Activitat Honeyd

L'activitat d'aquest tema es recomana fer-la en linux, tot i que tambe existeix el honeyd per a windows.

Passos a realitzar per a completar l'activitat:

1.- Us heu d'instalar el programa honeyd, i si voleu tambe tots els scripts addicionals que trobeu per la web o en fitxers addicionals (en el linu-toolkit o en honeyd-common).

2.- Heu de crear una maquina virtual mitjançant el honeyd que almenys sigui capaç de respondre a peticions Telnet, HTTP. Si voleu fer-ho mes complet, afegiu-hi despres que tambe pugui respondre FTP i SMTP.

3.- Proveu amb un nmap que la maquina virtual funcioni i amb els ports corresponents oberts.

4.- Entregeu en un fitxer .rar o .zip la configuració del honeyd i els scripts que responen als diferents serveis que hagueu programat !!!COMENTAT!!!!.

Sistemes: Ubuntu GNU/Linux (basat en Debian)

Instal·lació honeyd:

```
aptitude install honeyd farpd honeyd-common
```

Vull emular tant una màquina GNU/Linux (SuSE 8.0) amb els serveis indicats al enunciat com una màquina Windows. Per això utilitzaré els scripts de serveis que porta el propi honeyd, els quals els he d'adaptar lleugerament per que funcionin correctament, passos previs:

```
cd /etc/honeypot
ln -s /usr/share/honeyd/scripts/ .
cd scripts/
mkdir misc
cd misc
ln -s ../base.sh .
touch /var/log/honeypot/web.log
touch /var/log/honeypot/honeyd.txt
```

Del directori '/etc/honeypot/scripts/unix/linux/suse8.0/' modifico els fitxers:

- /etc/honeypot/scripts/unix/linux/suse8.0/apache.sh
  Indico a on es troba l'arxiu log pel servei web, modificant la linia
  LOG="/var/log/honeypot/web.log".

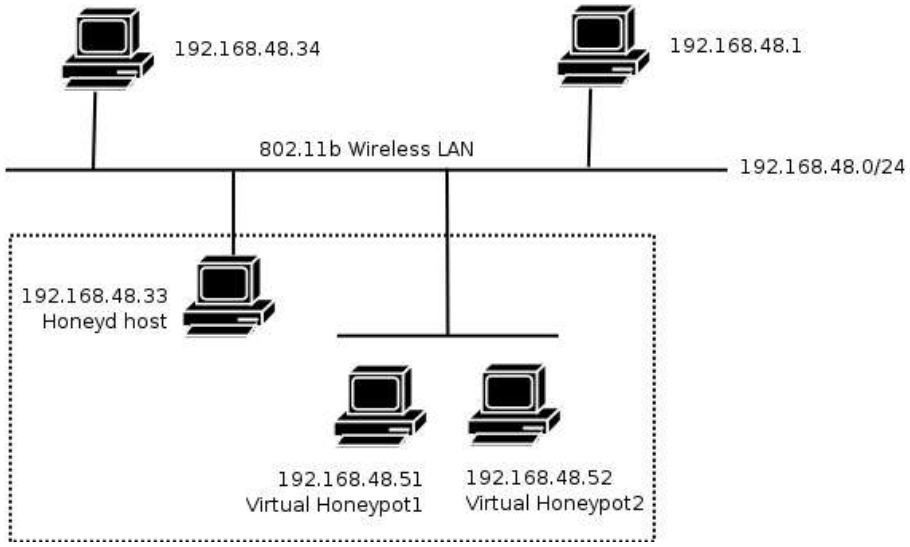
- /etc/honeypot/scripts/base.sh
  Indico l'arxiu de log general a la linia LOG="/var/log/honeypot/honeyd.txt".

- /etc/honeypot/scripts/win32/win2k/iis.sh
  Indico a on es troba l'arxiu log pel servei web, modificant la linia
  LOG="/var/log/honeypot/web.log"

He realitzat la pràctica provant dos topologies diferents:

- Mitjançant una xarxa inalàmbrica, utilitzo honeypots virtuals connectacts directament a la xarxa real.
- Ús d'una xarxa local (no wireless), utilitzo una honeynet (xarxa virtual) connectat amb un router virtual.

