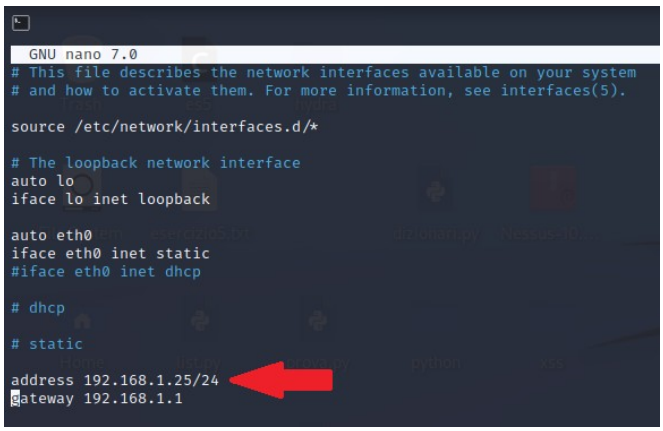
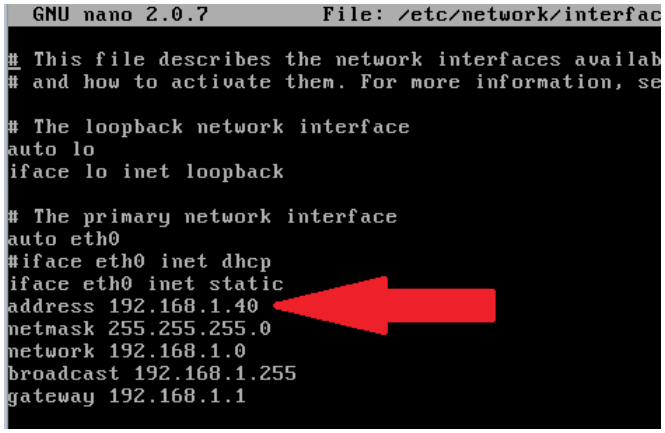
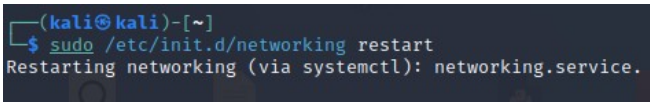
REPORT 06/12/2022 LORENZO SCORBAIOLI

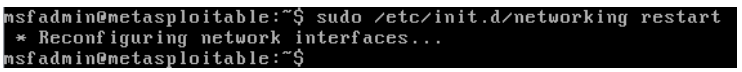
TASK:
Sfruttare la vulnerabilità Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable. Configurare l'IP di Kali con 192.168.1.245 e l'IP di Metasploitable con 192.168.1.40

Per prima cosa tramite il comando sudo nano /etc/network/interfaces sono andato a modificare gli indirizzi IP prima su kali e poi su Metasploitable. Dopo averli cambiati seguendo le indicazioni della traccia ho fatto ripartire i servizi di network per rendere effettivi i cambiamenti:

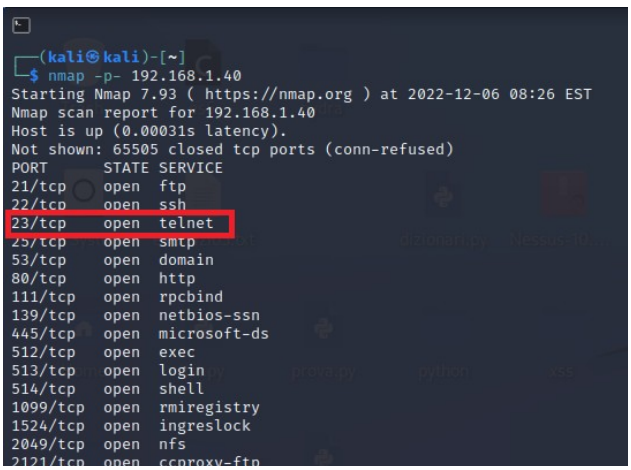




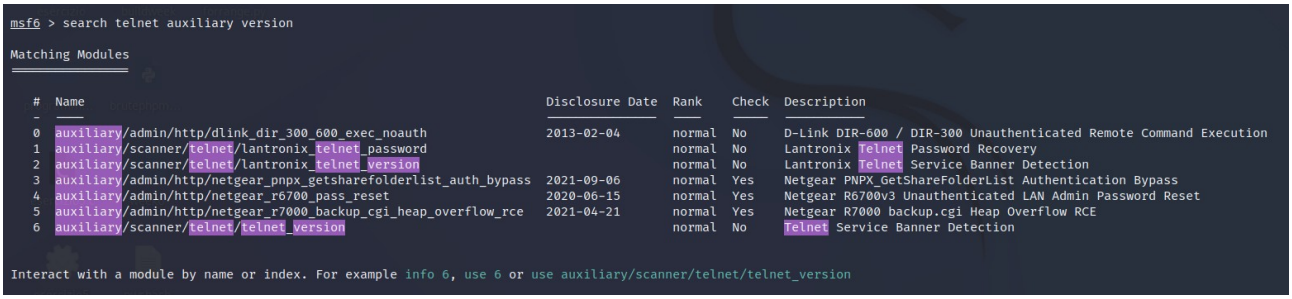




Prima di procedere ad utilizzare Metasploit ho lanciato nmap per vedere le porte attive e i relativi servizi collegati ad esse e nel riquadro rosso possiamo vedere il servizio tramite il quale attaccare la macchina:

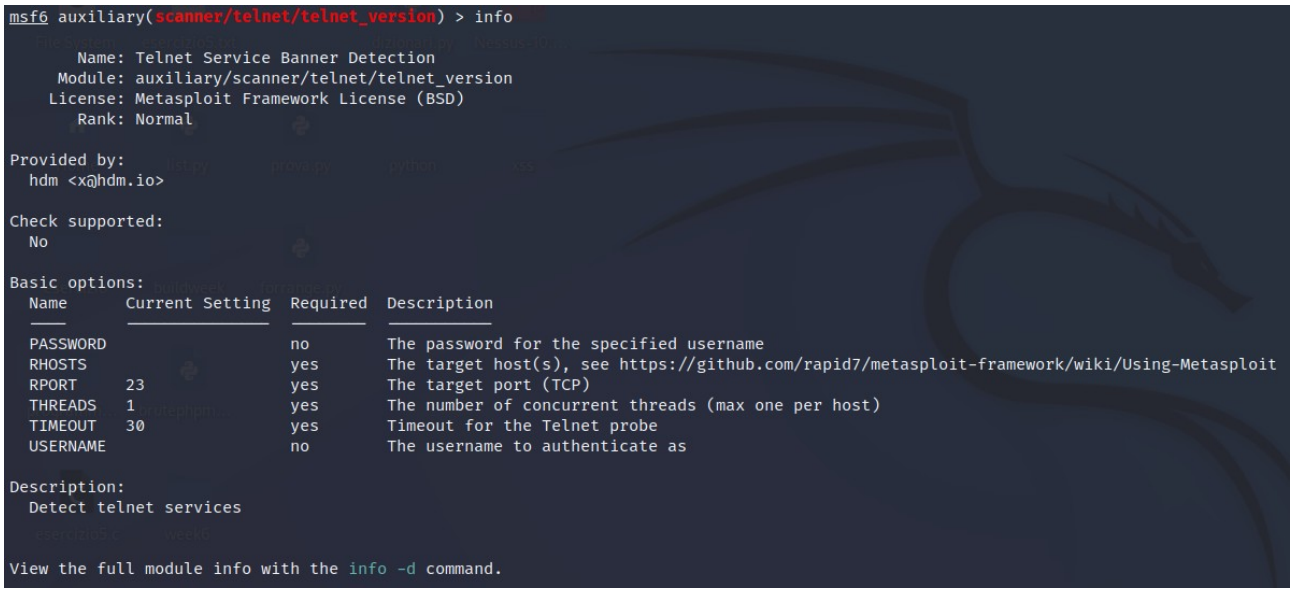


A questo punto ho avviato sulla macchina Kali ho lanciato il comando msfconsole e sono andato a cercare il modulo per il servizio auxiliary telnet_version:



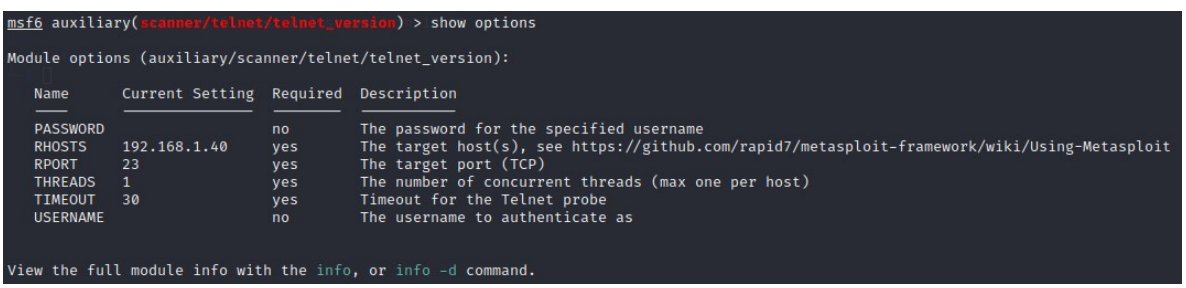
Il modulo che ci interessa è il 6 quindi sono andato a selezionare quello:

Sono prima andato a vedere le informazioni del modulo lanciando il comando info:



A questo punto sono andato a inserire RHOSTS che sarebbe l’IP della macchina attaccata, nel nostro caso Metsploitable:

Sono andato a controllare se dovessi inserire altre info per effettuare l’exploit e se dovessi inserire il payload ma non si è rilevato necessario:



Ho quindi lanciato l’exploit:

Da esso sono riuscito ad ottenere le informazioni per fare il login. A questo punto, per ottenere i provilegi di root sono andato sulla macchina attaccante e ho eseguito il comando telnet inserendo l’IP della maccchina che ho attaccato:

Una volta entrati tramite le credenziali recuperate precedentemente sono andato a fare un comando id per vedere chi fossi (sottolineato in verde). Per ottenere i privilegi di root ho quindi eseguito il comando sudo su (prima sottolineatura in rosso) e ho lanciato nuovamente il comando id per avere conferma di avere ottenuto i privilegi di root (seconda sottolineatura in rosso).