EJERCICIOS INTRODUCCIÓN A LOS MOVIMIENTOS LATERALES

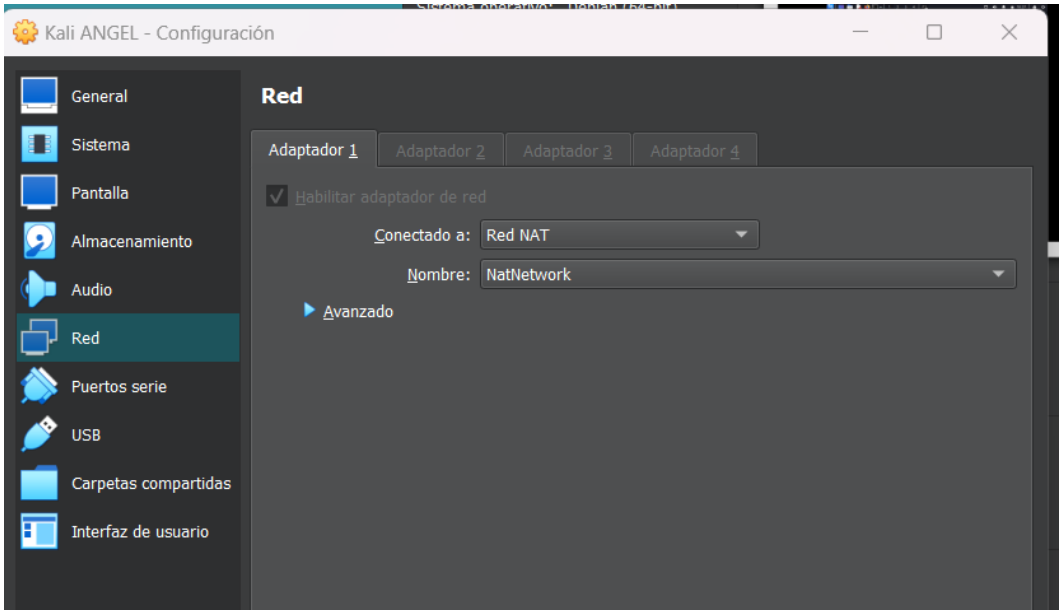
Prerrequisitos

- Kali Linux
- Metasploitable2
- DVL

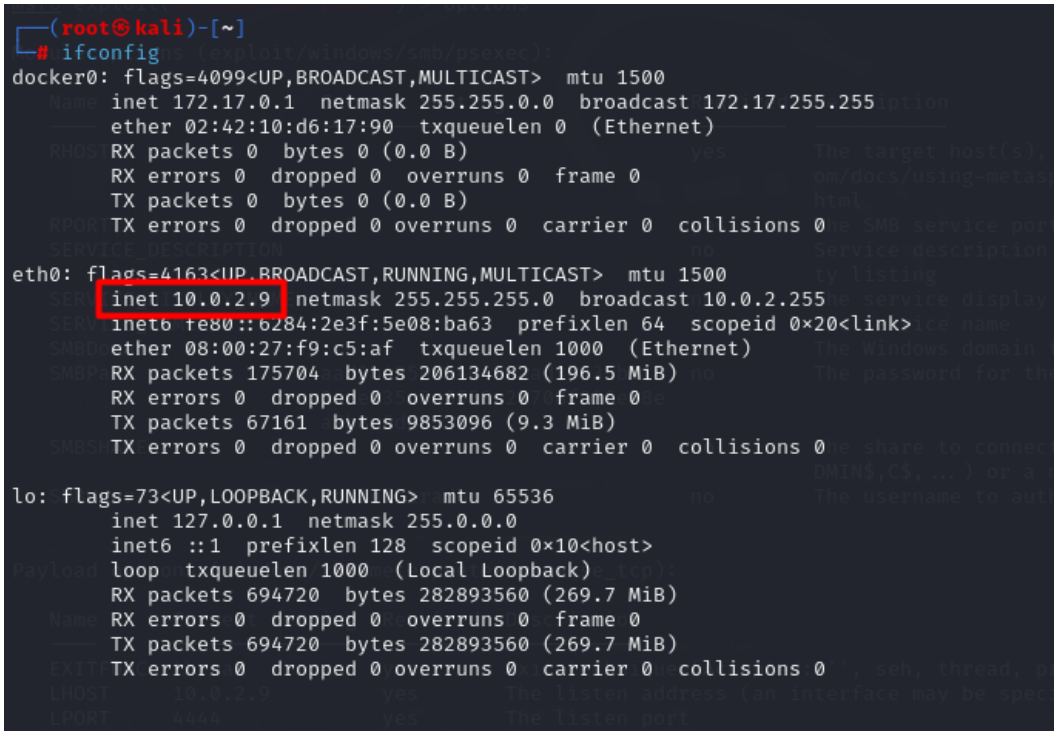
Ejercicio - SSH, Proxychains y Nmap

- **Crear un laboratorio de tres máquinas en dos segmentos de red de forma que solo una tenga acceso a las dos interfaces para realizar Local Port Forwarding.**

