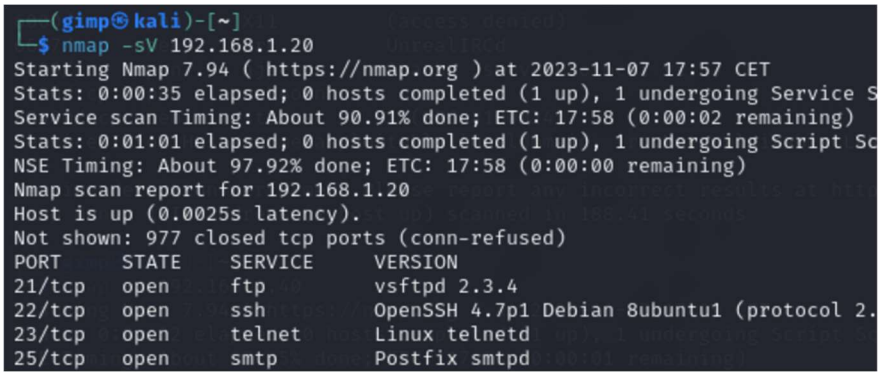
Esercizio S7-L2

Un exploit è un codice malevolo che agisce su una vulnerabilità già presente nel sistema, che essa sia nota o non nota.

L'obiettivo di oggi era sfruttare una vulnerabilità del protocollo telnet. Con la corretta esecuzione potremmo prendere il controllo della macchina vittima.

Dopo aver confermato la corretta connessione usando il ping, ho eseguito una scansione nmap per assicurarmi che la porta telnet fosse la 23 e che versione ci fosse.

L'ip corretto è 192.168.1.40, questo screen è frutto di un test precedente).



Poi ho aperto msfconsole:

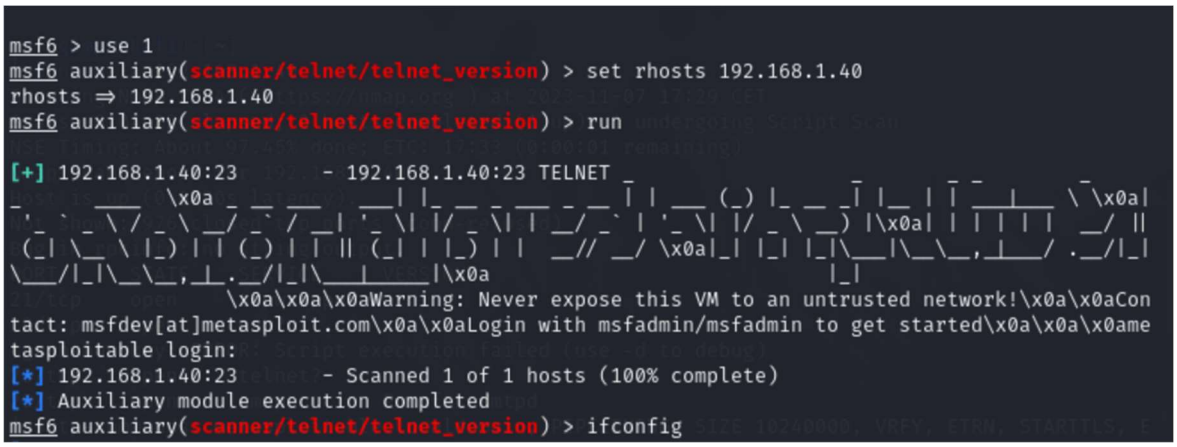
-search auxiliary telnet_version

-use “”

-show options

-set rhosts 192.168.1.40

-run



È possibile vedere che vengono fornite le credenziali di accesso a metasploitable.

Avviando il protocollo telnet 192.168.1.40 connettendolo al’ip vittima si potrà agire sul sistema vittima da remoto.