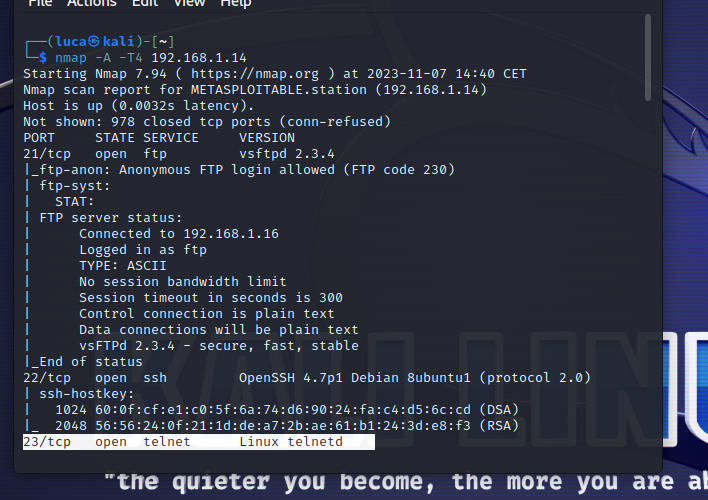
Metasploit con modo auxiliary

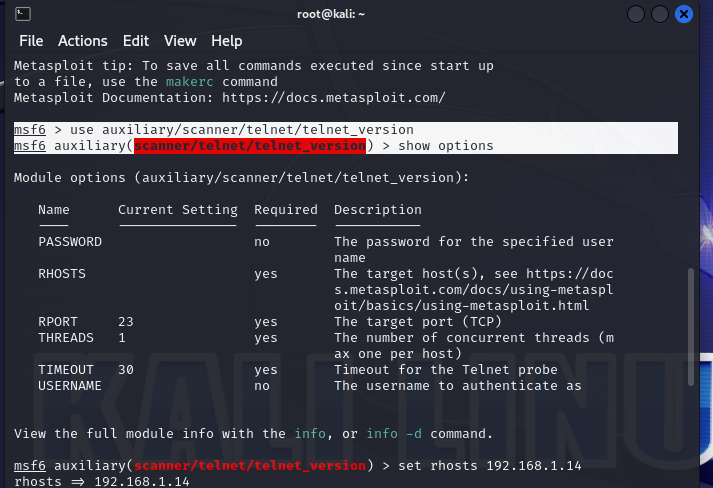
Utilizzando le due macchine Kali (Attaccante) e Metasploitable2 (Vittima) andremo a simulare un exploit con metodo ausiliare grazie a Metasploit.

Premettendo che le due macchine siano connesse tra loro la prima cosa che si andrà a verificare saranno i servizi aperti sulla macchina da exploitare, questo lo faremo grazie a Nmap (Il tipo di scansione sarà usato in base alle esigenze del caso).



Ora che abbiamo verificato che il servizio Telnet (utilizzato per la connessione non criptata tra due macchine) è aperto andiamo ad attivare il programma Metasploit con il comando msfconsole.

Per prima cosa andiamo ad utilizzare il metodo ausiliare di Metasploit utilizzando il comando use auxiliary/scanner/telnet/telnet\_version.



Fatto questo prima di lanciare l’exploit analizziamo i requisiti richiesti nella configurazione del comando (Show options). Notiamo che l’unica richiesta necessaria e non specificata è l’host target (RHOSTS), di conseguenza andiamo a settarlo con il comando set rhosts seguito dal IP target che vogliamo exploitare.

Una volta confermata questa configurazione possiamo lanciare l’exploit con il comando run o exploit, fatto questo riusciamo a scansionare il servizio telnet della macchina vittima e a recuperare le sue credenziali di accesso.