M6 Lab: Transport Layer

CITA 220: DATA COMM & NETWORK TECH

Gonzalez, Marco A.
SUNY CANTON | 34 CORNELL DRIVE, CANTON, NEW YORK 13617

TABLE OF CONTENTS

1 TABLE OF FIGURES

2 PREPARATION

If you cannot access a Windows PC but can run a virtual machine, download a Windows 11 virtual image from here and import it. Set the VM network setting to **Bridged Adapter** Launch a Windows command prompt and PowerShell using the **Run As Administrator** option. Set the CITA 220 VM's network setting to **Bridged Adapter** also. Start the VM. Log in and launch a Terminal program.

2.1 WINDOWS

In this section, some Windows transport layer-related commands are explored.

2.1.1 Local Open Ports

In this section, the network TCP and UDP ports that are currently open on the Windows computer you are currently logged in are examined.

2.1.1.1 TCP

The **netstat** command is used to display the currently opened TCP ports. The **-p tcp** option is used. See Figure 1. The **-n** and **-a** options display port numbers (not port names) and all connections. The port numbers are the numbers that come after IP addresses followed by a colon (:). The **0.0.0.0** local IP address means all network interface card addresses.

```
Microsoft Windows [Version 10.0.22621.2715]
(c) Microsoft Corporation. All rights reserved.

C:\Users\marco>netstat -nap tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49689          0.0.0.0:0              LISTENING
  TCP    10.11.65.11:139        0.0.0.0:0              LISTENING
  TCP    10.11.65.11:49432      52.159.127.243:443     ESTABLISHED
  TCP    10.11.65.11:51755      192.229.211.108:80     CLOSE_WAIT
  TCP    10.11.65.11:57461      20.49.109.142:443      ESTABLISHED
  TCP    10.11.65.11:57652      52.111.230.4:443       ESTABLISHED
  TCP    10.11.65.11:57705      52.182.143.211:443     TIME_WAIT
  TCP    10.11.65.11:57715      52.109.13.103:443      ESTABLISHED
  TCP    10.11.65.11:57716      104.117.182.41:80      TIME_WAIT
  TCP    10.11.65.11:57718      13.107.42.16:443       TIME_WAIT
  TCP    10.11.65.11:57719      8.8.4.4:443            TIME_WAIT
  TCP    10.11.65.11:57720      108.138.106.79:443     TIME_WAIT
  TCP    10.11.65.11:57721      54.158.163.31:443      TIME_WAIT
  TCP    10.11.65.11:57722      3.211.69.221:443       TIME_WAIT
  TCP    10.11.65.11:57723      8.8.4.4:443            TIME_WAIT
  TCP    10.11.65.11:57724      108.138.106.79:443     TIME_WAIT
  TCP    10.11.65.11:57725      204.79.197.200:443     ESTABLISHED
  TCP    10.11.65.11:57726      23.219.82.59:443       ESTABLISHED
  TCP    10.11.65.11:57727      23.219.82.59:443       CLOSE_WAIT
  TCP    10.11.65.11:57728      23.219.82.59:443       CLOSE_WAIT
  TCP    10.11.65.11:57731      13.89.178.27:443       ESTABLISHED
  TCP    127.0.0.1:8884         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49998        0.0.0.0:0              LISTENING
  TCP    192.168.29.1:139       0.0.0.0:0              LISTENING
  TCP    192.168.56.1:139       0.0.0.0:0              LISTENING
```

Figure 1. The netstat Command for TCP Connections

Note that the LISTENING ports are accepting external connections. The 0.0.0.0 foreign IP address means any IP address, which means any device can access these ports. System administrators and security professionals often inspect the listening port numbers to ensure all open ports are open for valid reasons. If an open port is not recognized, the process associated with the port may need to be investigated.

