EJERCICIOS - INTRODUCCIÓN A LOS MOVIMIENTOS LATERALES

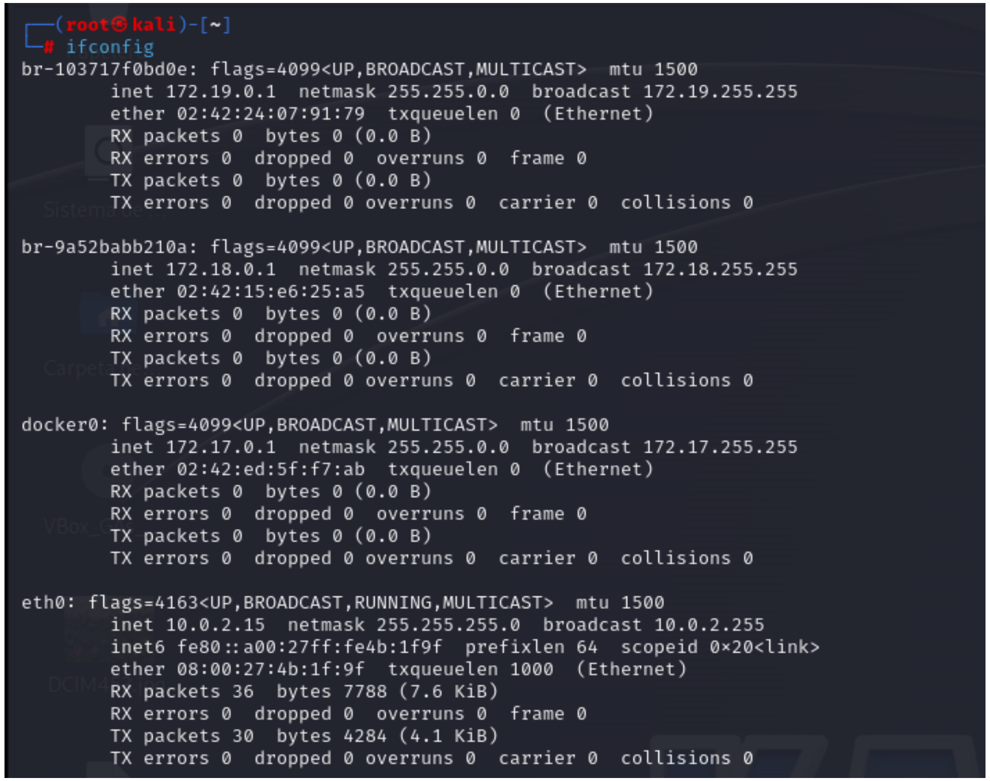
PREREQUISITOS

- KALI LINUX
- METASPLOITABLE2
- DVL

Ejercicio 1 – SSH

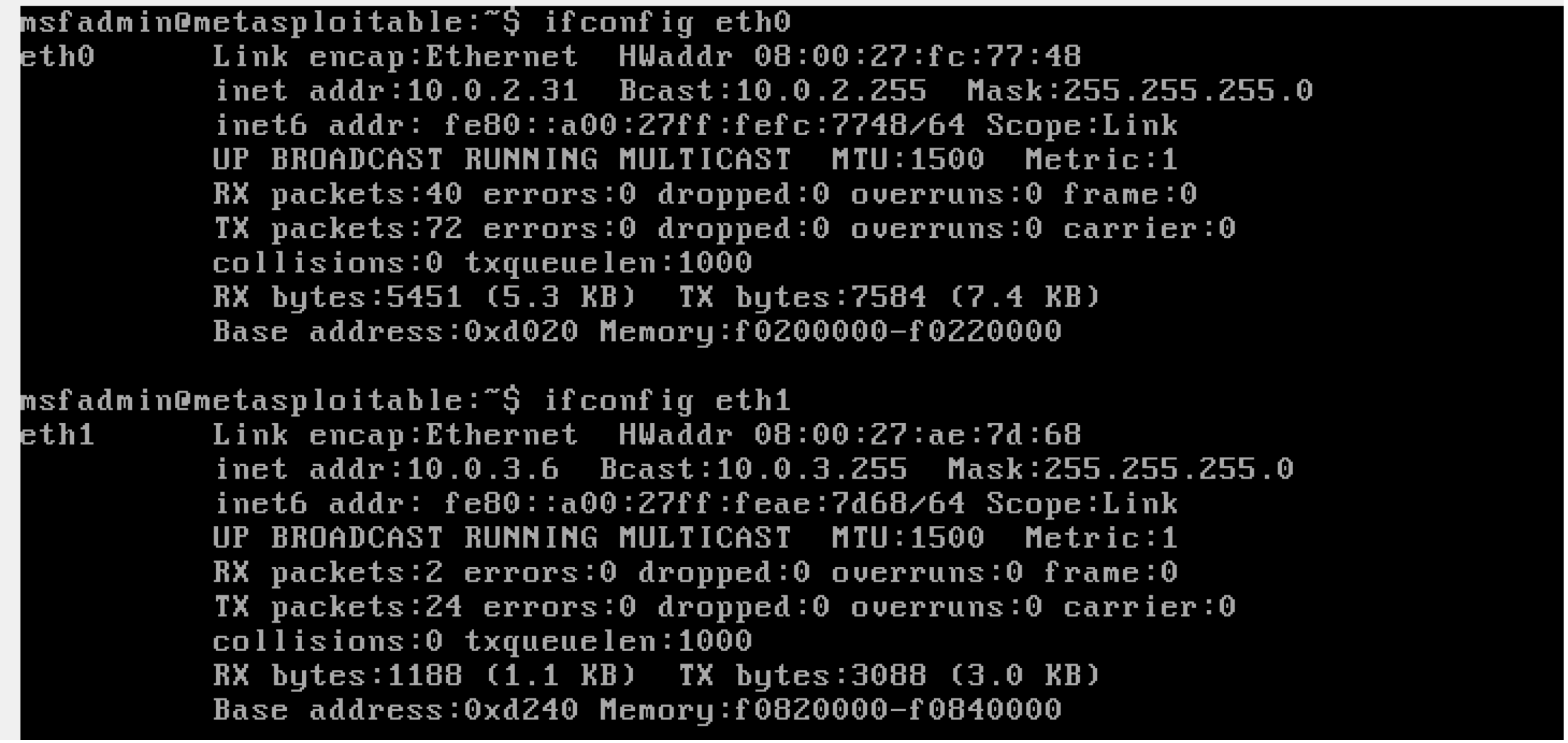
Con una configuración de tres máquinas en dos redes como la vista en clase realiza las siguientes tareas:

Kali linux



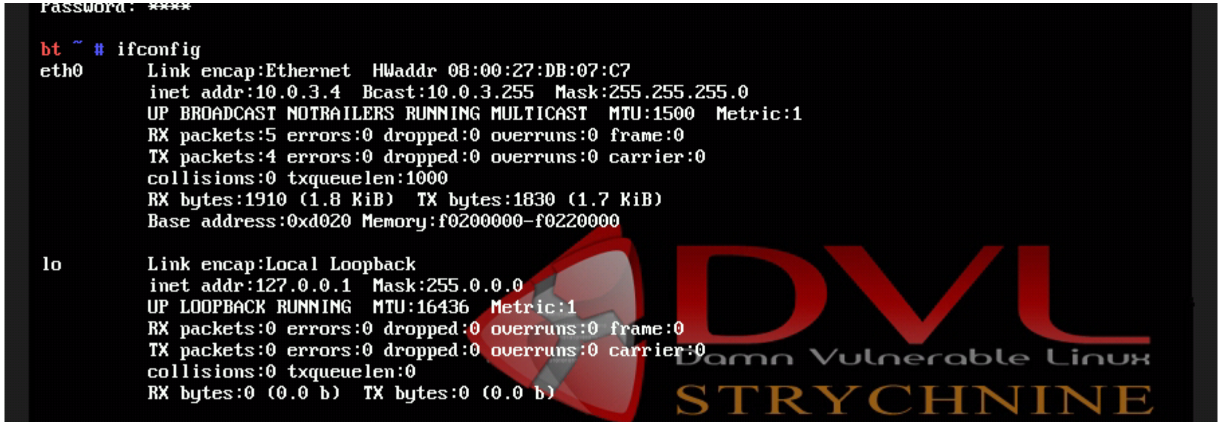
```
┌──(root㉿kali)-[~]
└─# ifconfig
br-103717f0bd0e: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.19.0.1  netmask 255.255.0.0  broadcast 172.19.255.255
        ether 02:42:24:07:91:79  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

br-9a52babb210a: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:15:e6:25:a5  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ed:5f:f7:ab  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe4b:1f9f  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:4b:1f:9f  txqueuelen 1000  (Ethernet)
        RX packets 36  bytes 7788 (7.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 4284 (4.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Metasploitable 2



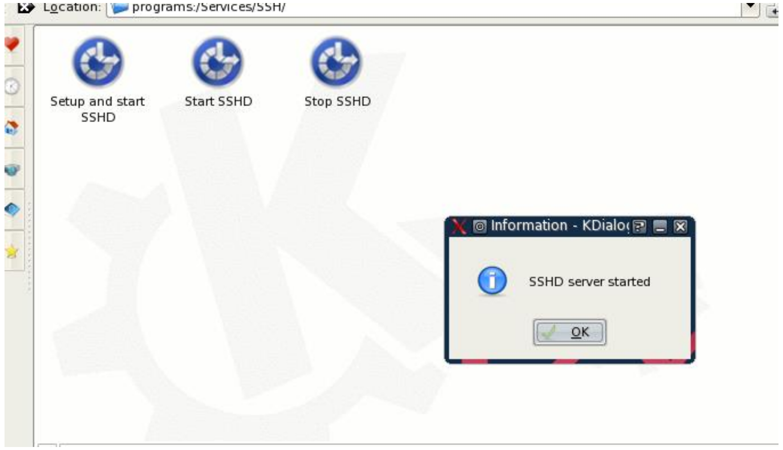
```
msfadmin@metasploitable:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:fc:77:48
          inet addr:10.0.2.31  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fefc:7748/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5451 (5.3 KB)  TX bytes:7584 (7.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

msfadmin@metasploitable:~$ ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:ae:7d:68
          inet addr:10.0.3.6  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feae:7d68/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3088 (3.0 KB)
          Base address:0xd240 Memory:f0820000-f0840000
```

DVL

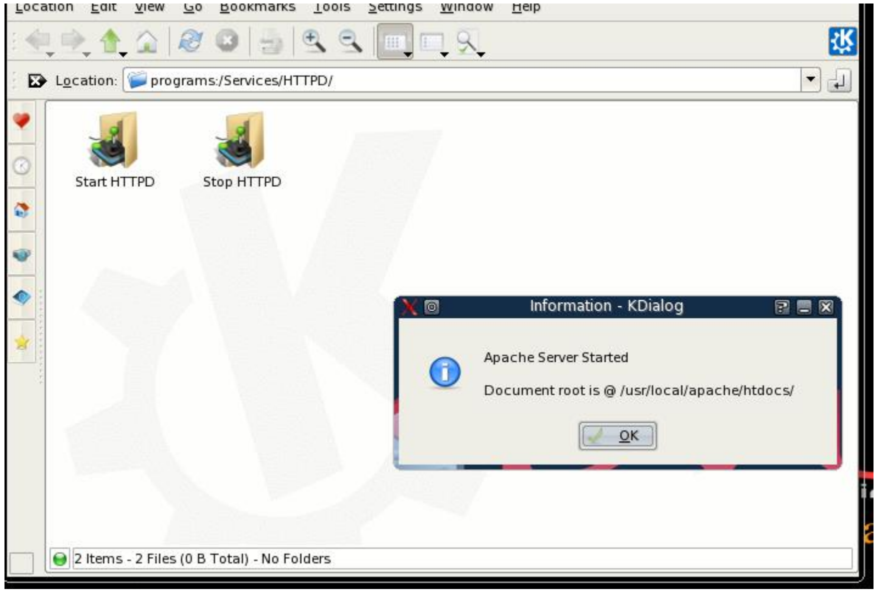


```
Password: ****

bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:DB:07:C7
          inet addr:10.0.3.4  Bcast:10.0.3.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 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:1910 (1.8 KiB)  TX bytes:1830 (1.7 KiB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

- Local Port Forwarding usando SSH de algún puerto de la máquina DVL.



