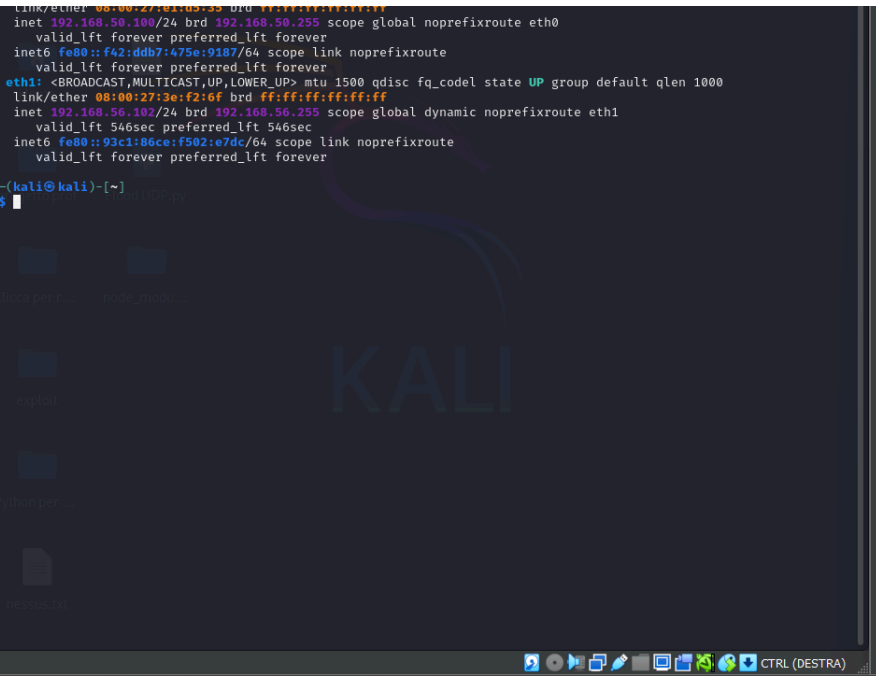
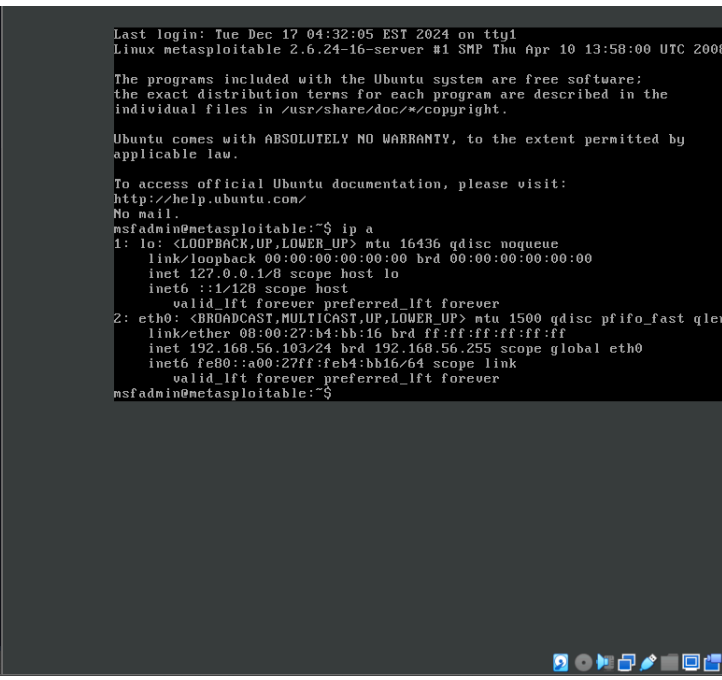
