Defending Against Public WiFi Hacker Attacks In Airports

1. Overview

What Students Will Learn:
Participants of this lab will gain experience and knowledge in *network administration*, *ports*, *protocols*, *IP addresses*, *port scanning* and *firewalling*. Participants should pair up with someone where one of you will play the "Black-Hat" attacker who will scan and attack an old, vulnerable (unpatched) Windows system for open ports and vulnerabilities, and the "White-Hat" defender will attempt to block and defend against these scans using the target system's host based or *personal (software) firewall* built into the OS.
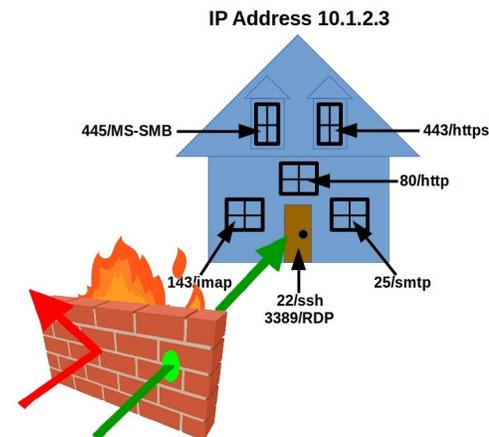
Lab Theory: Network *port scanners* are used by good guys and bad guys to identify and evaluate the status of ports and services running on a *host* or IP address, and *firewalls* are used to block unwanted access (or *scans*). If you imagine that a host or IP address is like a house in a "network neighborhood," and port numbers are like doors and windows on said "house," then ports represent the various ways of getting into a system via *service protocols* over the network.

Predefined and "well-known" ports are associated with the services (or protocols) that run *on* that port. For example, all unencrypted HTTP or web traffic being served from an Internet server is typically served over port 80, or port 80 is the pre-defined web traffic "window" into a web server.

Ports are like the doors and windows of an IP address

IP Address 10.1.2.3

445/MS-SMB · 443/https · 80/http · 143/imap · 22/ssh 3389/RDP · 25/smtp

As seen in the image (right), a firewall is a piece of hardware or software that is designed to block and allow traffic based on who (or what IPs) are trying to get in on specific service ports. Allowing a port or source IP through a firewall is casually called "poking a hole" (granting access), as illustrated in our house IP address image.

Malicious "Hackers" or "**Black-Hats**" *scan* and identify the open (or "unlocked") ports on target IP address or hosts by using a port scanner tool, and then expose what version of the service is running. Doing this reveals system *vulnerabilities* that can used to break in using *exploits* and hacker tools. Systems protected by a firewall can not be as easily scanned and probed back by Black-Hats.

Part of the job of Network/*System Administrators* or "**White-Hats**" is to secure open ports (unlocked doors and windows) on computer systems and networks, in part by configuring hardware or software firewalls to shield them from "Black-Hat" network scans.

> **WARNING:** *While scanning ports on systems is not a crime in most states, <u>always remember</u> that scanning a host (or a network full of hosts) is like walking down a street in your neighborhood and systematically rattle-checking every neighbor's house's doors and windows. No, it's not illegal, but someone is probably going to call the police and report you, or possibly charge you with trespassing. <u>ALWAYS GET PERMISSION of the host or network owner or admin before scanning a system or network.</u>*

VIRGINIA CYBER RANGE

2. Resources required

Virtual Machines (VMs) needed: Windows 7 and Kali Linux. The Kali Linux is the scanning VM and the Windows 7 is the target VM on the same network. If you do not have a Cyber Range account or do not have a Range courses invite, then see your instructor for an invite or access code.

3. Initial Setup
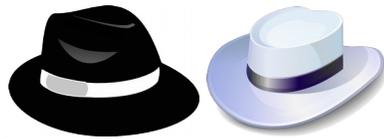
The scanning system Virtual Machine is kali.example.com and the target VM is aptly named target.example.com. Your two VMs are on the same virtual network in a "cloud network bubble" that can see and ping each other, but not touch any other student/instructor VMs or the outside (except over web proxy). In real life hacking attacks, Black-Hats will often utilize a variety of techniques (e.g., social engineering and security tools) to get onto the victim's network to discover and scan for such targets.