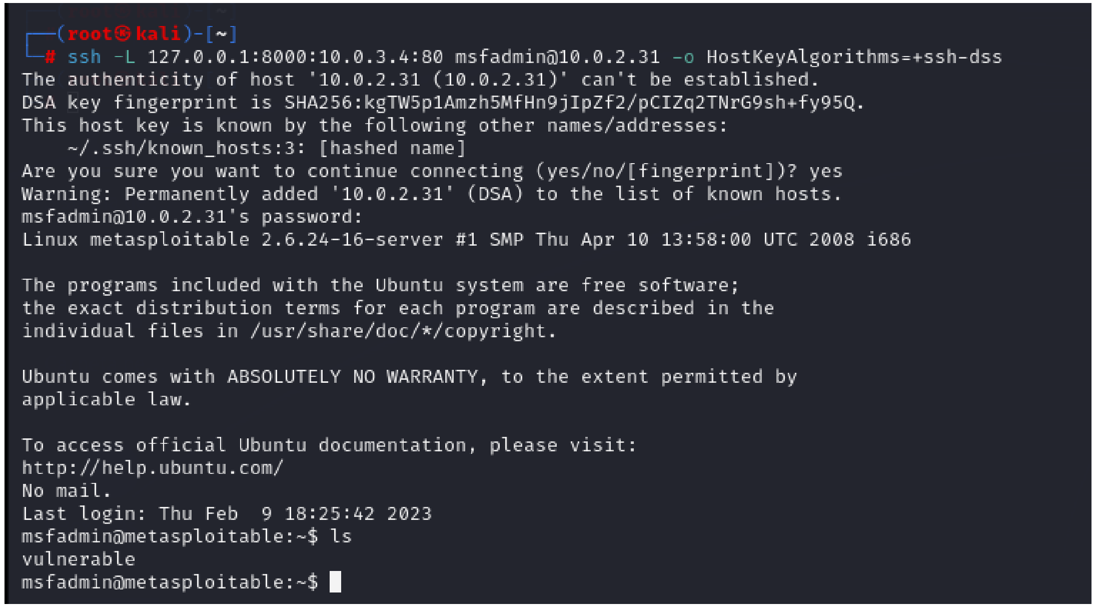
SSHD server started



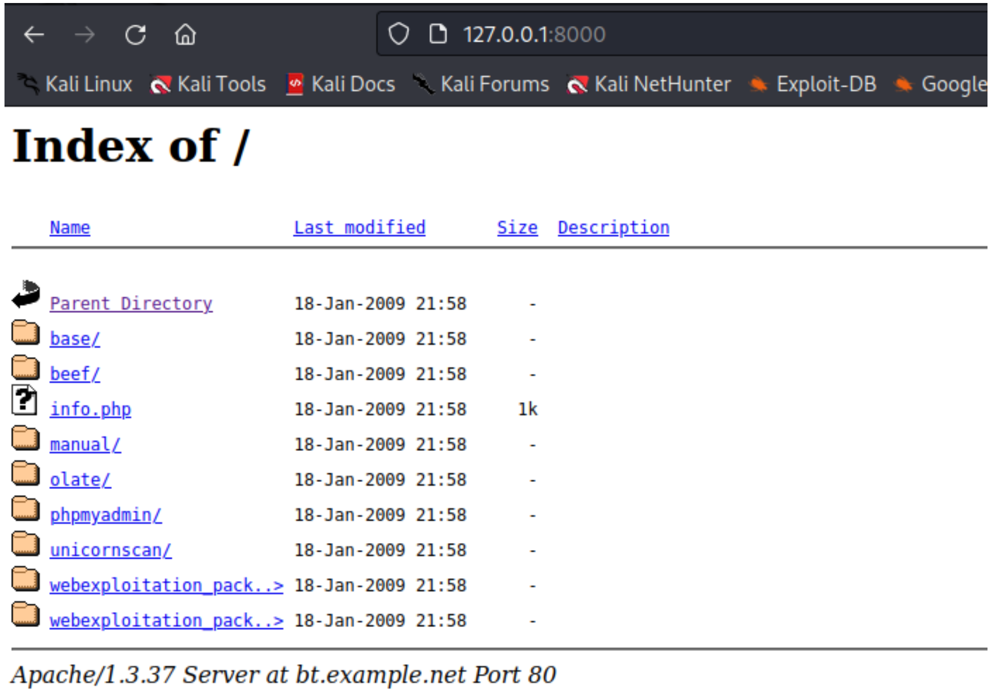
Apache Server Started

Document root is @ /usr/local/apache/htdocs/

2 Items - 2 Files (0 B Total) - No Folders



```
┌──(root㉿kali)-[~]
└─# ssh -L 127.0.0.1:8000:10.0.3.4:80 msfadmin@10.0.2.31 -o HostKeyAlgorithms=+ssh-dss
The authenticity of host '10.0.2.31 (10.0.2.31)' 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:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.31' (DSA) to the list of known hosts.
msfadmin@10.0.2.31'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: Thu Feb  9 18:25:42 2023
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ 
```

