

Amir Mansha  
Lab #4  
CYSE 425

3.5

```
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
amansha@gmu.edu:~$host kali.example.com
kali.example.com.v3-d3d03734-58c6-449b-a2c5-25dc8e368515.us-east-1.cyberrange.in
ternal has address 10.1.123.15
amansha@gmu.edu:~$host target.example.com
target.example.com.v3-d3d03734-58c6-449b-a2c5-25dc8e368515.us-east-1.cyberrange.
internal has address 10.1.116.236
amansha@gmu.edu:~$
```

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

4.1

```
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
amansha@gmu.edu:~$nmap -Pn kali.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 19:26 UTC
Nmap scan report for kali.example.com (10.1.123.15)
Host is up (0.00011s latency).
rDNS record for 10.1.123.15: ip-10-1-123-15.ec2.internal
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp   open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
amansha@gmu.edu:~$
```

Port 22 and 3389 are exposed on kali machine.

## 4.2

```
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
amansha@gmu.edu:~$nmap -Pn target.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 19:29 UTC
Nmap scan report for target.example.com (10.1.116.236)
Host is up (0.0014s latency).
rDNS record for 10.1.116.236: ip-10-1-116-236.ec2.internal
Not shown: 999 filtered ports
PORT      STATE SERVICE
3389/tcp   open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
amansha@gmu.edu:~$
```

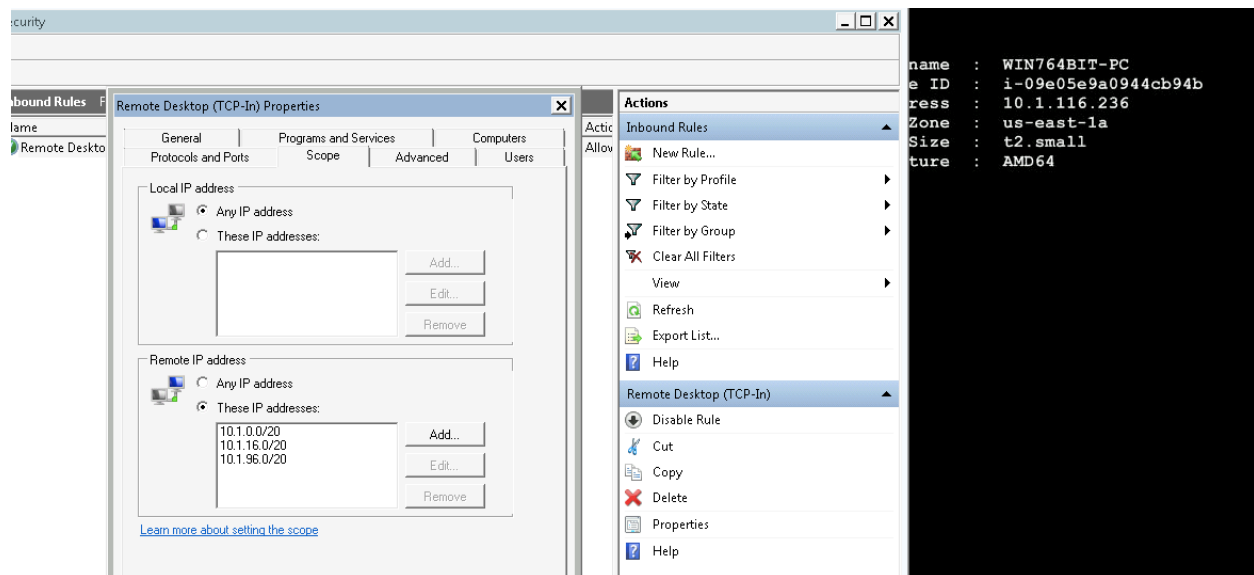
Port # 3389 is still exposed in windows target machine

```
amansha@gmu.edu:~$nmap -Pn target.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 19:31 UTC
Nmap scan report for target.example.com (10.1.116.236)
Host is up (0.00089s latency).
rDNS record for 10.1.116.236: ip-10-1-116-236.ec2.internal
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
3389/tcp    open  ms-wbt-server
5357/tcp   open  wsdapi
10243/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
amansha@gmu.edu:~$
```

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

```

Terminal - student@kali: ~
File Edit View Terminal Tabs Help
amansha@gmu.edu:~$ nmap -Pn target.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 19:35 UTC
Nmap scan report for target.example.com (10.1.116.236)
Host is up.
rDNS record for 10.1.116.236: ip-10-1-116-236.ec2.internal
All 1000 scanned ports on target.example.com (10.1.116.236) are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.34 seconds
amansha@gmu.edu:~$ nmap -Pn -max-rtt-timeout 100ms target.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-14 19:41 UTC
Failed to resolve "-max-rtt-timeout".
Failed to resolve "100ms".
Nmap scan report for target.example.com (10.1.116.236)
Host is up.
rDNS record for 10.1.116.236: ip-10-1-116-236.ec2.internal
All 1000 scanned ports on target.example.com (10.1.116.236) are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.39 seconds
amansha@gmu.edu:~$

```

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.