REPORT 06/12/2022

FACCILONGO DOMENICO

EXPLOIT TELNET CON METASPLOIT

TASK

EPICODE — Esercizio Traccia

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

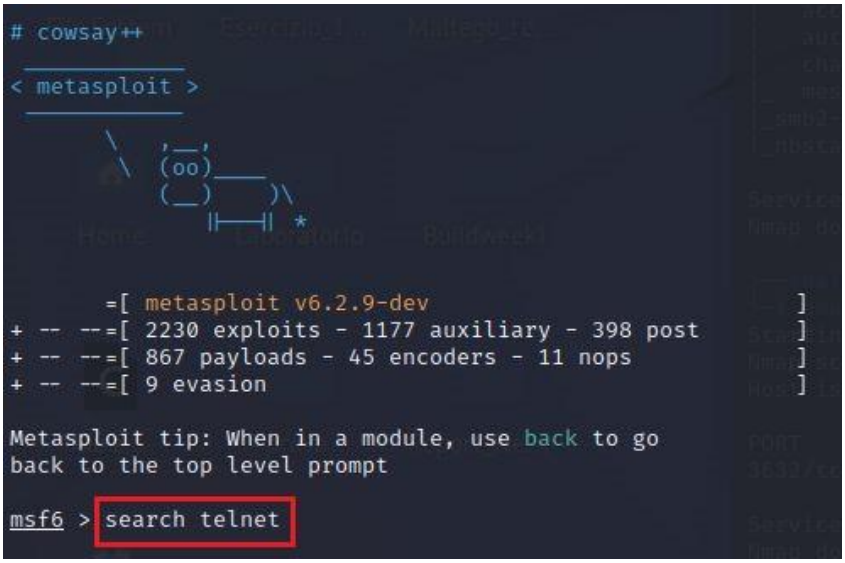
ANALISI E VALUTAZIONI

La prima cosa da fare è la configurazione degli indirizzi IP delle due macchine. Gli IP address di entrambi saranno i seguenti:

MACHINE	IP ADDRESS
Kali	192.168.1.25
Metasploitable	192.168.1.40

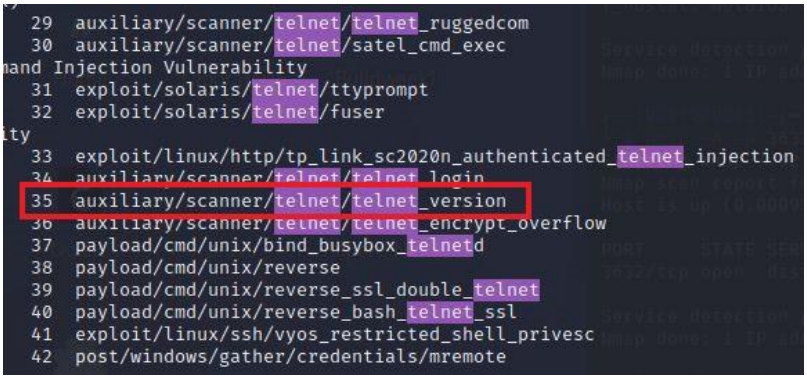
Successivamente avviamo Metasploit con il comando da terminale:

msfconsole



Dopo essere apparsa la schermata di benvenuto andiamo a cercare l'exploit che a noi interessa ovvero telnet della porta 23, quindi immettiamo

search telnet

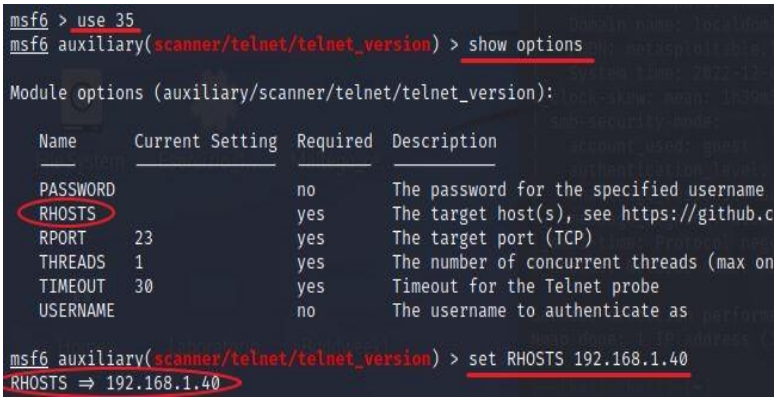


Tra i vari risultati ottenuti scegliamo quello che a noi interessa per sfruttare la vulnerabilità di sniffare la comunicazione e rubare dati sensibili.