After logging into the cyber range and then navigating to this course and exercise, you will be opening up two remote desktop sessions within your browser. One browser tab will contain the Kali Linux desktop VM and the other tab with contain your desktop session to the target Windows desktop VM.

The Black-Hat will log into and work from the Kali Linux VM, kali.example.com .

The White-Hat will log into the Windows target VM, target.example.com .

3.1. **Log into the Cyber Range:** To log into the range for the first time, either click on the email invite sent to you by your instructor, or if you were provided an "invitation code" then point your browser to the link provided by your instructor to use it. At the Range Login window, select the "Have an invitation code?" link, paste in your invitation code and then select your preferred authentication provider Facebook, Google, or Microsoft.

3.2. **"Black-Hat" Hacker, Log into Kali Linux VM:** Once logged into your instructor's course, click on the exercise as directed by your instructor, and click the start button (power icon) for your VM if not already started (it could take a couple of minutes if it has never been started before). Once it comes up, the Join (play icon) will appear. Click on it and select the Primary Machine to log into, the "kali.example.com" desktop VM. This will pop open another browser tab.
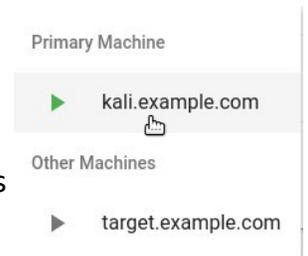
3.3. If your VM sessions do not auto-log you into the Kali Linux desktop and a graphic login window pops up, then log into the primary Kali desktop by using the **username=student** and **password=student**, which should place you at the Kali Linux VM's desktop.

(based on material of Dr. Jon Guo)

VIRGINIA
CYBER RANGE

3.4. Once logged in to the Kali desktop, open a terminal window by either right-clicking on the desktop and selecting **Open Terminal Here**, by clicking on the black terminal icon in the **Launch Bar** at the bottom of the desktop, or through the **Applications** menu at the top left (not shown). See image on the right.
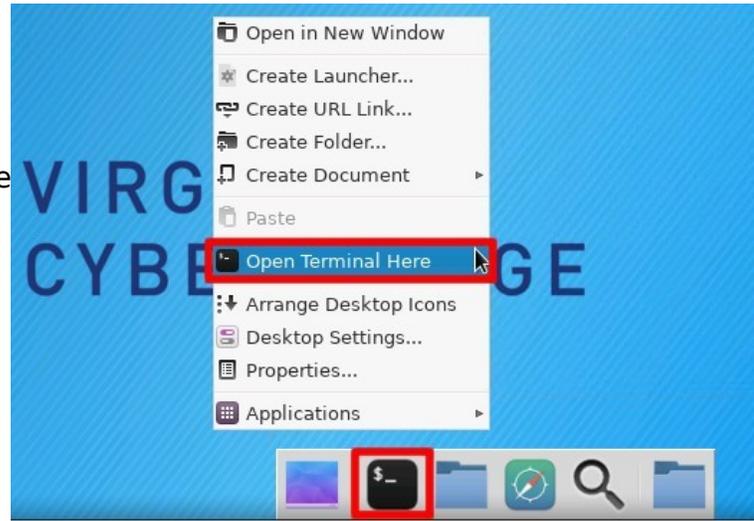
3.5. The Kali Linux desktop should have the host name kali.example.com.

Black-Hat: In the Linux terminal, type:

host kali.example.com (from the Kali VM)

to see your Kali Linux machine's IP address. Write down this IP below.

White-Hat: Use your partner's Kali Linux session to discover the IP of your Windows VM "target" by typing (in the Kali terminal):
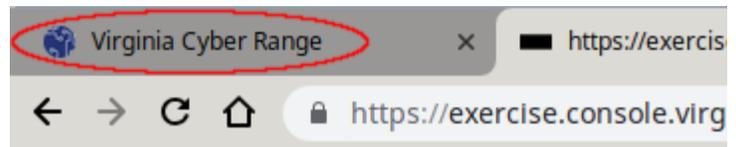
host target.example.com (from the Kali VM)

to see what your Windows "target" IP is. Record this IP address below.

