EPICODE

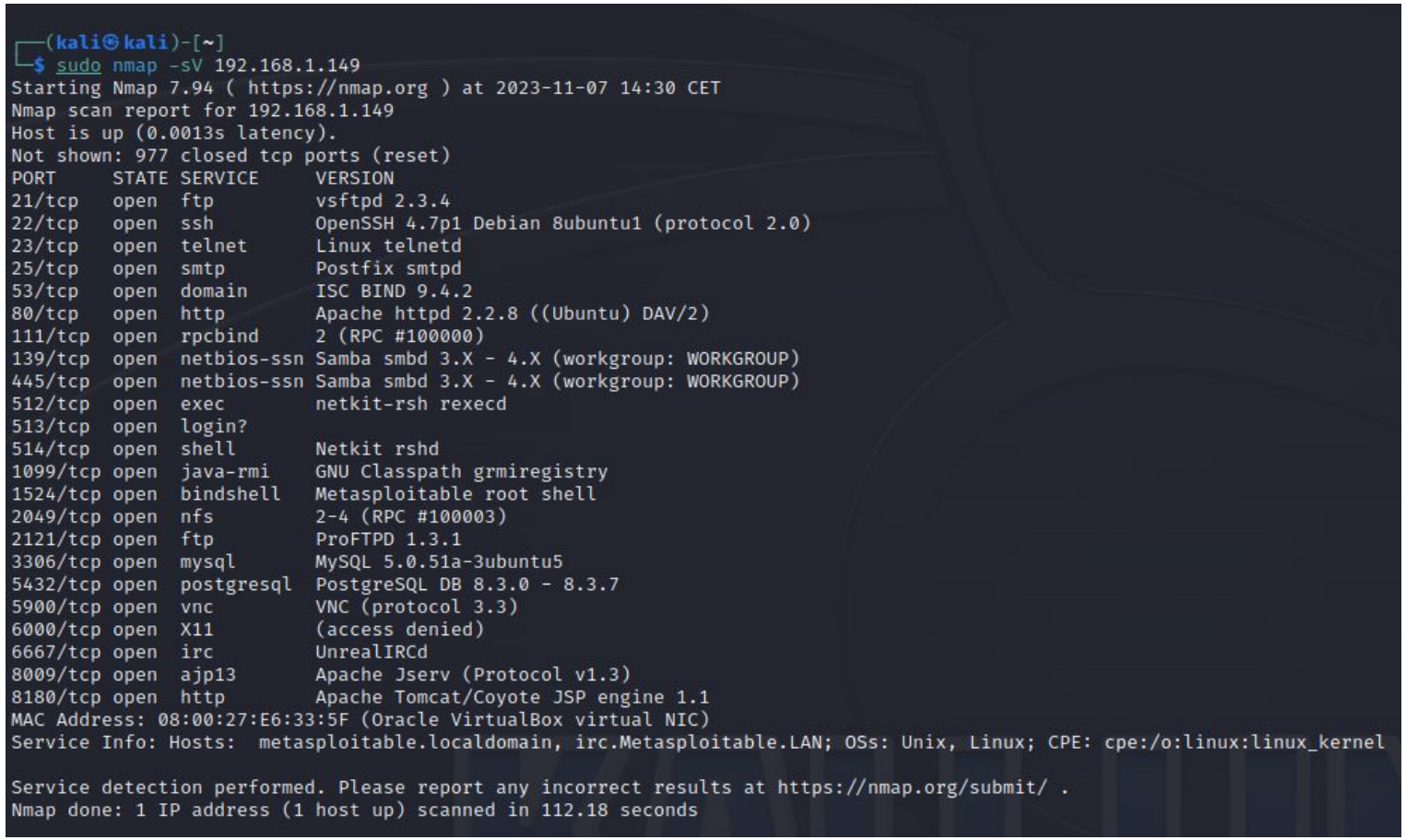
Progetto Alessandro Moscetti 07/11

Che cos’è un exploit?

Un exploit è del codice malevolo che sfrutta una vulnerabilità già presente nel codice, non ha bisogno di installazioni. Sfruttando la vulnerabilità ci permette di creare un varco nella macchina vittima.

Che cos’è il protocollo Telnet?