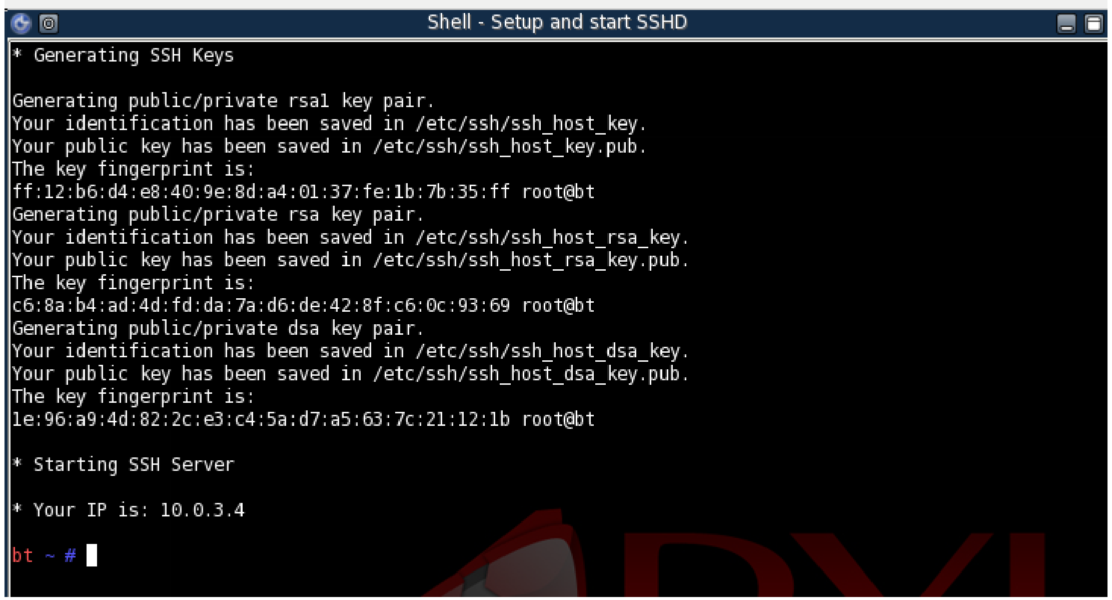


Index of /

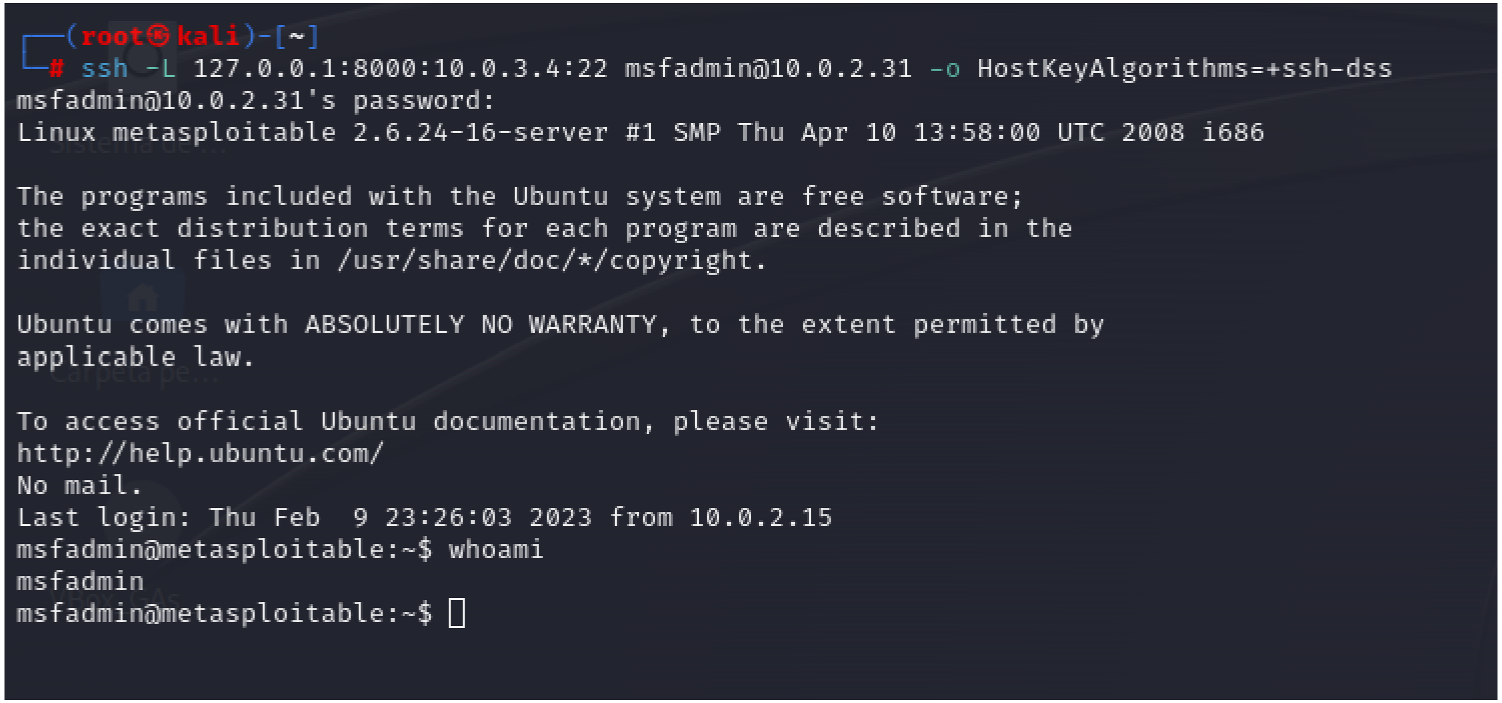
```
     Name                     Last modified      Size  Description
─────────────────────────────────────────────────────────────────────
     Parent Directory         18-Jan-2009 21:58     -
     base/                    18-Jan-2009 21:58     -
     beef/                    18-Jan-2009 21:58     -
     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

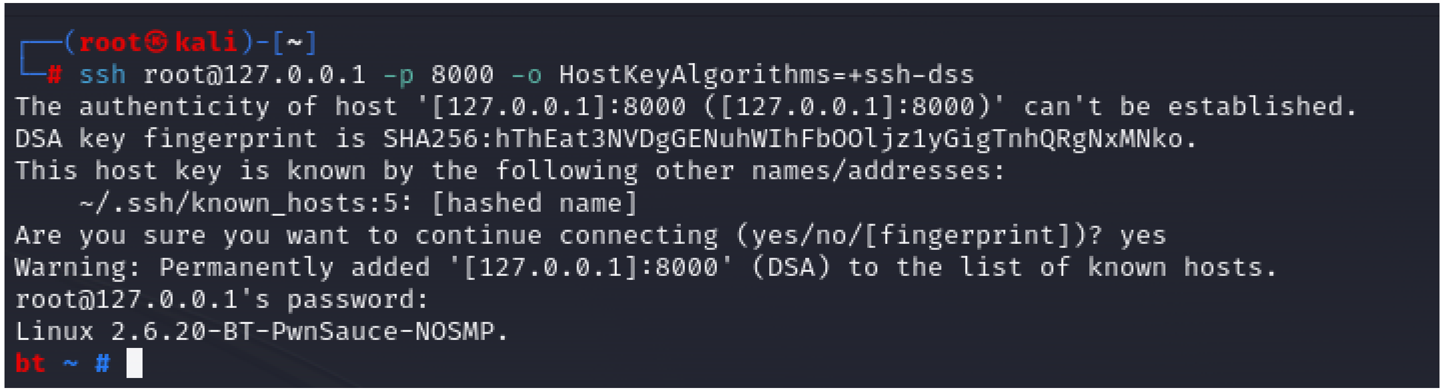
SOLO PARA CONSTANCIA



