

Roozah Khan

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

Task 3.5

```
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
student@kali:~$ export PS1="rkhan26@kali:~$"
bash: export: `=rkhan26@kali:~$': not a valid identifier
student@kali:~$ export PS1="rkhan26@kali:~$"
rkhan26@kali:~$ host kali.example.com
kali.example.com.v3-9c356449-da6c-42c5-a28f-4a8432f57722.us-east-1.cyberrange.in
ternal has address 10.1.118.37
rkhan26@kali:~$ host target.example.com
target.example.com.v3-9c356449-da6c-42c5-a28f-4a8432f57722.us-east-1.cyberrange.
internal has address 10.1.115.60
rkhan26@kali:~$
```

Kali Linux IP address: 10.1.118.37

Windows Target IP address: 10.1.115.60

Task 4.1

```
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
rkhan26@kali:~$ nmap -Pn kali.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-13 14:21 UTC
Nmap scan report for kali.example.com (10.1.118.37)
Host is up (0.00011s latency).
rDNS record for 10.1.118.37: ip-10-1-118-37.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 0.10 seconds
rkhan26@kali:~$
```

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

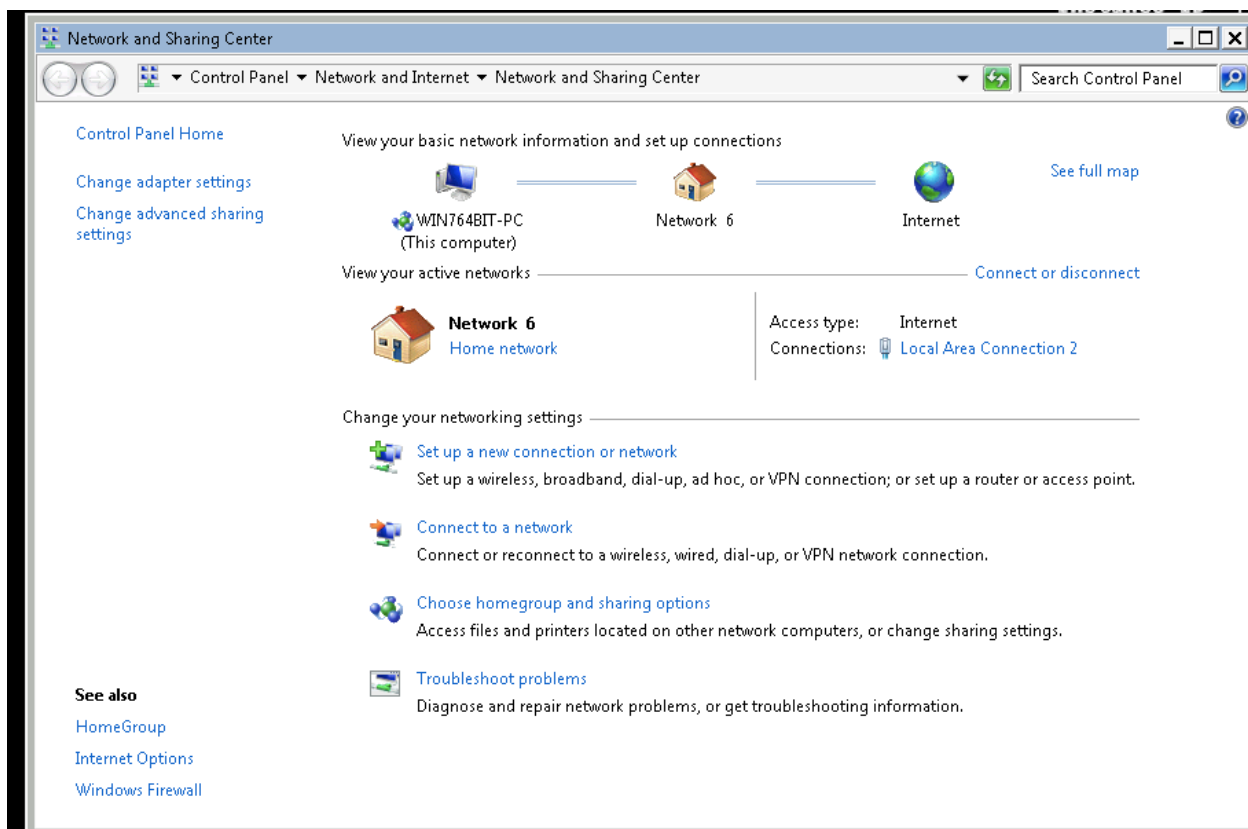
Task 4.2

```
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
rkhan26@kali:~$nmap -Pn target.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-13 14:30 UTC
Nmap scan report for target.example.com (10.1.115.60)
Host is up (0.0012s latency).
rDNS record for 10.1.115.60: ip-10-1-115-60.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 8.18 seconds
rkhan26@kali:~$
```

Port number 3389 is still exposed on the windows VM.

