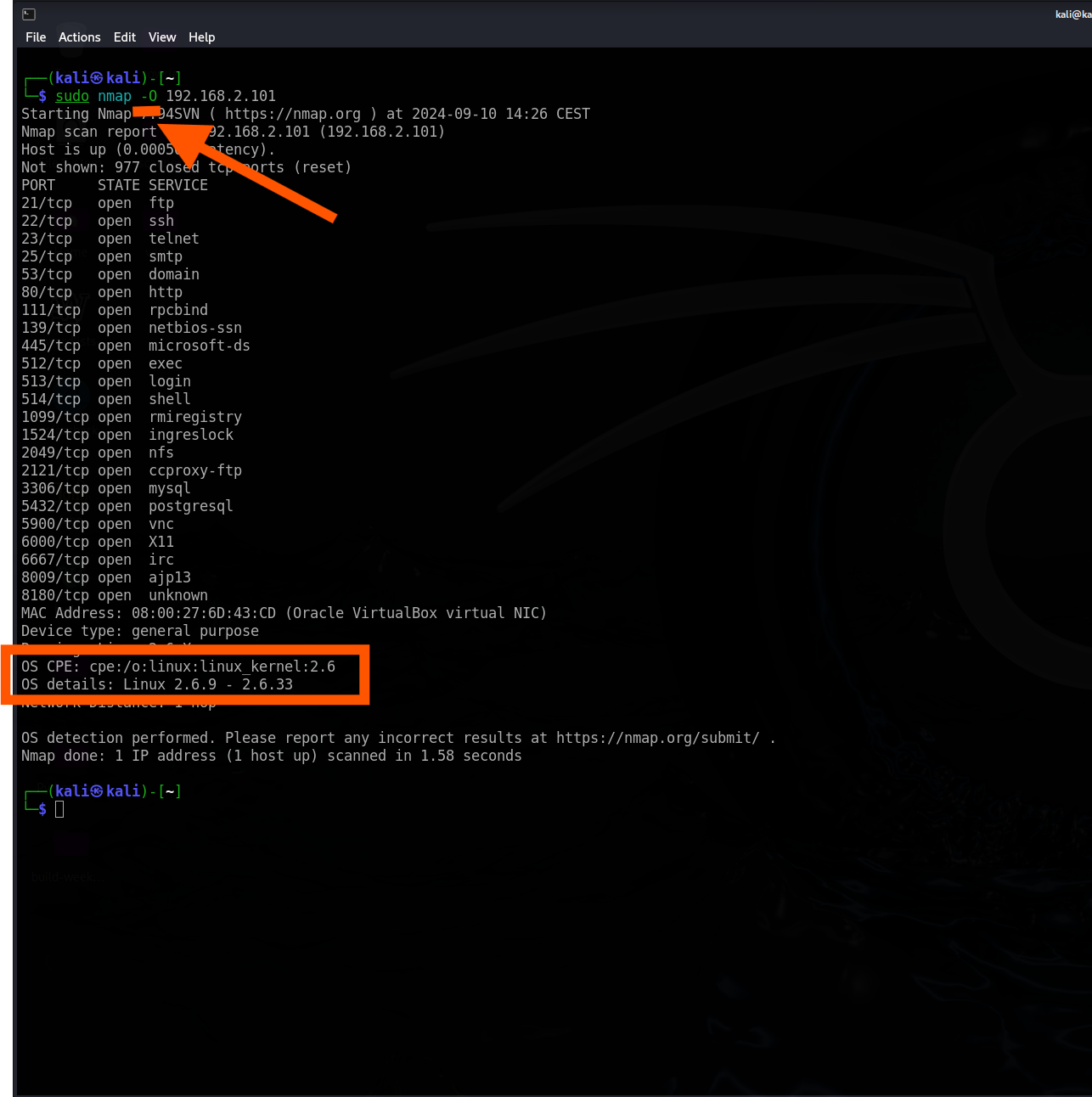
CONSEGNA 10 SETTEMBRE

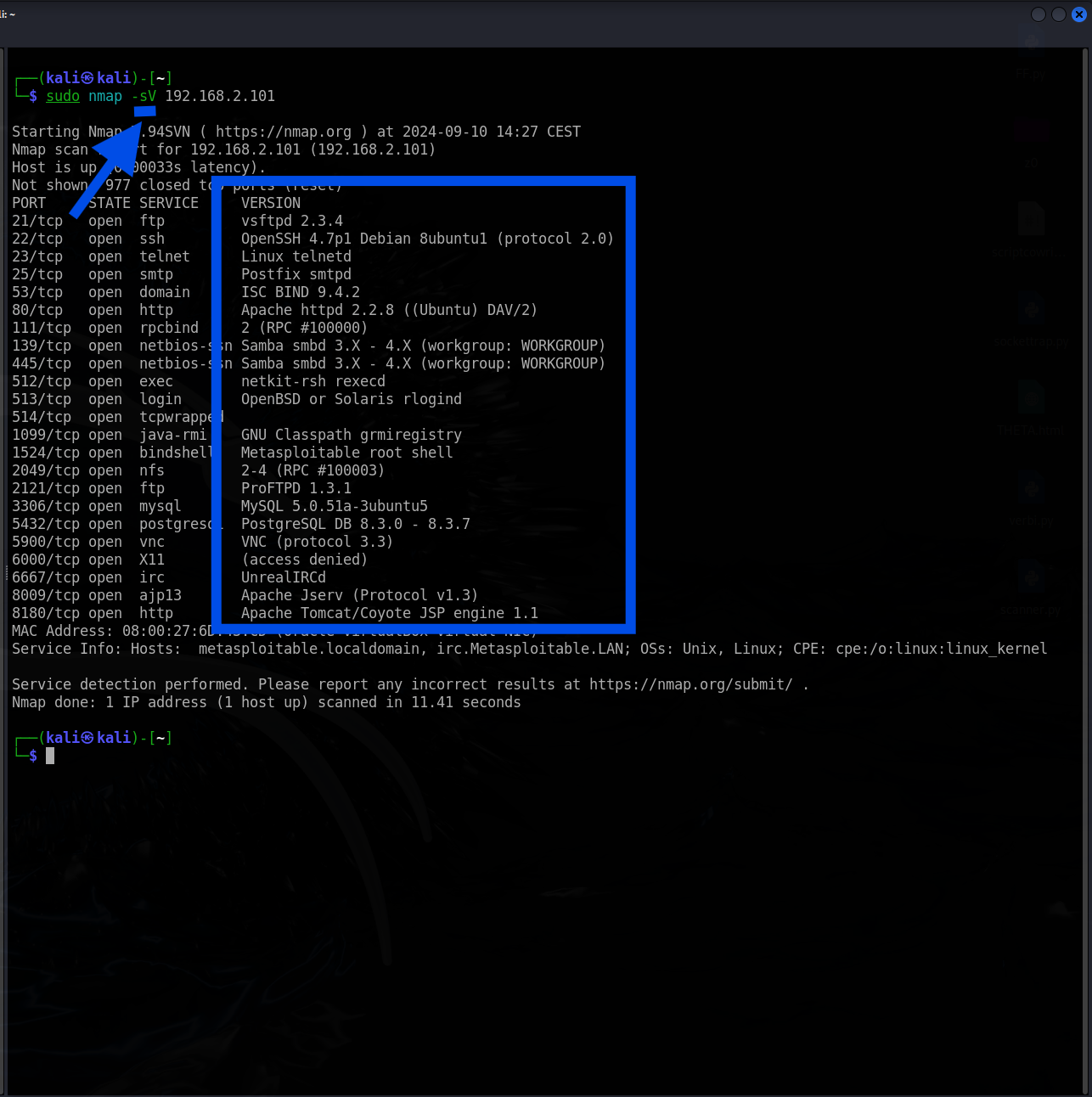
Sono risalito al tipo di OS usando il comando sudo nmap -O <IP TARGET METASPLOITABLE >.



