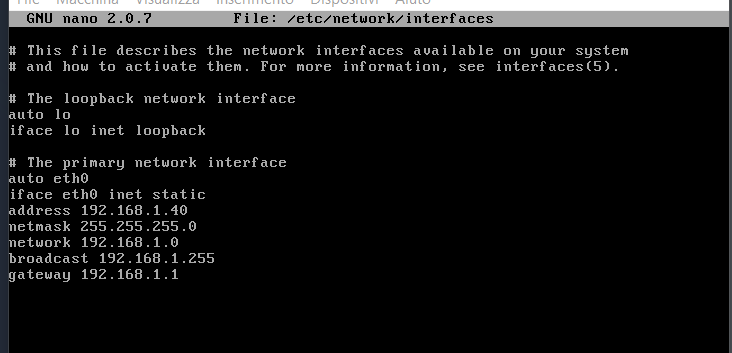
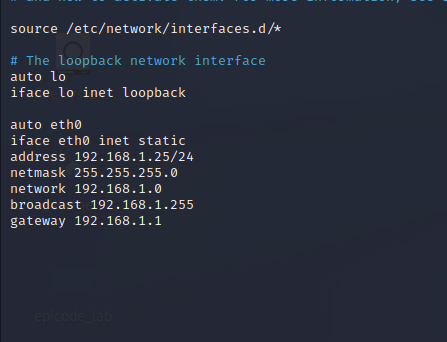
REPORT EXPLOIT TELNET- METASPLOITABLE

La macchina Metasploitable presenta un servizio Telnet su porta 23, che trasferisce il traffico su canale non cifrato, dando la possibilità ad un utente malintenzionato di rubare informazioni sensibili quali username, password e comandi scambiati tra client e server.

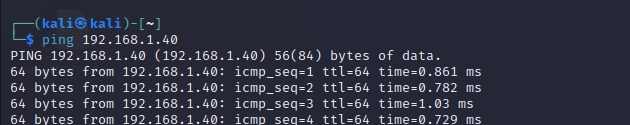
In questo caso specifico, verrà sfruttata proprio questa vulnerabilità dal tool Metasploit. Cambiamo gli indirizzi IP di entrambe le macchine:

192.168.1.40 per Metasploitable

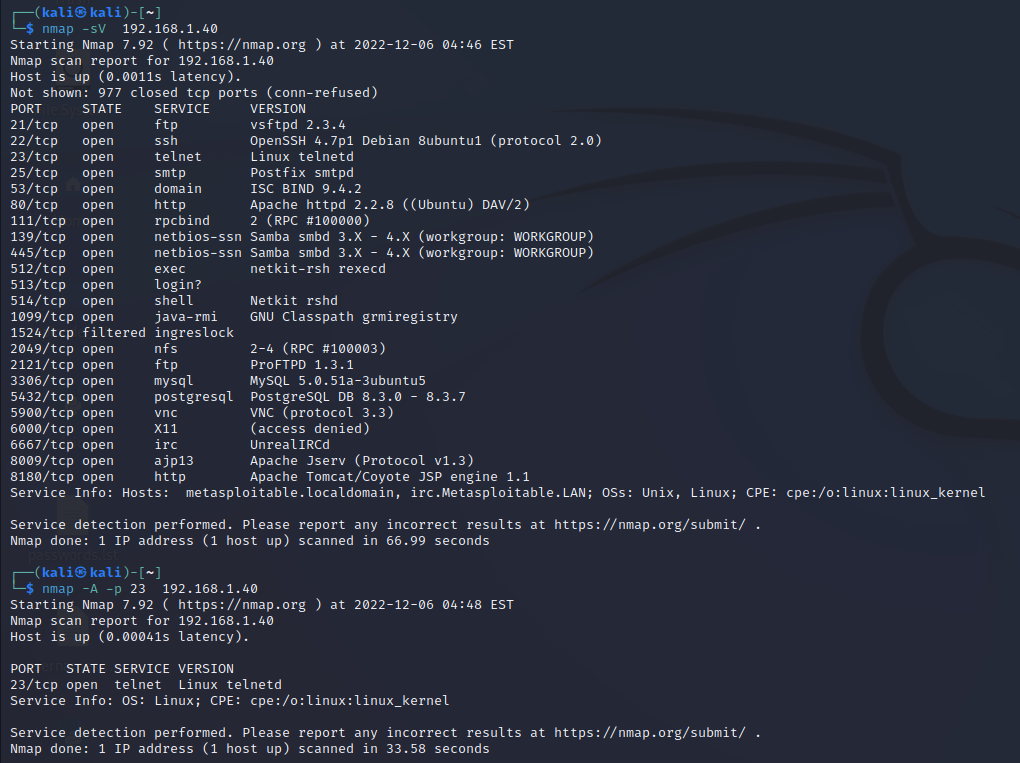
192.168.1.25 per Kali Linux



