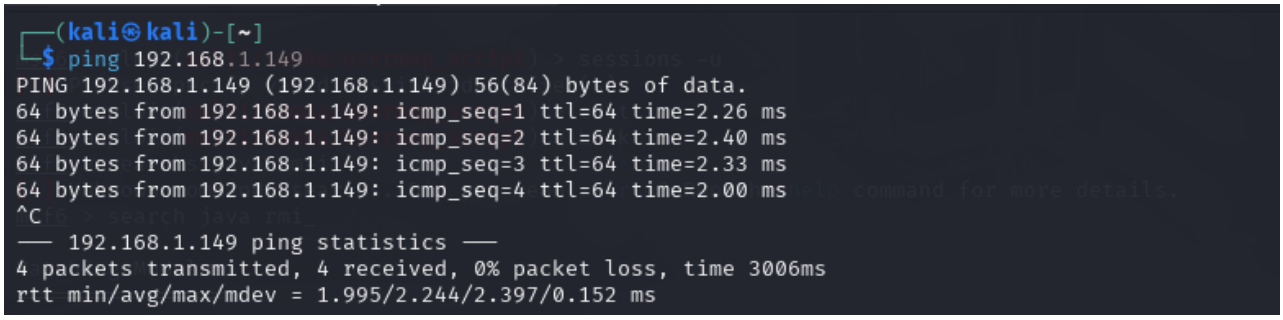
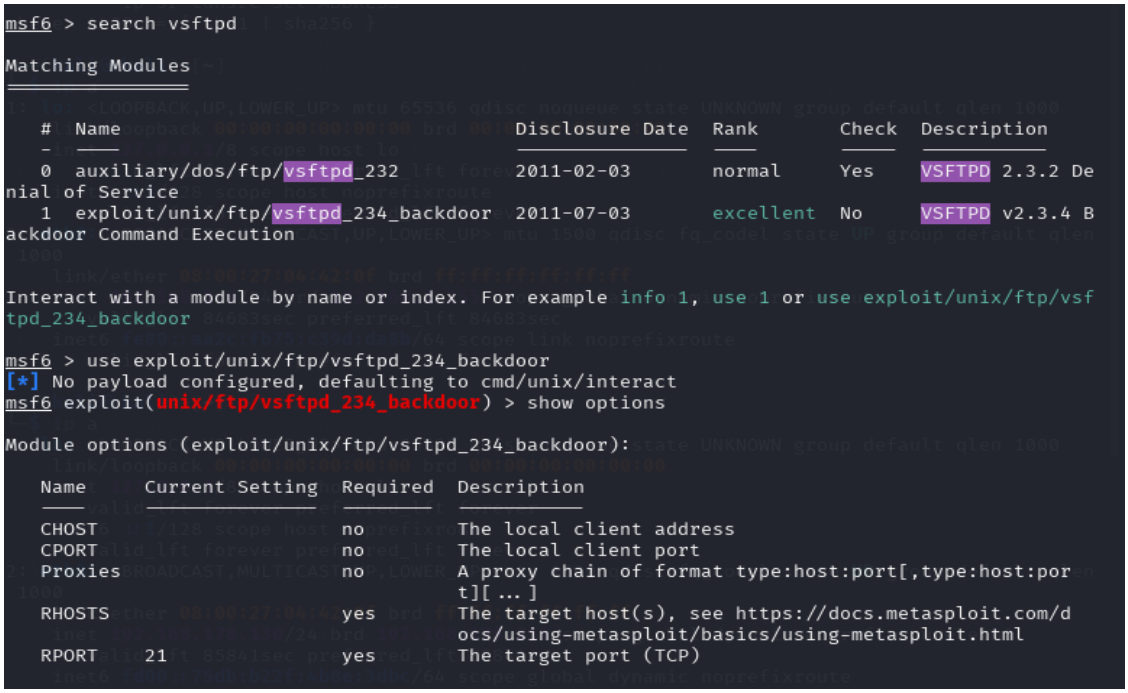
S7L1 HACKING CON METASPLOIT

Completare una sessione di hacking sul servizio “vsftpd” della macchina Metasploitable.

Come richiesto dall’esercizio ho dato alla macchina Metasploitable l’ip 192.168.1.149/24, ho poi verificato con il comando *ping* da Kali che comunicassero tra di loro.



Abbiamo aperto il terminale da Kali e digitato “*msfconsole*” come comando. Siamo così entrati nel prompt di Metasploit. Con “*search vsftpd*” ci mostrerà un elenco di expolit e moduli ausiliari relativi a vsftpd. Abbiamo individuato l’exploit da provare, c’è una backdoor e si può ottenere una shell di root. Con il comando *use* seguito dall’exploit che vogliamo utilizzare (*use exploit/unix/ftp/vsftpd_234_backdoor*). Visualizzeremmo le opzioni con *show options*.



Impostiamo l'indirizzo IP della macchina target con *set RHOSTS 192.168.1.149.* Con *show payloads* andremmo a vedere quelli disponibili, in questo caso solo uno ed andremo ad utilizzare quello che è configurato di default. Lanciamo poi l'attacco con il comando *exploit.*

Una volta dentro la macchina, abbiamo creato la cartella con il comando *mkdir /test_metasploit.*