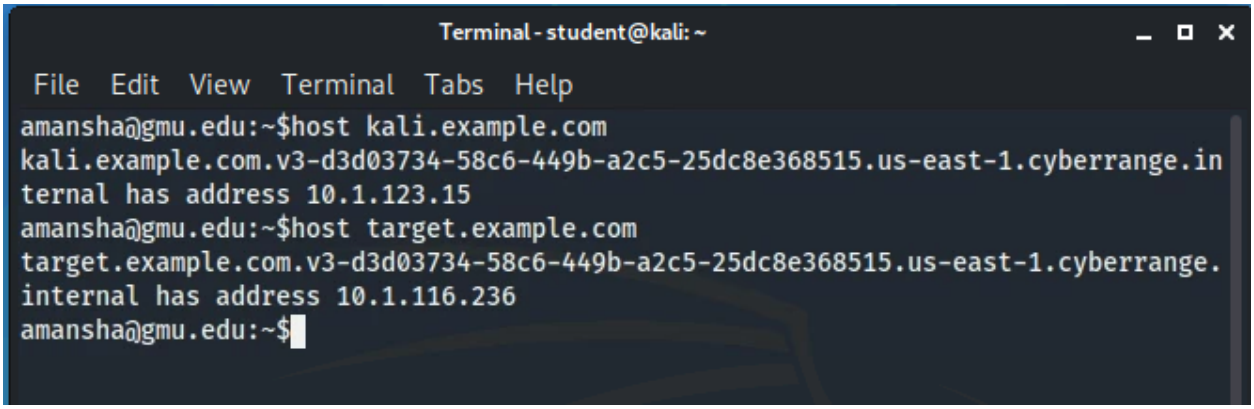
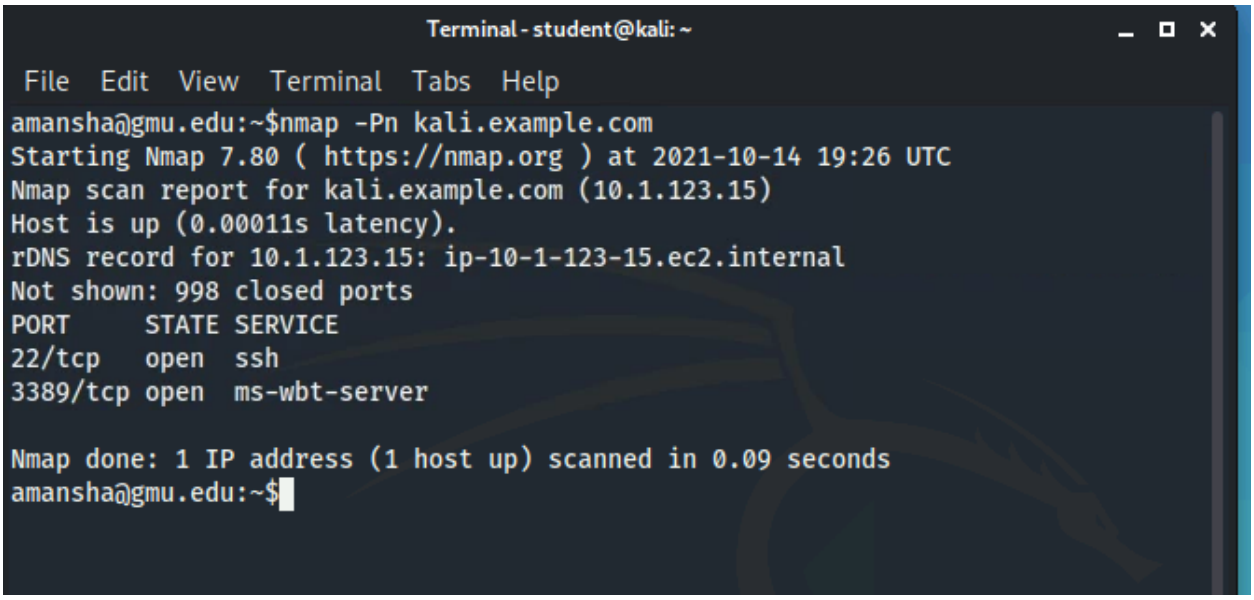
Amir Mansha
Lab #4
CYSE 425

