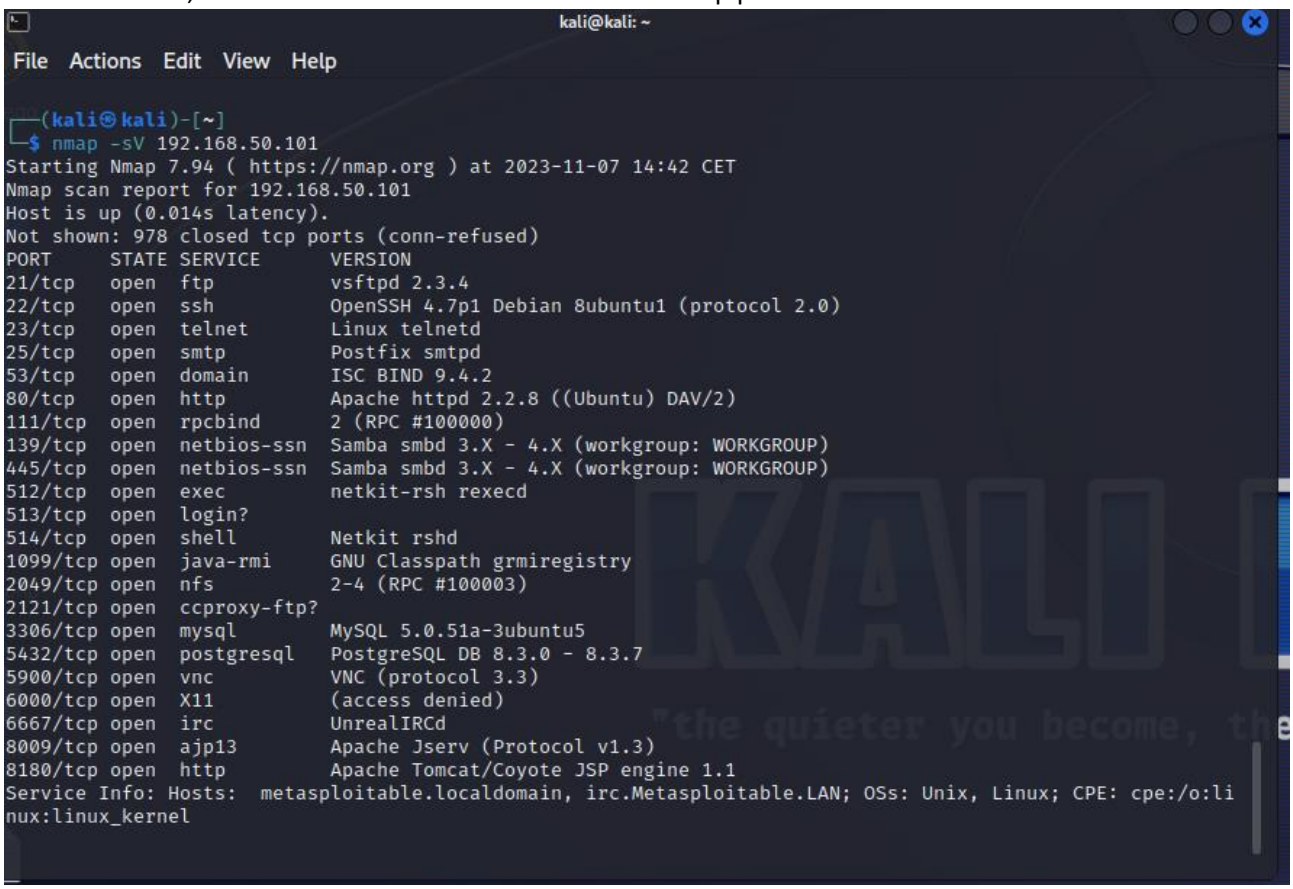
Oggi siamo andati ad exploitare il servizio Telnet di metasploitable.

