[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title
Term: (Fall, Spring, Summer, Winter) 20XX

Laboratory Exercise X – Defending Against Public WiFi Hacker Attacks in Airports

Due Date: Date
Points Possible: **Number of points out of total course points or recommended percent of course grade.**

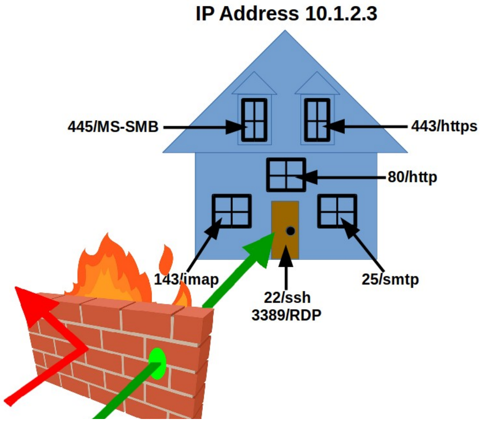
1. Overview

This lab exercise is based upon material by Dr. John Guo

What Students Will Learn:
During this lab, students will gain experience and knowledge in *network administration*, *ports*, *protocols*, *IP addresses*, *port scanning* and *firewalling*. Students should pair up with another student where one student will play the "Black-Hat" attacker and attack an old, vulnerable (unpatched) Windows system for open ports and vulnerabilities, and the other student will play the "White-Hat" defender 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.

Ports are like the doors and windows of an IP address



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 predefined web traffic "window" into a web server.

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 cannot be as easily scanned and probed back by Black-Hats.

© 2022 Virginia Cyber Range. Created by T. Weeks. (CC BY-NC-SA 4.0)

[Any blue text should be replaced by instructor using material and font color changed to black.]

Course Title
Term: (Fall, Spring, Summer, Winter) 20XX

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, always remember 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. ALWAYS GET PERMISSION of the system or network owner or admin before scanning a system or network.*

© 2022 Virginia Cyber Range. Created by T. Weeks. (CC BY-NC-SA 4.0)

2. Resources required

Virtual Machines (VMs) needed: Kali Linux and Vulnerable Windows 7(64bit) VMs environment. The Kali Linux is the scanning VM and the Windows 7 is the target VM on the same network, to simulate what happens when you open a laptop in the airport or Starbucks. 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.

[Note to instructors: This lab exercise requires an account on the Cyber Range. To sign up for an account on The Range, please visit our Sign-Up page. Your students will also require an account on the Cyber Range; this will be explained in the setup of your course.]

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.

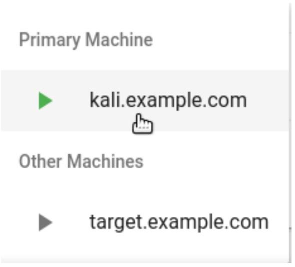
After logging into the cyber range and then navigating to this course and exercise, you will be opening up two remote desktop sessions within your browser. One browser tab will contain the Kali Linux desktop VM and the other tab with contain your desktop session to the target Windows desktop VM.

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.

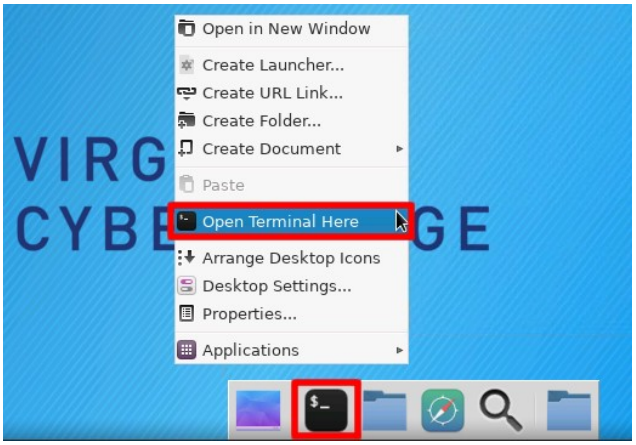
3.1. **Log into the Cyber Range:** To log into the range for the first time, either click on the email invite sent to you by your instructor, or if you were provided an “invitation code” then point your browser to the link provided by your instructor to use it. At the Range Login window, select the “Have 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.