Disseny de la configuració amb hosts integrats a la xarxa real (Wireless):



Configuració /etc/honeypot/honeyd.conf

```
create windows
set windows personality "Microsoft Windows XP Professional SP1"
add windows tcp port 80 "sh /etc/honeypot/scripts/win32/win2k/iis.sh"
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 default tcp action reset
set windows default udp action reset
bind 192.168.48.51 windows

create suseLinux
set suseLinux personality "Linux Kernel 2.4.20"
add suseLinux tcp port 80 "sh /etc/honeypot/scripts/unix/linux/suse8.0/apache.sh"
add suseLinux tcp port 23 "sh /etc/honeypot/scripts/unix/linux/suse8.0/telnetd.sh"
add suseLinux tcp port 21 "sh /etc/honeypot/scripts/unix/linux/suse8.0/proftpd.sh"
add suseLinux tcp port 25 "sh /etc/honeypot/scripts/unix/linux/suse8.0/sendmail.sh"
set suseLinux default tcp action reset
set suseLinux default udp action reset
bind 192.168.48.52 suseLinux
```

Iniciem serveis:

```
farpd -d 192.168.48.0/24

honeyd -f /etc/honeypot/honeyd.conf -l /var/log/honeypot/honeyd.log -p
/etc/honeypot/nmap.prints -a /etc/honeypot/nmap.assoc -0 /etc/honeypot/pf.os -x
/etc/honeypot/xprobe2.conf  -d 192.168.48.51-192.168.48.52
```

Des de l'ordinador 192.168.48.34 (segons el diagrama) es realitza un scan de ports:

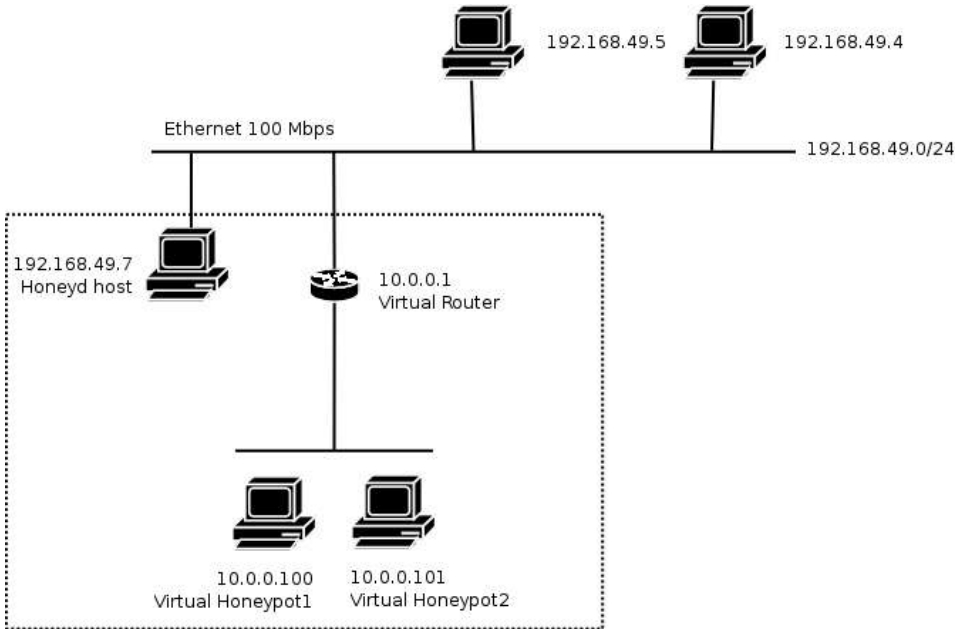
```
# nmap -sS  192.168.48.51 -o 192.168.48.51.nmap.log

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2005-01-23 15:47 CET
Interesting ports on 192.168.48.51:
(The 1656 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
80/tcp  open  http
137/tcp open  netbios-ns
139/tcp open  netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 2.679 seconds

# nmap -sS  192.168.48.52 -o 192.168.48.52.nmap.log
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2005-01-23 15:48 CET
Interesting ports on 192.168.48.52:
(The 1655 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
25/tcp open  smtp
80/tcp open  http

Nmap run completed -- 1 IP address (1 host up) scanned in 12.405 seconds
```