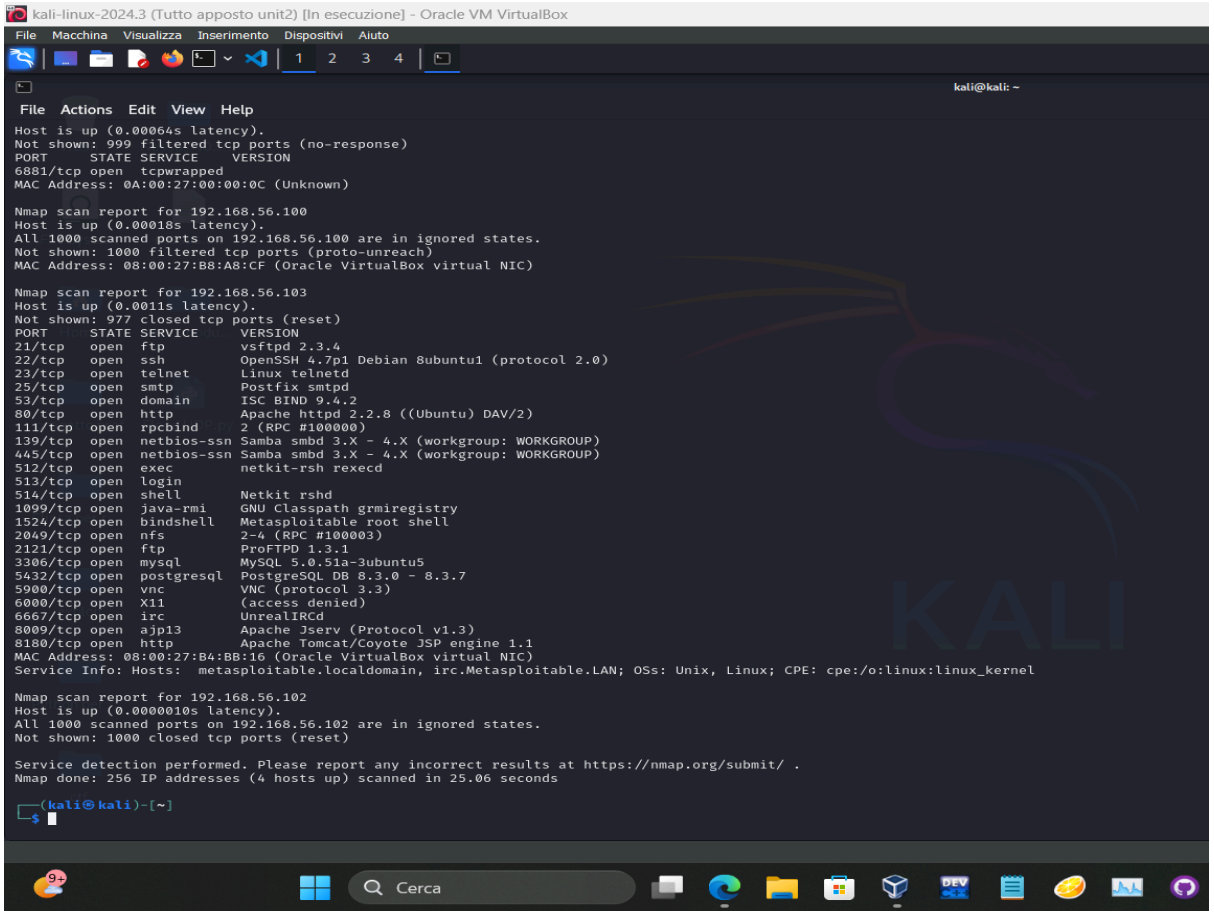
Vuln Telnet Scanner.

