Module 12: Evading IDS, Firewalls, and Honeypots

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.

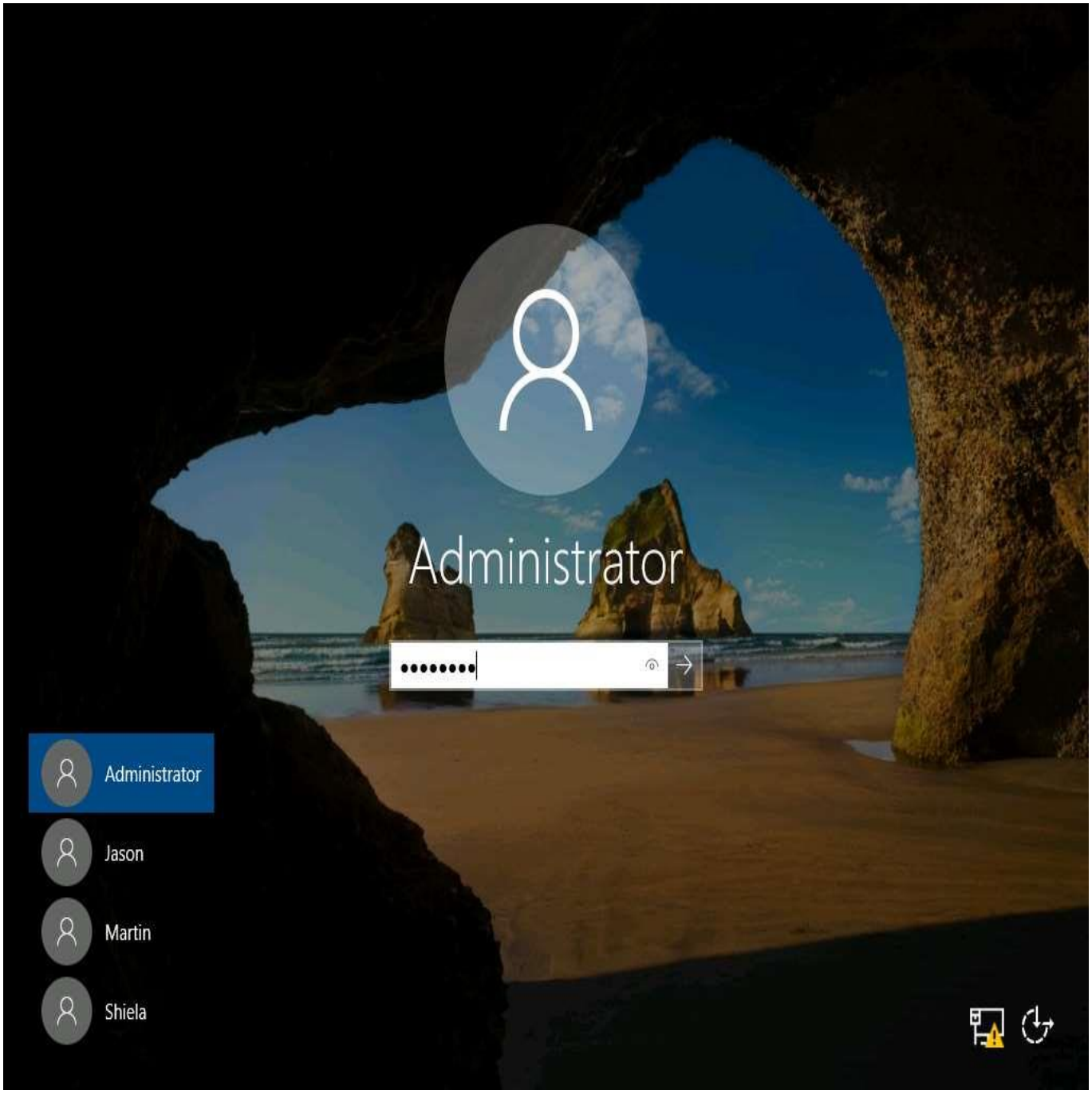
Uses of Snort:

- 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.

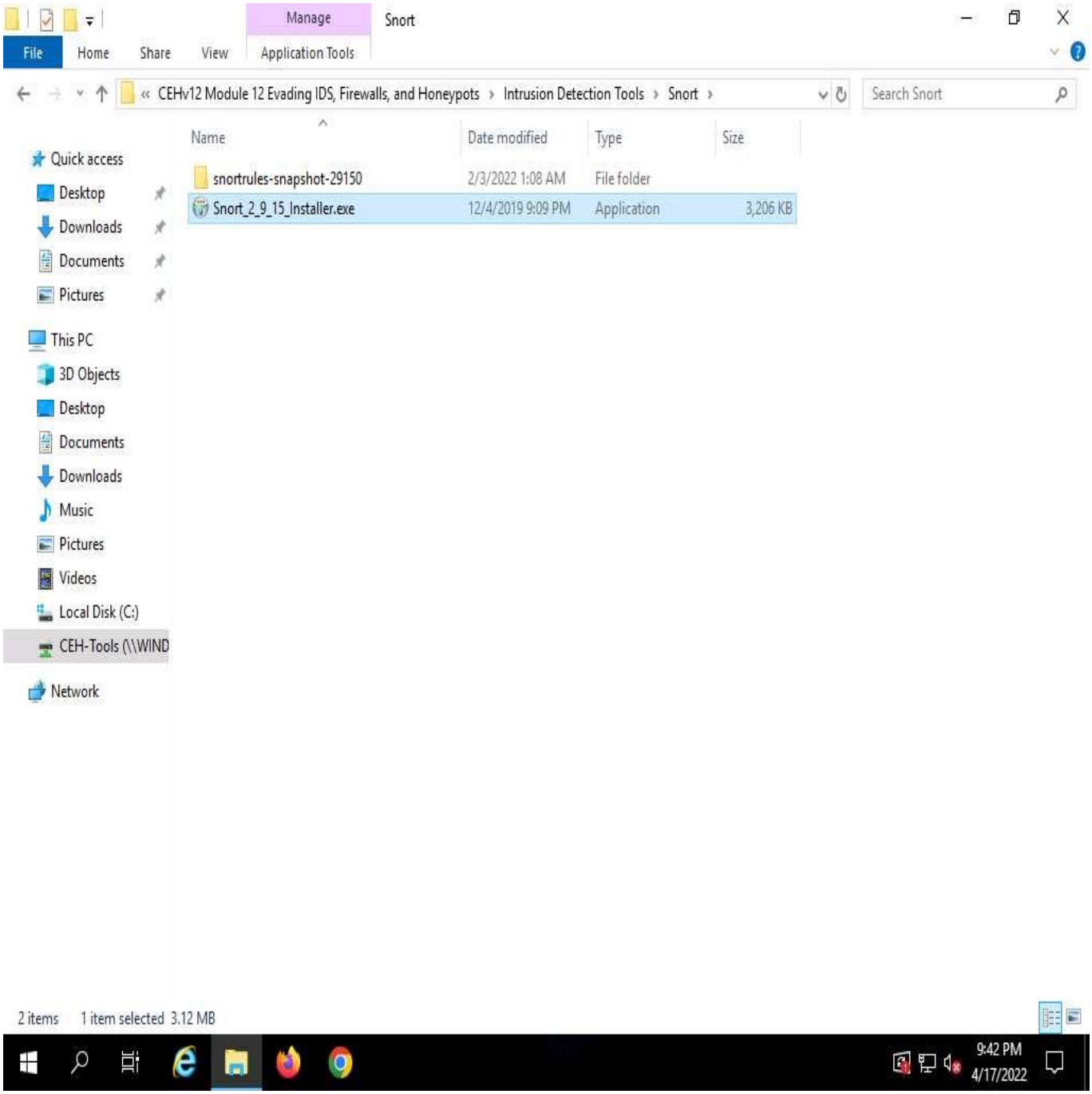
1. Click on Windows Server 2019 to switch to **Windows Server 2019** machine. Click Ctrl+Alt+Delete to activate the machine. By default, **Administrator** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

   Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.
   Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

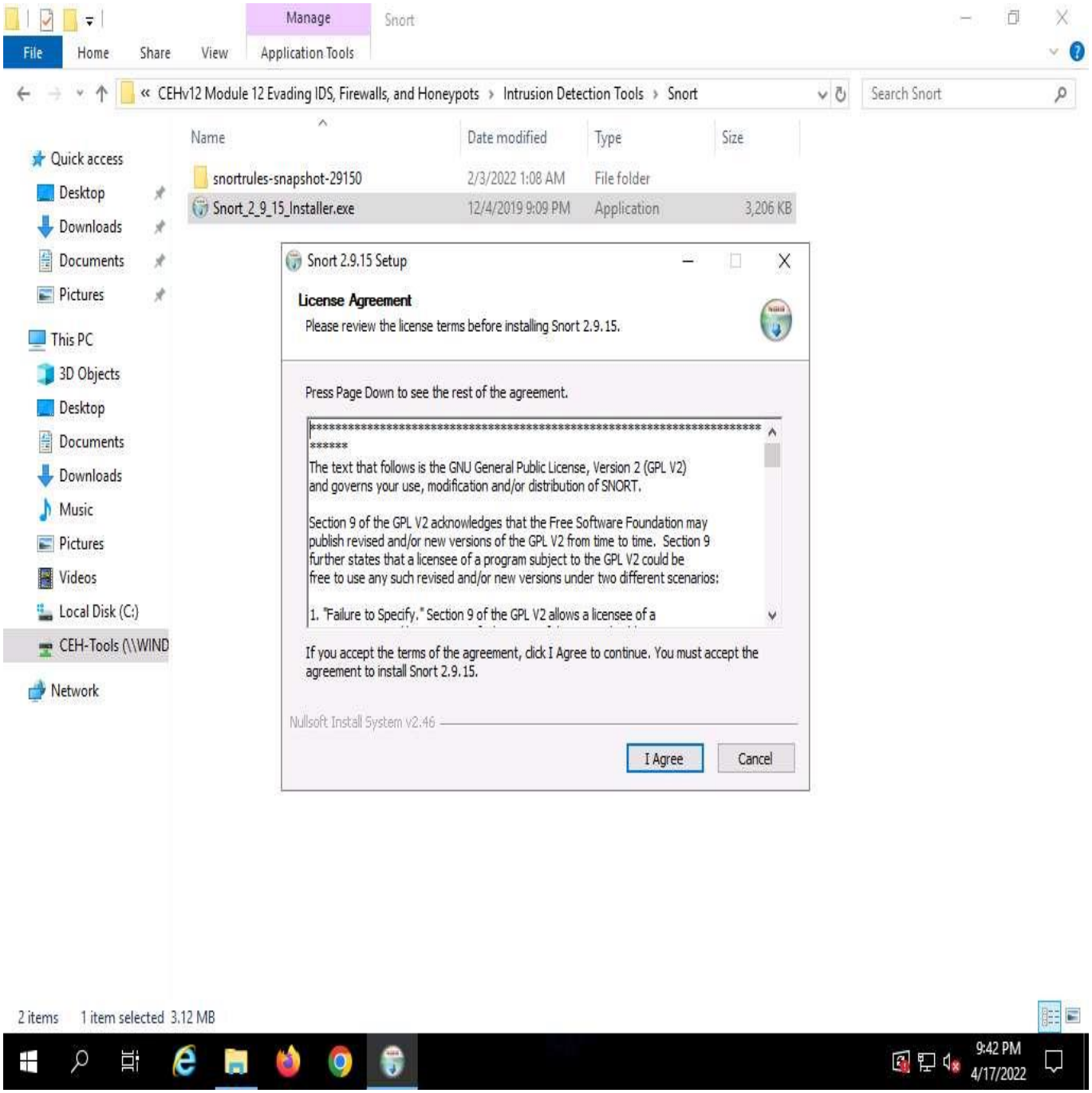


2. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort** and double-click the **Snort_2_9_15_Installer.exe** file to start the Snort installation.

