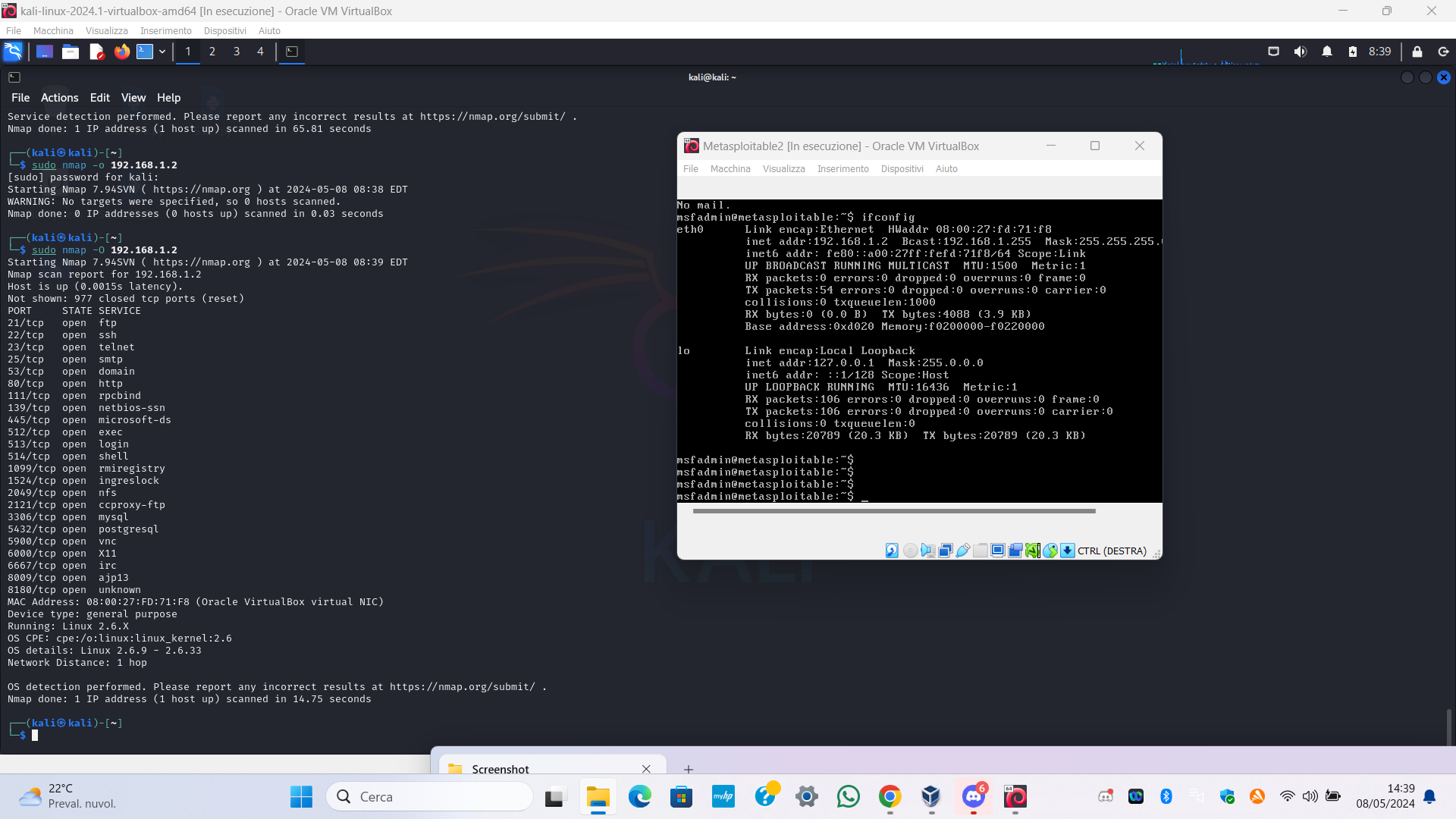
Per l’esercizio odierno ci avvaliamo di 3 macchine:

-Kali Linux (con IP 192.168.1.100/24)

-Metasploitable2 (con IP 192.168.1.2/24)

