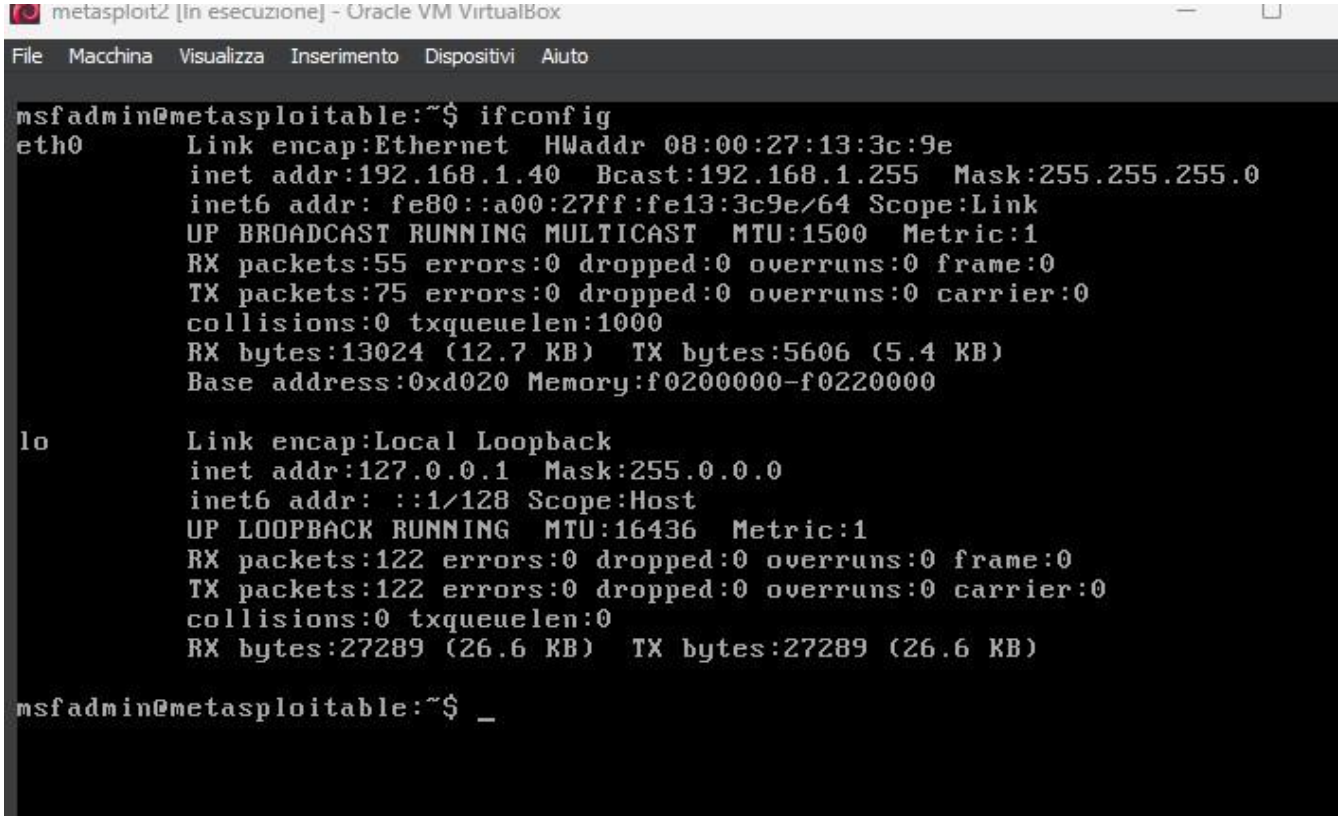
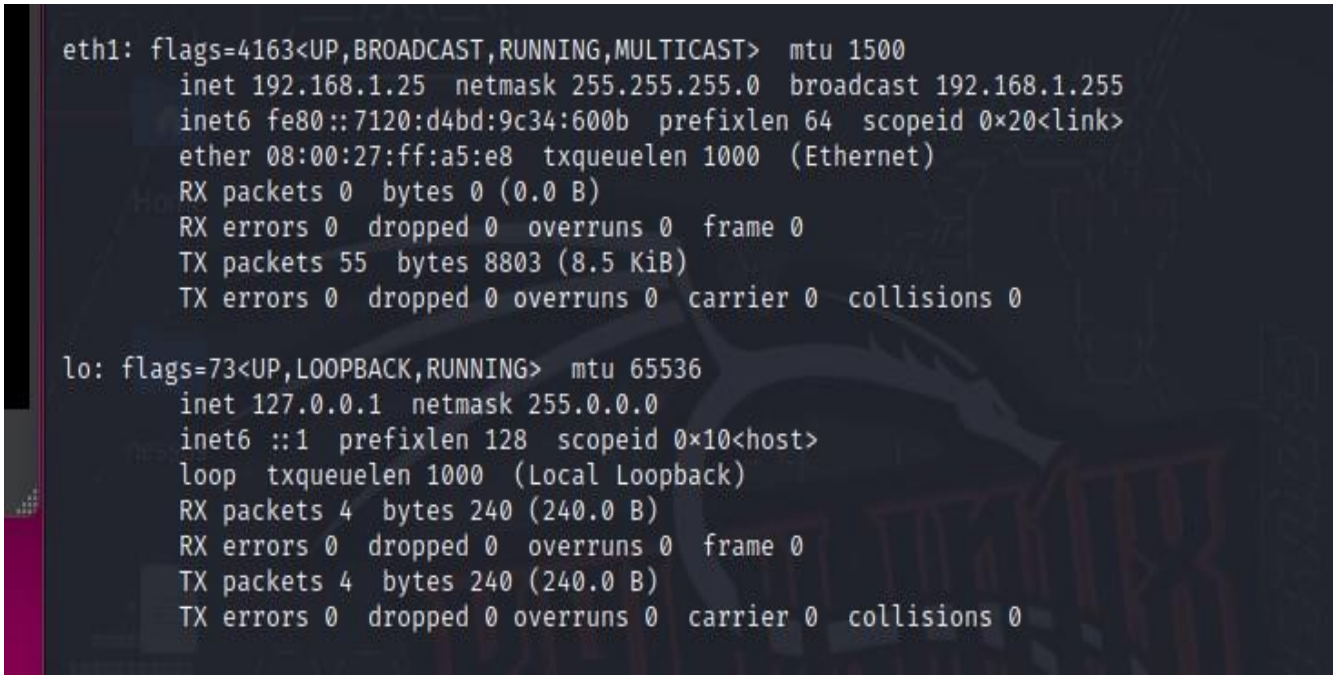
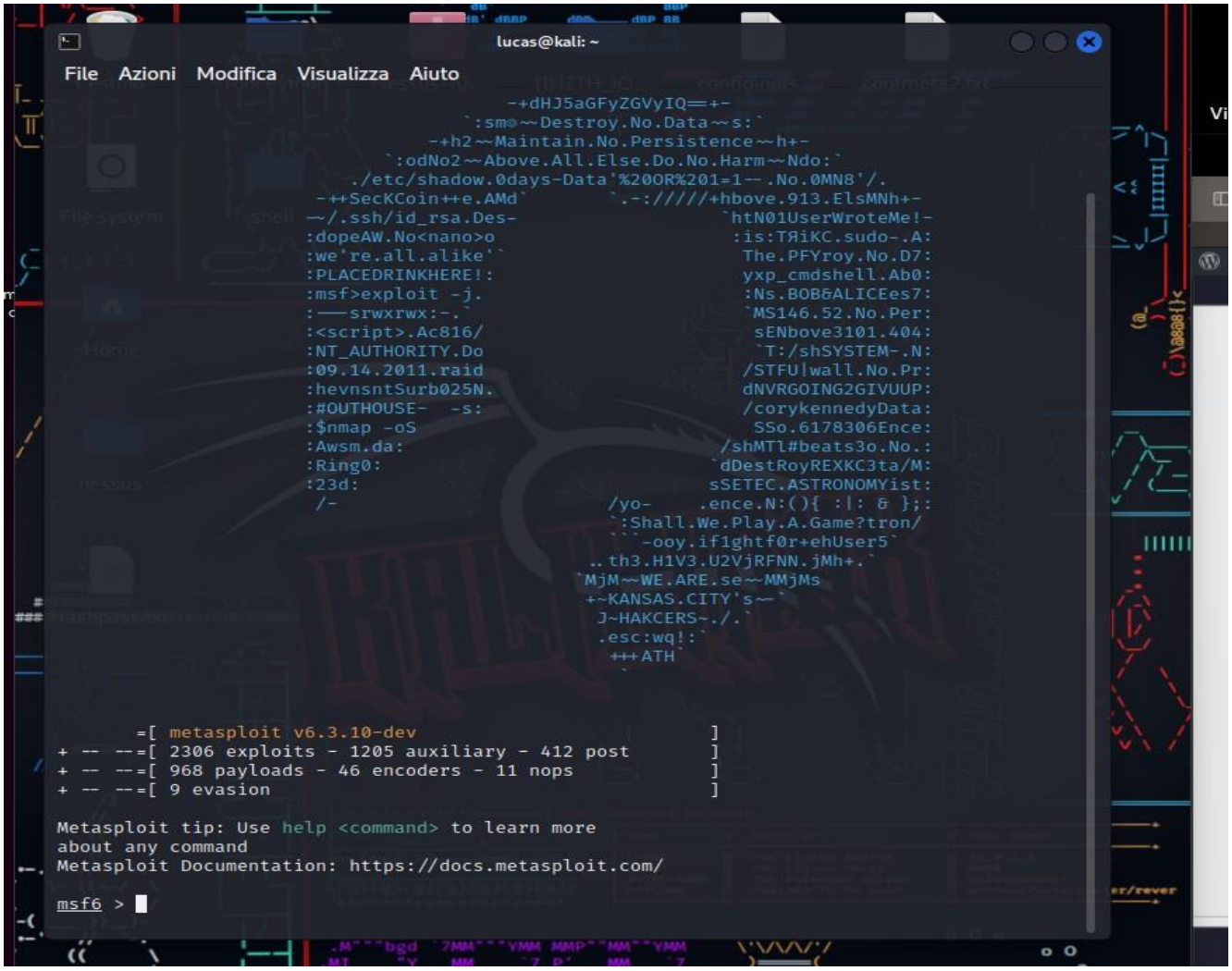
