Network Penetration Testing Methodology-Perimeter Devices

1 Hr 37 Min Remaining

**Exercise 3: HTTP Tunneling to Bypass Firewalls Using HTTPort**

**Scenario**

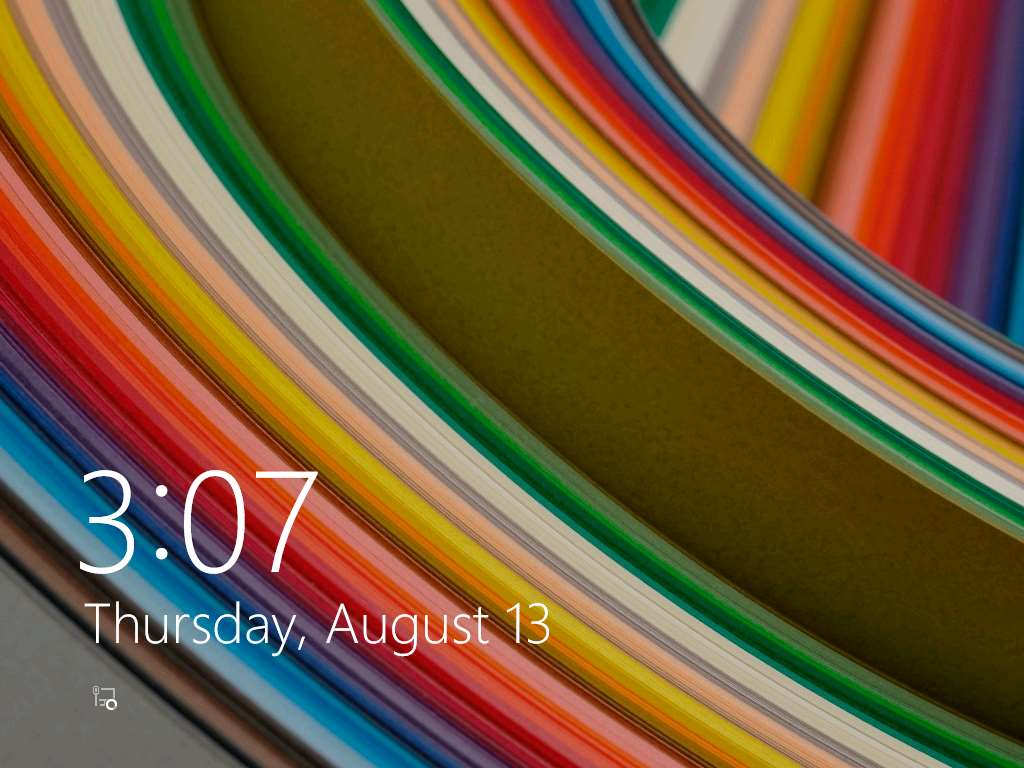
Attackers are constantly searching for vulnerable clients to penetrate their network through IP spoofing to damage or steal data. The attacker can access packets through a firewall by spoofing the IP address. If attackers are able to capture network traffic, as explained in the previous lab, they can perform Trojan attacks, registry attacks, password hijacking attacks, etc., which can be disastrous for an organization’s network.

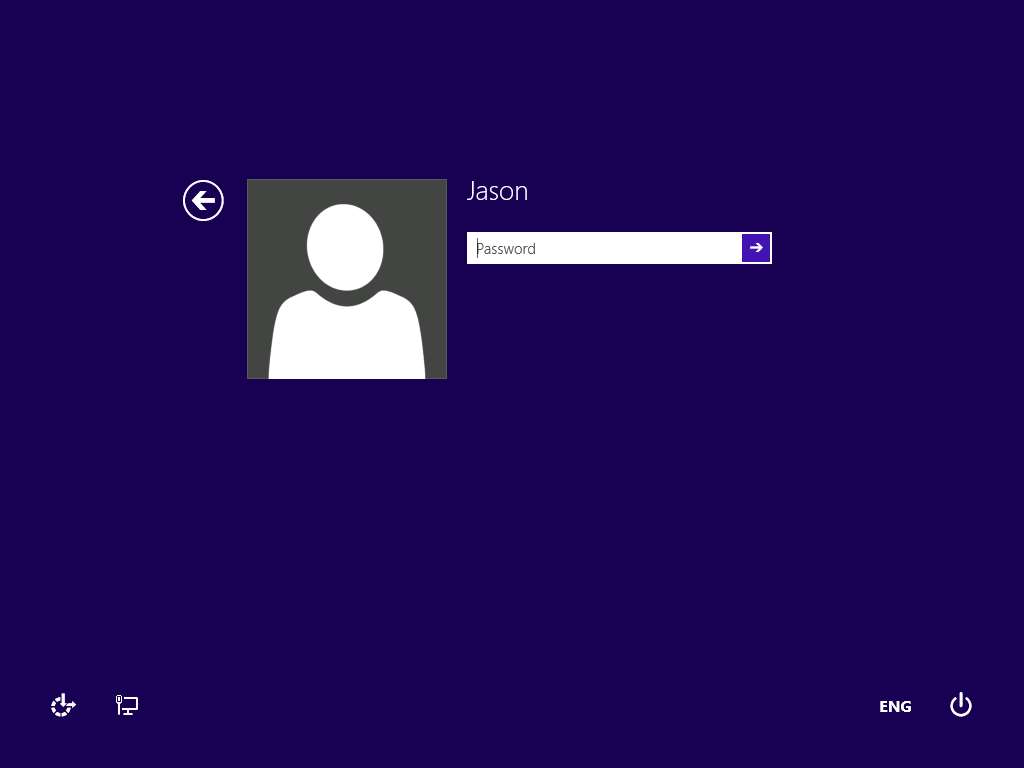
Therefore, as a network administrator, you should be able to identify attacks by extracting information from captured traffic such as source and destination IP addresses, protocol type, header length, source and destination ports, etc. and compare these details with modeled attack signatures to determine if an attack has occurred.

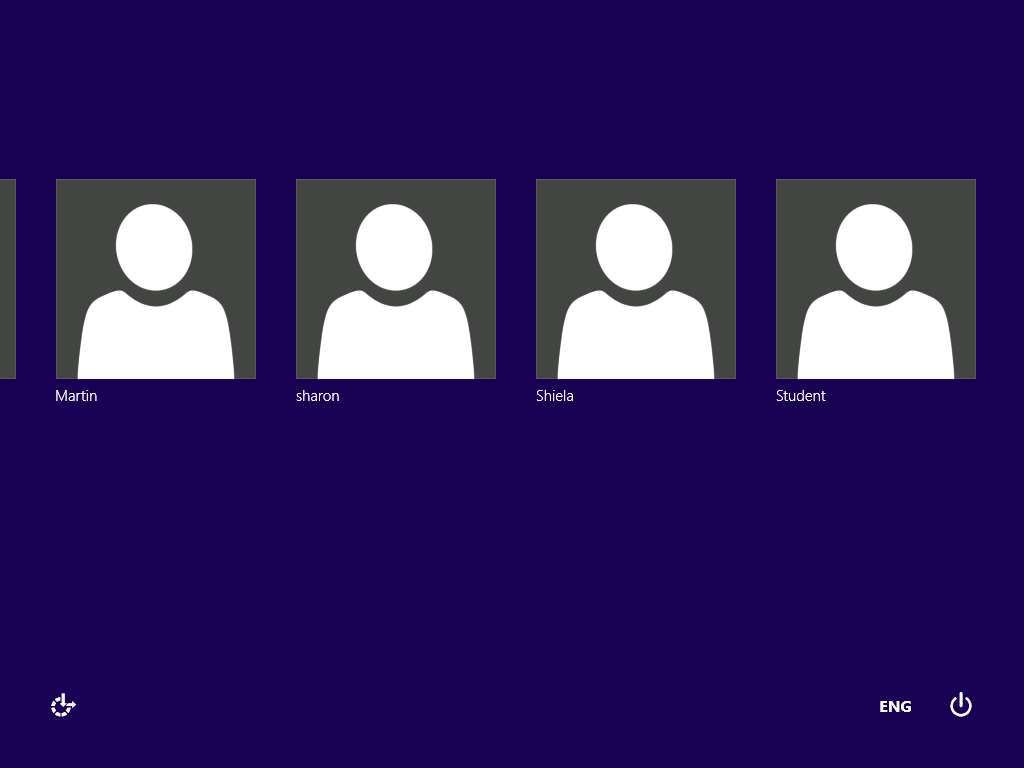
Also, familiarity with the HTTP tunneling technique is important as it helps in identifying additional security risks that may not be detected by conducting simple network and vulnerability scanning and determines to what extent a network IDS can identify malicious traffic within a communication channel.

**Lab Duration**: **30** Minutes

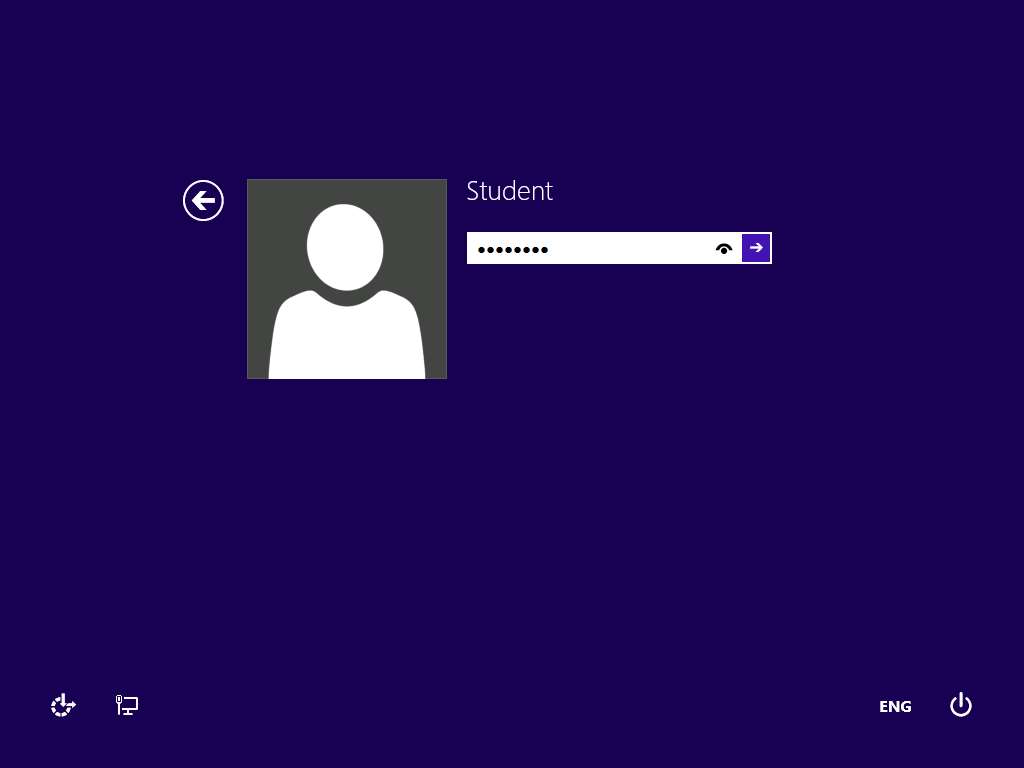
1. Click [FTP Server](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10). Click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10) and click **Back arrow** icon beside Jason user profile and then choose **Student** account to log in.





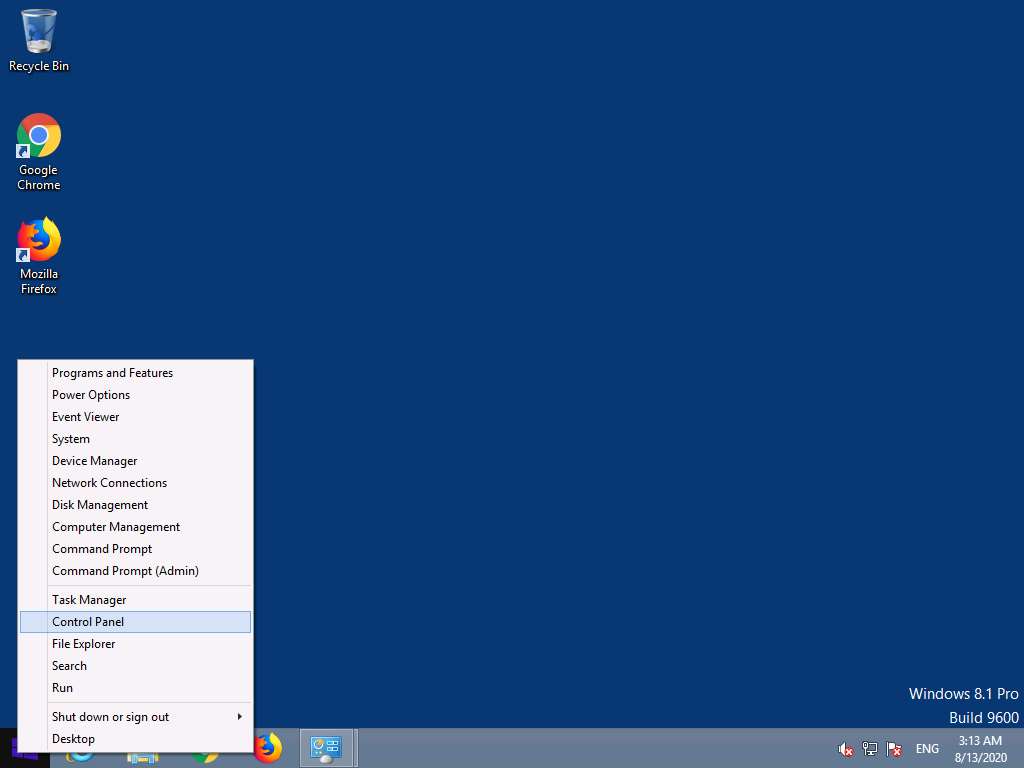


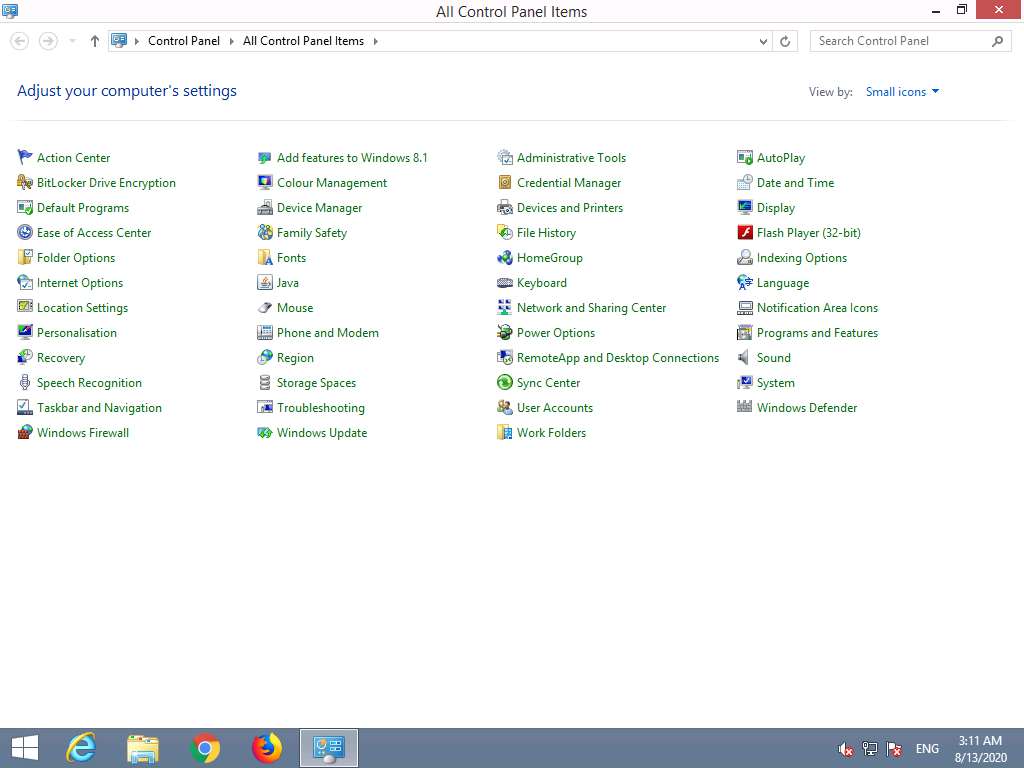
1. In the logon box password field click Pa$$w0rd.

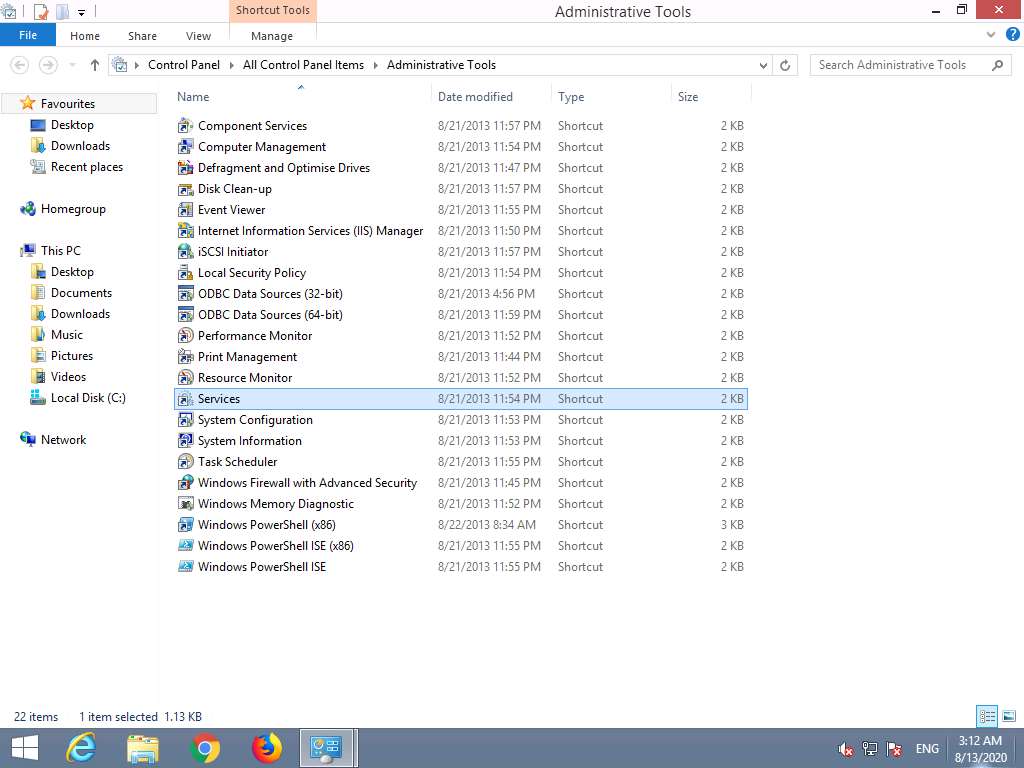


1. Right-click **Start** and click **Control Panel** from the context menu as shown in the screenshot. All Control Panel Items window appears, click **Administrative Tools**. In Administrative Tools window double-click **Services**.

