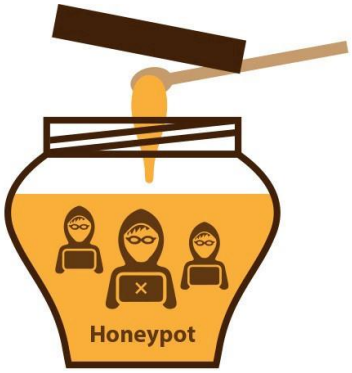
CÓMO CREAR UN HONEYPOT



¿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/pen
tbox-1.8.tar.gz
```

Encuéntralo 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        Pictures
 allports.xml                   htb                Public
'Currency Volume Report.xlsm'   libinput-gestures  shellshock.py
 Desktop                        Music              Templates
 Documents                      pentbox-1.8        Videos
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
```

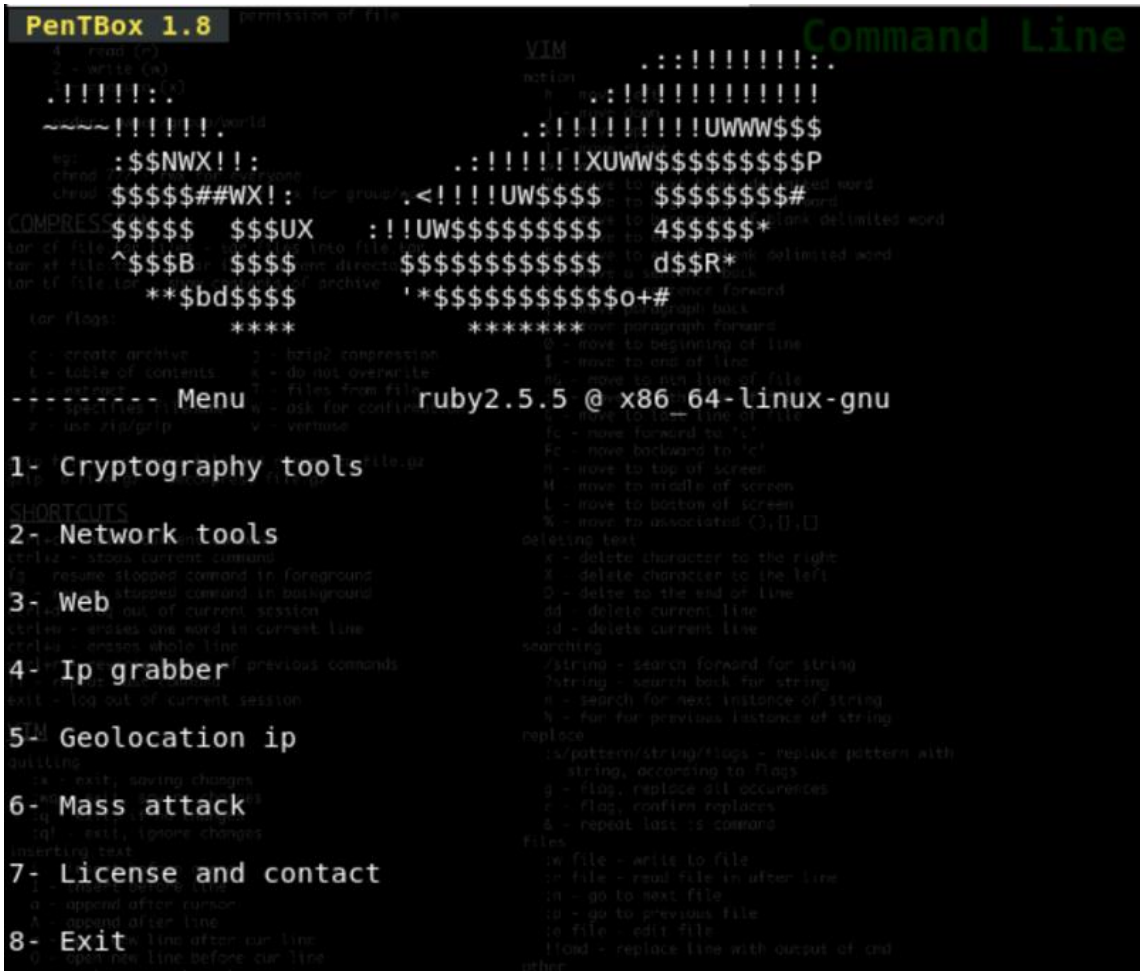
tar xvfz pentbox-1.8.tar.gz

A continuación, ejecutamos el comando para "descargar" las herramientas. El comando tar se utiliza para extraer una colección de archivos y directorios en un archivo altamente comprimido comúnmente llamado tarball.