```
* Generating SSH Keys

Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
The key fingerprint is:
ff:12:b6:d4:e8:40:9e:8d:a4:01:37:fe:1b:7b:35:ff root@bt
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
c6:8a:b4:ad:4d:fd:da:7a:d6:de:42:8f:c6:0c:93:69 root@bt
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
1e:96:a9:4d:82:2c:e3:c4:5a:d7:a5:63:7c:21:12:1b root@bt

* Starting SSH Server

* Your IP is: 10.0.3.4

bt ~ #
```



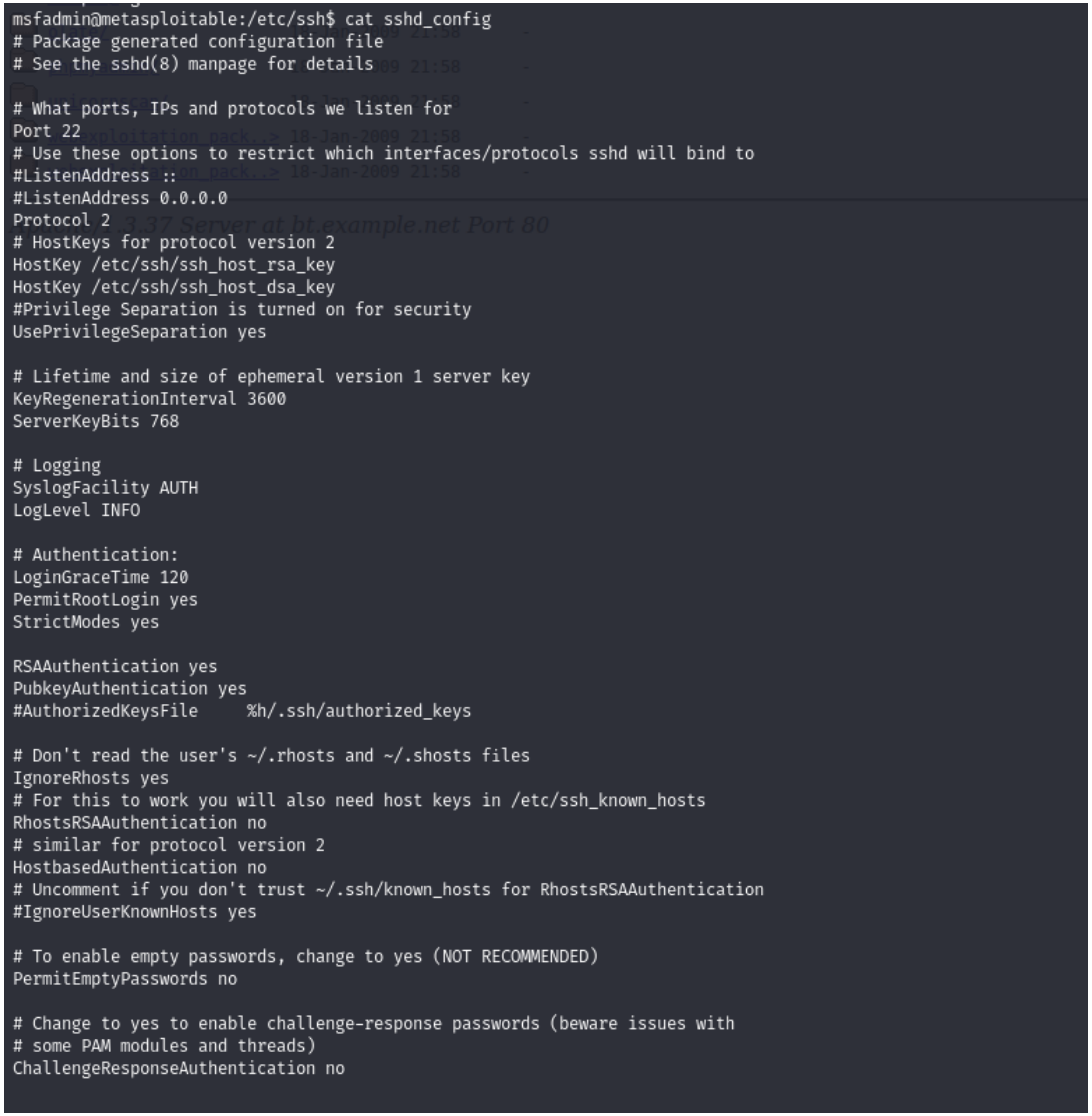
```
┌──(root㉿kali)-[~]
└─# ssh -L 127.0.0.1:8000:10.0.3.4:22 msfadmin@10.0.2.31 -o HostKeyAlgorithms=+ssh-dss
msfadmin@10.0.2.31's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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: Thu Feb  9 23:26:03 2023 from 10.0.2.15
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```