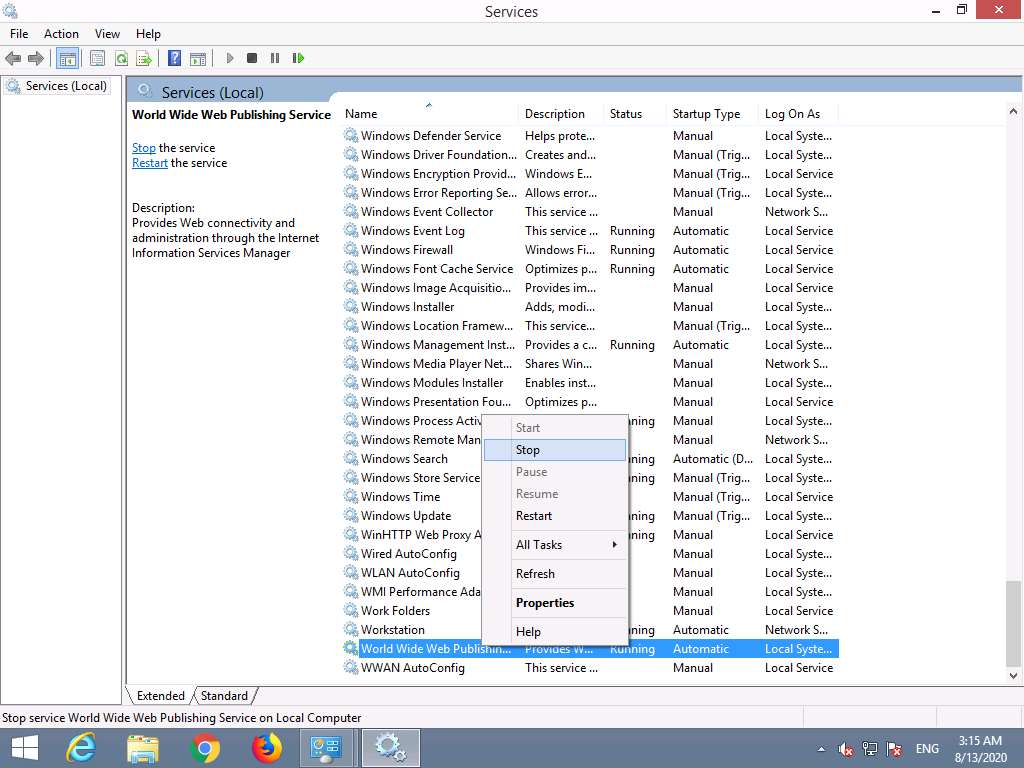
If any pop-up appears, click **No** to close.



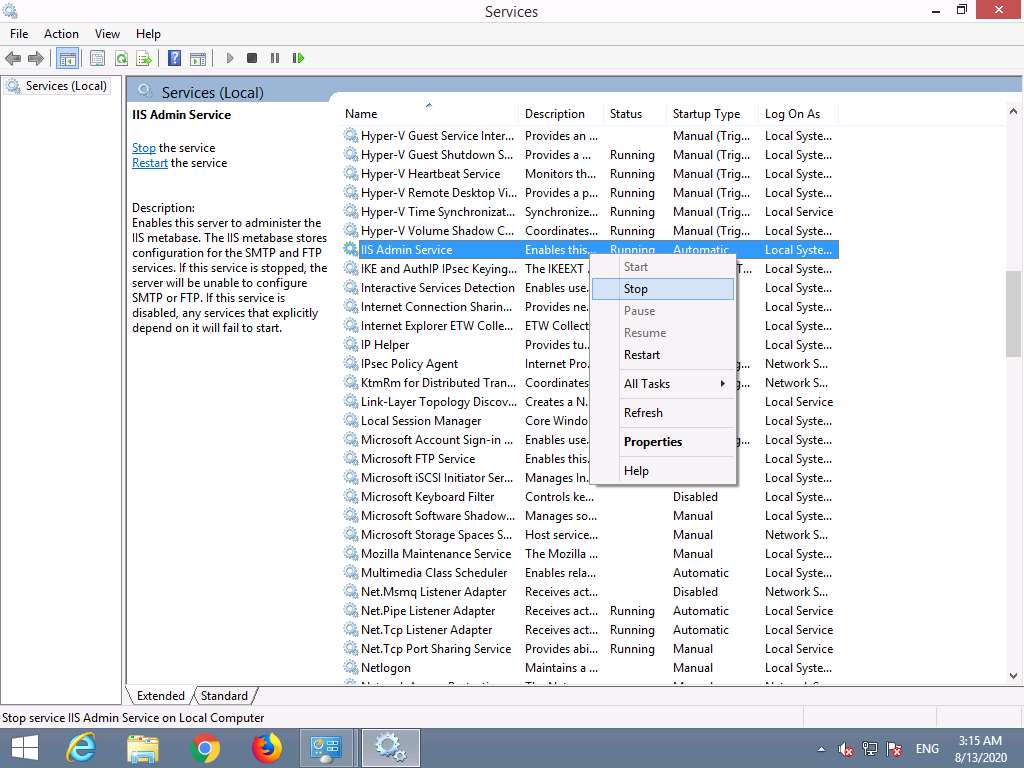




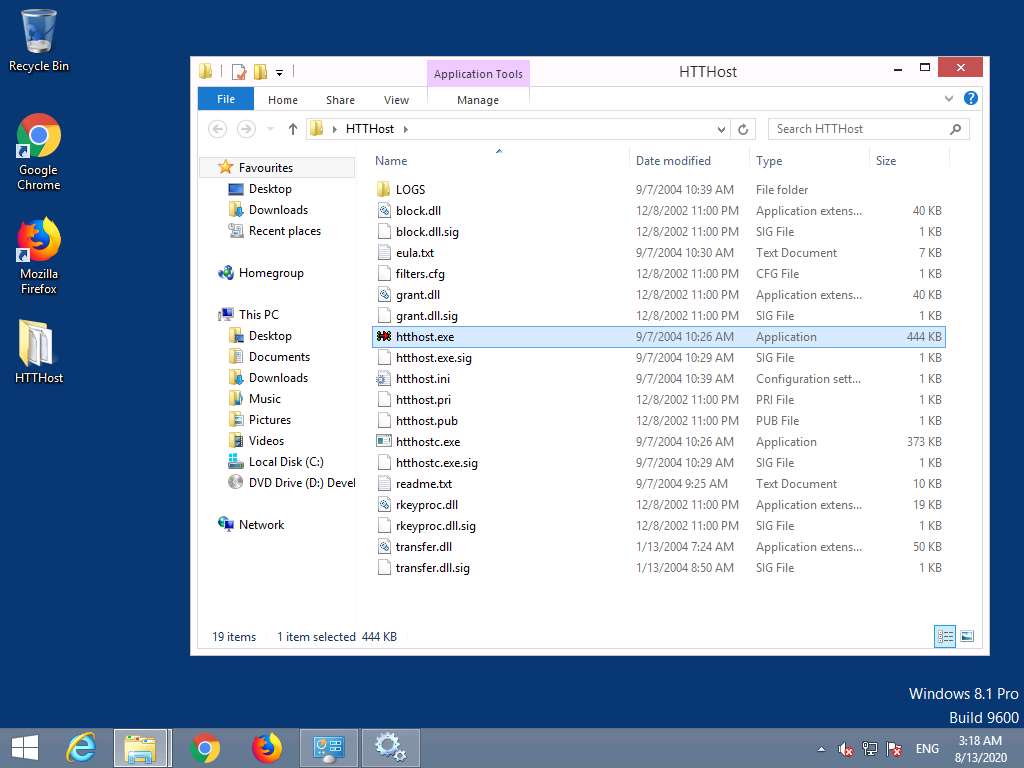
1. **Services** window appears. Scroll down and right-click on **World Wide Web Publishing Service** and click **Stop** option.



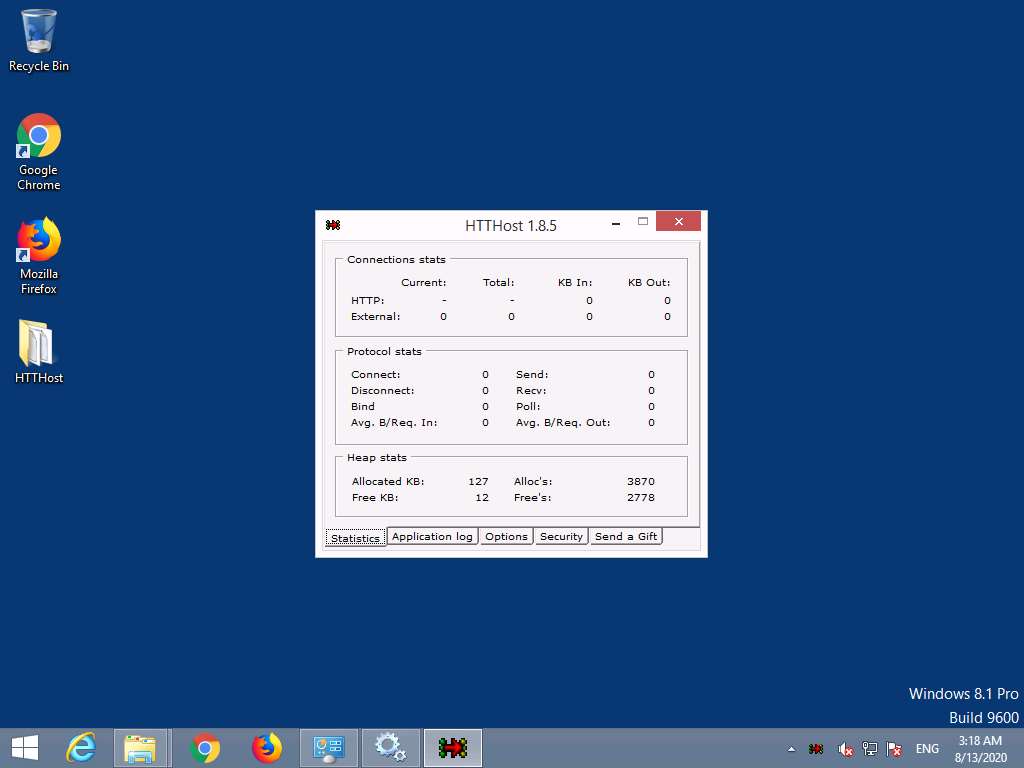
1. In the same way, Right-click on **IIS Admin Service** and click **Stop** option. Minimize the Services window.



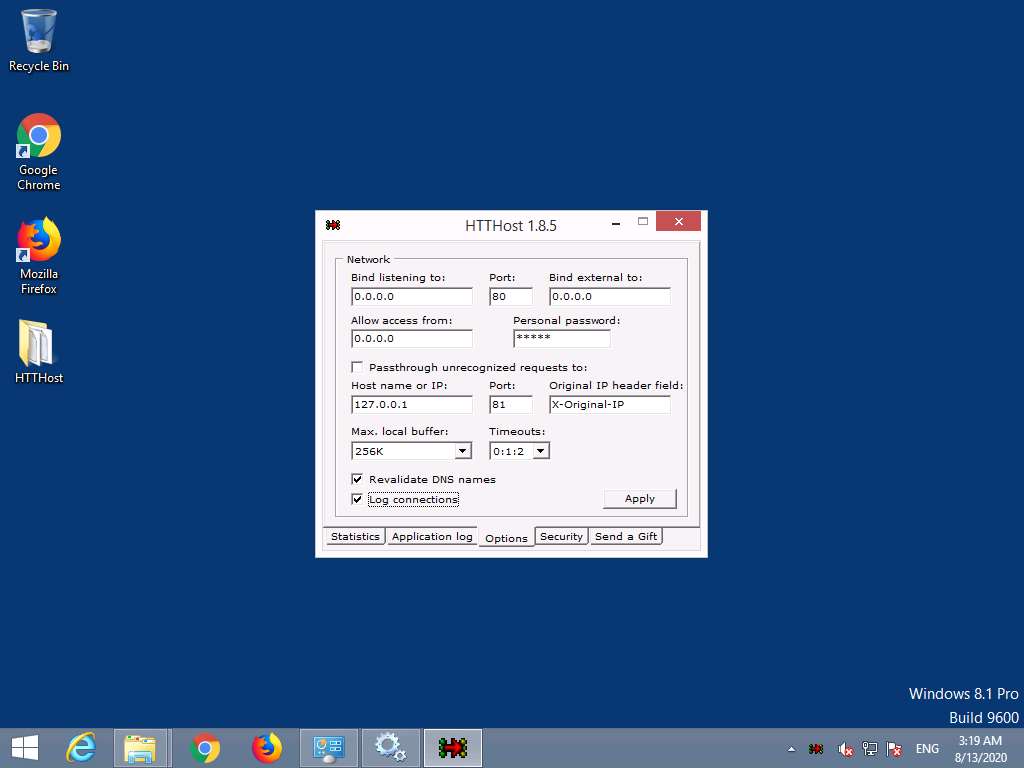
1. Double-click **HTTHost** folder on Desktop and double-click **htthost.exe**.



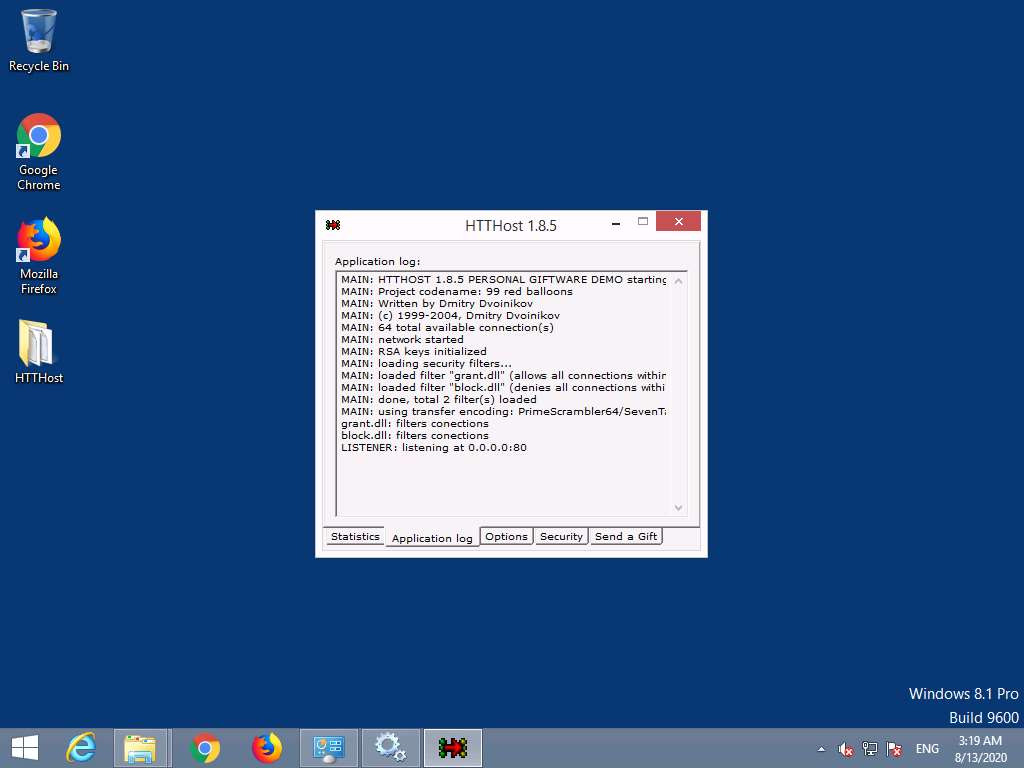
1. If The **Open File – Security Warning** pop-up appears on the screen, click **Run**.
2. The **HTTHost 1.8.5** window appears, as shown in the screenshot.



1. Select **Options** tab. In the Options tab, set all its settings to default except **Personal Password** field, which should be filled in with any password. In this lab, the personal password is set to **magic**. Check the **Revalidate DNS names** and **Log Connections** options, and click **Apply**.



1. Check if the last line is **Listener: listening at 0.0.0.0:80** in **Application** **Log**, which ensures that **HTTHost** is running properly and has started listening to port **80**.

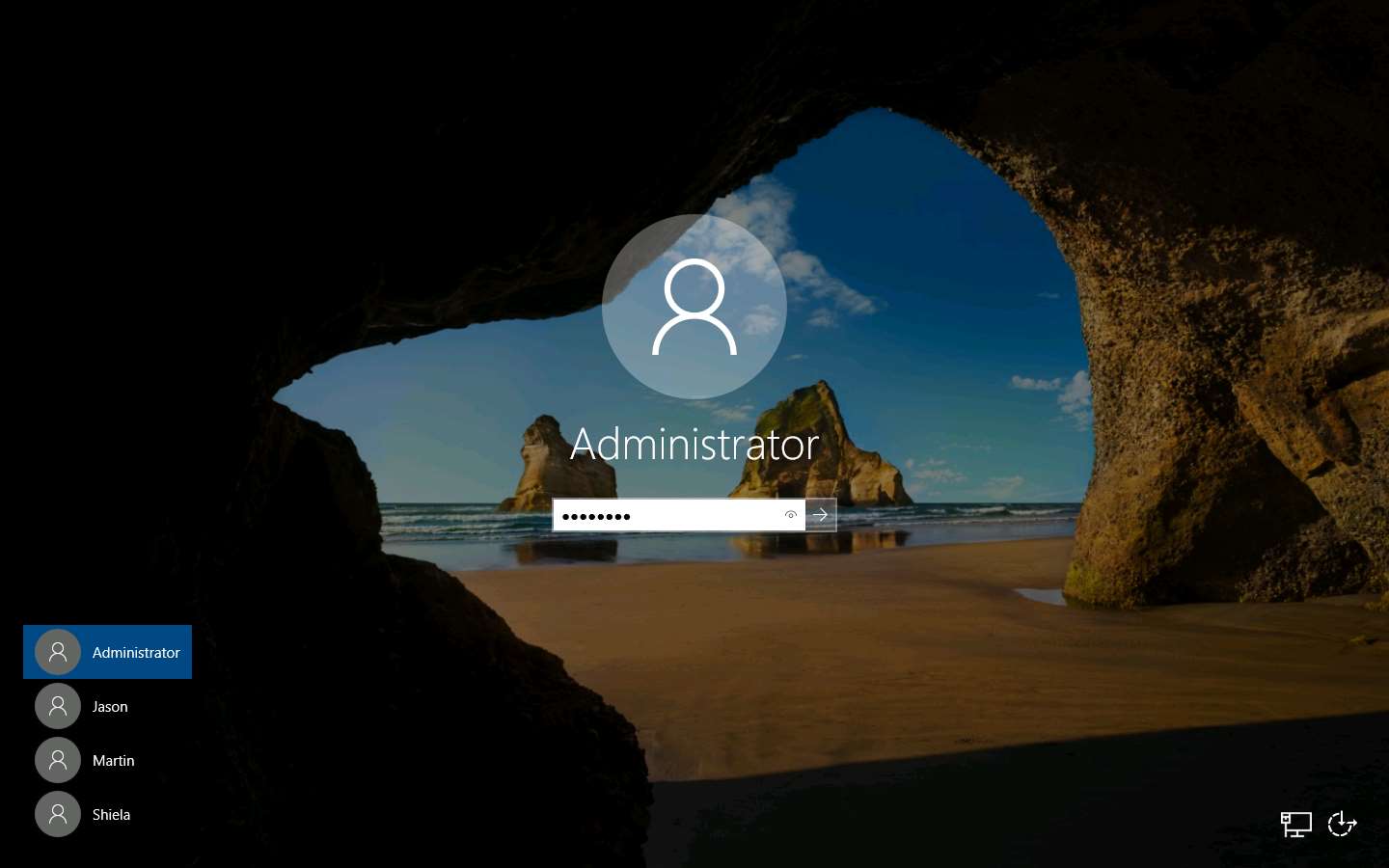


1. Close the **Services** console. Leave HTTHost running, and do not turn off the **FTP Server** machine.
2. Click [Windows Server 2019](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10) click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/2e9ecc61-2e0e-4b61-931e-5ada85a820dd?rc=10).