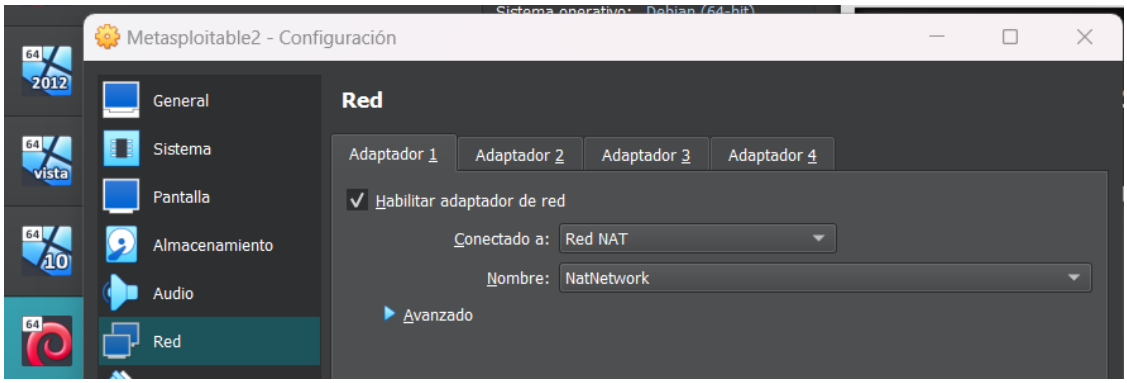
  Tenemos nuestra Kali en red nat

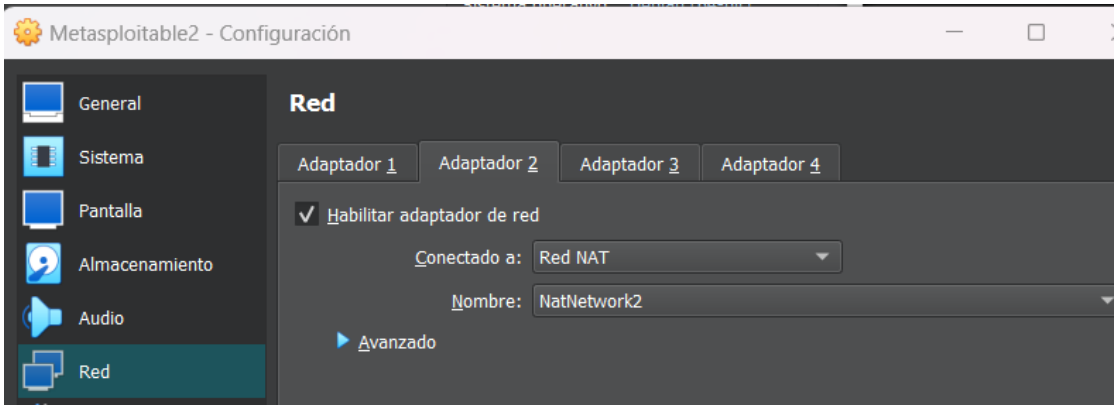


  Confirmamos la red



  En la metasploitable modificamos tambien los adaptadores de red





Entramos en la meta y vemos nuestra configuración de red

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1a:52:c2
          inet addr:10.0.2.19  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1a:52c2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:25 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3638 (3.5 KB)  TX bytes:5808 (5.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)
```

Para poder ver el tercer segmento tenemos que poner el siguiente comando

