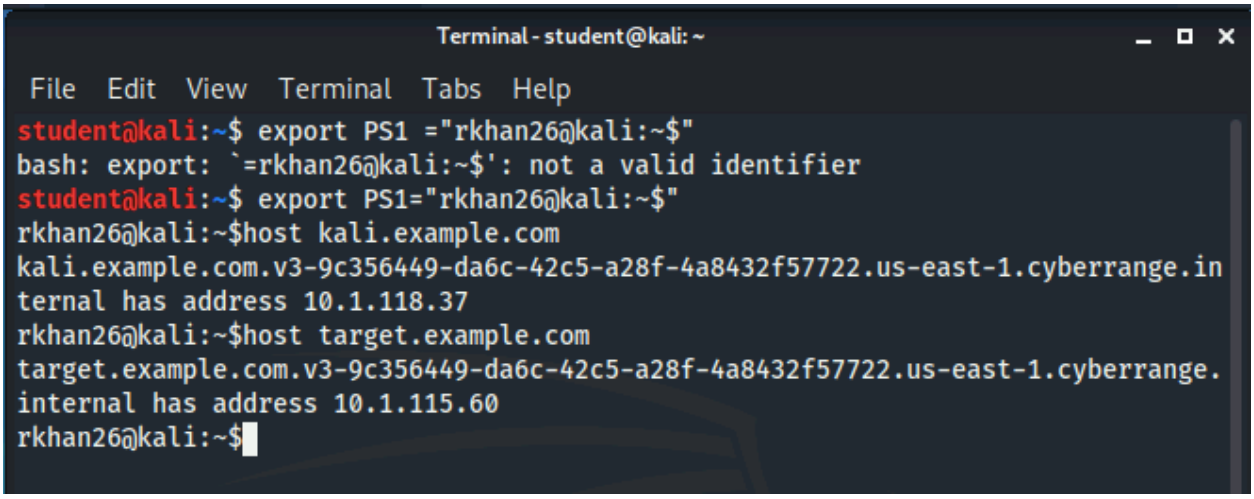
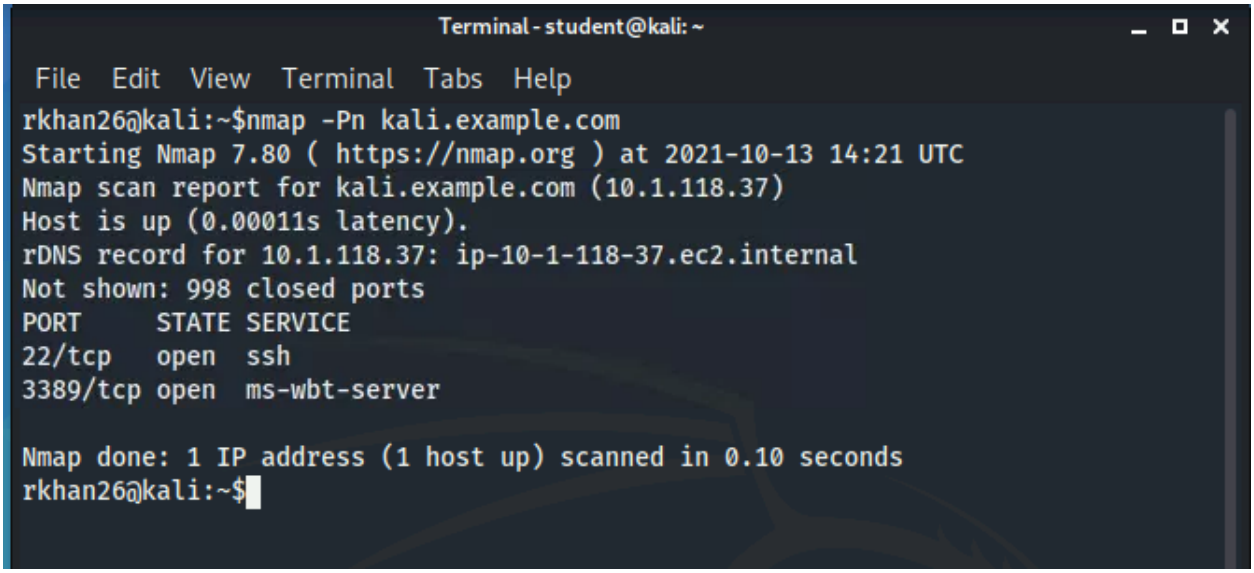
Roozah Khan
Laboratory Exercise 4 - Defending Against Public WiFi Hacker Attacks in Airports