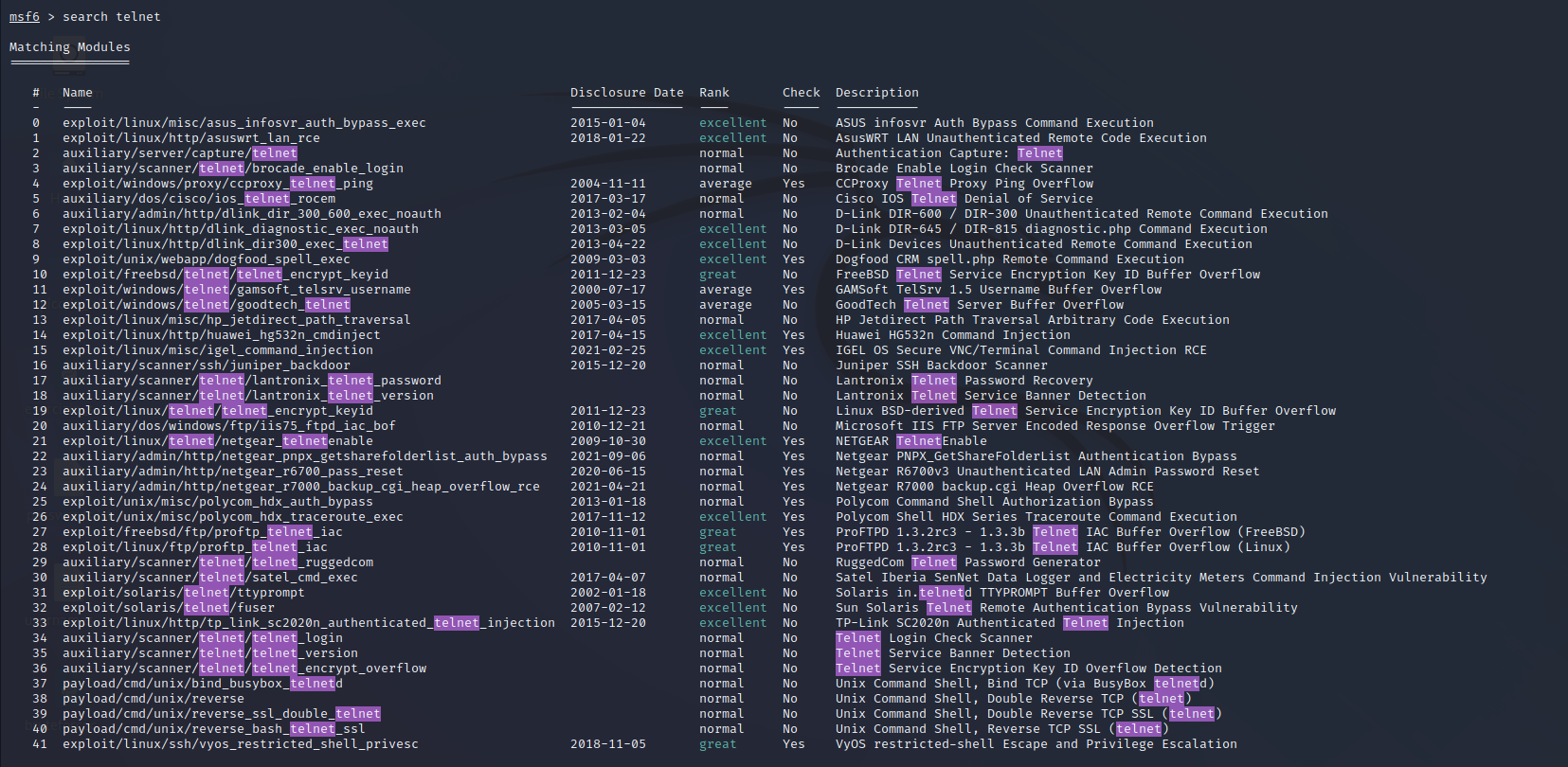
Necessario sarà testare la connessione tra le macchine tramite ping



