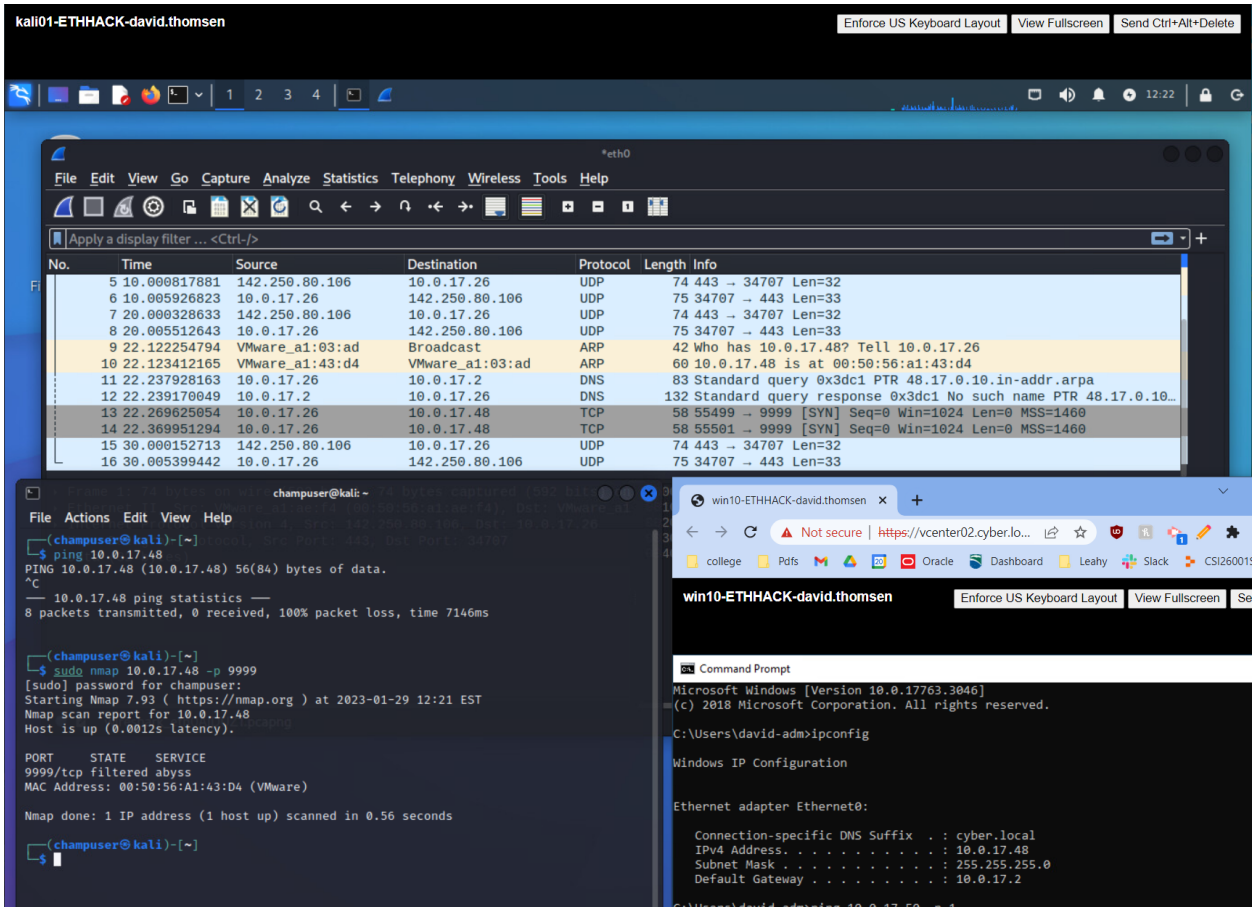
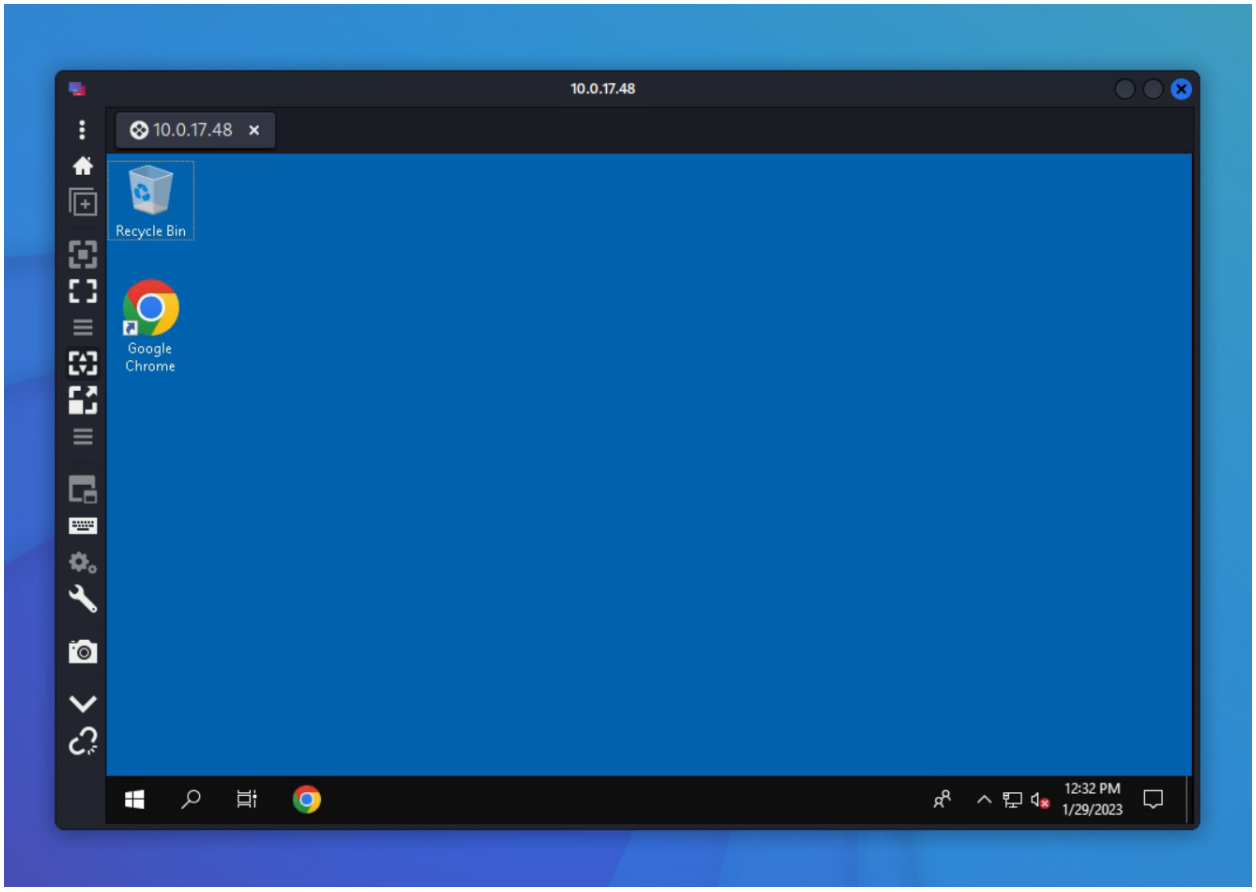
Deliverable 1. Observe and repeat the following interaction between kali and your win10 system (substitute your IP addresses). Provide screenshot(s) similar to the one below that show:



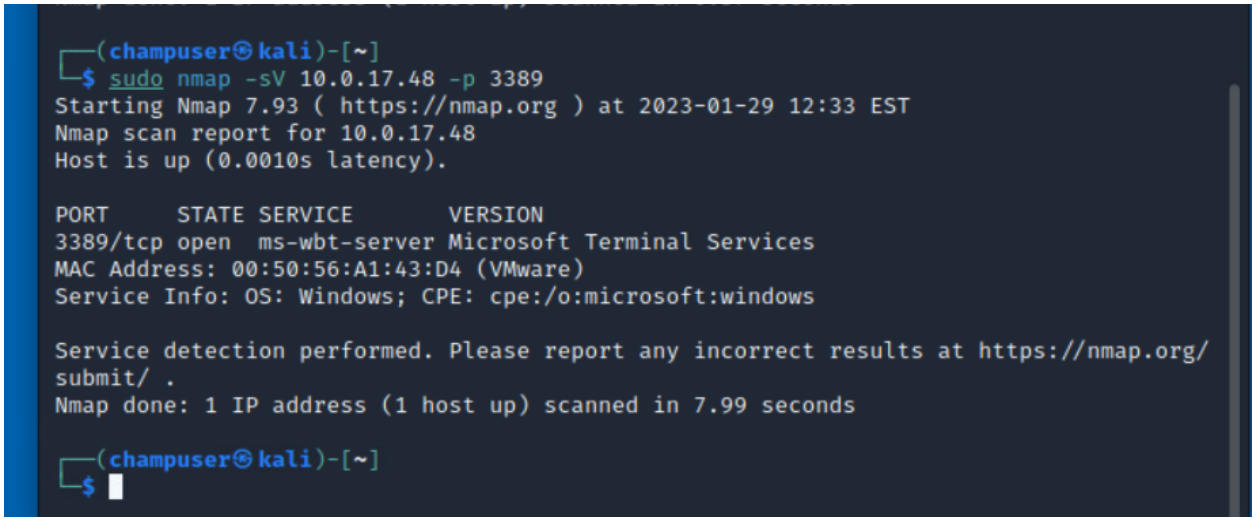
Deliverable 2. Figure out how to enable Remote Desktop Services on your windows 10 system using the gui, powershell or the command prompt and conduct an nmap scan against the rdp tcp port from your kali system. Show the nmap command and results similar to the one below.(make sure to document this in your tech journal)

```
┌──(champuser㉿kali)-[~]
└─$ sudo nmap 10.0.17.48 -p 3389
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-29 12:25 EST
Nmap scan report for 10.0.17.48
Host is up (0.0011s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:A1:43:D4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

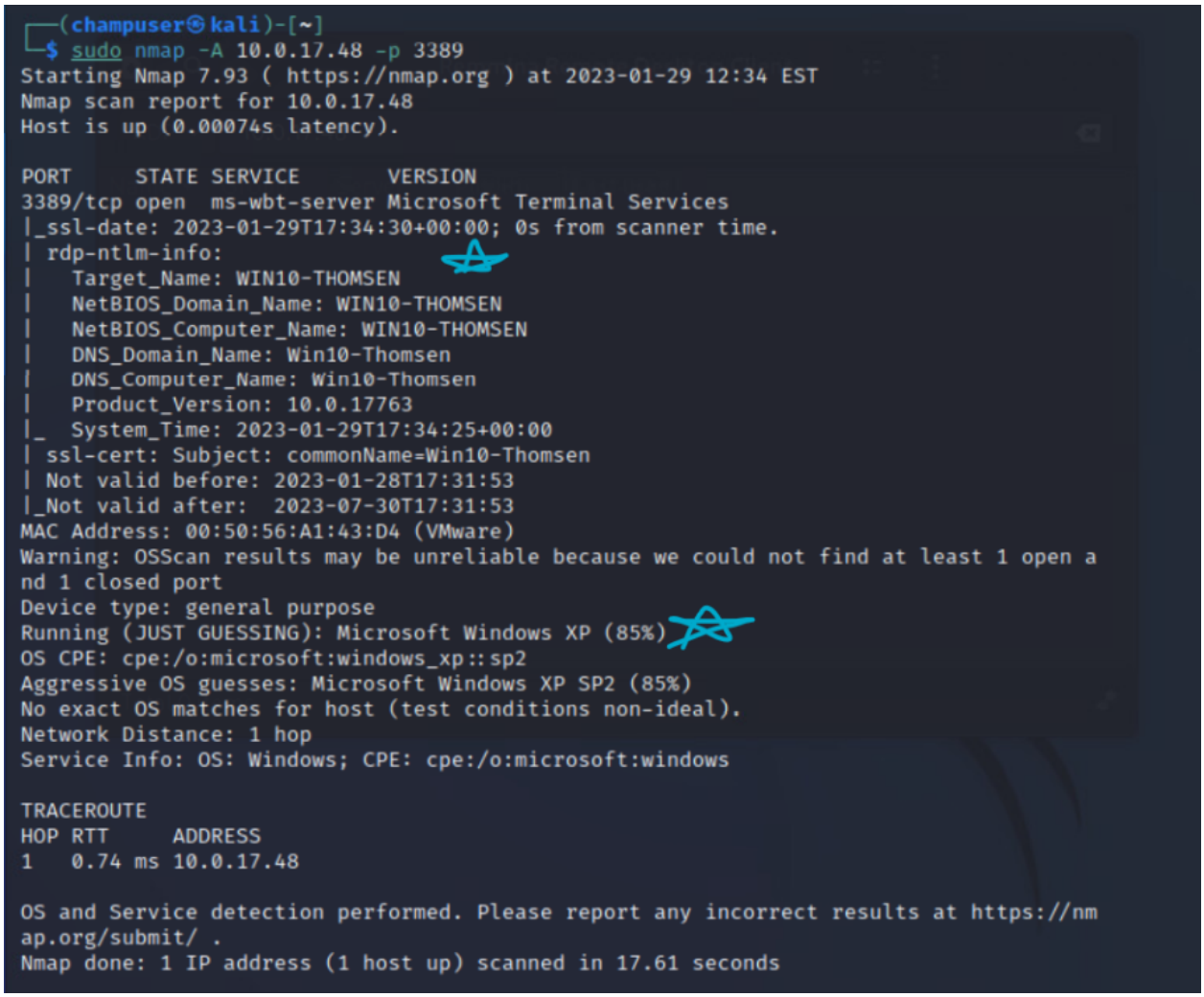
Deliverable 3. On Kali, make sure remmina is installed and figure out how to initiate an RDP session to your windows box. Provide a screenshot similar to the one below.



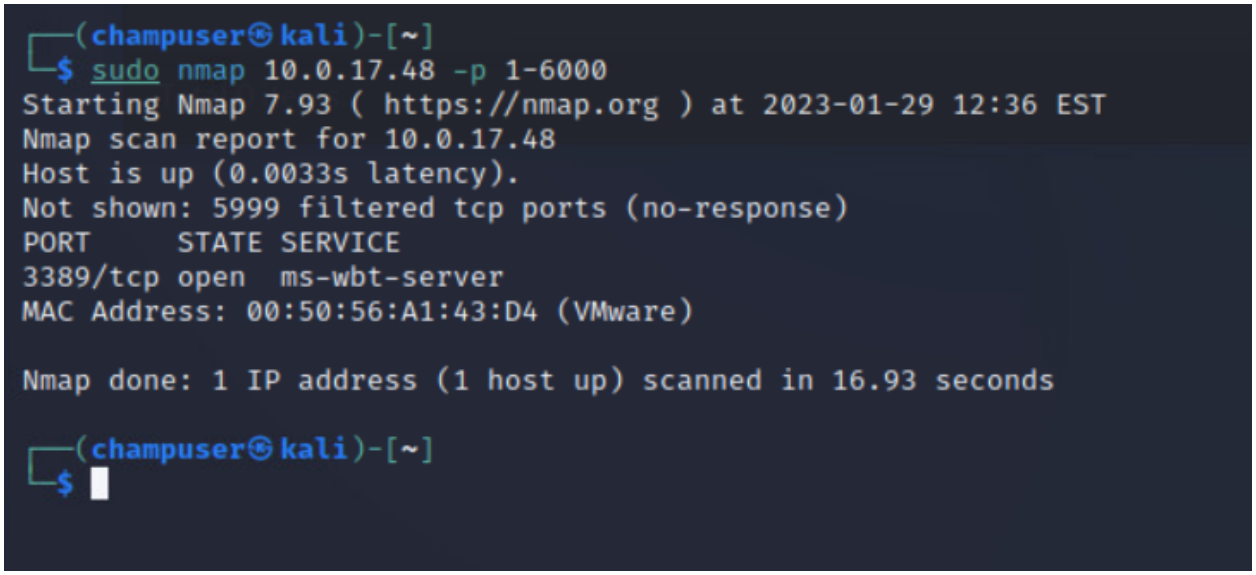
Deliverable 4. Add the -sV flag to your previous nmap scan against rdp on windows 10 and provide a screenshot similar to the one below (include your nmap command). You will note a bit more verbiage than seen without the flag.



