S7L2

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito:

Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40

Obiettivo

Utilizzare **Metasploit** per analizzare il servizio **Telnet** esposto su **Metasploitable2**, rilevandone la versione tramite il modulo auxiliary/scanner/telnet/telnet_version.

Configurazione IP

Kali Linux

sudo ip addr add 192.168.1.25/24 dev eth0
sudo ip link set eth0 up

Metasploitable2

sudo ifconfig eth0 192.168.1.40 netmask 255.255.255.0 up

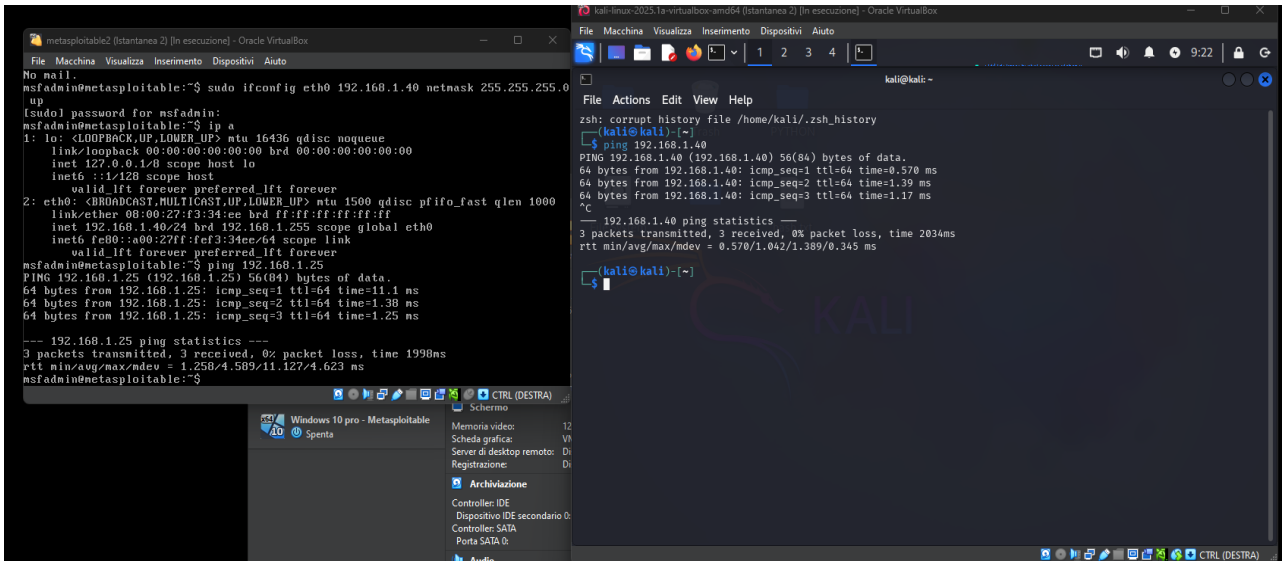
Verifica con ping

- Da Kali:

ping 192.168.1.40

- Da Metasploitable:

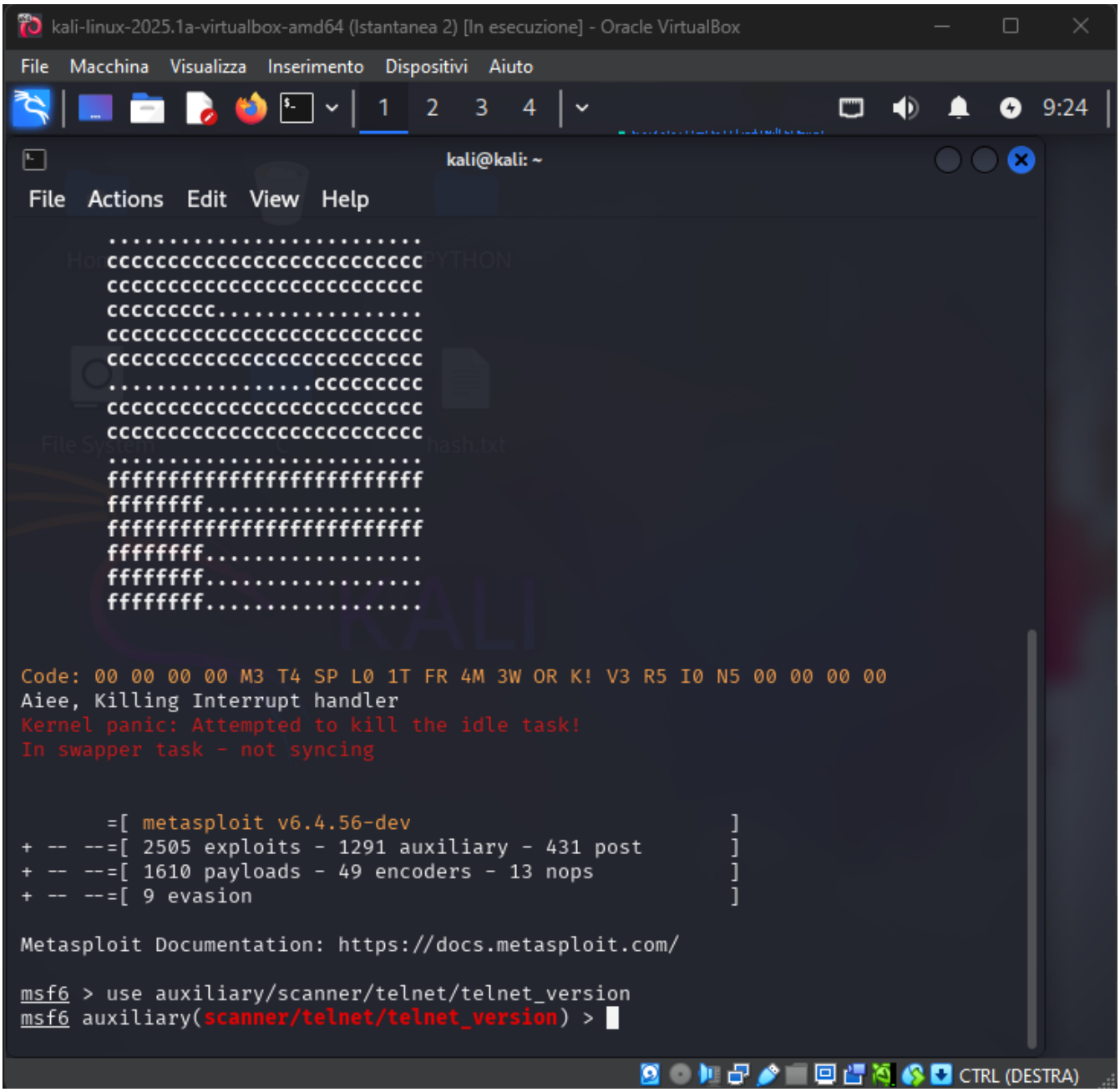
ping 192.168.1.25



Avvio di Metasploit

Su Kali:

Msfconsole



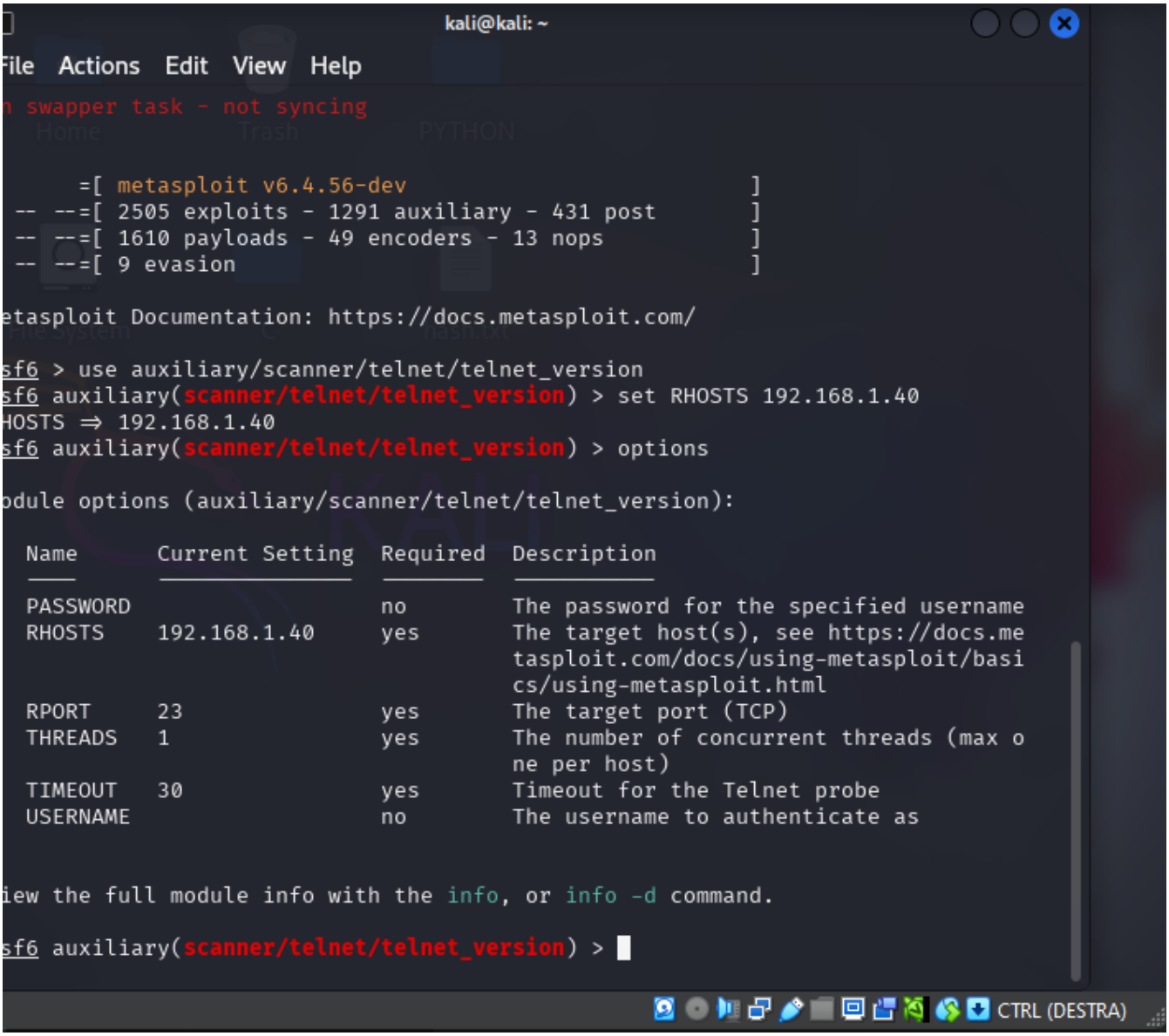
Scansione Telnet con telnet_version

Carico il modulo:

use auxiliary/scanner/telnet/telnet_version

Imposto il target:

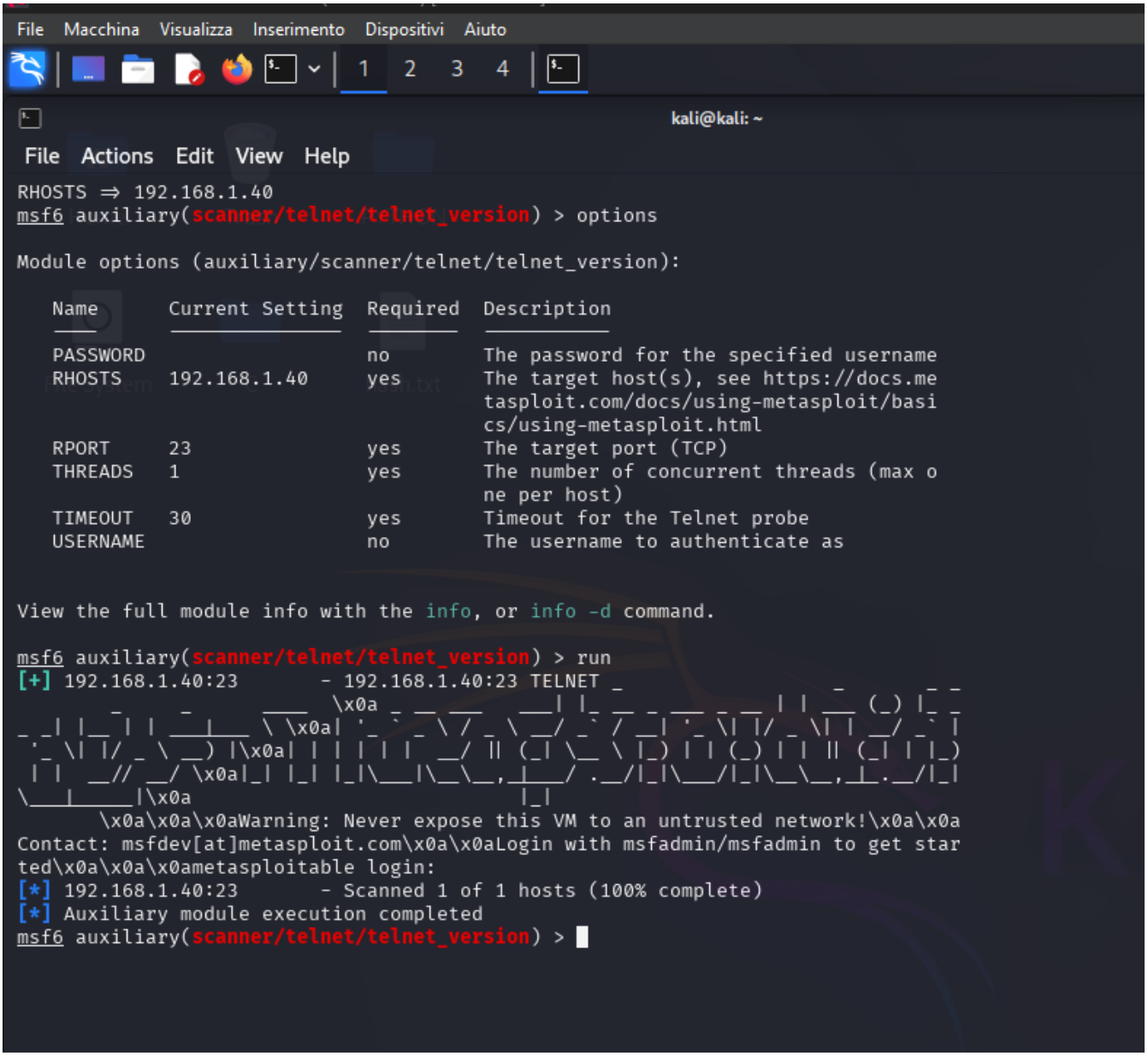
set RHOSTS 192.168.1.40



Mi accerto con il comando options che la configurazione di targhet sia corretta

Avvio la scansione:

Run



Risultato della scansione

L'output ottenuto conferma:

- **Il servizio Telnet è attivo** sulla porta 23 di Metasploitable2.
- È stato rilevato il **banner del servizio**, che include:
  - Una grafica ASCII che conferma l'ambiente Metasploitable
  - Il messaggio: Login with msfadmin/msfadmin to get started

Conclusione

- La scansione è andata a buon fine: **Telnet è attivo e vulnerabile**, pronto per ulteriori fasi di test o attacco.
- Abbiamo identificato:
  - L'indirizzo IP del target (192.168.1.40)
  - Il servizio attivo (Telnet)
  - Le credenziali di default suggerite (msfadmin/msfadmin)

Prossimi step possibili

Accesso diretto via Telnet:

telnet 192.168.1.40
Login: msfadmin
Password: msfadmin

Brute force con Metasploit:

use auxiliary/scanner/telnet/telnet_login
set RHOSTS 192.168.1.40
set USERNAME msfadmin
set PASSWORD msfadmin
run

Sfruttamento post-accesso (privilege escalation, pivot, ecc.)