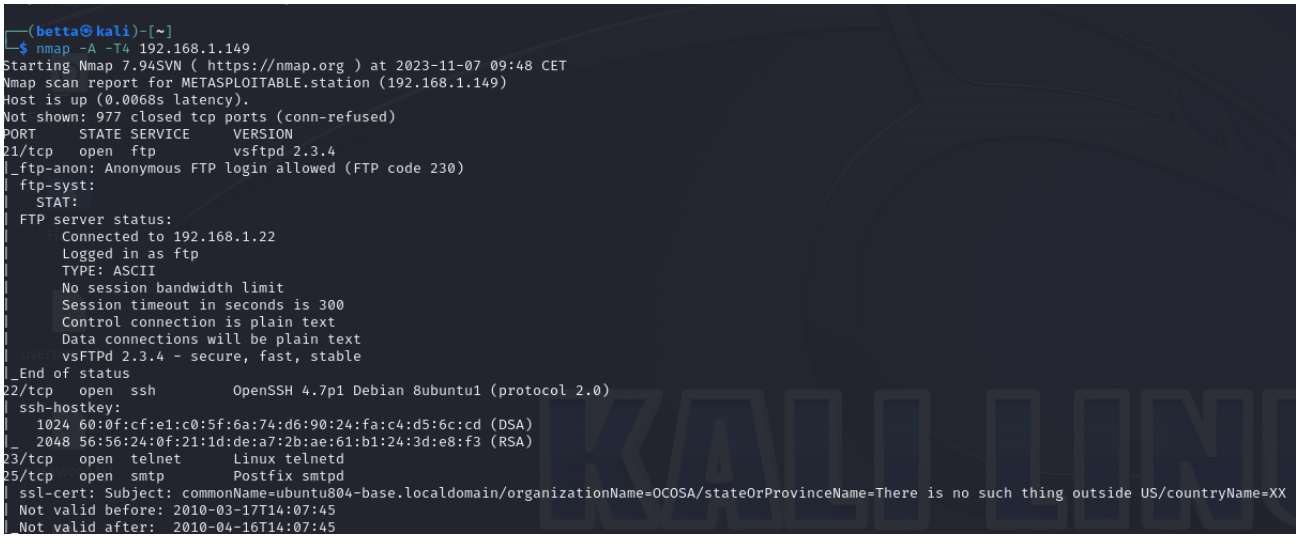
Exploit Telnet con Metasploit

Un **Exploit** è un software o un codice che sfrutta le vulnerabilità di un sistema, applicazione o dispositivo per ottenere accesso non autorizzato o compiere azioni dannosi.

Come primo step verifico se Kali e Metasploitable comunicano. Effettuo un Ping.

Successivamente, con l'aiuto di nmap, faccio una scansione completa con il rilevamento delle versioni abilitato e un timing aggressivo.

Il timing aggressivo non è sempre consigliato in quanto invia pacchetti in modo più rapido e frequente, dunque crea tanto rumore.



Nmap trova i seguenti servizi: FTP, SSH, TELNET, SMTP.

FTP (porta 21) è il protocollo per il trasferimento di file su una rete.

SSH (porta 22) è il protocollo per la connessione sicura e crittografata tra due dispositivi su una rete.

TELNET (23) è il protocollo di rete utilizzato per stabilire una connessione remota a un server/dispositivo da un computer client.

