Exploit Telnet con Metasploit

Indice

Traccia

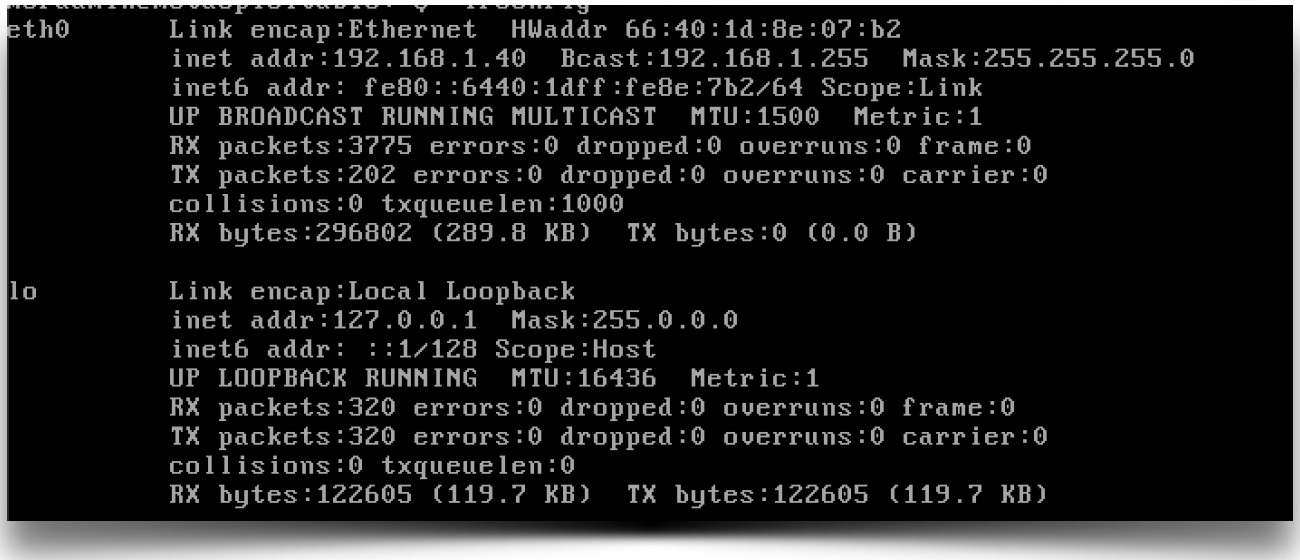
Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito:
Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40.

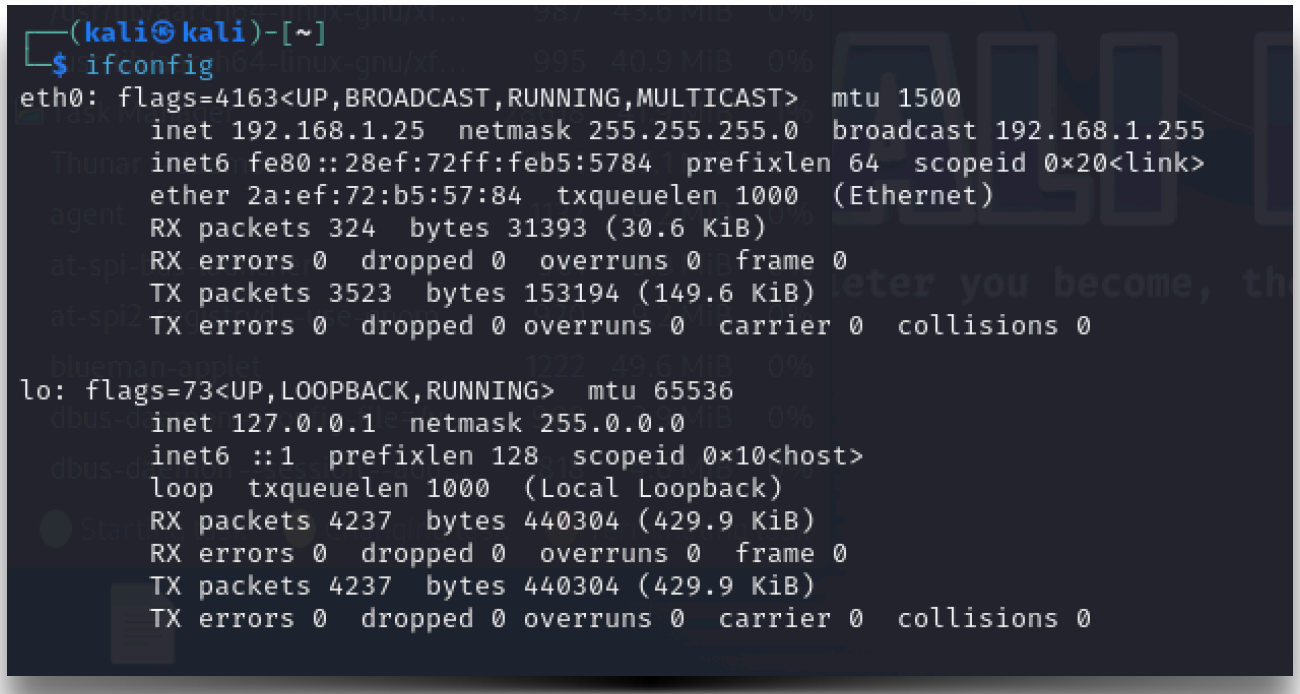
1 Configurazione delle macchine Metasploitable e Kali