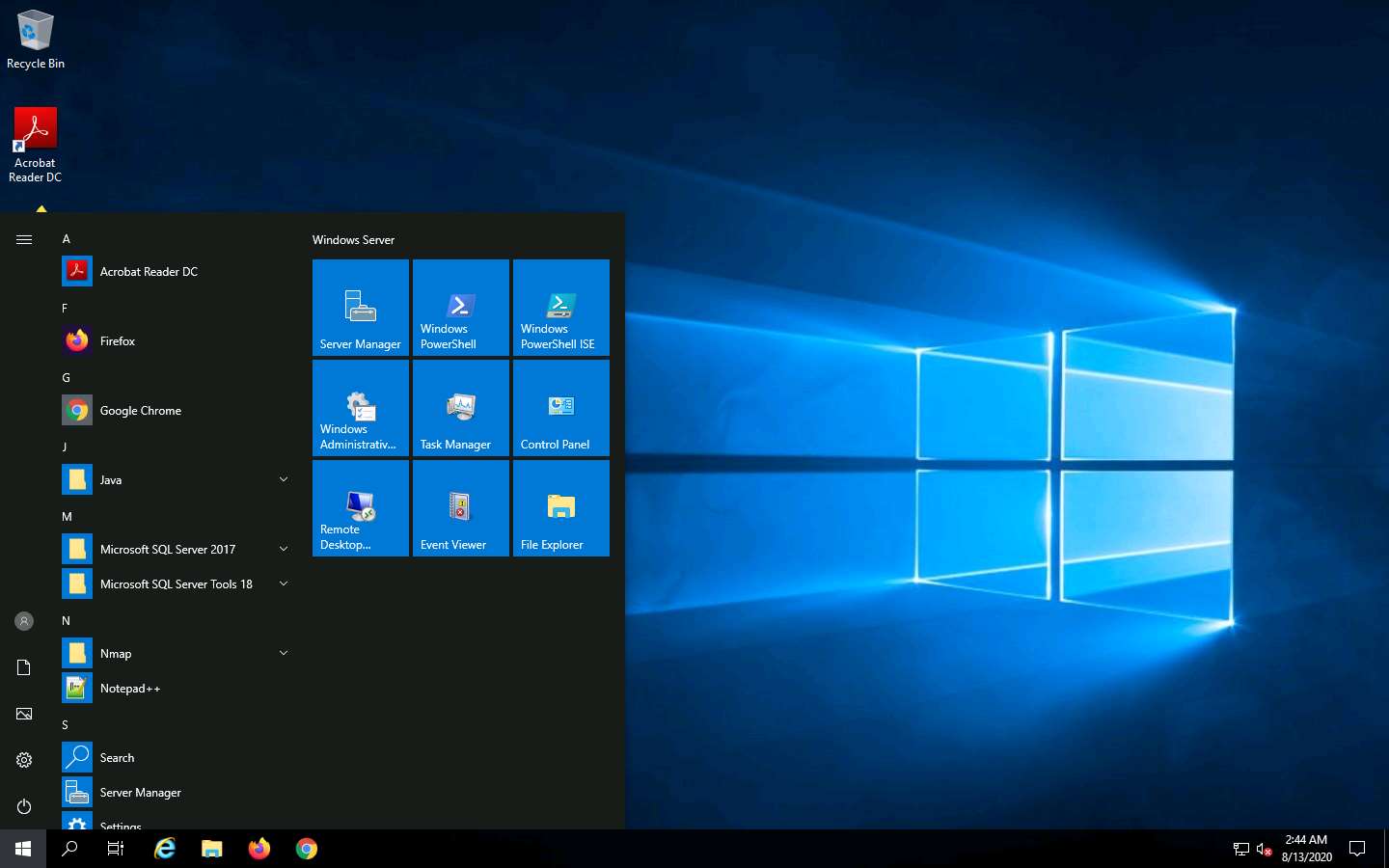


1. In the log on box click Pa$$w0rd and press **Enter**.

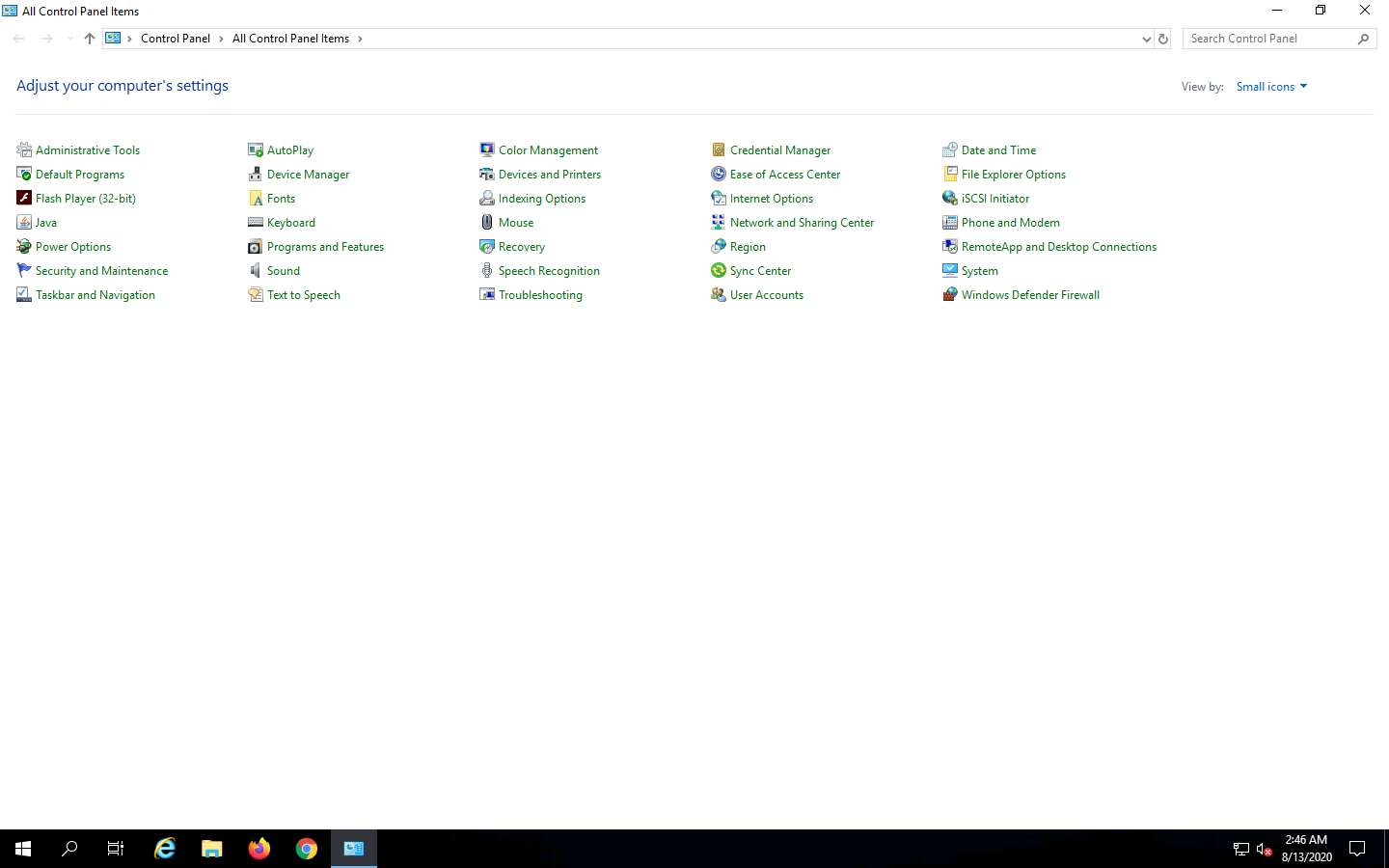
You can use the **Type Password** option from the **Commands** menu to enter the password.



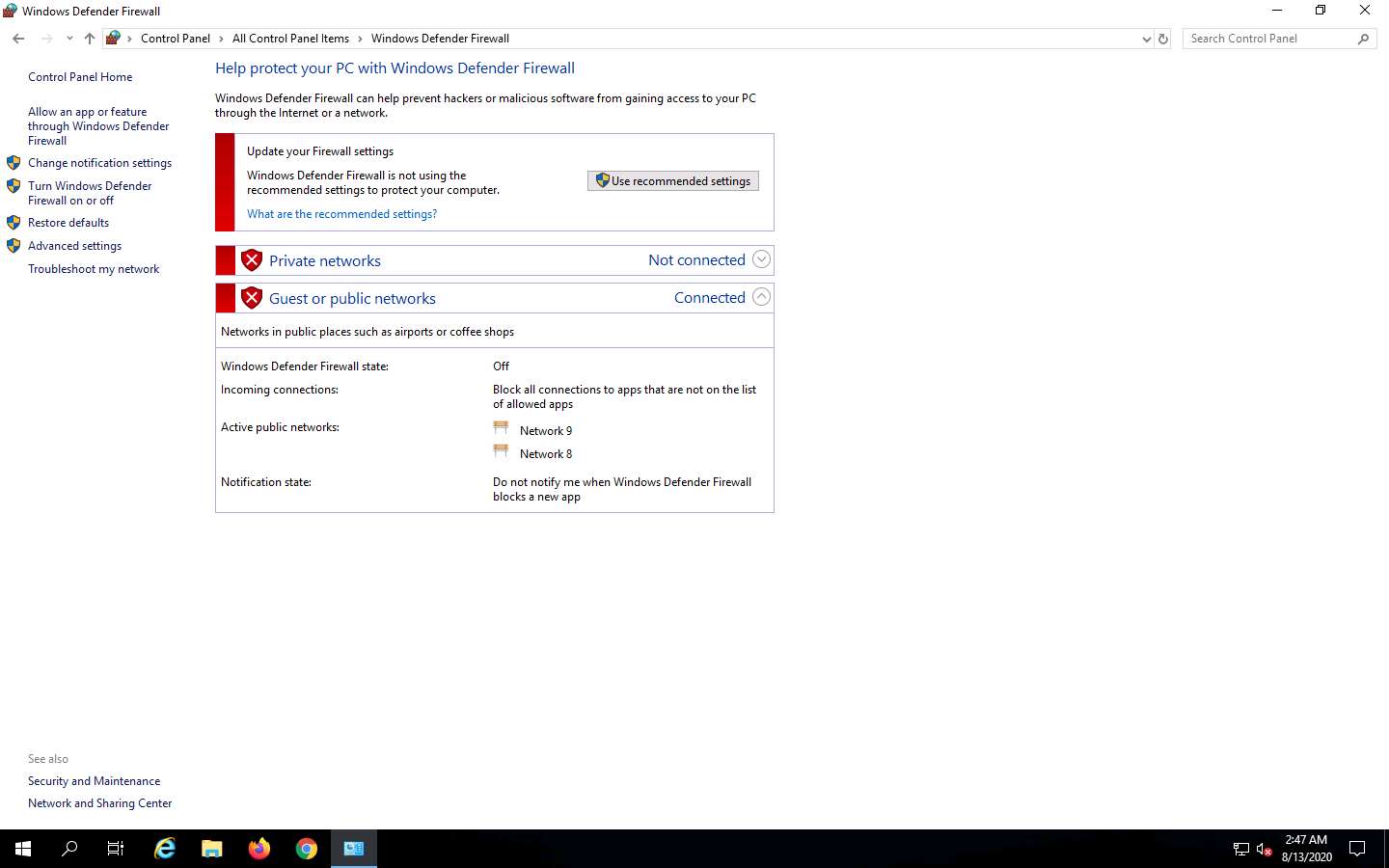
1. Launch **Control Panel**. To launch Control Panel click **Start** and click **Control Panel** app from the apps menu.



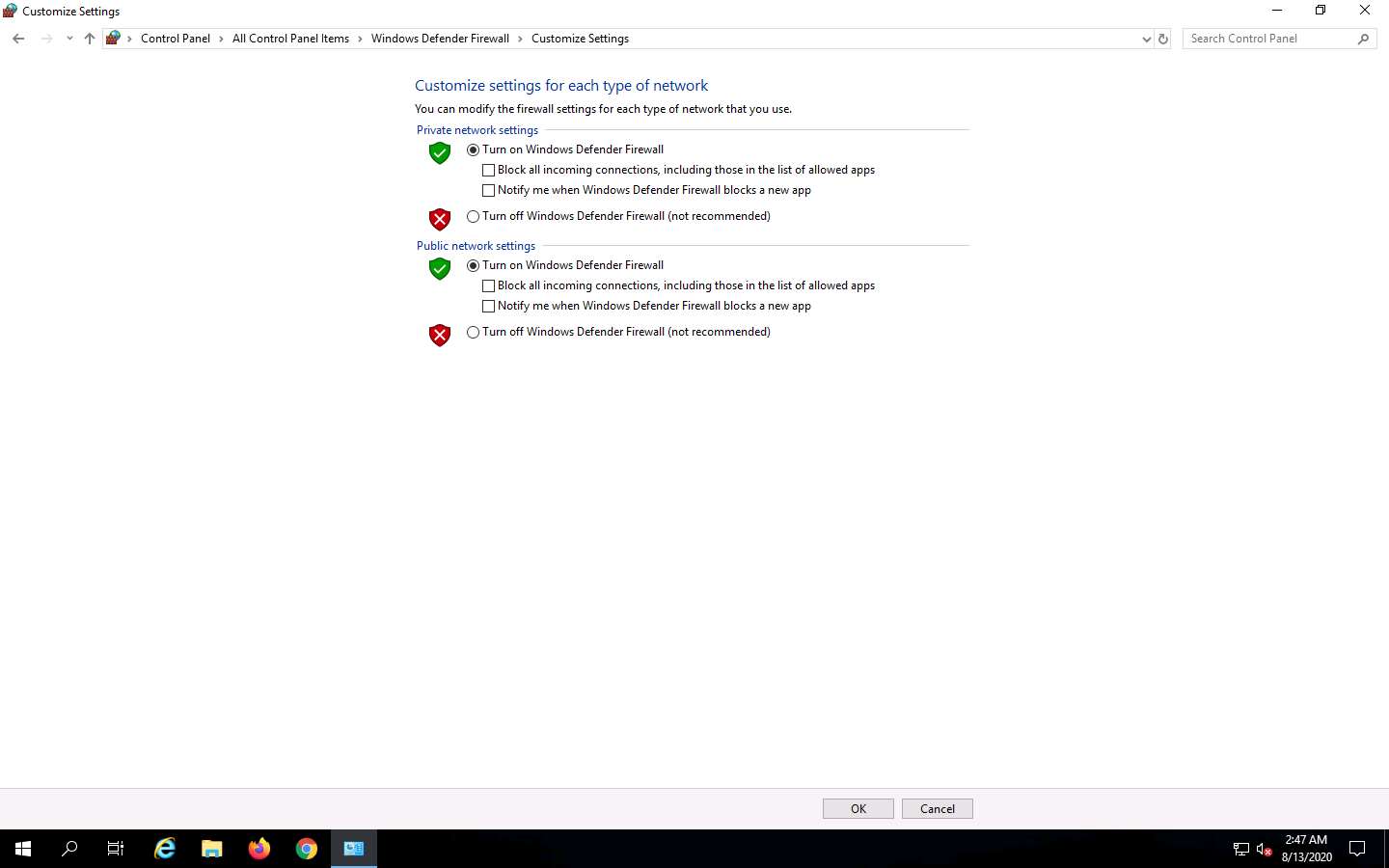
1. The **All Control Panel Items** window appears and displays all control panel items. Click **Windows Defender Firewall**.



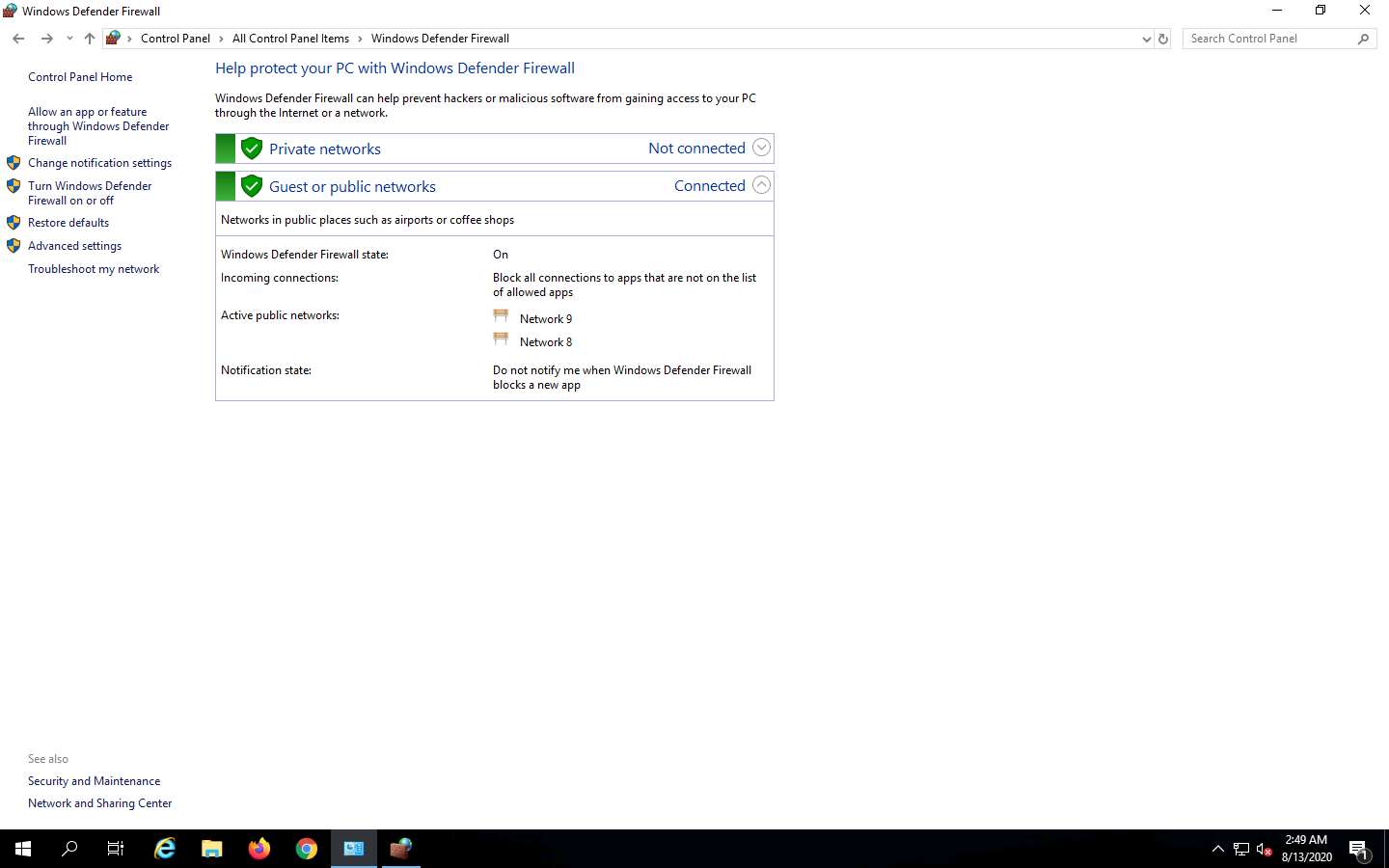
1. The **Windows Defender Firewall** control panel appears; click **Turn Windows Firewall on or off** link in the left pane.