```
msfadmin@metasploitable:~$ sudo ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:71:38:39
          inet addr:10.0.3.5  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe71:3839/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:594 (594.0 B)  TX bytes:810 (810.0 B)
          Base address:0xd240 Memory:f0820000-f0840000
```

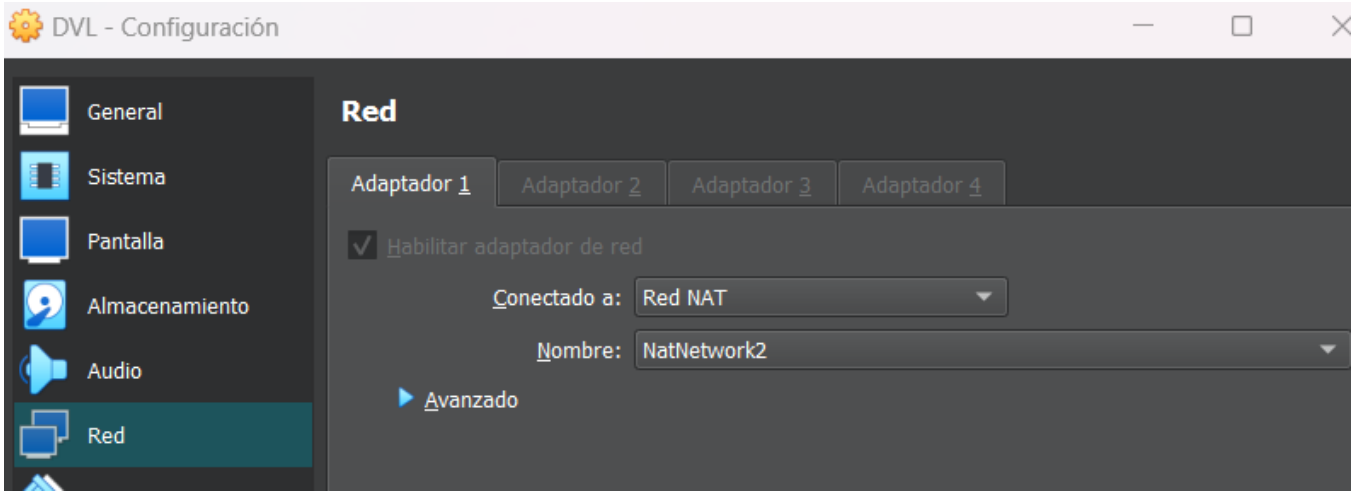
Una vez hecho esto, realizamos el siguiente

```
msfadmin@metasploitable:~$ sudo dhclient eth1
There is already a pid file /var/run/dhclient.pid with pid 4699
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.0.6
Copyright 2004-2007 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth1/08:00:27:71:38:39
Sending on   LPF/eth1/08:00:27:71:38:39
Sending on   Socket/fallback
DHCPREQUEST of 10.0.3.5 on eth1 to 255.255.255.255 port 67
DHCPACK of 10.0.3.5 from 10.0.3.3
bound to 10.0.3.5 -- renewal in 255 seconds.
```

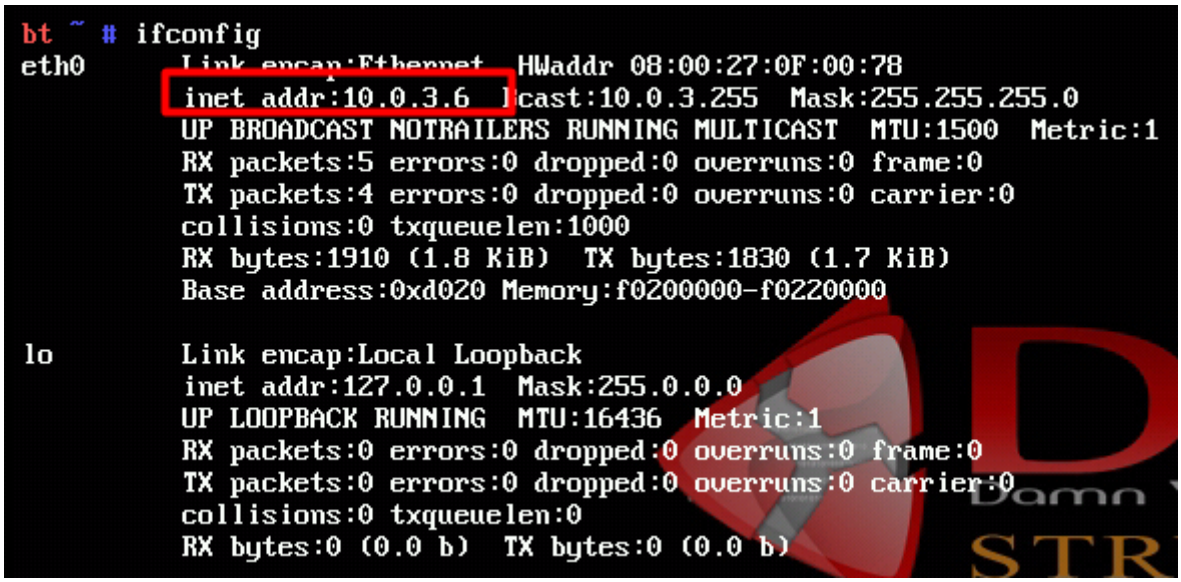
Volvemos a preguntar la configuración de red y obtenemos esto