Nella prima fase dell'esercizio sono stati configurati gli IP delle macchine Metasploitable e Kali.
L'indirizzo IP della macchina Metasploitable è stato configurato con ***192.168.1.40.***
Mentre l'indirizzo IP della macchina Kali è stato configurato con ***192.168.1.25,*** come si può vedere nelle immagini riportate qui sotto.

Configurazione di Metasploitable



Configurazione di Kali

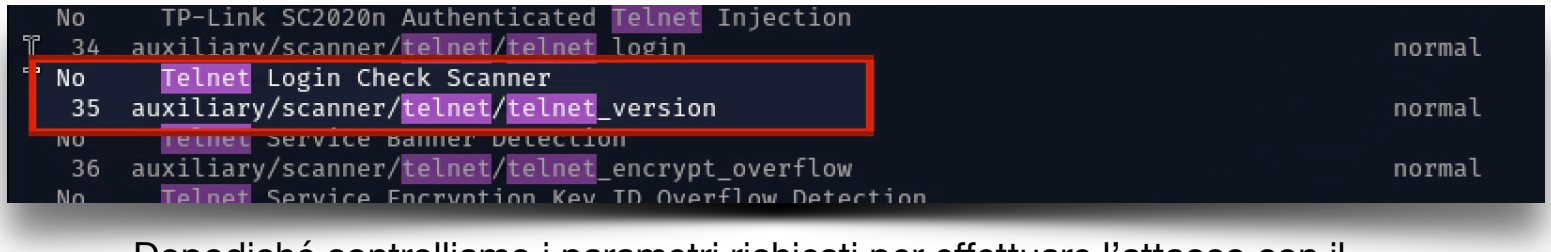


2 Exploit Telnet con Metasploit

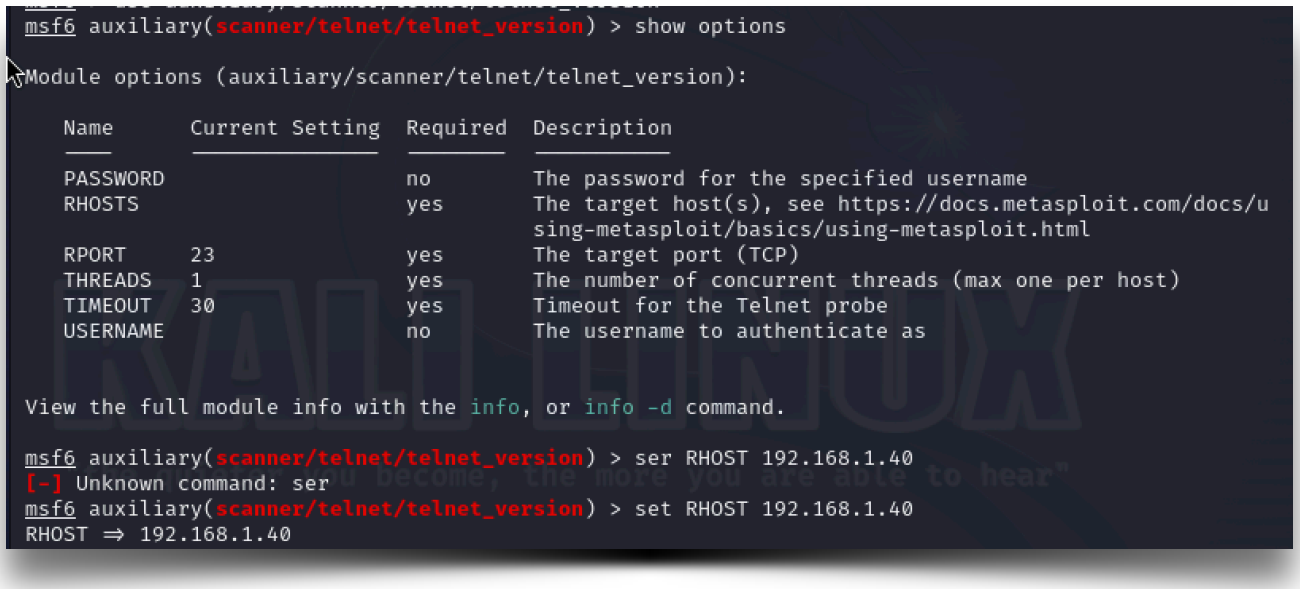
Dopo aver configurato correttamente le macchine passiamo alla fase successiva dell' esercizio, ovvero quella di utilizzare ***Metasploit*** per