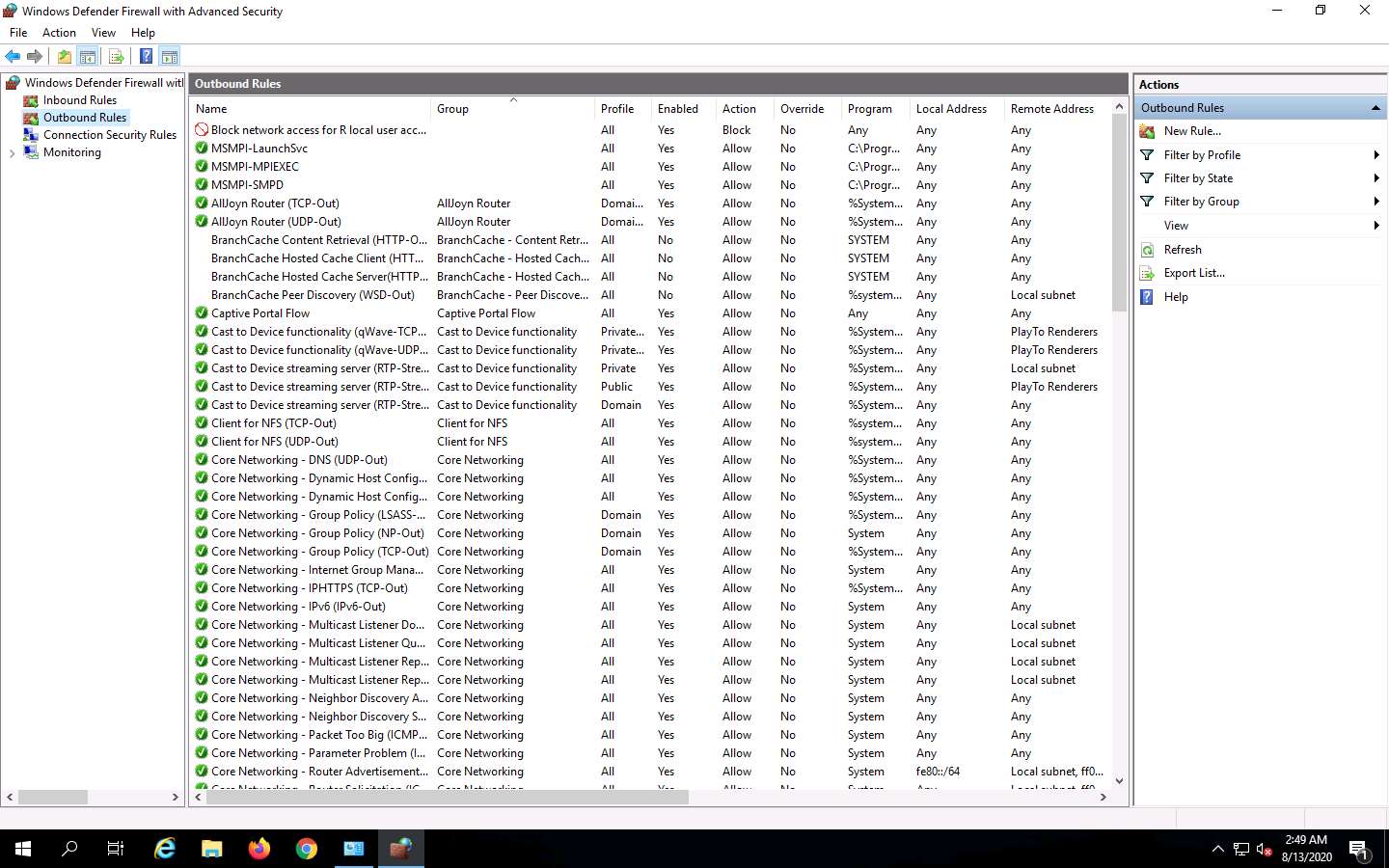
1. The **Customize settings** window appears. Select the **Turn on Windows Firewall** (under **Private network settings** and **Public network settings**). Click **OK**.



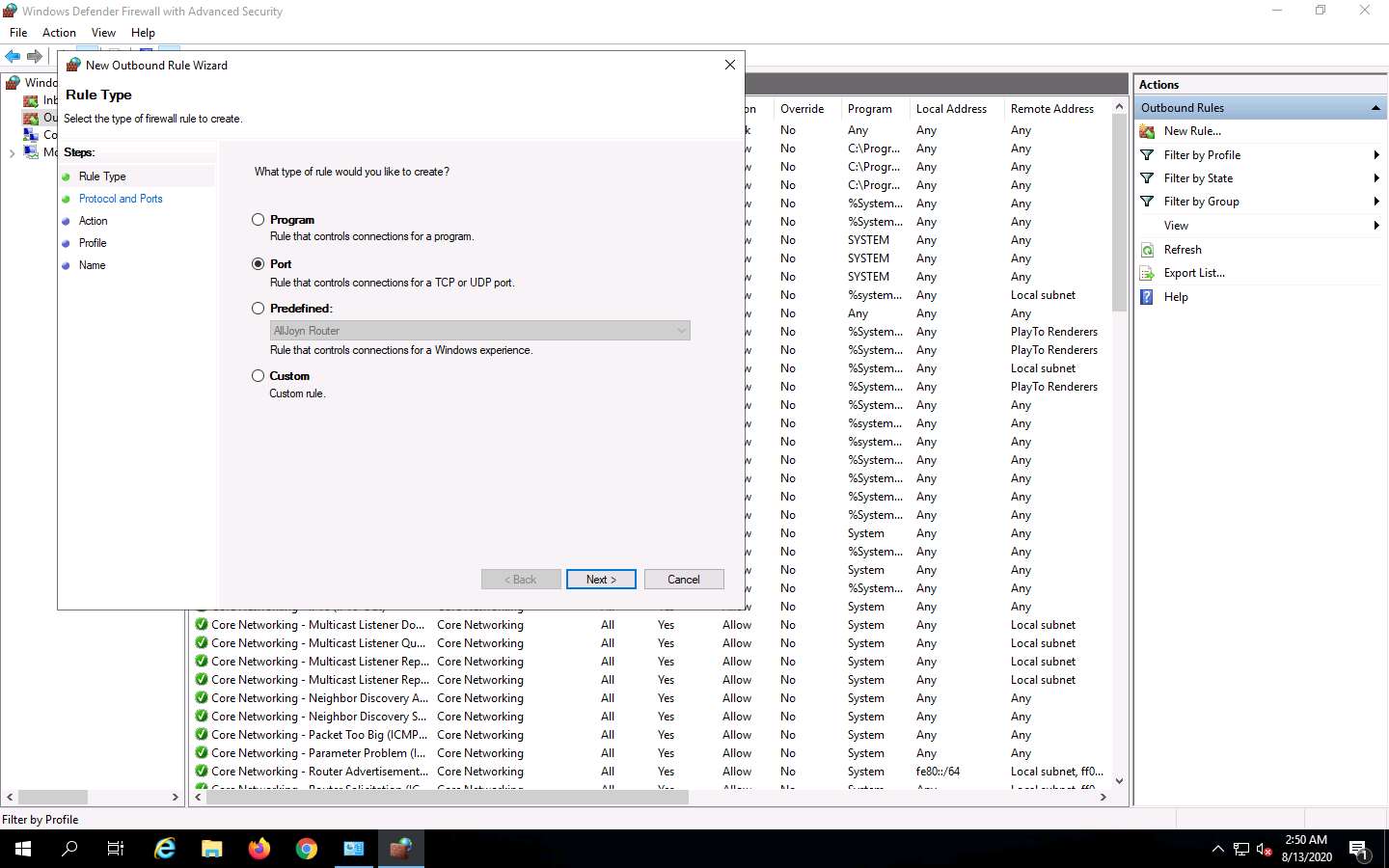
1. Firewall is successfully turned on. Now, click **Advanced settings** in the left pane.



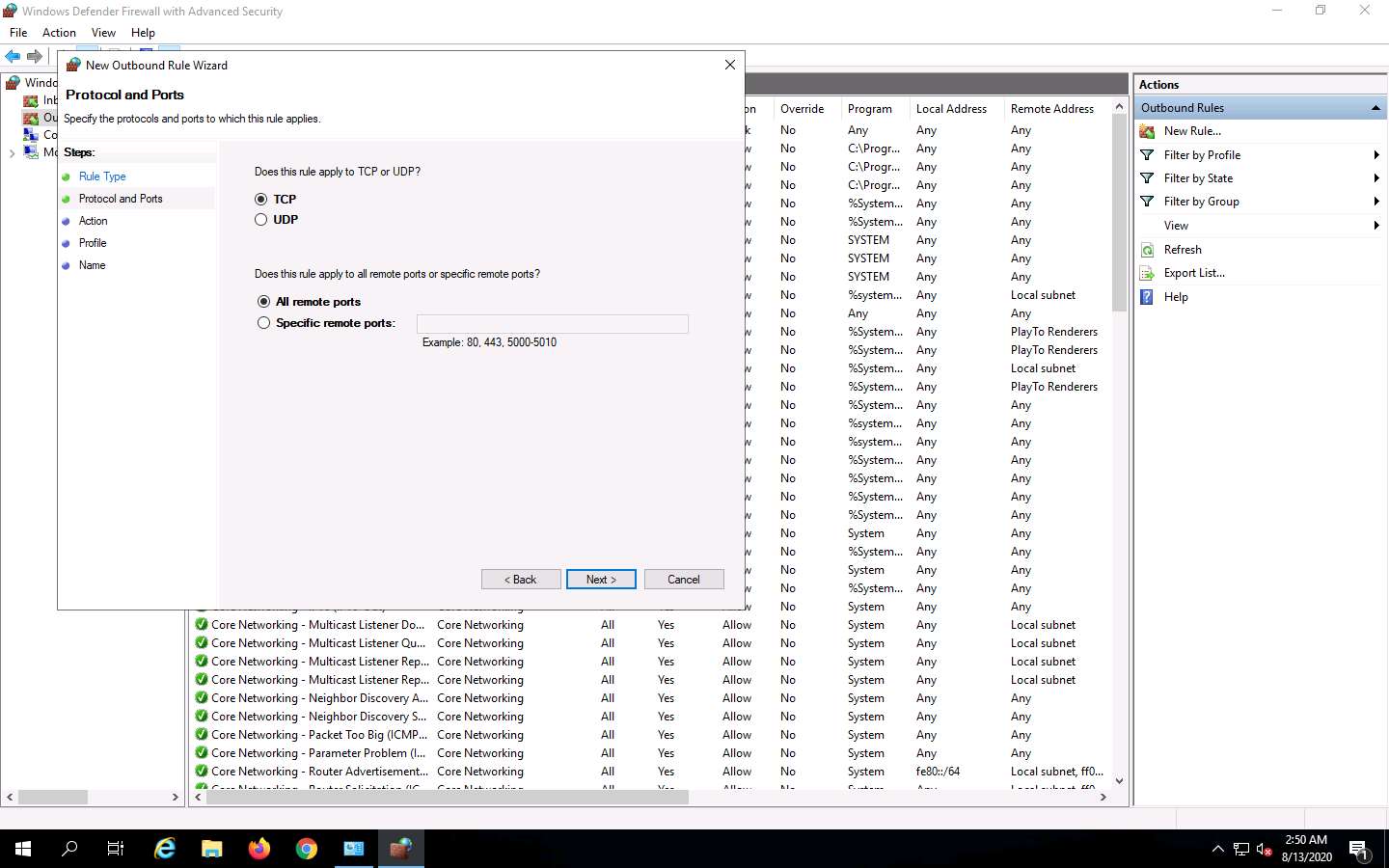
1. The **Windows Defender Firewall with Advanced Security** window appears. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule…** in the right pane (under **Outbound Rules**).



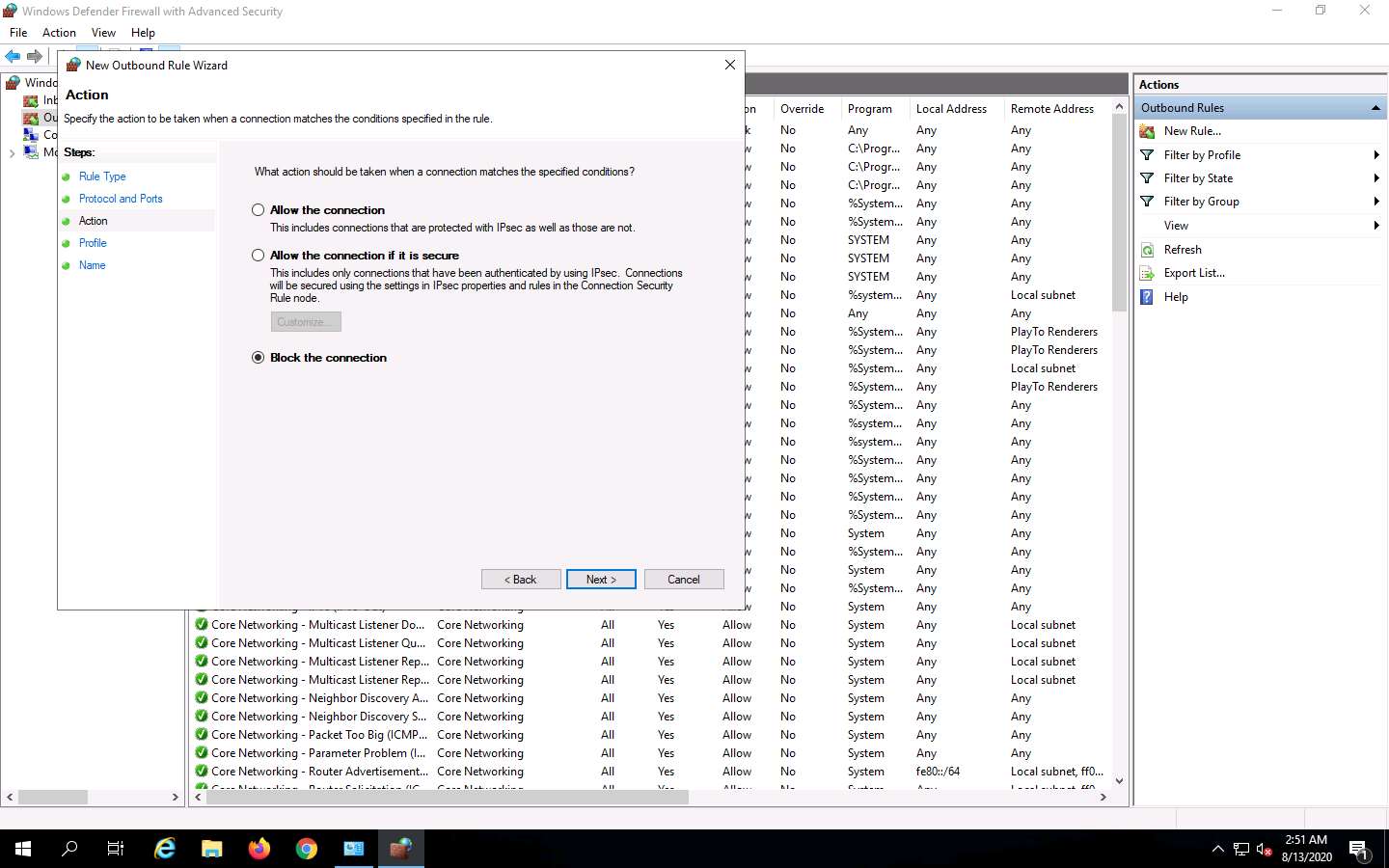
1. In the **New Outbound Rule Wizard**, select **Port** as the **Rule Type**, and click **Next**.



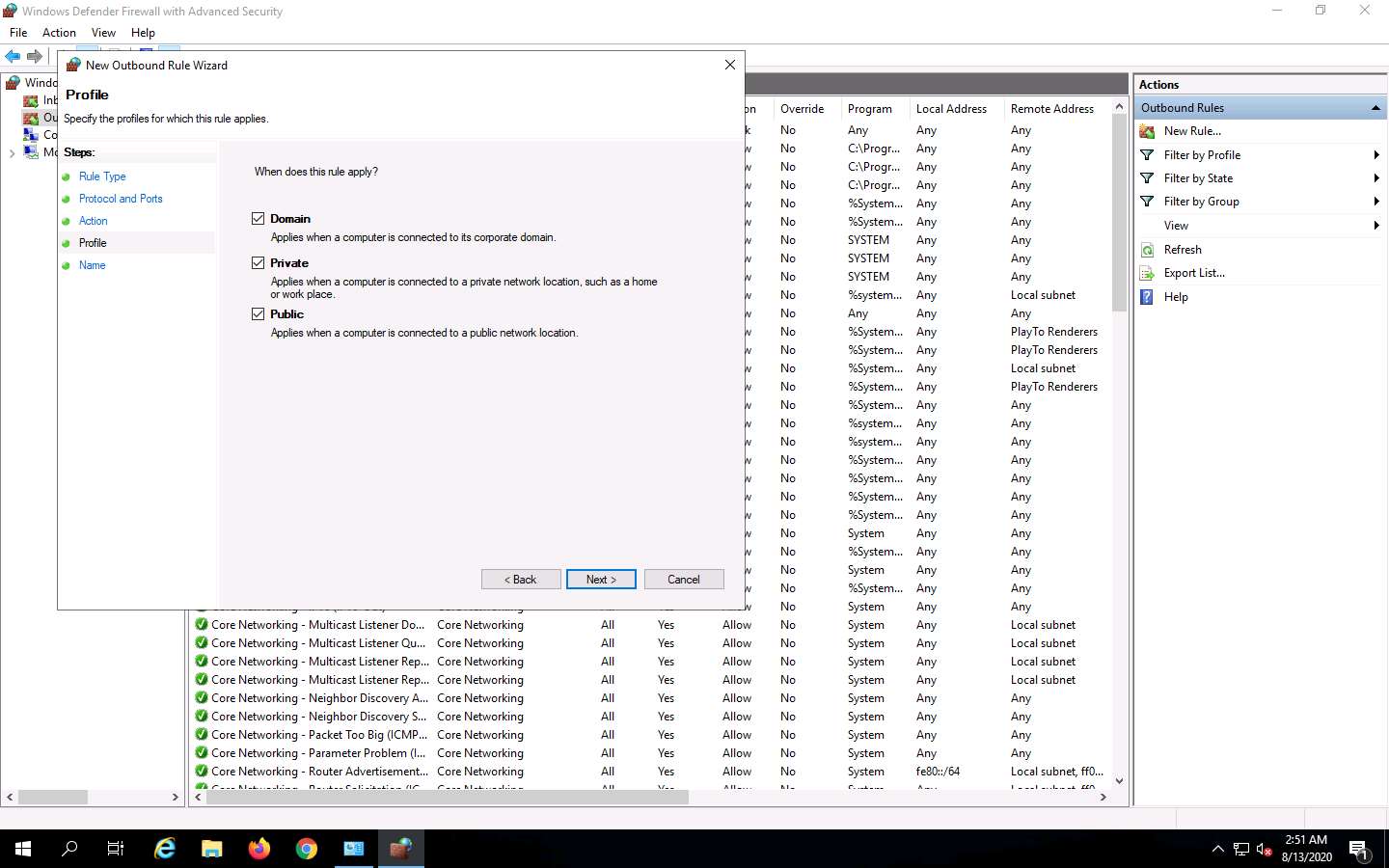
1. Select **All remote ports**, under **Protocol and Ports**, and click **Next**.