3.5



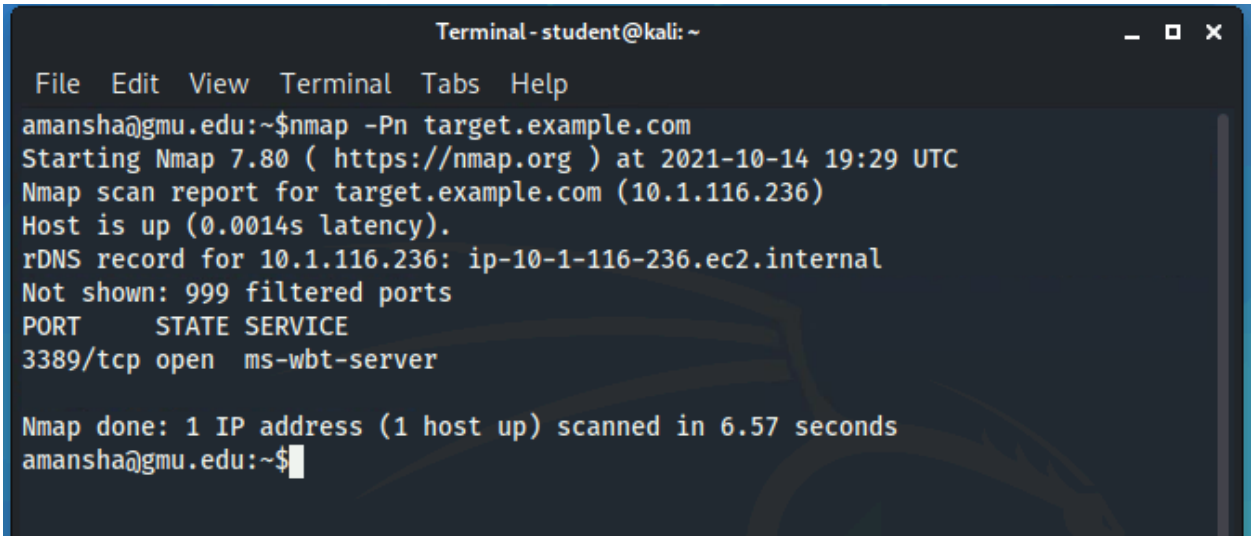
Ip address for Kali: 10.1.123.15
Ip address for target: 10.1.116.236