To list only the listening ports, using the netstat command, modify the command, as shown in Figure 2.

```
C:\Users\marco>netstat -nap tcp | find /i "listen"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
```

Figure 2. Display Listening TCP Ports Only

If the netstat command is used with the **-b -o** options, the processes and their process IDs (PIDs) using the local ports are displayed. To use this "-b" option, the command prompt must be launched as the administrator. See Figure 3 and Figure 4.

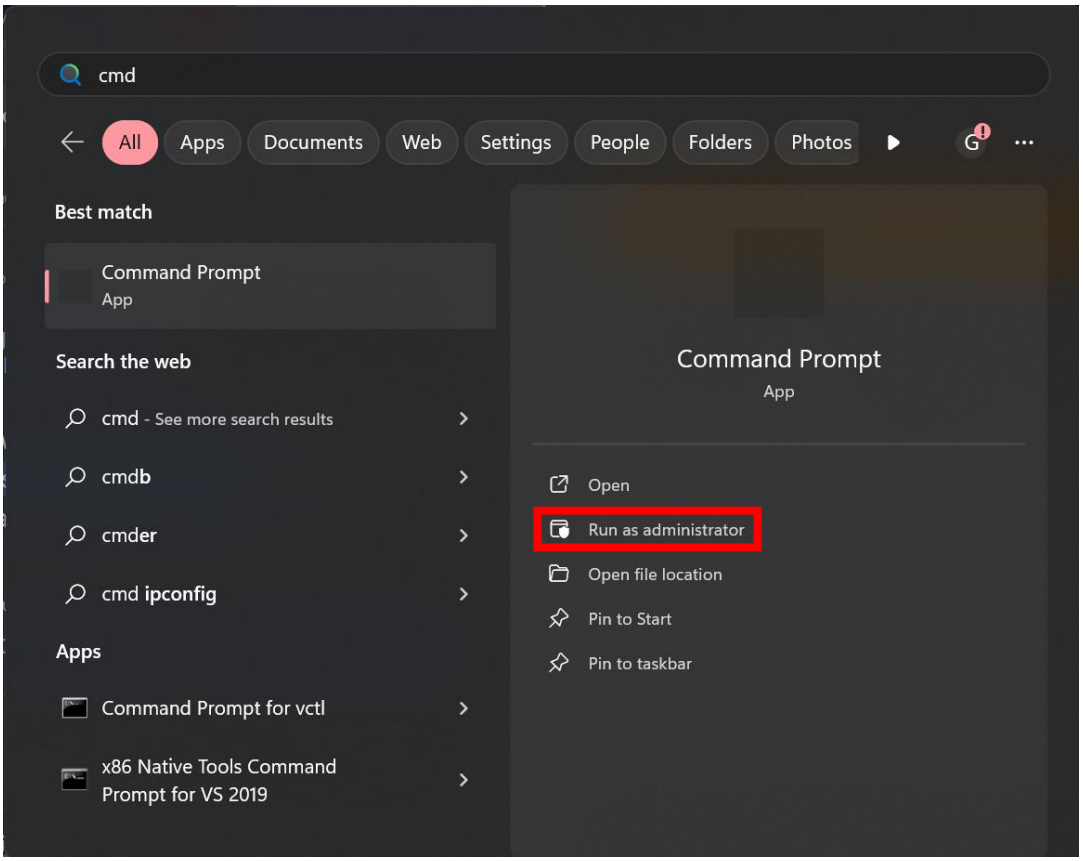

Figure 3. Launching Command Prompt as Administrator

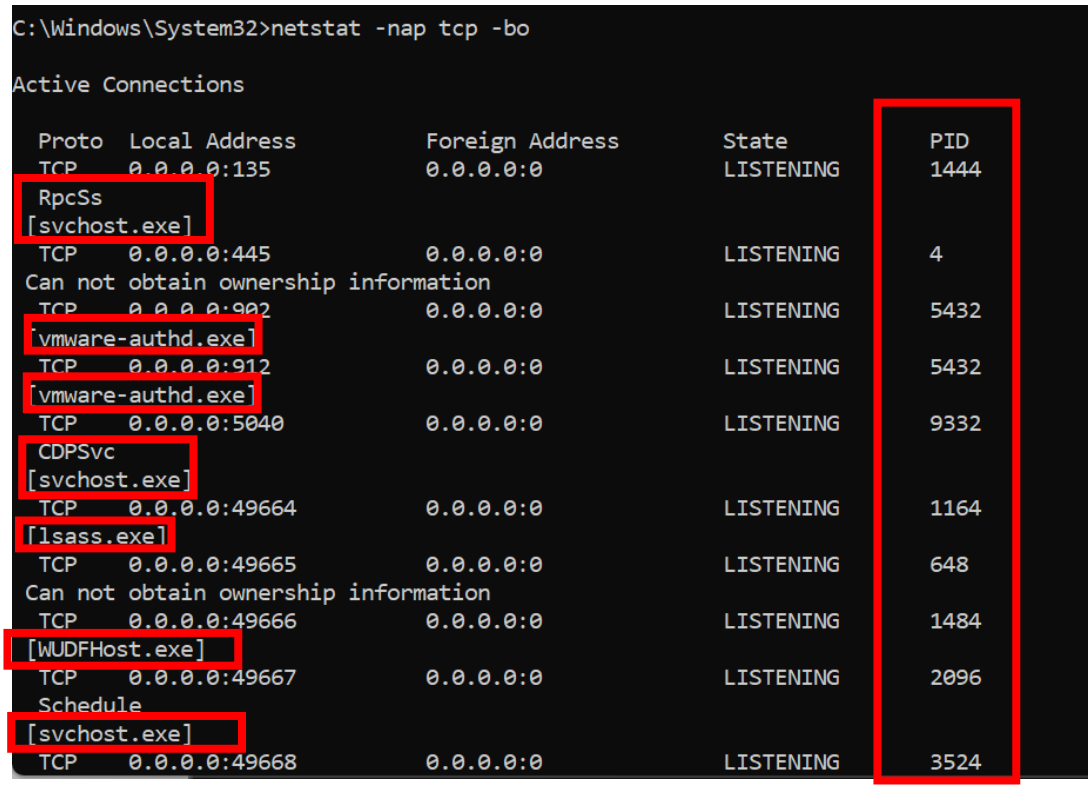

Figure 4. TCP Ports, Processes, and PIDs

2.1.1.2 UDP

The **netstat** command is also used to display the currently opened UDP ports. The **-p udp** option is used. See Figure 5.

The -b and -o options can also display the processes and PIDs using those ports. See Figure 6.