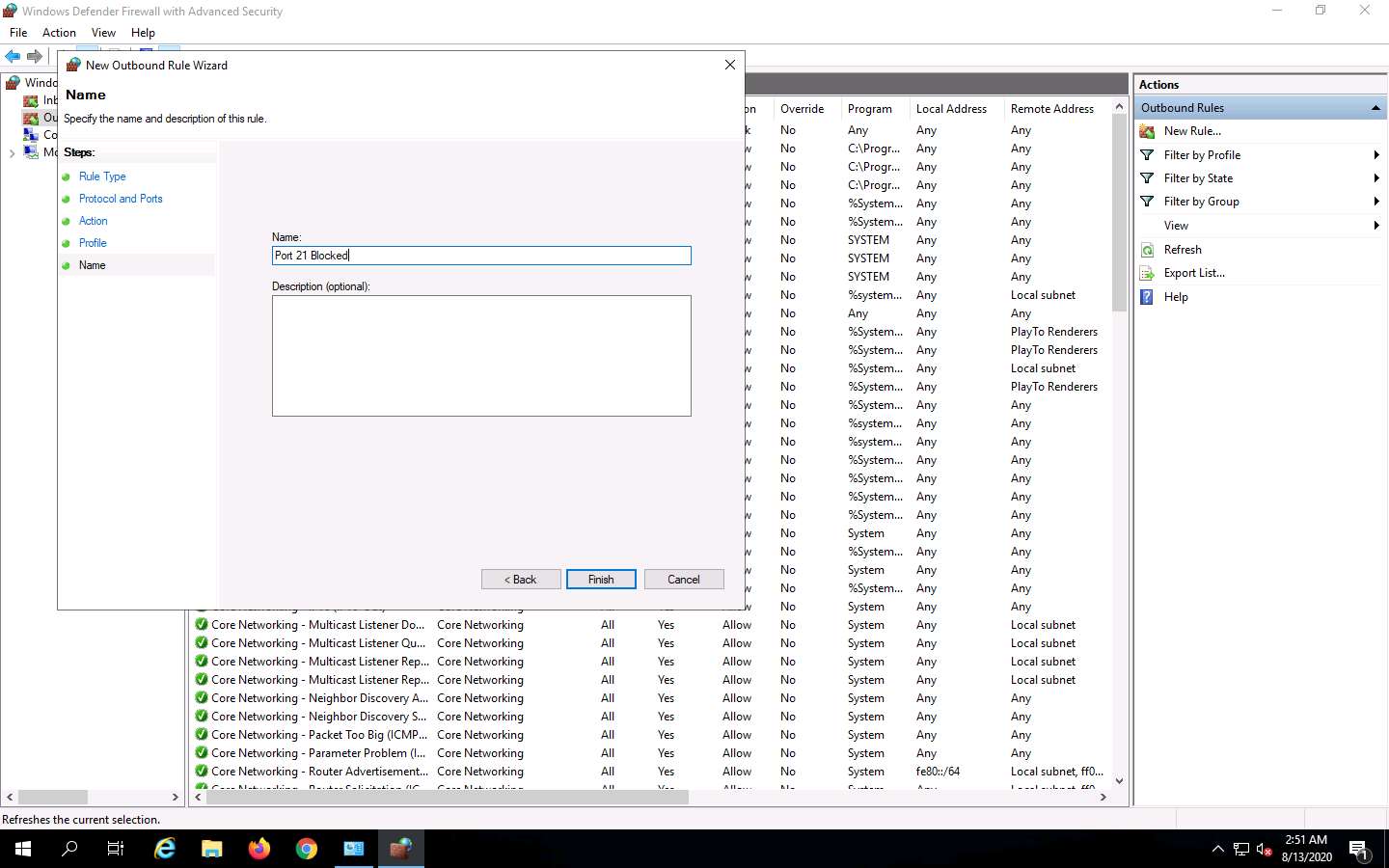
1. Under **Action**, **Block the connection** is selected by default. Click **Next**.



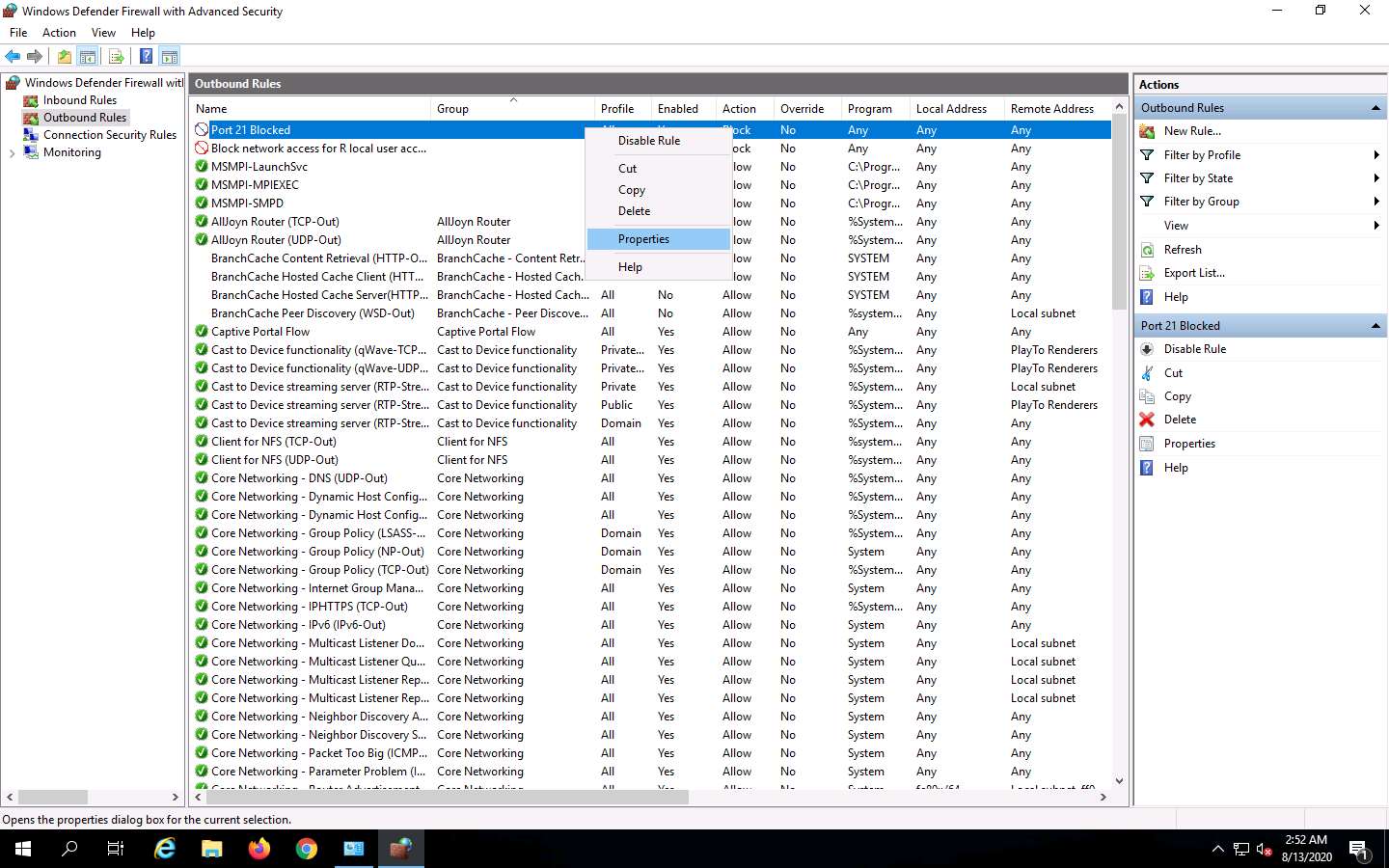
1. In the **Profile** section, ensure that all the options (Domain, Private and Public) are checked, and click **Next**.



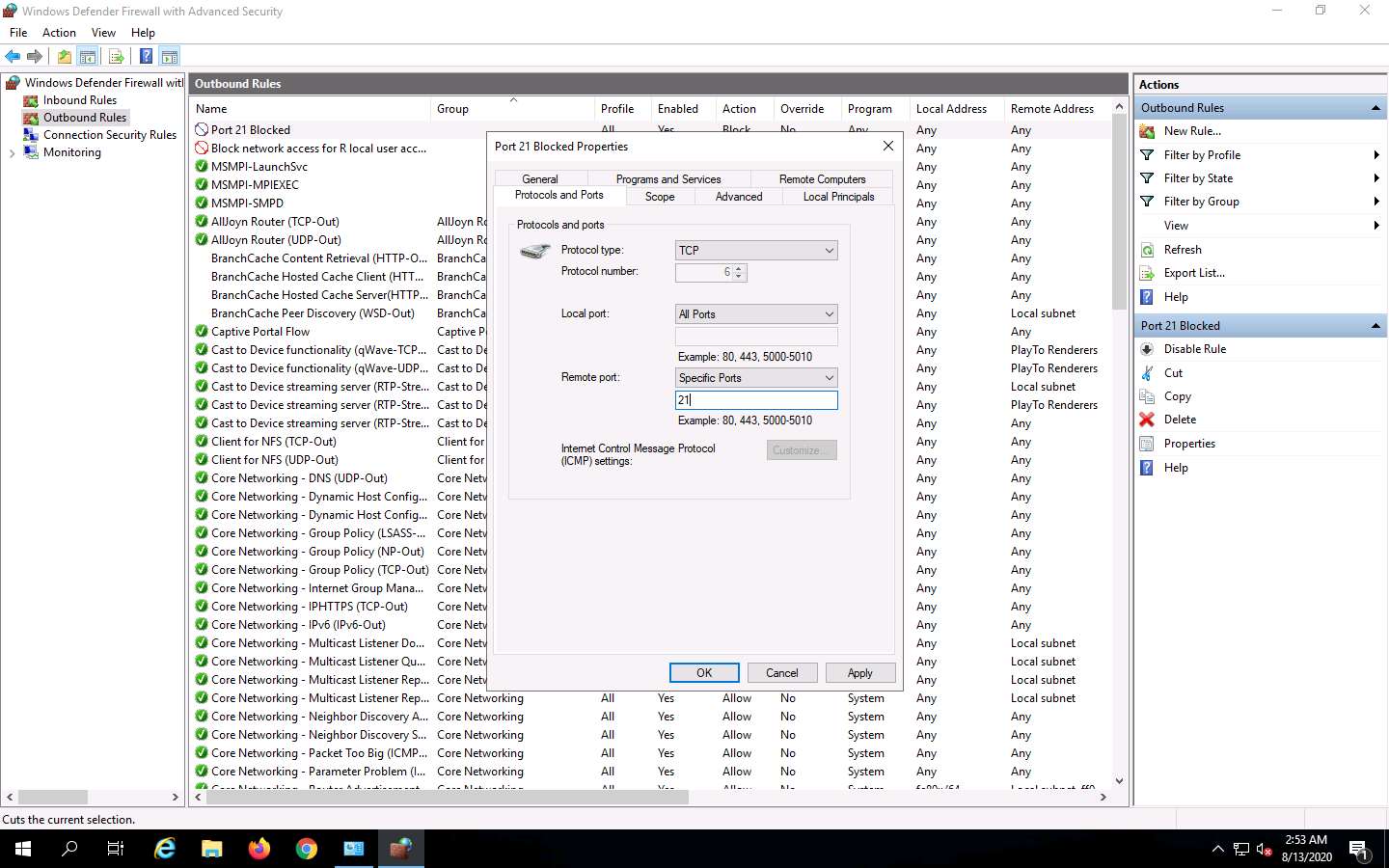
1. Under **Name**, type **Port 21 Blocked** in the **Name** field, and click **Finish**.



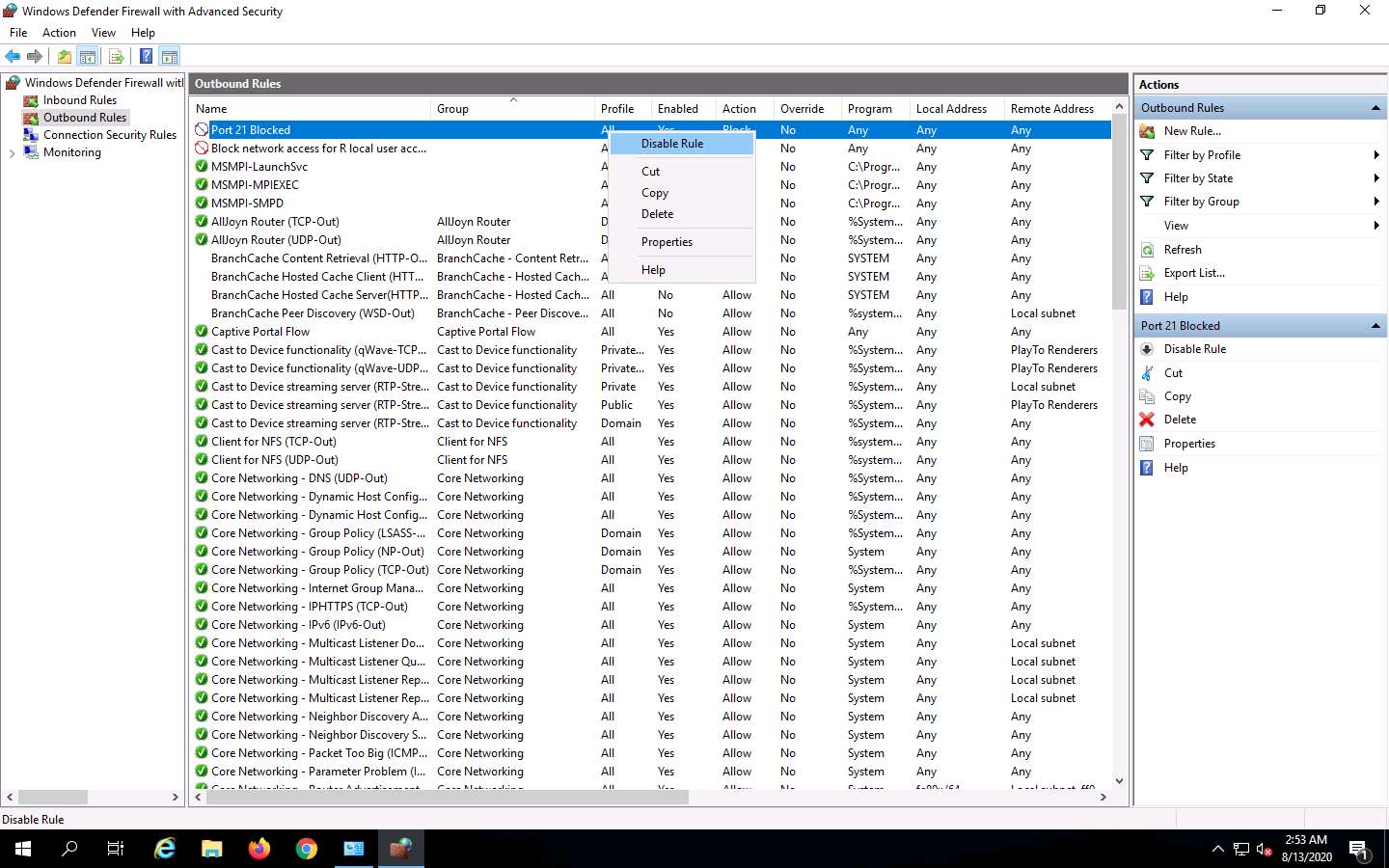
1. The new rule **Port 21 Blocked** is created, right-click the newly created rule (**Port 21 Blocked**), and click **Properties**.



1. The **Properties** window for **Port 21 Blocked** rule appears. Select the **Protocols and Ports** tab. In the **Remote Port** field, select **Specific Ports** option from the drop-down list and enter **21** as **Port Number**. Leave the other default settings, click **Apply**, and click **OK**.

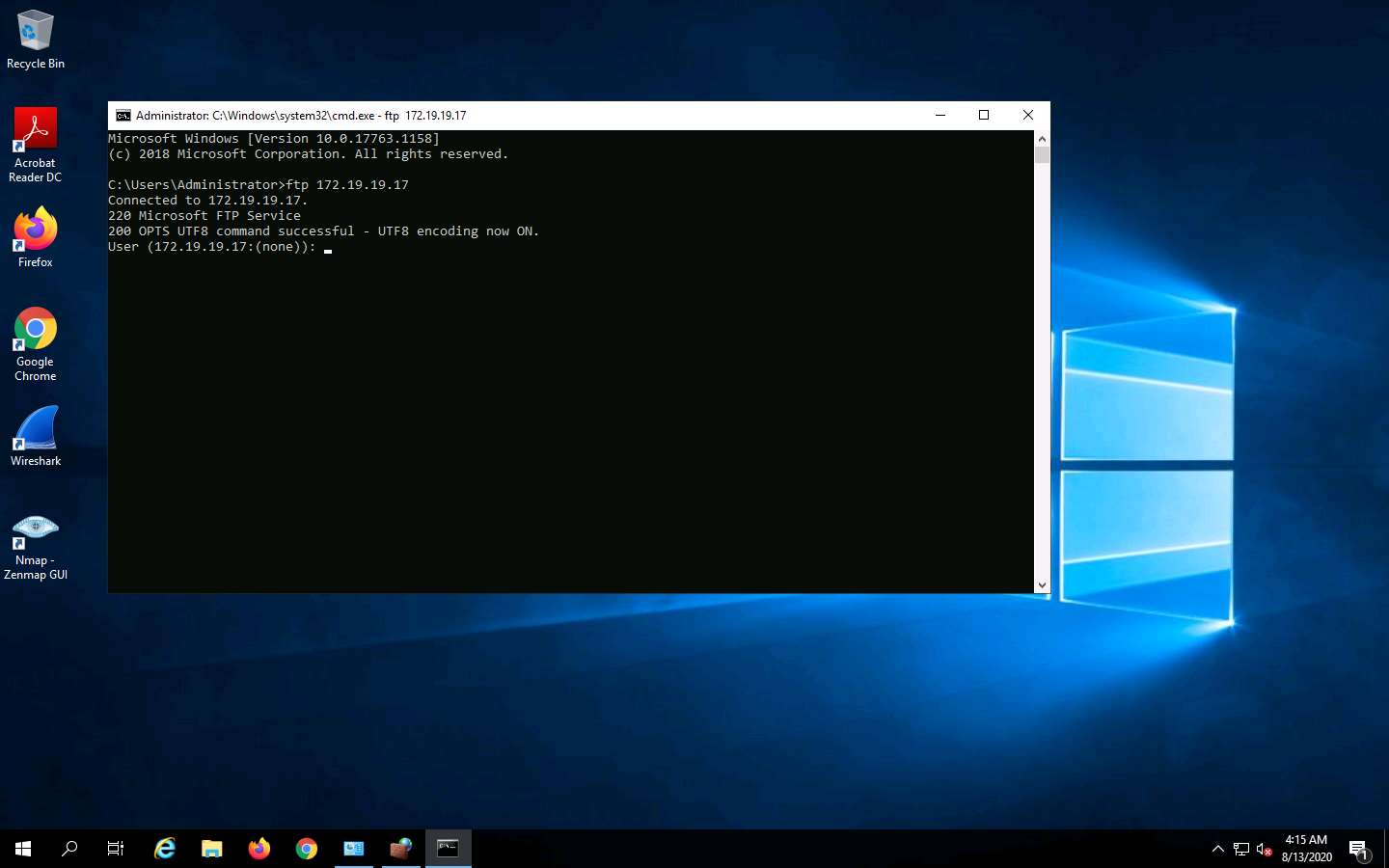


1. **Disable** the rule, and check if you are able to connect to the FTP site. Right-click the newly added rule, and click **Disable Rule**.

