	209.178.160.203
24.23.96.119	208.246.224.220
216.68.192.50	172.144.77.208
216.127.194.37	172.142.226.94
213.104.51.132	

MY.NET.70.121 as Source (Pingee)	
64.252.35.162	24.129.222.8
24.64.14.47	24.112.94.71
24.3.92.152	213.200.186.173
24.214.40.72	209.49.106.28
24.17.201.70	165.247.120.106
24.168.8.137	157.91.4.81
	141.208.208.81

Also included in the 22,000+ total were "PING-ICMP Destination Unreachable" alerts generated wherein the external host was not only a source, but also a destination in relation to MY.NET.70.121. The following table lists these hosts:

Hosts that were both Sources & Destinations	
63.205.40.169	216.68.192.50
4.54.47.148	212.204.188.51
24.4.52.197	172.142.226.94

Two theories here:

1) a SYN scan may have been launched from MY.NET.70.121 and the "Dest. Unreachable" packets were sent in return. Valid connections would then respond with a SYN/ACK to MY.NET.70.121 but since the scan was sent so rapidly, it soon overflowed itself and began responding to external hosts with the "Dest. Unreachable" packets.
2) a SYN scan was started as a Denial-of-Service attack using MY.NET.70.121 as a crafted source address. The same results would occur in the data.

MY.NET.140.9

This host received more than 5,800 "ICMP – Time Exceeded" packets on August 8th at 6:30 PM. This activity lasted for about 44 minutes. A correlation was discovered in which more than 5,800 "Dest. Unreachable" alerts were also recorded.

Name lookups were done against the sources of these alerts and most were found to have either "nlanr" or "amp" in their names. NLANR – the National Laboratory for Applied Network Research is involved in gathering (among other data) metrics for Internet performance. AMP (Active Monitoring Program) is a part of NLANR that is also involved in this project. Please see http://moat.nlanr.net for additional information.

If MY.NET.140.9 is involved in this study, then this traffic can be considered as friendly fire.

Watchlist 222 Computer Network Center Chinese Academy of Sciences

Due to a large volume of suspicious traffic, watchlist 222 – NET NCFC was created to alert on traffic originating from a specific domain owned by the Computer Network Center Chinese Academy of Sciences. Your site has been receiving a great deal of traffic from this domain targeted at the following hosts:

Destinations Targeted From NCFC	
MY.NET.6.7	MY.NET.100.230
MY.NET.6.35	MY.NET.6.35
MY.NET.253.53	MY.NET.253.42
MY.NET.253.52	MY.NET.145.9
MY.NET.253.43	
MY.NET.253.41	
MY.NET.110.150	

Specifically, on June 28th, a large email was sent to MY.NET.253.41 at 10:47 AM and completing at 11:13 AM. This could indicate that an attachment was contained in this email since it took about 26 minutes to send. Email attachments are a common way to distribute and perhaps install software, viruses, etc. onto networks.

More importantly, is the existence of telnet connections that were made to MY.NET.6.7 on two separate occasions. On July 10th, at 7:13 AM and also on August 4th, at 9:25 PM. This means that the NCFC domain has gained access to this host and additional research should be done to determine if the host has been compromised and if so, how and to what extent.

Traffic To and From Israel

Another watchlist, 220 – IL-ISDNNET-990517, was created to alert on traffic originating from this source domain. A great deal of this traffic seems to be related to NAPSTER using ports 6699 and 6700 and accounts for the large amount of packets being generated by these connections. The rest of this watchlist's traffic should be considered as unidentified and suspect. Not only can Napster contain exploitable vulnerabilities (CAN-2000-0281, CAN-2000-0412 at http://cve.mitre.org) but also other ports used by connections from this domain are known to be used for information gathering. Some examples are:

Port	Well-Known Description
1965	Tivoli NPM
1032	NT INETINFO.EXE

Additional research should be undertaken to determine the nature of these connections.

WinGate Scans

Wingate proxy servers are a favorite target, not only because they can be exploited in various ways but also because they can be used to forward attacks to other hosts. Numerous scans for WinGate servers were found in the data set. See CVE-1999-0290, CVE-1999-0291, CVE-1999-0441, CVE-1999-0494, and CAN-1999-0657 at http://cve.mitre.org for further exploit definition.

Hosts having the most WinGate traffic were:

Host	Alerts
MY.NET.253.10 5	2,908
MY.NET.60.11	303
MY.NET.60.8	259

These hosts, above, appear to have WinGate servers installed since the traffic shows the characteristics of a true proxy connection – not a scan.

SYN-FIN SCANS

Several SYN-FIN scans have been detected against your network. These scans are designed to penetrate perimeter defenses by using port 53 (DNS – which most firewalls allow) in an effort to identify host operating systems. These scans send a packet with both the SYN and FIN flags set creating an anomalous packet which is reacted to in different ways by different operating systems, thus allowing identification.

Since no further attempts to gain additional access to scanned hosts were detected, these scans seemed to be on a recon. mission only.

The following hosts initiated these scans during the monitoring period:

202.0.178.98

inetnum: 202.0.160.0 - 202.0.179.255
netname: CMNET-HK
descr: China Motion Telcom Holdings Ltd.
descr: Roaming Paging Services Provider
descr: Roaming Trunking Services Provider
descr: Hong Kong
country: HK

admin-c: DS1-HK
tech-c: AY1-HK
notify: dickys@hk.super.net
changed: dickysum@hk.super.net 950914
source: APNIC

person: Dicky Shum
address: Rm 2604-2608, Harbour Centre, Wan Chai,
address: Hong Kong
phone: +852 2507 0852
fax-no: +852 2827 9883
e-mail: dickysum@cm.com.hk
nic-hdl: DS1-HK
notify: dickys@hk.super.net
mnt-by: MAINT-NULL
changed: dickysum@hk.super.net 19950914
source: APNIC

person: Alan Yu
address: Rm 2604-2608, Harbour Centre, Wan Chai,
address: Hong Kong
phone: +852 2507 0845
fax-no: +852 2827 9883
e-mail: alanyu@cm.com.hk
nic-hdl: AY1-HK
notify: dickys@hk.super.net
mnt-by: MAINT-NULL
changed: dickysum@hk.super.net 19950914
source: APNIC

63.69.63.2

Query: 63.69.63.2
Registry: whois.arin.net
Results:
UUNET Technologies, Inc. (NETBLK-UUNET63) UUNET63 63.64.0.0 - 63.123.255.255
Guthrie & Assoc. & Realty (NETBLK-UU-63-69-63) UU-63-69-63
63.69.63.0 - 63.69.63.255

63.16.52.48

Query: 63.16.52.48
Registry: whois.arin.net
Results:
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
Maintainer: UUDA

Coordinator:
UUnet, AlterNet - Technical Support (OA12-ARIN) help@UUNET.UU.NET
+1 (800) 900-0241

Domain System inverse mapping provided by:

DIALDNS1.UU.NET 153.39.194.10
DIALDNS2.UU.NET 153.39.194.26

ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE

Record last updated on 31-Jul-2000.
Database last updated on 28-Sep-2000 18:07:38 EDT.

212.177.241.139

inetnum: 212.177.0.0 - 212.177.255.255
netname: IT-UUNET-990512
descr: PROVIDER
country: IT
admin-c: RM997-RIPE
tech-c: SC301-RIPE
status: ALLOCATED PA
mnt-by: RIPE-NCC-HM-MNT
changed: hostmaster@ripe.net 19990512
source: RIPE

person: Ron Milner
address: UUNET International
address: 332 Science Park
address: Cambridge CB4 4BZ
address: United Kingdom
phone: +44 1223 250444
fax-no: +44 1223 250373
e-mail: ronm@uk.uu.net
e-mail: milner@uu.net
nic-hdl: RM997-RIPE
changed: ronm@uk.uu.net 19980108
source: RIPE

person: Sam Critchley
address: UUNET European Operations Centre BV
address: Muyskenweg 22
address: 1096 CJ Amsterdam
address: NL
phone: +31 20 711 6082
fax-no: +31 20 711 6071
e-mail: samc@uu.net
nic-hdl: SC301-RIPE
changed: pwhite@uu.net 20000301
source: RIPE

