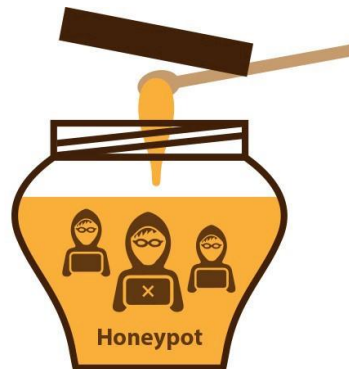


CÓMO CREAR UN HONEYPOT



¿Qué es un honeypot? ¿Cuál es su importancia y por qué es crucial que instalemos uno? Los honeypots son esencialmente servidores señuelo desplegados junto a su sistema real en la red. Su propósito es atraer a los atacantes maliciosos que intentan entrar en su red. Los Honeypots pueden desviar a los atacantes y a sus componentes para que no entren en tu red. También puede servir como una gran manera de añadir oportunidades de supervisión de seguridad para los equipos azules.

He aquí cómo atraer a posibles atacantes a una trampa honeypot con Linux.

Necesitarás una instalación Linux y descargar una herramienta llamada pentbox.

Abre el terminal y descarga pentbox con el comando

```
wget http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz
```

Lo que hace este comando es apuntar a este sitio web y descargar la herramienta.

```
root@kali:~# wget http://downloads.sourceforge.net/project/pentbox18realised/pentbox-1.8.tar.gz
```

Encuétralo en tu directorio, el que sea, el mío es el directorio de inicio.

```
root@kali:~# ls
allports.gnmap  Downloads  pentbox-1.8.tar.gz
allports.nmap  Hooli-theme
allports.xml    htb
'Currency Volume Report.xlsx' libinput-gestures
Desktop         Music
Documents      pentbox-1.8
root@kali:~# cd pentbox-1.8/
root@kali:~/pentbox-1.8# ls
changelog.txt  lib  pb_update.rb  readme.txt  tools
COPYING.txt   other  pentbox.rb    todo.txt
root@kali:~/pentbox-1.8# ./pentbox.rb
```

```
root@kali:~# tar xvfz pentbox-1.8.tar.gz
```

```
tar xvfz pentbox-1.8.tar.gz
```

Ahora la parte interesante, la razón por la que estamos aquí. Para atraer a los atacantes.

Desde aquí seleccionamos 2 para Herramientas de red y luego 3 para Honeypot.

```
-> 2
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
0- Back
-> 3
// Honeypot //
You must run PentBox with root privileges.
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
```

A continuación, seleccione la opción 1 para Fast Auto Configuration. Una vez seleccionado esto, se iniciará el honey pot y por defecto en el puerto 80.

```

root@kali: ~/pentbox-1.8

File Edit View Search Terminal Help

8- Exit
-> 2
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back
-> 3
// Honeypot //

You must run PentBox with root privileges.

Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
-> 1

HONEYPOT ACTIVATED ON PORT 80 (2019-10-08 00:47:27 -0400)

```

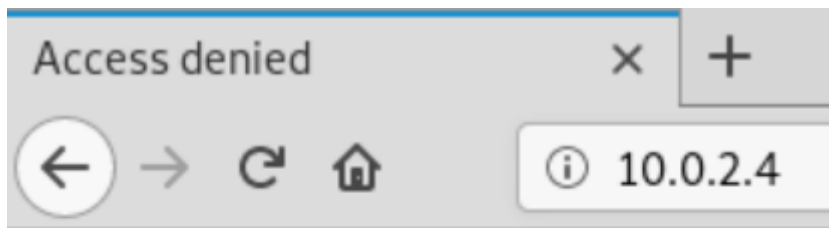
Ahora abra un navegador web en otra máquina como su máquina host y apúntelo a la dirección IP de su máquina Linux. La IP de mi Linux era 10.0.2.4. Puede utilizar los comandos `ip address` o `ifconfig | grep inet`.

```

root@kali:~/pentbox-1.8# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gro
   link/ether 08:00:27:e9:86:b8 brd ff:ff:ff:ff:ff:ff
   inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 1047sec preferred_lft 1047sec
   inet6 fe80::a00:27ff:fee9:86b8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@kali:~/pentbox-1.8# ifconfig | grep inet
inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fee9:86b8 prefixlen 64 scopeid 0x20<link>
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>

```

Usted debe obtener un acceso denegado y si lo que hizo es correcto.



Access denied

IP Address login failed

2019-10-08 00:47:27 -0400

Debería ver lo siguiente.

```
HONEYPOT ACTIVATED ON PORT 80 (2019-10-08 00:47:27 -0400)
400

INTRUSION ATTEMPT DETECTED! from 10.0.2.4:42770 (2019-10-08 00:51:21 -0400)
-----
GET / HTTP/1.1
Host: 10.0.2.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

INTRUSION ATTEMPT DETECTED! from 10.0.2.4:42784 (2019-10-08 00:51:24 -0400)
-----
GET /favicon.ico HTTP/1.1
Host: 10.0.2.4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

Si desea profundizar y hacer que su honeypot escuche un puerto específico. Deberías ejecutar pentbox como tal y seleccionar 2 y luego 3 seguido de 2. Cuando el script te pida que introduzcas un puerto teclea 22. El puerto 22 es para SSH

Cuando intento conectarme por SSH a la dirección IP obtengo el siguiente mensaje “INTRUSION ATTEMPT DETECTED!” -> “¡INTENTO DE INTRUSIÓN DETECTADO!”.

```
root@kali:~/pentbox-1.8# ssh root@10.0.2.4
ssh_exchange_identification: Connection closed by remote host
```

```
root@kali: ~/pentbox-1.8 x root@kali: ~/pentbox-1.8
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
-> 2
Insert port to Open.
-> 22
Insert false message to show.
-> SSH Port Test
Save a log with intrusions?
(y/n) -> n
Activate beep() sound when intrusion?
(y/n) -> n
HONEYPOT ACTIVATED ON PORT 22 (2019-10-08 00:57:14 -0400)
INTRUSION ATTEMPT DETECTED! from 10.0.2.4:48554 (2019-10-08 00:58:21 -0400)
-----
SSH-2.0-OpenSSH_7.9p1 Debian-10
```

Puedes ver que el intento fue registrado y la IP donde se originó.

Ya hemos configurado con éxito el Honeypot.