Extra Points 4.2

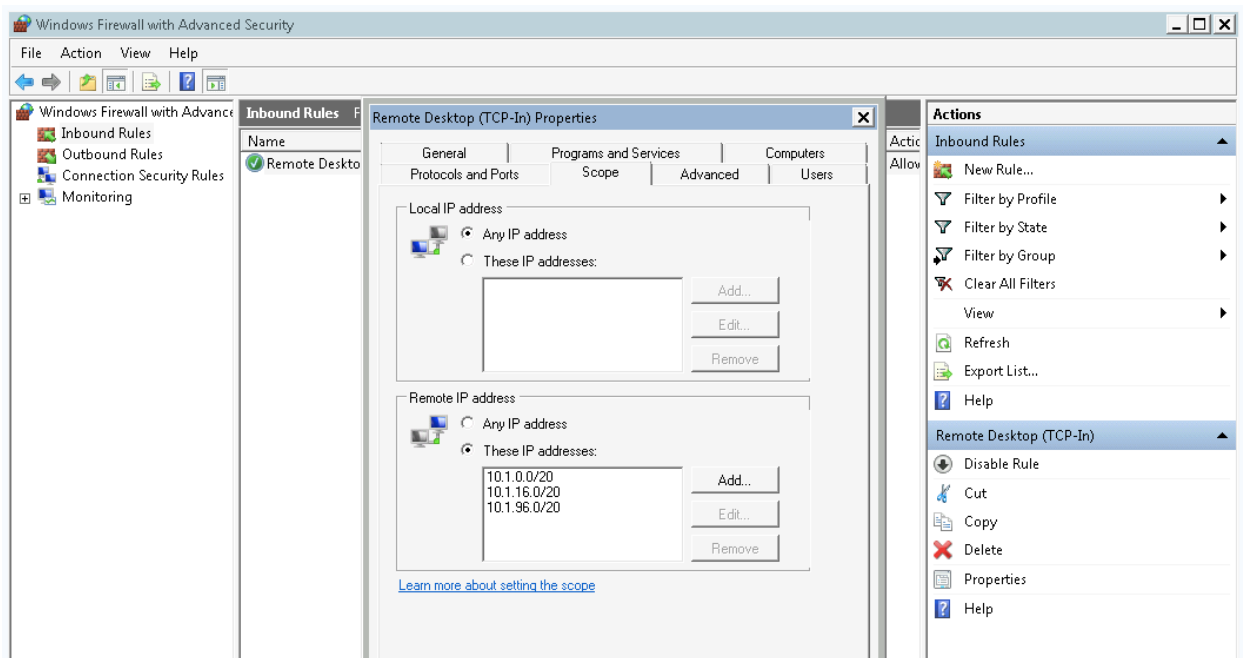


```
Terminal - student@kali: ~
File Edit View Terminal Tabs Help
rkhan26@kali:~$nmap -Pn target.example.com
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-13 14:33 UTC
Nmap scan report for target.example.com (10.1.115.60)
Host is up (0.0011s latency).
rDNS record for 10.1.115.60: ip-10-1-115-60.ec2.internal
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  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.45 seconds
rkhan26@kali:~$
```

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

```
Terminal - student@kali: ~  
File Edit View Terminal Tabs Help  
rkhan26@kali:~$nmap -Pn target.example.com  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-13 14:47 UTC  
Nmap scan report for target.example.com (10.1.115.60)  
Host is up.  
rDNS record for 10.1.115.60: ip-10-1-115-60.ec2.internal  
All 1000 scanned ports on target.example.com (10.1.115.60) are filtered  
  
Nmap done: 1 IP address (1 host up) scanned in 201.33 seconds  
rkhan26@kali:~$
```

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.

```
rkhan26@kali:~$nmap -Pn -max-rtt-timeout 100ms target.example.com  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-10-13 15:03 UTC  
Failed to resolve "-max-rtt-timeout".  
Failed to resolve "100ms".  
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 2.00% done; ETC: 15:07 (0:04:05 remaining)  
Nmap scan report for target.example.com (10.1.115.60)  
Host is up.  
rDNS record for 10.1.115.60: ip-10-1-115-60.ec2.internal  
All 1000 scanned ports on target.example.com (10.1.115.60) are filtered  
  
Nmap done: 1 IP address (1 host up) scanned in 201.36 seconds  
rkhan26@kali:~$
```

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.