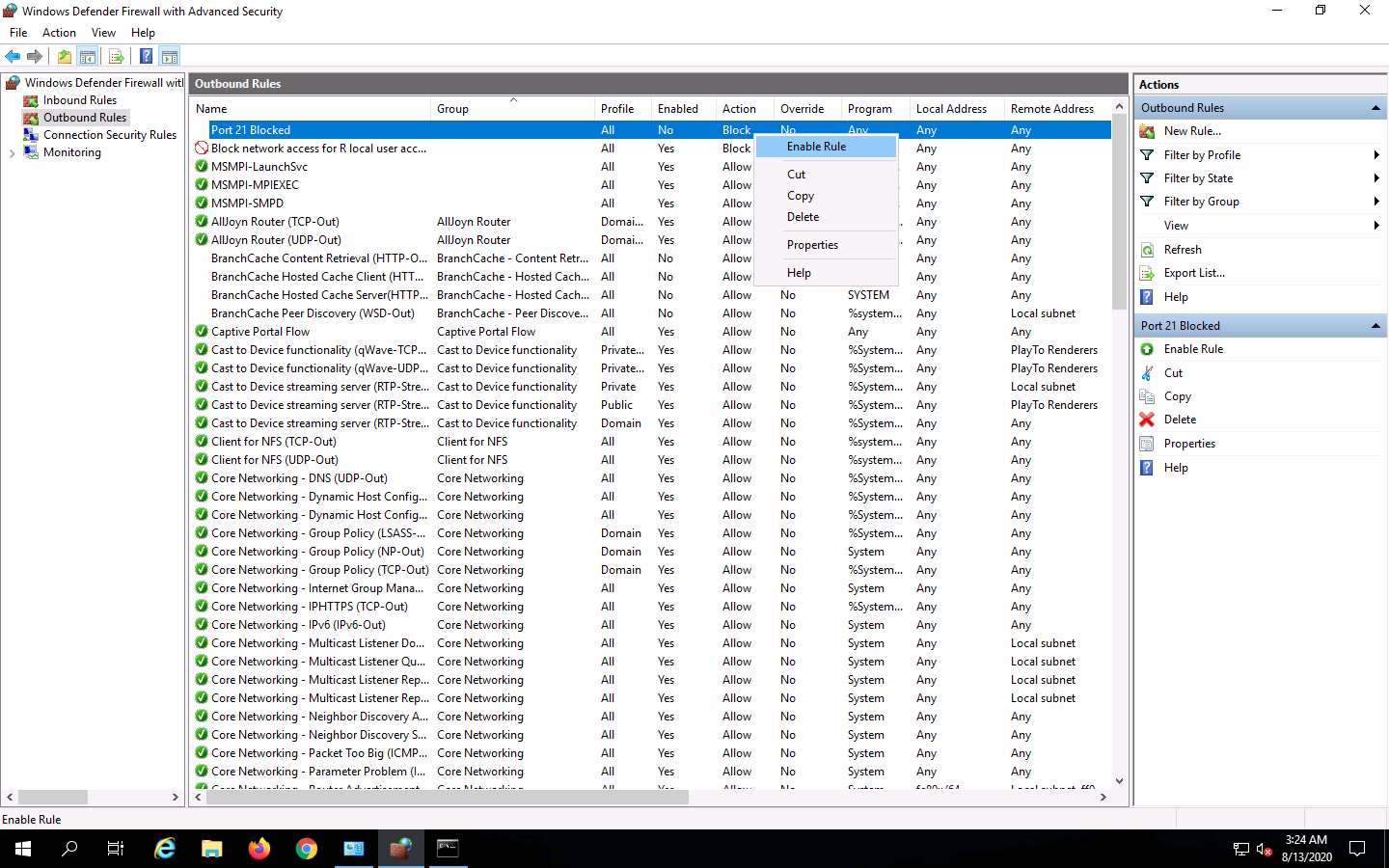


1. Launch the **command prompt**, and issue **ftp 172.19.19.17**. You will be asked to enter the username. This means you are able to establish an FTP connection. Press **Ctrl+C** to terminate the session. Minimize or close the command prompt.

172.19.19.17 is the IP address of the Sales Department machine.

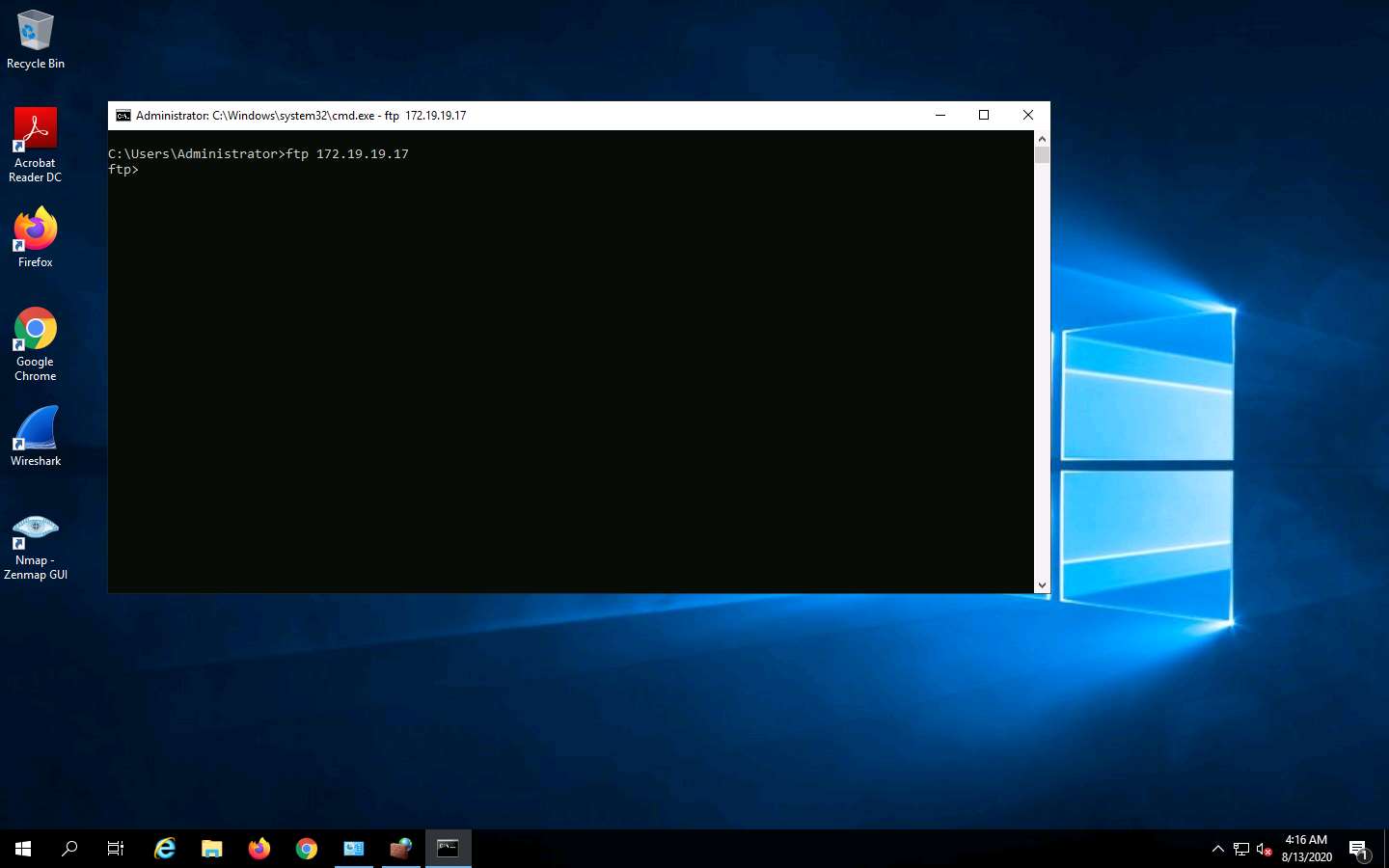


1. Maximize the Windows Defender Firewall with Advanced Security window. Now, enable the rule, and check whether you can establish a connection. Right-click the newly added rule, and click **Enable Rule**.

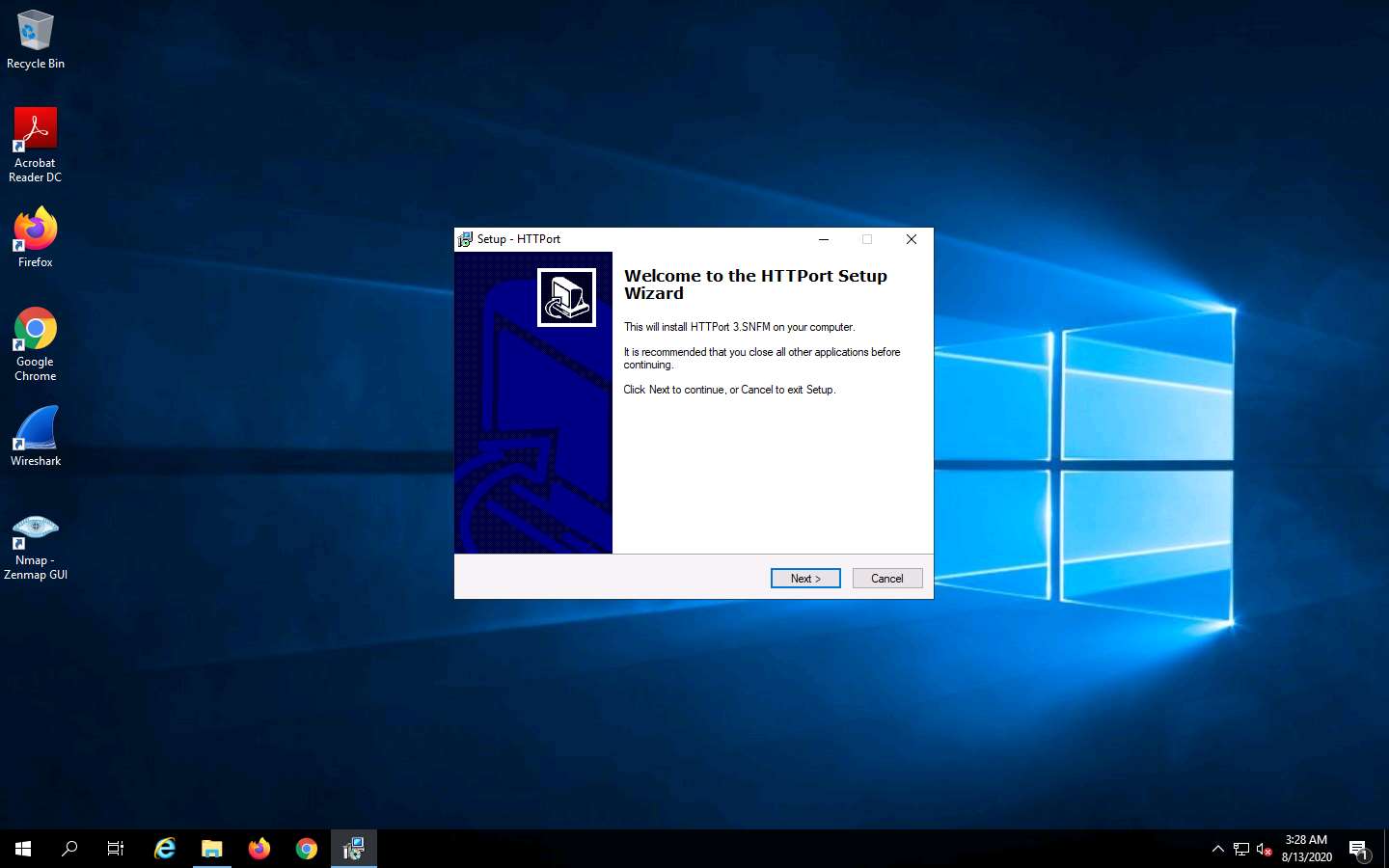


1. Launch the **Command Prompt** and check whether you are able to connect to the FTP site by issuing the command **ftp 172.19.19.17**. The added outbound rule should block the connection shown in the screenshot.

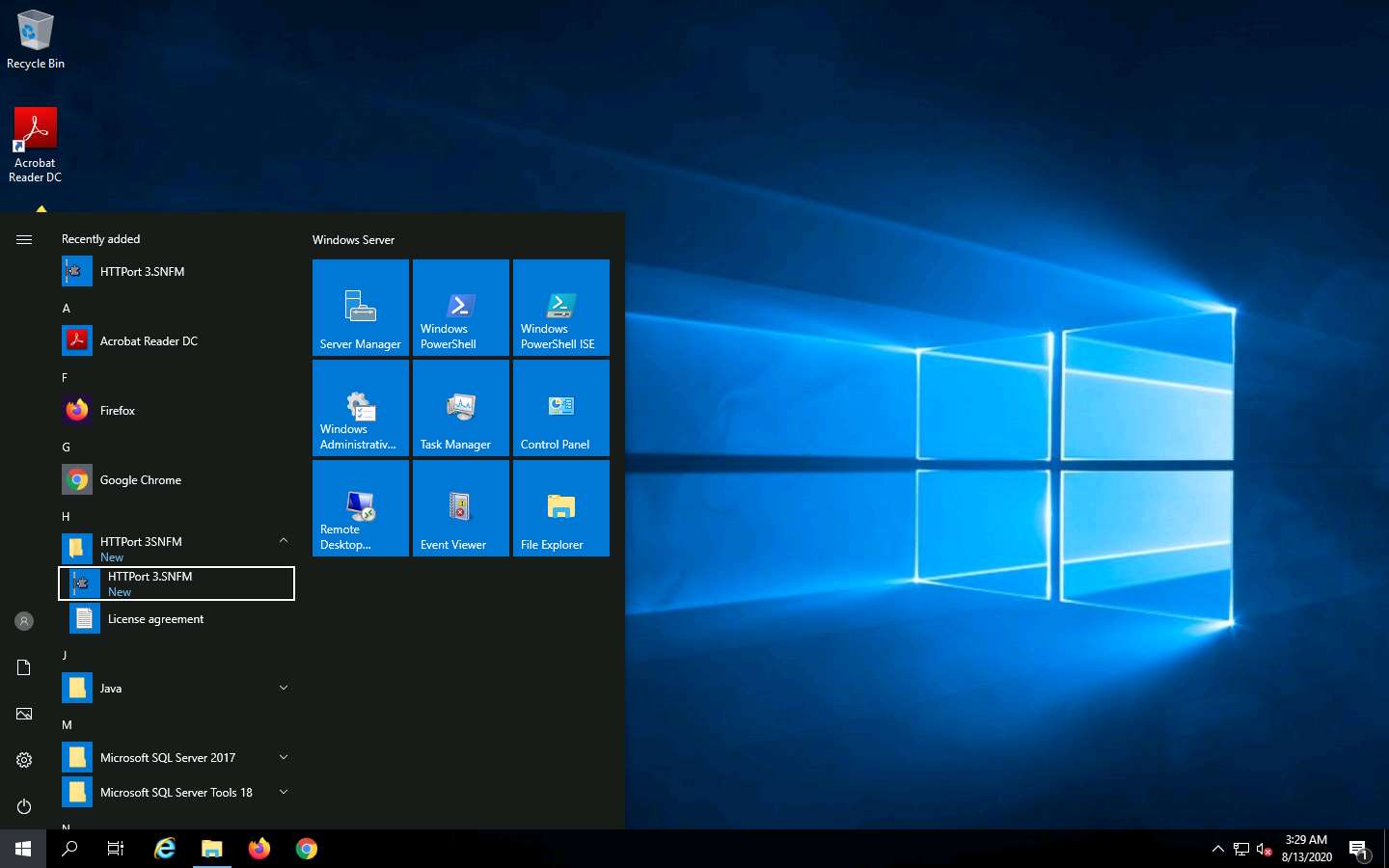
If you are not asked to enter credentials, it means that the connection is blocked.



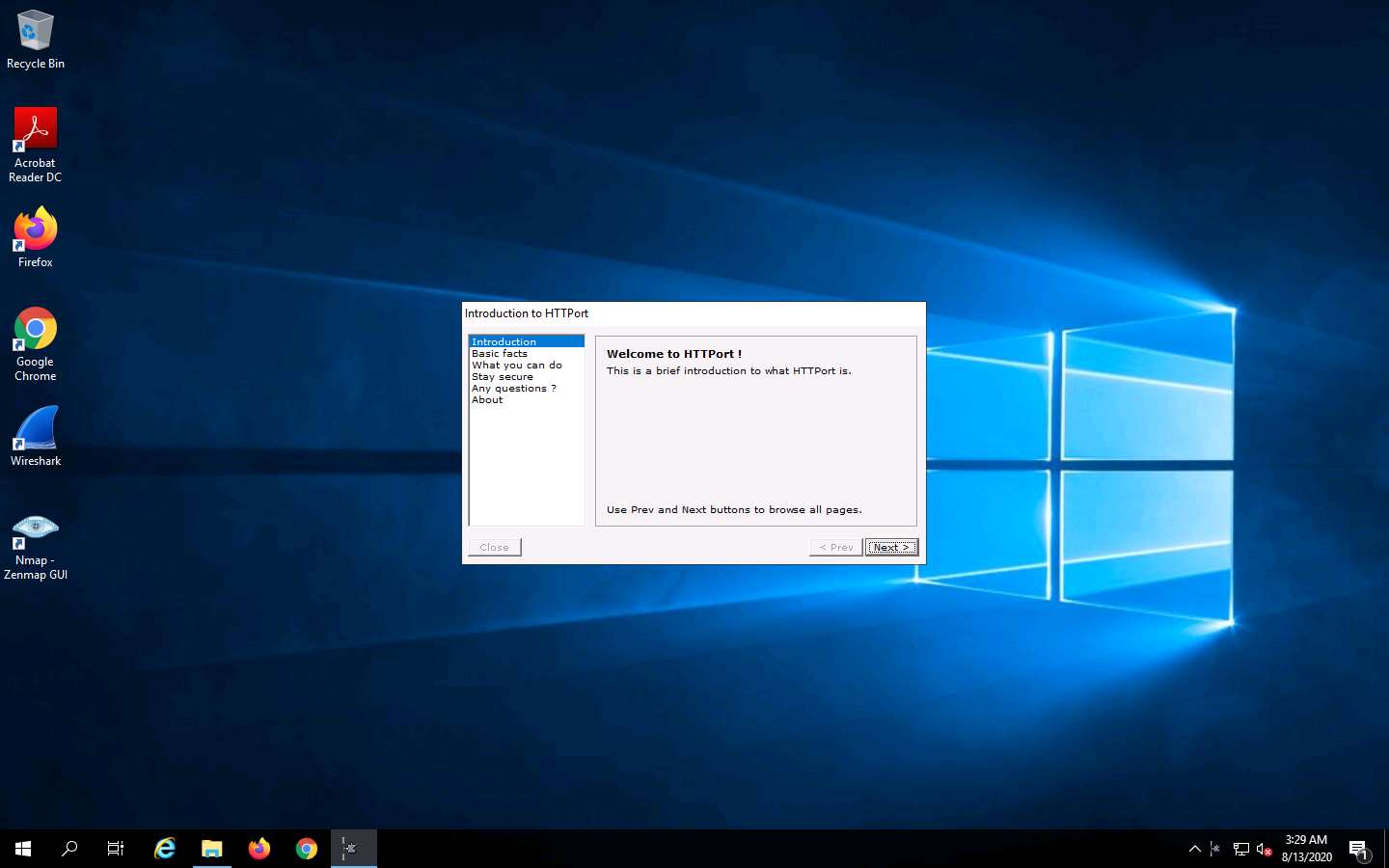
1. Close all the windows. Now, perform tunneling using **HTTPort** to establish a connection with the **FTP site** located on **FTP Server** machine.
2. Navigate to **E:\CPENT Module 07 Network Penetration Testing Methodology-Perimeter Devices\HTTP Tunneling** and double-click **httport3snfm.exe**. Follow the wizard-driven installation steps to install **HTTPort**.