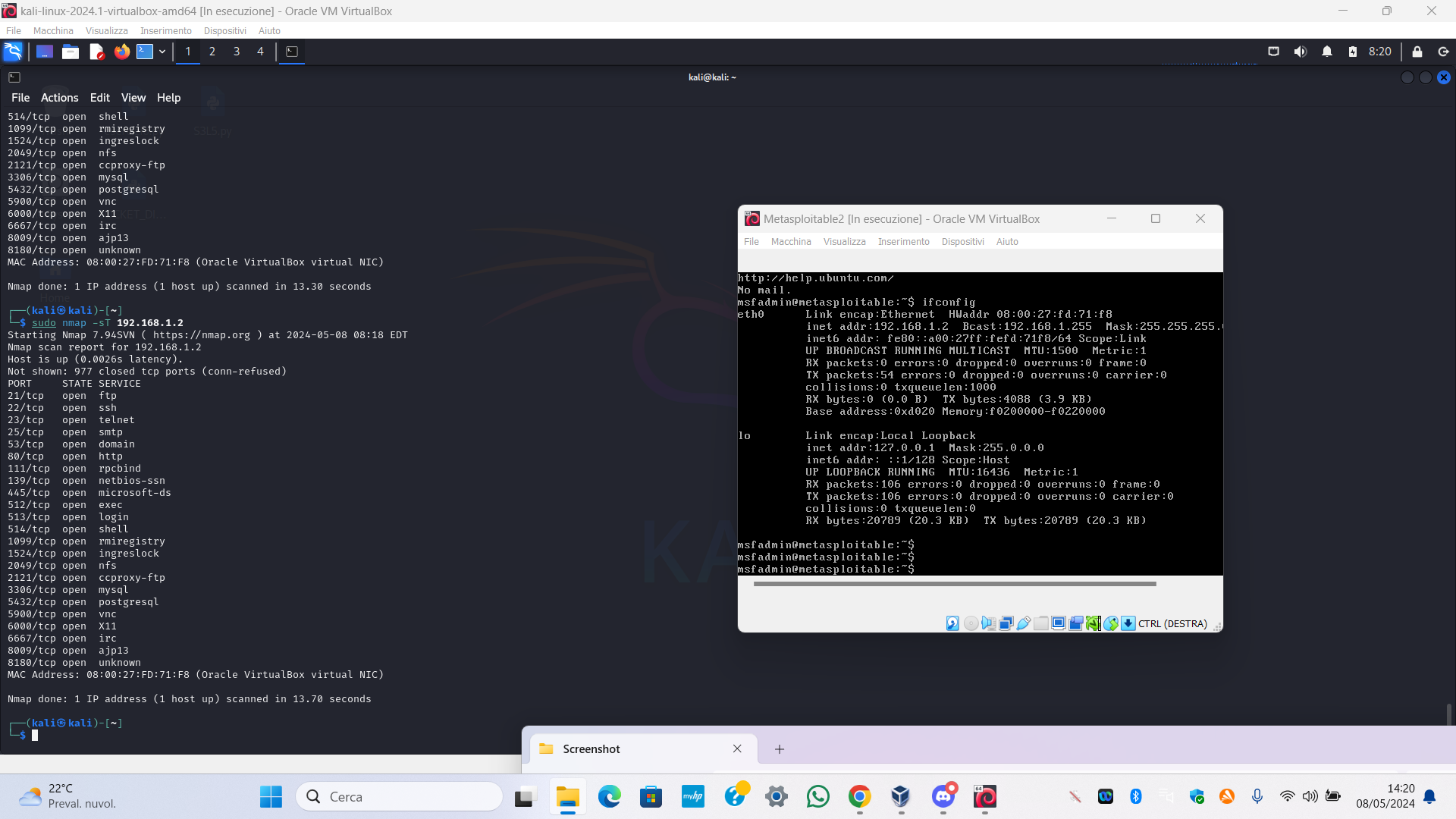
