# EJERCICIOS - PORT FORWARDING Túnel Local

## Prerrequisitos Tres máquinas, por ejemplo:

- Kali Linux – máquina 1

- Metasploitable – máquina 2

- DVL – máquina 3

Configurar las 3 máquinas en la misma red para hacer túnel local

Utilizar los recursos donde vienen los comandos de Túnel Local – SSH puerto 22– web

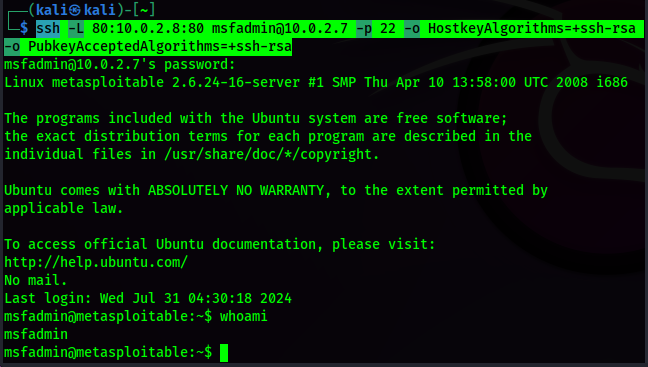
puerto 80

# Ejercicio 1

Túnel Local – puerto 80 web

Máquina 1 atacante (Kali), mediante servidor SSH y puerto 22 a máquina 2 (Metasploitable)

y a través del puerto 80 web hacia máquina 3 (DVL)

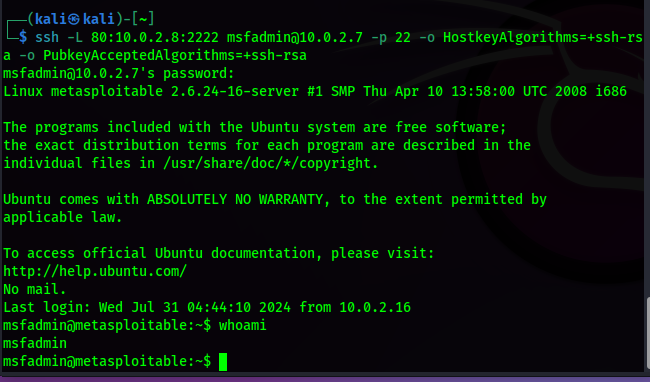
* Ponemos el siguiente comando para crear un tunel a través de DVL y conectarnos a a metasploitable:  
  ssh -L 80:10.0.2.8:80 msfadmin@10.0.2.7 -p 22 -o HostkeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
* 

#Ejercicio 2

Túnel Local ssh puerto 2222

Máquina 1 atacante (Kali), mediante servidor SSH y puerto 22 a máquina 2 (Metasploitable)

y mediante servidor SSH a través del puerto 2222 hacia máquina 3 (DVL)

* 
* Aqui ponemos el mismo comando pero cambiamos el puerto de salida al puerto 2222

#Ejercicio 3

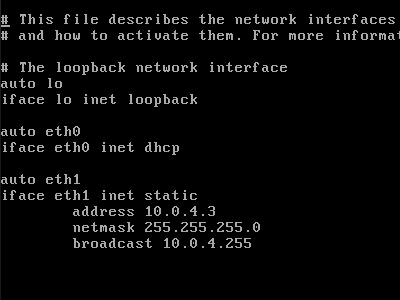
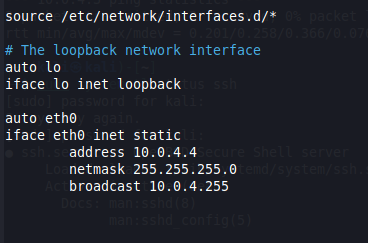
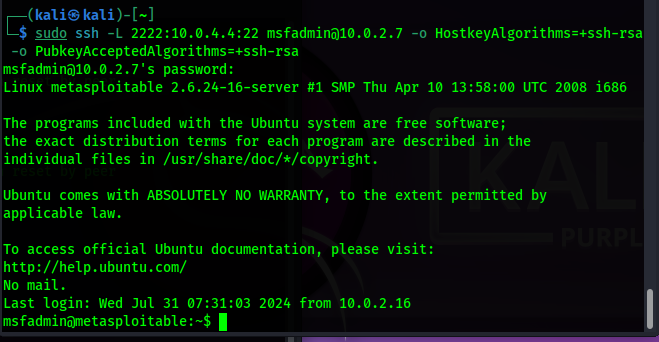
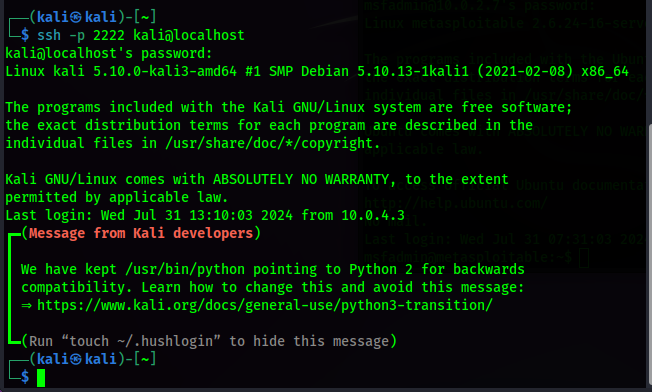
Túnel Local con las máquinas en redes distintas