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.

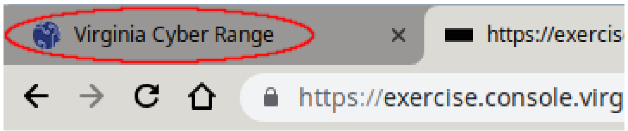
White-Hat: Use your partner's Kali Linux session to discover the IP of your Windows VM “target” by typing (in the Kali terminal):

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

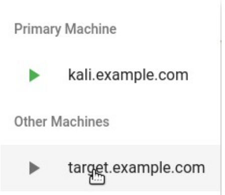
to see what your Windows “target” IP is. Record this IP address below.

Both students, write down both the attacker and target’s IP addresses:
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.

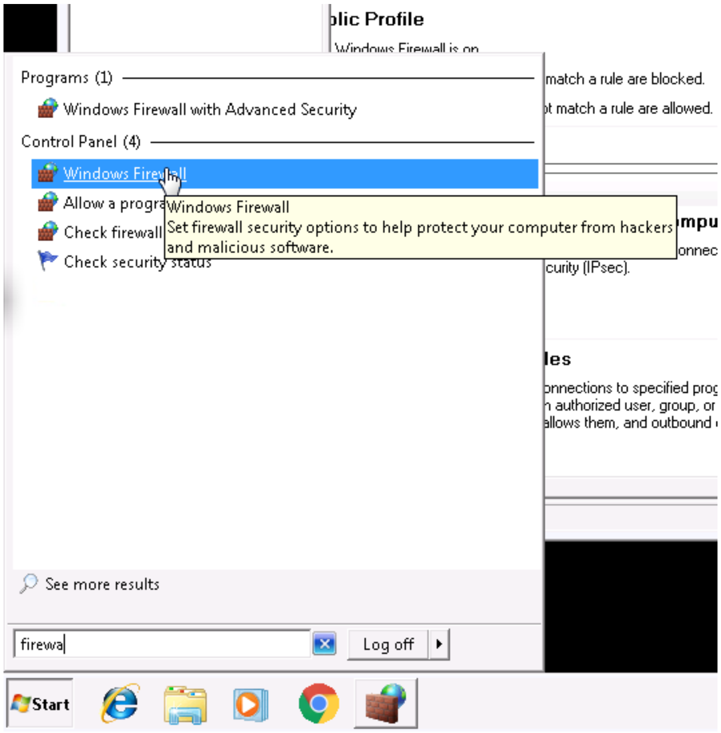


3.7.Again, click on the Join (play) icon, but this time select the login for the target.example.com machine.

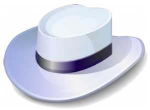


3.8.Once logged into the Windows desktop, a one-time “Windows Activation” window may pop up. If it does, just bypass this by selecting “Ask Me Later” (we're not registering this OS since this is for temporary, educational use).

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.



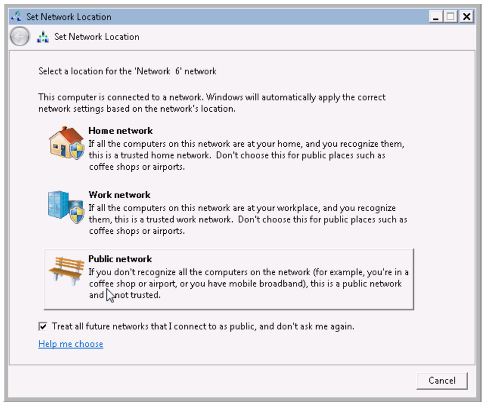
Windows Firewall
Set firewall security options to help protect your computer from hackers and malicious software.



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.