sfruttare la vulnerabilità relativa al ***Telnet*** con il modulo ***auxiliary telnet_version*** sulla macchina ***Metasploitable***.

Iniziamo con avviare Metasploit tramite il comando ***msfconsole.***
Con il comando ***search telnet*** andiamo a cercare il modulo corretto per il nostro attacco.

Per sfruttare questa vulnerabilità del servizio Telnet, utilizziamo il modulo ausiliario ***auxiliary/scanner/telnet/telnet_version*** che andremo ad utilizzare con la keyword ***use*** davanti.

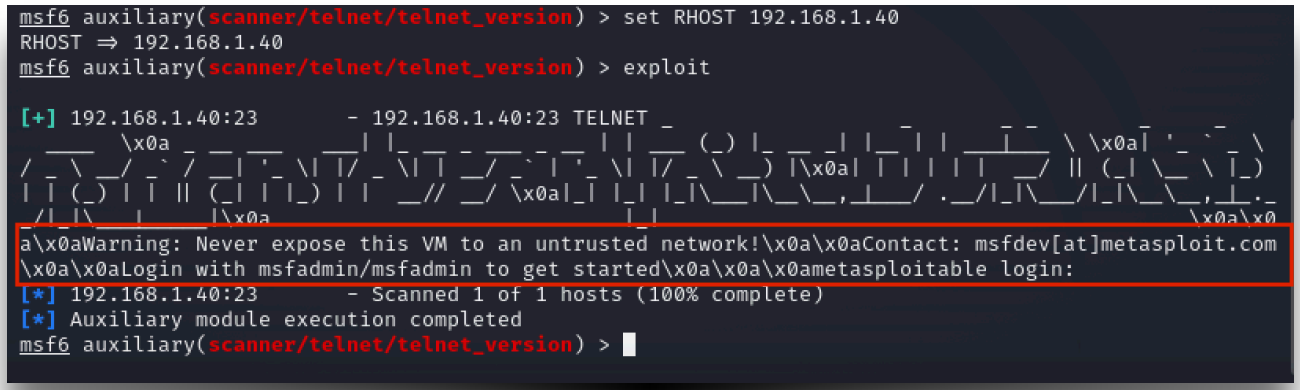


Dopodiché controlliamo i parametri richiesti per effettuare l'attacco con il comando ***show options***.

