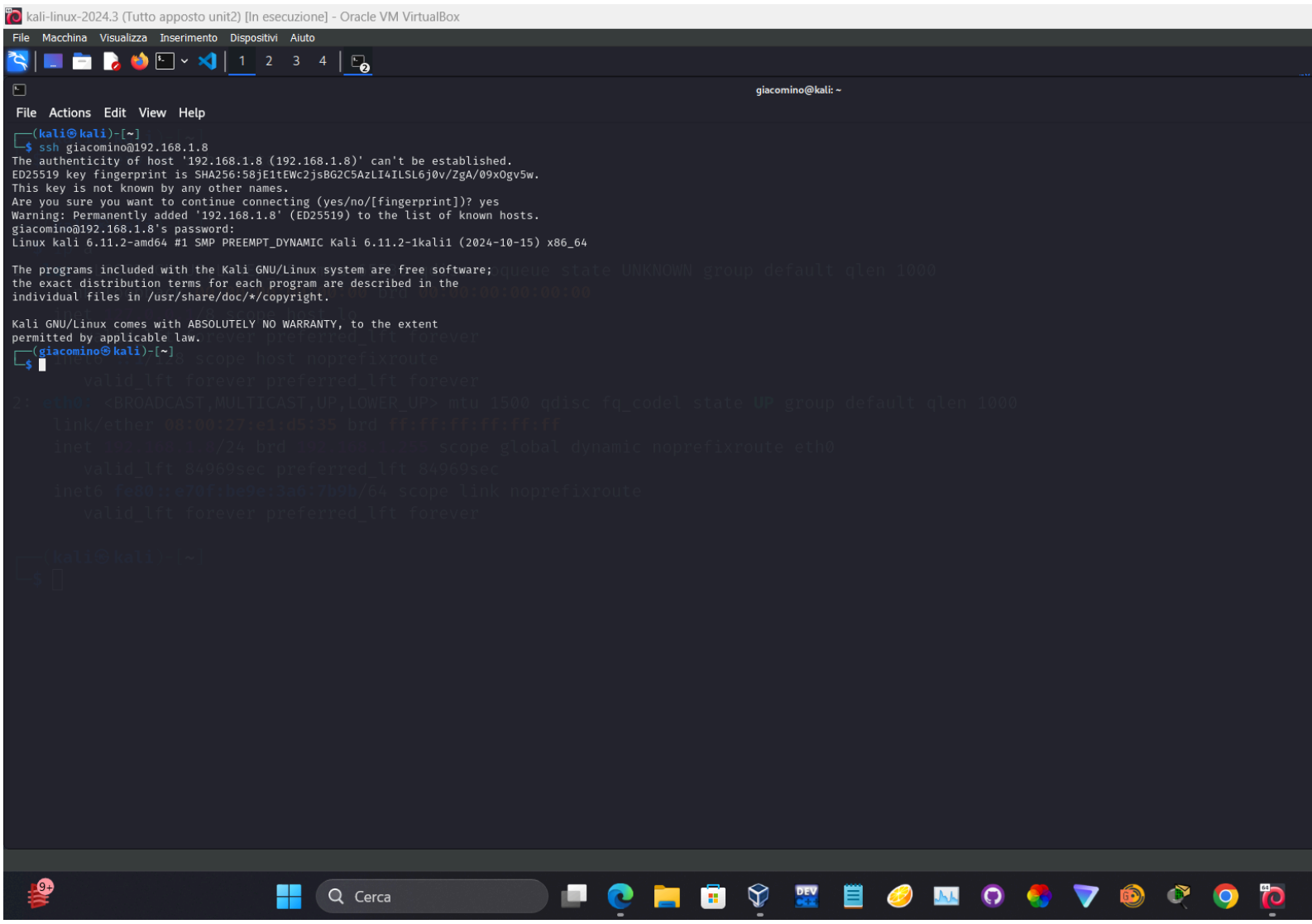
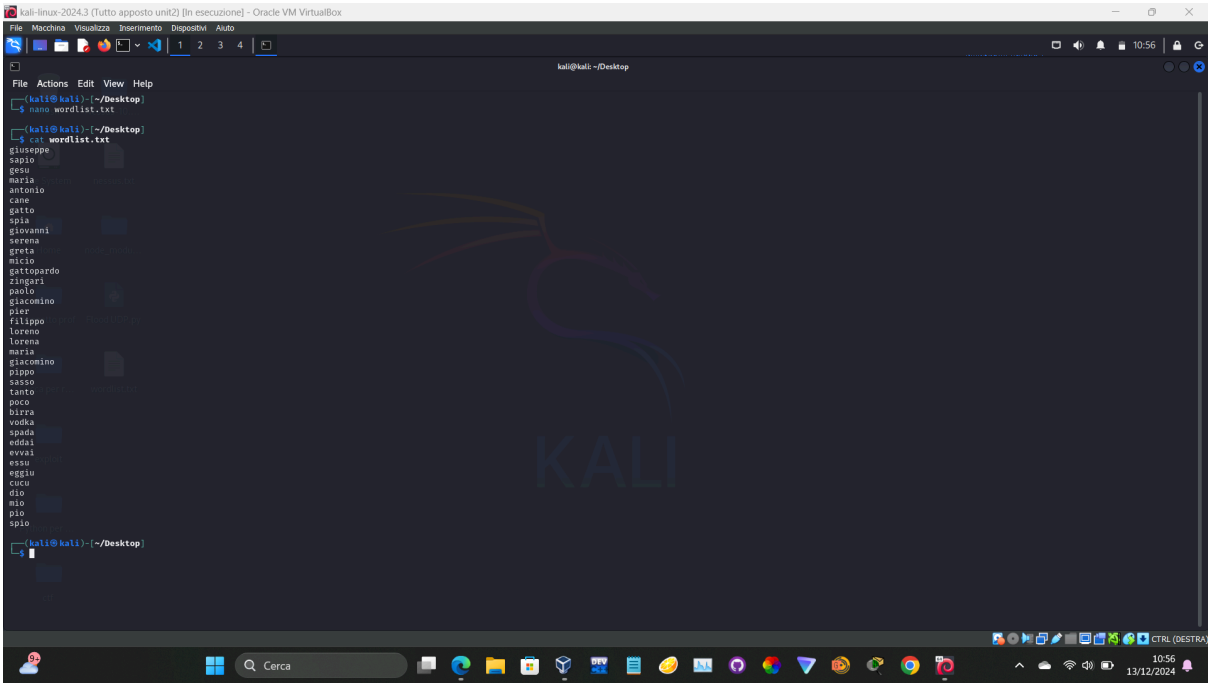
Oggi ho craccato la psw di un utente fatto da me sulla mia stessa macchina. Ho proceduto col crearlo e lo chiamato giacomino e come psw gli ho dato sempre giacomino, ho proceduto con l'attivare la comunicazione ssh dal file config che ho trovato nella path /etc/ssh/sshd_config. Dopodichè ho verificato se potevo connettermi al mio user tramite ssh ci son riuscito posto qua lo screen.




CONTINUA GIU

Ho proseguito creando una mia wordlist che daremo ad Hydra




Successivamente col parametro -l gli ho specificato il nome utente dell'user e con -P la wordlist per craccare le psw e per finire l'indirizzo di loopback (127.0.0.1) dato che era un attacco rivolto a me stesso, un'alternativa poteva essere come detto dalle slide il parametro -L per usare la wordlist anche per craccare il nome utente ci ho riprovato anche con questa formula ma ormai avevo già usato il metodo elencato qui sopra e non rielaborava il cracking, un'altra alternativa valida poteva essere spostare il servizio ssh di giacomino su un'altra porta per scagliare l'attacco usando l'ip della mia macchina e non il loopback, ho proceduto col primo metodo perchè è quello che mi è venuto in mente per primo in caso di autotest di seguito provo quanto ho scritto!