Your Kali Linux Desktop's IP address: _____
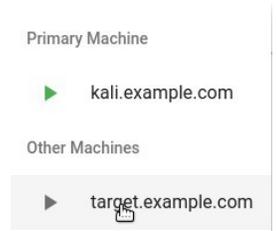Your Target Windows's IP address: _____

3.6. **White-Hat: Log into Target Windows VM:** In your browser's tabs at the very top of your screen, click back on the Cyber Range tab to access the console of your target Windows VM.

3.7. Again, click on the Join (play) icon, but this time select the login for the target.example.com machine.

3.8. Once logged into the Windows desktop, a one-time "Windows Activation" window may pop up. If it does, just bypass this by selecting "Ask Me Later" (we're not registering this OS since this is for temporary, educational use).

NOTE: For "Windows Activation", DO NOT select "Activate Now" or this will cause problems and you'll have to ask your instructor to reset your VMs.

3.9.   **Set Windows Network Location:** If you have never booted this VM before, you may also get this one-time network security check the first time this windows system comes on line and sees a new network*.

If you get this "Set Network Location" requester, you will get three options, "Home Network" (trusted), "Work Network" (trusted), or "Public Network" (untrusted). **Select "Public network"** as seen to the right.

Check the box "**Treat all future networks as public...**" so that your machine stays safe by default. This will configure your system to block most of the ports hackers scan for.
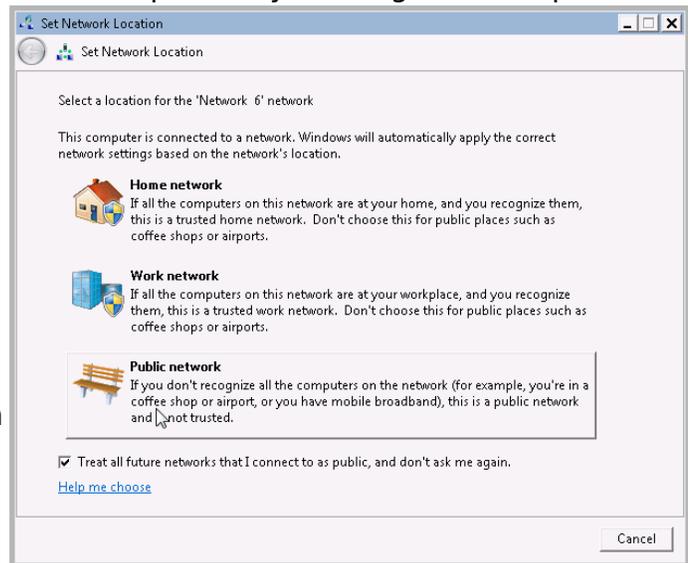
*** NOTE:** *If the "Set Network Location" Window (above) does not pop up, you need to invoke it by clicking **Start**, and in the search field type `sharing`, and then clicking on the **Network and Sharing Center** icon. Under the "View your active networks" window, if you do not see the "Public" park-bench icon shown here (i.e. if it says "Home network" or*

*"Work network"), then click on the blue link of your network so that the "Set Network Location" user interface pops up, then select **Public Network** and then click Close.*