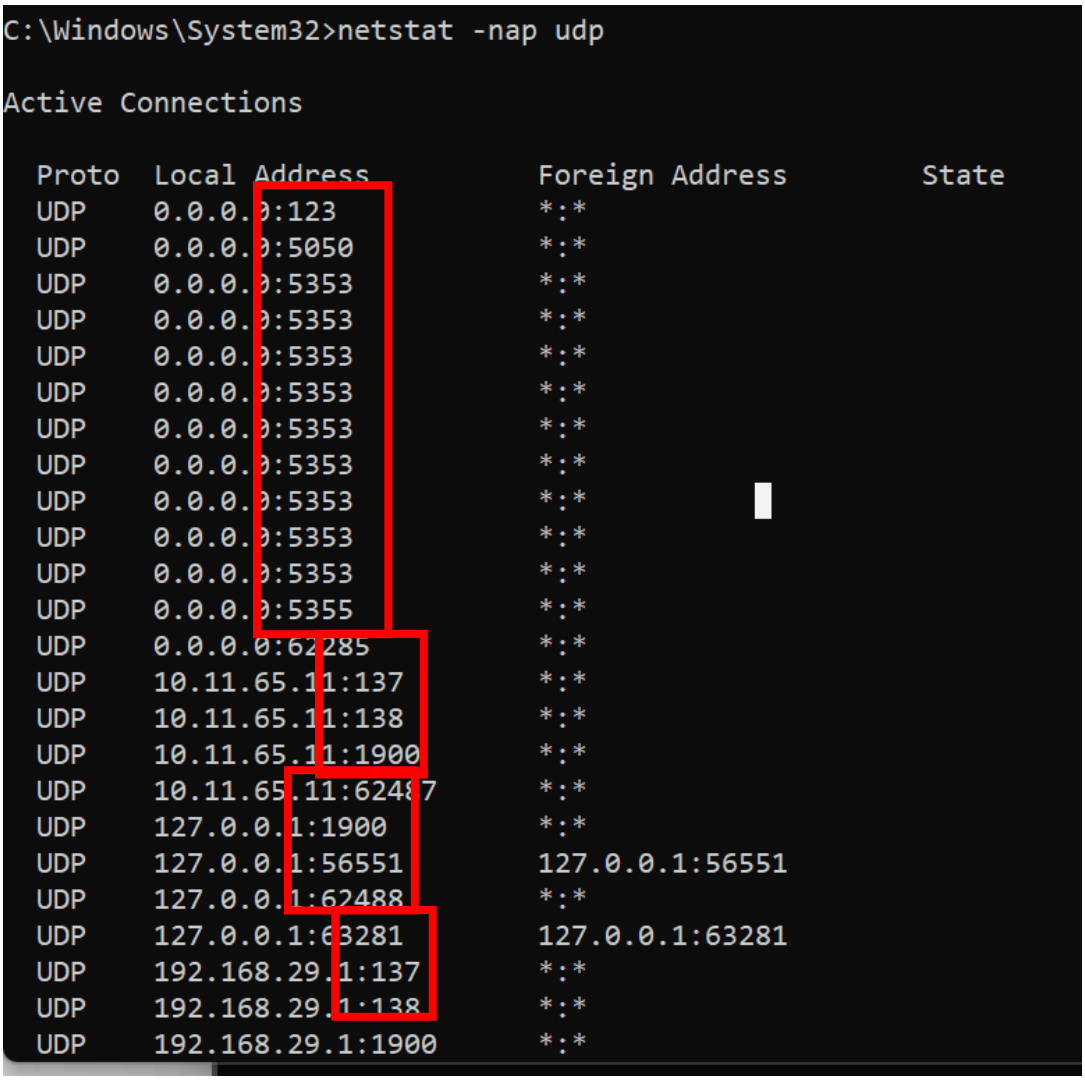

Figure 5. The netstat Command for UDP Connections

```
C:\Windows\System32>netstat -nap udp -bo

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  UDP    0.0.0.0:123            *:*                                    12580
  W32Time
 [svchost.exe]
  UDP    0.0.0.0:5050           *:*                                    9332
  CDPSvc
 [svchost.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
 [msedge.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
 [msedge.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
 [msedge.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
 [msedge.exe]
  UDP    0.0.0.0:5353           *:*                                    2776
  Dnscache
 [svchost.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
 [msedge.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
 [msedge.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
 [msedge.exe]
  UDP    0.0.0.0:5353           *:*                                    6288
```

Figure 6. UDP Ports, Processes, and PIDs

2.1.2 Remote Open Ports

The **Test-NetConnection** PowerShell command is used to test if a port on a remote device is open. In this example, the CITA VM is used as a remote device. This command tests if TCP port 80 on the CITA VM is open. The current CITA 220 VM's IP address is obtained first. Then the Test-NetConnection command is used to test if the TCP 80 port is open. See Figure 7 and Figure 8.

The **Test-NetConnection** command can be abbreviated as **TNC**. See Figure 9.

Warning: In this example, you are scanning your computers. You must not scan other people's computers without their explicit permission. It can cause issues on scanned computers. Unauthorized scanning is considered **unethical hacking**.