4.1

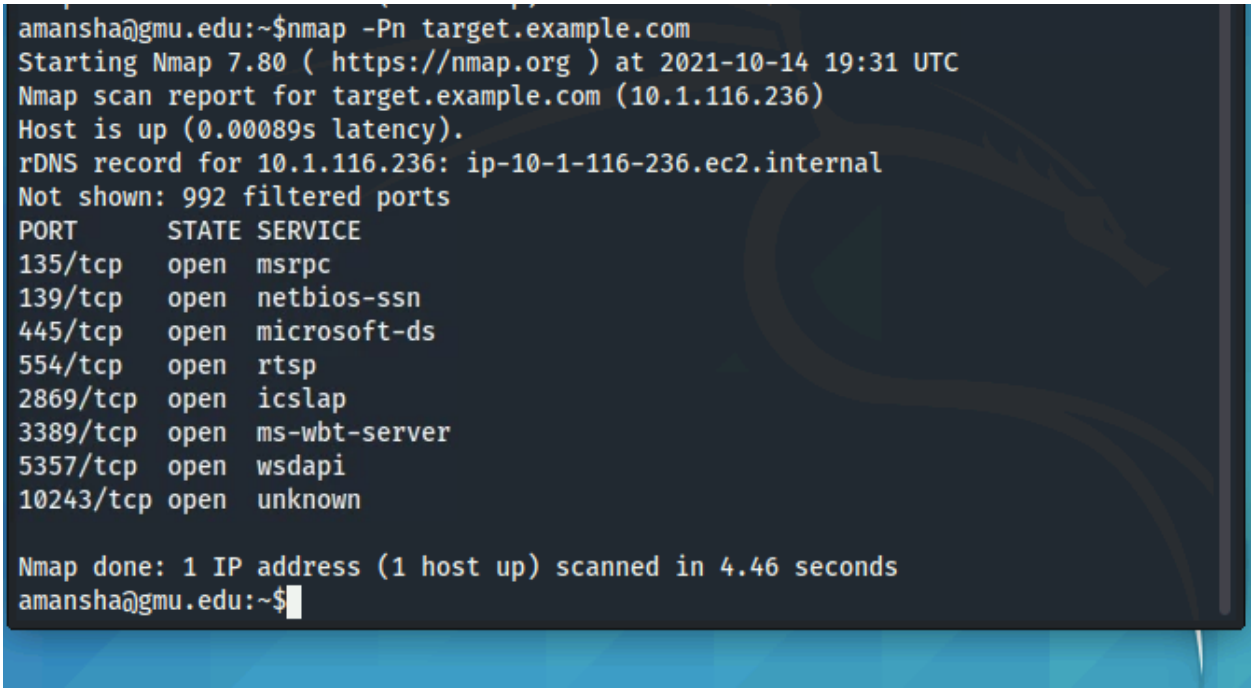


Port 22 and 3389 are exposed on kali machine.

