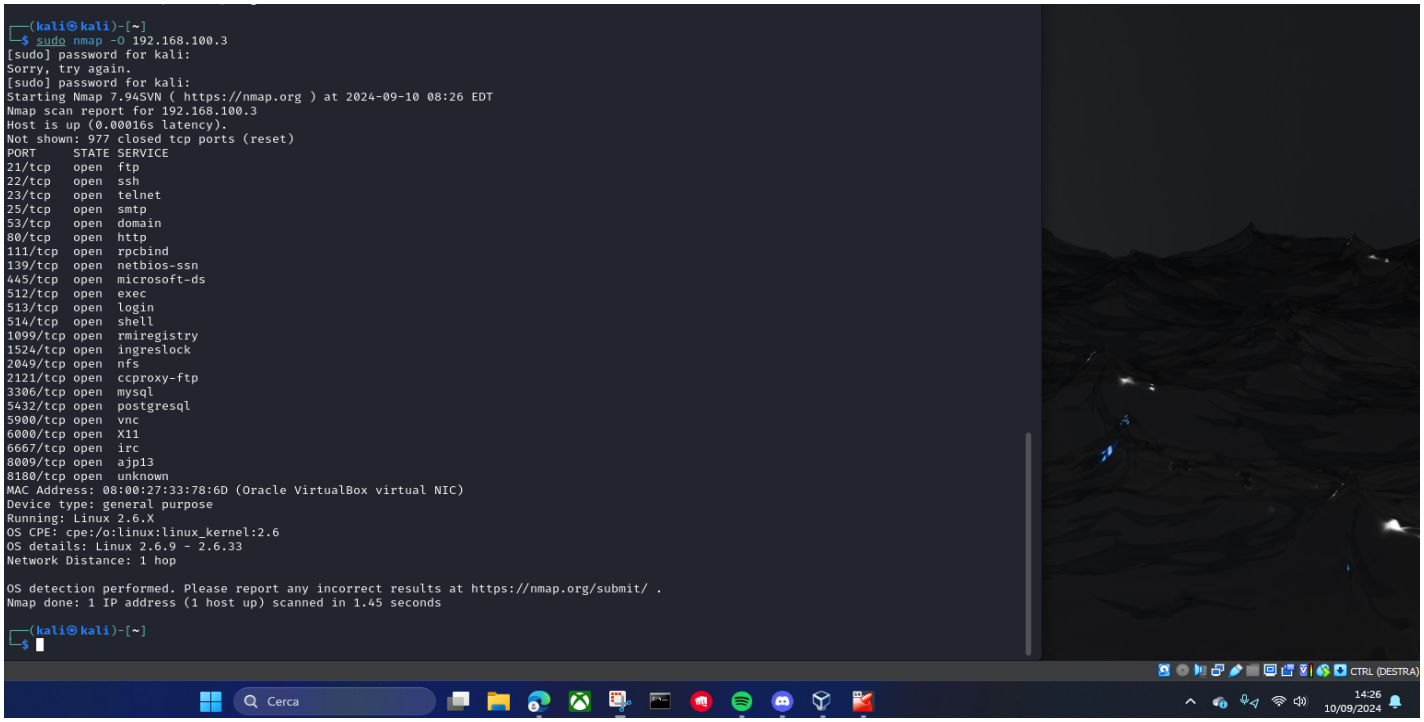
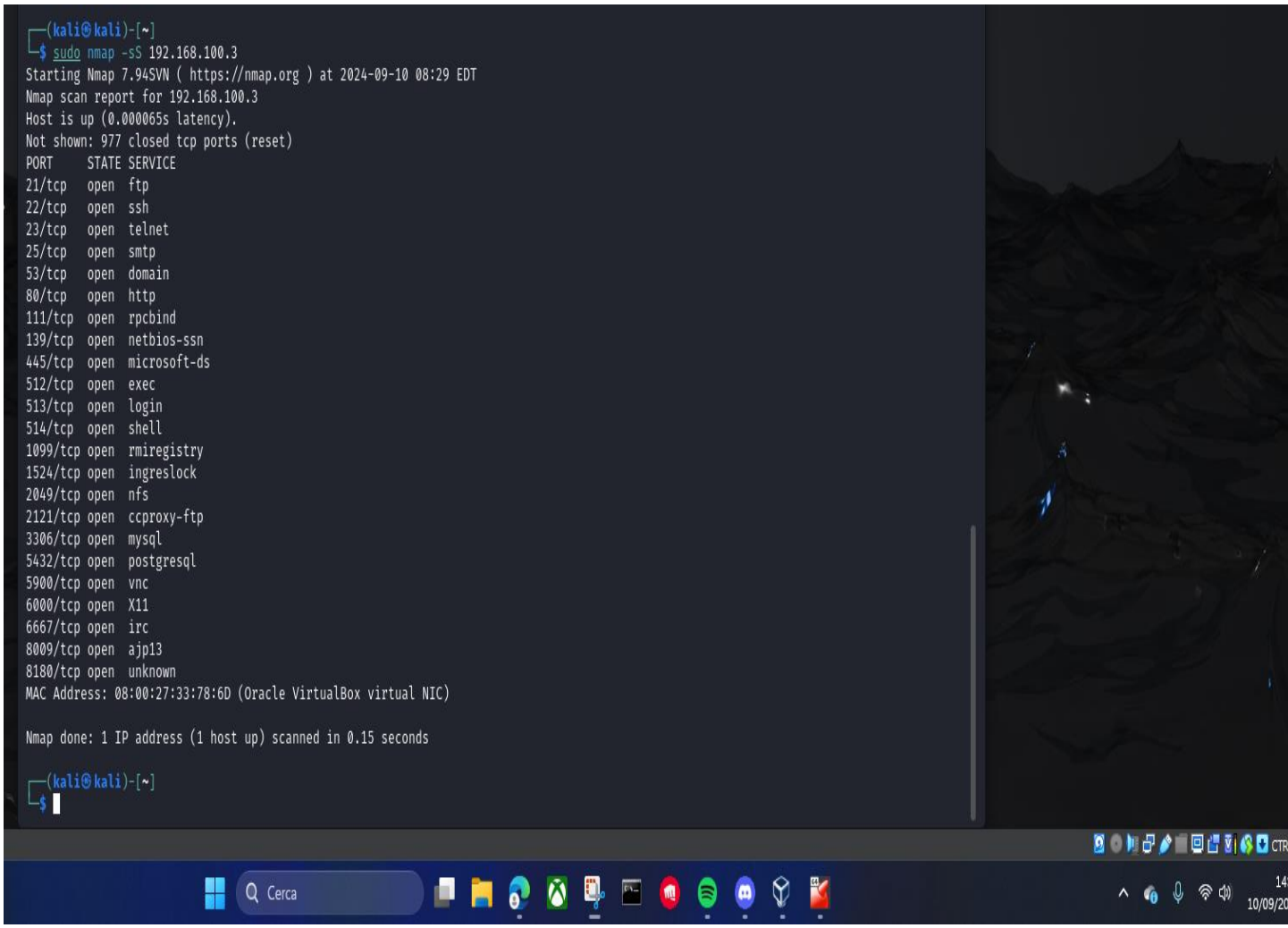
RELAZIONE NMAP

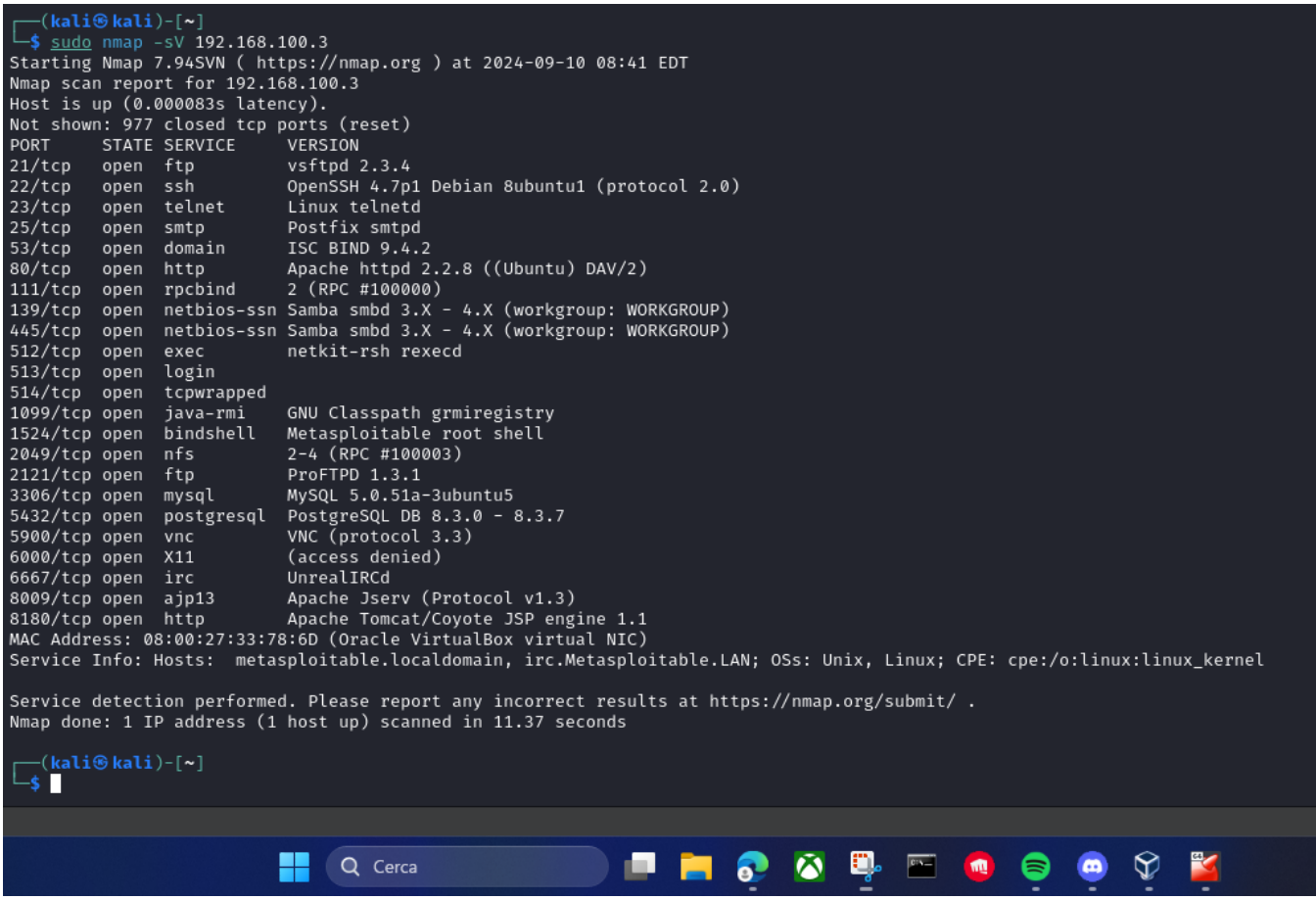
1. Con il comando fping -ag e la possibilità grazie alla shell di Linux di dividere gli output ho creato un file .txt contente tutti gli IP attivi della rete , poi con il comando nmap ho aperto tutta la lista comandi per nmap :

2. Una volta trovati gli IP delle macchine ho iniziato ad esaminare tutte le richieste come da traccia :





3. Tra la scan di TCP e SYN ho notato la differenza nel tempo di esecuzione dellla richiesta dove TCP ha impiegato 0.11s e SYN ne ha impiegati 0.15s .
4. Infine ho ricercato la versione di Meta tramite il comando nmap -Sv:



5. Come ultimo passo ho ricercato tramite il comando nmap -O il fingerprint di Win XP: