CUORE ANDREA

06/12/2022

EXPLOIT PORT 23 TELNET

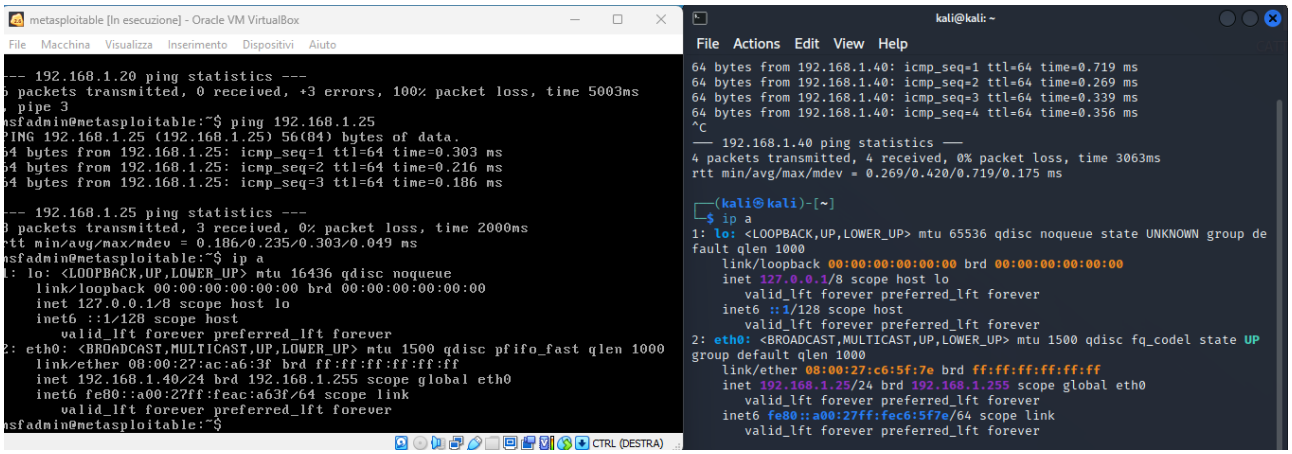
CONFIGURAZIONE INDIRIZZI IP ED EXPLOIT CON MSFCONSOLE.

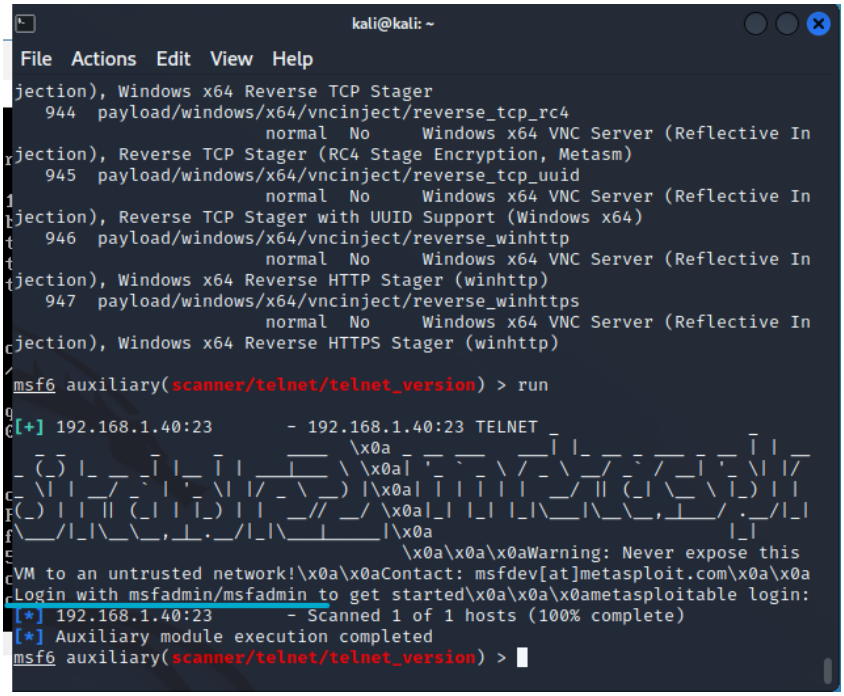
Per lo svolgimento dell'esercizio di oggi ci è stato richiesto di impostare gli indirizzi IP della macchina kali e della macchina metasploit nel seguente modo:

Metasploit: 192.168.1.40

Kali: 192.168.1.25

Dopo la configurazione abbiamo utilizzato il tool msfconsole per fare l'exploit di tale servizio, la tecnica utilizzata è la stessa vista a lezione, ovvero con l'ausilio del modulo "auxiliary/scanner/telnet/telnet_version".





PRIVILEGE ESCALATION:

Dopo aver ottenuto le credenziali d’accesso del nostro exploit, ci basterà lanciare telnet da terminale inserendo le credenziali recuperate, e successivamente lanciare un sudo su per ottenere i permessi di root