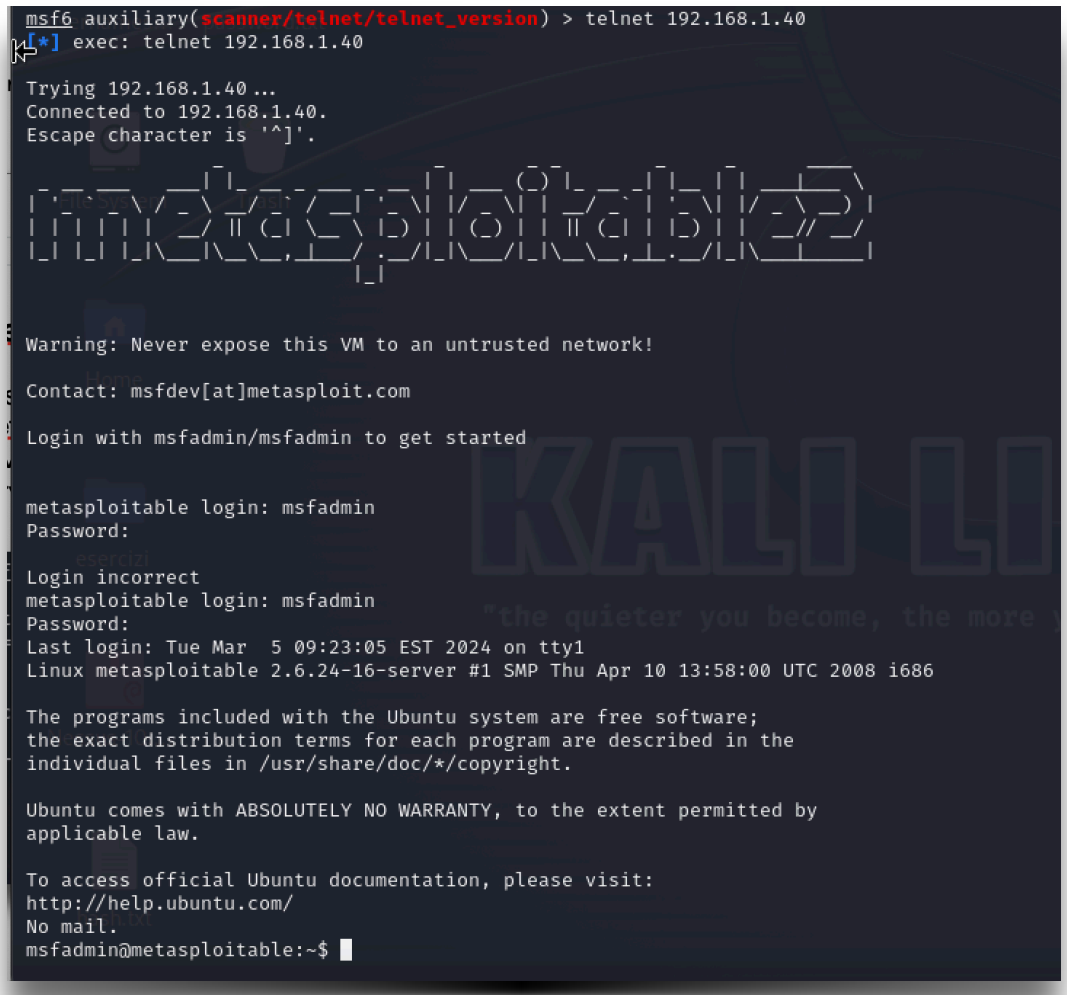


Come possiamo notare ci viene richiesto di inserire il RHOST che andremo a configurare con ***set RHOST 192.168.1.40***.

A questo punto possiamo eseguire l'attacco con il comando ***exploit***



Dai risultati ottenuti notiamo che il modulo è riuscito ad ottenere le credenziali di accesso del servizio, username ***msfadmin*** e password ***msfadmin.***
Facciamo un test per verificare che le informazioni ottenute sono corrette, quindi eseguiamo il comando ***telnet 192.168.1.40.***



Il servizio ci richiede di loggarci, quindi proviamo con le informazioni che ci ha restituito Metasploit, quindi username ***msfadmin***, password ***msfadmin.*** Siamo riusciti ad ottenere l'accesso, in modo non autorizzato, alla macchina Metasploitable. Quindi possiamo dire che l'attacco è andato a buon fine.