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

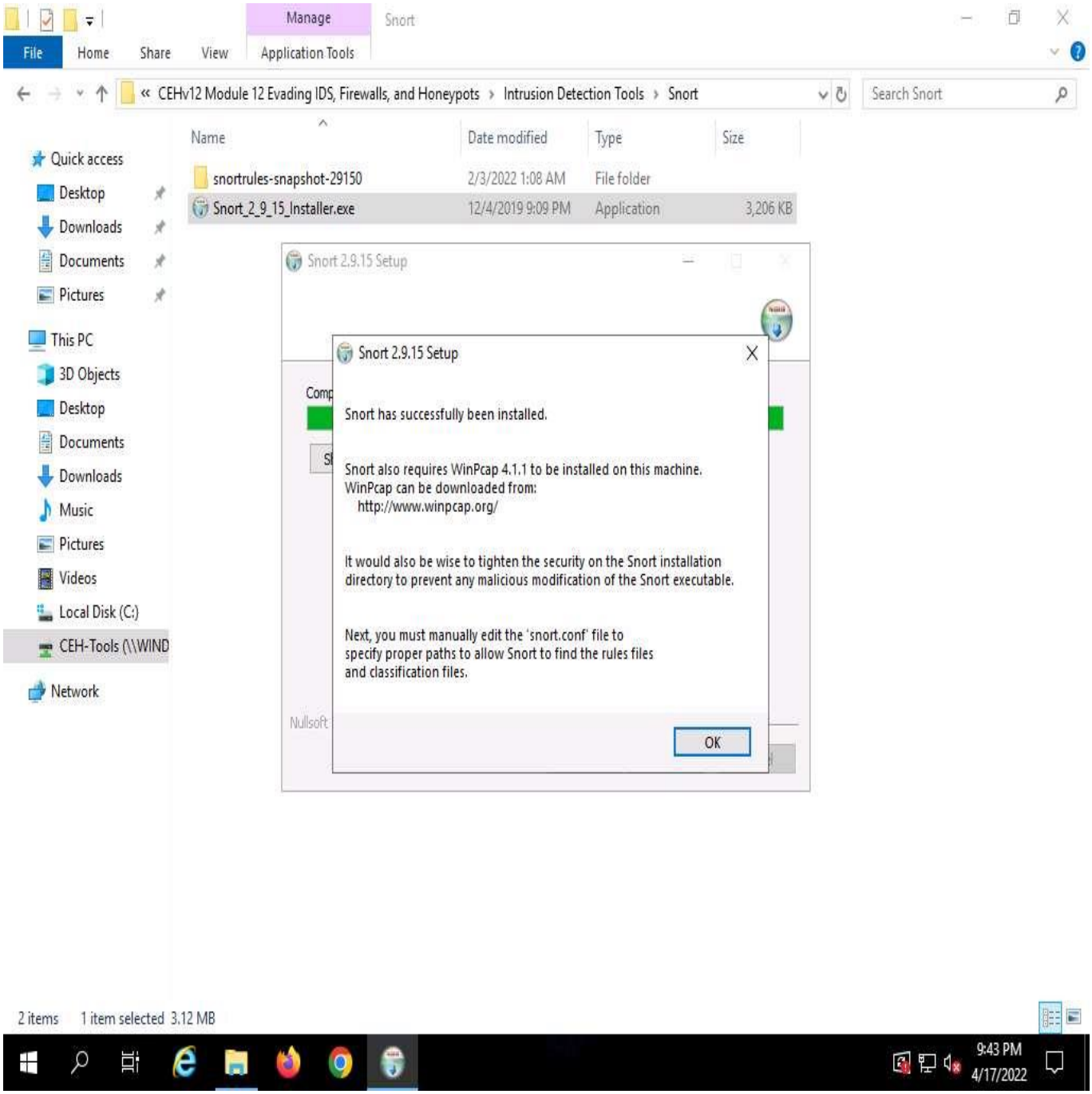


3. Accept the **License Agreement** and install Snort by selecting the default options that appear step by step in the wizard.

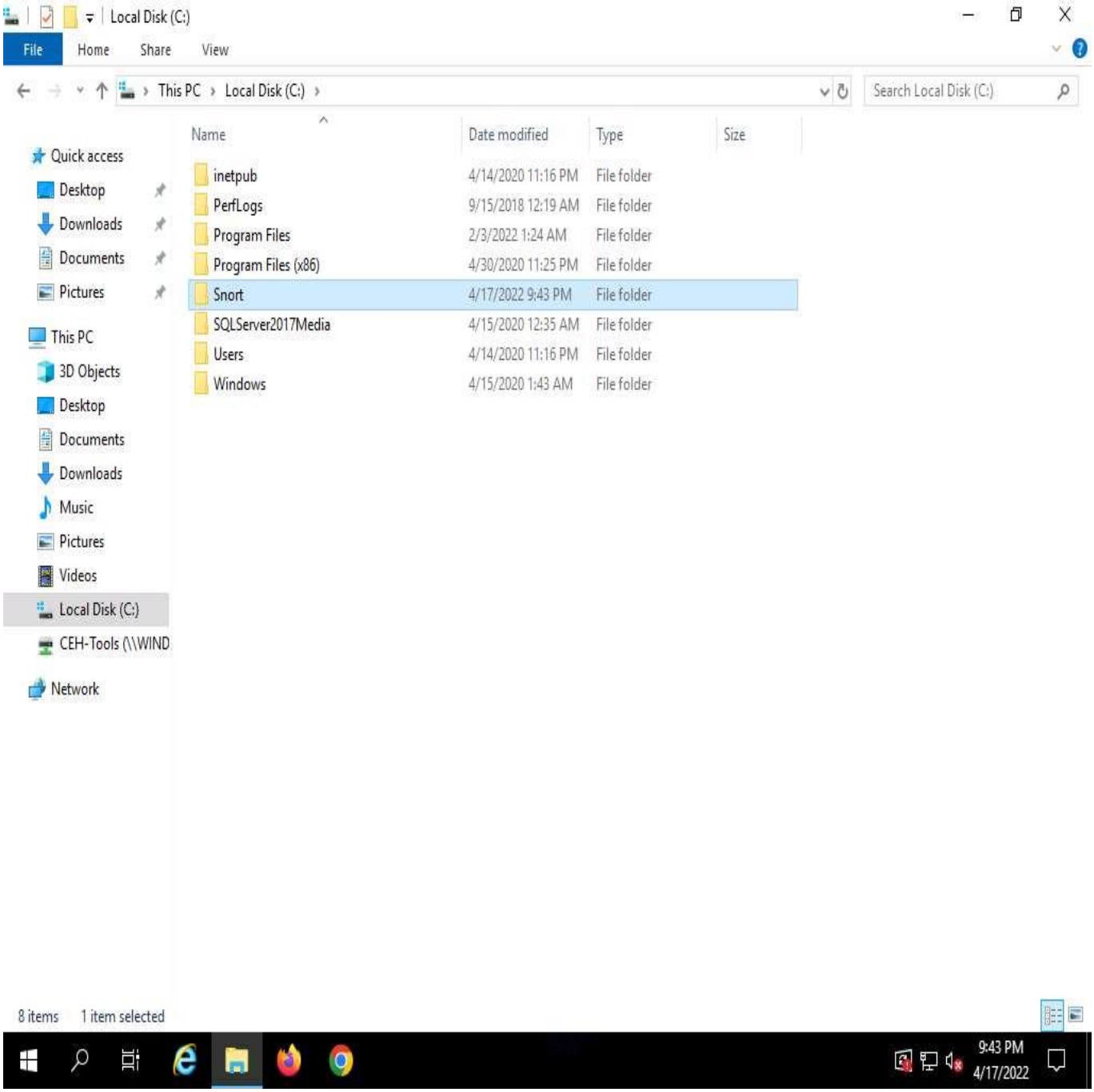


4. A window appears after the successful installation of Snort; click **Close**.
5. Click **OK** to exit the **Snort Installation** window.

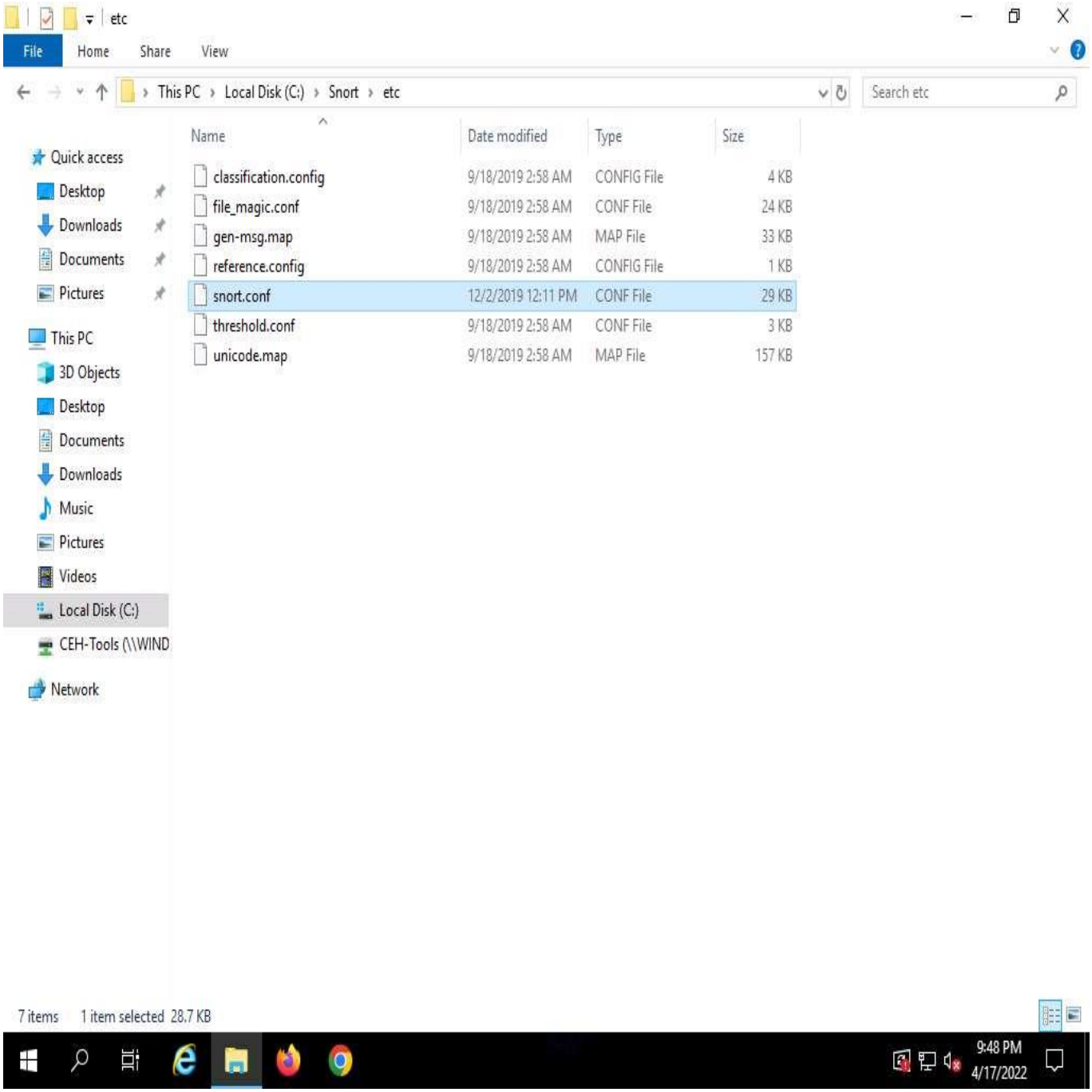
Snort requires **WinPcap** to be installed on your machine. In this task environment, we have already installed WinPcap drivers for packet capturing.