4.2

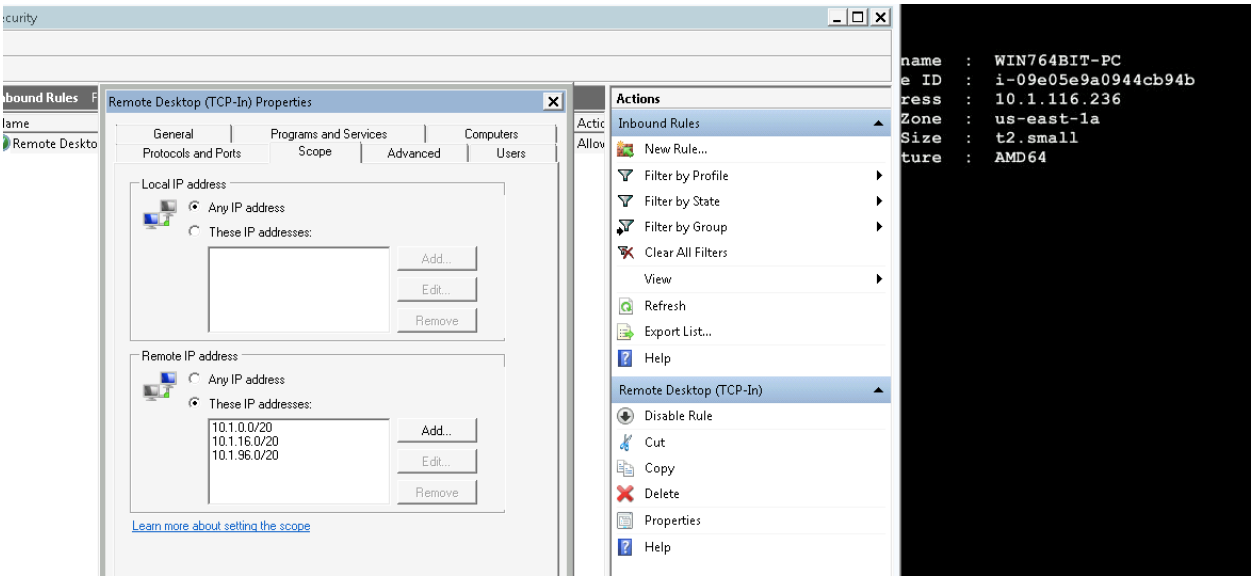


Port # 3389 is still exposed in windows target machine



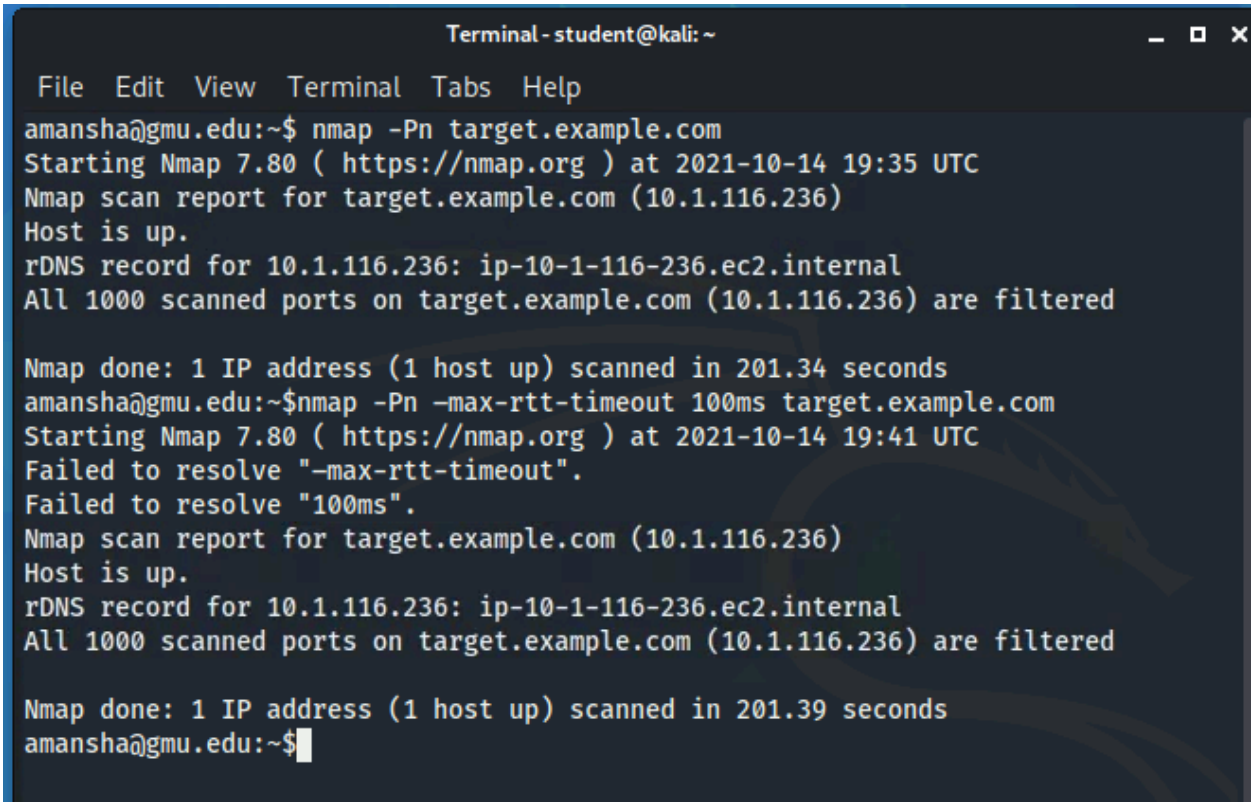
The ports in the above screenshot are now open after I switched to the Home network mode.

4.3



I added these IP addresses under Remote IP address in firewall settings.

4.4



The scan showed that all 1000 scanned ports on the target machine are filtered. And 1 IP address is scanned.
It took 201.34 seconds for nmap to scan and the 100ms scan 201.39 seconds.

Class Discussion:

If I was a hacker, I would utilize the port scan knowledge to my advantage by scanning what ports are open and listening to find vulnerable systems. If I was a defender, I would enable firewall so only chosen ports go through.

The pros are that that incoming threats cannot go through the 3389 port since it is remote desktop protocol. The con is that now you can RDP into the port since it is closed.

Network cannot be trustworthy. If someone scan your ports and find a system vulnerable then your LAN is compromised.