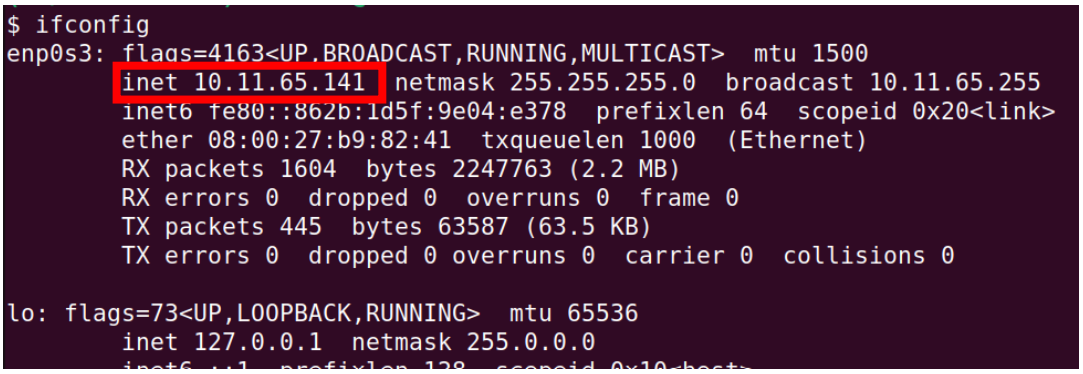

Figure 7. The IP Address of the Remote Device

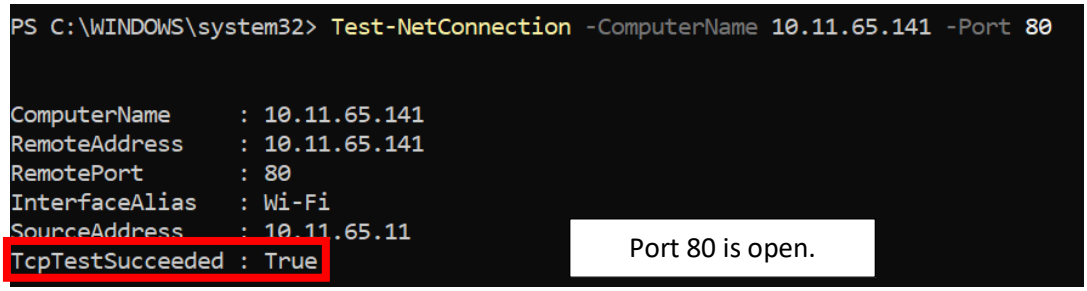

Figure 8. Successful Port 80 Test

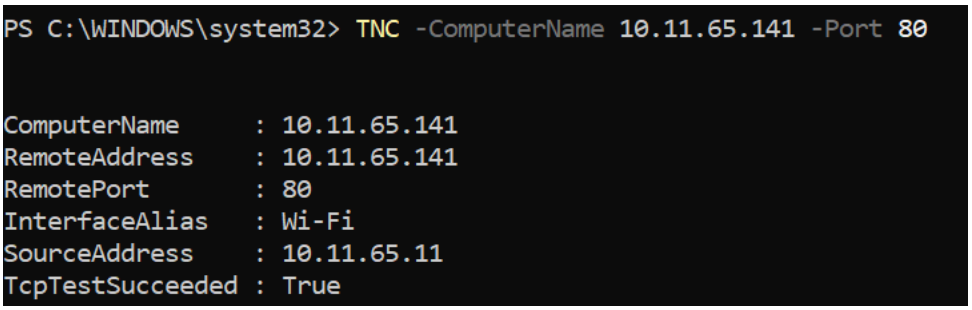

Figure 9. The Abbreviated Command

3 LINUX

In this section, some Linux transport layer-related commands are explored.

3.1.1 Local Open Ports

In this section, the network TCP and UDP ports that are currently open on the Linux computer you are currently logged in in are examined.