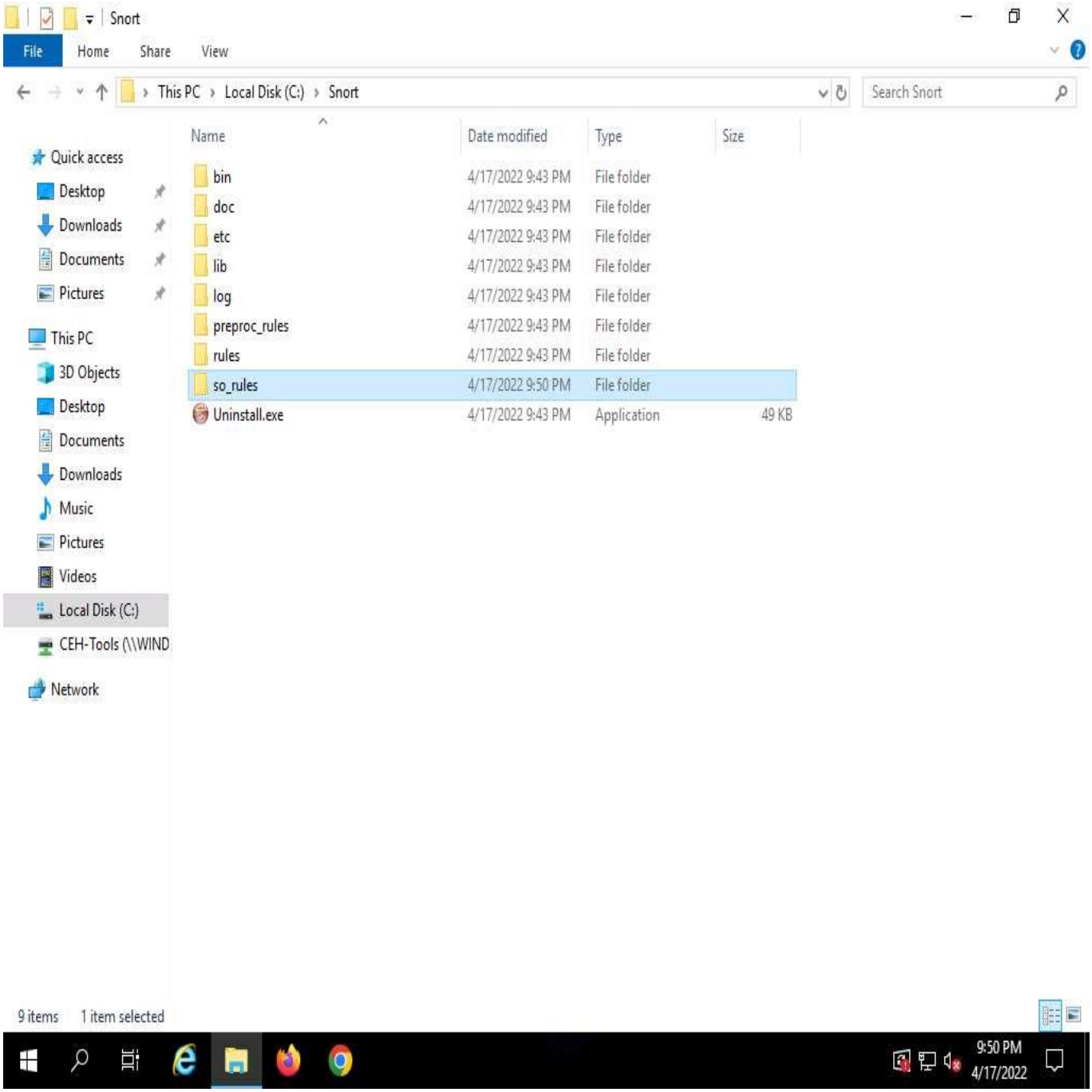
6. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).



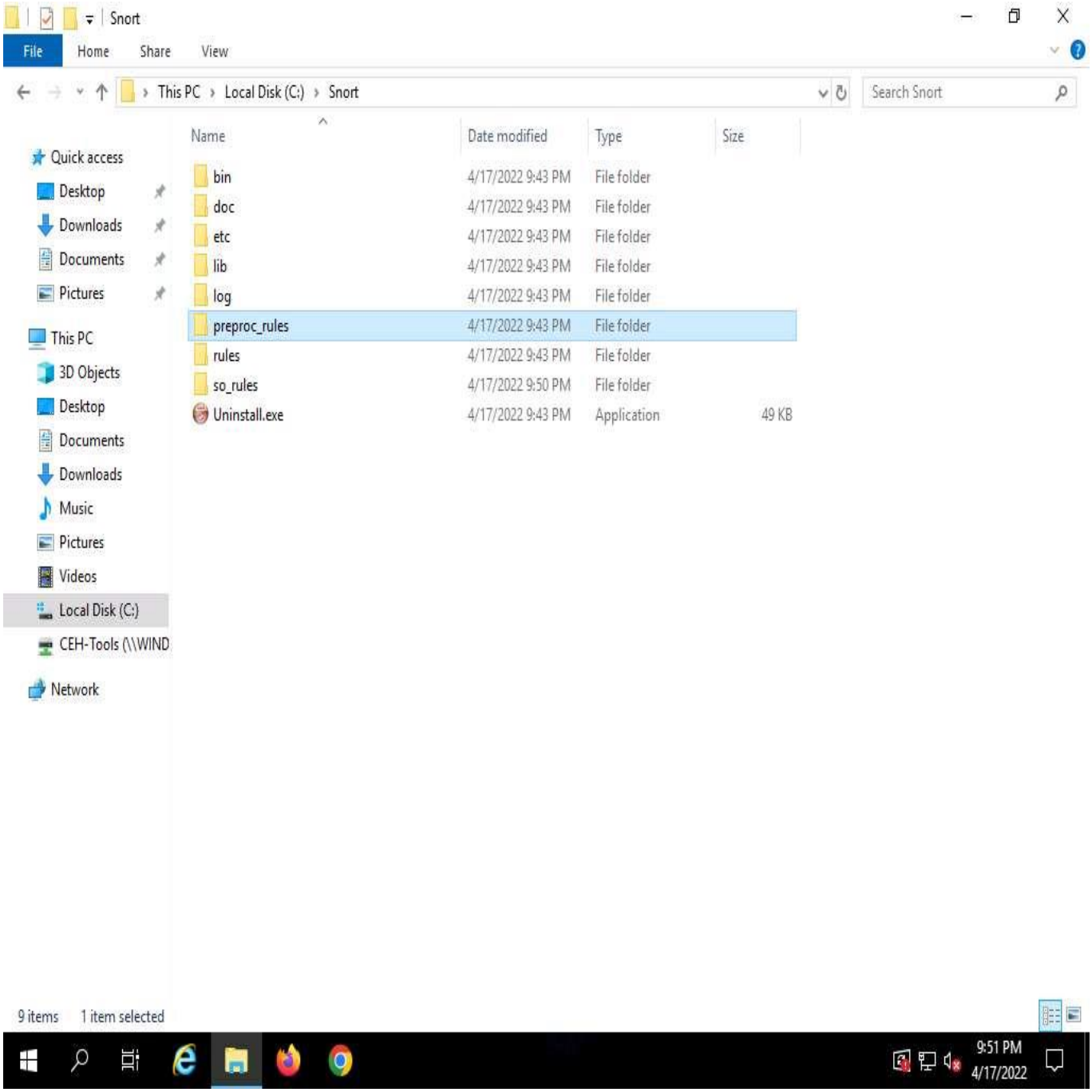
7. ☐ Navigate to the **etc** folder in the specified location, **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.
8. ☐ **snort.conf** is already present in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



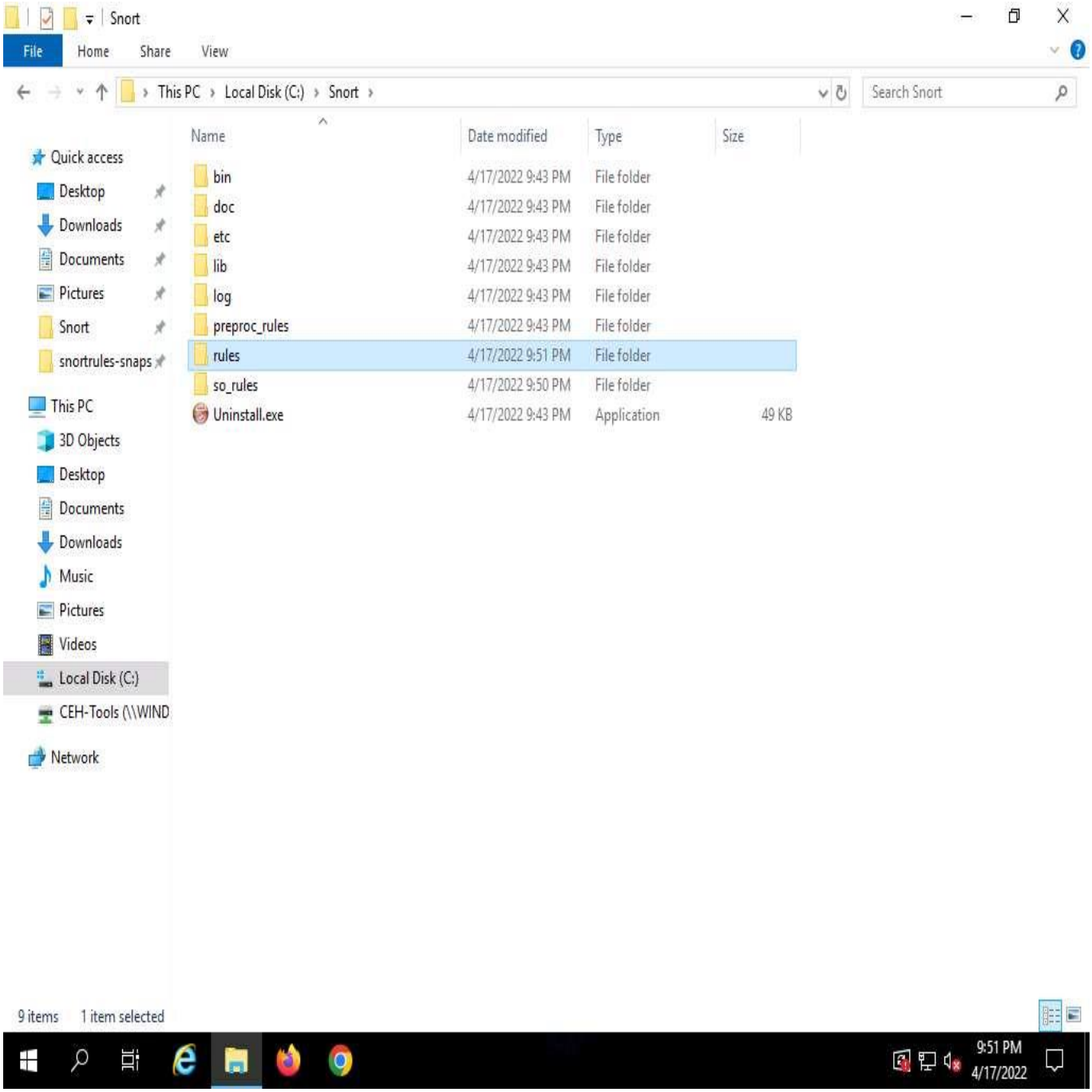
9. ☐ Copy the **so_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