**Task 3.5**



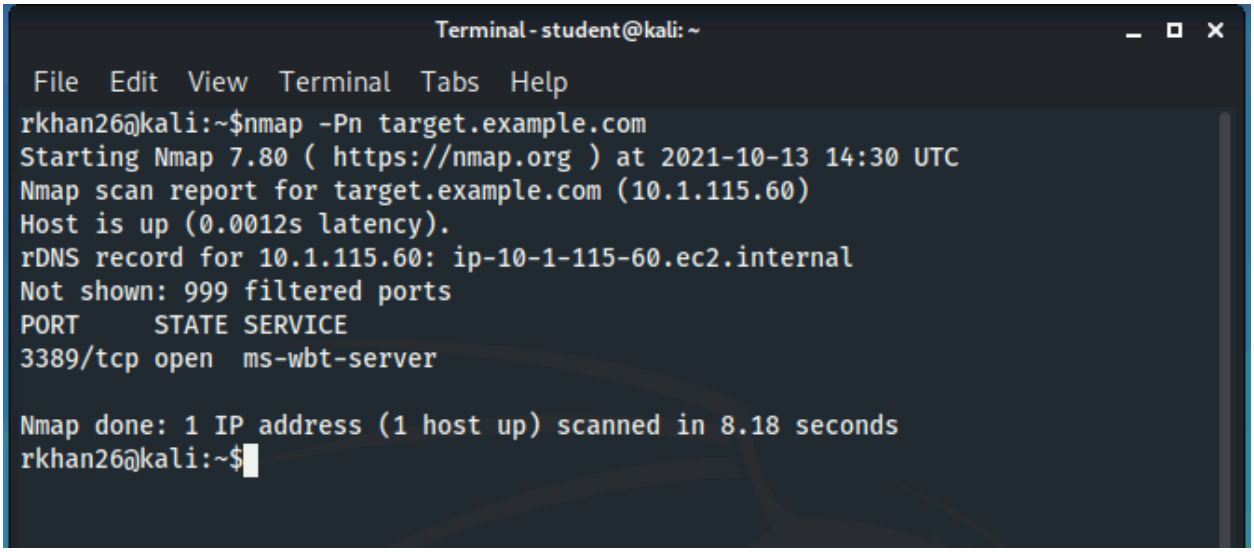

Kali Linux IP address: 10.1.118.37
Windows Target IP address: 10.1.115.60

**Task 4.1**



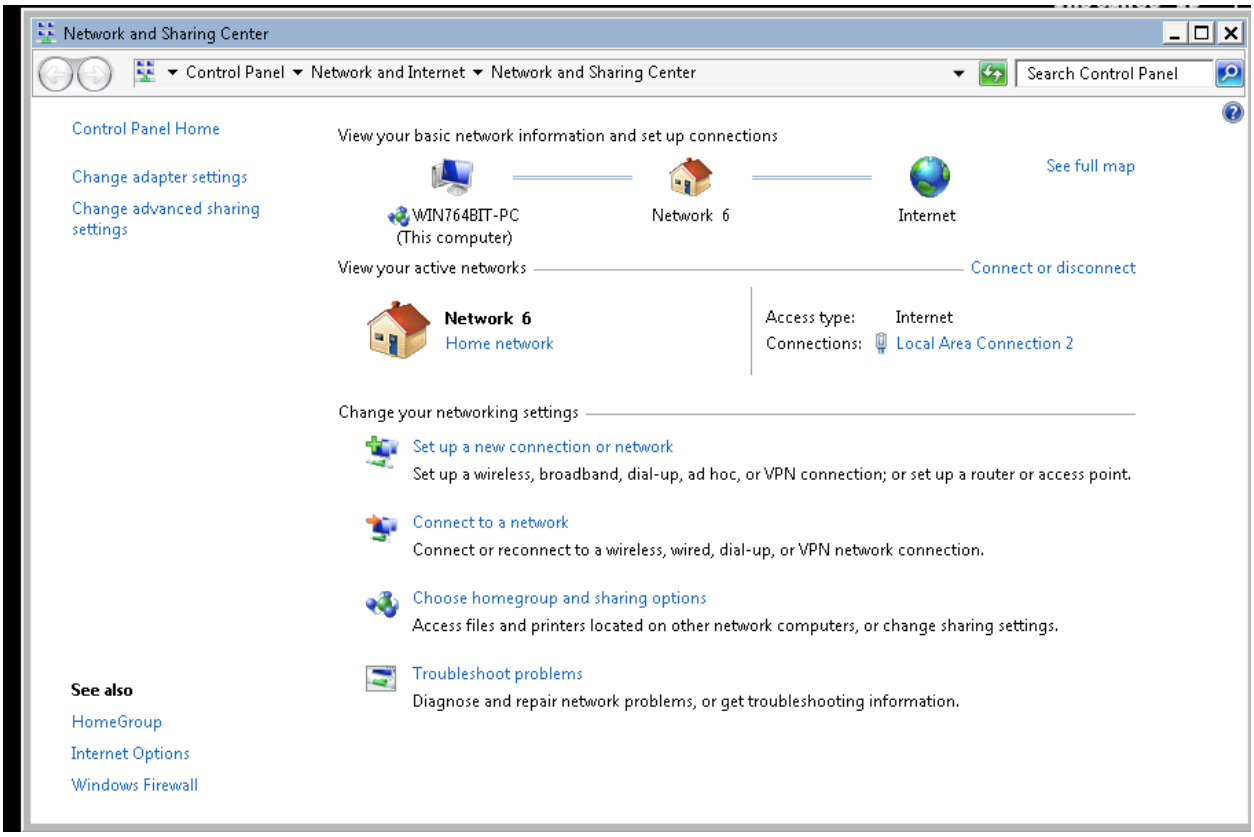

The ports that are exposed in my kali linux machine are port 22 and port 3389.

