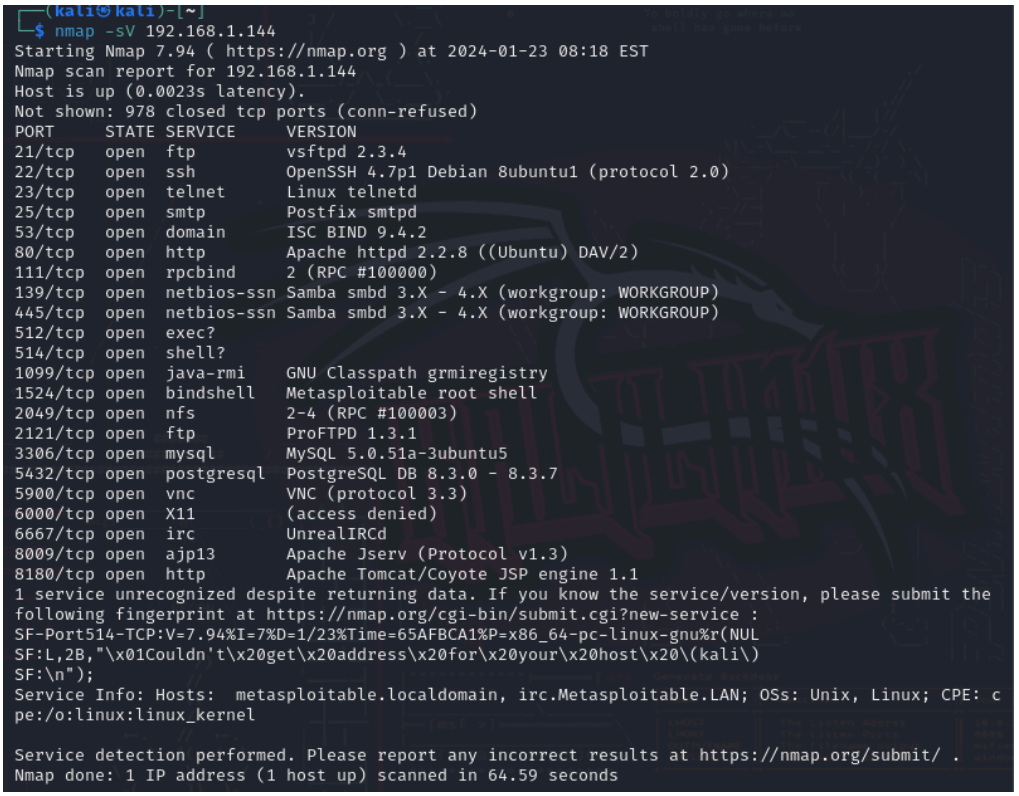
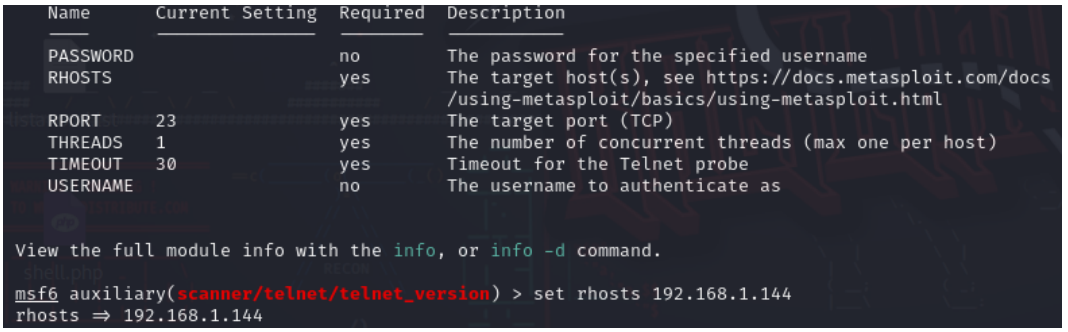
Partiamo utilizzando nmap per fare una scansione dei servizi attivi con tanto di versioni del nostro target




una volta individuato il servizio al quale andremo ad applicare l'exploit, in questo caso telnet, passiamo ad utilizzare metasploit per trovare tutti gli exploit presenti in quel servizio


scelto l'exploit che andremo ad applicare passiamo alla configurazione, impostando i dati necessari come l'IP del target



per concludere diamo il via a l'exploit il quale come possiamo vedere ci dà con successo le credenziali di accesso (msfadmin/msfadmin)