Now the Public network firewall rules are in a more secure state, configured for use in a public coffee shop or airport (where hackers scan for vulnerable machines).
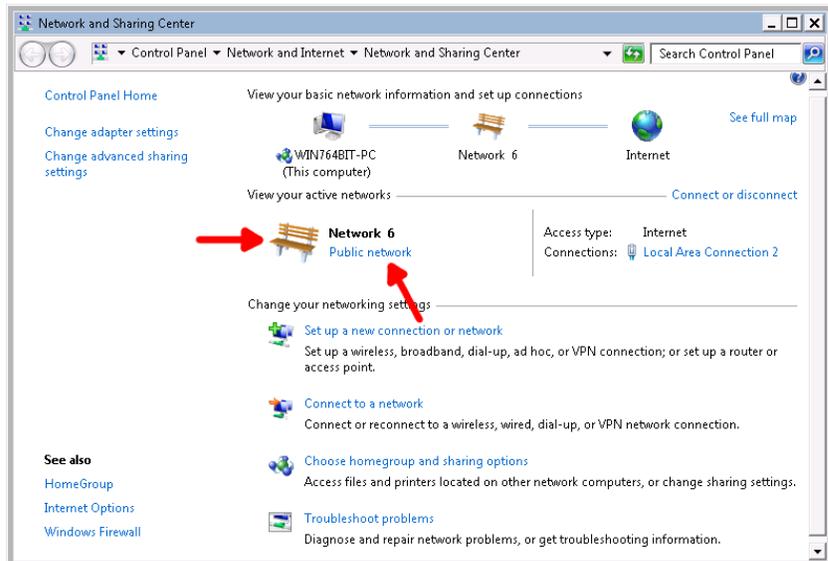
Even with your default Public network firewall set up, you may still not be safe. After the next step, we'll have the Black-Hat scan your system.

(CC) 2020 Virginia Cyber Range. by T.Weeks. (CC BY NC SA 4.0)   4
(based on material of Dr. Jon Guo)

VIRGINIA CYBER RANGE

3.10. **White-Hat, Verify Windows Firewall Is Turned On:**
To verify the firewall is turned on for your Public and Home network location configurations, click the **Start** menu, and type `firewall` and click on the **Windows Firewall** application as seen below:

Invoking the Windows Firewall interface
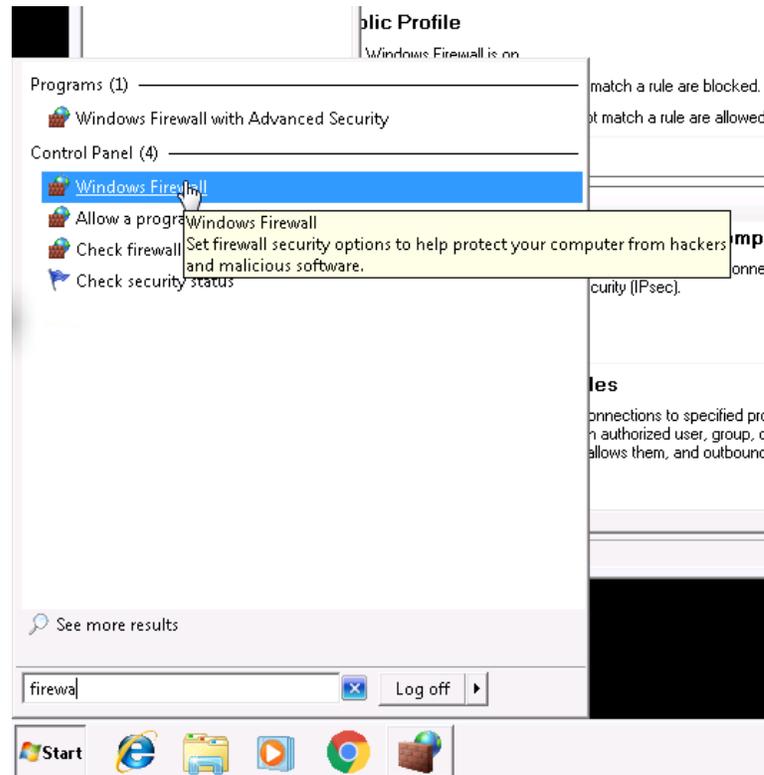
3.10.1. Once the Control Panel for the Windows Firewall comes up, on the left, click on **Turn Windows Firewall on or of** to bring up the Windows Firewall / Customize Settings menu, pictured here, and verify that the "Turn on Windows Firewall" button under the "Home or work…" network button for is enabled, and click "OK".
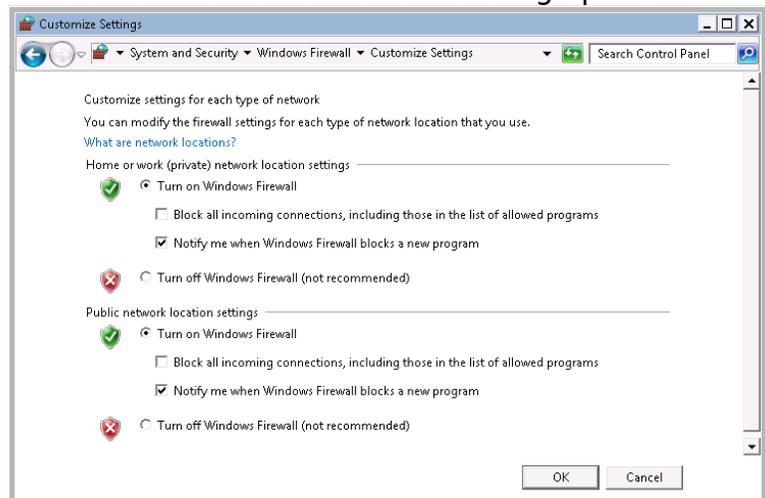
WARNING: *Do NOT select "Block all incoming connections…" or you can inadvertently lock yourself out of your Cyber Range RDP session (remote desktop). If you do this, your Instructor will have to reset your entire Range VM environment for you to continue.*

