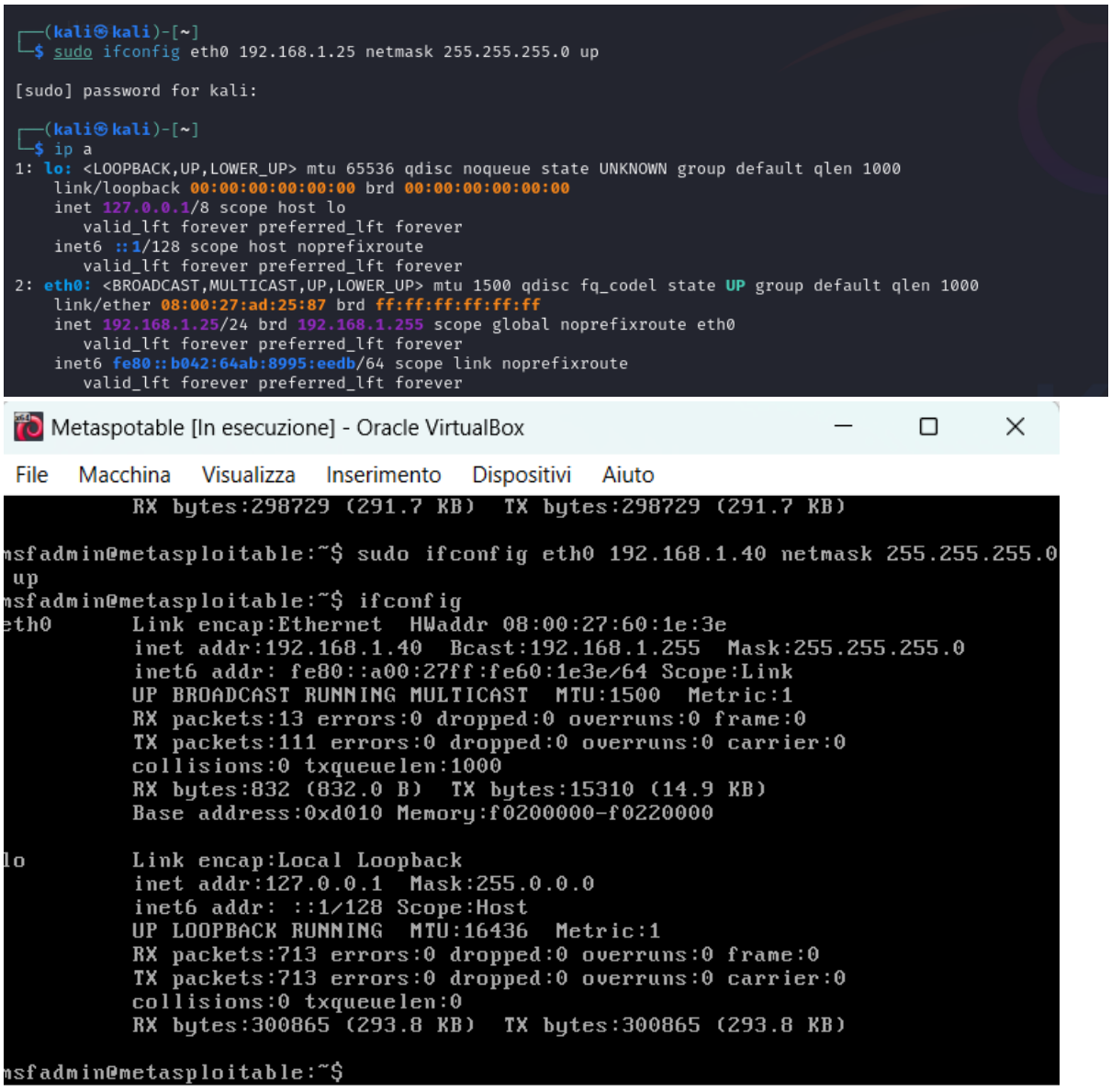
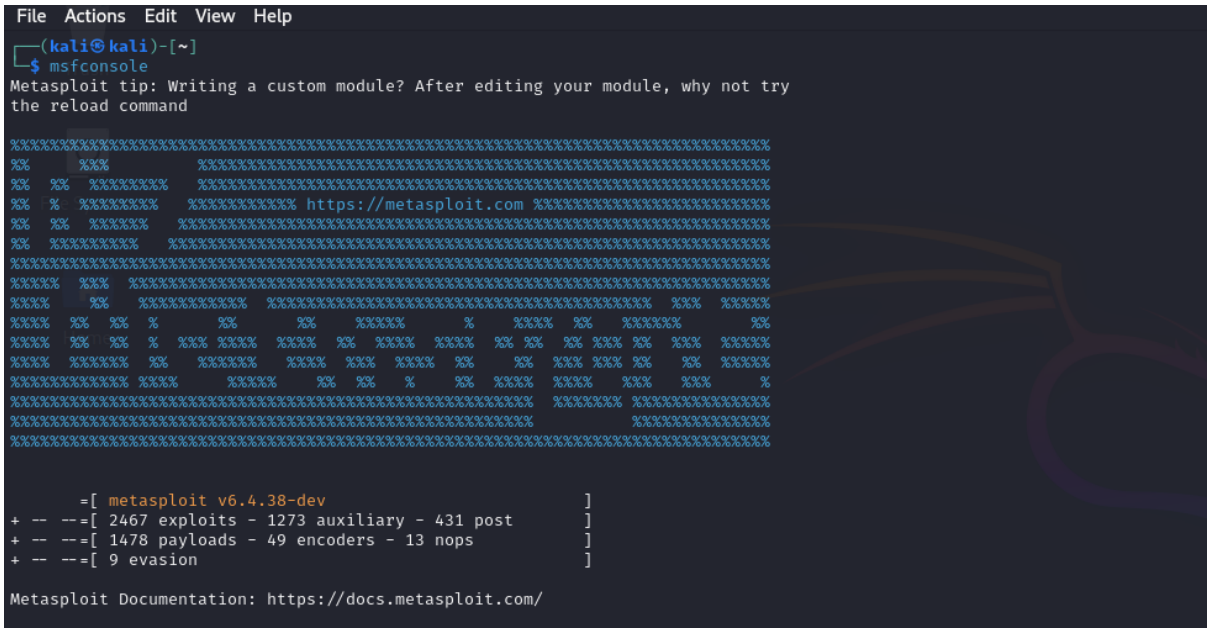
Relazione 17-12

L’obiettivo dell’esercizio è stato quello di analizzare la vulnerabilità del servizio Telnet in esecuzione sulla macchina Metasploitable utilizzando il modulo auxiliary/scanner/telnet/telnet_version di Metasploit.

Per prima cosa ho modificato gli indirizzi IP della Kali e della metasploit come richiesto dalla traccia.



Metasploit è stato avviato con il comando msfconsole



Scrivendo search telnet_version ci trova l'auxiliary che ci interessa, utilizzo il modulo auxiliary/scanner/telnet/telnet_version di Metasploit per analizzare il servizio Telnet attivo sulla macchina Metasploitable. Dopo aver caricato il modulo, è stato configurato il parametro RHOSTS con l'indirizzo IP del target (192.168.1.40) per definire l'host remoto da analizzare. Successivamente, l'attacco è stato avviato tramite il comando run, consentendo al modulo di raccogliere informazioni sul servizio Telnet.

L'esecuzione del modulo ha confermato la presenza del servizio Telnet in ascolto sulla porta standard 23/TCP. 192.168.1.40:23 TELNET

Con il comando Telnet 192.168.1.40 tento di stabilire una connessione con l'IP della metasploit e verifico che va a buon fine.