Máquina 1 atacante (Kali) – mediante servidor SSH y puerto 22 a máquina 2

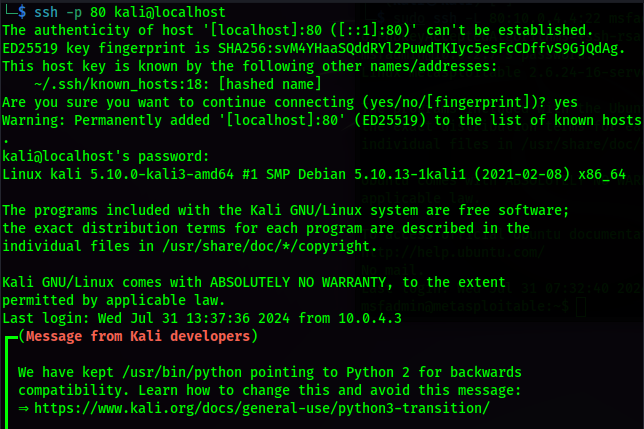
(Metasploitable). Y hacia la máquina 3 DVL, dos opciones:

* Para esto voy a usar 2 kalis y metasploitable, una kali normal y la otra OPENVAS

1. Mediante servidor SSH a través del puerto 2222 hacia máquina 3 (OPENVAS)

* Primero tuve que configurar el networking de la máquina metasploitable y OPENVAS para que estén en una red NAT aparte de la kali “atacante”, si no configuro esto aunque haya creado una red NAT diferente con un prefijo IPv4 distinto me va a dar el mismo rango de IP,. Esta configuración la hice cambiando el archivo etc/network/interfaces (tanto en metasploitable como en kali OPENVAS)
* 
* Como en metasploitable tenemos 2 interfaces de red habilitadas, la primero (eth0) vamos a dejarla tal cual porque es la que esta conectada a natnetwork, que es la misma a la que está kali “atacante” y nos vale las ip default (las del estilo 10.0.2.x)
* Lo que cambiamos es eth1 que es la interfaz que está conectada a natnetwork1 y si lo ponemos **iface eht1 inet dhcp** vamos a obtener una ip 10.0.2.x lo que está en el mismo rango que eth0 por lo que podríamos acceder a ella desde kali “atacante” y no queremos eso, queremos una red para kali “atacante” y metasploitable y otra red para metrasploitable y kali OPENVAS.
* La configuración en kali OPENVAS es:
* 
* todo igual excepto que usamos la interfaz eth0 ya que solo tenemos habilitada una interfaz de red y le cambiamos a que sea la ip 10.0.4.4 (para que tenga una ip distinta)
* Ahora ya deberíamos de tener las maquinas configuradas correctamente, si probamos las conexiones usando ping, en kali “atacante” solo podríamos hacer ping a metasploitable y no a kali OPENVAS, en kali OPENVAS solo a metasploitable y no a kali “atacante” y en metasploitable a las 2.
* Ahora ya solo nos queda crear el tunel con el siguiente comando:
* sudo ssh -L 2222:10.0.4.4:22 msfadmin@10.0.2.7 -o HostkeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
* introducimos las credenciales de metasploit:
* 
* en este punto deberíamos de tener el tunel activo por lo que si, en otra terminal ejecutamos el siguiente comando: ssh -p 2222 kali@localhost
* 
* Nos conectamos a kali OPENVAS.

2. A través del puerto 80 web hacia máquina 3 (OPENVAS)

* Esto sería lo mismo pero en vez de usar el puerto 2222 el 80. El comando quedaría de esta manera:
* sudo ssh -L 80:10.0.4.4:22 msfadmin@10.0.2.7 -o HostkeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
* 
* Nos conectamos a OPENVAS igualmente