(CC) 2020 Virginia Cyber Range. by T.Weeks. (CC BY NC SA 4.0)   5
(based on material of Dr. Jon Guo)

VIRGINIA
CYBER RANGE

4. Tasks

4.1. Black-Hat on Kali, Scan Yourself:
On the Kali Linux (hacker) system, open a terminal and type:

nmap -Pn kali.example.com

You should see output similar to this showing what ports are open on your own computer (kali.example.com or your My-Kali-IP from step 3.5):

```
$ nmap -Pn kali.example.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 19:33 UTC
Nmap scan report for kali.example.com (10.1.58.61)
Host is up (0.000092s latency).
rDNS record for 10.1.58.61: ip-10-1-58-61.ec2.internal
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh            <--------- remote ssh access port
3389/tcp open  ms-wbt-server  <--------- remote desktop port

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

***NOTE:** As seen above, anything in* **bold print** *is what you type. Anything* non-bold print *is output from your commands, and anything in* print-italics *is to call your attention to something.*

Q: What port numbers are exposed on your own machine (kali.example.com)?

_____
_____
_____

4.2. Kali Black-Hat, Scan the Target Windows System:
 (or let the white hat do it :)
After scanning yourself, now turn your attention to the target system and scan target.example.com for any exposed ports:

```
$ nmap -Pn target.example.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-16 20:12 UTC
Nmap scan report for target.example.com (10.1.61.99)
Host is up (0.00098s latency).
rDNS record for 10.1.61.99: ip-10-1-61-99.ec2.internal
Not shown: 999 filtered ports
PORT      STATE SERVICE
XXX/tcp open  XXXXXXXXXXXX <----- vulnerable Windows port!
```

This command just scanned over 1,000 ports on the target (like doors and windows on the target system) in just a few seconds.. and should have found something the Windows firewall isn't blocking.