SISTEMA OPERATIVO: LINUX 2.6.9 – 2.6.33

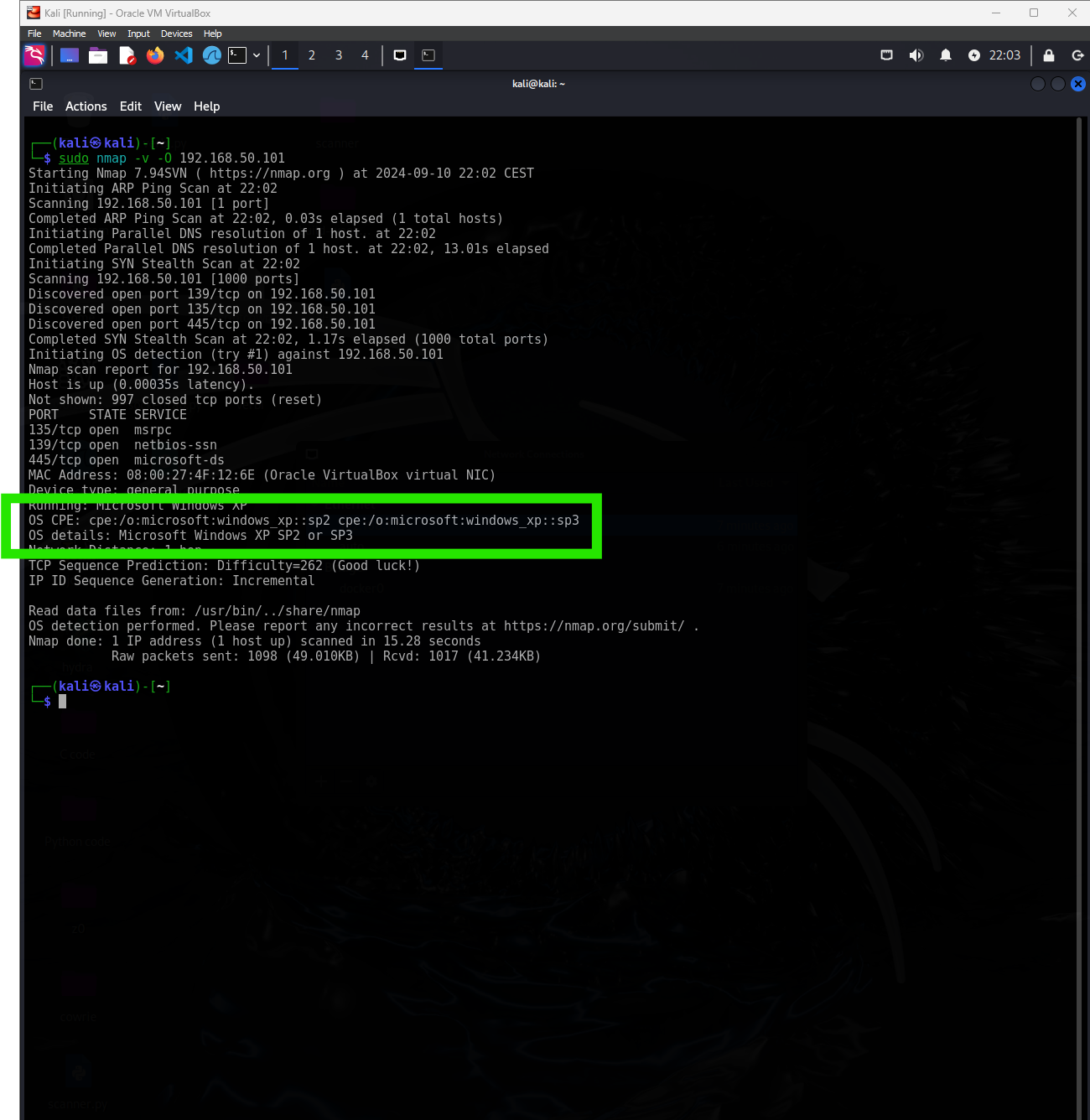
IP METASPLOITABLE: 192.168.2.101 – IP KALI: 1922.168.2.103

Ho ottenuto in output tutte le versioni delle porte aperte sulla macchina Metasploitable immettendo il comando sudo nmap -sV <IP TARGET METASPLOITABLE>.