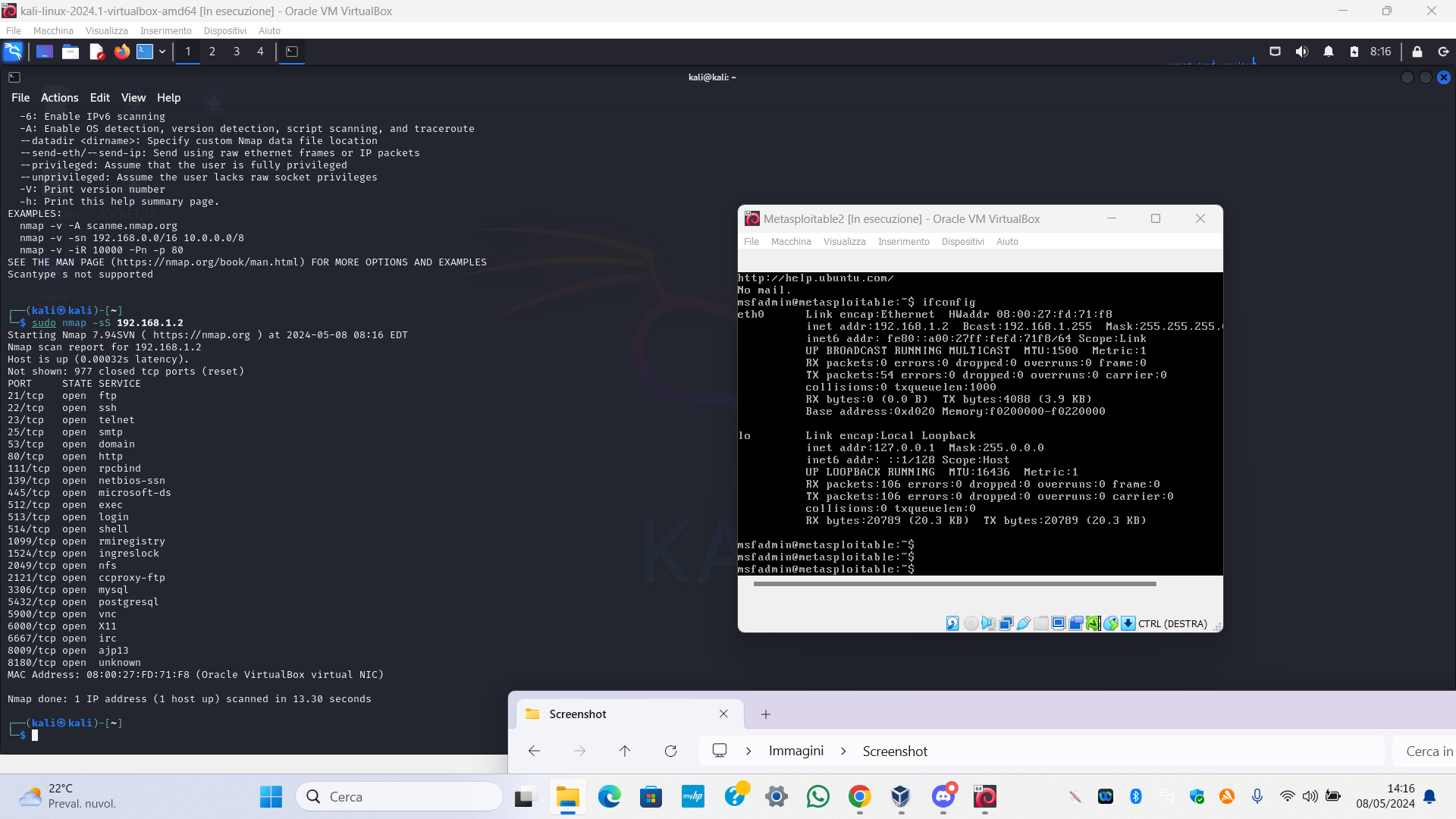
-Windows 7(con IP 192.168.1.3/24)