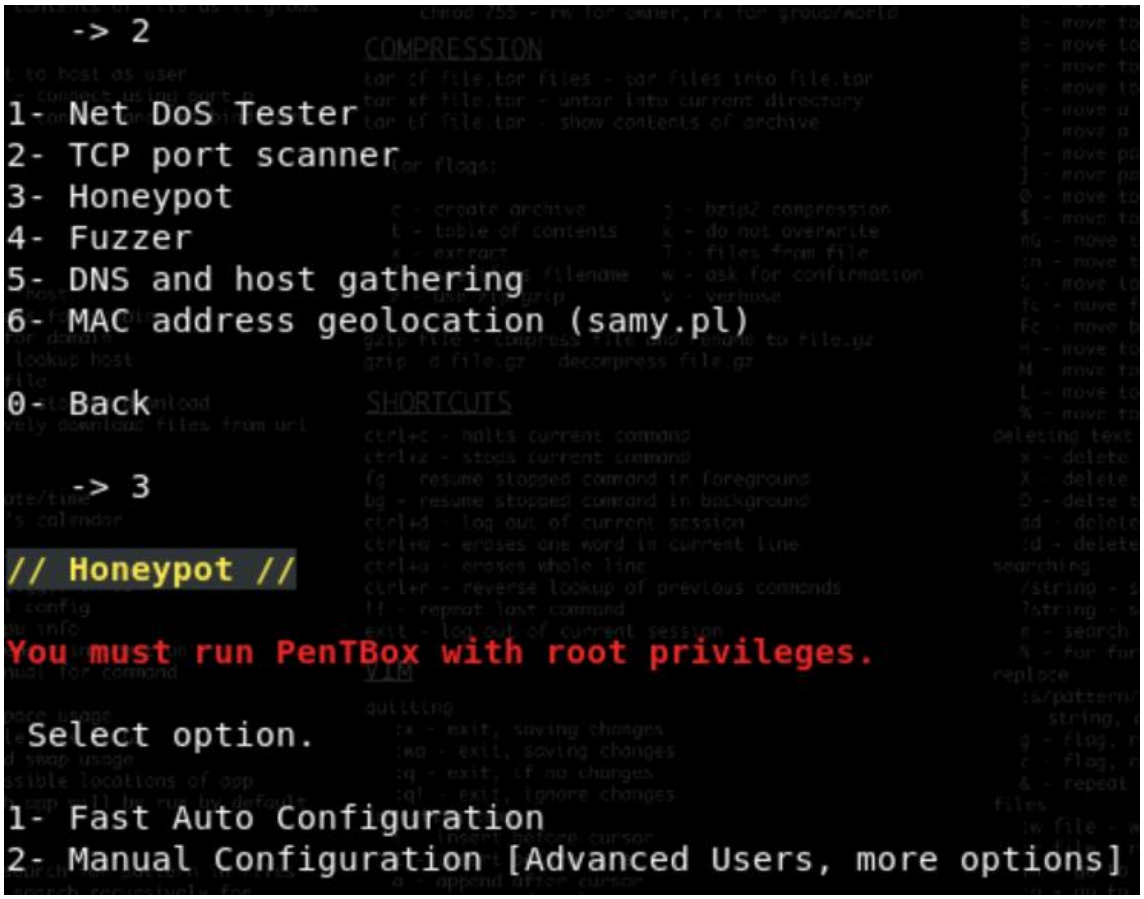
Luego ejecutamos el siguiente comando **`sudo ./pentbox.rb`**

Y entonces, debería aparecer lo siguiente.

