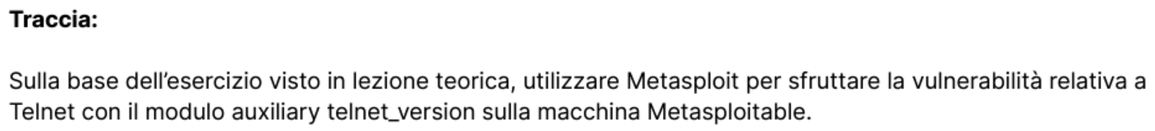
S7L2

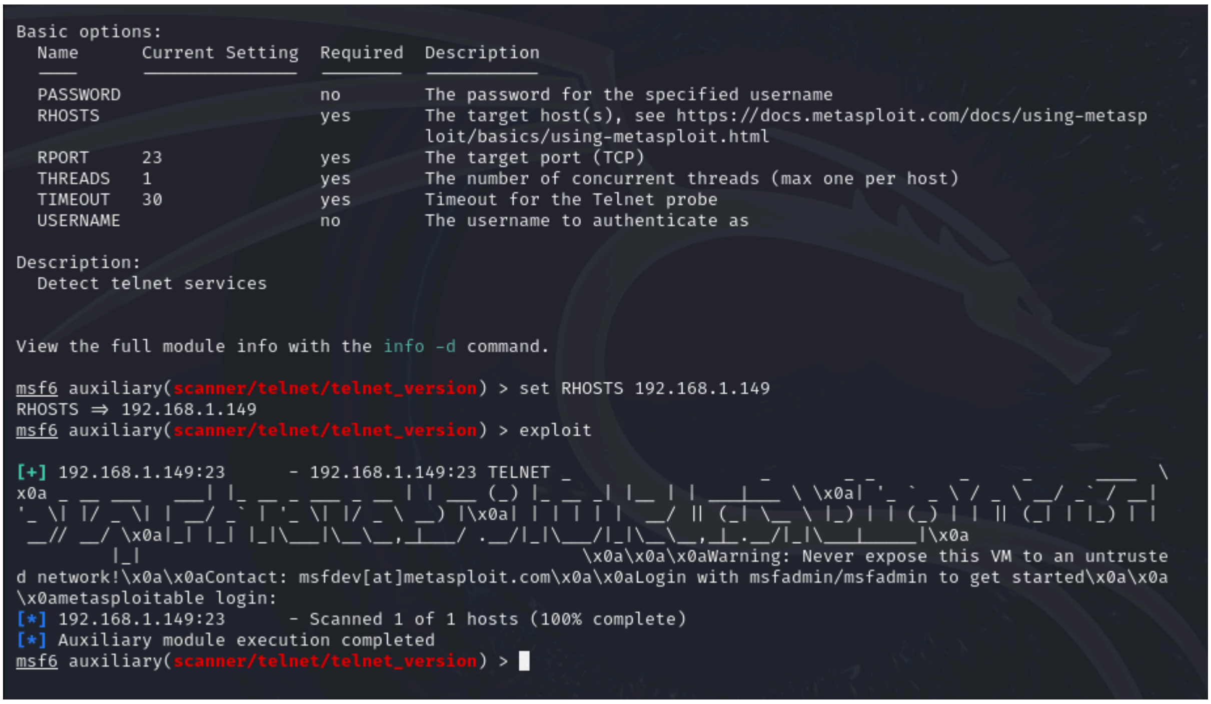


Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Avviato msfconsole ho eseguito il comando use auxiliary “scanner/telnet/telnet_version” per selezionare e usare il modulo Telnet ho successivamente eseguito uno show options per controllare i parametri, a quel punto ho usato “set RHOSTS 192.168.1.149” per impostare l’host con l’indirizzo del target ovvero Metasploit.

Una volta settato ho eseguito il comando exploit e a quel punto dall’output si può notare le credenziali di accesso “msfadmin/msfadmin”; quindi ho chiuso msfconsole e ho eseguito Telnet con indirizzo di Metasploitable e ho eseguito l’accesso con msfadmin/msfadmin.