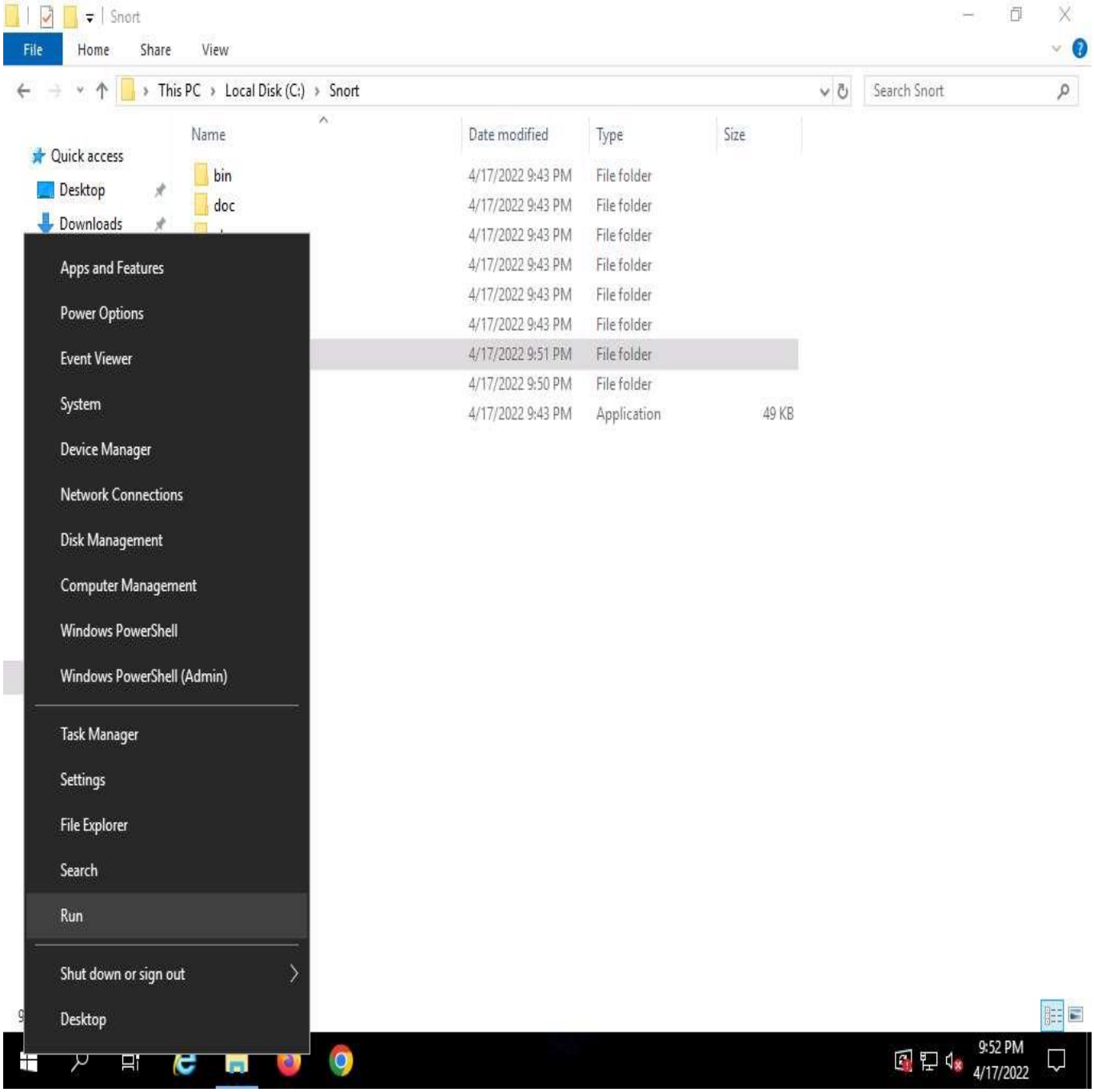
10. ☐ Copy the **preproc_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules**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



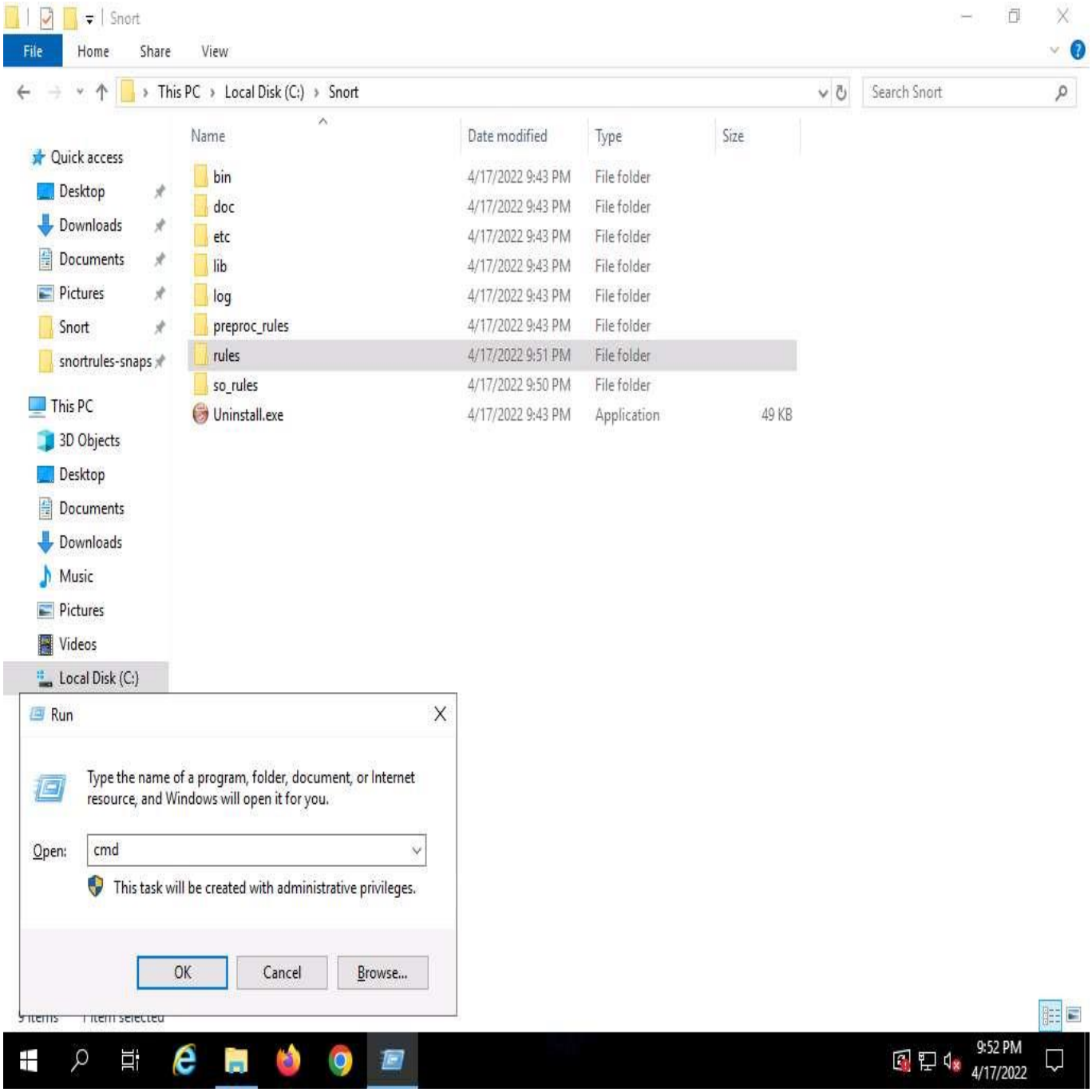
11. ☐ Using the same method, copy the **rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



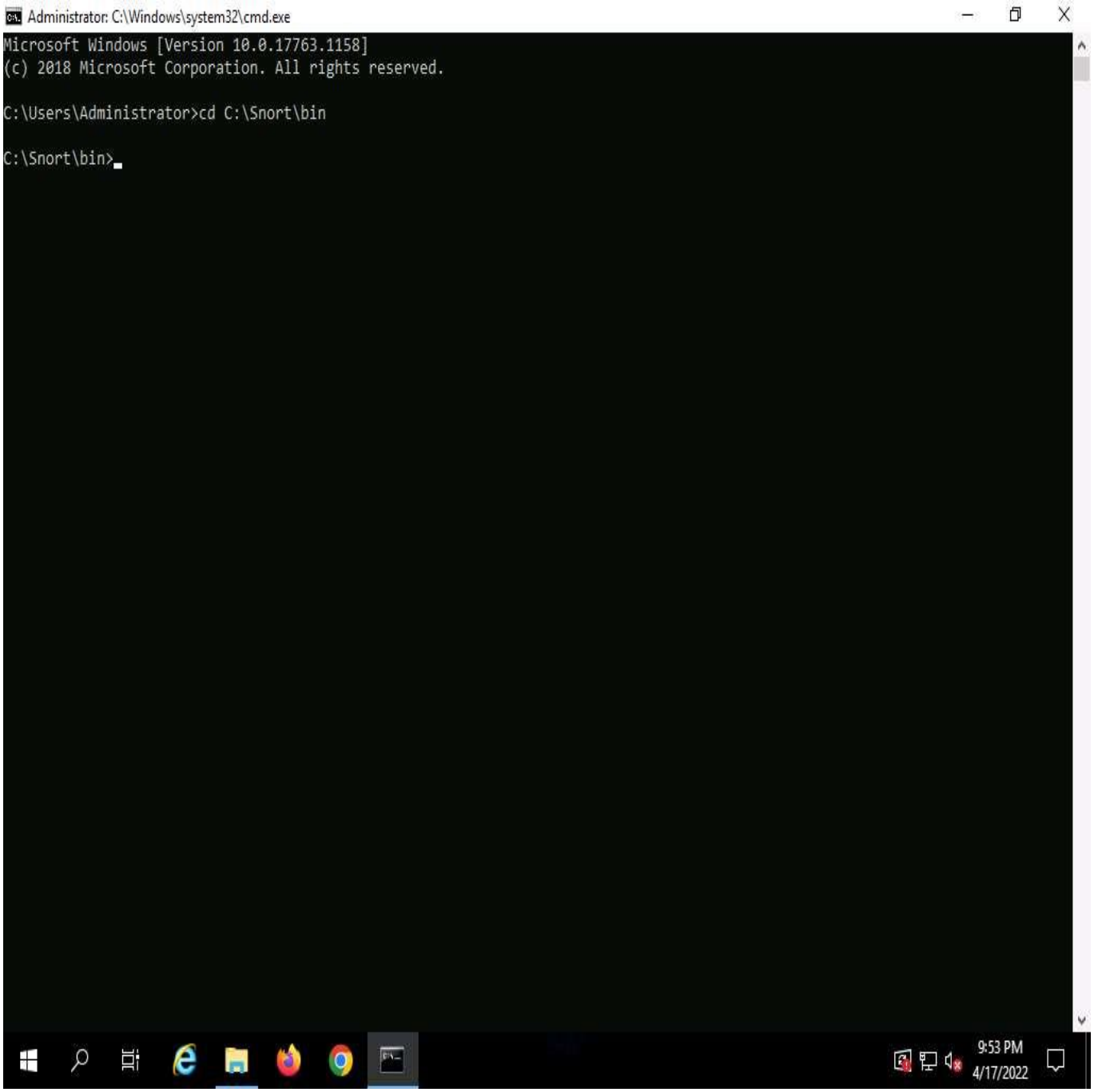
12. ☐ Now right-click on the **Windows Start** icon and click **Run** from the menu.



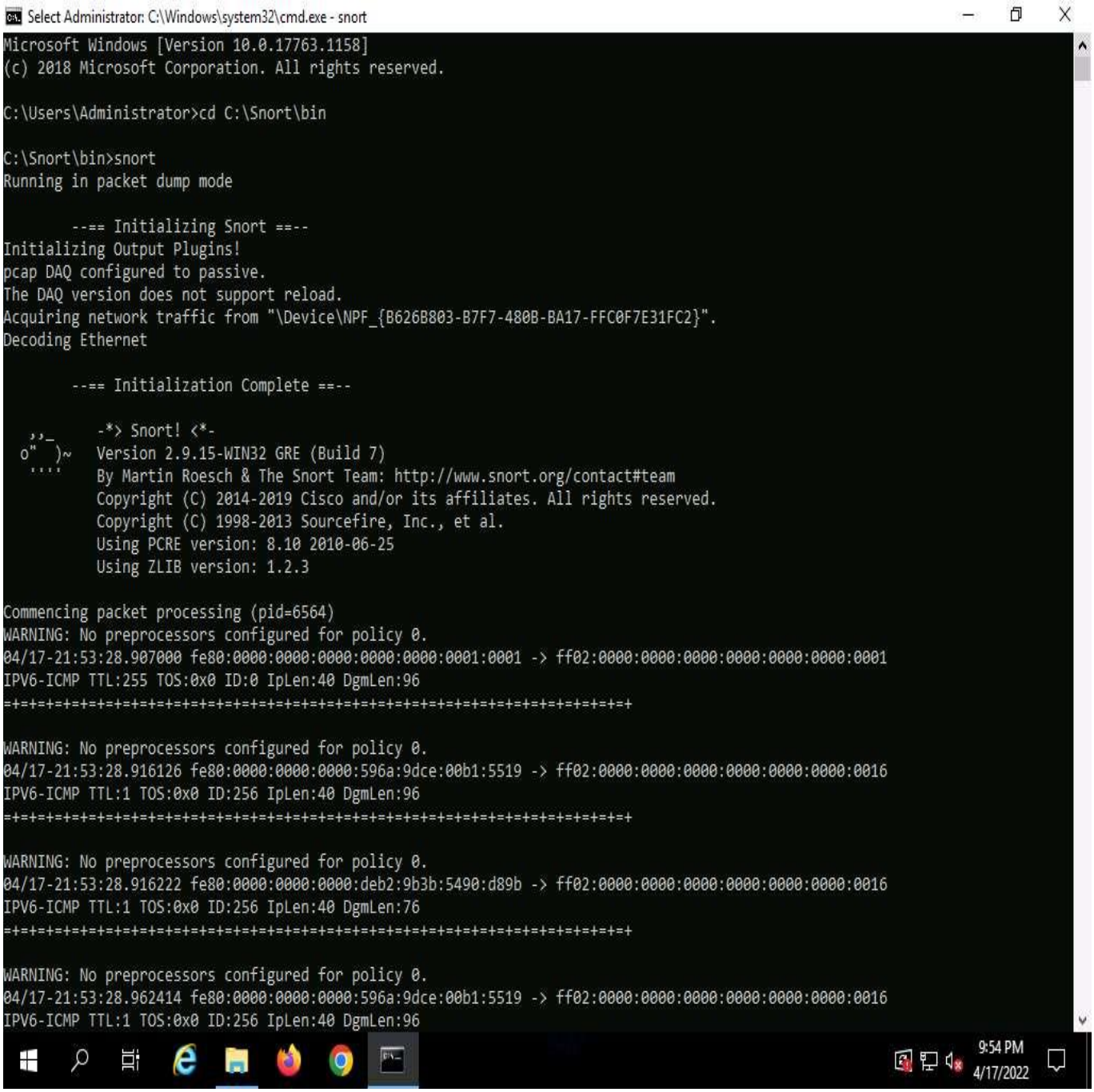
13. ☐ The **Run** window appears; type **cmd** in the **Open** field and click **OK** to launch command prompt window.



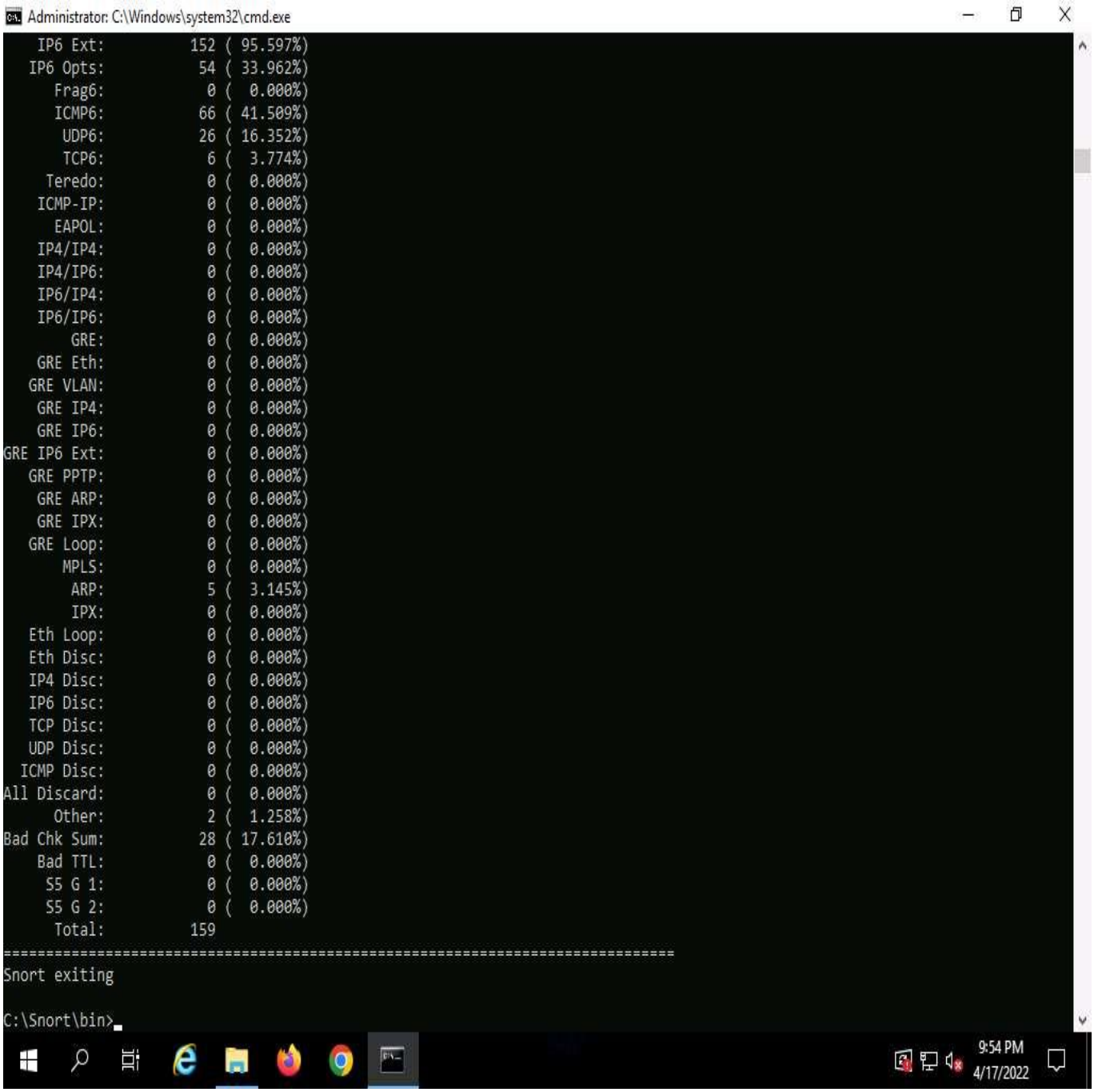
14. ☐ The **Command Prompt** window appears; type **cd C:\Snort\bin** and press **Enter** to access the bin folder in the command prompt.



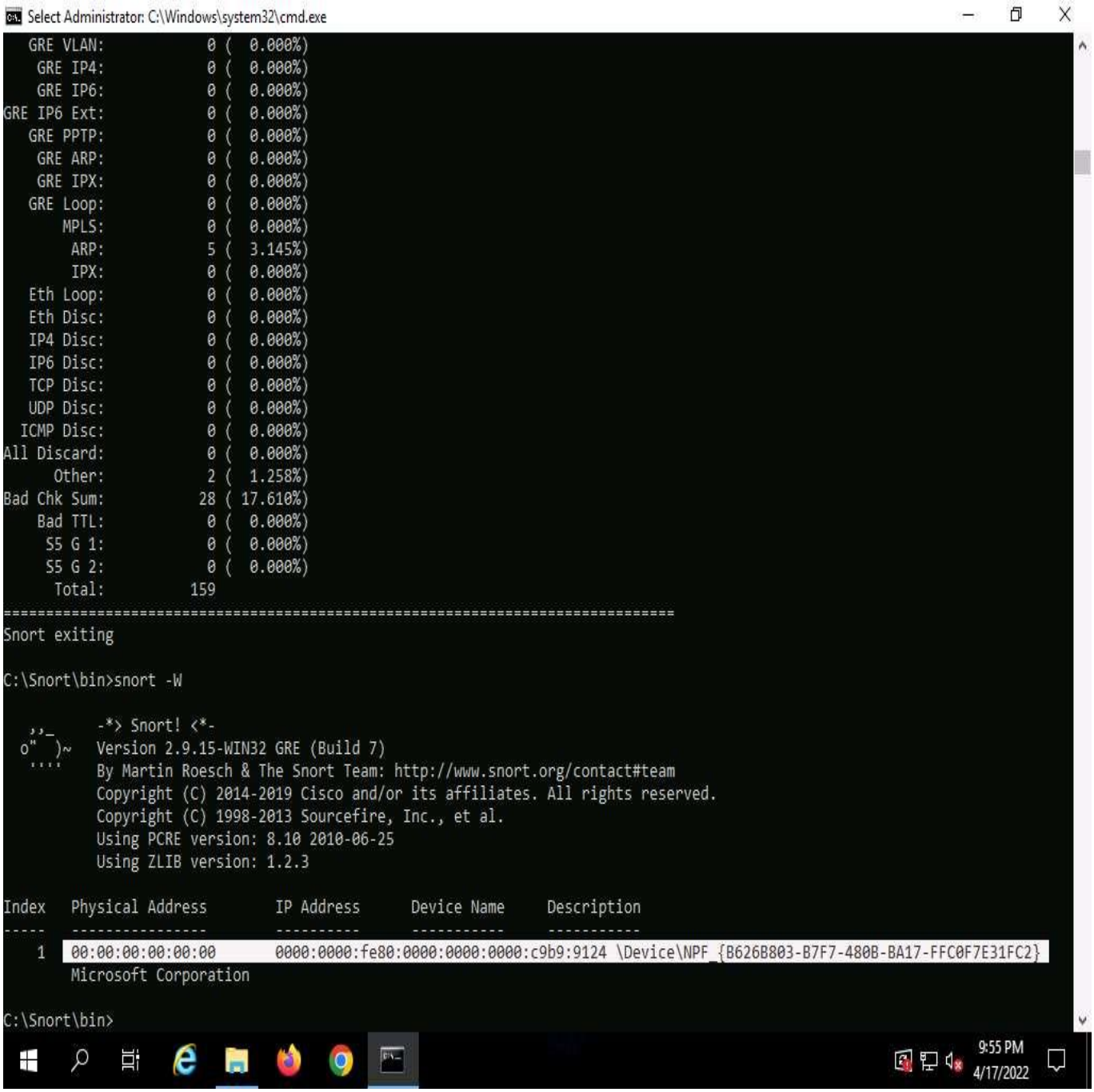
15. ☐ Type **snort** and press **Enter**.



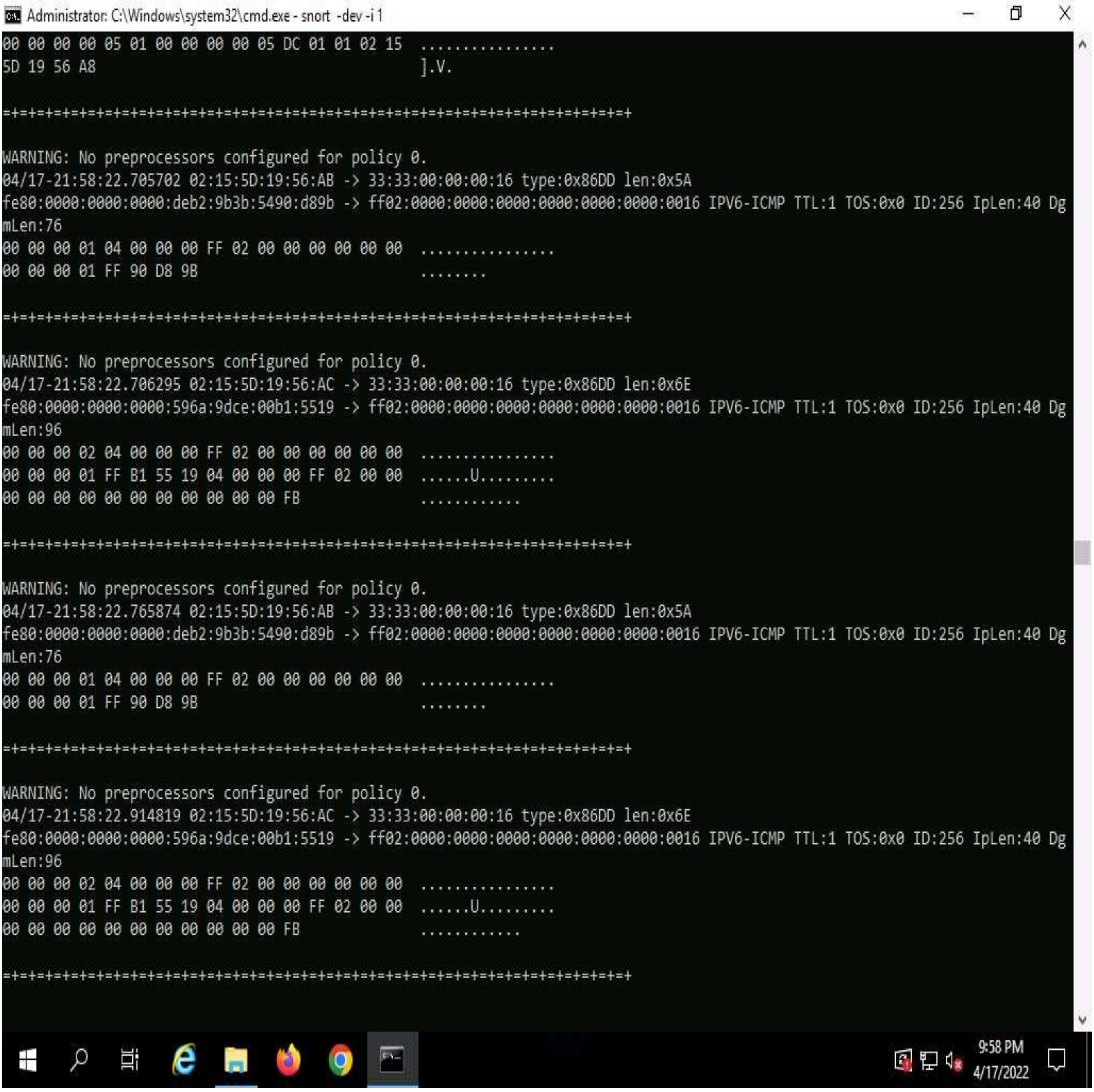
16. ☐ Snort initializes; wait for it to complete. After completion press **Ctrl+C**, Snort exits and comes back to **C:\Snort\bin**.



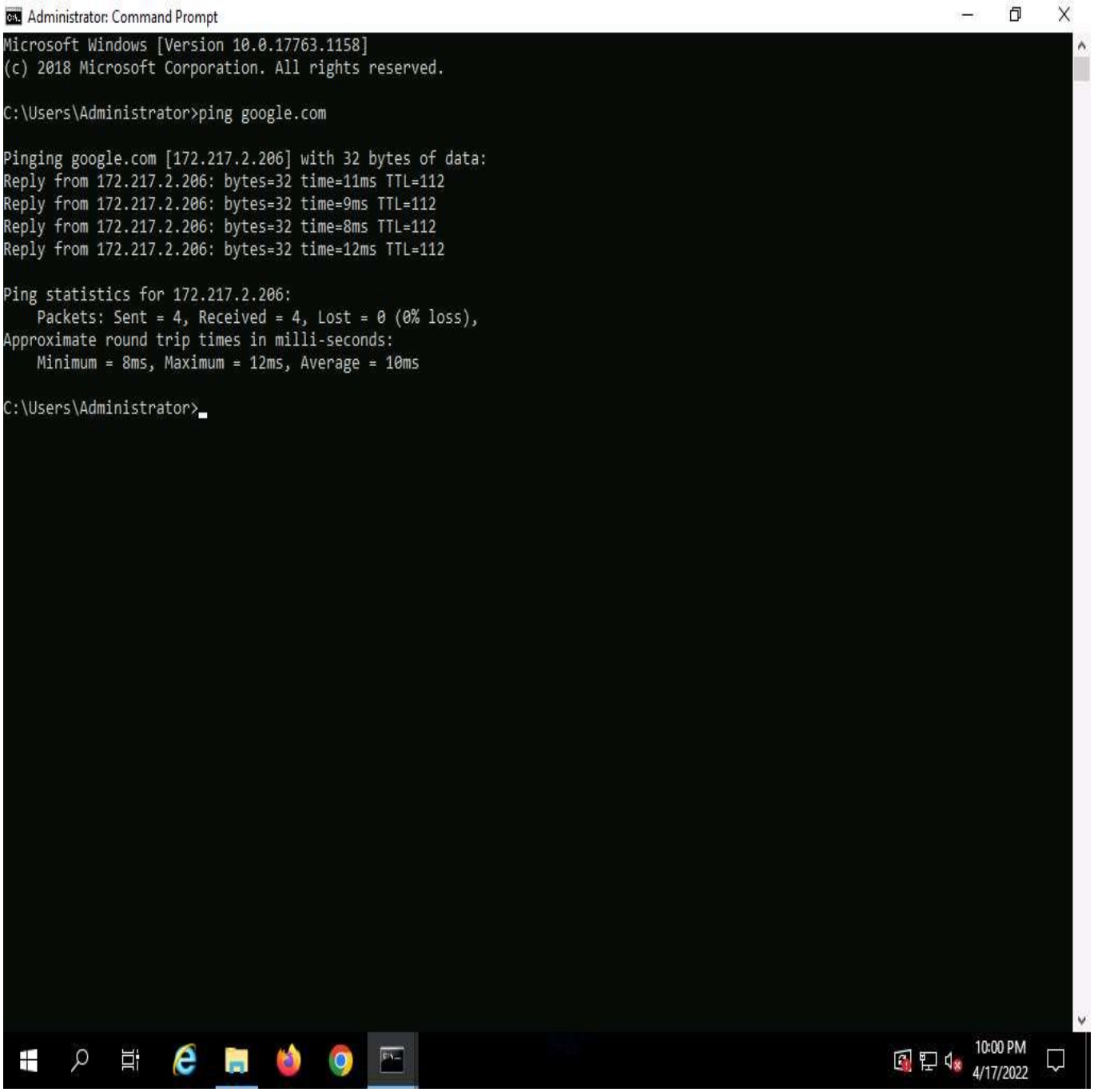
17. ☐ Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.



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.

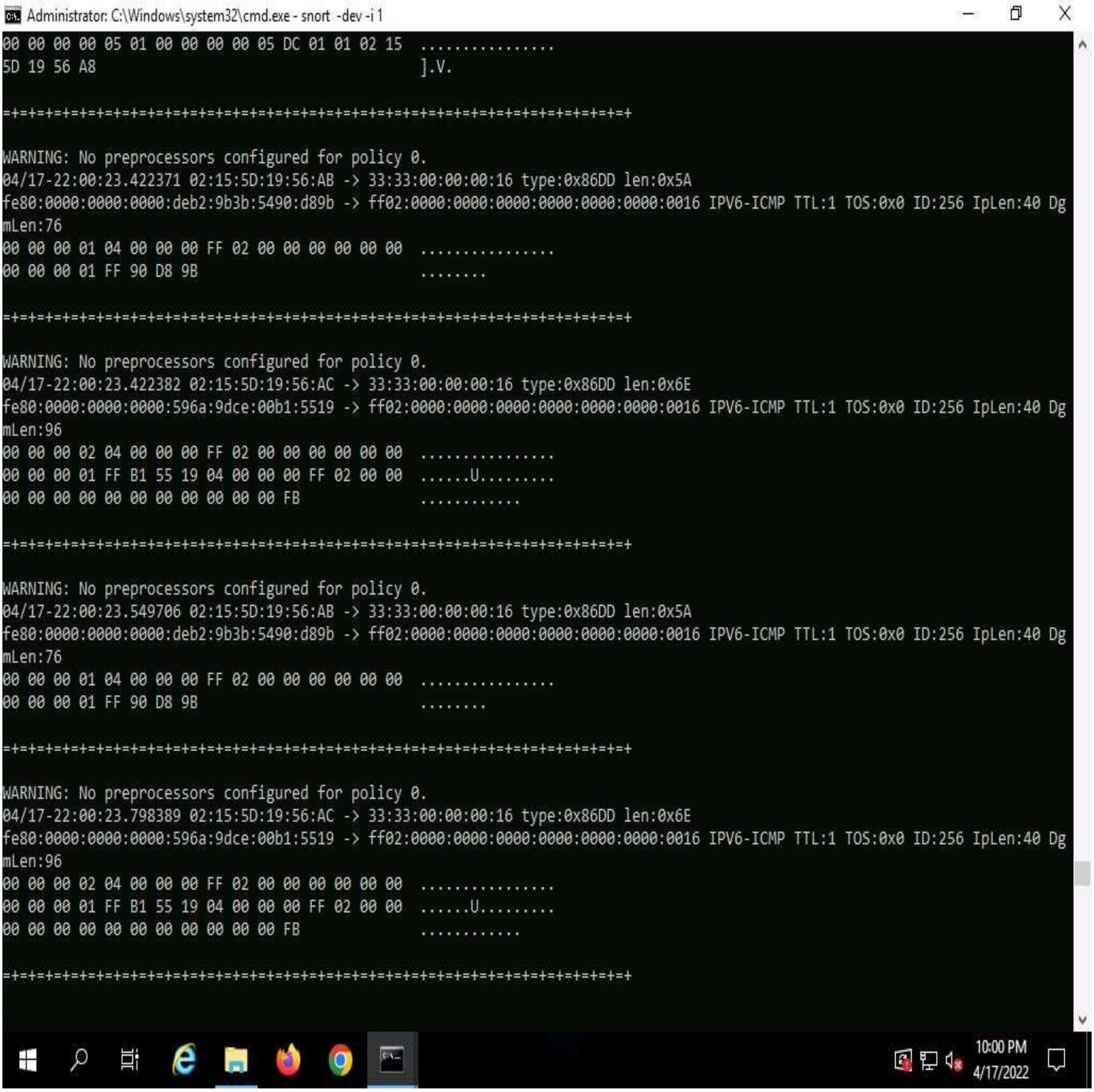


21. ☐ Leave the Snort command prompt window open, and launch another command prompt window.
22. ☐ In a new command prompt, type **ping google.com** and press **Enter**.