També es possible accedir a tots els serveis definits utilitzant telnet, per exemple al port 80 del servidor web fem una petició incorrecte amb “GET /” i veiem que la resposta correspon al servidor indicat:

```
# telnet 192.168.48.51 80
Trying 192.168.48.51...
Connected to 192.168.48.51.
Escape character is '^]'.
GET /

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: dom ene 23 15:50:52 CET 2005
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body></html>Connection closed
by foreign host.
Connection closed by foreign host.

# telnet 192.168.48.52 80
Trying 192.168.48.52...
Connected to 192.168.48.52.
Escape character is '^]'.
GET /

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
 to /index.php not supported.<P>
<P>alid method in request GET /
<HR>
<ADDRESS>Apache/1.3.23 Server at bps-pc10.local.mynet Port </ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
```

Disseny de la configuració amb subxarxa virtual connectada per router virtual a xarxa real (No wireless):



Configuració /etc/honeypot/honeyd.conf

```
route entry 10.0.0.1 network 10.0.0.0/24
route 10.0.0.1 link 10.0.0.0/24

create router
set router personality "Cisco 7206 running IOS 11.1(24)"
set router default tcp action reset
set router default udp action reset
add router tcp port 23 "sh /etc/honeypot/scripts/router-telnet.pl"
set router uptime 1327650
bind 10.0.0.1 router

create windows
set windows personality "Microsoft Windows XP Professional SP1"
add windows tcp port 80 "sh /etc/honeypot/scripts/win32/win2k/iis.sh"
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 default tcp action reset
set windows default udp action reset
bind 10.0.0.100 windows

create suseLinux
set suseLinux personality "Linux Kernel 2.4.20"
add suseLinux tcp port 80 "sh /etc/honeypot/scripts/unix/linux/suse8.0/apache.sh"
add suseLinux tcp port 23 "sh /etc/honeypot/scripts/unix/linux/suse8.0/telnetd.sh"
add suseLinux tcp port 21 "sh /etc/honeypot/scripts/unix/linux/suse8.0/proftpd.sh"
add suseLinux tcp port 25 "sh /etc/honeypot/scripts/unix/linux/suse8.0/sendmail.sh"
set suseLinux default tcp action reset
set suseLinux default udp action reset
bind 10.0.0.101 suseLinux
```

Iniciem serveis:

```
ifconfig eth0 promisc

farpd -i eth0 -d 10.0.0.0/24

honeyd -f /etc/honeypot/honeyd.conf -l /var/log/honeypot/honeyd.log -p
/etc/honeypot/nmap.prints -a /etc/honeypot/nmap.assoc -0 /etc/honeypot/pf.os -x
/etc/honeypot/xprobe2.conf -i eth0 -d 10.0.0.0/24
```

Des de l'ordinador 192.168.49.5 (segons el diagrama) es realitza un scan de ports:

```
# route -n add -net 10.0.0.0/24 192.168.49.7

# nmap -v -sS 10.0.0.1 -o 10.0.0.1.nmap.log

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2005-01-23 17:35 CET
Host 10.0.0.1 appears to be up ... good.
Initiating SYN Stealth Scan against 10.0.0.1 at 17:35
Adding open port 23/tcp
The SYN Stealth Scan took 73 seconds to scan 1659 ports.
Interesting ports on 10.0.0.1:
(The 1658 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap run completed -- 1 IP address (1 host up) scanned in 74.305 seconds

# nmap -v -sS 10.0.0.100 -o 10.0.0.100.nmap.log

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2005-01-23 17:36 CET
Host 10.0.0.100 appears to be up ... good.
Initiating SYN Stealth Scan against 10.0.0.100 at 17:36
Adding open port 80/tcp
Adding open port 139/tcp
Adding open port 137/tcp
The SYN Stealth Scan took 1 second to scan 1659 ports.
Interesting ports on 10.0.0.100:
(The 1656 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
80/tcp  open  http
137/tcp open  netbios-ns
139/tcp open  netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 2.147 seconds

# nmap -v -sS 10.0.0.101 -o 10.0.0.101.nmap.log

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2005-01-23 17:36 CET
Host 10.0.0.101 appears to be up ... good.
```

```
Initiating SYN Stealth Scan against 10.0.0.101 at 17:36
Adding open port 23/tcp
Adding open port 21/tcp
Adding open port 80/tcp
Adding open port 25/tcp
The SYN Stealth Scan took 1 second to scan 1659 ports.
Interesting ports on 10.0.0.101:
(The 1655 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
25/tcp open  smtp
80/tcp open  http

Nmap run completed -- 1 IP address (1 host up) scanned in 1.469 seconds
```

També es possible accedir a tots els serveis definits utilitzant telnet, de la mateixa forma que la configuració anterior.

Alumne: Sergio Blanco Cuaresma