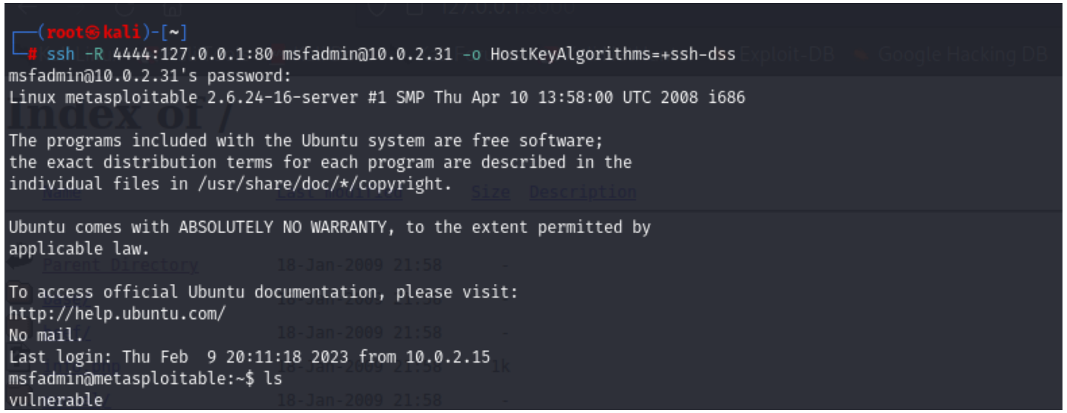
```
┌──(root㉿kali)-[~]
└─# ssh root@127.0.0.1 -p 8000 -o HostKeyAlgorithms=+ssh-dss
The authenticity of host '[127.0.0.1]:8000 ([127.0.0.1]:8000)' can't be established.
DSA key fingerprint is SHA256:hThEat3NVDgGENuhWIhFbOOljz1yGigTnhQRgNxMNko.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:8000' (DSA) to the list of known hosts.
root@127.0.0.1's password:
Linux 2.6.20-BT-PwnSauce-NOSMP.
bt ~ # 
```

- Remote Forwarding usando SSH de algún puerto de la máquina DVL

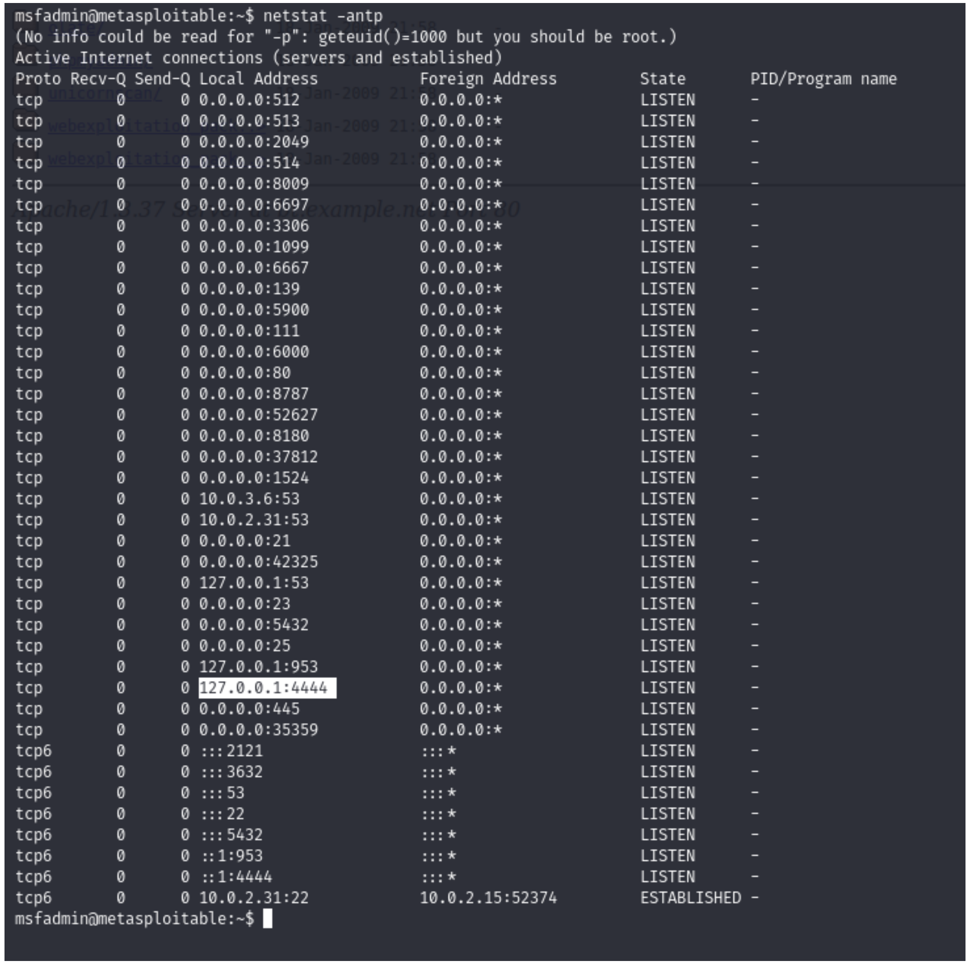
El GatewayPorts no esta



```
msfadmin@metasploitable:/etc/ssh$ cat 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

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```