212.171.169.46

inetnum: 212.171.168.0 - 212.171.169.255
netname: TIN
descr: Telecom Italia Net
descr: TIN Standard service in OSPF Area 03
descr: PROVIDER

```
country:    IT
admin-c:    EB339-RIPE
tech-c:     DSF11
tech-c:     MC4803-RIPE
tech-c:     CC297-RIPE
tech-c:     MP3870
tech-c:     SP46-RIPE
status:     ASSIGNED PA
notify:     network@cgi.interbusiness.it
mnt-by:     INTERB-MNT
changed:    cgiadmin@cgi.interbusiness.it 19991111
source:     RIPE

route:      212.171.0.0/16
descr:      INTERBUSINESS
origin:     AS3269
advisory:   AS690 1:701 2:1800
mnt-by:     INTERB-MNT
changed:    cgiadmin@cgi.interbusiness.it 19990524
source:     RIPE

person:     Enzo Berti
address:    Via Val Cannuta, 182
address:    I-00166 RM
phone:      +39 06 36888592
fax-no:     +39 06 36889863
e-mail:     e.berti@tin.it
nic-hdl:    EB339-RIPE
changed:    registdom@tin.it 20000406
changed:    hostmaster@nic.it 20000407
source:     RIPE

person:     Fabio De Simone
address:    Via di Valcannuta 182 00166 Roma
phone:      +39 6 36884847
fax-no:     +39 6 36889863
e-mail:     f.desimone@tin.it
nic-hdl:    DSF11
changed:    registdom@tol.it 19970613
changed:    hostmaster@nis.garr.it 19970616
source:     RIPE

person:     Mauro Carissimi
address:    Telecom Italia
address:    Direzione Rete
address:    Via Val Cannuta, 250
address:    I Roma
address:    Italy
phone:      +39 6 36888849
fax-no:     +39 6 6633553
e-mail:     mauro.carissimi@telecomitalia.it
nic-hdl:    MC4803-RIPE
mnt-by:     INTERB-MNT
changed:    cgiadmin@cgi.interbusiness.it 19991223
source:     RIPE
```

person: Claudio Ciotola
address: Telecom Italia
address: Divisione Clienti Business
address: Via Oriolo Romano, 257
address: I Roma
address: Italy
phone: +39 6 36879293
fax-no: +39 6 33659922
e-mail: ciotola@cgi.interbusiness.it
nic-hdl: CC297-RIPE
changed: domain@cgi.interbusiness.it 20000921
source: RIPE

person: Paolo Malara
address: viale Trento, 39
address: I-09123 CAGLIARI
phone: +39 070 46011
fax-no: +39 070 4601400
e-mail: paolo.malara@tin.it
nic-hdl: MP3870
changed: malara@tin.it 20000705
source: RIPE

person: Salvatore Pulvirenti
address: Video On Line
address: Viale Regina Elena, 20
address: I-09100 Cagliari
address: Italy
phone: +39 70 6013354
fax-no: +39 70 6013312
e-mail: pulvi@vol.it
nic-hdl: SP46-RIPE
changed: hostmaster@vol.it 19970709
changed: hostmaster@nis.garr.it 19970714
source: RIPE

210.84.179.196

inetnum: 210.84.0.0 - 210.84.255.255
netname: OZEMAIL2-AU
descr: OzEmail Pty Ltd
descr: 39 Herbert St
descr: St Leonards, 2065
descr: New South Wales, Australia
country: AU
admin-c: NO7-AP
tech-c: NO7-AP
remarks: service provider
mnt-by: APNIC-HM
mnt-lower: OZEMAIL-NOC
changed: hostmaster@apnic.net 19990617
source: APNIC

person: Network Operations
address: OzEmail Pty Ltd
address: 39 Herbert Street

address: St Leonards, 2065
address: New South Wales, Australia
phone: +61 2 9433 2400
fax-no: +61 2 9437 5888
country: AU
e-mail: network-ops@oznet19.ozemail.com.au
nic-hdl: NO7-AP
mnt-by: OZEMAIL-NOC
changed: stuartt@aone.com.au 19990729
source: APNIC

210.222.31.100

Korea Internet Information
IP Address : 210.222.31.96-210.222.31.127
Connect ISP Name : KORNET
Connect Date : 1999.09.17
Registration Date: 19991027
Network Name : KRJD-GAME