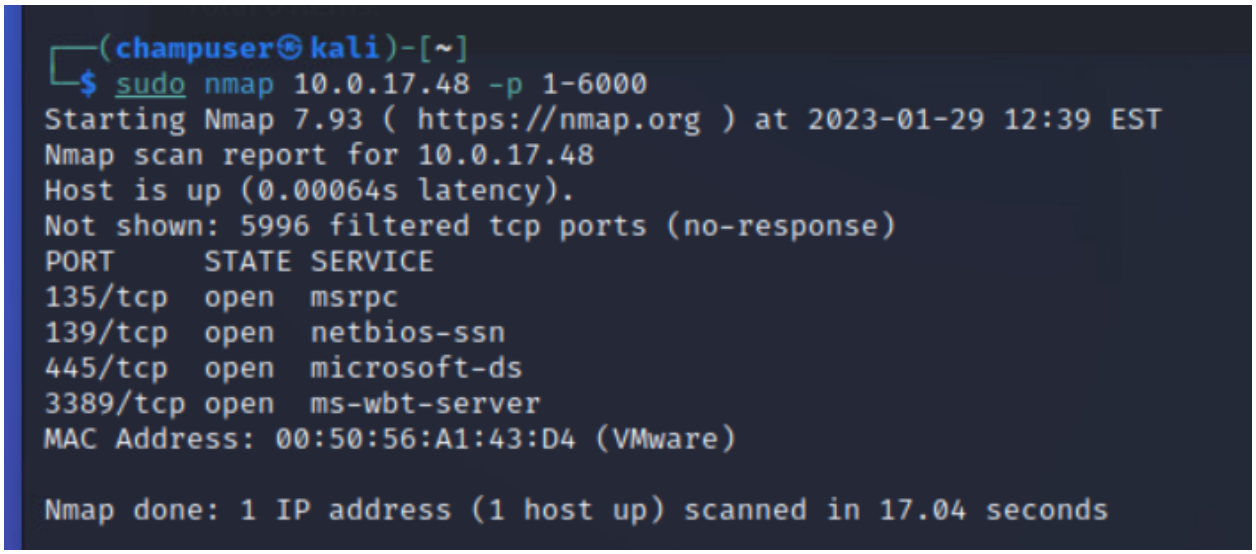
Deliverable 5. Replace -sV with -A to attempt to derive more information on the host and exposed service. Provide a screenshot similar to the one below. You will notice that the rdp-ntlm-info script provides a good deal of information (1) and that the OS detection output is not very accurate at all.



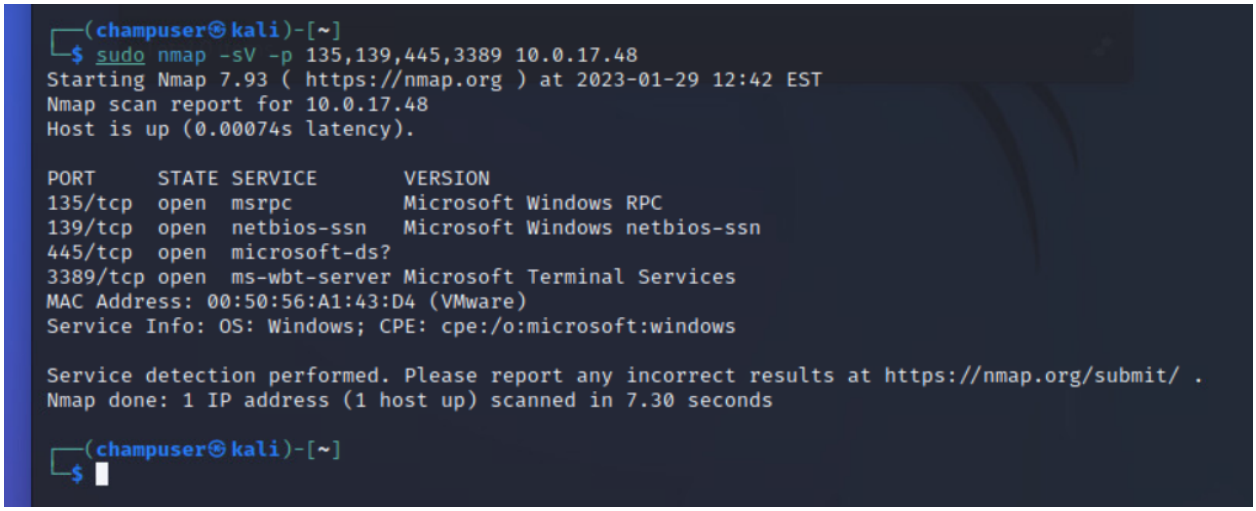
Deliverable 6. Run an nmap scan against your windows 10 system. Only target tcp ports 1-6000. Provide a screenshot showing your command and output.



