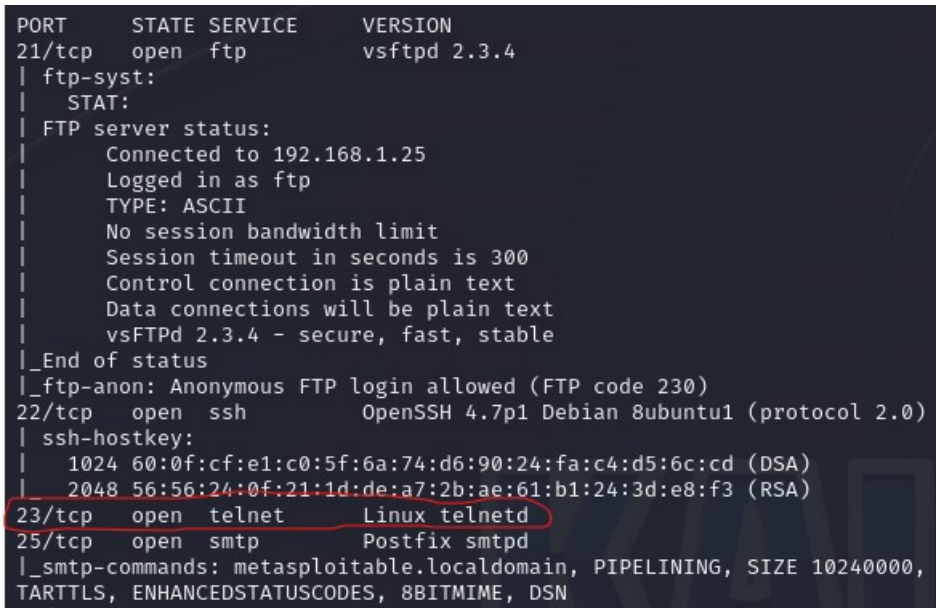
Report Telnet exploit

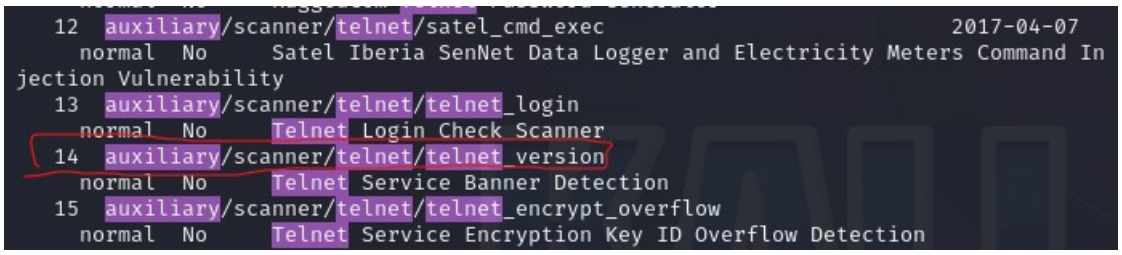
Nell'esercizio di oggi dobbiamo sfruttare il protocollo Telnet per un exploit su Metasploitable.

Un exploit è un tipo di codice malevolo che sfrutta una vulnerabilità già presente in un sistema.
Lo scopo di un exploit è penetrare un sistema target per rubare dati, caricare codice malevolo, creare una connessione (shell) su un dispositivo target in modo da potervi accedere liberamente. Possiamo creare due tipi di shell: bind shell (la connessione ha direzione attaccante > taget) o reverse shell (direzione target > attaccante). La reverse shell è molto più comune, in quanto evita il problema di un eventuale stateful firewall (che blocca i pacchetti in ingresso, ma non quelli in uscita).

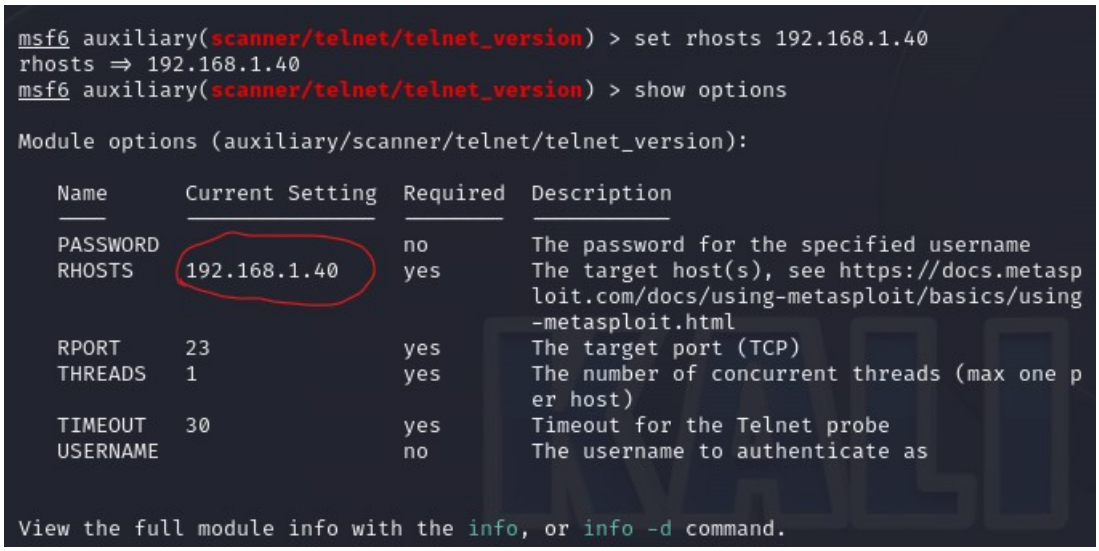
Iniziamo facendo una scansione dell'indirizzo IP target con Nmap per verificare che il servizio Telnet sia effettivamente attivo su Metasploitable. Usiamo una scansione aggressiva, che ci da più informazioni possibile. Vediamo che il servizio Telnet è abilitato sulla porta standard numero 23.
Telnet è un protocollo usato per la connssione da remoto; non è un protocollo che usa crittografia, quindi è già di per se vulnerabile. Inoltre, per quanto la porta 23 sia quella standard, è buona pratica spostare Telnet su una porta con numero superiore alla 1023 (le “well known ports”), per dare meno riferimenti ad un eventuale attaccante.



Ora apriamo Metasploit e cerchiamo i possibili exploit che possiamo usare contro il protocollo Telnet.
Troviamo il modulo ausiliario che ci serve; i moduli ausiliari sono moduli di supporto che forniscono maggiori informazioni sulla rete target, normalmente non portano payload e non sono quindi usati per attacchi diretti.
Nell'immagine sotto troviamo il modulo che ci serve, l'auxiliary telnet version.



Impostiamo l'indirizzo IP target, necessario per far funzionare l'exploit. Vediamo tra l'altro che questo exploit non richiede payload.



Possiamo quindi procedere con l'exploit. Vediamo che con questa particolare scansione abbiamo ottenuto lo username e la password del sistema target.