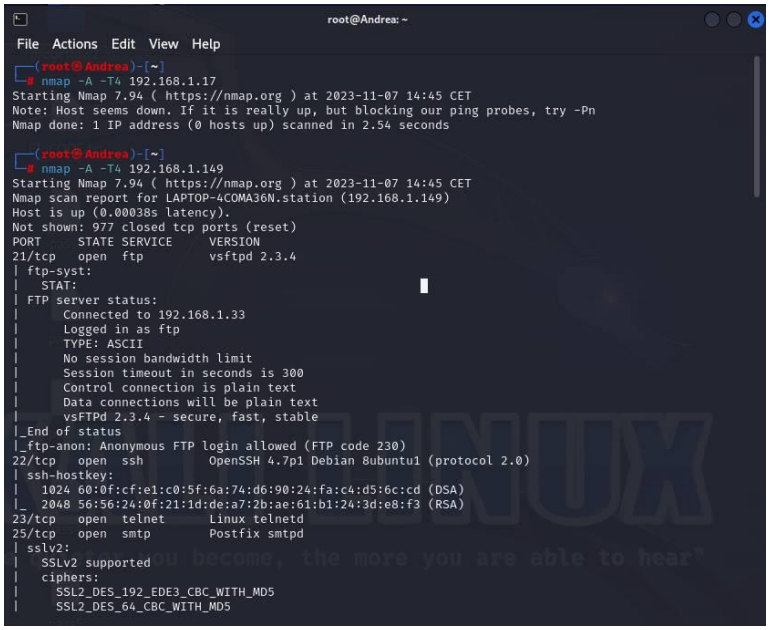
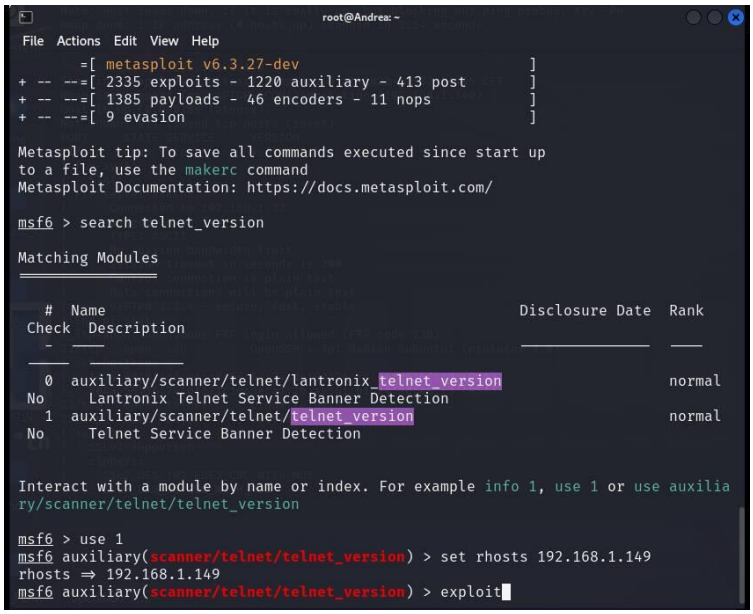
Esercizio 2 Settimana 7

Metasploit Telnet

Oggi andremo ad utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet sulla macchina Metasploitable. Il servizio Telnet è in ascolto sulla porta 23 ed è relativo alla connessione remota tra host di una rete (ormai sostituito con i protocolli SSH più sicuri).
Iniziamo con la scansione aggressiva della macchina vittima per andare a vedere se la porta è effettivamente aperta dopodiché apriamo Metasploit su Kali con il comando *'msfconsole'*.

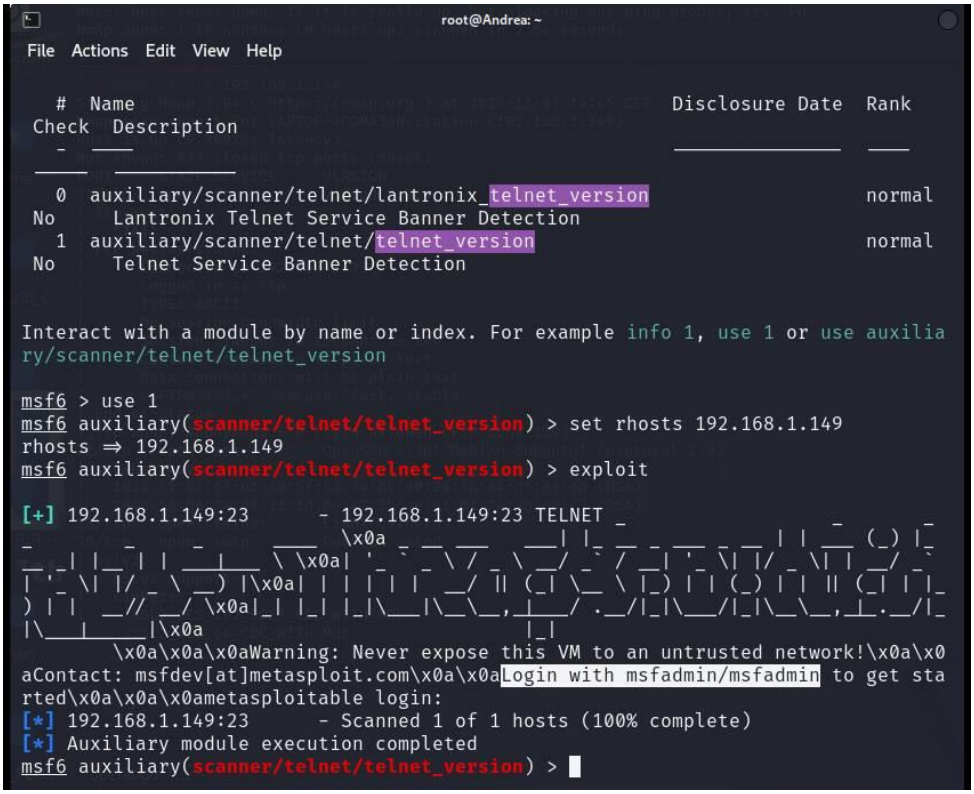


A questo punto andiamo a cercare l'exploit con il comando *'search + parametri di ricerca'* e con *'use 1'* selezioniamo il numero dell'exploit (si può inserire anche il path) che vogliamo utilizzare. Non serve altro se non settare nel modo corretto le impostazioni inerente all'host tramite *'set rhosts 192.168.1.149'*.



.

Con il comando *'exploit'* andiamo ad eseguirlo e Metasploit andrà a cercare user e password della macchina vittima fino a fare il login.



L'exploit è una tecnica o codice malevolo che permette di sfruttare una vulnerabilità di un determinato sistema o dispositivo informatico per poterne prendere possesso. Inoltre, a differenza dei malware, non hanno bisogno dell'azione diretta dell'utente essendoci la vulnerabilità intrinseca nella macchina vittima.