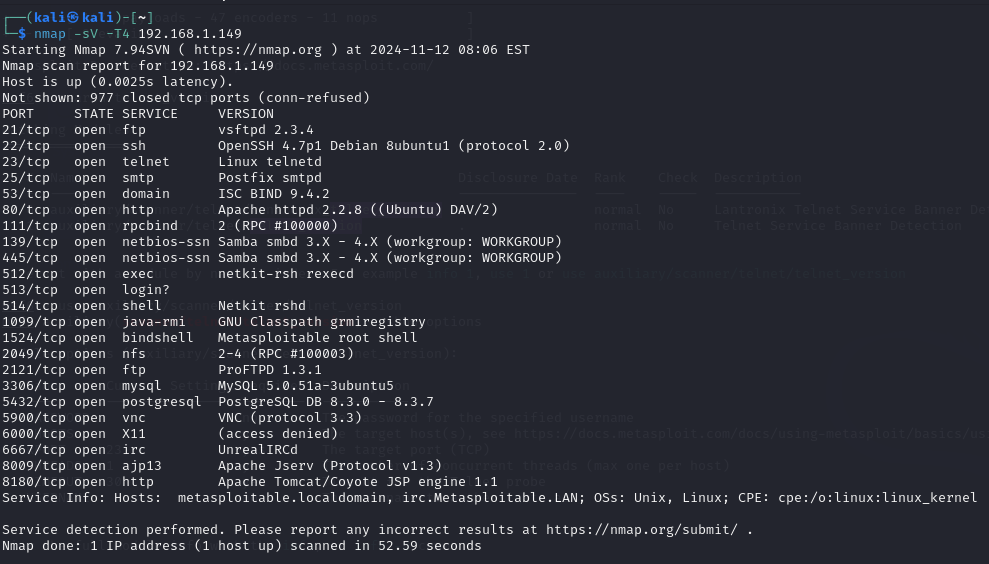
**PRATICA 12 NOVEMBRE 2024**

**Exploit Telnet con Metasploit**

Oggi andremo ad exploitare il protocollo telnet utilizzando il modulo auxiliary telnet\_version sulla macchina vittima Metaspoitable2

**NMAP**

Come prassi andremo ad utilizzare nmap per scansionare la vittima  


Possiamo vedere che la porta 23 telnet è vulnerabile perché i driver non sono aggiornati all’ultima versione.

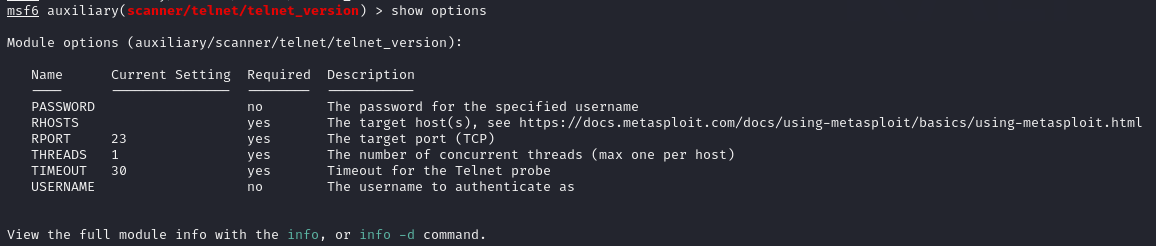
**UTILIZZO DI METASPLOIT**

Una volta scelta la porta da attaccare, andremo a selezionare il modulo auxiliary da utilizzare:  
  

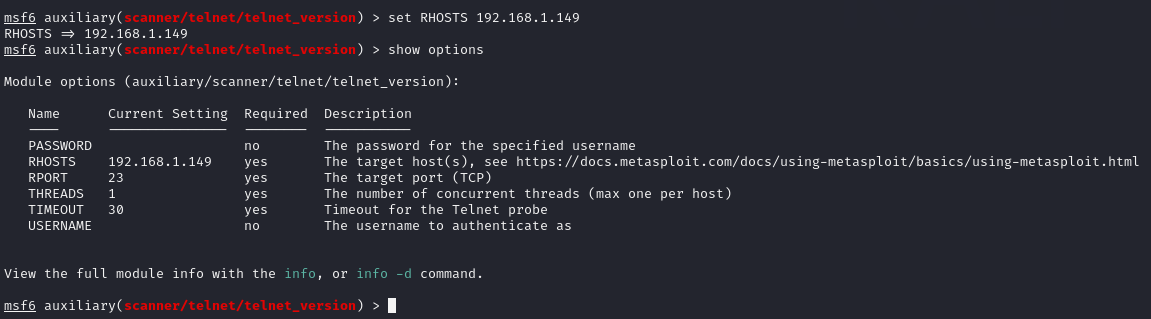

Per il nostro attacco utilizzeremo il modulo **auxiliary/scanner/telnet/telnet\_version.**

Procediamo utilizzando il comando **use** seguito dal path selezionato:

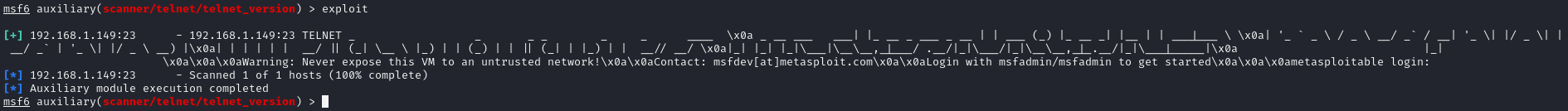


Continuiamo con **show options** per controllare i parametri standard:  


Possiamo vedere che l’opzione RHOSTS manca di indirizzo IP. Utilizzeremo il comando **set** per aggiungere l’indirizzo IP della macchina vittima:



Una volta settato l’indirizzo IP riproviamo con il comando **show options** per confermare l’avvenuto abbinamento tra RHOST e indirizzo IP.

Concludiamo il test utilizzando il comando exploit per vedere se l’attacco andrà a buon fine:  
  
  
  
Possiamo vedere che grazie a questo exploit siamo riusciti a recuperare username e password della macchina vittima tramite attacco a dizionario, riuscendo dunque ad accedere da remoto al dispositivo designato.