[Organization Information]
Orgnization ID : ORG83658
Name : JD-GAME
State : KANGWON
Address : 156-1 Okchon-Dong Kangreung-Shi
Zip Code : 210-090

[Admin Contact Information]
Name : Wonje Park
Org Name : JD-GAME
State : KANGWON
Address : 156-1, Okchon-Dong, Kangreung-Shi
Zip Code : 210-090
Phone : 0391-647-0508
Fax : 0391-651-6499
E-Mail : kangr2@soback.kornet.ne.kr

[Technical Contact Information]
Name : Wonje Park
Org Name : JD-GAME
Address : 156-1, Okchon-Dong, Kangreung-Shi
Zip Code : 210-090
Phone : 0391-647-0508
Fax : 0391-651-6499
E-Mail : kangr2@soback.kornet.ne.kr

210.189.72.176

Link, Incorporated
AT-LINKNET [210.189.72.0 <-> 210.189.72.255] 210.189.72.0

210.167.143.44

SHINANO E&E Co., Ltd.
SHINANO-NET [210.167.143.0 <-> 210.167.143.255] 210.167.143.0

208.50.27.150

UB Networks (NETBLK-FGC-REQ000000004806-1) FGC-REQ000000004806-1
208.50.24.0 -208.50.27.255

207.236.111.226

Bell Global Network Operations (NETBLK-BELLGLOBAL-2)
160 Elgin Street, Floor 12
Ottawa, Ontario K2P 2C4
Ca

Netname: BELLGLOBAL-2
Netblock: 207.236.0.0 - 207.236.255.255
Maintainer: LINX

Coordinator:
Daoust, Philippe (PD135-ARIN) noc@in.bell.ca
1-800-450-7771 +1 (416) 215-5423 +1 (416) 215-5423

206.78.1.18

Kings County Office of Education (NETBLK-SCOOPNET4) SCOOPNET4
206.78.0.0 - 206.78.255.255
Tulare County Office of Education (NETBLK-TCOENET-0-31) TCOENET-0-31
206.78.0.0 - 206.78.31.255

200.255.45.37

inetnum: 200.255.45/24
aut-num: AS4230
owner: CRUISER INFORMATICA S/C LTDA
ownerid: 001.212.126/0001-92
address: Rua Moreira Cesar, 229, 1911
address: 24230-063 - niteroi - RJ
owner-c: VID
tech-c: VID
inetrev: 200.255.45/24
nserver: SERVER01.CRUISER.COM.BR
nsstat: 19991213 AA
nslastaa: 19991213
nserver: NS.EMBRATEL.NET.BR
nsstat: 19991213 AA
nslastaa: 19991213
inetnum-up: 200.255/16

nic-hdl-br: CAP12
person: Cezar Augusto Vargas Pereira
e-mail: hostmaster@EMBRATEL.NET.BR
address: Rua Senador Pompeu, 119, 6 and
address: 20080-001 - Rio de Janeiro - RJ
phone: (021) 5192505 []
created: 19980202
changed: 20000719

nic-hdl-br: VID

person: Vinicius DAntonio
e-mail: vda@CRUISER.COM.BR
address: rua moreira cesar , 229, 1911
address: 24230-063 - niteroi - RJ
phone: (021) 6110111 []
created: 19980108
changed: 19980108

remarks: Security and abuse issues should also be addressed to
remarks: nbso@nic.br, http://www.nic.br/nbso.html

149.225.111.69

inetnum: 149.221.0.0 - 149.250.255.255
netname: EU-ZZ-990225
descr: European Regional Registry
descr: Europe
country: NL
admin-c: NN32-RIPE
tech-c: OPS4-RIPE
tech-c: CREW-RIPE
status: ALLOCATED UNSPECIFIED
remarks: initial assignment was to University of Dortmund
remarks: do whois -m to see more specific assignments
mnt-by: RIPE-NCC-HM-MNT
mnt-lower: RIPE-NCC-HM-MNT
changed: hostmaster@ripe.net 19990225
changed: hostmaster@ripe.net 20000615
changed: hostmaster@ripe.net 20000927
source: RIPE

route: 149.224.0.0/13
descr: EUNET-AGG-I
origin: AS1270
mnt-by: AS1270-MNT
changed: at@Germany.EU.net 19970710
source: RIPE