```
eth1      Link encap:Ethernet  HWaddr 08:00:27:71:38:39
          inet addr:10.0.3.5  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe71:3839/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:594 (594.0 B)  TX bytes:810 (810.0 B)
          Base address:0xd240 Memory:f0820000-f0840000
```

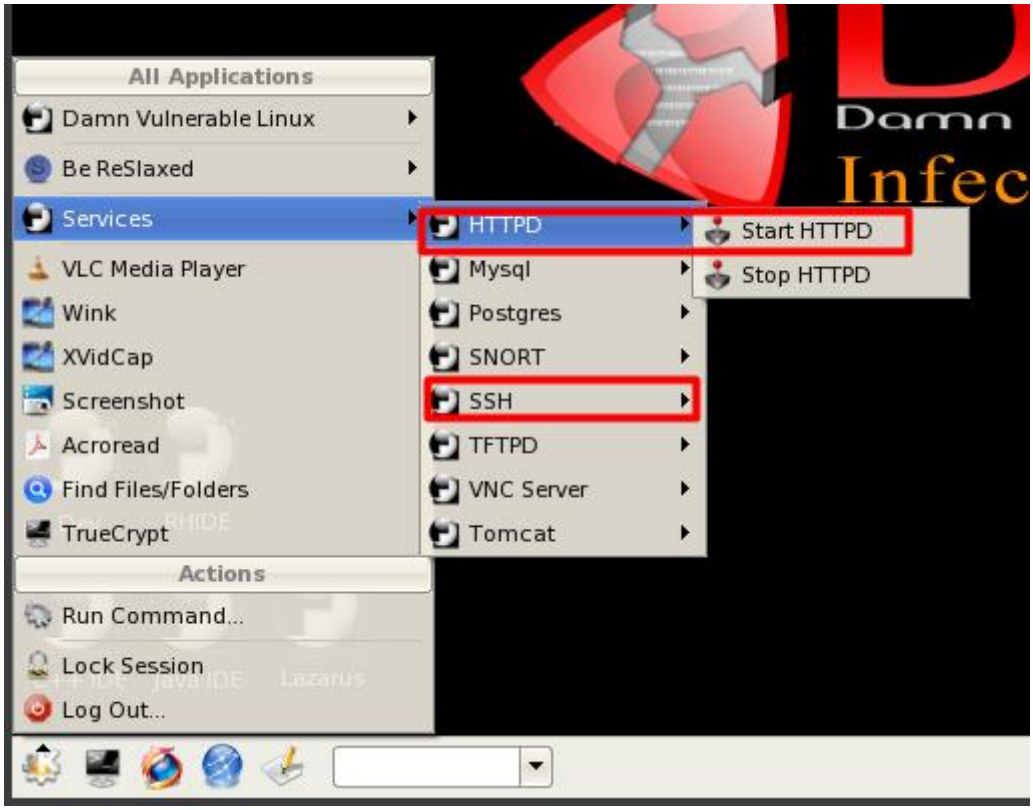
Volvemos a VB a las opciones de configuración de la máquina DVL



Dentro de esta máquina comprobamos también lo mismo



También activamos los siguientes procesos



- **Realizar un esquema explicativo del comando a utilizar.**
  - **Inicio del túnel:** 10.0.2.9:PUERTO donde quiera visualizar el destino
  - **Destino del túnel:** 10.0.3.6:PUERTO de la máquina destino que yo quiero visualizar
  - **Intermedio del túnel:** usuario@IP_METASPLITABLE2 ssh -L 10.0.2.9:5555:10.0.3.6:80 msfadmin@10.0.2.19 -oHostKeyAlgorithms=+ssh-dss
- **Hacer Local Port Forwarding usando SSH de algún puerto de la máquina DVL.**

  Nos conectamos a la meta desde nuestra Kali

```
┌──(root㉿kali)-[~]
└─# ssh msfadmin@10.0.2.19 -oHostKeyAlgorithms=+ssh-dss
The authenticity of host '10.0.2.19 (10.0.2.19)' can't be established.
DSA key fingerprint is SHA256:kgTW5p1Amzh5MfHn9jIpZf2/pCIZq2TNrG9sh+fy95Q.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.19' (DSA) to the list of known hosts.
msfadmin@10.0.2.19's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Nov 27 11:43:53 2023
msfadmin@metasploitable:~$ whoami
msfadmin
```

Visualizamos el archivo sshd_config