Pertanto scegliamo il n.35 come indicato nell'immagine.

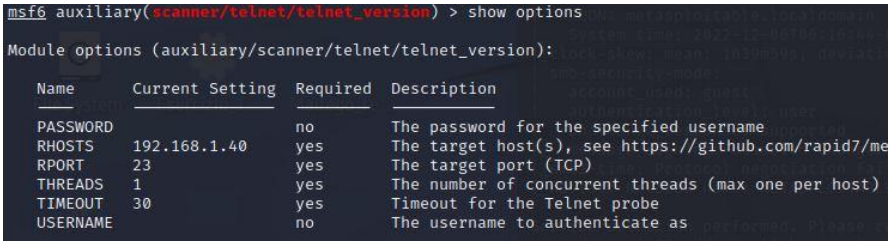
Per selezionare l'exploit utilizziamo il comando

use 35



Successivamente andiamo a visionare l'exploit con il comando "***show options***". Come si può notare abbiamo bisogno di settare l'IP della macchina da attaccare (RHOSTS) e per farlo usiamo il comando "***set RHOSTS 192.168.1.40***". Dopo averlo fatto ci apparirà l'hosts settato (vedi ultimo cerchietto rosso).

Facciamo una verifica per vedere se è stato settato l'host, sempre con il comando "***show options***"



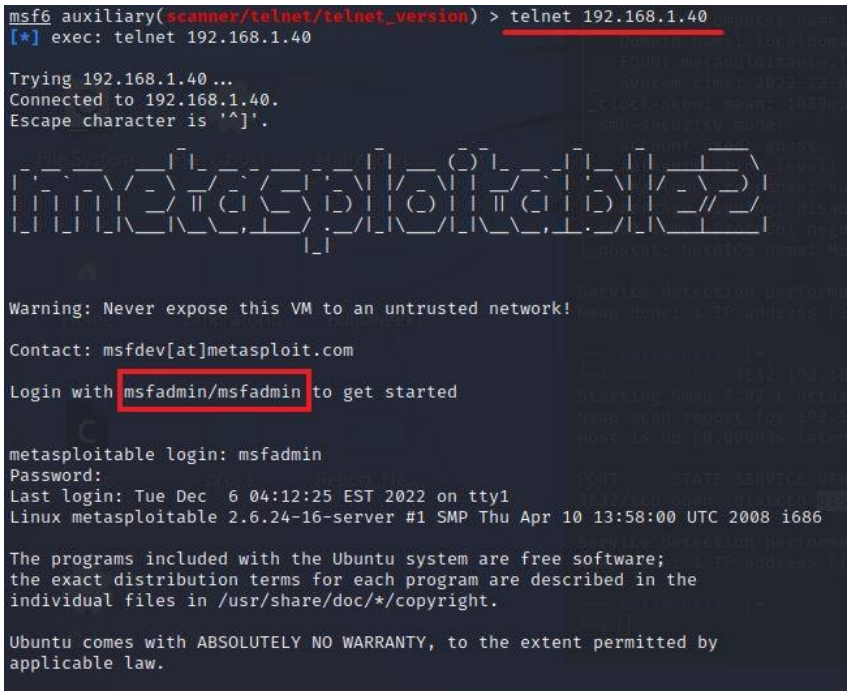
La particolarità è che questo exploit non ha bisogno di un payload quindi possiamo già passare alla fase di exploit.

FASE DI EXPLOIT:

Passiamo alla fase di Exploit con il comando "***exploit***"

Come si può vedere da ultima riga il modulo di esecuzione è stato completato correttamente. Pertanto non ci resta che aprire la connessione con il comando

telnet 192.168.1.40



La connessione è stata instaurata e come si può vedere dall'immagine la grafica è proprio la stessa di meta e ci fornisce infatti anche user e password.

Possiamo fare un ultimo test per vedere se abbiamo i privilegi da root con il comando

Id