role: RIPE NCC Operations
address: Singel 258
address: 1016 AB Amsterdam
address: The Netherlands
phone: +31 20 535 4444
fax-no: +31 20 535 4445
e-mail: ops@ripe.net
admin-c: OK65
tech-c: OK65
tech-c: MCS3-RIPE
tech-c: JLSD1-RIPE
nic-hdl: OPS4-RIPE
mnt-by: RIPE-NCC-MNT
changed: olaf@ripe.net 19981208
changed: mark@ripe.net 19990803
changed: gerard@ripe.net 19991101
changed: lee@ripe.net 20000308
source: RIPE

role: RIPE NCC Hostmaster Team
address: RIPE Network Coordination Centre
address: Singel 258
address: 1016 AB Amsterdam
address: The Netherlands
phone: +31 20 535 4444
fax-no: +31 20 535 4445
e-mail: hostmaster@ripe.net
admin-c: NN32-RIPE
tech-c: EIRE-RIPE
tech-c: PTC2-RIPE
tech-c: SAWA1-RIPE
tech-c: PUNK1-RIPE
tech-c: AVA4-RIPE
tech-c: EW21-RIPE
tech-c: AS13636-RIPE
tech-c: MVH8-RIPE
tech-c: LH2166-RIPE
tech-c: LLV-RIPE
tech-c: GAC5-RIPE
tech-c: RA2490-RIPE
tech-c: SE2731-RIPE
nic-hdl: CREW-RIPE
mnt-by: RIPE-NCC-HM-MNT
changed: hostmaster@ripe.net 20000615
changed: hostmaster@ripe.net 20000822
source: RIPE

person: Nurani Nimpuno
address: RIPE Network Coordination Centre (NCC)
address: Singel 258
address: 1016 AB AMSTERDAM
address: Netherlands
phone: +31 20 535 4444
fax-no: +31 20 535 4445
nic-hdl: NN32-RIPE
mnt-by: RIPE-NCC-HM-MNT
changed: hostmaster@ripe.net 19990805
changed: hostmaster@ripe.net 20000615
source: RIPE

Tiny Fragments

TCP traffic occurred on your network that was fragmented smaller than is normally done by operating systems and network routers. This could indicate a possible covert communication channel allowing a packet payload to pass through IDS devices that do not reassemble packets before checking for events. Packet payloads can contain malicious commands or code.

The destinations of these packets should be studied further for the existence of Trojans and backdoors.

Source: 202.76.177.204

inetnum: 202.76.160.0 - 202.76.191.255
netname: VIVANET
descr: Vivanet Pty Ltd

descr: Port Rental and Wholesaling
descr: Melbourne Australia
country: AU
admin-c: BE7-AP
tech-c: BE7-AP
mnt-by: APNIC-HM
mnt-lower: MAINT-AU-VIVA
changed: hostmaster@apnic.net 20000609
changed: maint-request@apnic.net 20000815
changed: hostmaster@apnic.net 20000911
source: APNIC

Destination: MY.NET.70.20

Source: 63.236.34.174

Qwest Communications (NETBLK-NET-QWEST-BLKS2) NET-QWEST-BLKS2
63.236.0.0 - 63.239.255.255
Qwest Cybercenters (NETBLK-QWEST-CYBERCENTER) QWEST-CYBERCENTER
63.236.0.0 - 63.236.127.255
QUOKKA SPORTS (NETBLK-QWEST-JSV-QUOKKA) QWEST-JSV-QUOKKA
63.236.34.168 - 63.236.34.175

Destination: MY.NET.1.8

Sun RPC High Port

Alerts for this vulnerability were triggered due to numerous outside hosts attempting a connection to hosts on MY.NET via port 32771 (ruserd). Port 32771 is often targeted by "gain root" attacks exploiting Sun RPC buffer overflows.