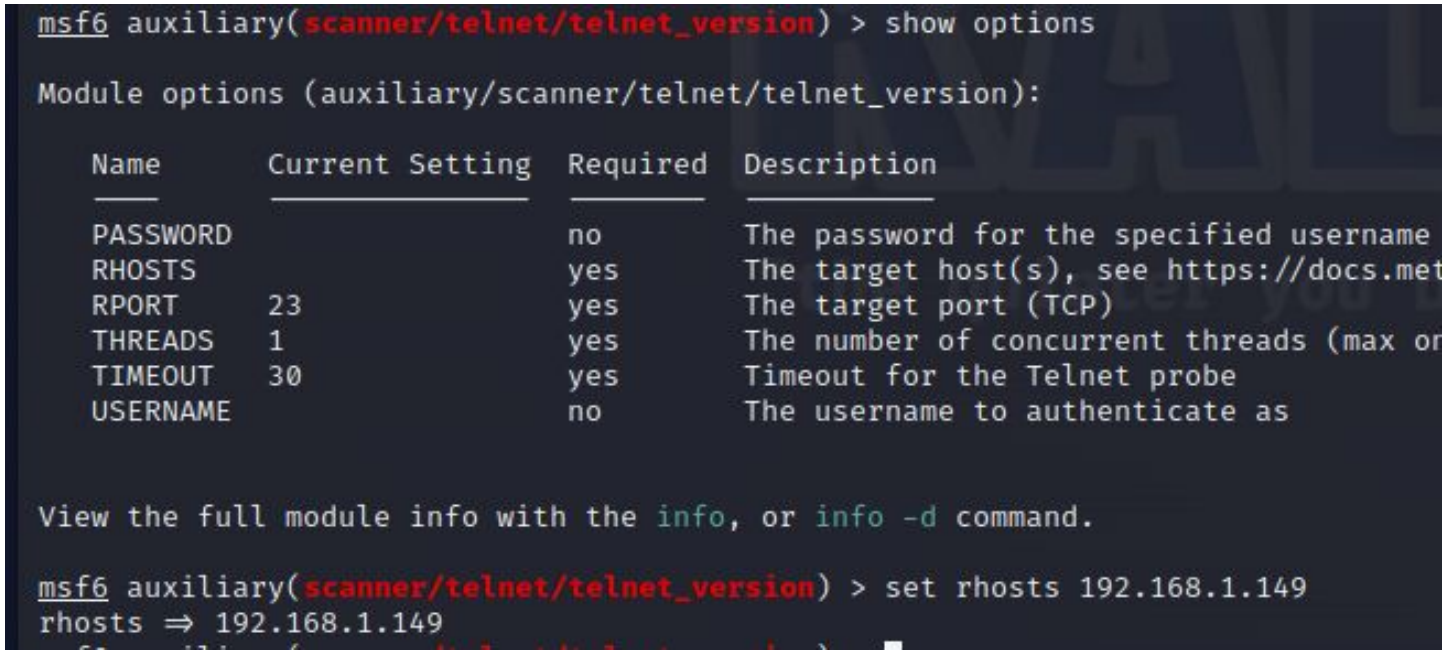
Telnet è un protocollo che consente agli utenti di stabilire una connessione remota verso un altro dispositivo su una rete permettendo agli utenti di controllarlo in remoto.



