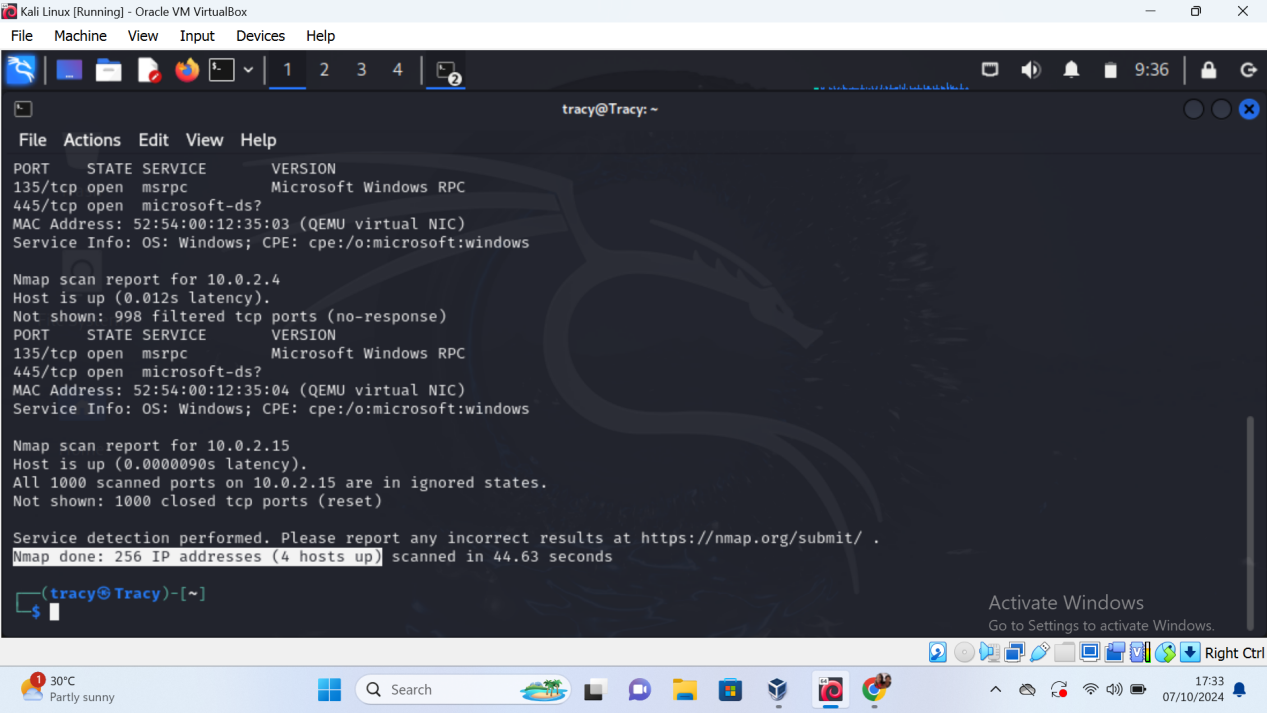
# ACYBERSECURITY MOD2

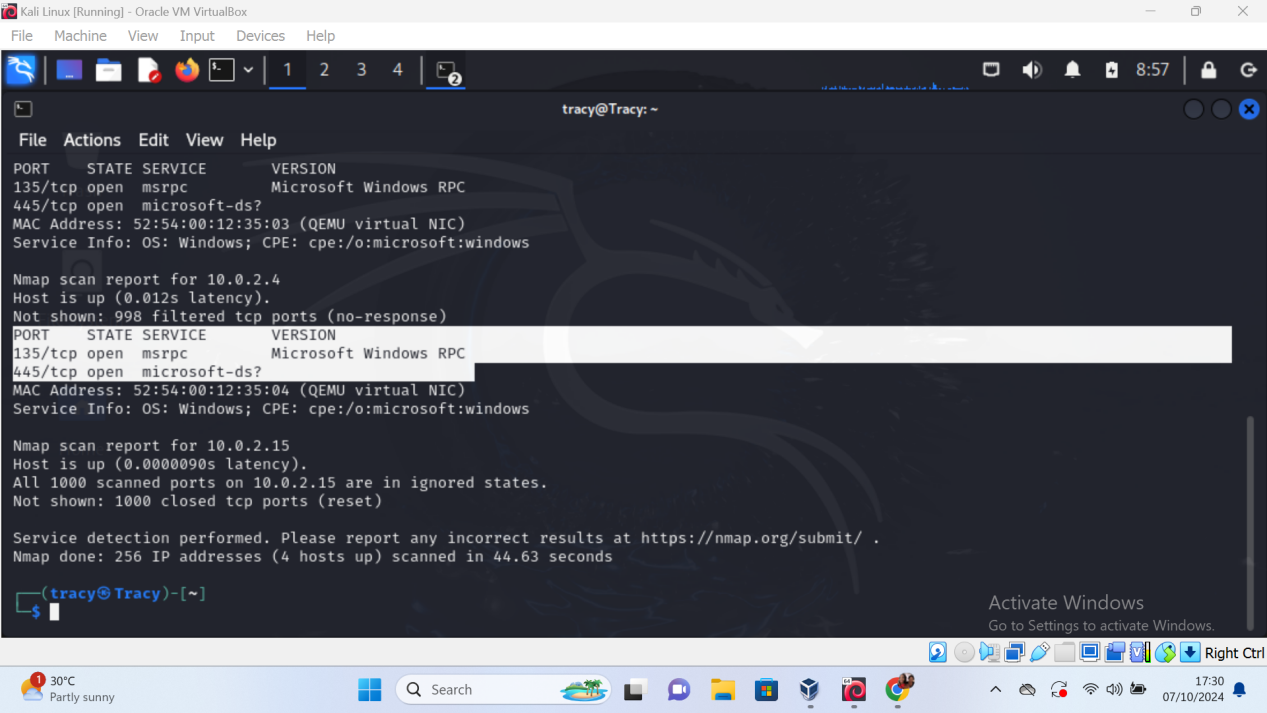
## NMAP

A network map is a well known cybersecurity tool that shows all devices connected to a particular network, what devices are connected, also discloses open ports which can be exploited.

I decided to explore the tool by running commands on the Linux operating system in a virtual machine. By no way should you run nmap in your local OS because you might just set your network up for hackers to exploit any vulnerabilities and trust me that isn’t what you’d want. It can cause more damage on your end



On this screenshot you are able to see all the scanned ports that are available on my IP address. Out of 256 hosts only 4 hosts were found to be up. They are port 135 and 445 which are transport communication protocols.



The script used to run is:

$nmap -sV (ip address)