```
msfadmin@metasploitable:~$ cat /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768
```

Y comprobamos de que X11Forwarding esté en yes

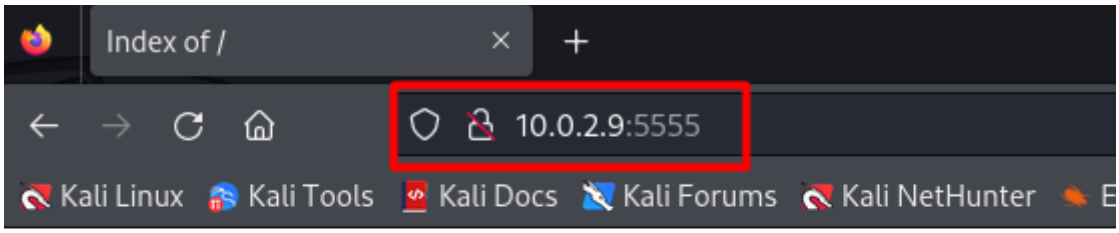
```
X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net
```

Una vez hecho esto tunelizamos de la siguiente forma

```
┌──(root㉿kali)-[~]
└─# ssh -L 10.0.2.9:5555:10.0.3.6:80 msfadmin@10.0.2.19 -oHostKeyAlgorithms=+ssh-dss
msfadmin@10.0.2.19's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Nov 27 12:45:05 2023 from 10.0.2.9
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$
```

- **Demostrar que el túnel funciona.**

  Nos dirigimos al buscador y buscamos la IP con el puerto correspondiente



Index of /

Name	Last modified	Size	Description
Parent Directory	18-Jan-2009 21:58	-	
base/	18-Jan-2009 21:58	-	
beef/	18-Jan-2009 21:58	-	
info.php	18-Jan-2009 21:58	1k	
manual/	18-Jan-2009 21:58	-	
olate/	18-Jan-2009 21:58	-	
phpmyadmin/	18-Jan-2009 21:58	-	
unicornscan/	18-Jan-2009 21:58	-	
webexploitation_pack..>	18-Jan-2009 21:58	-	