Q-4.2: What port # is still exposed on the Windows target.example.com VM?

_____
_____
_____

(CC) 2020 Virginia Cyber Range. by T.Weeks. (CC BY NC SA 4.0)   6
(based on material of Dr. Jon Guo)

VIRGINIA
CYBER RANGE

Q-4.2-EX: EXTRA POINTS: What does the target system look like if the Windows White-Hat opens up all the ports by switching into "Home network" mode? (see how to switch in the notes of step 3.9) What ports are now open?

_____
_____
_____
_____
_____
_____

IMPORTANT :*If you switch to "Home network' mode, be sure to switch back to "Public network" mode after doing so (so the rest of this lab works as written).*

FIREWALLING TIP: *For more information on the risks of leaving the RDP protocol exposed to anything except your own machines and networks, just google for "RDP security risks". Other high-risk ports/protocols that are commonly left open on Windows systems are the port/protocols 135/MS Endpoint Mapper, 139/NetBIOS, and 445/MS SMB (file sharing), among others. Completely blocking these ports to everyone could cause your home file and print sharing, or connections & shares between home PCs to break, so always test before blindly blocking. Switch back to "Public network" mode and re-scan the target system.*

4.3. **White-Hat – Block "Remote Desktop Protocol" (RDP)..**
Without Locking Yourself Out:
Now that you have seen the remaining exposed (possibly vulnerable) open port(s) into your Windows system, let's take a moment and block it.

4.4.1. **Open the Windows Firewall Tool:**
From the "Start" menu, in the search field type `firewall` and click on **Windows Firewall with Advanced Security**.

