S7 L2

Davide Andreozzi

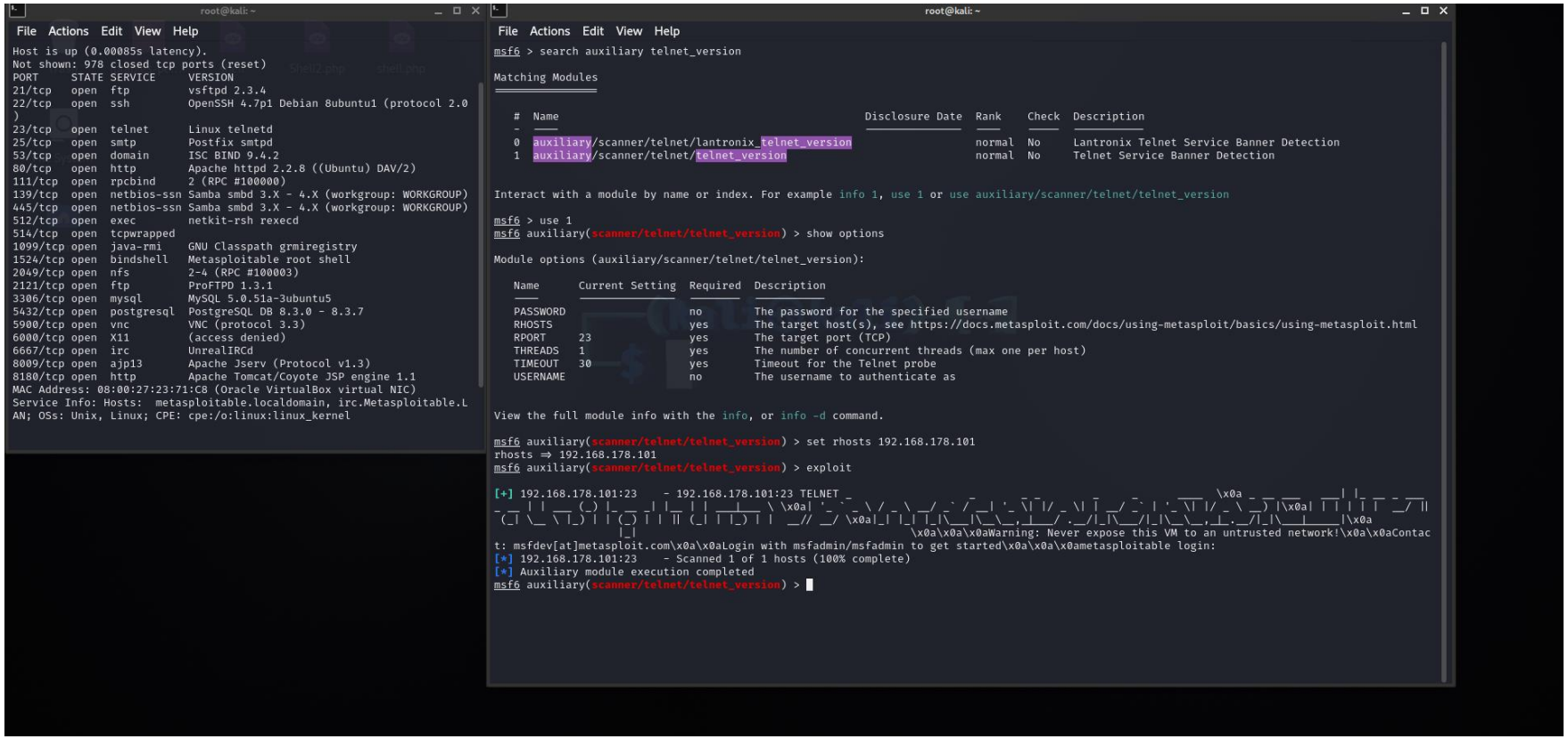
Andiamo ad utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

1- Scansioniamo l'ip target tramite nmap e vediamo il servizio attivo sulla porta 23

2- Avviamo Metasploit e cerchiamo il modulo ausiliario che ci serve tramite il comando «search auxiliary telnet_version», diamo invio e utilizziamo il #1 (use 1)

3- Settiamo il modulo, in particolare *rhosts* con l'ip target su cui eseguire l'exploit

4- Tramite il comando «exploit» avviamo l'exploit e analizziamo l'output, in particolare la riga «login with msfadmin/msfadmin» che ci va a indicare user e password per il login per telnet



Testiamo la connessione con le credenziali exploitate da Metasploit.
1- Tramite riga di comando ci colleghiamo con telnet sulla macchina target e inseriamo le credenziali che ci ha dato l'output di Metasploit (Screen 1).
2- Una volta entrati vediamo che tramite il comando *ifconfig* ci restituisce l'ip della macchina bersaglio (Screen 2).