Inizialmente ho messo le mie 2 macchine sotto dhcp per bypassare la mia rete di casa.

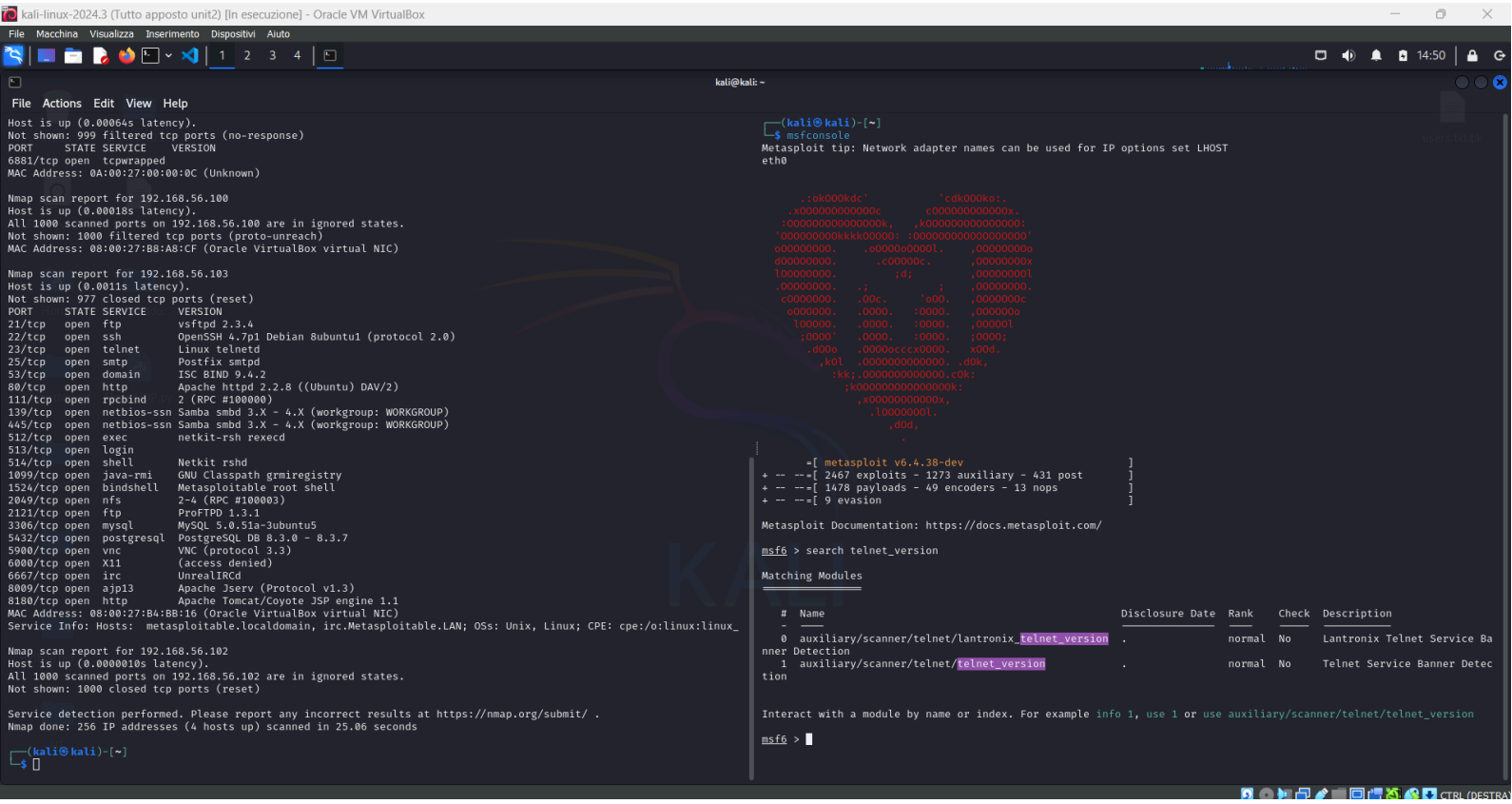




Poi ho eseguito un nmap -Sv su tutti gli ip attivi nella rete per sgamare l'ip della metasploitable e di tutti i suoi servizi aperti con corrispettiva versione.



A seguire ho aperto msfconsole per ricercare la vulnerabilità di telnet.



In seguito ho selezionato la vulnerabilità corretta ed ho settato il mio target col comando set RHOST <ip target> ed ho dato un run per dare il via all'exploit e farmi droppare le credenziali di accesso.