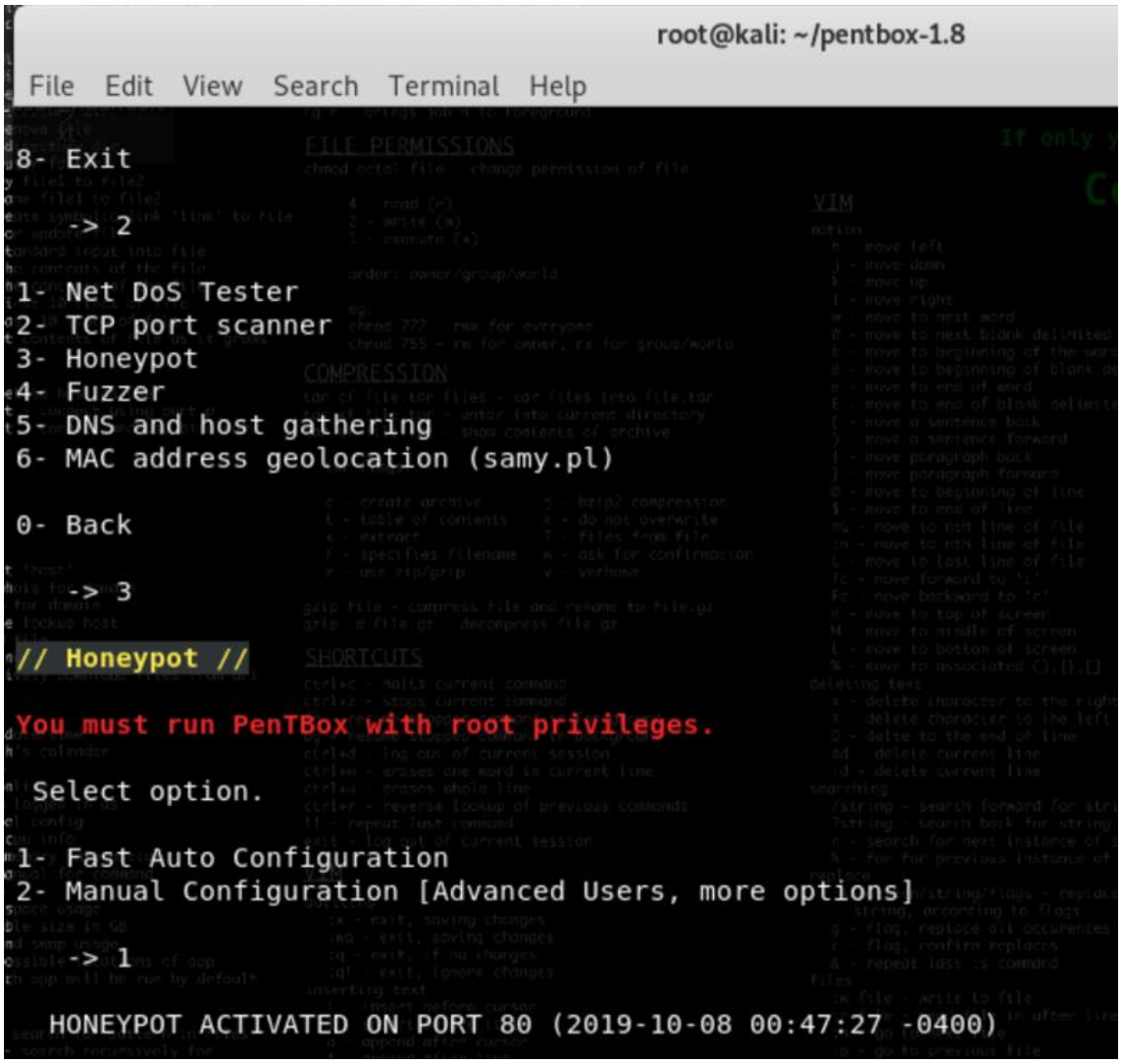
Ahora la parte interesante, la razón por la que estamos aquí. Para atraer a los atacantes.



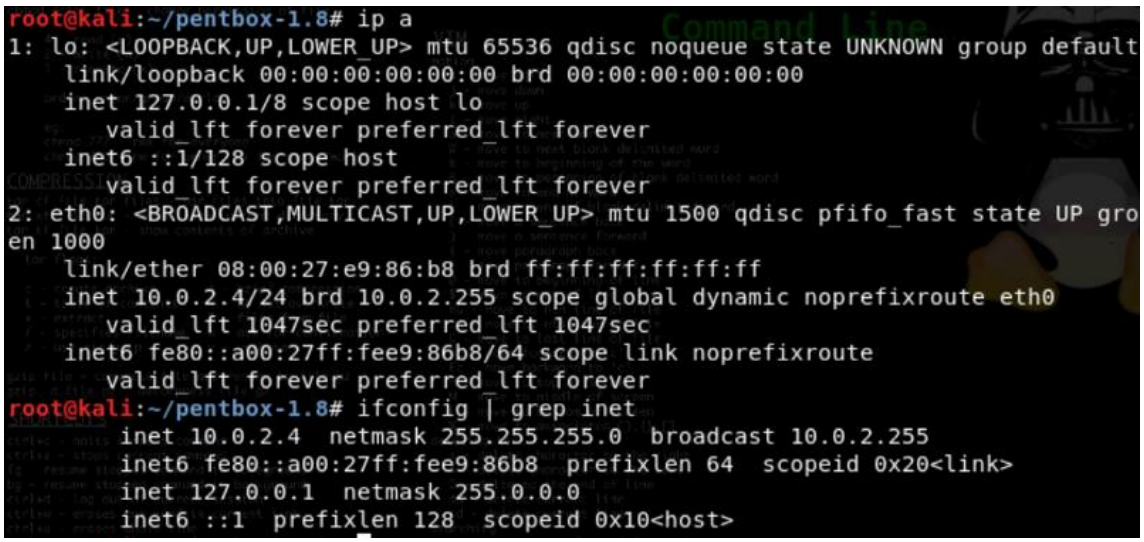
Desde aquí seleccionamos 2 para Herramientas de red y luego 3 para Honeypot.