Select a location for the 'Network 6' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

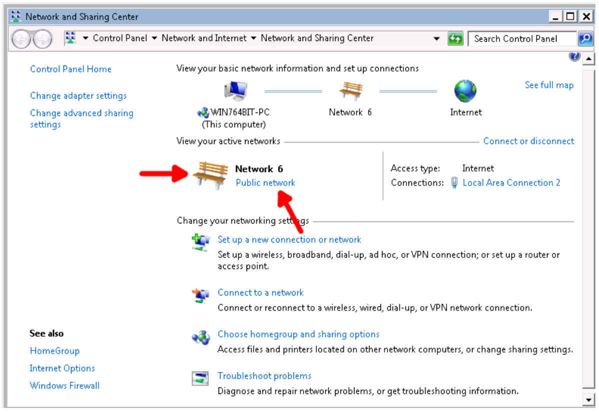
Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and not trusted.

☑ Treat all future networks that I connect to as public, and don't ask me again.

*** 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.*



View your basic network information and set up connections

View your active networks

Network 6 Public network	Access type: Internet Connections: Local Area Connection 2

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

*In Network Sharing, 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.*

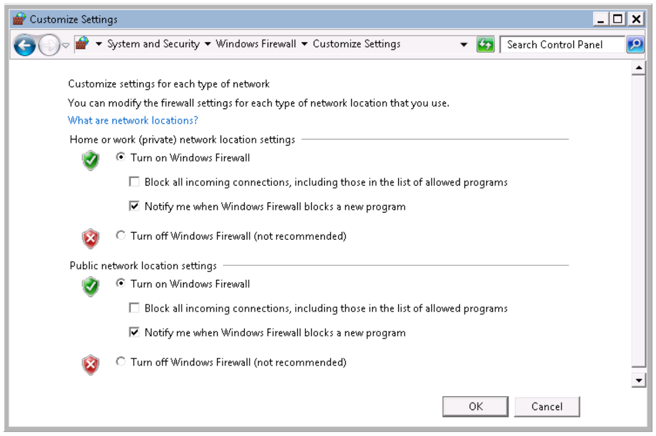
Now the Public network firewall rules are in a more secure state, configured for use in a public coffee shop or airport (where hackers scan for vulnerable machines).

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.

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 here:

Once the Control Panel for the Windows Firewall comes up, on the left, click on **Turn Windows Firewall on or off** to bring up the Windows Firewall / Customize Settings menu (below) and verify that the “Turn on Windows Firewall” button under the “Home or work…” network button for is enabled, and click “OK”.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

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.*

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-4.1: 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  XXXXXXXXXXXXX <----- 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?

____

____

____

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 the white-hat switched to “Home network' mode, once done with step 4.2, be sure to switch back to “Public network” mode after doing so everything will work as expected, with the public firewall rules turned on.*