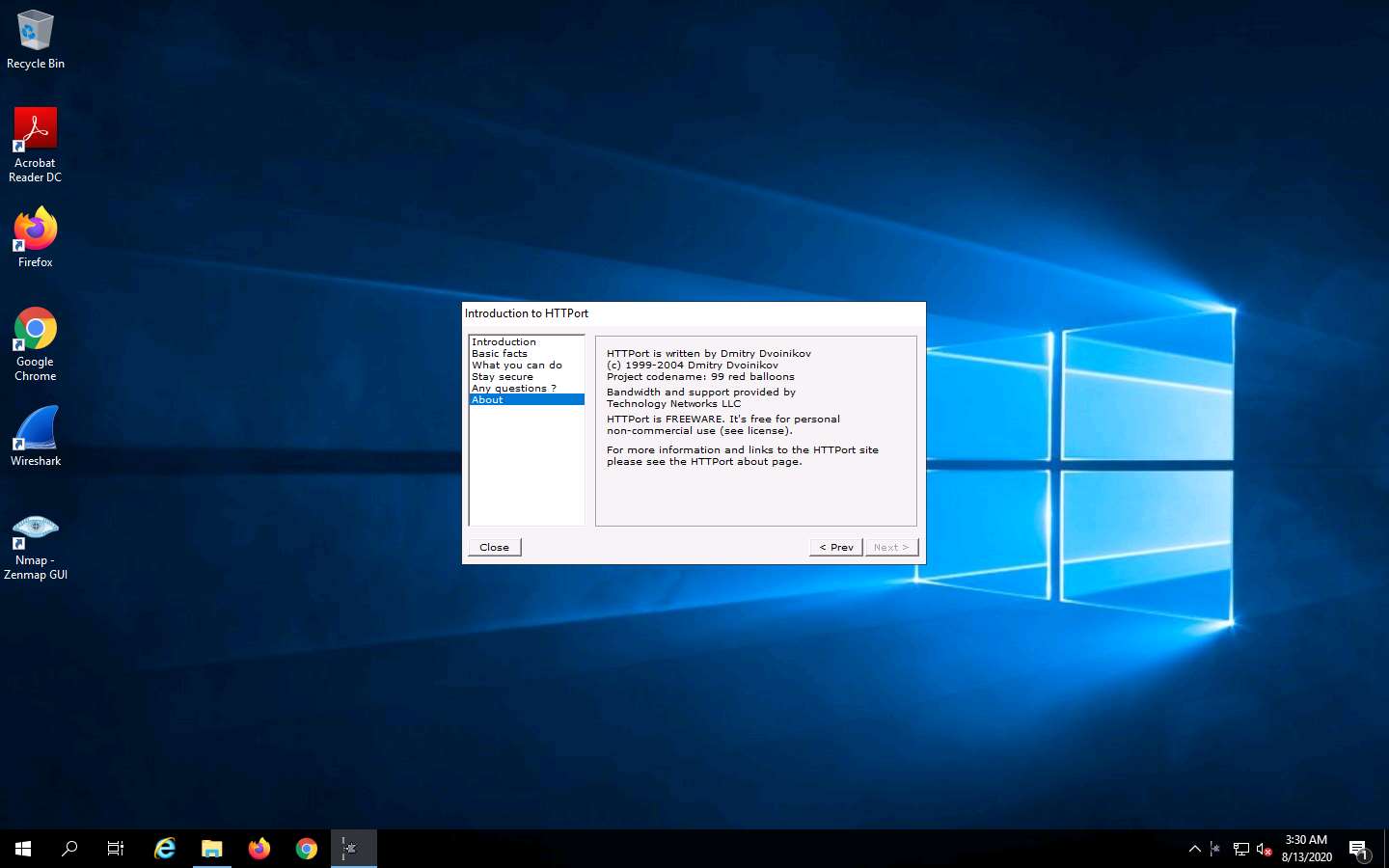


1. Click on Start and navigate to HTTPort 3.SNFM folder and **HTTPort 3.SNFM**.

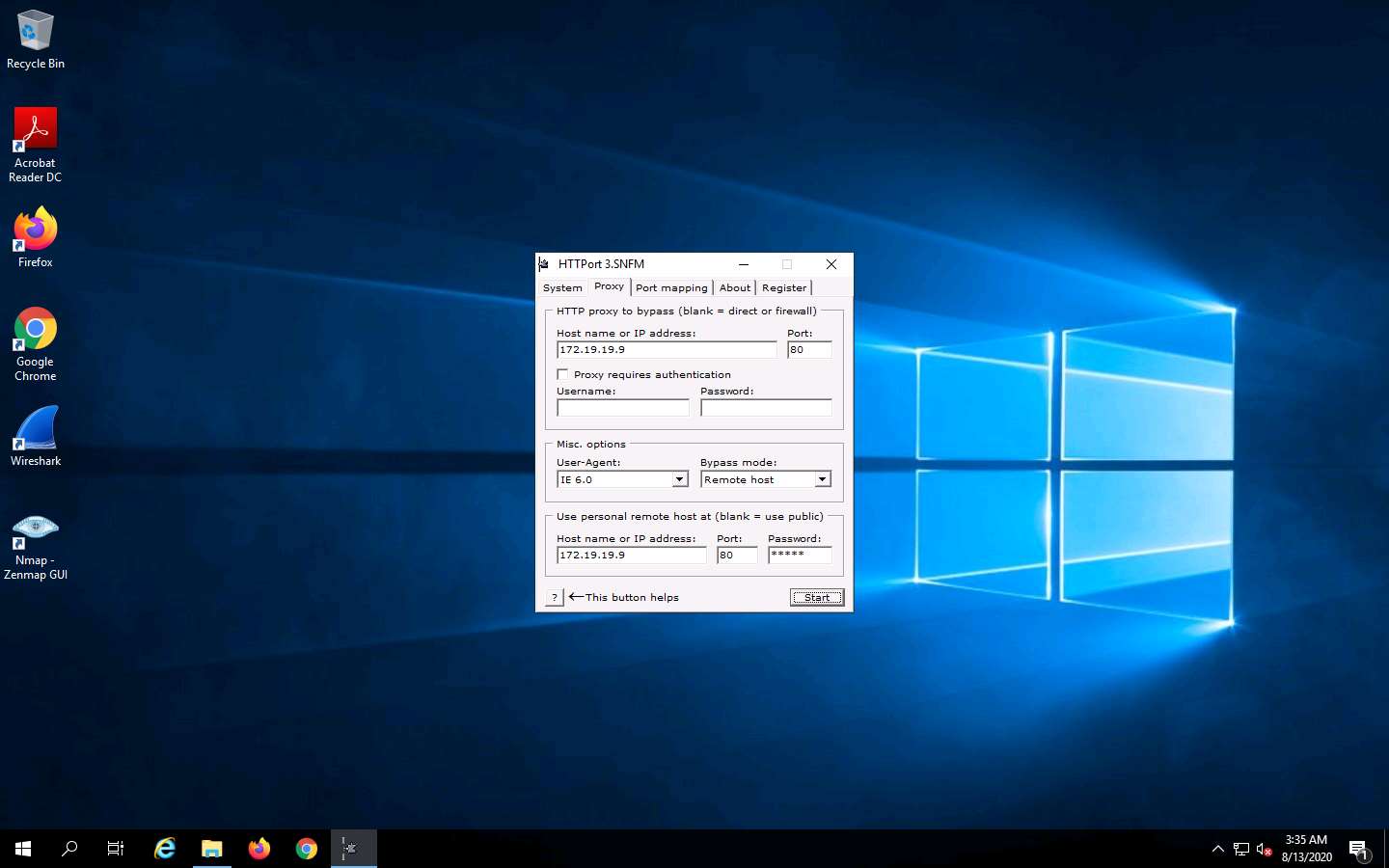


1. An Introduction wizard appears, click **Next** (5 times) till the end of the wizard and then click **Close**.

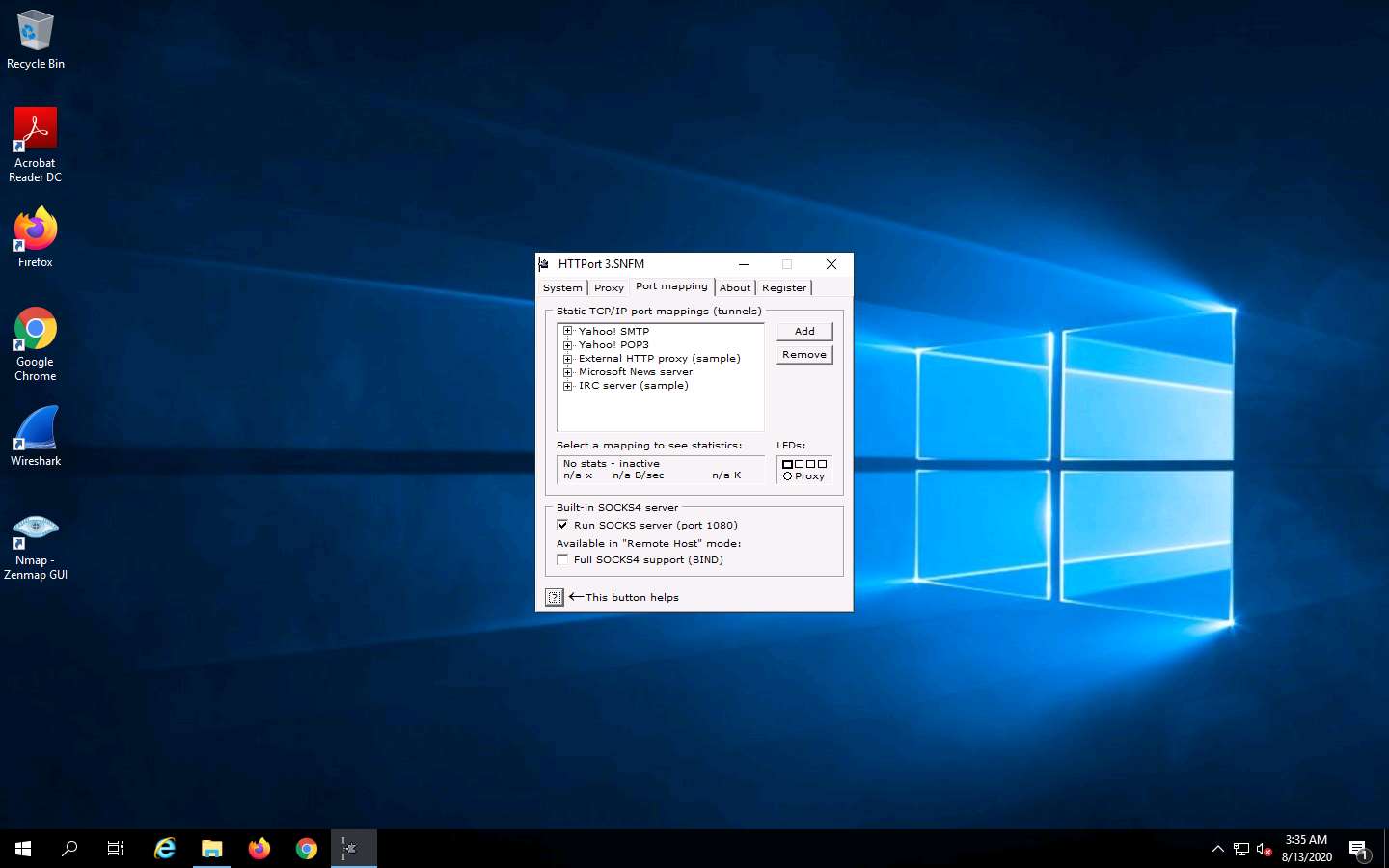




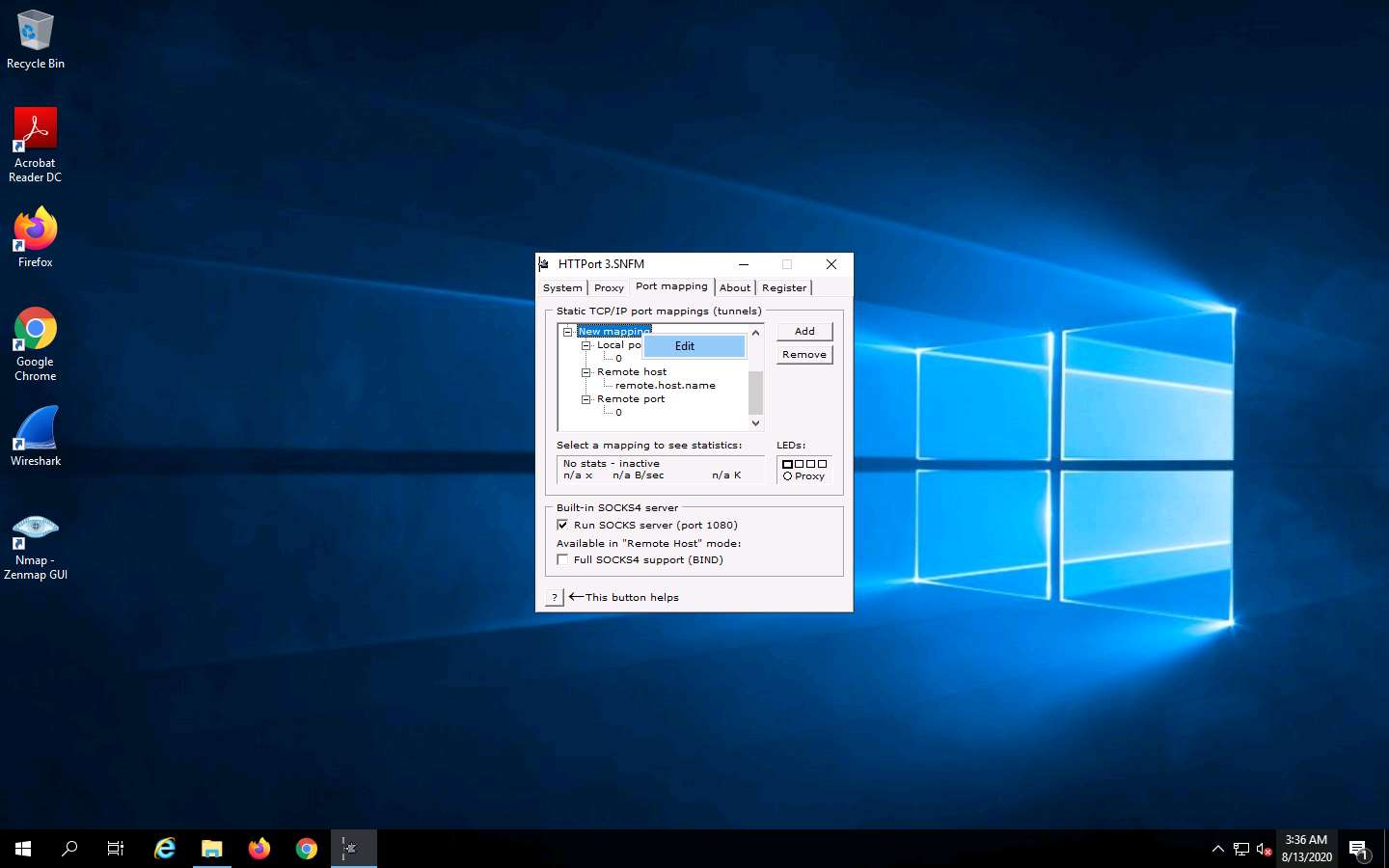
1. The HTTPort main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.
2. Select the **Proxy** tab and enter the IP address of **FTP Server** machine i.e., **172.19.19.9** (since **HTTHost** is running in that machine), and enter **80** as Port number. In the **Misc. options** section, under the **Bypass mode:** field, select **Remote host** option from the drop-down list. In the **Use personal remote host at (blank = use public)** section, re-enter the IP address **FTP Server** i.e., **172.19.19.9** and 80 as the port number. Enter **magic** in the **Password:** field.