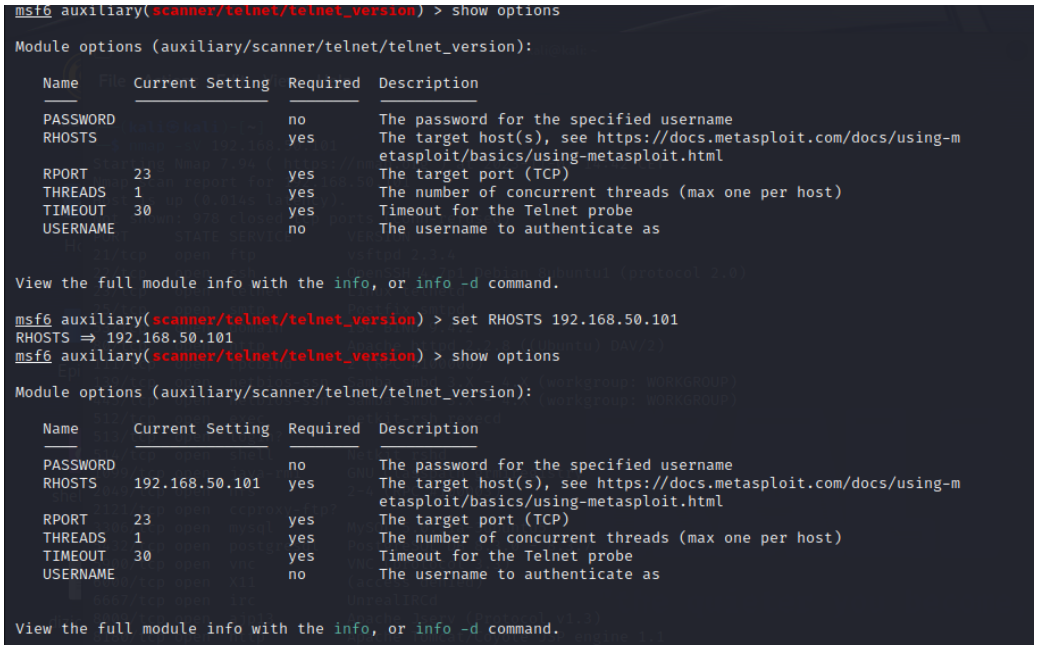
Cosa è un exploit? Gli exploit sono vettori di attacco che vengono utilizzati per sfruttare le vulnerabilità trovate nelle fase precedenti di un pentesting.

Nel nostro caso, abbiamo effettuato una scansione con nmap per vedere i servizi attivi.



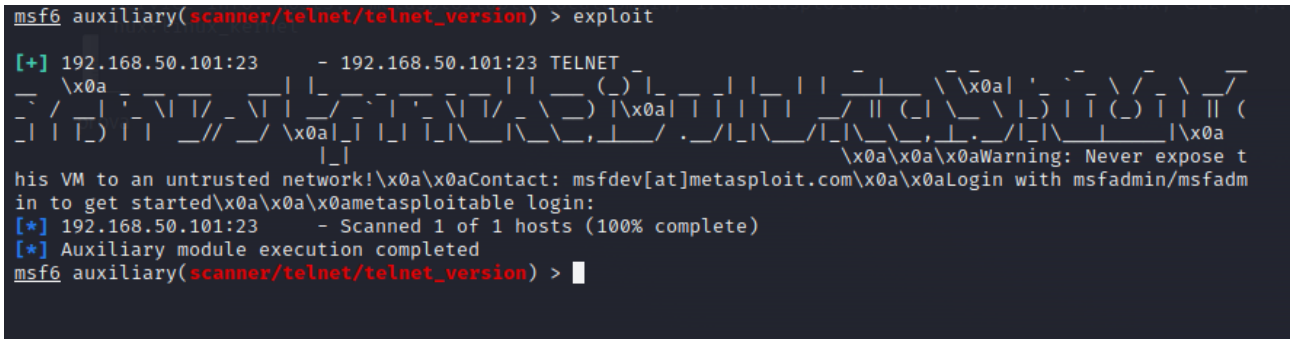
Una volta effettuata la scansione, possiamo notare che sulla porta 23 è attivo il servizio telnet.

Successivamente, usando msfconsole, andremo a configurare il nostro exploit per poi lanciarlo.



Per configurare il nostro exploit, andremo a controllare quali sono i dati necessari e non già presenti, come da screen:

Una volta eseguita la configurazione (qua siamo solo andati a configurare il campo “RHOSTS” inserendo l’ip del nostro Metasploitable) eseguiremo il nostro exploit. Il risultato sarà il seguente:



Come possiamo notare, nel corpo dell’exploit vengono mostrate le credenziali per poter accedere a metasploitable. Consideriamo quindi l’exploit eseguito con successo.