webexploitation_pack..>	18-Jan-2009 21:58	-	

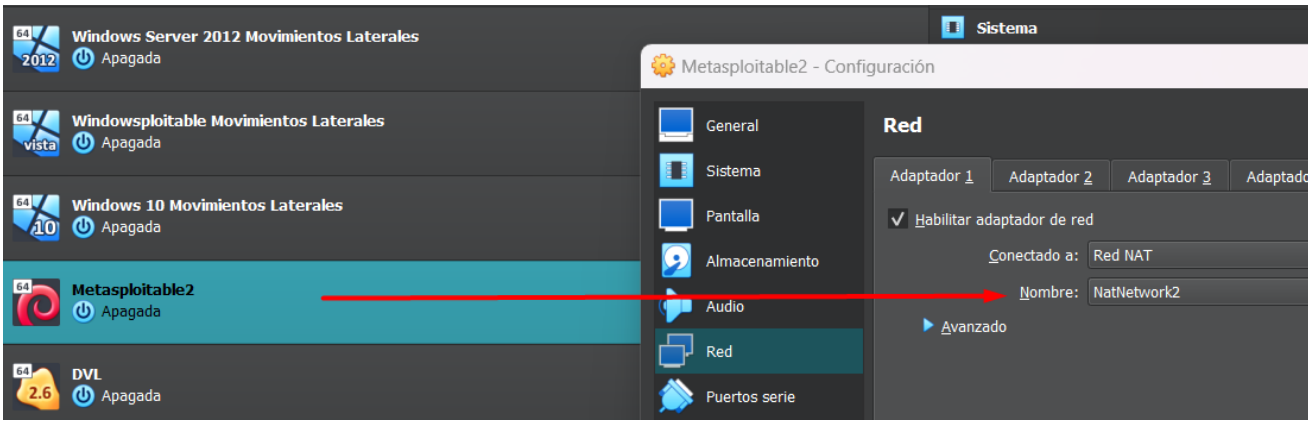
Apache/1.3.37 Server at bt.example.net Port 80

- **Crear un laboratorio de tres máquinas en dos segmentos de red de forma que solo una tenga acceso a las dos**

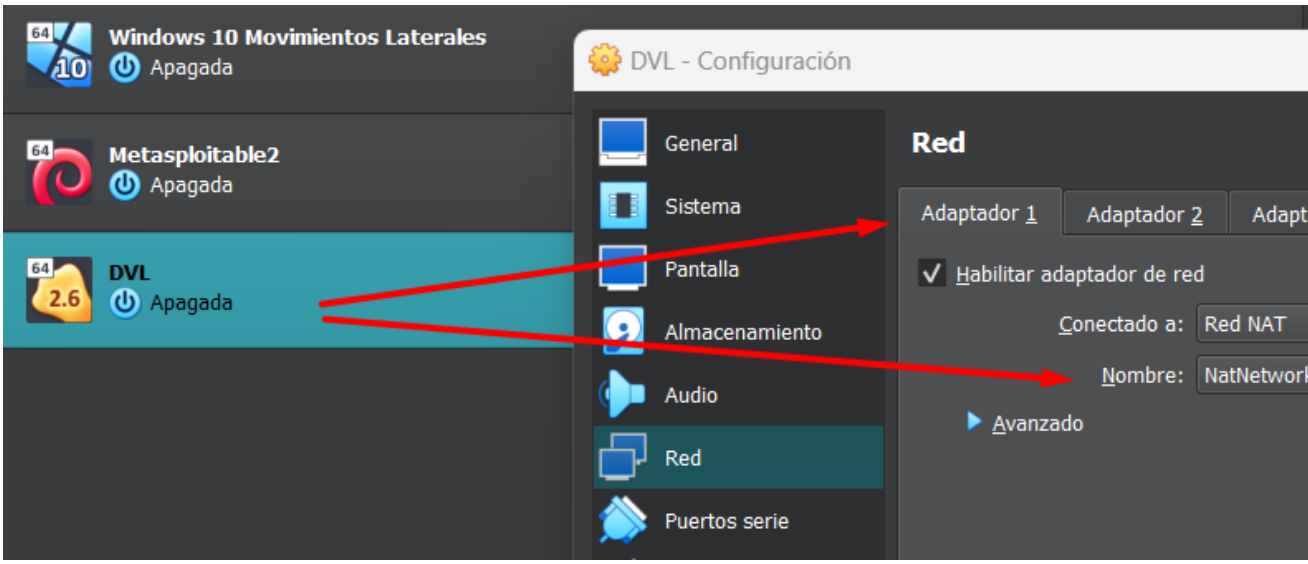
interfaces para realizar Remote Port Forwarding.

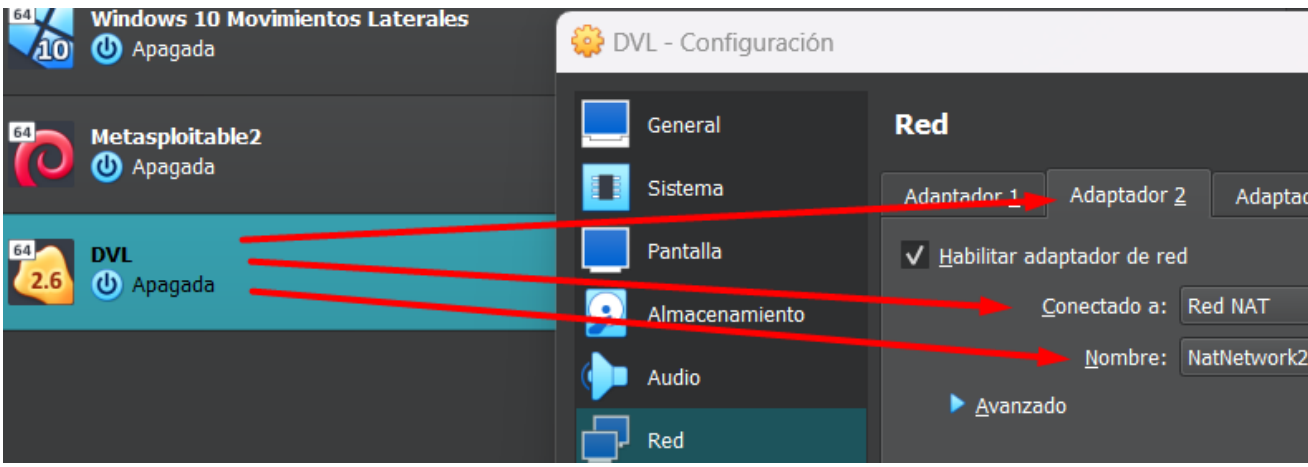
Para esto dejamos la configuración de red de Kali intacta y modficamos la de DVL y metasploitable de la siguiente forma

- Meta: la ponemos en el segmento de red 2



- DVL: creamos un segundo adaptador y modificamos los segmentos de red





Verificamos las respectivas IP's en las máquinas

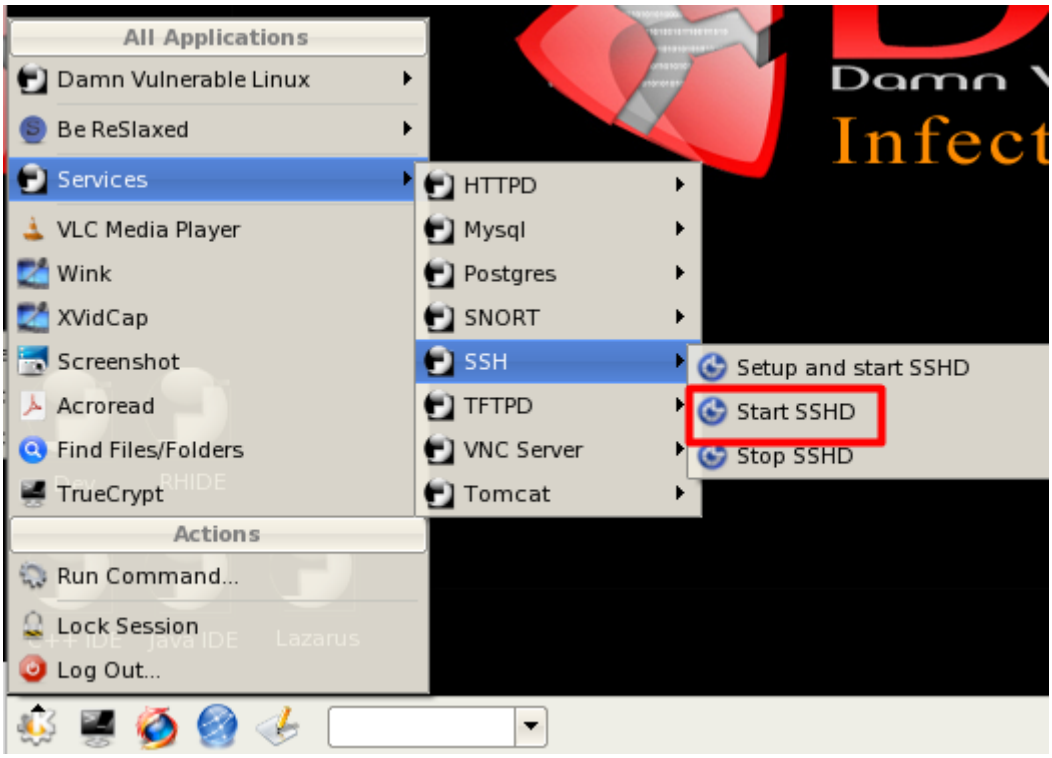
- Meta

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1a:52:c2
          inet addr:10.0.3.4  Bcast:10.0.3.255  Mask:255.255.255.
          inet6 addr: fe80::a00:27ff:fe1a:52c2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7168 (7.0 KB)  TX bytes:7224 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

- DVL