4.4.2. In the upper left, click on the **Inbound Rules**. This will display hundreds of firewall port/protocol rules. To whittle it down to see only the Remote Desktop firewall rule, click on the **Filter by Group** on the right, and then on **Filter by Remote Desktop**, as seen on the right:

VIRGINIA CYBER RANGE
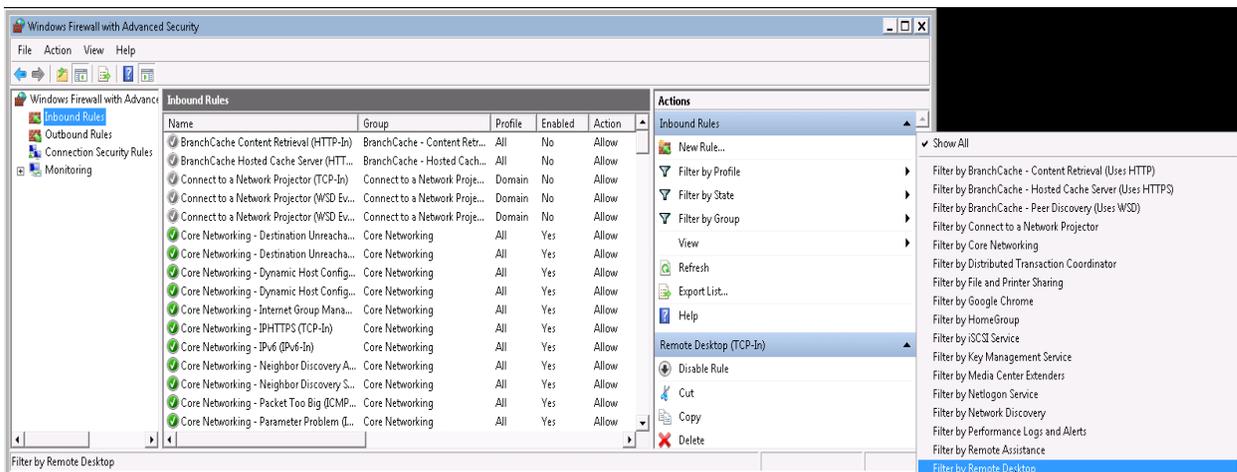
4.4.3. Modify the Firewall Rule for Remote Desktop sessions:

By default, the Remote Desktop Firewall Rule is open to everyone. By allowing only certain IP ranges, the Windows firewall's behavior is to block all other (not listed) IP addresses and networks. As seen above, after double clicking on the **Remote Desktop (TCP-In)** rule, the rule properties pops up:
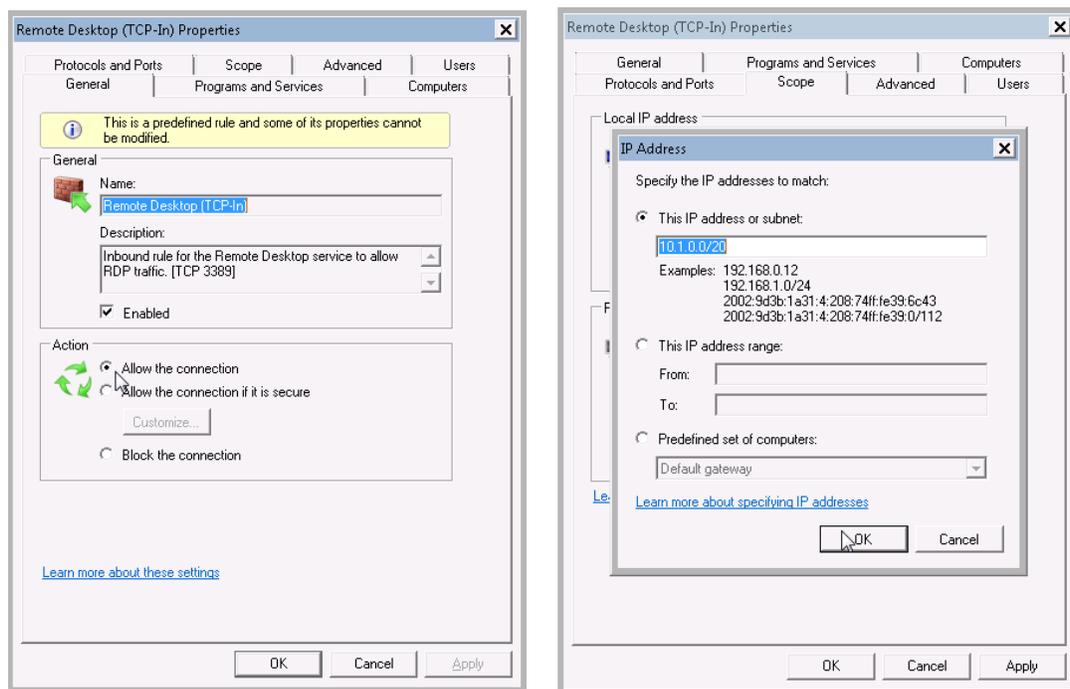
Ensure the "Action" is set to "Allow the connection", then click on the **Scope** tab. Under the Scope's "Remote IP addresses", select **These IP addresses**, and then under **This IP address or subnet**, add the following IP/network blocks (representing the CyberRange's networks):
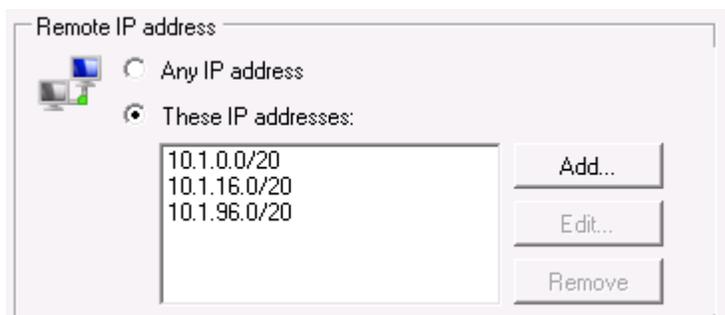
These Cyber Range RDP-friendly networks/IPs will keep you from locking yourself out of your remote desktop session on the Cyber Range, while locking everyone else on the Internet out.

> ***WARNING:*** *If you get these Remote IP addresses wrong, you can completely lock yourself out of your own Cyber Range session and your Virtual Machine environment will need to be reset by your instructor, losing any work you've done.*

(CC) 2020 Virginia Cyber Range. by T.Weeks. (CC BY NC SA 4.0)   8
(based on material of Dr. Jon Guo)

VIRGINIA
CYBER RANGE

4.4. Kali Black-Hat, Re-Scan the Target Windows System:

Now that the White-Hat sys-admin has locked down their firewall settings to disallow all IPs and networks except special Cyber Range IP ranges, rescan the target and record the results.

4.4.1. Scan the target system for any exposed ports:

```
$ nmap -Pn target.example.com
...
```

NOTE: This time you scan the target, you might realize it is taking much longer. It does not come back in mere seconds, but may take a couple of minutes. This is normal as the more closed/filtered ports that are encountered, the longer the scan typically takes. When scanning your own network for open ports, for local network scans, and more aggressive timeout/port value of around 100ms can be used to speed things up. This format can be forced with the command:

`nmap Pn —max-rtt-timeout 100ms target.example.com`

which, on this system, completes in 1/10th the time.. potentially saving you a few minutes per host scanned!

Q-4.4.1a: What did *this* scan show?
_____
_____

Q-4.4.1b: How long did it take?
How long did it take with the 100ms timeout from the note?
_____
_____
_____
_____

TIP: You can "break out" of most long running commands (or just something you want to stop) with the keystroke CTRL-C (called "control c"), which sends the BREAK signal to the running process. It will quickly stop a long running nmap scan.

4.5. WHITE-HAT, RESET YOUR FIREWALL SETTINGS: Once done with all
scans, go back to the target Windows VM, pull up the "Start" menu, and the "Windows Firewall with Advanced Security" interface, pull up the "Filter Remote Desktop" rule again and under "Scope", set "Remote IP addresses" to **Any IP addresses** and click **OK**.

WARNING: If you do not undo the firewall block from step 4.4, then other labs in this environment may fail for you. If you're having problems accomplishing this last step, then simply ask your instructor to reset your VM environment on the Range.

(CC) 2020 Virginia Cyber Range. by T.Weeks. (CC BY NC SA 4.0)   9
(based on material of Dr. Jon Guo)

VIRGINIA
CYBER RANGE

Class Discussion Points:

If you were a hacker or defender, how would you utilize the knowledge of port scans to your advantage?

Based on the scanning results, what are the pros and cons of turning off incoming port 3389 firewall settings?

If all the machines on your local LAN belong to you, is your own network "trustworthy?" Why or why not?

(CC) 2020 Virginia Cyber Range. by T.Weeks. (CC BY NC SA 4.0)   10
(based on material of Dr. Jon Guo)

VIRGINIA
CYBER RANGE

5. References

- None

[This portion of the lab exercise template is provided for instructors that will be using this lab in a class they are teaching.]

Answers to lab Questions: *[IGNORE written for the zenmap version of this lab]*

4.2) The kali.example.com scan "OS details" should show something like "`Linux 3.8 – 4.14`", if Kali has been updated, this might change.

4.3) Click on the target.example.com scan, then on the "Ports / Hosts" tab, and then on port 445. The "Version" filed should show something like "Windows 7 Enterprise 7601, Service Pack 1..."

4.4) After turning on and blocking port 445 connections, no one on the local network can now connect to File/Print SMB (incoming) connections on the target Windows system, nor connect to it. This is very good from a security perspective; however, it's not very usable if you're trying to do any file or print sharing, or have any other machines trying to connect to the target.

BEST PRACTICE: Most experienced network/host administrators will block all incoming connections (ports) and only allow or "poke holes" for hosts, networks and services that actually need access to get work done.

CLASS DISCUSSION:
Malicious or "Black Hat" Hackers will use port scans to find vulnerable hosts, operating systems and network services to identify target systems that have not been patched or updated. They then attack target machines with known vulnerabilities and deliver malicious payloads that can do anything from take over your machine and hold your data for ransom (called ransomware), or sit quietly and record your email or banking logins and passwords, or run "scanning worms" that will find and exploit more machines to add to their DoS attack bot farms.

Firewalls are not typically 100% on or 100% off. You can configure the Windows firewall to "allow" any connections from your local network only (or specific machines, hosts or domain names), and get the best of both worlds, i.e., a locked-down personal firewall **with** specific allowances or "holes poked" for known hosts, services or networks.

Points to Keep in mind:
1) The less network services and OS ports you can expose on the local network and Internet, the better. Only expose what you must to get your work done. However:
2) Even other trusted machines on your local network, if hacked, can **become** malicious, so keep in mind there's no such thing as a "100% trusted network." Once one machine on your local LAN is compromised, the entire LAN and all machines are at much higher risk.

VIRGINIA
CYBER RANGE

KSAs from NIST SP 800-181:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

- K0167 Knowledge of basic system administration, network, and operating system hardening techniques.
- K0212 Knowledge of cybersecurity-enabled software products.

- S0016 Skill in configuring and optimizing software.
- S0039 Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.
- S0040 Skill in implementing, maintaining, and improving established network security practices.

- A0093 Ability to identify/describe techniques/methods for conducting technical exploitation of the target.

NSA/DHS CAE Knowledge Units:
https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf
(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

- Network Defense (NDF)

VIRGINIA
CYBER RANGE