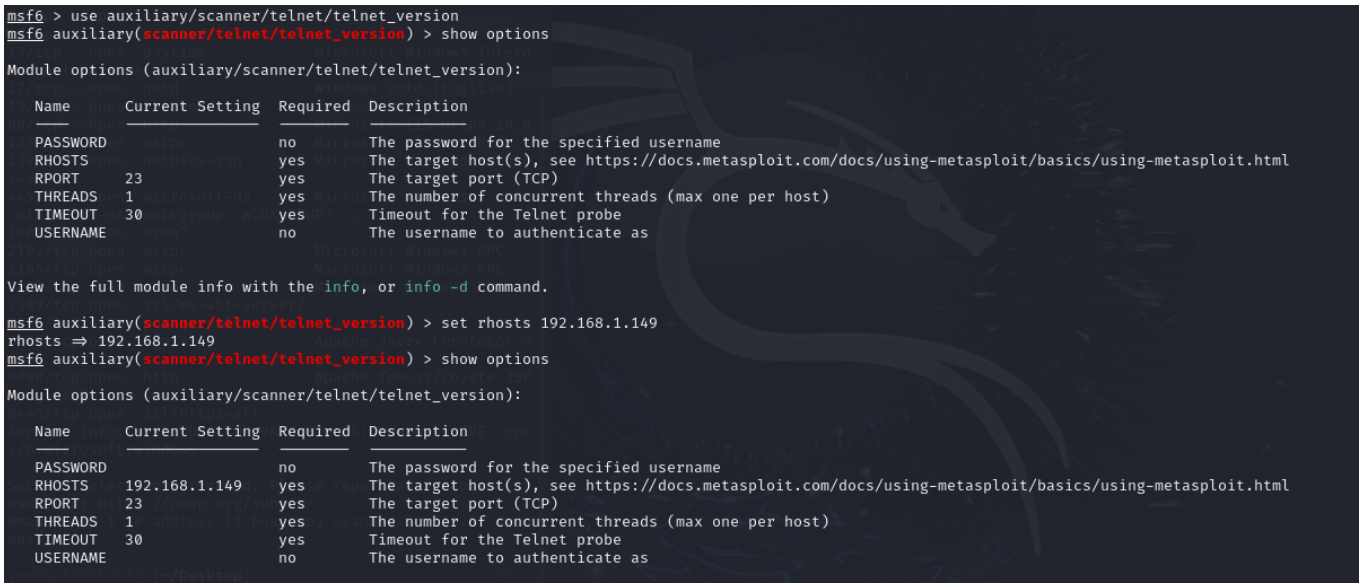
EXPLOIT TELNET CON METASPLOIT:

Nel compito di oggi abbiamo attaccato telnet di metasplotable per trovare user e password.

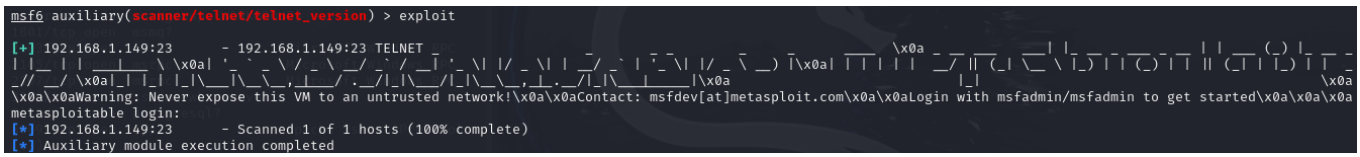
Abbiamo utilizzato metasploit con il modulo ausiliario per colpire precisamente la vulnerabilità interessata.

Come vediamo nell'immagine qui sotto utilizzando il modulo ausiliario con il comando "use auxiliary/scanner/telnet/telnet_version" ci da diversi parametri, e noi dobbiamo impostare l'rhosts, cioè l'ip di metasploitable che è la macchina target.