```
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0F:00:78
          inet addr:10.0.2.20  Bcast:10.0.2.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1782 (1.7 KiB)  TX bytes:1830 (1.7 KiB)
          Base address:0xd020 Memory:f0200000-f0220000

eth1      Link encap:Ethernet  HWaddr 08:00:27:EB:F9:15
          inet addr:10.0.3.7  Bcast:10.0.3.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:31 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6120 (5.9 KiB)  TX bytes:1240 (1.2 KiB)
          Base address:0xd240 Memory:f0820000-f0840000
```

En esta ultima máquina activamos el servicio SSH



- **Realizar un esquema explicativo del comando a utilizar.**
  - **Inicio del túnel:** 10.0.3.4:PUERTO donde el cliente visualiza lo que ocurre en mi IP:PUERTO
  - **Destino del túnel:** 10.0.2.9:PUERTO de la máquina donde quiero dar acceso al cliente

- **Intermedio del túnel:** usuario:IP_DVL ssh -R 10.0.3.4:5555:10.0.2.9:8080 root@10.0.2.20 -oHostKeyAlgorithms=+ssh-dss

  Esto ultimo lo ponemos en marcha para crear un túnel remoto

```
┌──(root㉿kali)-[~]
└─# ssh -R 10.0.3.4:5555:10.0.2.9:8080 root@10.0.2.20 -oHostKeyAlgorithms=+ssh-dss
The authenticity of host '10.0.2.20 (10.0.2.20)' can't be established.
DSA key fingerprint is SHA256:0qPXpJ+JV9t53U9ZFdN0Aazcljac53e5N97nrxwR6+o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.20' (DSA) to the list of known hosts.
root@10.0.2.20's password:
Linux 2.6.20-BT-PwnSauce-NOSMP.
bt ~ #
```

- **Hacer Remote Forwarding usando SSH de algún puerto de la máquina Kali Linux.**

  Verificamos la configuración de DVL, así que creamos una sesión desde Kali

```
┌──(root㉿kali)-[~]
└─# ssh root@10.0.2.20 -oHostKeyAlgorithms=+ssh-dss
root@10.0.2.20's password:
Linux 2.6.20-BT-PwnSauce-NOSMP.
bt ~ # pwd
/root
```

  Visualizamos la configuración ssh de la siguiente forma