Tramite uno scan con tool Nmap controlliamo i servizi attivi sulle porte dell’indirizzo target ed in seguito, se ne effettuerà uno specifico per la porta d’interesse in questo caso la porta numero 23

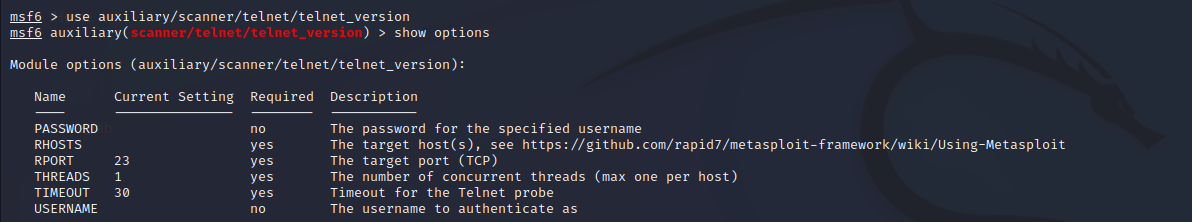


A questo punto apriamo Metasploit tramite msfconsole, cercando il modulo di exploit ausiliario richiesto, in questo caso auxiliary/scanner/telnet/telnet\_version

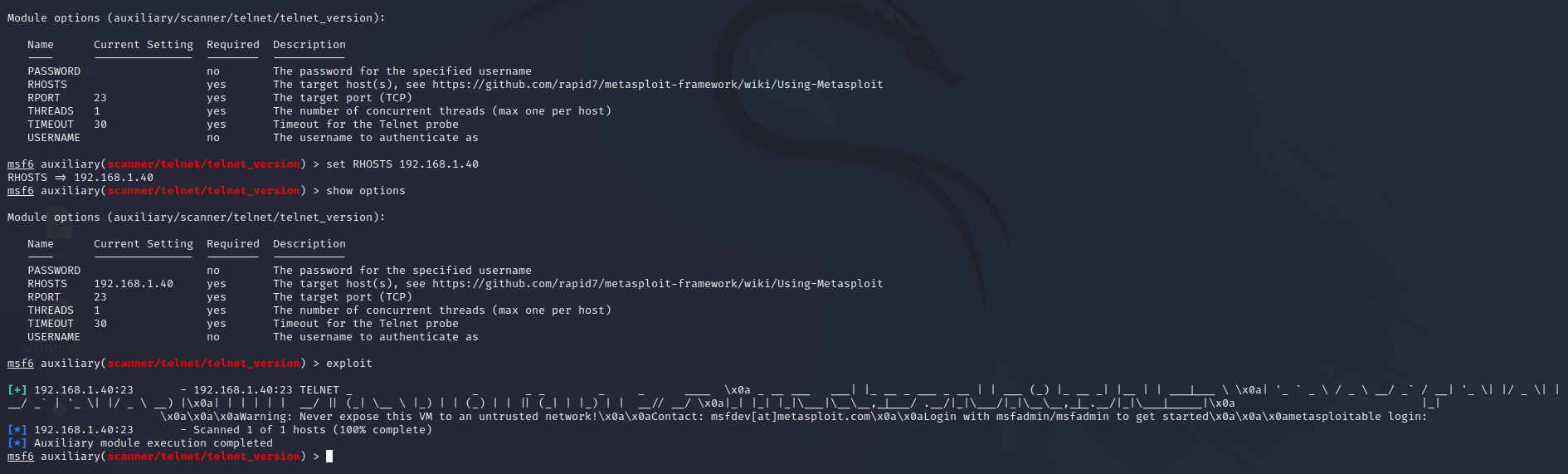


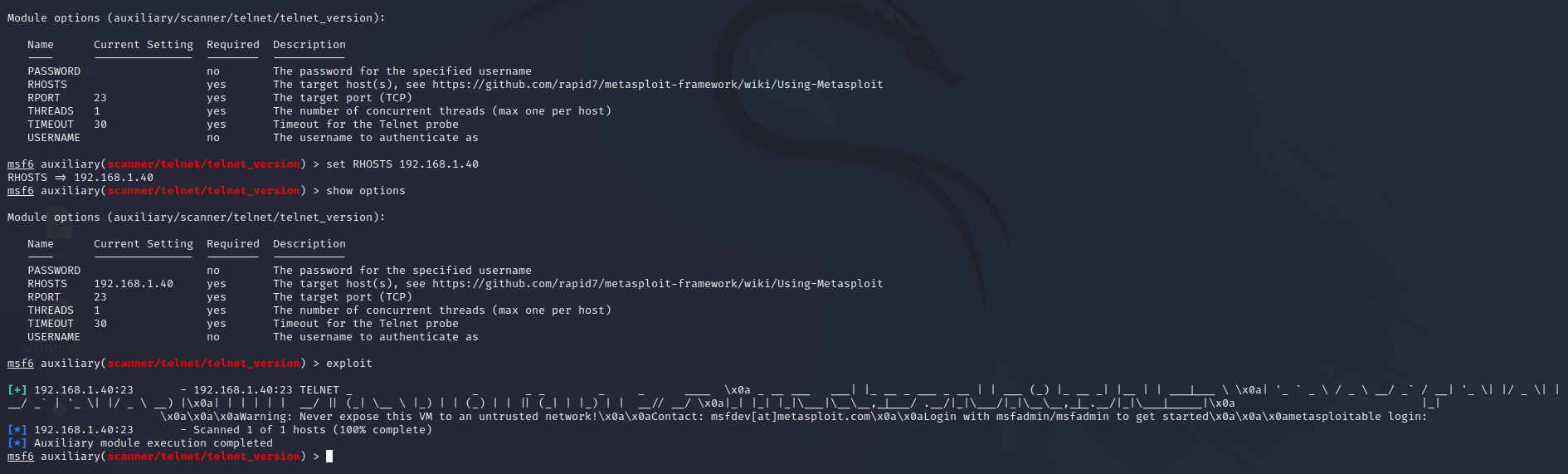
L’exploit necessario in questo caso sarà al numero 35 dell’elenco .

Opportuno sarà il controllo dei parametri da settare con ‘show options’, e completiamo i campi ‘required’ ossia obbligatori.



Una volta settate inserendo l’Ip di Metasploitable, procediamo con comando ‘exploit’



 Sarà stato possibile ottenere username/password per login di Metasploitable.

Inoltre, sempre importante e necessario effettuare un test per assicurarsi che l’exploit sia andato a segno e/o per completarlo.