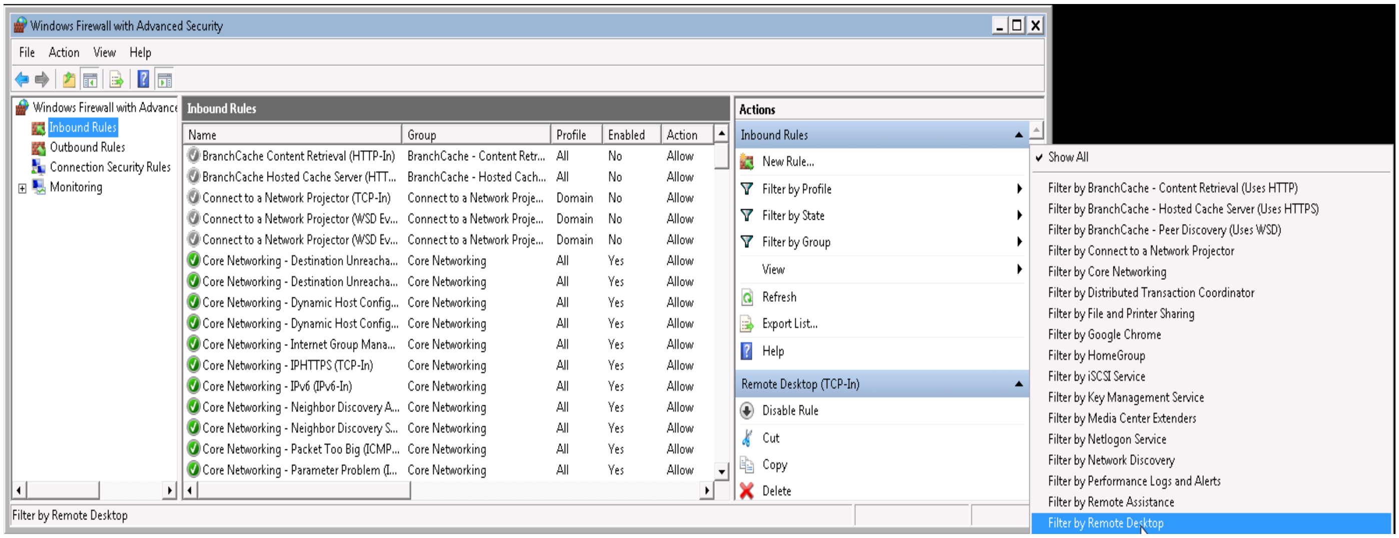
FIREWALLING TIP: *For more information on the risks of leaving the RDP protocol exposed to anything except your own machines and networks, just google for “RDP security risks”. Other high-risk ports/protocols that are commonly left open on Windows systems are the port/protocols 135/MS Endpoint Mapper, 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.

4.3.1. **Open the Windows Firewall Tool:**
From the “Start” menu, in the search field type **`firewall`** and this time click on **Windows Firewall with Advanced Security**.

4.3.2. 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 below:

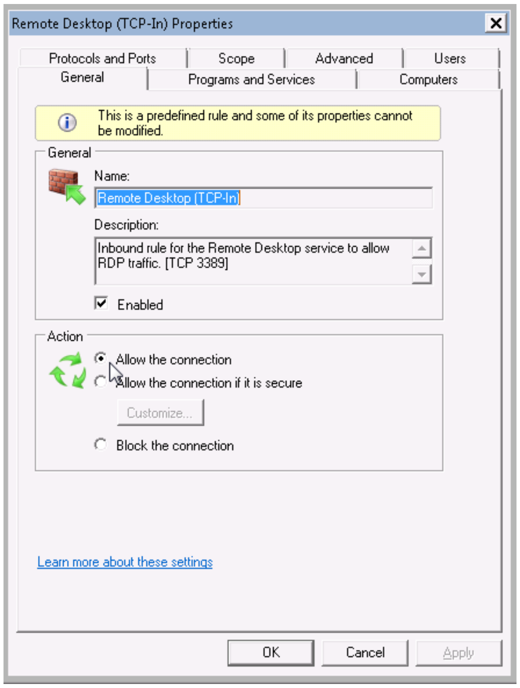

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Remote Desktop (TCP-In)
Disable Rule
Cut
Copy
Delete
✓ Show All
Filter by BranchCache - Content Retrieval (Uses HTTP)
Filter by BranchCache - Hosted Cache Server (Uses HTTPS)
Filter by BranchCache - Peer Discovery (Uses WSD)
Filter by Connect to a Network Projector
Filter by Core Networking
Filter by Distributed Transaction Coordinator
Filter by File and Printer Sharing
Filter by Google Chrome
Filter by HomeGroup
Filter by iSCSI Service
Filter by Key Management Service
Filter by Media Center Extenders
Filter by Netlogon Service
Filter by Network Discovery
Filter by Performance Logs and Alerts
Filter by Remote Assistance
Filter by Remote Desktop
Filter by Remote Desktop

Inbound Rules

Name	Group	Profile	Enabled	Action
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow

4.3.3. **Modify the Firewall Rule for Remote Desktop sessions:**

By default, the Remote Desktop Firewall rule allows everyone on the Internet to access RDP. By “Scoping” or allowing only certain IP ranges, the Windows firewall's behavior is to block all other (not Scoped) IP addresses and networks. As seen above, after double clicking on the **Remote Desktop (TCP-In)** rule, the rule properties pops up (left):