1. Select the **Port mapping** tab and click **Add** to create New Mapping.

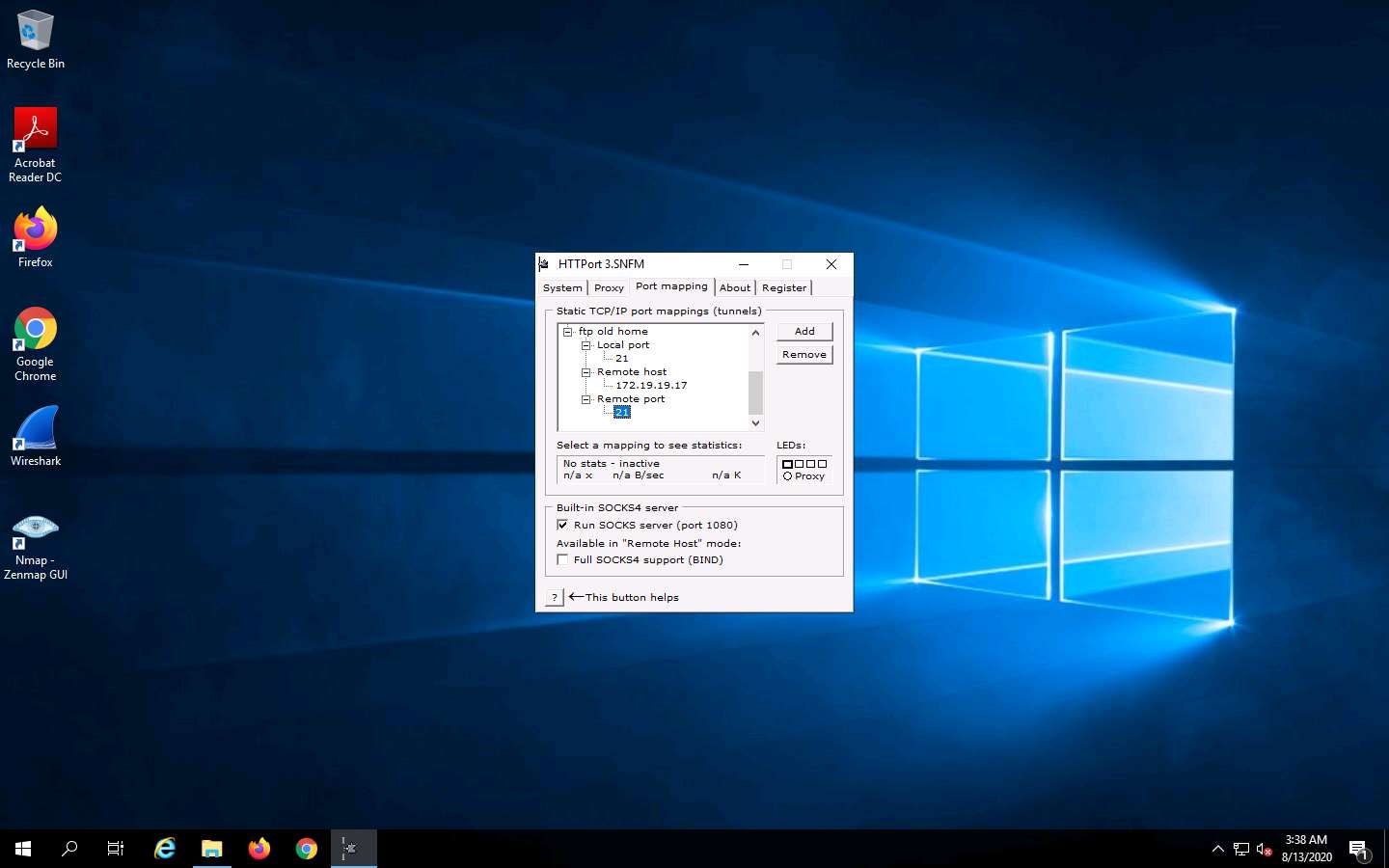


1. Right-click **New Mapping** node, and click **Edit**.

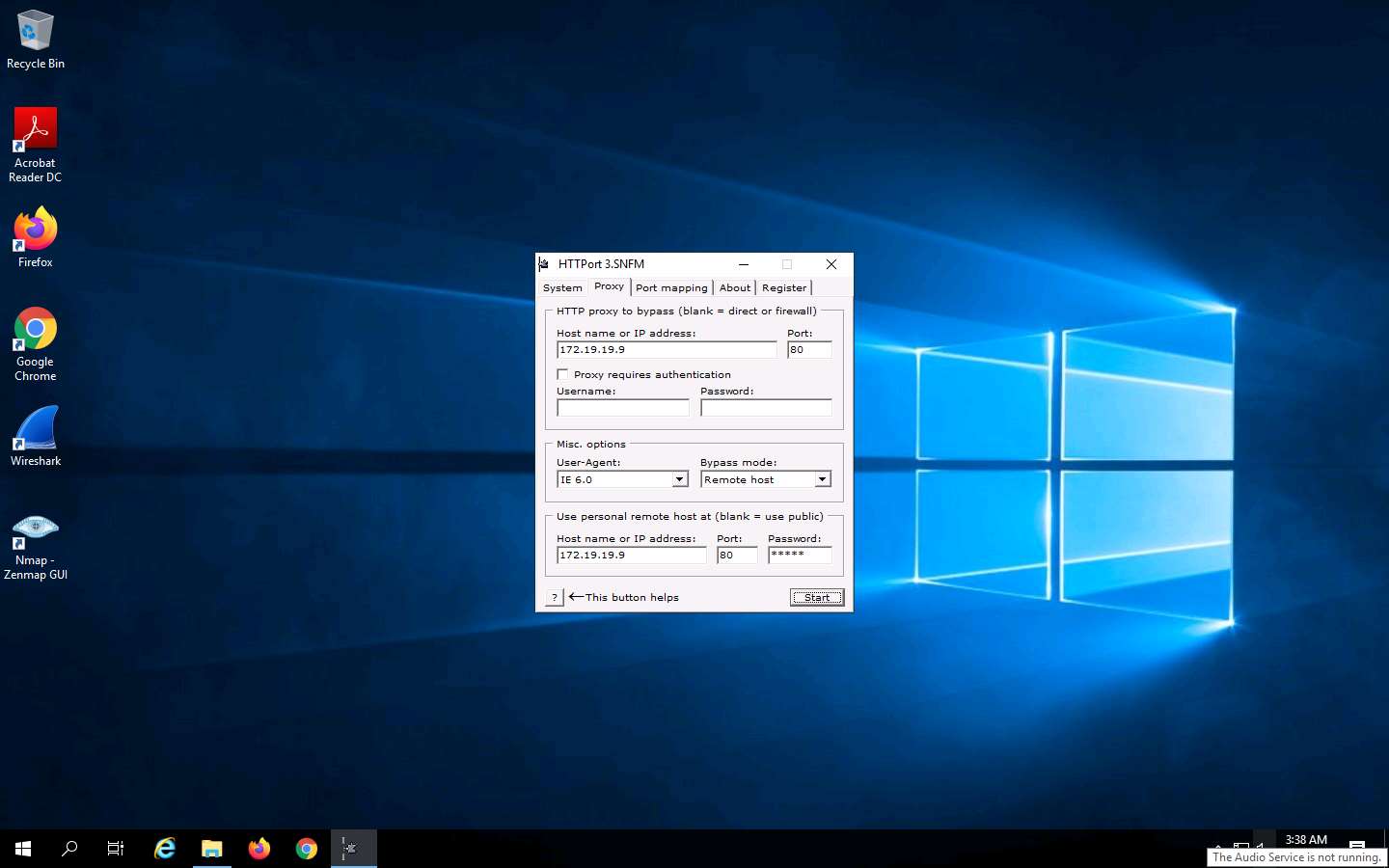


1. Rename this to **ftp old home** (you can enter a name of your choice). Right-click the node below **Local port**, then click **Edit** and enter 21 as the port value. Right-click the node below **Remote host**, click **Edit** and rename it as **172.19.19.17**. Right-click the node below **Remote port**, then click **Edit** and enter 21 as the port value.

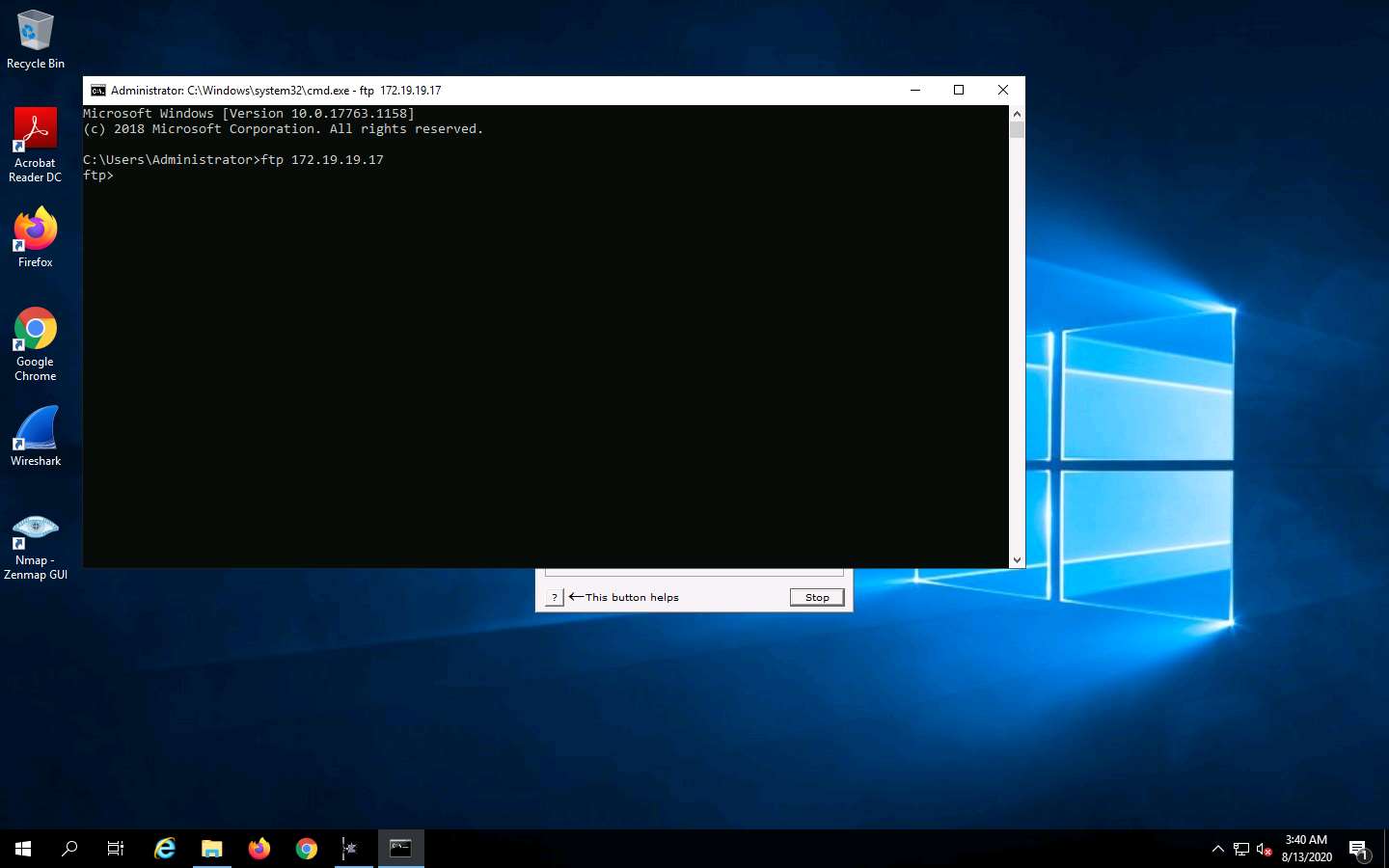
**172.19.19.17** specified in **Remote host** node is the IP address of the FTP site hosted on **Sales Department**.



1. Switch back to **Proxy** tab and click **Start** to begin the **HTTP tunneling**.

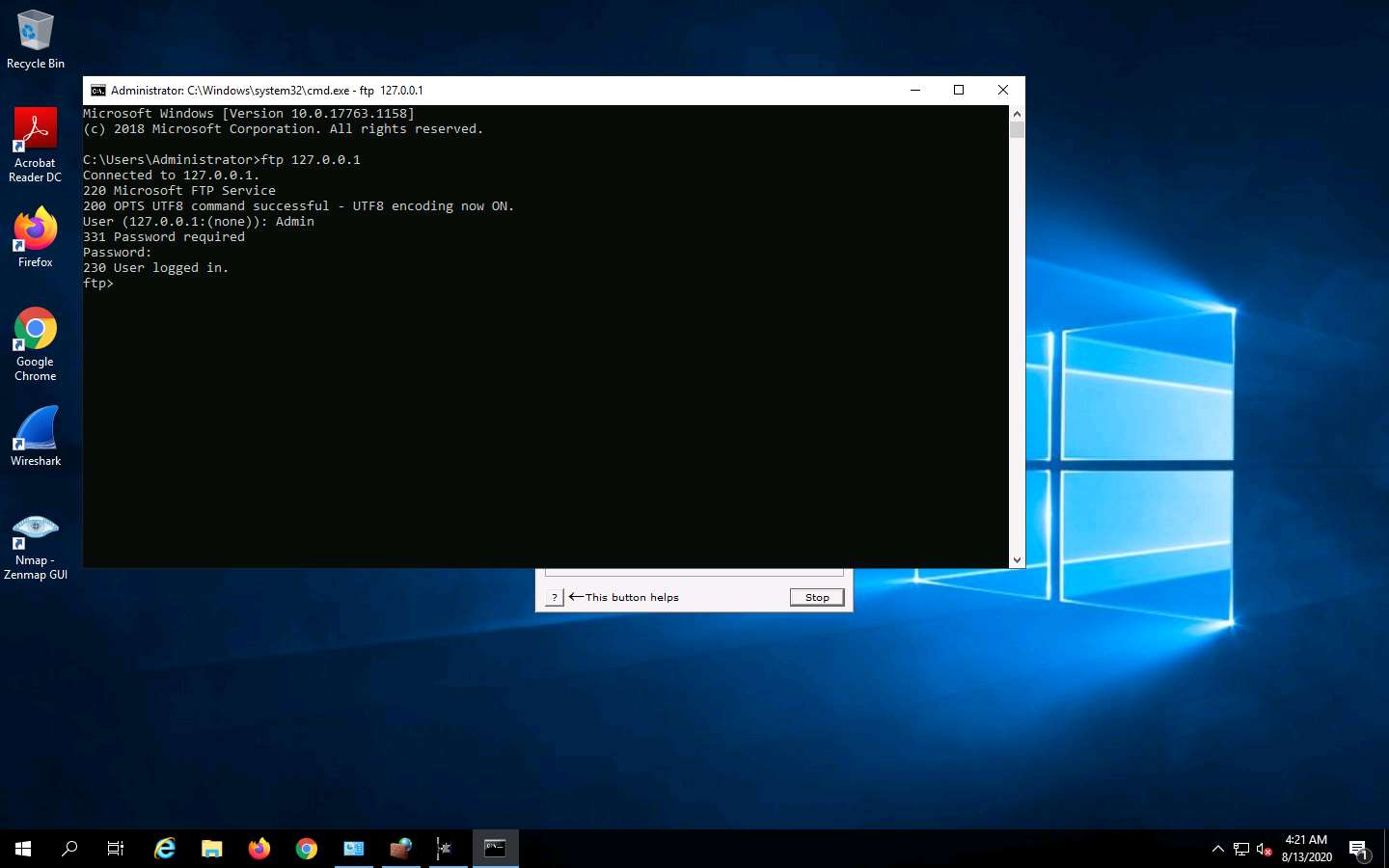


1. **HTTPort** intercepts the FTP request to localhost and tunnels through it. HTTHost installed on the remote machine connects you to **172.19.19.9**. This means you may not access FTP site directly by issuing ftp **172.19.19.9** in the command prompt, but you will be able to access it through the local host by issuing the command **ftp 127.0.0.1**.
2. Launch **Command Prompt** and type **ftp 172.19.19.17**, and press **Enter**. The ftp connection will be blocked by the outbound firewall rule.

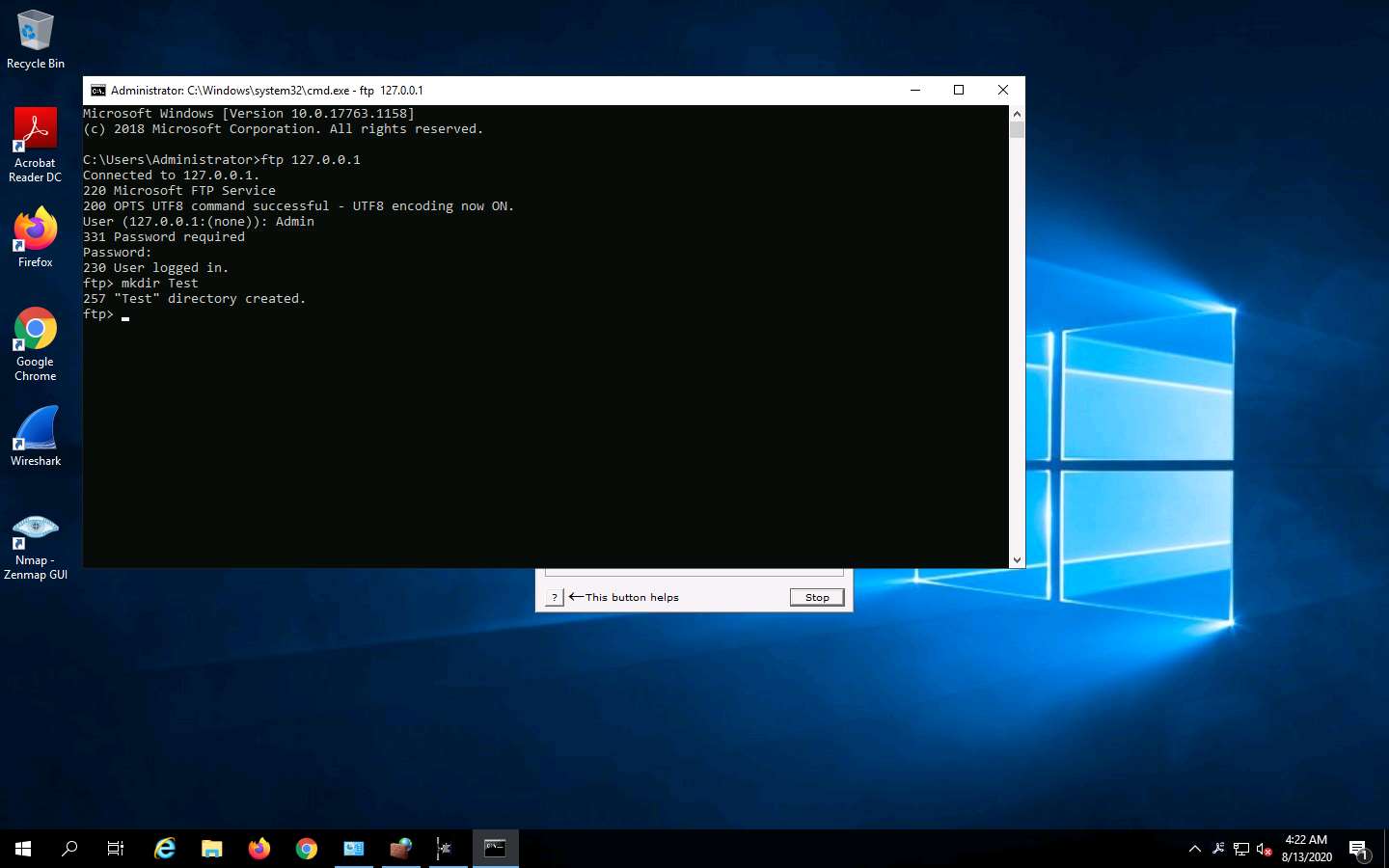


1. Now launch a new **Command Prompt**, type **ftp 127.0.0.1** and Press **Enter**. You should be able to connect to the site.
2. Enter the credentials of any user account of **Sales Department**. In this lab, we are using the credentials of the **Admin** account. Type the username (**Admin**) and password (**test@123**), and press **Enter**.

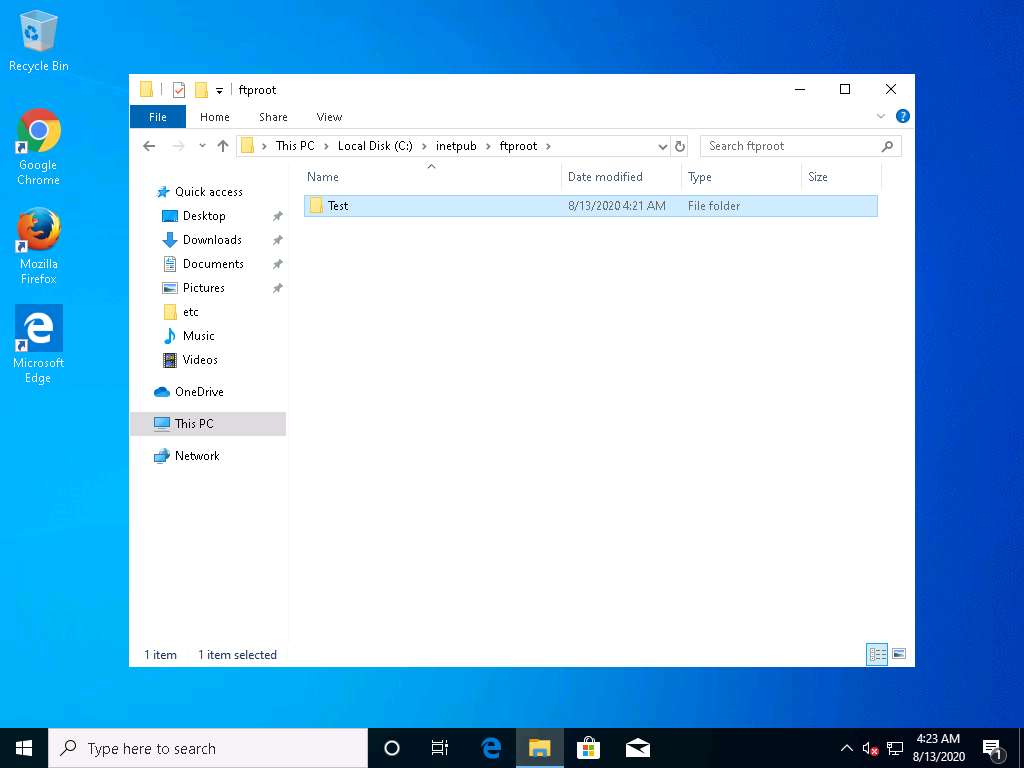
The password you enter won't be visible.



1. You have successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by **HTTPort** and **HTTHost**, bypassing the firewall. Now you have access to add files in the ftp directory located in **Sales Department** machine. Type **mkdir Test** and press **Enter**.



1. Click @lab.VirtualMachine(SalesDepartmentSubnetD).SelectLink. Login to the machine with Username **Admin** and password as **test@123**.
2. Navigate to **C:\inetpub\ftproot**. A directory named **Test** will be created in the **ftproot** folder as shown in the screenshot.



1. Thus, you have successfully bypassed windows firewall using HTTP Tunneling. On completion of the exercise, delete the created outbound rule, stop HttHost and HTTPort and disable the firewall (which was enabled in the beginning of the lab) in the host machine i.e., Windows Server 2019. Also, start the World Wide Web Publishing Service in **FTP Server** machine. Close all the applications, files, and folders that were opened while performing this exercise.

In this lab you have learned how to analyze and document the results related to the lab exercise. Give your opinion on your target’s security posture and exposure.