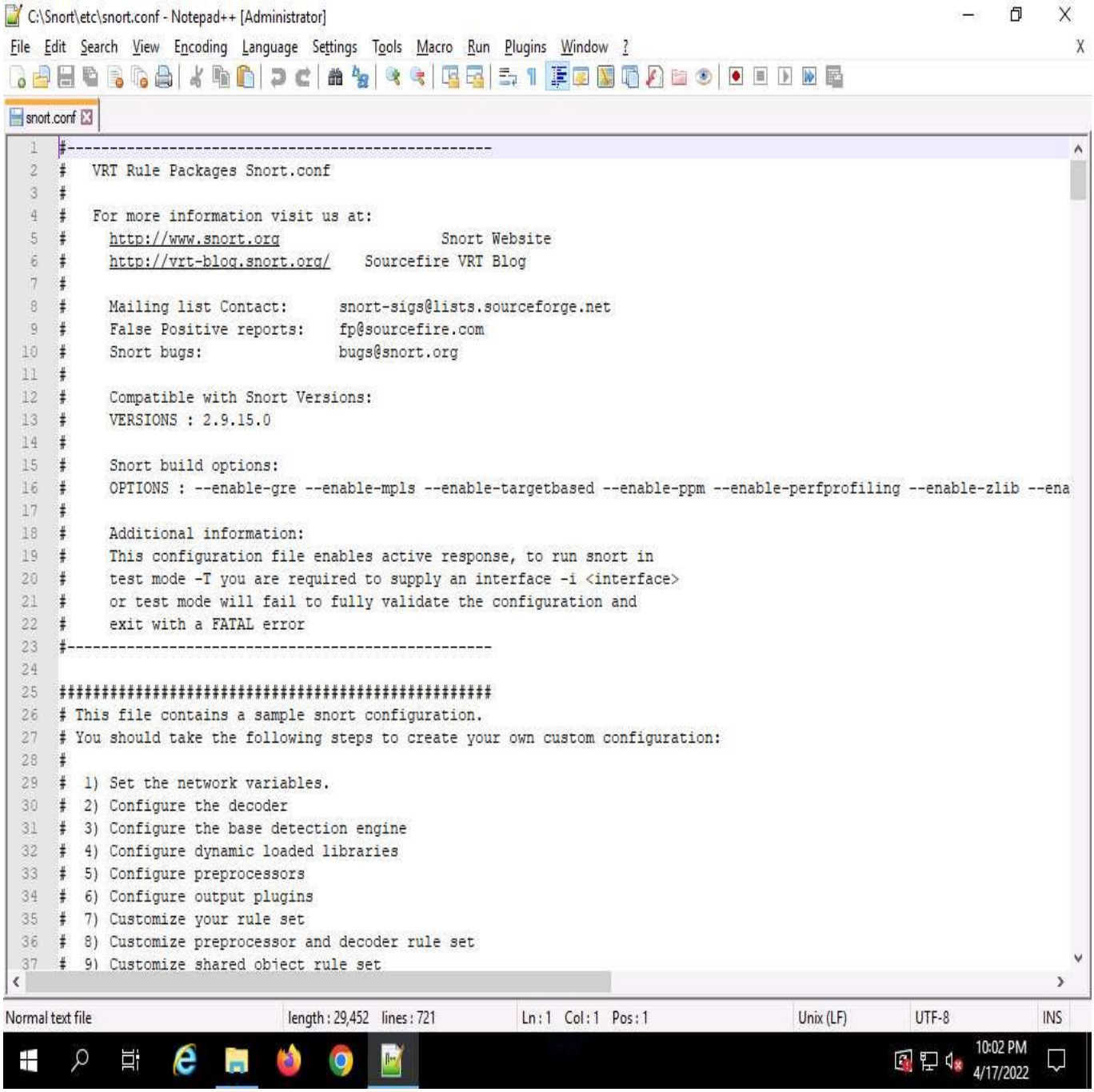


23. ☐ This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

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++**.

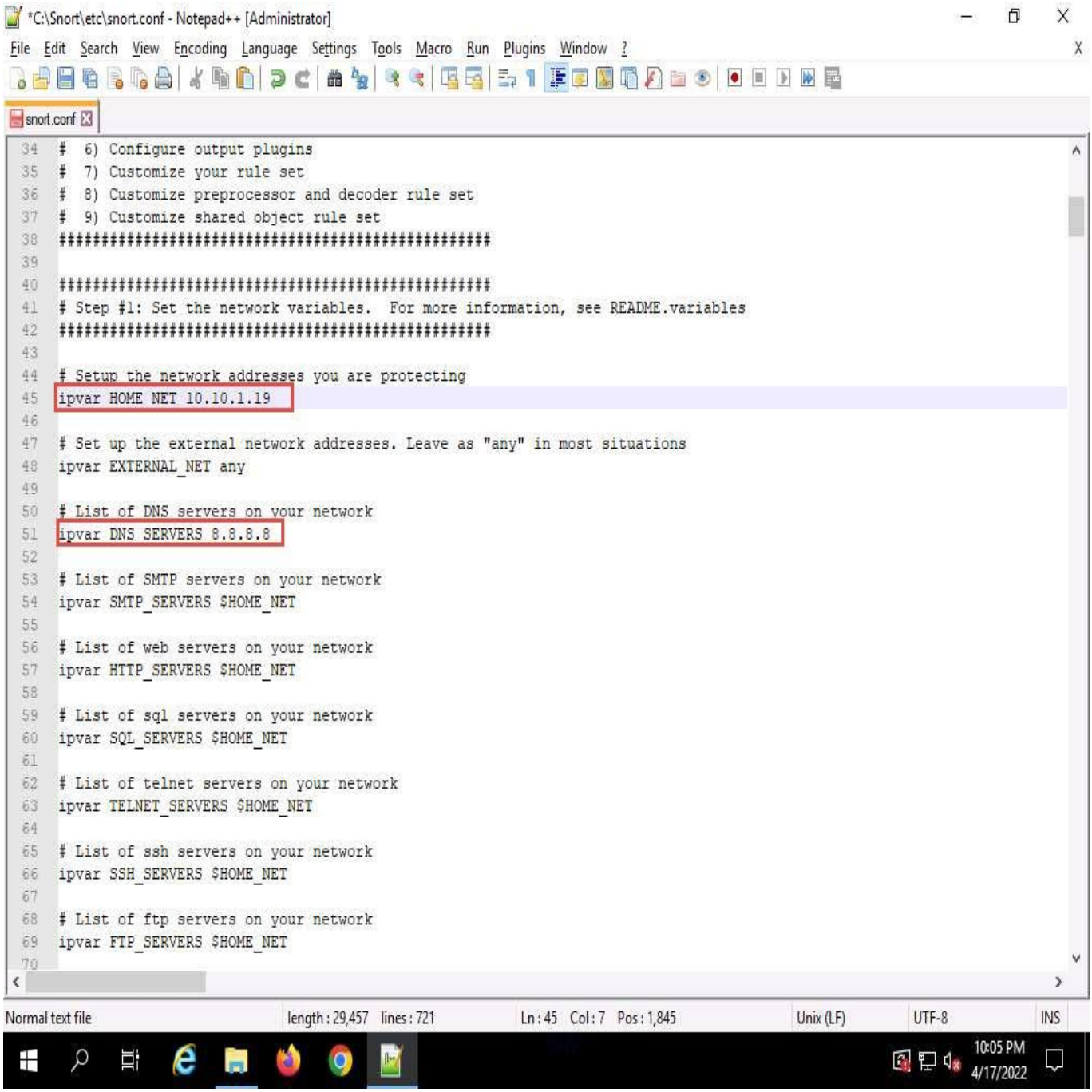


27. ☐ Scroll down to the **Step #1: Set the network variables** section (Line 41) of the **snort.conf** file. In the **HOME_NET** line (Line 45), replace **any** with the IP addresses of the machine (target machine) on which Snort is running. Here, the target machine is **Windows Server 2019** and the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

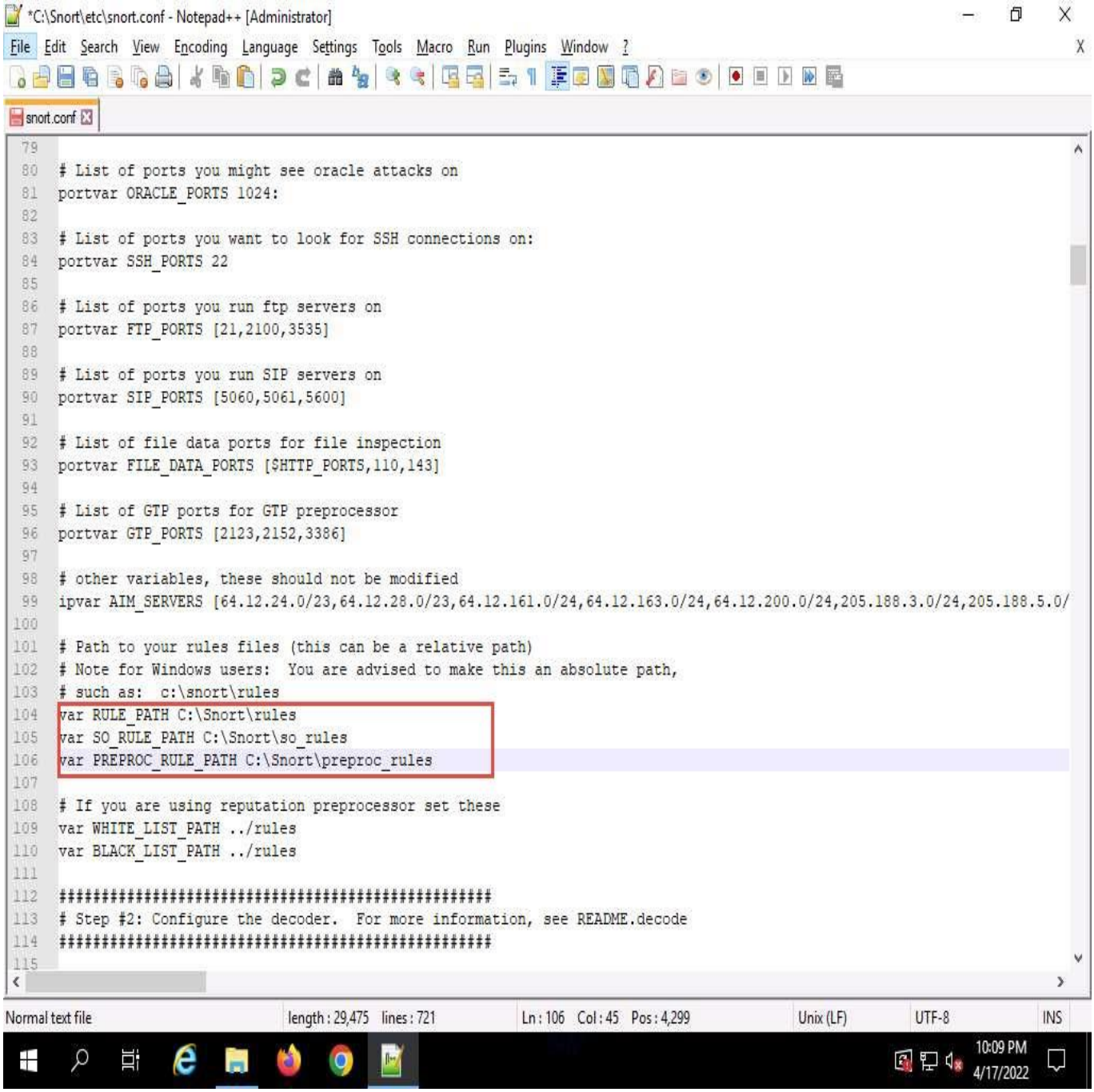
This IP address may vary when you perform this task.

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.