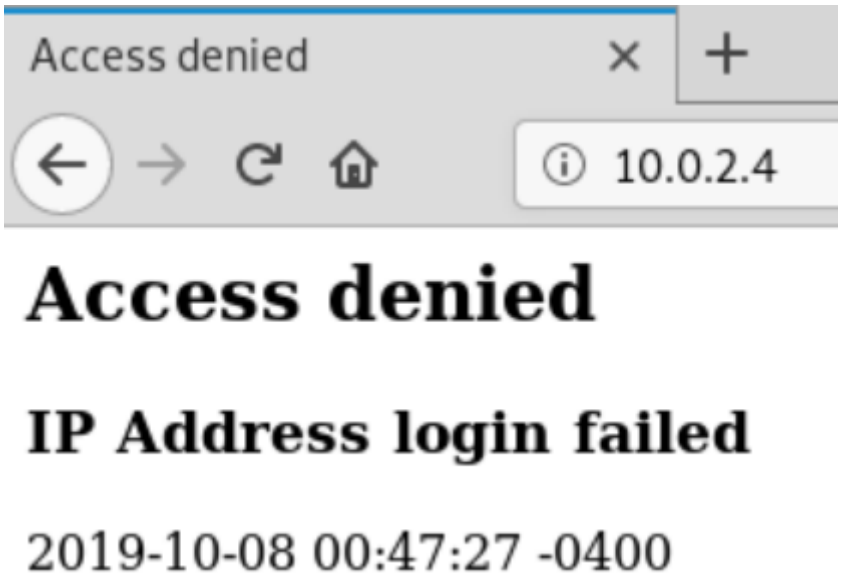
A continuación, seleccione la opción 1 para Fast Auto Configuration. Una vez seleccionado esto, se iniciará el honey pot y por defecto en el puerto 80.



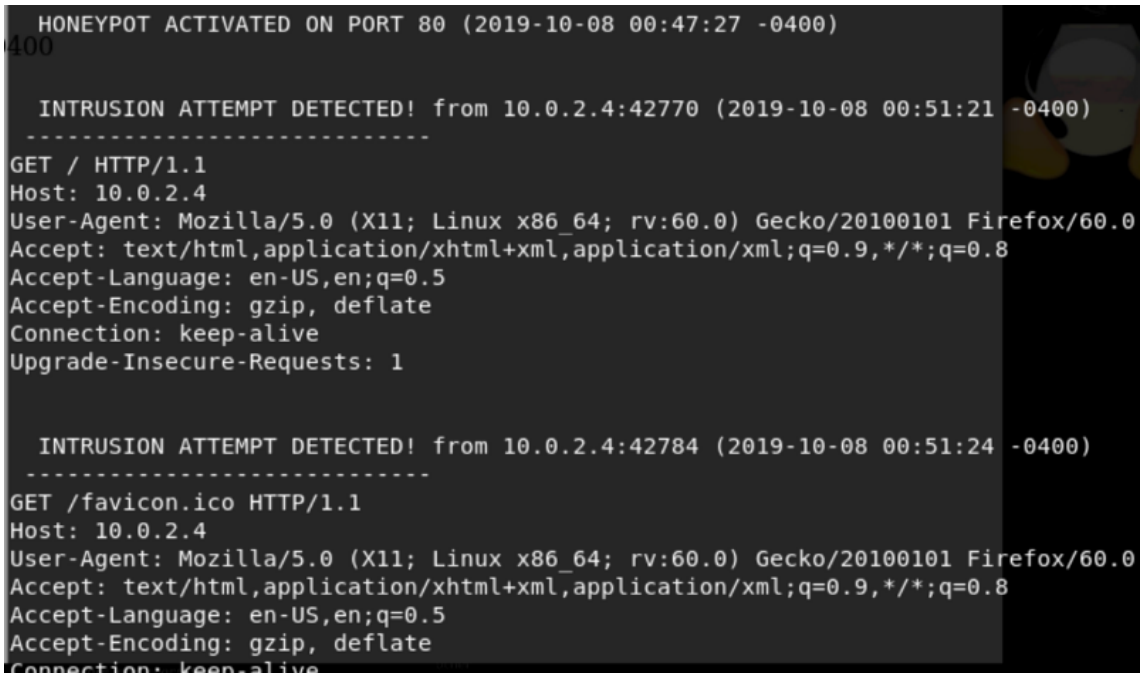
Ahora abra un navegador web en otra máquina como su máquina host y apúntelo a la dirección IP de su máquina Linux. La IP de mi Linux era 10.0.2.4. Puede utilizar los comandos **`ip address`** o **`ifconfig | grep inet`**.



