

Introduction to Honeypots “honeyd”

Kartik Shinde
Consultant – Information Security

What's all about Research?

- Information Security – Technologically fast paced arena.
- Research – Known /Unknown attacks, threats.
- Learn how attackers work, protect yourself and the community.

Avenues of Research

- Intrusion Detection Systems
- Honeypots / Honeynets
- Reverse Engineering Malicious code
- Exploit code analysis

Honeynets / Honey pots

- Potentially a weak network / system deployed as a bait for hackers.
- Generally deployed on a protected and monitored base.
- Once compromised, data is collected to learn the tools, tactics, and motives of the blackhat community.

Enter – “honeyd”

Open source Honeypots

- [Honeyd](#) is a small daemon that creates virtual hosts on a network. The hosts can be configured to run simulated TCP services or proxy the service to another machine. The TCP/IP personality (OS Fingerprints) can be adapted so that they appear to be running certain versions of operating systems.
- [Arpd](#) enables a single host to claim all unassigned addresses on a LAN by answering any ARP request for an IP address with the MAC address of the machine running arpd.

```

sample + (/usr/home/vacuum/honeyd) - VIM
Eterm Font Background Terminal
annotate "FreeBSD 2.2.1 - 4.1" fragment old
create template
set template personality "FreeBSD 2.2.1 - 4.1"
add template tcp port 80 "sh scripts/web.sh"
add template tcp port 22 "sh scripts/test.sh $ipsrc $dport"
add template tcp port 23 proxy 10.23.1.2:23
#set template default tcp action reset
set template uid 32767 gid 32767

bind 192.168.1.11 template
set 192.168.1.11 uptime 1327650
~
~
~
~
~
~
~
~
~
~

vacuum@toshiba: /home/vacuum/honeyd
Eterm Font Background Terminal
[root@toshiba honeyd]# ./honeyd -f sample -p nmap,prints -i fxp0 -d
sample:14: illegal token
sample:14: syntax error
honeyd[2318]: listening on fxp0: (tcp or icmp or udp) and not ether src 00:00:3
9:e6:0c:0f
[]

vacuum@toshiba: /home/vacuum
Eterm Font Background Terminal
toshiba# ./arpd -i fxp0 -d 192.168.1.11
arpd[476]: listening on fxp0: arp and dst net 192.168.1.11 and not ether src 00:
00:39:e6:0c:0f
toshiba# []

nmap,prints - (/home/vacuum/honeyd) - VIM
Eterm Font Background Terminal
Fingerprint FreeBSD 2.2.1 - 4.1
TSeq(Class=RI%god=<8%SI=<38E50&>906)
T1(DF=Y%W=403D|C0B7|402E|C08A|FFFF%ACK=S++%F1ags=AS%0ps=MNWNNTIM)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=403D|C0B7|402E|C08A|FFFF%ACK=S++%F1ags=AS|A%0ps=MNWNNTINNTIM)
T4(DF=N%W=4000|0|0%ACK=0%F1ags=R%0ps=)
T5(DF=N%W=0%ACK=S++%F1ags=AR%0ps=)
T6(DF=N%W=0%ACK=0%F1ags=R%0ps=)
T7(DF=N%W=0%ACK=S%F1ags=AR%0ps=)
PU(DF=N%TOS=0%IPLen=38%RIPTL=148%RID=F%RIPCK=F%UCK=0|F%ULEN=134%DAT=E)

# Thanks to Alexandr D. Kanevskiy <kad@dgtu.donetsk.ua>
Fingerprint FreeBSD 2.1.0 - 2.1.5 # Thanks to Jan Koum!
TSeq(Class=64K)
T1(DF=NIY%W=402E|403D%ACK=S++|0%F1ags=AS|A%0ps=M|NNT|MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=NIY%W=402E|403D%ACK=S++|0%F1ags=AS|A%0ps=M|NNT|MNWNNT)
T4(DF=N%W=4000%ACK=0%F1ags=R%0ps=)
T5(DF=N%W=0%ACK=S++%F1ags=AR%0ps=)
T6(DF=N%W=0%ACK=0%F1ags=R%0ps=)
T7(DF=N%W=0%ACK=S%F1ags=AR%0ps=)
PU(DF=N%TOS=0%IPLen=38%RIPTL=148%RID=F%RIPCK=0%UCK=0%ULEN=134%DAT=E)
[]