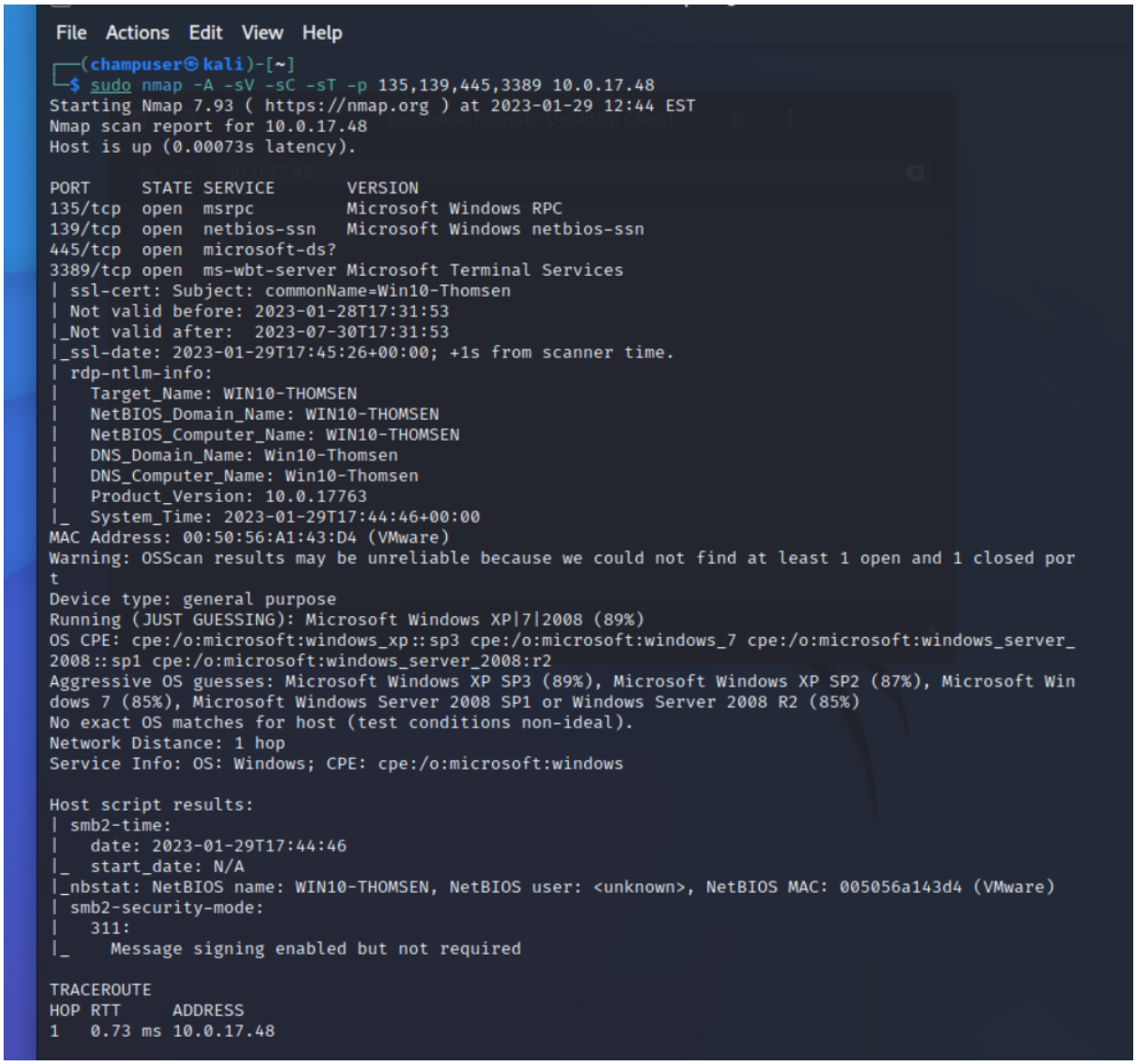
Deliverable 7, Rescan ports 1-6000. Provide a screenshot similar to the one below that shows your command and results. You will note that 3 new ports have been exposed.



Deliverable 8. Figure out how to run a version scan against only the ports exposed above. Provide a screenshot showing your nmap command and the output similar to the one below.



Deliverable 9. Increase the output by running OS Detection, Version Detection, Script Scanning and traceroute against the exposed ports from your previous scan. Provide a screenshot showing your command and output similar to the one below. You will notice we have smb and netbios related information



GIT: https://github.com/dthomsen116/SEC-335/wiki/Lab-2.2---Port-Scanning-2