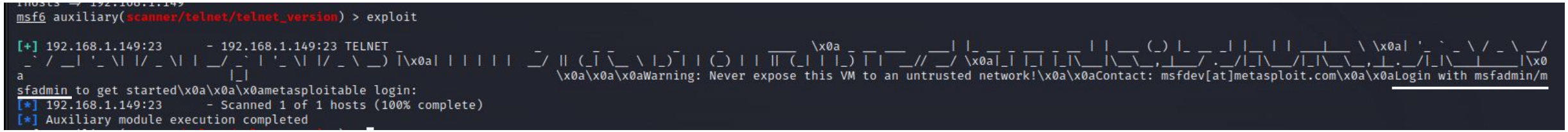
Scansione con nmap verso la macchina Metasploitable per vedere le porte aperte con i relativi servizi e la loro versione.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) >
```

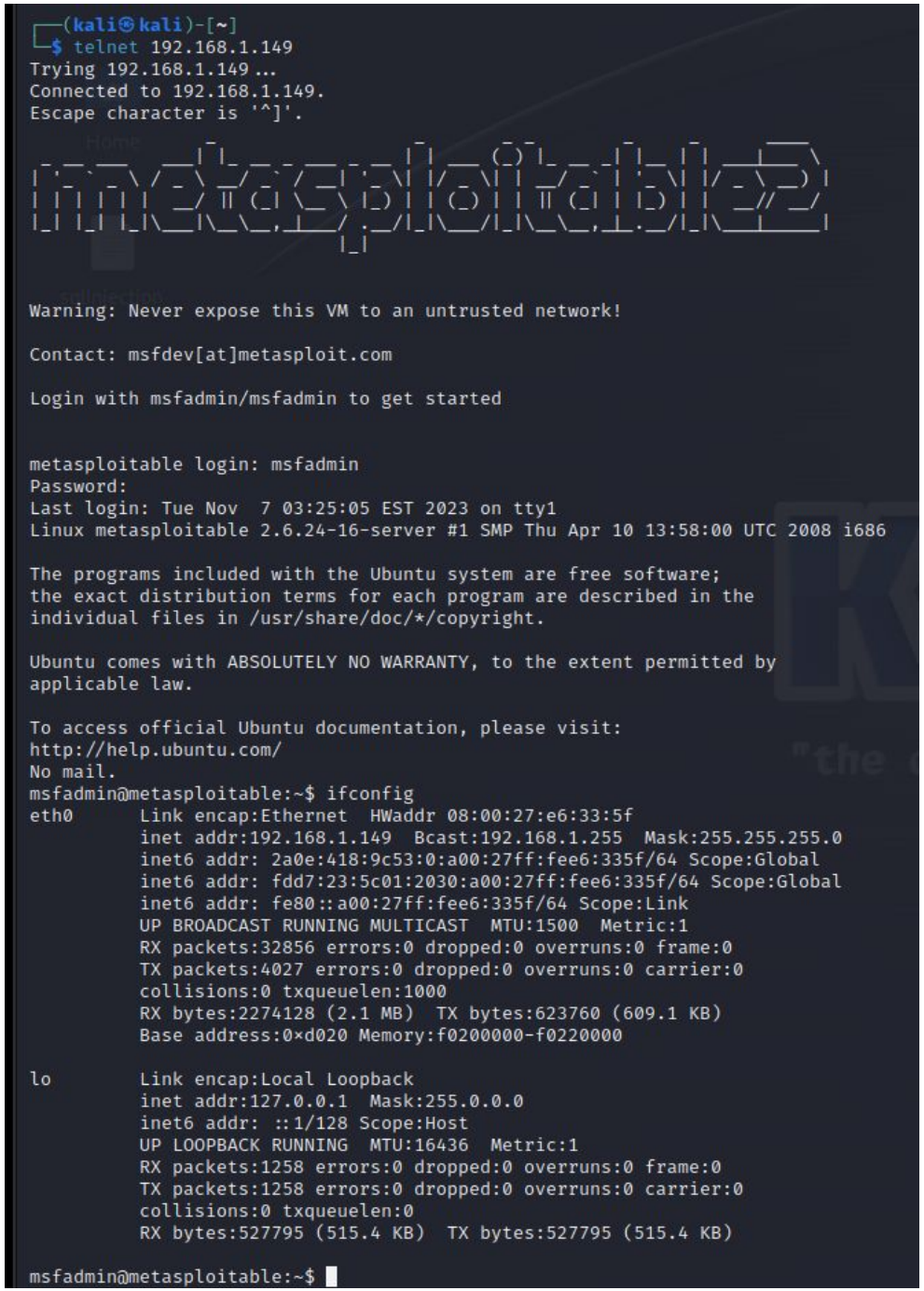
In questo caso avevamo già il modulo da utilizzare, andiamo quindi a selezionarlo tramite il comando ‘use’ seguito dal percorso. Trattandosi di un modulo ausiliario non utilizza il payload.



Con il comando ‘show options’ andiamo a vedere le opzioni, per vedere i parametri necessari per l’exploit.
Si possono notare dalla colonna ‘Required’ dove è presente ‘yes’, in questo caso ‘RHOSTS’ è quello mancante.
Per andare ad aggiungerlo utilizziamo il comando ‘set’ seguito dal nome del parametro mancante e l’informazione.



Andiamo ad eseguire l'attacco tramite il comando 'exploit'. Come possiamo vedere dall'output nell'immagine, il modulo ha recuperato le credenziali d'accesso del servizio.



Per concludere verificare il tutto andiamo a collegarci al servizio tramite il comando ‘telnet’ seguito dall’ip della Metasploitable ed eseguiamo l’accesso con le credenziali trovate in precedenza. Come possiamo vedere dall’immagine è andato a buon fine.

Grazie per l’attenzione.