3.1.1.1 TCP

The **netstat** command is used to display the currently opened TCP ports. The **-t** option is used. See Figure 10. The **-n** and **-a** options are to display port numbers (not port names) and all connections. Note that **:::80** is an IPv6 representation of 0.0.0.0:80.

```
(12/06 15:51:27) student@cita220-vm: ~
$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 10.11.65.141:33776      35.224.170.84:80        TIME_WAIT
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
```

Figure 10. The netstat Command for TCP Connections

To list only the listening ports, modify the command, as shown in Figure 11.

```
$ netstat -ntl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
```

Figure 11. Displaying Listening TCP Ports Ony

If the netstat command is used with the **-p** option, the processes and their process IDs (PIDs) using the local ports are displayed. This option must be used with the **sudo** command. (Use *cita220* for the password.) See Figure 12.

```
$ sudo netstat -nat -p
[sudo] password for student:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      663/cupsd
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      410/systemd-resolve
tcp6       0      0 :::80                   :::*                    LISTEN      699/apache2
tcp6       0      0 ::1:631                 :::*                    LISTEN      663/cupsd
```

Figure 12. TCP Ports, Processes, and PIDs

3.1.1.2 UDP

The **netstat** command is also used to display the currently opened UDP ports. The **-u** option is used. See Figure 13.

The -p options can also display the processes and PIDs using those ports. See .

```
$ netstat -nau
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:34043           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 10.11.65.141:68         172.17.112.2:67         ESTABLISHED
udp6       0      0 :::5353                 :::*
udp6       0      0 :::49210                :::*
```

Figure 13. The netstat Command for UDP Connections

```
$ sudo netstat -nau -p
[sudo] password for student:
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           563/avahi-daemon: r
udp        0      0 0.0.0.0:34043           0.0.0.0:*                           563/avahi-daemon: r
udp        0      0 0.0.0.0:631             0.0.0.0:*                           804/cups-browsed
udp        0      0 127.0.0.53:53           0.0.0.0:*                           410/systemd-resolve
udp        0      0 10.11.65.141:68         172.17.112.2:67         ESTABLISHED 567/NetworkManager
udp6       0      0 :::5353                 :::*                                563/avahi-daemon: r
udp6       0      0 :::49210                :::*                                563/avahi-daemon: r
```

Figure 14. UDP Ports, Processes, and PIDs

3.2 Remote Open Ports

The **nmap** command tests if a port on a remote device is open. In this example, the Windows (or VM) is a remote device. This command tests if TCP port 445 is open on the Windows (or Windows VM).

Before this test can be conducted, the Windows firewall must be turned off temporarily. Follow these steps. Remember to re-enable it after the test.

1. Make sure the CITA 220 VM is using the **Bridged Adapter**.
2. If you use a Windows VM, make sure it also uses the **Bridged Adapter**.
3. Execute the **ipconfig** command to obtain the IP address of the Windows computer.
4. Click the Windows (⊞) key and type *fire*.
5. Look for and click **Windows Defender Firewall**.
6. On the left, look for and click **Turn Windows Defender Firewall on or off**.
7. Click **Turn off Windows Defender Firewall** for both the Private and Public network settings.
8. Click **OK**.

Go to the CITA 220 VM and execute the nmap command. See Figure 15 and Figure 16. Go back to the Windows Defender Firewall and click **Turn on Windows Defender Firewall** for both the Private and Public network settings. Click **OK**.

Warning: In this example, you are scanning your computers. You must not scan other people's computers without their explicit permission. It can cause issues on scanned computers. Unauthorized scanning is considered **unethical hacking**.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cd0c:fa2e:80:9244%21
   IPv4 Address. . . . . . . . . . . : 10.11.65.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.11.65.1
```

Figure 15. The IP Address of the Windows Computer

```
$ nmap -p 445 10.11.65.11
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-06 16:47 EST
Nmap scan report for 10.11.65.11
Host is up (0.00082s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

Figure 16. Successful Port 445 Test