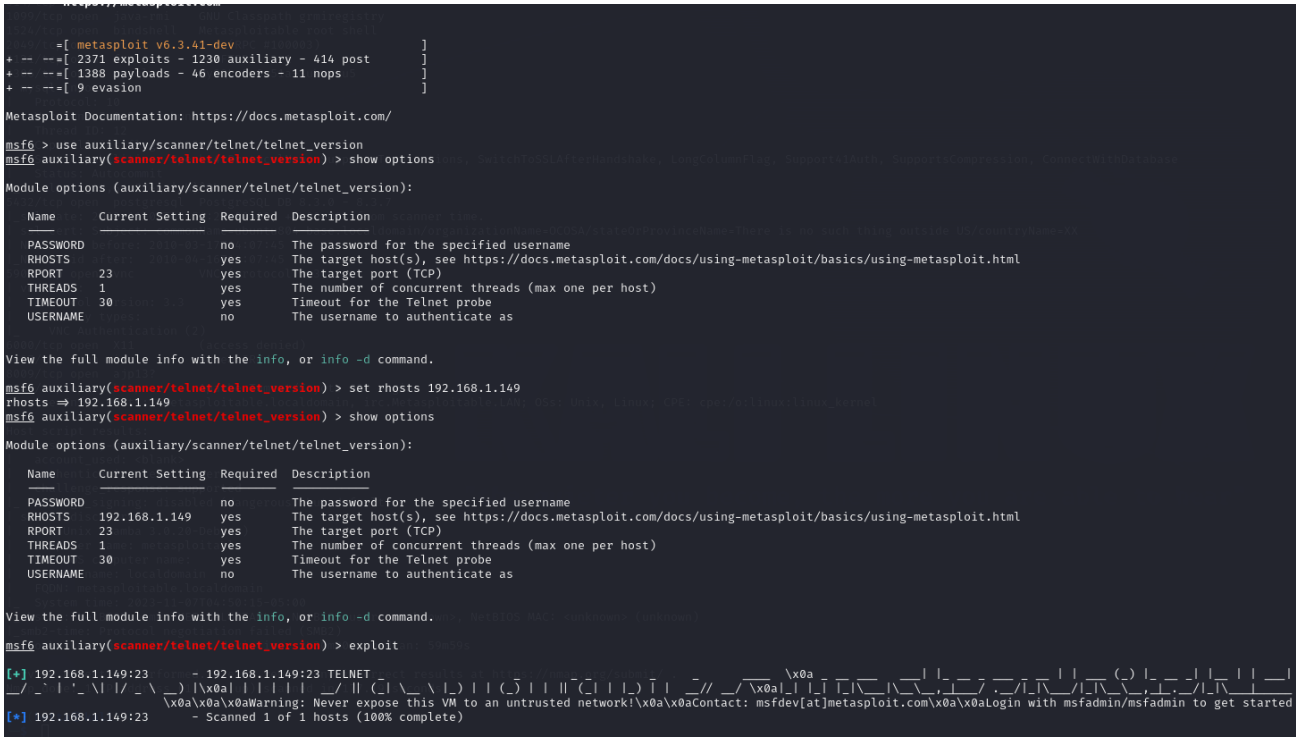
SMTP (25) è il protocollo per inviare mail.

In questo esercizio, andrò a sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version.

I moduli ausiliari forniscono funzioni di supporto per raccogliere informazioni e condurre attività di valutazione della sicurezza, non utilizzano payload a differenza dei metodi normali che lo utilizzano e sono progettati per sfruttare vulnerabilità e fare attacchi diretti.