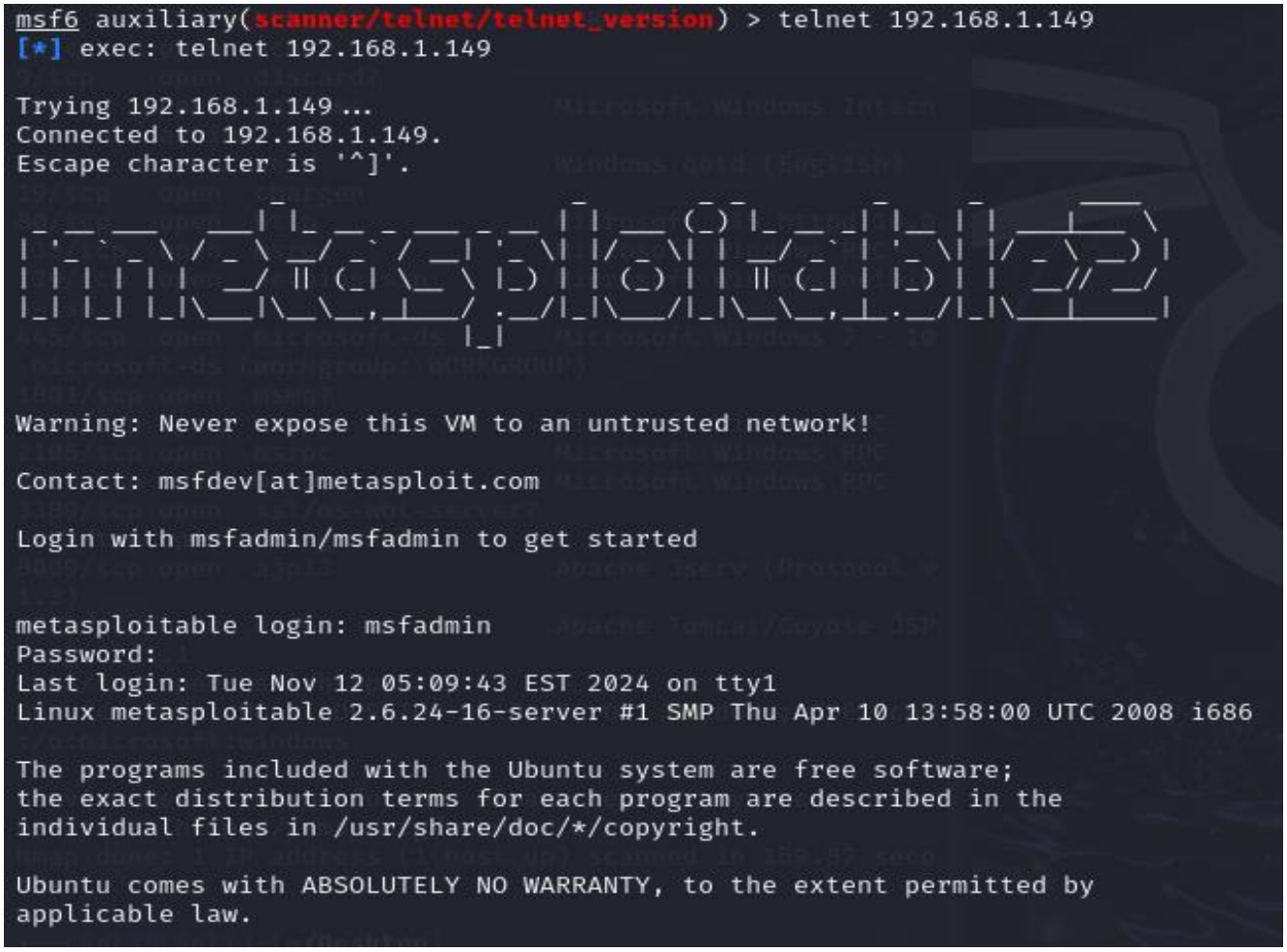


Una volta settato l'ip target abbiamo tutti i parametri necessari, adesso possiamo lanciare l'exploit.

In output vediamo tra le varie informazioni msfadmin/msfadmin che sono appunto le credenziali di metasploitable, quindi l'attacco è andato a buon fine:



Per avere una controprova dell'esattezza delle credenziali, possiamo provaare a fare l'accesso con il comando "telnet 192.168.1.149" dove ci chiederà di inserirle e ci dirà se siamo entrati o meno.


msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.149
[*] exec: 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 Nov 12 05:09:43 EST 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.