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

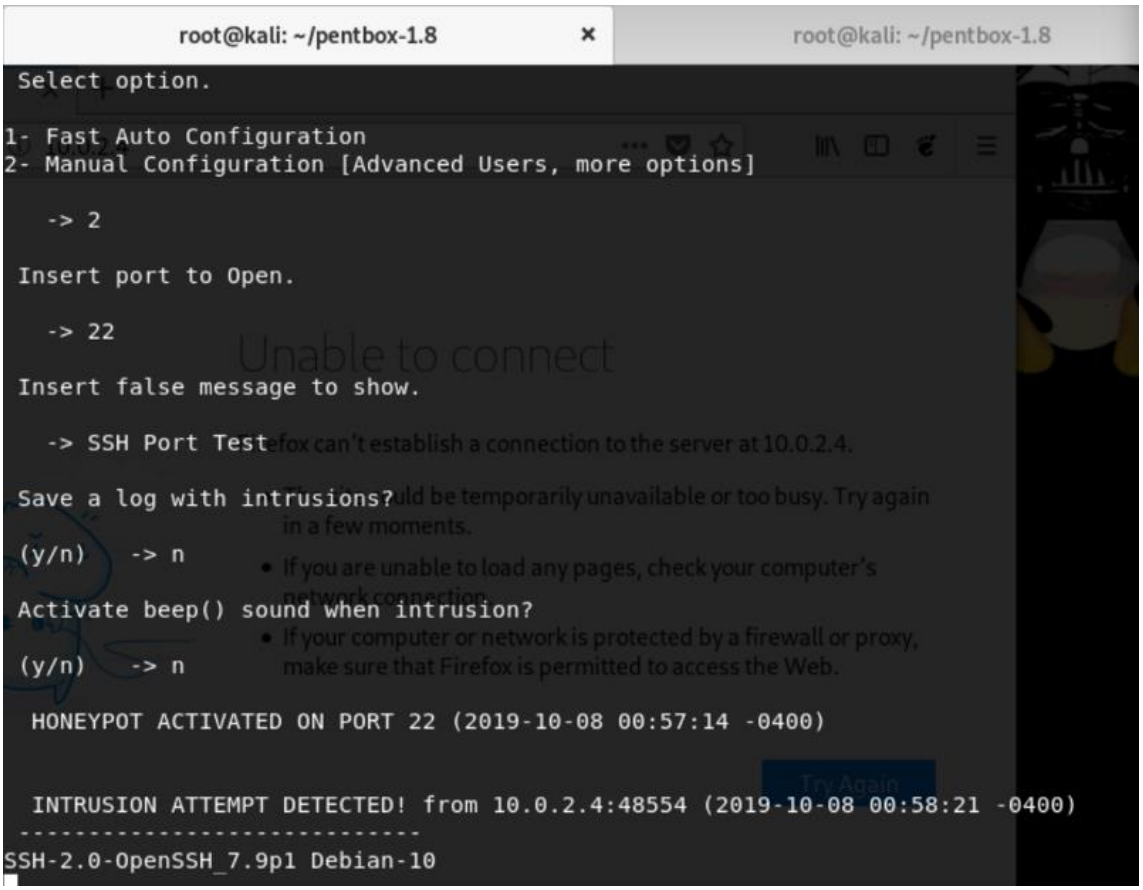


Debería ver lo siguiente.



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!".



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

Ya hemos configurado con éxito el Honeypot.