```
┌──(root㉿kali)-[~]
└─# ssh -R 4444:127.0.0.1:80 msfadmin@10.0.2.31 -o HostKeyAlgorithms=+ssh-dss
msfadmin@10.0.2.31'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: Thu Feb  9 20:11:18 2023 from 10.0.2.15
msfadmin@metasploitable:~$ ls
vulnerable
```

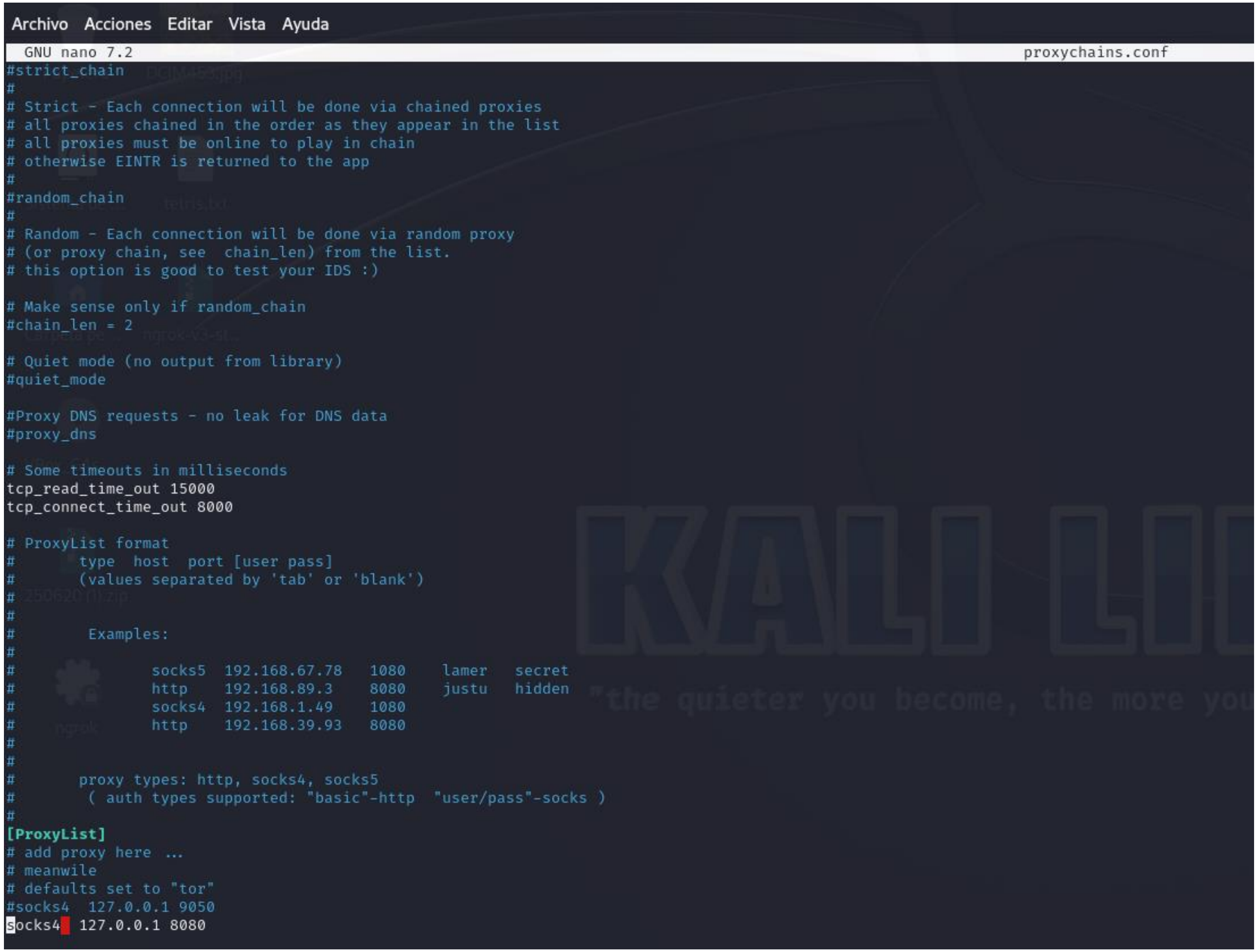