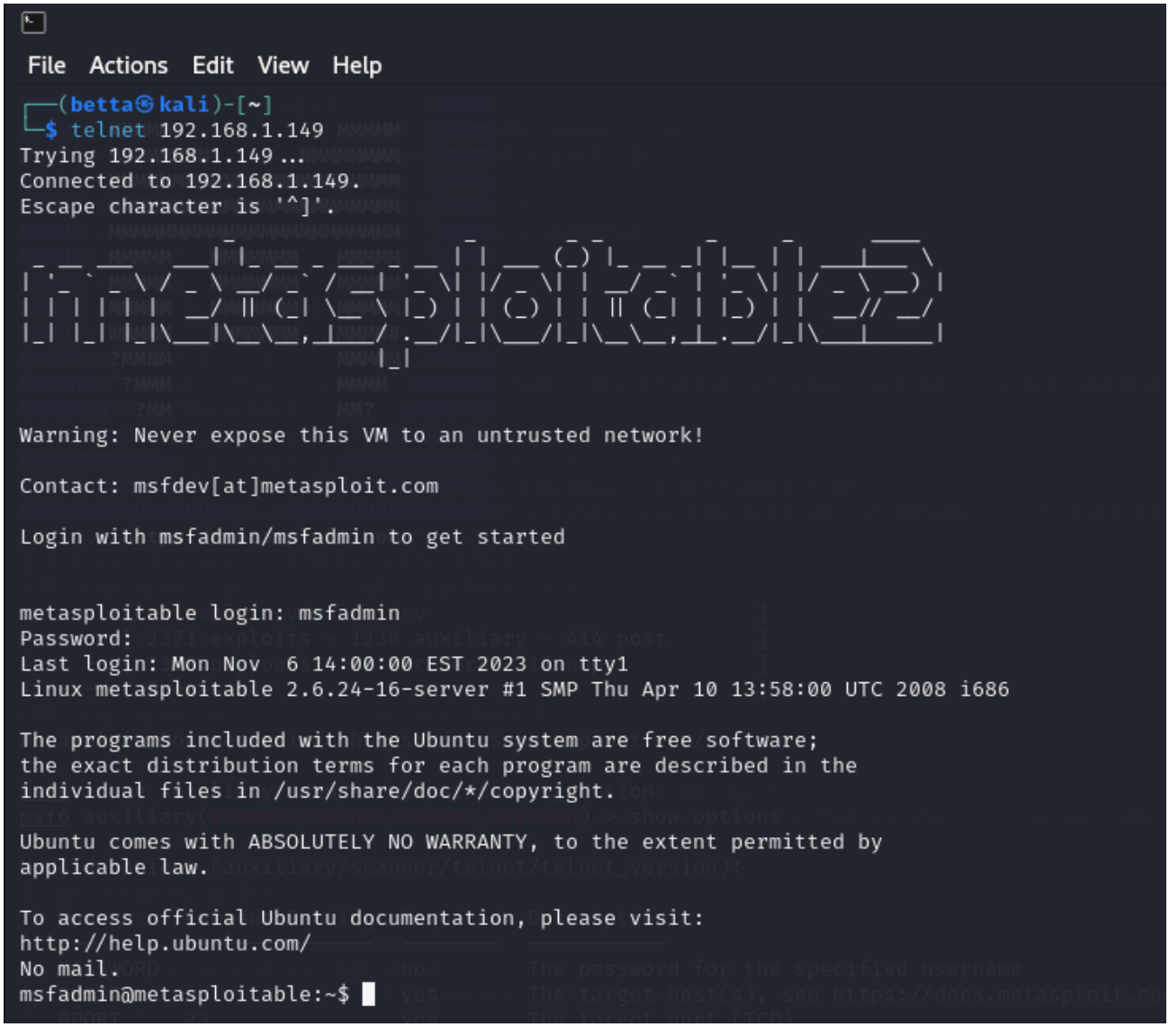
Inizio avviando Metasploit, utilizzo un modulo ausiliare e verifico le opzioni necessarie per lanciare l'attacco. Tra i parametri da specificare, ho bisogno dell'indirizzo RHOSTS, che corrisponde all'indirizzo della macchina vittima in cui è in esecuzione il servizio Telnet. Tutte le altre configurazioni necessarie sono preimpostate per i valori di default.

Setto RHOSTS con l'indirizzo Ip della macchina vittima, effetto un controllo per verificare se la modifica è andata a buon fine e lancio l'exploit.



Il modulo ha estratto con successo le informazioni di accesso per il servizio. Mi sta comunicando che le credenziali da utilizzare sono le seguenti: nome utente "msfadmin" e password "msfadmin".

Per confermare l'accuratezza delle informazioni, procedo con un test. Utilizzo Metasploit per eseguire il comando "telnet" seguito dall'indirizzo IP della macchina Metasploitable. Nell'ambiente di laboratorio, l'indirizzo IP di Metasploitable è 192.168.1.149, pertanto eseguo il comando "telnet 192.168.1.149", proprio come mostrato nell'immagine.



Accesso eseguito correttamente.