The following hosts sent traffic to the reported destinations and further analysis, such as checking system logs, should be done to determine if the host was compromised:

Source	Destination
204.137.237.8	MY.NET.97.112
64.27.29.2	MY.NET.1.8
24.3.45.104	MY.NET.115.95
212.62.17.145	MY.NET.1.10
207.230.26.34	MY.NET.1.8
209.138.185.157	MY.NET.253.114
205.188.3.205	MY.NET.98.145
192.102.249.3	MY.NET.130.94
24.4.129.16	MY.NET.115.91
203.197.88.130	MY.NET.1.8

Upon further analysis the following connections, while reported under the same alert description, exhibit the characteristics of ICQ sessions. ICQ is a popular instant messaging service which listens on port 4000 and responds on port 32771. This was verified by doing a name server lookup on these hosts with the results contained in the table:

Source	Source Name	Destination
205.188.179.36	fes-d024.icq.aol.com	MY.NET.105.2
205.188.179.35	fes-d023.icq.aol.com	MY.NET.53.15
205.188.153.111	fes-d015.icq.aol.com	MY.NET.217.126

SNMP Public Access

MY.NET.101.192 is configured with an SNMP community string of "Public" – the default. The alert records indicate that no outside host has tried to access this host. This host's address is one that could be a subnet boundry and may indicate that it is a router. Anyone with access to this host can query and obtain a good amount of network architecture information.

This device should be reconfigured to use some other, not easily guessable, community string.

SMB Name Wildcard

A few alerts were generated indicating that Netbios traffic may be accessable to outside sources. Further analysis shows that all access to this information was done by hosts located on MY.NET. If external hosts were to access this information, it could be used to gather recon. information to focus an attack strategy.

Queso Fingerprint

The following external hosts executed Queso Fingerprint exploits against several hosts on MY.NET. This utility is used to determine the current operating system and version running on the target.

Sites 212.171.169.46 and 210.84.179.96 ran this exploit immediately after a SYN/FIN scan (information

contained in the above text) indicating hostile intentions.

Source	Target
194.159.73.26	MY.NET.100.230
24.3.29.155	MY.NET.6.44
212.171.169.46	MY.NET.1.3 (SYN-FIN Scan)
212.171.169.46	MY.NET.1.5
210.84.179.196	MY.NET.60.8 (SYN-FIN scan)
193.233.7.65	MY.NET.99.23
193.233.7.254	MY.NET.99.20
192.203.80.142	MY.NET.99.23
129.21.145.131	MY.NET.217.98

This traffic, and all traffic from 212.171.169.46 and 210.84.179.96, should be blocked at the network's perimeter. More discussion on Queso Fingerpinting can be found at cve.mitre.org CAN-1999-0454.

Happy 99 Virus

The Happy 99 virus was detected as being delivered to the following hosts via email:

Source	Destination
200.233.11.7	MY.NET.110.150
208.130.42.17	MY.NET.6.34
206.67.51.242	MY.NET.6.47
203.151.136.2	MY.NET.253.42

If you have virus protection installed, this virus should have already been detected and cleaned. It is recommended that you still check the above mentioned hosts for the virus. See the URL http://www.usd.edu/compserv/helpdesk/VirusInfo/Happy99.html for a complete discussion of how this virus works and how to inoculate your hosts.

Napster

Napster traffic has been detected on MY.NET between the following hosts:

Host on MY.NET	Host on Other End of Connection	Port (6666 – 9999 are known)
MY.NET.201.2	24.43.49.24	Client
MY.NET.97.229	64.217.145.98	Client
MY.NET.97.229	24.93.231.63	Client
MY.NET.97.230	24.115.14.33	Client
MY.NET.130.65	216.78.33.54	Client
MY.NET.130.65	172.139.77.50	Client
MY.NET.97.229	148.231.51.2	Client
MY.NET.97.230	128.143.245.137	Client
MY.NET.98.136	208.184.216.208	8888
MY.NET.97.230	208.184.216.208	8888
MY.NET.201.2	208.184.216.189	8888
MY.NET.201.2	208.184.216.191	8888
MY.NET.10.89	208.184.216.190	8888
MY.NET.98.146	208.184.216.190	7777
MY.NET.97.229	208.184.216.178	7777
MY.NET.97.204	208.184.216.183	7777
MY.NET.217.70	208.184.216.179	7777

MY.NET.217.158	208.184.216.198	7777
MY.NET.201.2	208.184.216.213	7777
MY.NET.162.200	208.184.216.221	7777
MY.NET.130.65	208.184.216.198	7777

Napster is a popular music download service. It works by using servers (located in 208.184.216.xxx/24) to locate specific titles that a user is searching for. These music files reside on Napster clients (which are hosts that can exist on any network) and then creating a connection between the host that initiated the search and the host that houses the file. By default, Napster uses ports 6666, 7777, 8888, and 9999 to download files over the Internet.

