Passive Host Monitoring

John Kristoff

DePaul University

jtk@depaul.edu

February 2001

Overview

- Linux Redhat 6.2 default install
- University network environment
- NOT a honeypot
- Capture every packet

As Seen on the Net

- RPC and FTP mostly
- NetBIOS, most from internal network
- ICMP host unreachables
- Some TELNET and DNS
- Barely any HTTP

Observations

- Packet analysis is slow, but educational
- It was relatively easy to protect the host
- Nothing I could do to stop DoS/spoofed packets
- Attackers are lamerz too, their tools suck
- Monitoring log files is helpful, need better tools
- Basic system config tricks would stop/slow attackers

Example 1 - Crafted Packets

```
No.  Time       Source    Destination   Length   Protocol
1  0.000000     suspect     igunda        60       TCP
   sunrpc > sunrpc [FIN, SYN] Seq=1597357078 Ack=1032676069 Win=1028 Len=0
```

Example 2 - Suspicious Packets

```
No. Time            Source    Destination   Length   Protocol
 1 0.0000000        suspect      igunda       60       TCP
   0 > 1024 [SYN, ACK] Seq=713323970 Ack=2383656254 Win=0 Len=0

 2 0.000262         suspect      igunda       60       TCP
   0 > 1024 [RST, ACK] Seq=713323971 Ack=2383656254 Win=0 Len=0
```

Example 3 - Correlation

```
No. Time            Source    Destination   Length   Protocol
 1 0.000000        suspect-1     igunda       60     TCP
   www > 1538 [RST, ACK] Seq=0 Ack=674711610 Win=0 Len=0

 2 1117.980147     suspect-2     igunda       60     TCP
   www > 1538 [SYN, ACK] Seq=897862236 Ack=674711610 Win=16384 Len=0

 3 1117.981982      igunda     suspect-2      60     TCP
   1538 > www [RST] Seq=674711610 Ack=0 Win=0 Len=0

 4 1117.986725     suspect-2     igunda       60     TCP
   www > 1538 [RST, ACK] Seq=897862237 Ack=674711610 Win=16384 Len=0
```

Example 4 - Attack Packet

```
Byte  Hex                                               ASCII
 3d0  9090 9090 9090 9090 31c0 eb7c 5989 4110   ........1..|Y.A.
 3e0  8941 08fe c089 4104 89c3 fec0 8901 b066   .A....A........f
 3f0  cd80 b302 8959 0cc6 410e 99c6 4108 1089   .....Y..A...A...
 400  4904 8041 040c 8801 b066 cd80 b304 b066   I..A.....f.....f
 410  cd80 b305 30c0 8841 04b0 66cd 8089 ce88   ....0..A..f.....
 420  c331 c9b0 3fcd 80fe c1b0 3fcd 80fe c1b0   .1..?.....?.....
 430  3fcd 80c7 062f 6269 6ec7 4604 2f73 6841   ?..../bin.F./shA
 440  30c0 8846 0789 760c 8d56 108d 4e0c 89f3   0..F..v..V..N...
 450  b00b cd80 b001 cd80 e87f ffff ff00         ..............
```

Example 5 - Log files

```
Sep  5 02:39:31 igunda in.ftpd[7594]: connect from suspect
Sep  5 02:39:41 igunda ftpd[7594]: lost connection to suspect
Sep  5 02:39:41 igunda ftpd[7594]: FTP session closed
Sep  5 02:39:41 igunda inetd[478]: pid 7594: exit status 255

Oct  8 06:19:29 igunda rpc.statd[340]: gethostbyname error for ...

Oct 27 13:27:54 igunda rpc.statd[353]: SM_MON request for hostname
Oct 27 13:27:54 igunda rpc.statd[353]: POSSIBLE SPOOF/ATTACK ATTEMPT!
Oct 27 13:27:54 igunda rpc.statd[353]: STAT_FAIL to localhost for SM_MON of
```

Statistics

- A VERY unscientific look at the sources
  - Non-US (29)
  - ISP DSL/Cable/Modem pools (10)
  - Big ISP netblocks (10)
  - Internal NetBios (5)
  - US Universities (4)
  - Other (18)

Statistics [continued]

- A VERY unscientific look at destinations
  - assumed wu-ftpd (28)
  - assumed rpc.statd (17)
  - ICMP destination unreachables (11)
  - telnet (9)
  - NETBIOS (9)
  - DNS (3)

Resources

- http://www.cert.org
- http://www.ethereal.com
- http://www.rfc-editor.org
- http://packetstorm.securify.com
- http://www.securityfocus.com
- http://project.honeynet.org

The End

- For further analysis see:

  http://condor.depaul.edu/∼jkristof/igunda.pdf

  or http://condor.depaul.edu/∼jkristof/igunda.ps