Configurazione IP: 192.168.1.40 metasploitable2



Configurazione IP: 192.168.1.25 kali

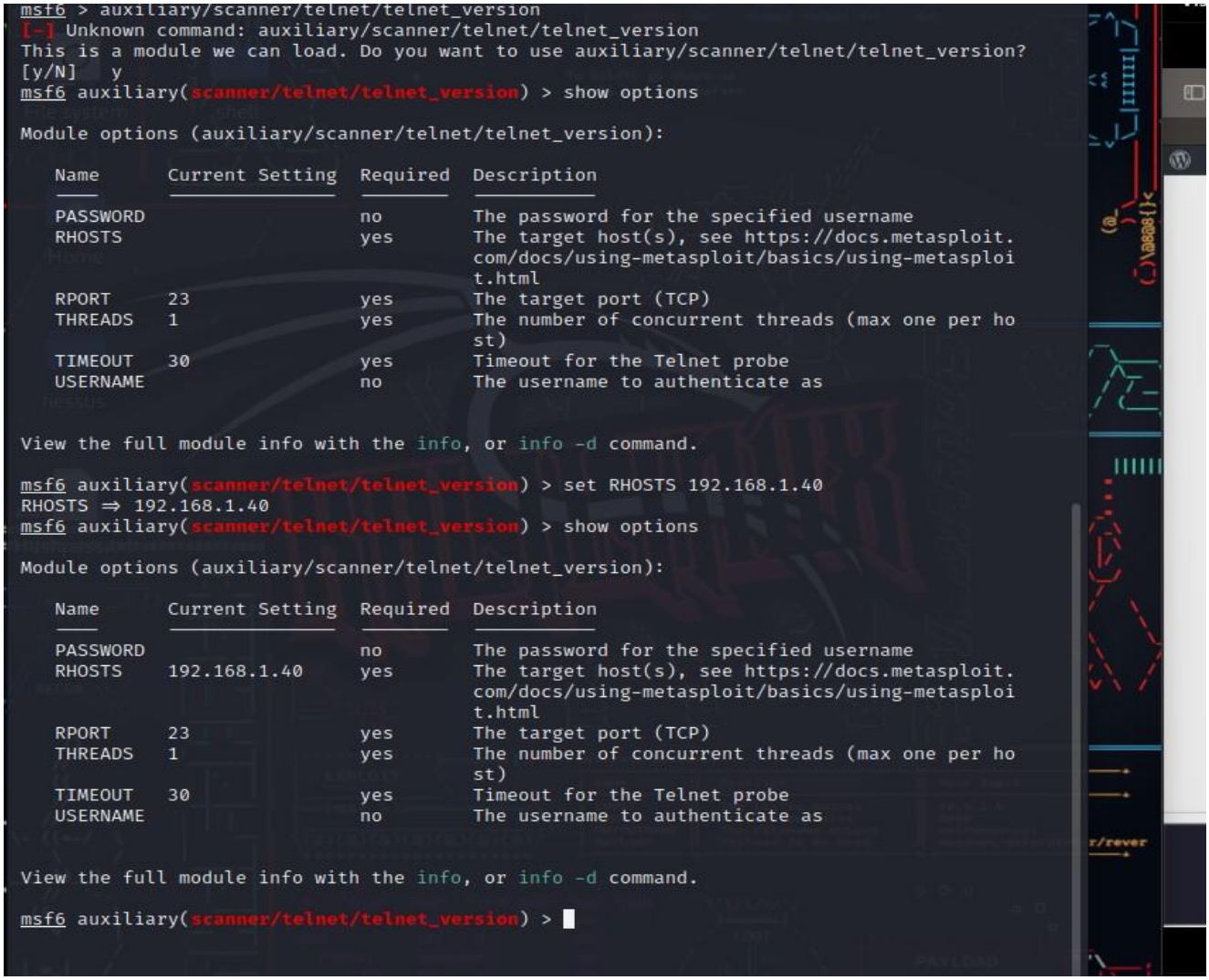


Lanciamo msfconsole



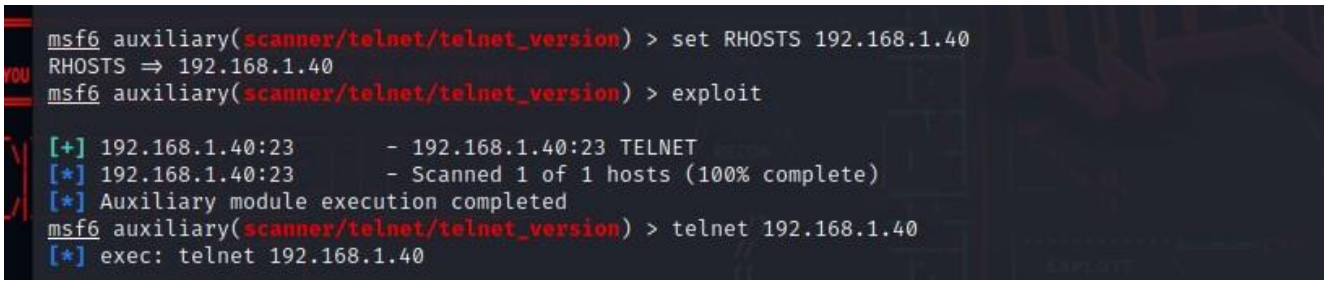
Nella figura in basso, vediamo come abbiamo sfruttare la vulnerabilità del servizio telnet utilizzando il path.