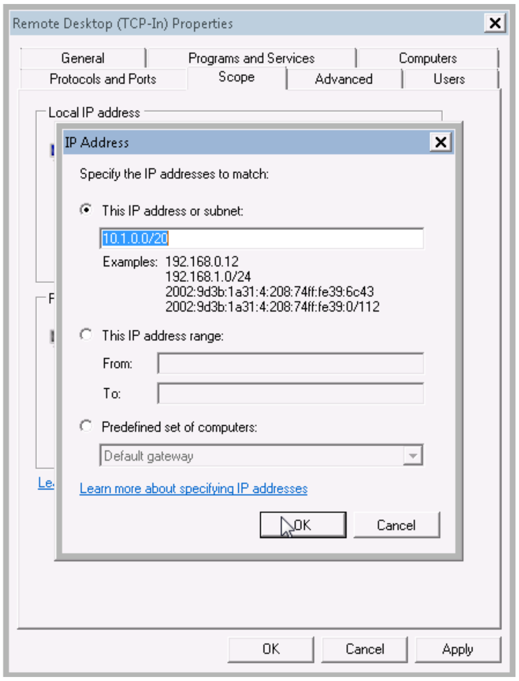


Remote Desktop (TCP-In) Properties

This is a predefined rule and some of its properties cannot be modified.

General
Name: Remote Desktop (TCP-In)
Description: Inbound rule for the Remote Desktop service to allow RDP traffic. [TCP 3389]
☑ Enabled

Action
● Allow the connection
○ Allow the connection if it is secure
○ Block the connection



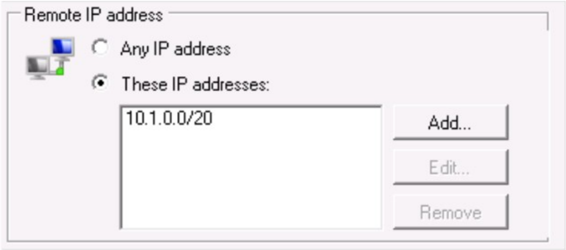
Remote Desktop (TCP-In) Properties

IP Address

Specify the IP addresses to match:
● This IP address or subnet:
10.1.0.0/20
Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112
○ This IP address range:
From:
To:
○ Predefined set of computers:
Default gateway

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** (right), and then under **This IP address or subnet**, add the following IP/network block, which represents the CyberRange's networks where you are connecting to your VM using RDP:

This scoped, network allow of 10.1.0.0/20 is what allows remote IPs coming from IPs 10.1.0.0 – 255 (the Cyber Range system) to access RDP on this VM. Scoping this IP range will keep you from locking yourself out of your own Windows remote desktop session, but *will* lock out everyone else on the Internet out, including the black-hat.



Remote IP address
○ Any IP address
● These IP addresses:
10.1.0.0/20

WARNING: *If you get this 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.*

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 RDP on all IPs and networks (except special Cyber Range IP ranges), now rescan the target and record the results.

4.4.1. Scan the target system for any exposed ports:

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

Q-4.4.1a: What did *this* scan show in the way of open ports?

____

____

____

NOTE: *You might realize it is taking much longer to scan when the firewall is blocking everything. It does not come back in mere seconds, but may take a several 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-per-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-4.4.1b: How long did the second, faster scan 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"). You can also time a command by starting the command with the* **`time`** *command.*

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.*

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?

5. References

- [1] - https://en.wikipedia.org/wiki/Black_and_white_hat_symbolism_in_film
- [1] - https://en.wikipedia.org/wiki/Black_hat_(computer_security)#Origin
- [2] - https://www.bridewellconsulting.com/different-types-of-hackers-and-what-they-mean-for-your-business
- [3] - https://www.dictionary.com/browse/blackball
- [4] - https://www.greecehighdefinition.com/blog/2021/3/7/how-was-the-voting-in-ancient-greece
- [5] - https://www.wordsense.eu/ballotta/#Italian

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

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)