```
bt ~ # cat /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.74 2006/07/19 13:07:10 dtucker Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/sbin:/sbin:/usr/local/bin:/usr/bin:/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

  Verificamos que la GatewatPorts esté en no para que exista una doble negación y se quede activa

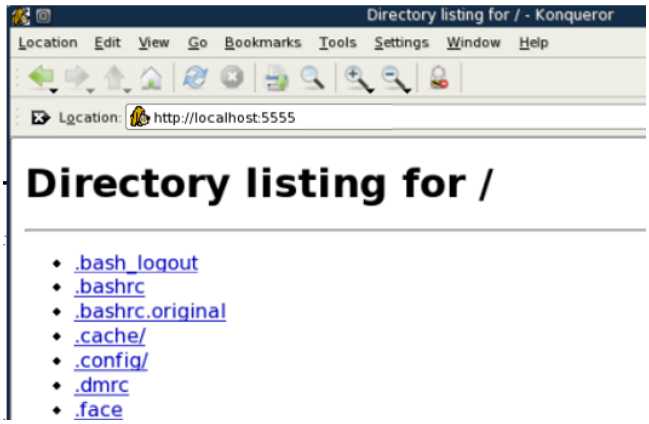
```
#AllowTcpForwarding yes
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS yes
#PidFile /var/run/sshd.pid
#MaxStartups 10
#PermitTunnel no
```

- **Demostrar que el túnel funciona.**

  Con el siguiente comando comprobamos que hemos tunelizado

```
┌──(root㉿kali)-[~]
└─# ps aux | grep ssh
kali        1311  0.0  0.0   7952  3572 ?        Ss   09:41   0:00 /usr/bin/ssh-agent x-session-manager
root        6446  0.0  0.2  14468  8576 pts/0    S+   19:16   0:00 ssh root@10.0.2.20 -oHostKeyAlgorithms=+ssh-dss
root        6497  0.0  0.0   6364  2176 pts/1    S+   19:19   0:00 grep --color=auto ssh
```

  Además de esto podemos verificarlo en el buscador de la máquina



- **Crear un laboratorio de tres máquinas en dos segmentos de red de forma que solo una tenga acceso a las dos interfaces para realizar Dynamic Port Forwarding.**
- **Realizar un esquema explicativo del comando a utilizar.**
  - **Kali:** 10.0.2.9
  - **Meta:** 10.0.3.4
  - **DVL:** 10.0.2.20 10.0.3.7
  - ssh -D 8080 root@10.0.2.20 -oHostKeyAlgorithms=+ssh-dss
- **Hacer Dynamic Port Forwarding usando SSH con Proxy Socks para poder escanear puertos con Proxychains y Nmap de la máquina DVL. Demostrar que el túnel funciona.**

  Para esto nos dirigimos a la carpeta /etc y modificamos el archivo proxychains.conf

```
┌──(root㉿kali)-[~]
└─# cd /etc

┌──(root㉿kali)-[/etc]
└─# nano proxychains.conf
```

  Nos dirigimos abajo del todo del archivo y modificamos el puerto del socks5 y socks4 lo dejamos conectado

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4 127.0.0.1 9050
socks5  127.0.0.1 8080
```

  Guardamos el archivo y nos dirigimos a una terminal para poder poner el siguiente comando

```
┌──(root㉿kali)-[~]
└─# ssh -D 8080 root@10.0.2.20 -oHostKeyAlgorithms=+ssh-dss
root@10.0.2.20's password:
Linux 2.6.20-BT-PwnSauce-NOSMP.
bt ~ #
```

Desde otra terminal realizamos lo siguiente

```
┌──(root㉿kali)-[/etc]
└─# proxychains -q nmap 10.0.3.7 -sT
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-27 19:39 CET
Nmap scan report for 10.0.3.7 (10.0.3.7)
Host is up (0.0031s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
631/tcp  open  ipp
3306/tcp open  mysql
6000/tcp open  X11

Nmap done: 1 IP address (1 host up) scanned in 3.77 seconds
```

Y volvemos a confirmar la conexión

```
┌──(root㉿kali)-[/etc]
└─# ps aux | grep ssh
kali        1311  0.0  0.0   7952  3572 ?        Ss   09:41   0:00 /usr/bin/ssh-agent x-session-manager
root        6789  0.9  0.2  14508  8704 pts/0    S+   19:37   0:01 ssh -D 8080 root@10.0.2.20 -oHostKeyAlgorithms=+
ssh-dss
root        6897  0.0  0.0   6364  2304 pts/1    S+   19:39   0:00 grep --color=auto ssh

┌──(root㉿kali)-[/etc]
```