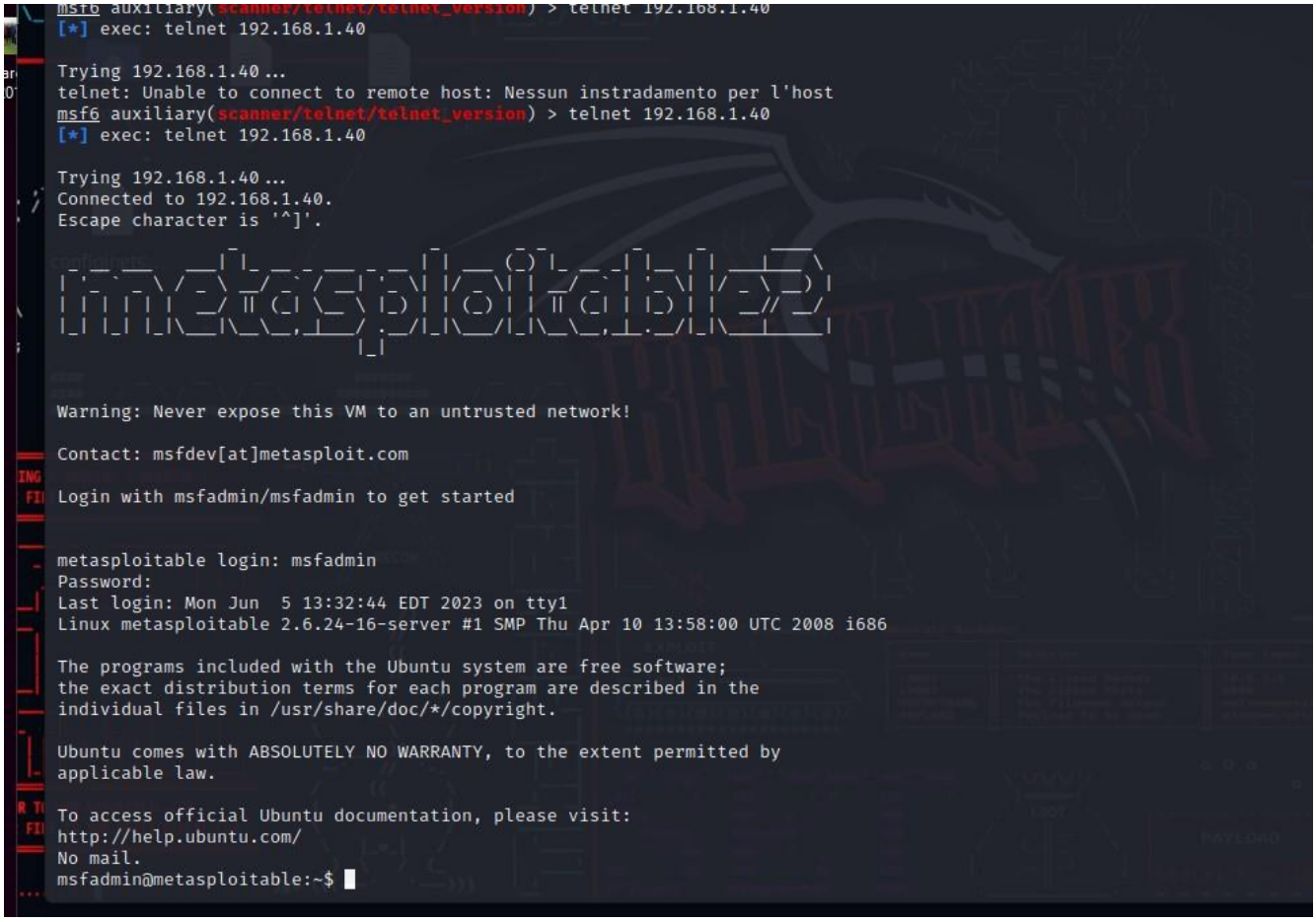
controlliamo i vari parametri necessari per lanciare l'exploit, con il comando show options possiamo modificare le opzioni.