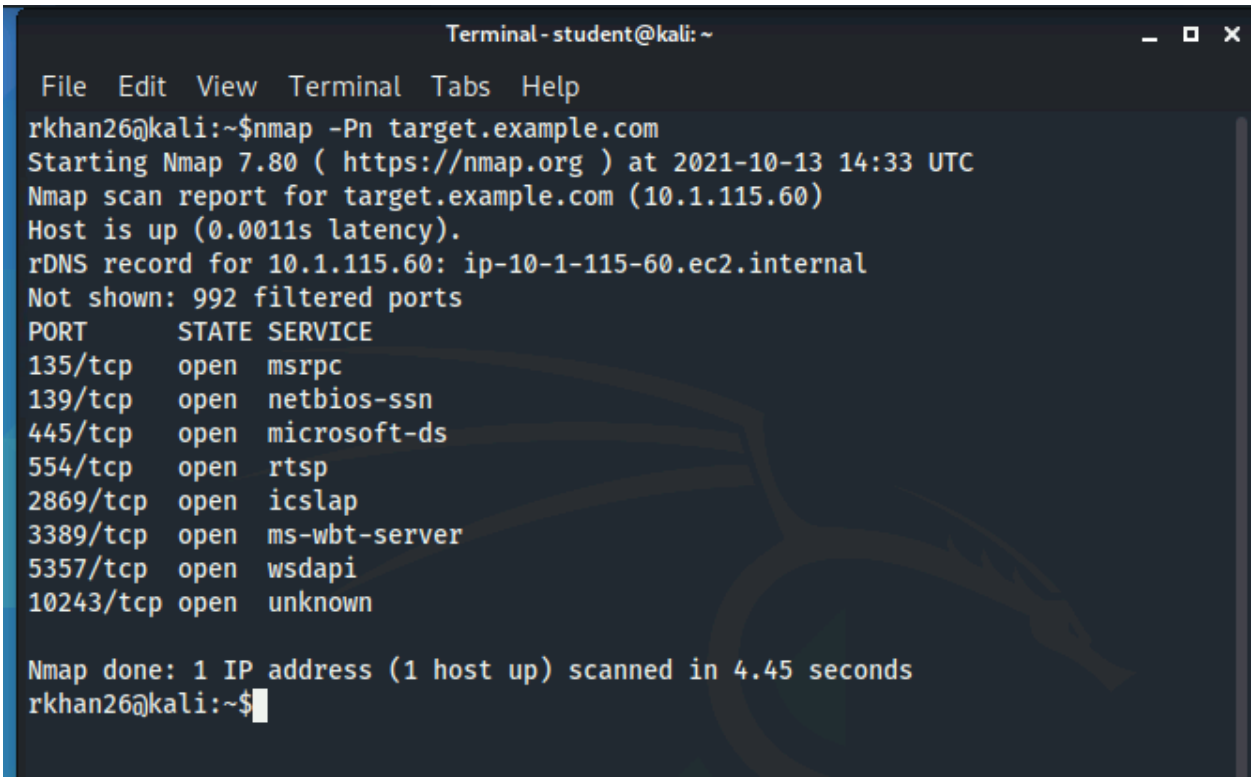
**Task 4.2**




Port number 3389 is still exposed on the windows VM.