Grazie allo strumento nmap possiamo effettuare una serie di controlli sulle altre macchine. Vediamo di seguito le scansioni effettuate grazie alla macchina Kali Linux che hanno come bersaglio Metasploitable2.



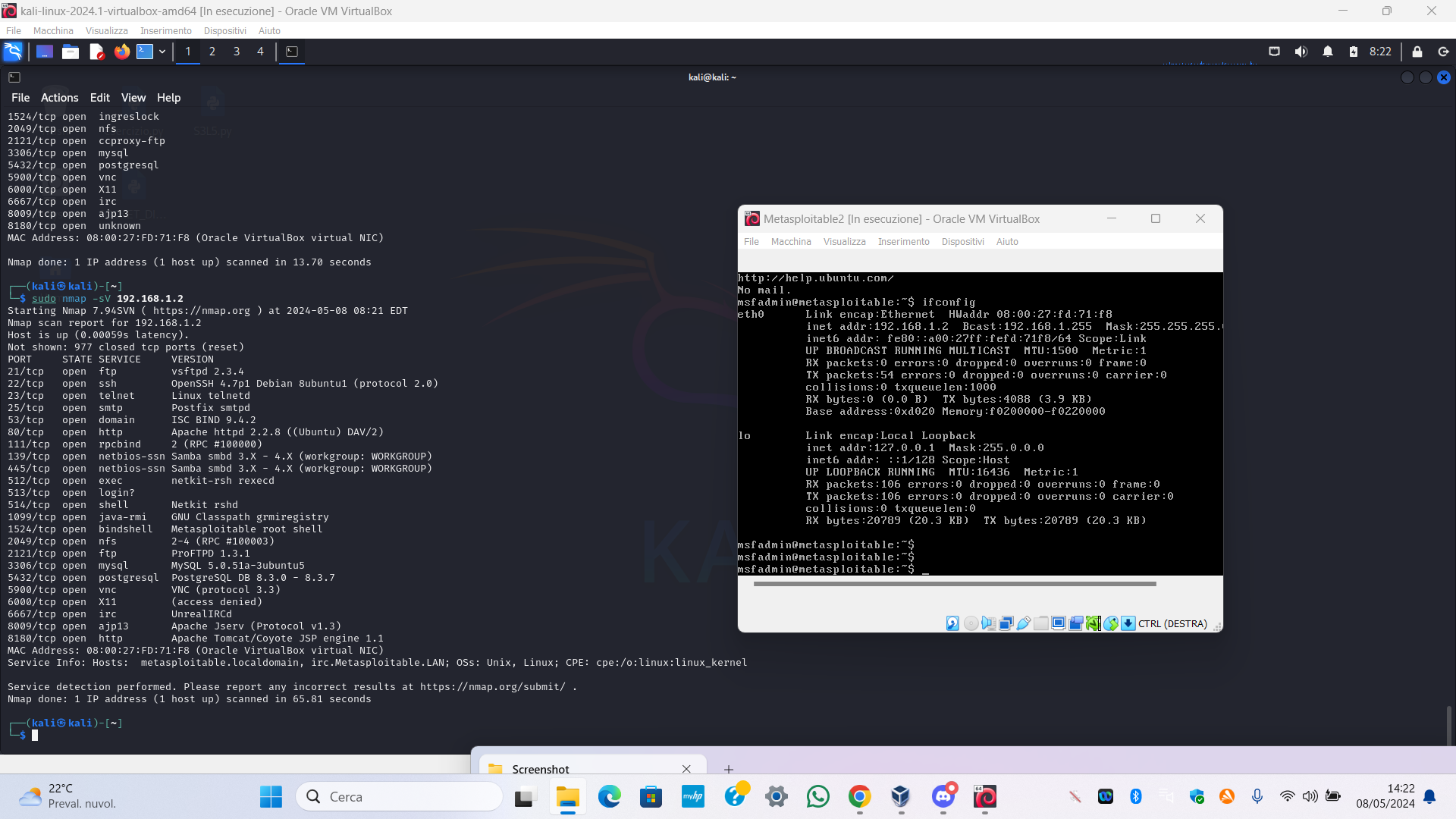
Nell’immagine sopra abbiamo utilizzato il comando più comune di nmap ovvero OS Fingerprint (tramite il comando “nmap -O”), che ci restituisce il sistema operativo della macchina target, tuttavia con un errore: la macchina in esame è Metasploitable. Negli esempi successivi vedremo che esistono altri tipi di analisi più approfonditi (in particolare “nmap –sV”) che compiono un’analisi più approfondita sulla macchina target. Il programma, poi, ci restituisce anche il MAC address del dispositivo specificando che si trova all’interno di una macchina virtuale. Oltre a questo, possiamo notare che vengono esplicitate tutte le porte aperte con i relativi servizi in funzione su quelle specifiche porte (es. porta 21 con protocollo ftp: aperta ecc….)

Proviamo ora ad effettuare un Syn scan e un TCP connect.



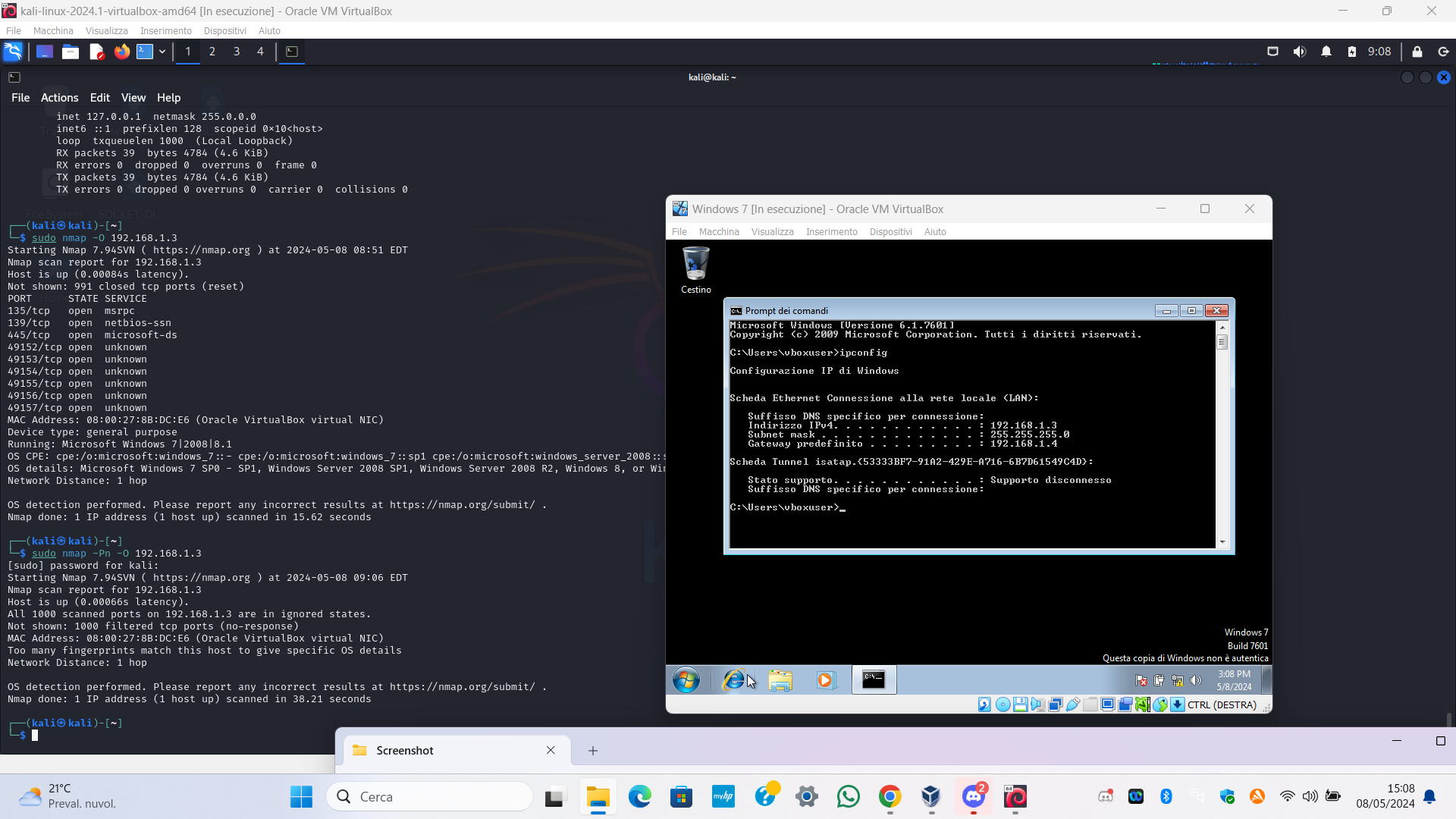
Naturalmente, i risultati che ci vengono restituiti non cambiano dalle due scan non cambiano tra loro.

Proviamo ora ad effettuare un Version detection (tramite il comando “nmap –sV”). Si tratta di un comando molto importante poiché restituisce le versioni dei programmi che sono in funzione su ogni porta aperta, mettendone in evidenza eventuali vulnerabilità.