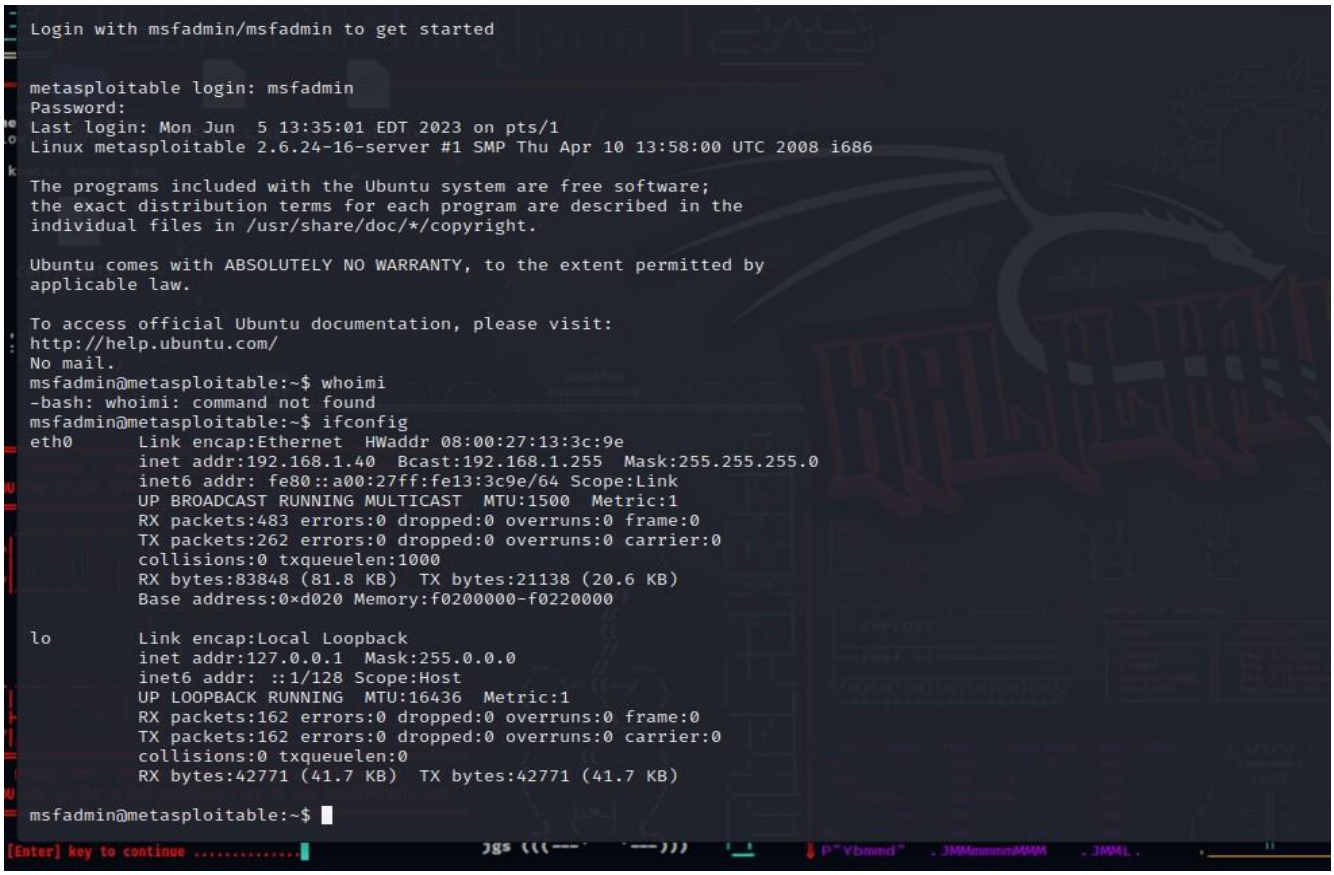


Abbiamo configurato RHOSTS della nostra macchina vittima metasploitable2 con l'IP 192.168.1.40

Lanciamo il comando exploit per eseguire l'attacco, il modulo ha recuperato username e password




msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40
Trying 192.168.1.40 ...
telnet: Unable to connect to remote host: Nessun instradamento per l'host
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: msfadmin
Password:
Last login: Mon Jun 5 13:32:44 EDT 2023 on tty1
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:~$


Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Mon Jun 5 13:35:01 EDT 2023 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:~$ whoimi
-bash: whoimi: command not found
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:13:3c:9e
inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe13:3c9e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:483 errors:0 dropped:0 overruns:0 frame:0
TX packets:262 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:83848 (81.8 KB) TX bytes:21138 (20.6 KB)
Base address:0x4020 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:162 errors:0 dropped:0 overruns:0 frame:0
TX packets:162 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:42771 (41.7 KB) TX bytes:42771 (41.7 KB)
msfadmin@metasploitable:~$
[Enter] key to continue .....