S7 L2

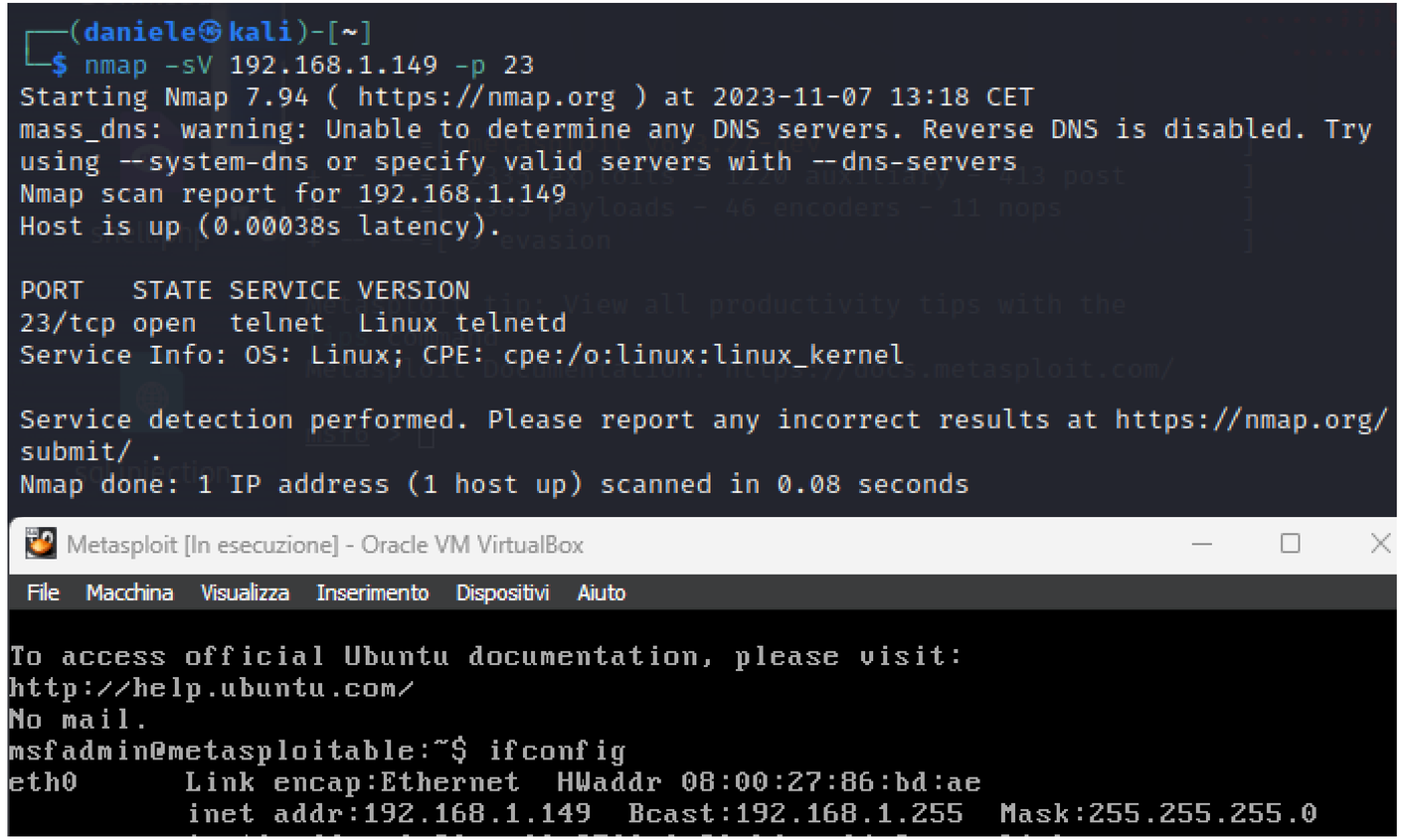
EXPLOIT TELNET META

Daniele Zizzi

EXPLOIT

Un exploit è un programma informatico, un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità per provocare un certo comportamento nel software, nell'hardware o in qualsiasi dispositivo elettronico. Questi comportamenti possono includere l'assunzione del controllo di un sistema, la concessione di privilegi di amministratore a un intruso o l'avvio di attacchi di negazione del servizio (DoS o DDoS)

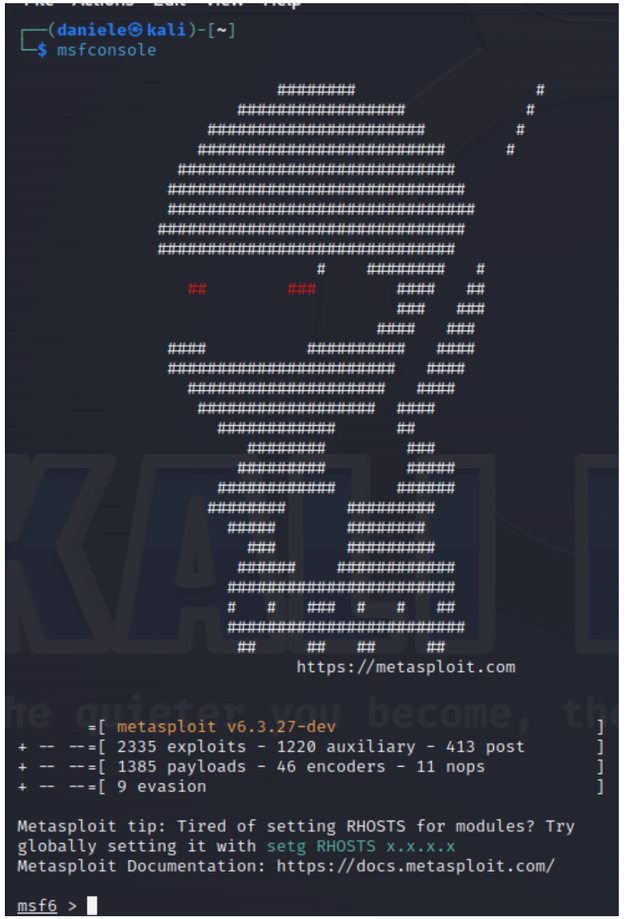
Ho effettuato una scansione con nmap con lo switch -sV, che mi permette di visualizzare la versione del servizio scansionato, in questo caso il telnet su porta 23.



Avvio metasploit da kali, attraverso il comando msfconsole.

Cerco l'exploit di cui ho bisogno attraverso il comando "search telnet_version". Telnet è un protocollo per la connessione remota verso un host con l'utilizzo di una shell di comando.

Possiamo notare due exploit possibili, ma andremo ad utilizzare il secondo, come da traccia.




```
msf6 > search telnet_version

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank    Che
ck  Description
   -  ----                                                  ---------------  ----    ---
--  -----------
   0  auxiliary/scanner/telnet/lantronix_telnet_version                      normal  No
    Lantronix Telnet Service Banner Detection
   1  auxiliary/scanner/telnet/telnet_version                                normal  No
    Telnet Service Banner Detection


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/s
canner/telnet/telnet_version
```

Diciamo al tool di utilizzare l’exploit desiderato attraverso il comando “use 1”. Impostiamo l’ip della macchina vittima e poi visualizziamo le opzioni dell’exploit scelto, in modo da vedere se è configurato correttamente. L’exploit è configurato correttamente, quando i campi “required” sono tutti compilati.
Lanciamo l’attacco attraverso il comando “exploit”.
L’exploit và a buon fine e ci restituisce user e password per collegarci all’interfaccia telnet.