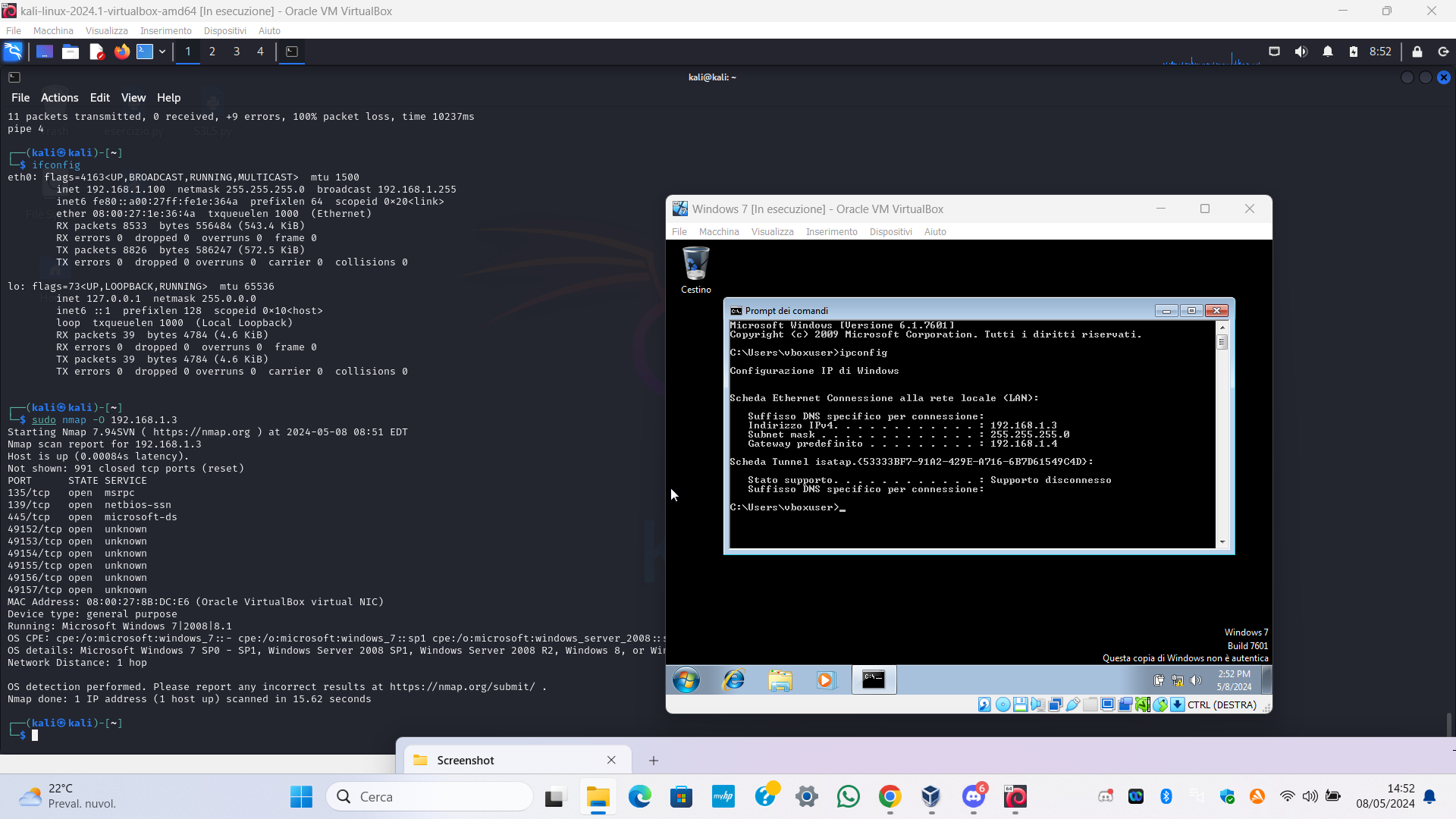
Come possiamo osservare, questa è un’analisi piuttosto approfondita (infatti stavolta è stato determinato correttamente che la macchina in esame è Metasploitable).