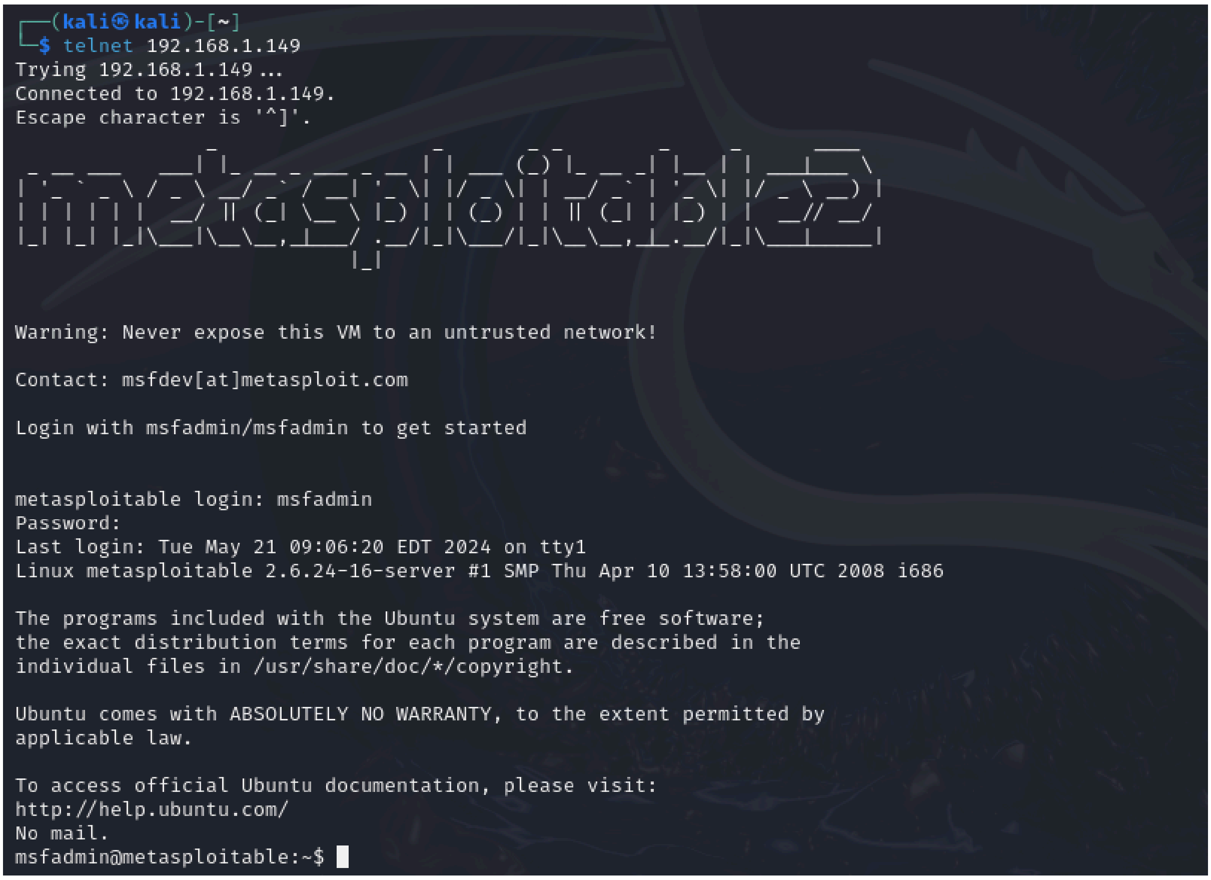
```
Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  PASSWORD                   no        The password for the specified username
  RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasp
                                       loit/basics/using-metasploit.html
  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


View the full module info with the info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.149:23      - 192.168.1.149:23 TELNET _                  _       _ _        _     _      ____  \
x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __|
'_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |
 __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a
           |_|                                          \x0a\x0a\x0aWarning: Never expose this VM to an untruste
d network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a
\x0ametasploitable login:
[*] 192.168.1.149:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```



```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.149
Trying 192.168.1.149...
Connected to 192.168.1.149.
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 May 21 09:06:20 EDT 2024 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:~$
```