```

Honeyd - Components

```

[root@chameleon honeyd]# ll
total 1564
-rwxr-xr-x    1 krypt    root      558368 Feb 10 00:26 arpd
-rwxr-xr-x    1 krypt    root      662892 Feb 20 20:20 honeyd
-rw-r--r--    1 krypt    krypt     1327 Feb 21 11:46 honeyd.conf
-rw-r--r--    1 krypt    root      5809 Feb 10 01:11 nmap.assoc
-rw-r--r--    1 krypt    root     278316 Feb  8 07:51 nmap.prints
-rw-r--r--    1 krypt    krypt     2695 Feb 20 19:19 README
drwxr-xr-x    3 krypt    krypt     4096 Feb 10 00:18 scripts
-rwxr-xr-x    1 root     root      232 Feb 21 11:50 start-arpd_new.sh
-rwxr-xr-x    1 krypt    krypt     231 Feb 20 19:21 start-arpd.sh
-rwxr-xr-x    1 root     root      324 Feb 21 11:53 start-honeyd_new.sh
-rwxr-xr-x    1 krypt    krypt     320 Feb 20 19:21 start-honeyd.sh
-rw-r--r--    1 krypt    root     45207 Feb 10 01:08 xprobe2.prints
[root@chameleon honeyd]# cd scripts/
[root@chameleon scripts]# ll
total 32
-rwxr-xr-x    1 krypt    krypt     4773 Sep 28 2002 ftp.sh
drwxr-xr-x    5 krypt    krypt     4096 Feb 10 01:27 iis-0.95
-rwxr-xr-x    1 krypt    krypt     2479 Sep 28 2002 pop3.sh
-rwxr-xr-x    1 krypt    krypt     2499 Sep 28 2002 router-telnet.pl
-rwxr-xr-x    1 krypt    krypt     3770 Sep 28 2002 smtp.sh
-rwxr-xr-x    1 krypt    krypt     151 Sep 28 2002 test.sh
-rwxr-xr-x    1 krypt    krypt     2126 Sep 28 2002 web.sh
[root@chameleon scripts]# _

```

honeyd.conf

```
[root@chameleon honeydl]# more honeyd.conf
## Honeyd configuration file ##

### Windows computers
create windows
set windows personality "Windows NT 4.0 Server SP5-SP6"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "perl scripts/iis-0.95/iisemul8.pl"
add windows tcp port 139 open
add windows tcp port 137 open
add windows udp port 137 open
add windows udp port 135 open
set windows uptime 3284460
bind 172.16.222.101 windows

### Linux 2.4.x computer
create linux
set linux personality "Linux 2.4.16 - 2.4.18"
set linux default tcp action reset
set linux default udp action reset
#set linux subsystem "/usr/sbin/httpd"
add linux tcp port 110 "sh scripts/pop3.sh"
add linux tcp port 25 "sh scripts/smtp.sh"
--More-- (54%)_
```

arpd script

```
[root@chameleon honeyd]# more start-arpd_new.sh
#!/bin/sh
#
# Aprd startup script.
# Marcus Ranum/Lance Spitzner 3 Jan, 2003
#
# PURPOSE: To start the Arpd process
# Add '-d' to command line for debug information

set -x

# Monitor just these IP addresses
./arpd 172.16.222.0/24

[root@chameleon honeyd]# _
```

honeyd script

```
[root@chameleon honeyd]# more start-honeyd_new.sh
#!/bin/sh
#
# Honeyd startup script.
# Marcus Ranum/Lance Spitzner 3 Jan, 2003
#
# PURPOSE: To start the Honeyd process
# Add '-d' to command line for debug information

set -x

./honeyd -p nmap.prints -f honeyd.conf -x xprobe2.prints -a nmap.assoc \
        -l /var/log/honeyd 172.16.222.101 172.16.222.101-172.16.222.224

[root@chameleon honeyd]# _
```

nmap.prints

```
T4 (DF=N/W=0/ACK=0/Flags=R/Ops=)
T5 (DF=N/W=0/ACK=S++/Flags=AR/Ops=)
T6 (DF=N/W=0/ACK=0/Flags=R/Ops=)
T7 (DF=N/W=0/ACK=S/Flags=AR/Ops=)
PU (DF=N/TOS=0/IPLEN=38/RIPTL=148/RID=E/RIPCK=E/UCK=E/ULEN=134/DAT=E)
```

```
Fingerprint Cisco 2620 running IOS 12.1(6)
TSeq (Class=RI/gcd=<6/SI=<ABC2&>78/IPID=Z/TS=U)
T1 (DF=N/W=1020/ACK=S++/Flags=AS/Ops=ME)
T2 (Resp=Y/DF=N/W=0/ACK=S/Flags=AR/Ops=)
T3 (Resp=Y/DF=N/W=1020/ACK=S++/Flags=AS/Ops=M)
T4 (DF=N/W=0/ACK=0/Flags=R/Ops=)
T5 (DF=N/W=0/ACK=S++/Flags=AR/Ops=)
T6 (DF=N/W=0/ACK=0/Flags=R/Ops=)
T7 (DF=N/W=0/ACK=S/Flags=AR/Ops=)
PU (Resp=N)
```

```
Fingerprint Cisco 3600 running IOS 12.2(6c)
TSeq (Class=TR/gcd=<6/IPID=Z/TS=U)
T1 (DF=N/W=1020/ACK=S++/Flags=AS/Ops=ME)
T2 (Resp=Y/DF=N/W=0/ACK=S/Flags=AR/Ops=)
T3 (Resp=Y/DF=N/W=1020/ACK=S++/Flags=AS/Ops=M)
T4 (DF=N/W=0/ACK=0/Flags=R/Ops=)
T5 (DF=N/W=0/ACK=S++/Flags=AR/Ops=)
--More-- (19%)_
```

You can try this at home..!!!

Honeytrap for Unicode worms

- Perl program simulating an IIS server
 - Responds to any HTTP request with a valid IIS header
 - Purpose : To detect even the Code Blue worm which attacks only IIS servers
 - Demonstrates the speed at which these worms attack servers on the internet
 - Logs the attack patterns/signatures of the attack
 - Gather any further attack patterns not know
- Easiest honeypot (home-made ;))
 - ✓ `nc -l -n -vv -p 80` (watch the worms attack in real-time)