Vediamo adesso una scansione OS fingerprint su Windows 7:

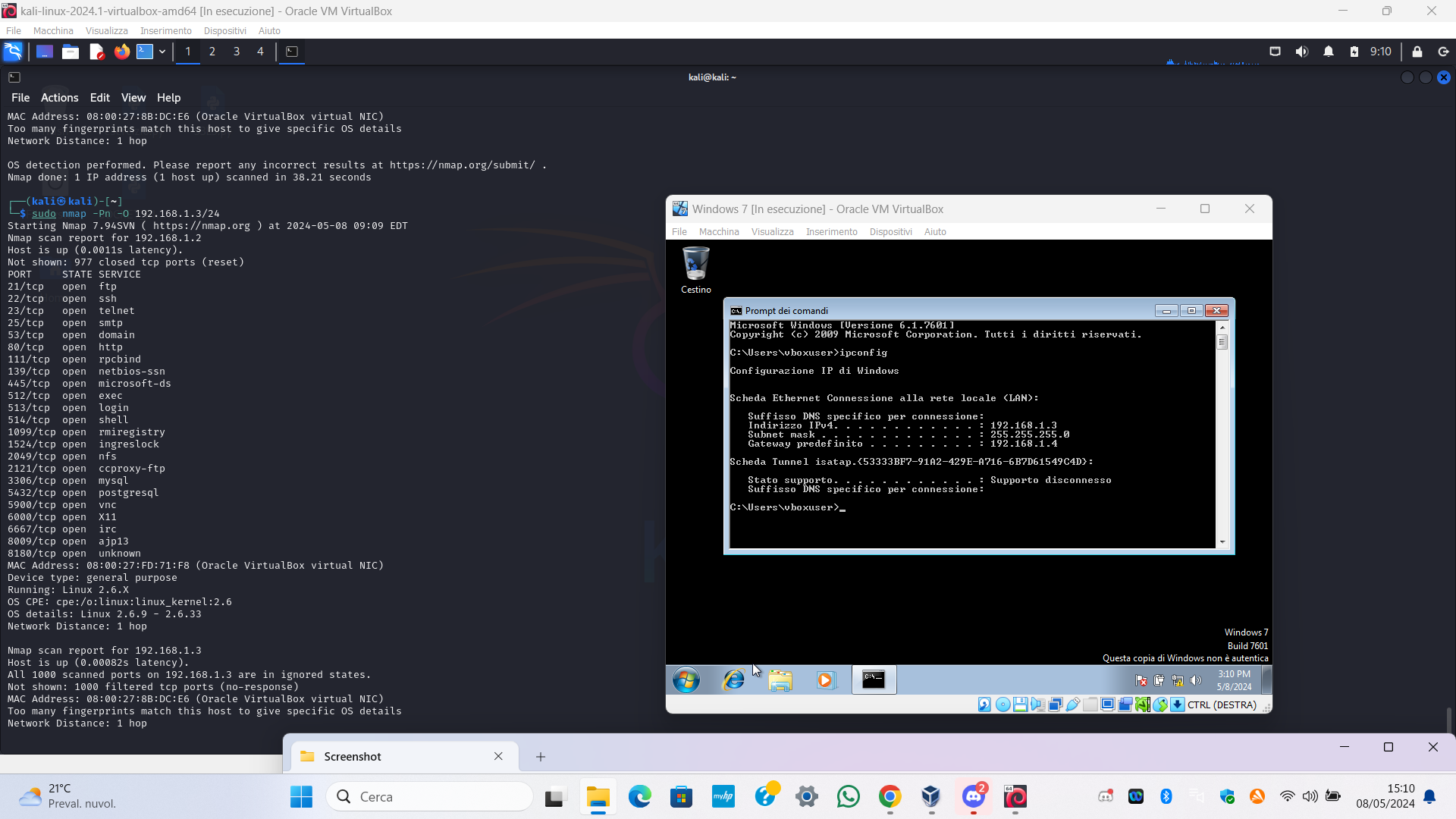


Qui possiamo osservare come, nonostante Kali e Windows siano sulla stessa rete, Kali non riesce ad effettuare correttamente la scansione. In effetti Windows ha in questo momento il firewall attivo e pertanto viene bloccato l’invio di pacchetti da parte di Kali.

Naturalmente la scansione va a buon fine se disattiviamo il firewall di Windows:



C’è però un altro modo per aggirare il firewall ed eseguire correttamente lo scan: attraverso il comando “nmap –Pn –O”.



Lo scan è avvenuto con successo, nonostante Windows firewall sia attivo.