The table, above, lists those hosts on MY.NET that not only were used as "Clients" from which files were downloaded but also those hosts on MY.NET that downloaded files. If use of the Napster application is not in compliance with your system policy, consider uninstalling the Napster application. It may also be helpful to remind users of your system policy regarding the use of Napster or similar applications.

Misc – Large UDP Packets

1,166 alerts were generated from source 211.40.176.214 to MY.NET.98.179:6970 between 6:30:03 and 6:59:58 on August 8th. This rule fires when packets greater than 1200 bytes are detected. RFC 2507 can be referenced for further information on large packets.

Port 6970 is known to be used for the "Gate Crasher" backdoor as well as RealAudio. The amount of traffic generated seems to indicate RealAudio and that these alerts are false-positives.

It is curious, however, that the alerts occur from the half-hour to the hour only. Also to be considered is the source of the traffic. A "whois" query returns the following information:

IP Address : 211.40.176.0-211.40.179.255
Connect ISP Name : BORANET
Connect Date : 1999.11.20
Registration Date: 20000601
Network Name : DACOM-KIDC

[Organization Information]
Orgnization ID : ORG105718
Name : DACOM
State : SEOUL
Address : 261-1 Nonhyun-dong Kangnam-gu
Zip Code : 135-010

[Admin Contact Information]
Name : Sanggyu chang
Org Name : DACOM
State : SEOUL
Address : 261-1 Nonhyun-dong Kangnam-gu
Zip Code : 135-010
Phone : +82-2-6220-2921
Fax : +82-2-6220-2909
E-Mail : sgjang@kidc.net

[Technical Contact Information]
Name : Taeung kim
Org Name : DACOM
Address : 261-1 Nonhyun-dong Kangnam-gu

```
Zip Code        : 135-010
Phone           : +82-02-6220-2925
Fax             : +82-02-6220-2909
E-Mail          : apecs8@kidc.net
```

Therefore, further analysis should be done to determine if this host has been compromised. "Gate Crasher" is known to contain a robust feature set that could cause this type of traffic.

If use of the RealAudio application is not in compliance with your system policy, consider uninstalling the RealAudio application. It may also be helpful to remind users of your system policy regarding the use of RealAudio or similar applications.

III. Analysis Process

The first step in my analysis process was to download the data from the SANS site. This step is mentioned because although it may seem trivial, care had to be taken to be sure that all the available files were downloaded and that they were taken from the correct SANS site. It was important to start with the correct data and all of it. I made a small checklist which I used to track my download progress which listed each file's name. Each file was checked, on the list, after it was downloaded. Once downloading was completed, I double checked the list of files with the files contained on my hard drive's directory.

Since I knew I wanted to be able to sort and count the data from various points of interest, the next step was to get all of the data into a format that I could then import into an MS Access database. This meant that the data had to be "normalized" which really means that I needed to split each alert record into data fields. This was done using MS Notepad to replace " -> ", " [**] ", and space characters with a semicolon ";" – using the replace function.

I then went to the DOS prompt and used the COPY command to copy each individual file into one large data set. The command format was: COPY file1,file2,file3,… DataSet. This places all listed files into the file DataSet.

The data was then imported into MS Access. I originally planned to import directly to MS Excel, but due to the amount of records I was forced to first use Access. Excel has a limit of 65,535 rows in a worksheet but since I am more familiar with Excel, it was important to me to get the data into that application. Importing the data as semicolon delimited allowed each field to be placed into its own column and to be labeled.

Once the import was complete, I selected half of the records in the database and used the copy and paste function to transfer the records into Excel. The first half of the data set was put into one worksheet and the second half copied into a second worksheet. This, in effect, got me around the size limitation issue in Excel.

I then had the ability to sort and perform subtotal (count) functions on each field. This gives the ability to study the data by source, destination, time stamp, or any other point of view.

The data was then manually analyzed. The Internet was widely used to do name lookups and other research on the Web. One great resource was the Sam Spade site (`www.samspade.org`) which allowed me to do several whois queries.