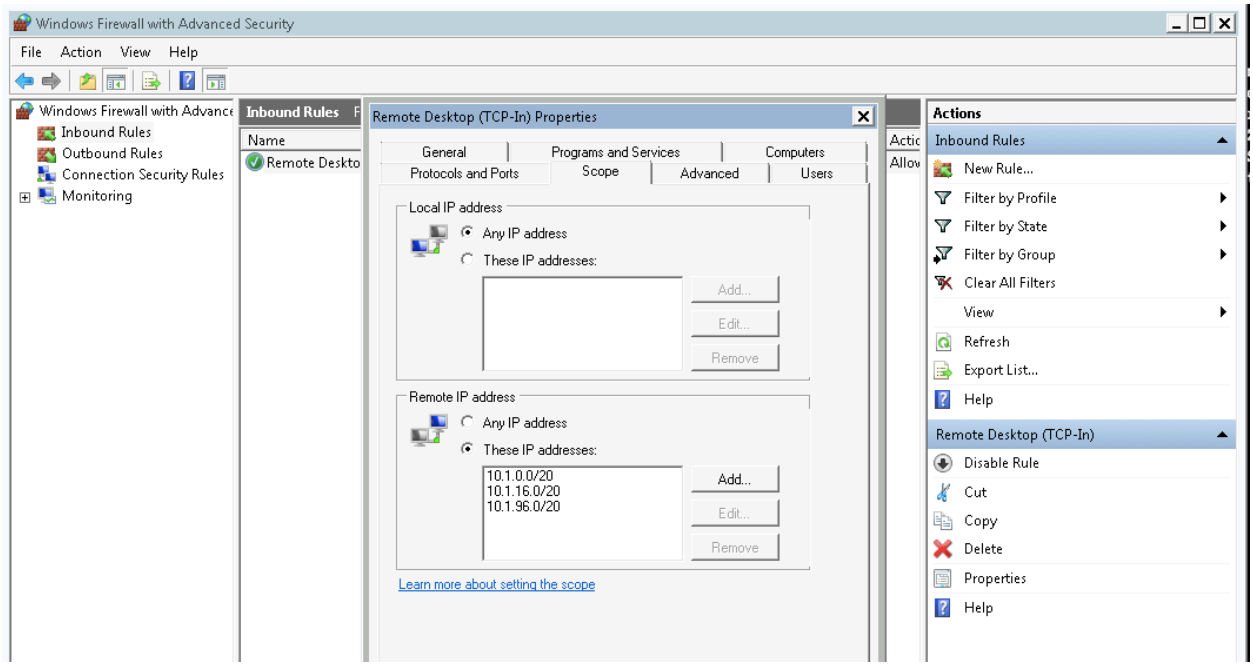
**Extra Points 4.2**





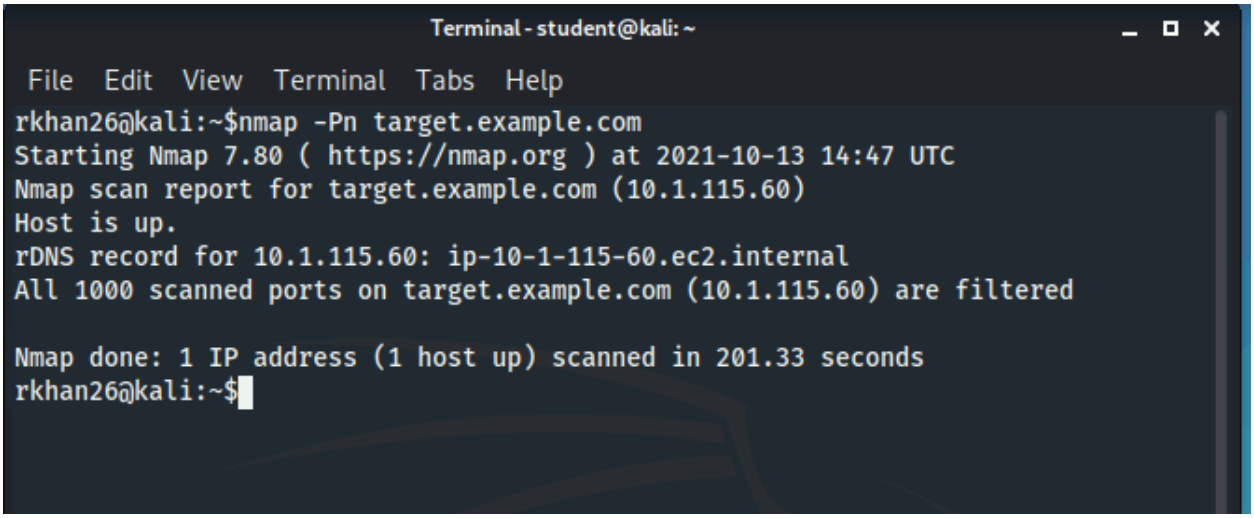

I searched “network and sharing center” in the Windows start button and changed from Public to home network mode. I scanned the Windows VM again and these are the ports that are now open in the screenshot above.

## Task 4.3



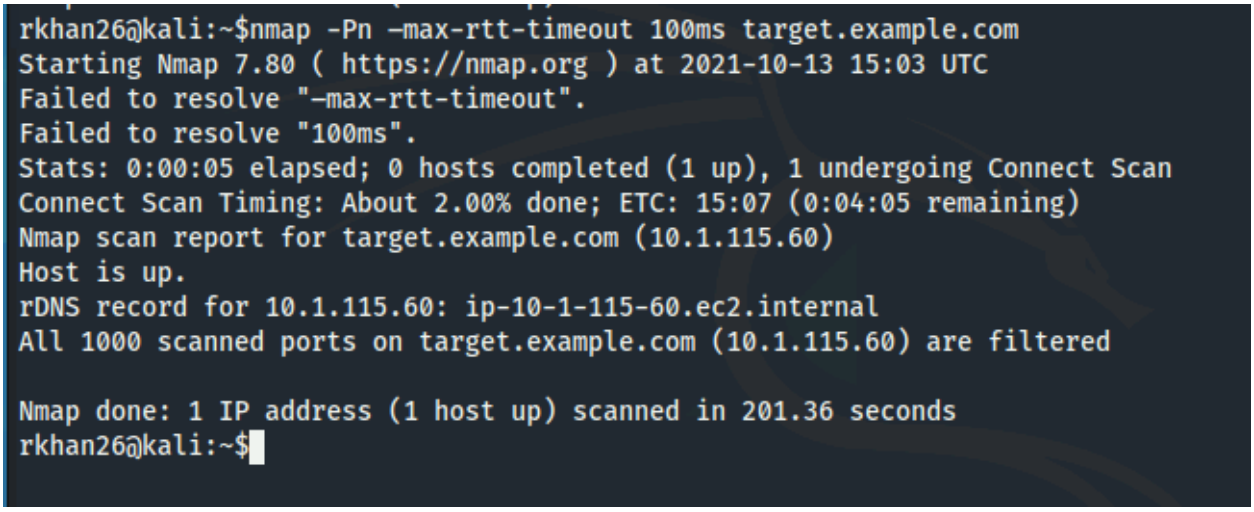

I went to “Firewall with advanced security” application and clicked on inbound rules then clicked on filter by group where I selected “filter by remote desktop.” I double clicked on what showed up and then clicked on the “scope” tab where I selected “These IP addresses” under “Remote IP address” then I clicked on “add” where I added the 3 IP addresses and clicked on “Apply” then “OK.”

**Task 4.4**




The scan showed that all 1000 ports are filtered on the windows target machine and 1 host is up.

It took 201.33 seconds which is about 3 minutes for it to scan with the regular nmap command.




I used the nmap 100ms command to force it to be faster, but for some reason it did not work.

It took a ms longer than the regular scan. It took 201.36 seconds which is about 3 minutes.