Report Esercizio

W16-D2

Redatto da Andrea Sciattella

05/06/2024

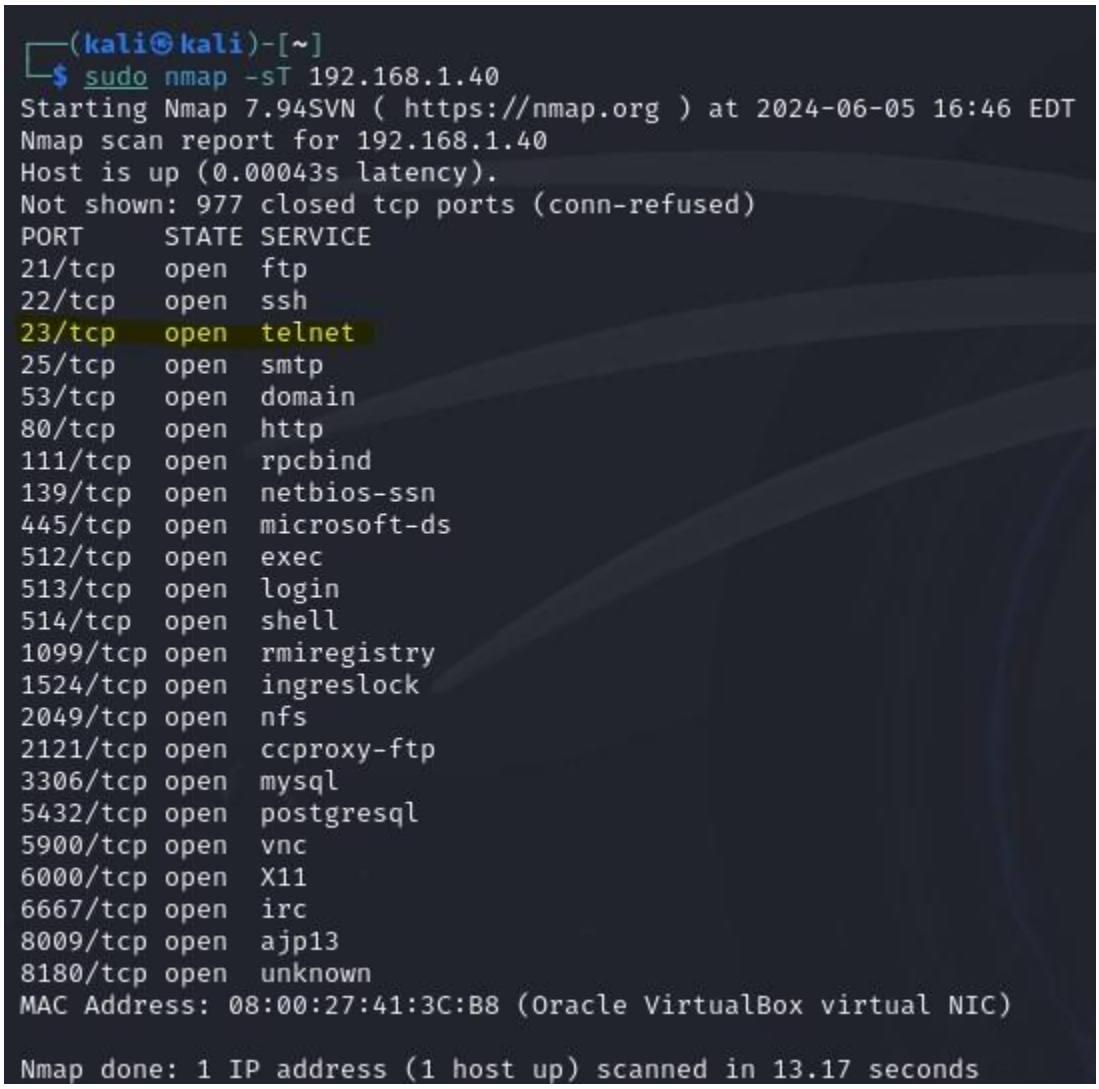
TRACCIA

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

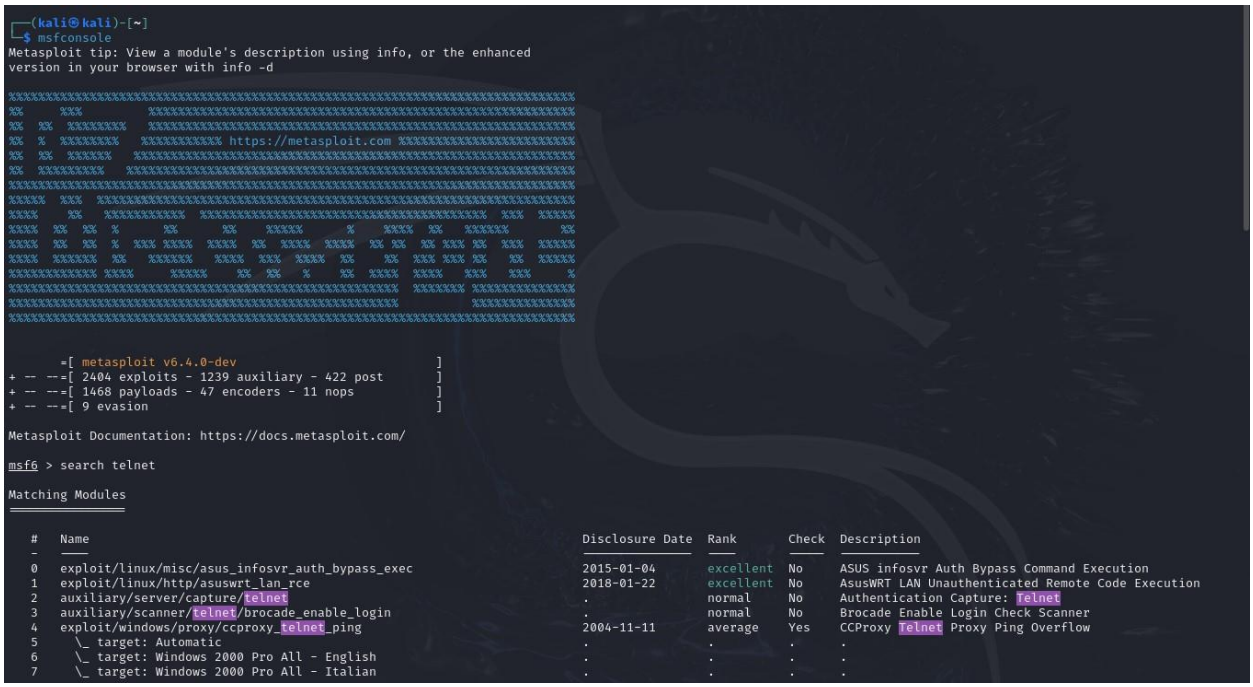
Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'IP della vostra Kali con 192.168.1.25 e l'IP della vostra Metasploitable con 192.168.1.40.

MESSA IN PRATICA ESERCIZIO: EXPLOIT TELNET CON METASPLOIT

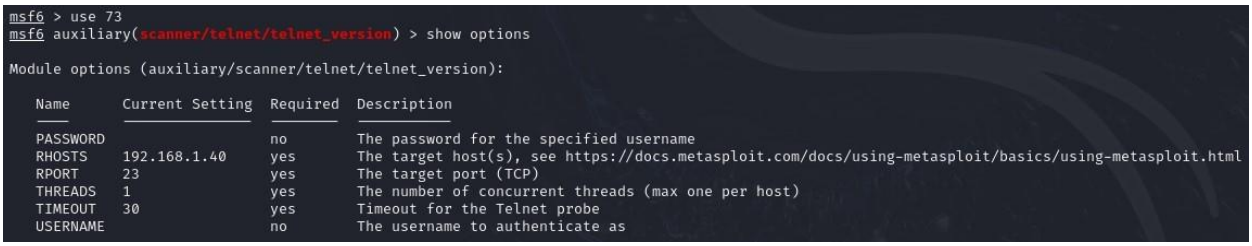
- Configuriamo il laboratorio delle due macchine modificando gli indirizzi IP come richiesto dalla traccia, successivamente verifichiamo la connettività. Ora possiamo procedere con una scansione della macchina per confermare il nostro bersagllio.



- Confermiamo il nostro obiettivo alla porta 23 (servizio ***TELNET***) e proseguiamo accedendo alla console di **metasploit** con "**msfconsole**".



- Abbiamo inserito nel campo di ricerca del framework metasploit "**search telnet**", che darà come risultato qualsiasi modulo che avrà presente nel titolo ***TELNET***, facilitandoci la ricerca.



- Trovato! Useremo il modulo numero 73, "*auxiliary scanner/telnet/telnet_version*", che ci indicherà come continuare. Digitiamo "**use 73**" e una volta apparso nella nostra parte, useremo "**show options**". Nei campi obbligatori andremo inserire le informazioni richieste, come nel nostro caso "**RHOST**" (*Remote Host*).

- Inserito l'host con la nostra macchina target **Metasploitable** (*192.168.1.40*), possiamo andare ad eseguire il nostro modulo con run o exploit.

- "*Auxiliary module execution completed*" significa che la nostra operazione è riuscita ed abbiamo recuperato delle credenziali "**msfadmin/msfadmin**".

- Colleghiamo alla macchina obiettivo con il servizio telnet per provare la veridicità delle credenziali e… **<u>siamo dentro!</u>**