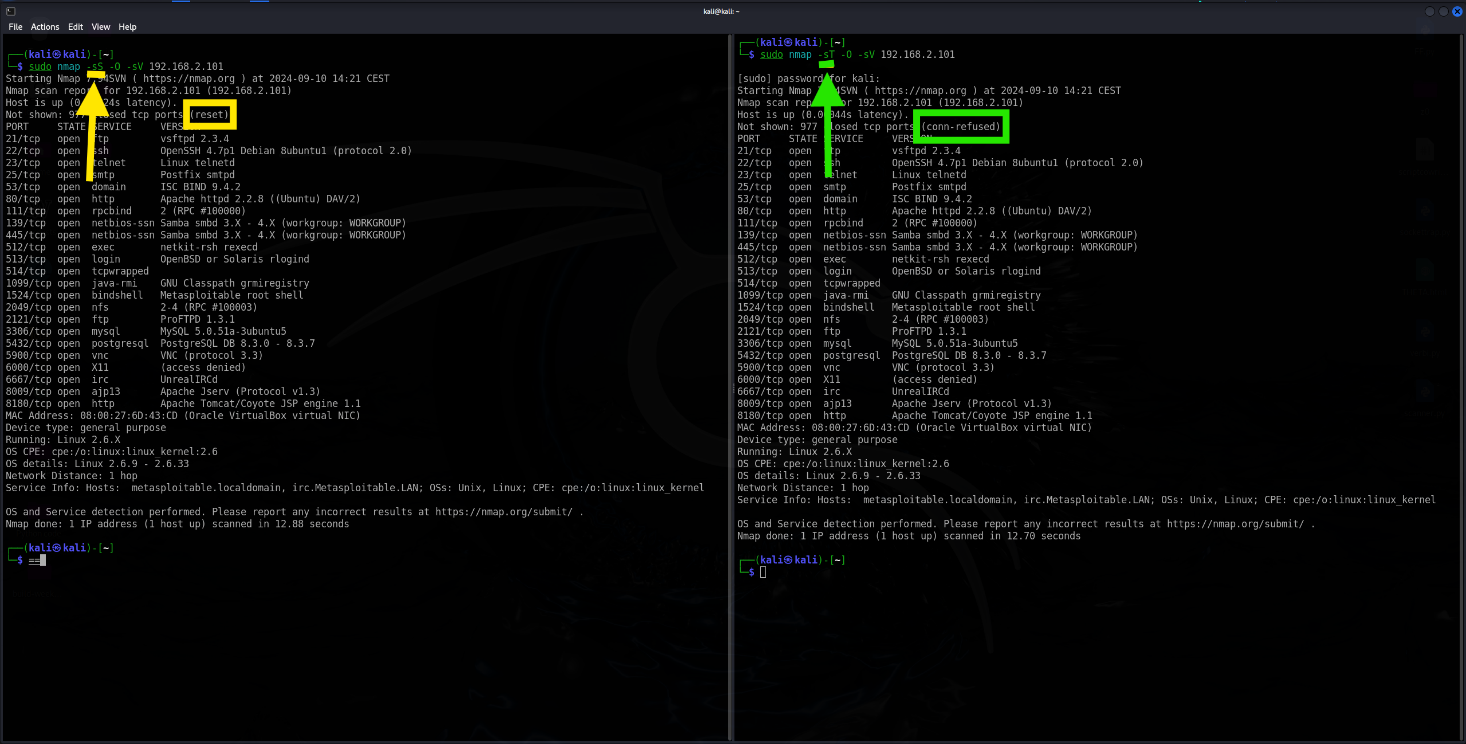


SERVIZI IN ASCOLTO CON LA LORO VERSIONE NEL RIQUADRO BLU.

Immettendo il comando sudo nmap -O <IP TARGET WINDOWS XP> sono risalito alla versione OS di quest’ ultimo.



IP WINDOWS XP: 192.168.50.101 – IP KALI 192.168.50.100



La differenza principale fra l’ opzione -sS e -sT e’che l’opzione TCP SYN scan (-sS) a differenza del TCP connect scan (-sT)non attende la risposta ACK dalla destination generando un RESET e non completando la three-handshake-way e qundi meno rilevabile da un analisi essende piu’ “stealth”. In oltre il metodo -sS ha bisogno di permessi di root a differenza di -sT.