```
msfadmin@metasploitable:~$ netstat -antp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:52627           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:37812           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN      -
tcp        0      0 10.0.3.6:53             0.0.0.0:*               LISTEN      -
tcp        0      0 10.0.2.31:53            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:42325           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:4444          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:35359           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::2121                 :::*                    LISTEN      -
tcp6       0      0 :::3632                 :::*                    LISTEN      -
tcp6       0      0 :::53                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::5432                 :::*                    LISTEN      -
tcp6       0      0 ::1:953                 :::*                    LISTEN      -
tcp6       0      0 ::1:4444                :::*                    LISTEN      -
tcp6       0      0 10.0.2.31:22            10.0.2.15:52374         ESTABLISHED -
msfadmin@metasploitable:~$
```

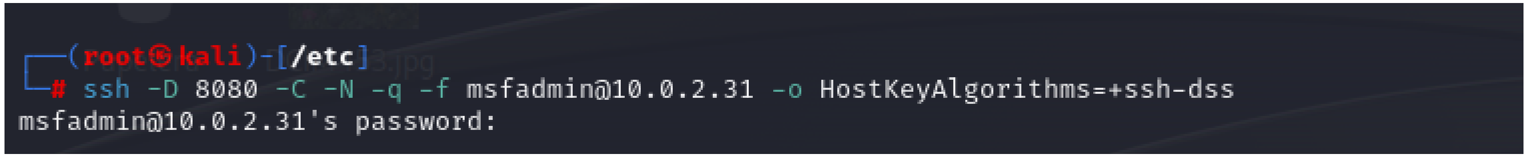
Ejercicio 2 - SSH, Proxychains y Nmap

Con una configuración de tres máquinas en dos redes como la vista en clase realiza las siguientes tareas:

- Dynamic Port Forwarding (proxy SOCKS) usando SSH.

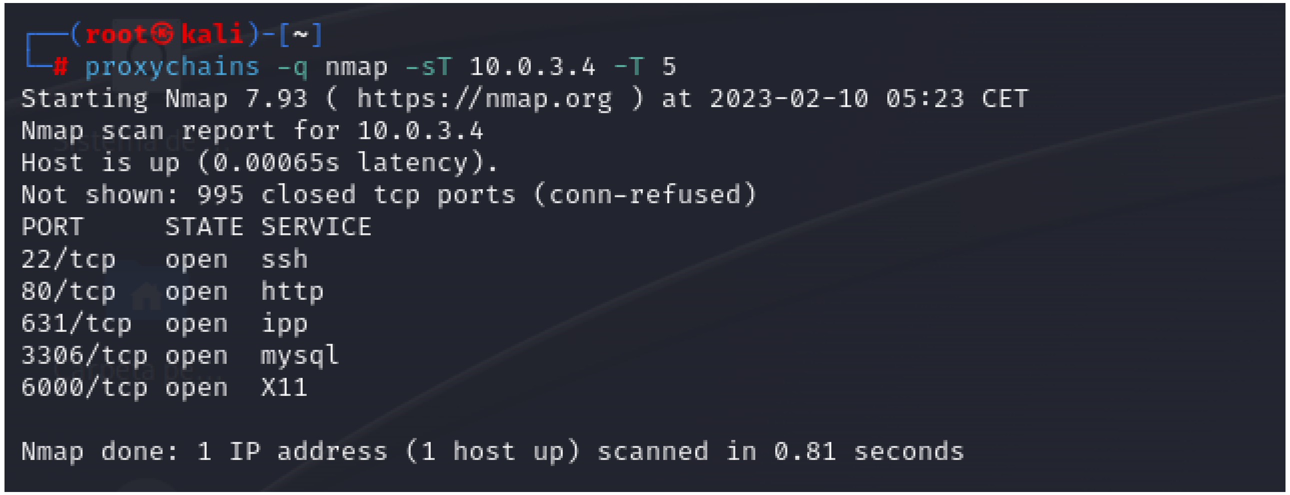


```
  GNU nano 7.2                                                                                   proxychains.conf
#strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2

# Quiet mode (no output from library)
#quiet_mode

#Proxy DNS requests - no leak for DNS data
#proxy_dns

# Some timeouts in milliseconds
tcp_read_time_out 15000
tcp_connect_time_out 8000

# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4  127.0.0.1 9050
socks4  127.0.0.1 8080
```

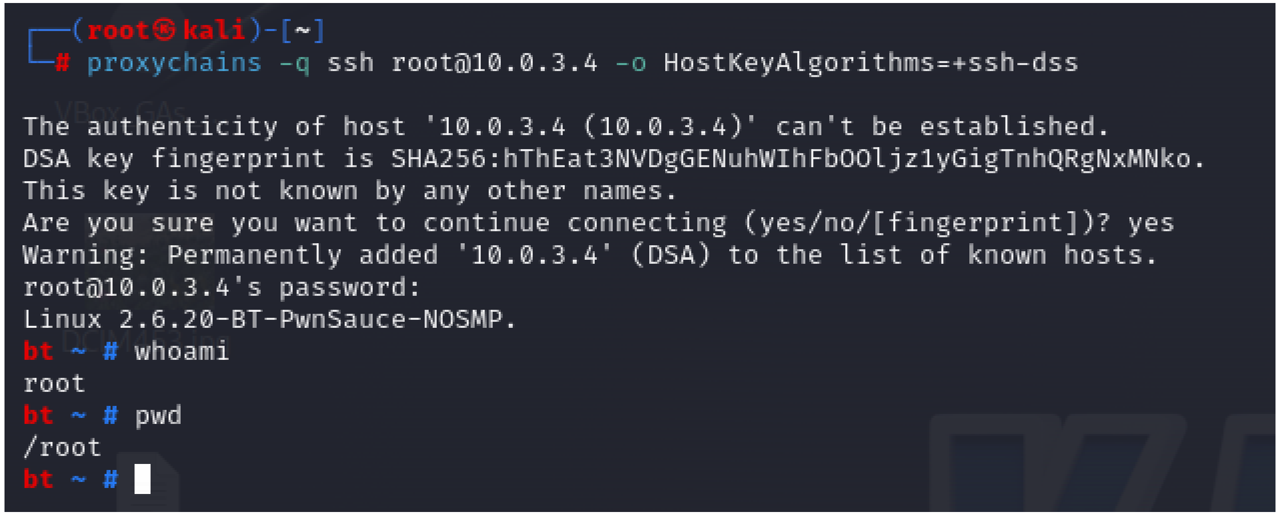


```
┌──(root㉿kali)-[/etc]
└─# ssh -D 8080 -C -N -q -f msfadmin@10.0.2.31 -o HostKeyAlgorithms=+ssh-dss
msfadmin@10.0.2.31's password:
```

- Escaneo de puertos usando proxychains y nmap.



```
┌──(root㉿kali)-[~]
└─# proxychains -q nmap -sT 10.0.3.4 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-10 05:23 CET
Nmap scan report for 10.0.3.4
Host is up (0.00065s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
631/tcp  open  ipp
3306/tcp open  mysql
6000/tcp open  X11

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```



```
┌──(root㉿kali)-[~]
└─# proxychains -q ssh root@10.0.3.4 -o HostKeyAlgorithms=+ssh-dss

The authenticity of host '10.0.3.4 (10.0.3.4)' can't be established.
DSA key fingerprint is SHA256:hThEat3NVDgGENuhWIhFbOOljz1yGigTnhQRgNxMNko.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.4' (DSA) to the list of known hosts.
root@10.0.3.4's password:
Linux 2.6.20-BT-PwnSauce-NOSMP.
bt ~ # whoami
root
bt ~ # pwd
/root
bt ~ #
```