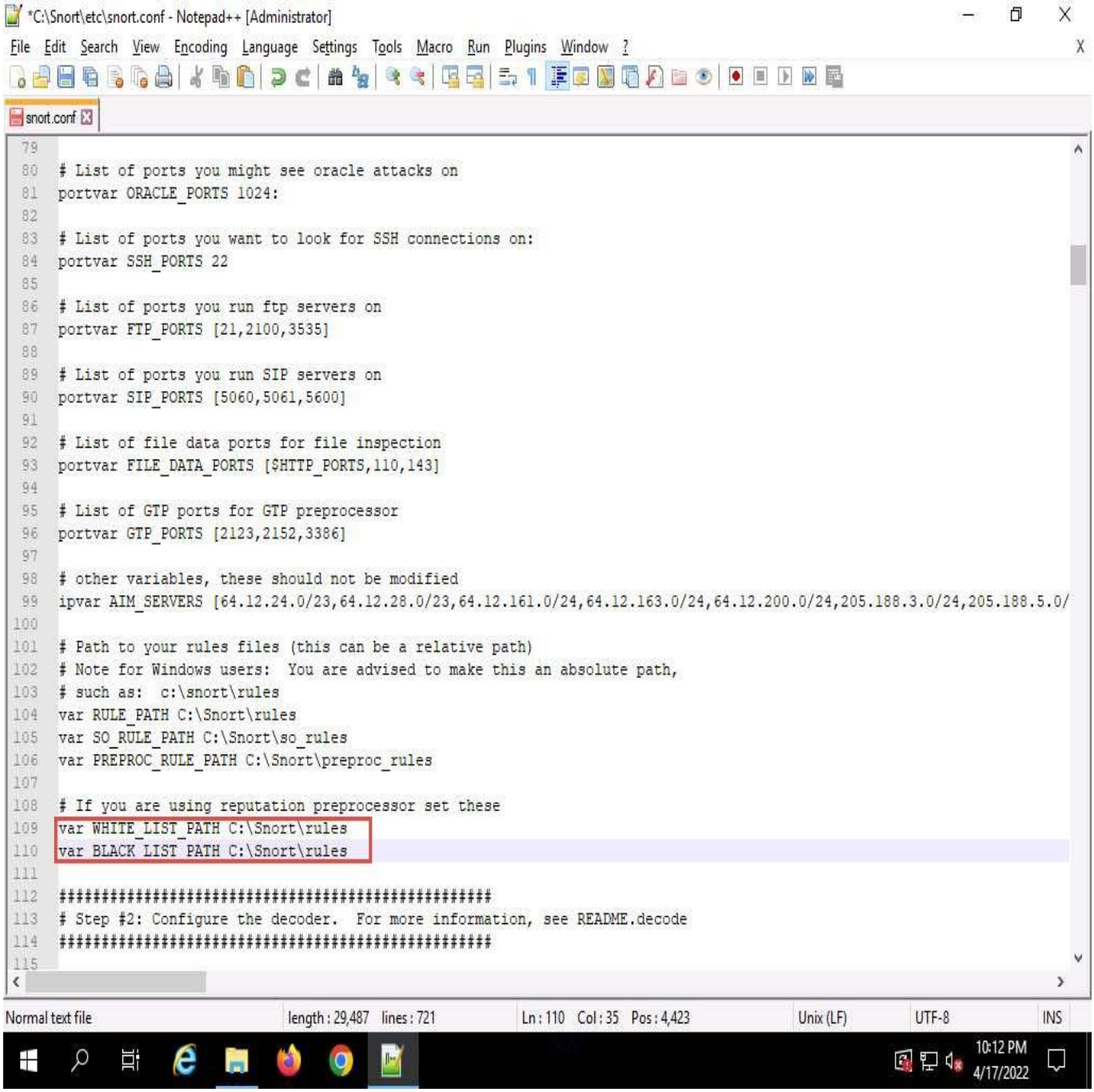
Here, the DNS server is **8.8.8.8**.



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**.

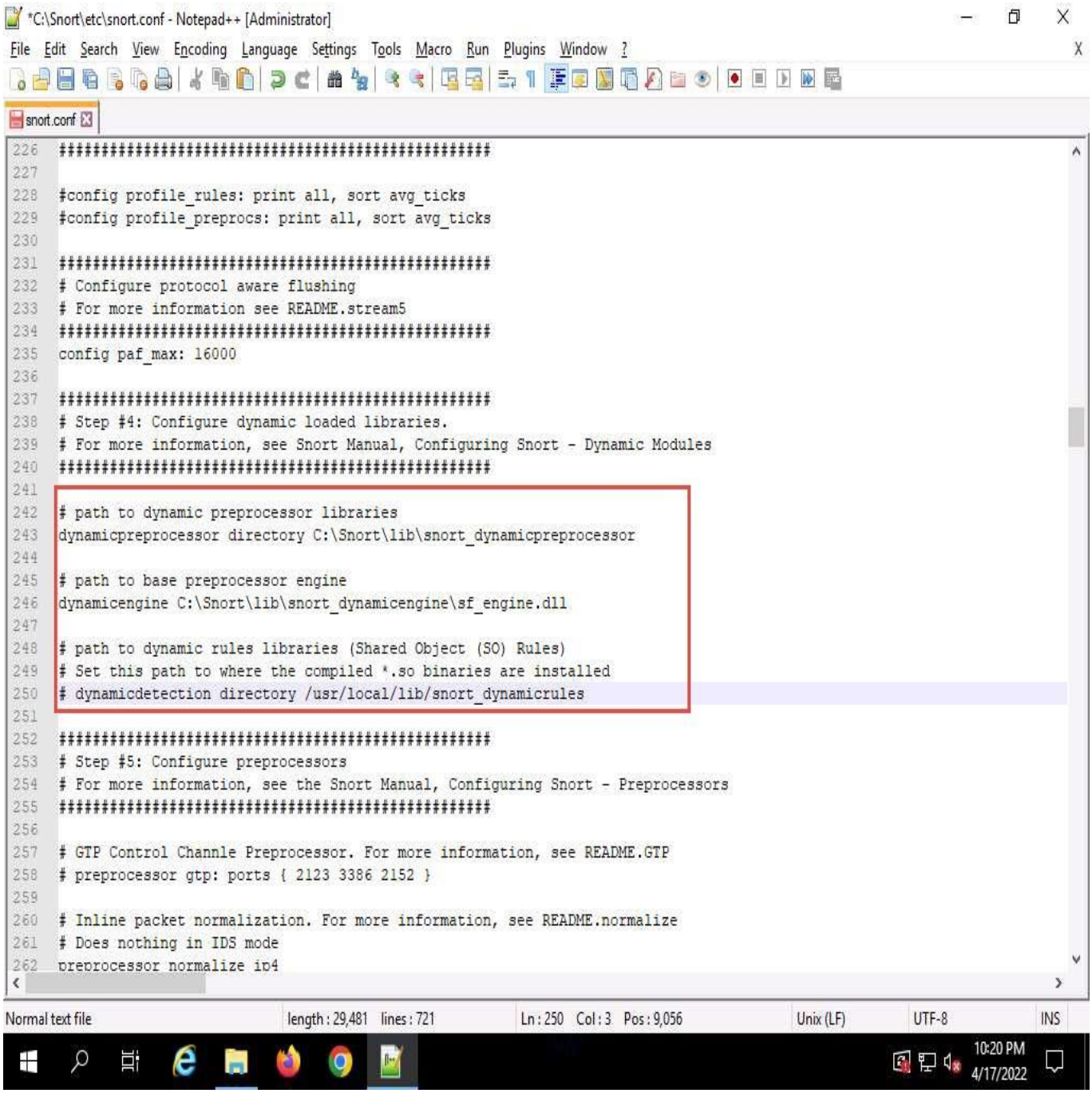
To create a text file, right-click anywhere inside the rules window and navigate to **New --> Text Document**.

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.

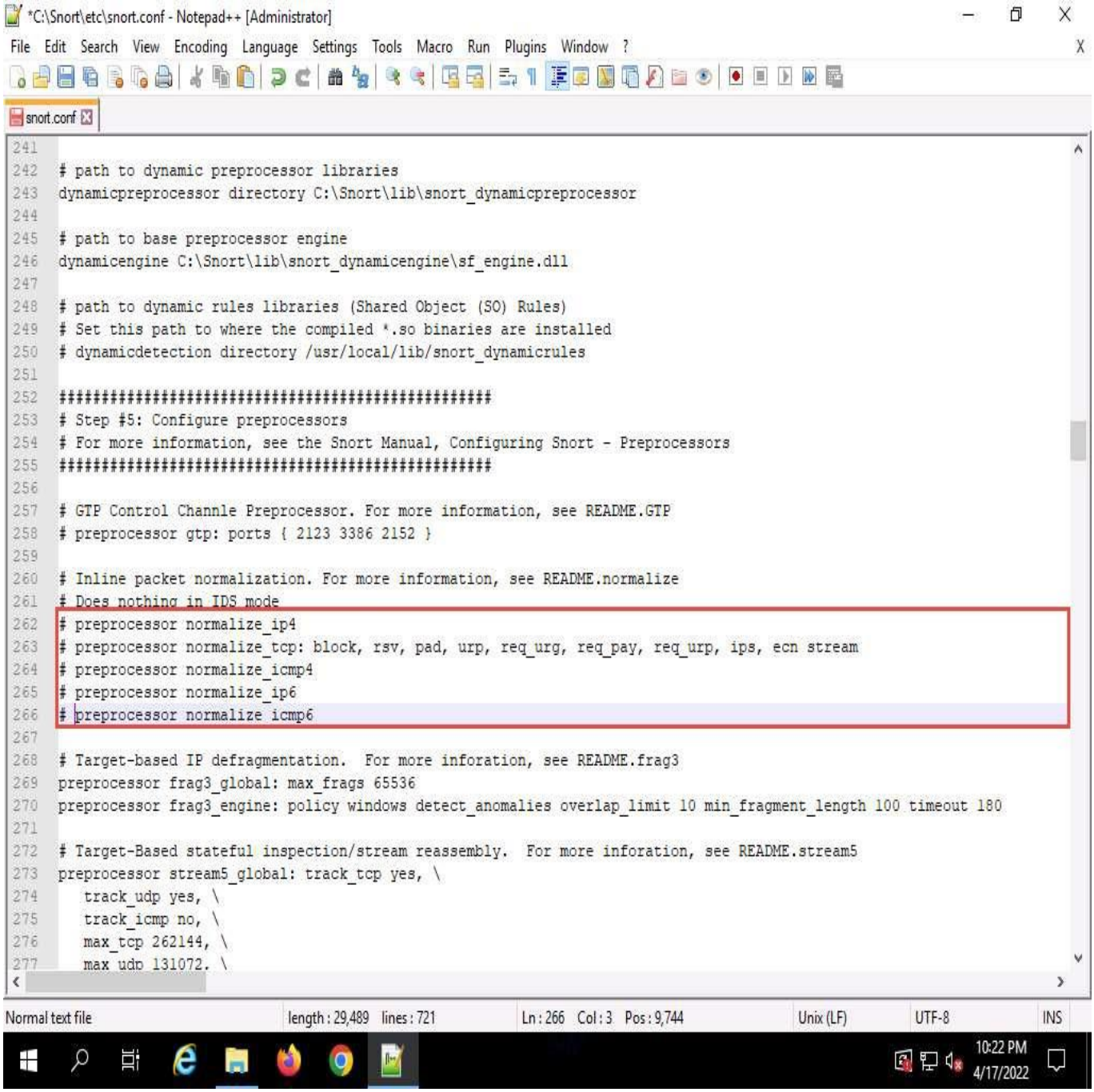
Add (**space**) in between **#** and dynamicdetection (Line 250).



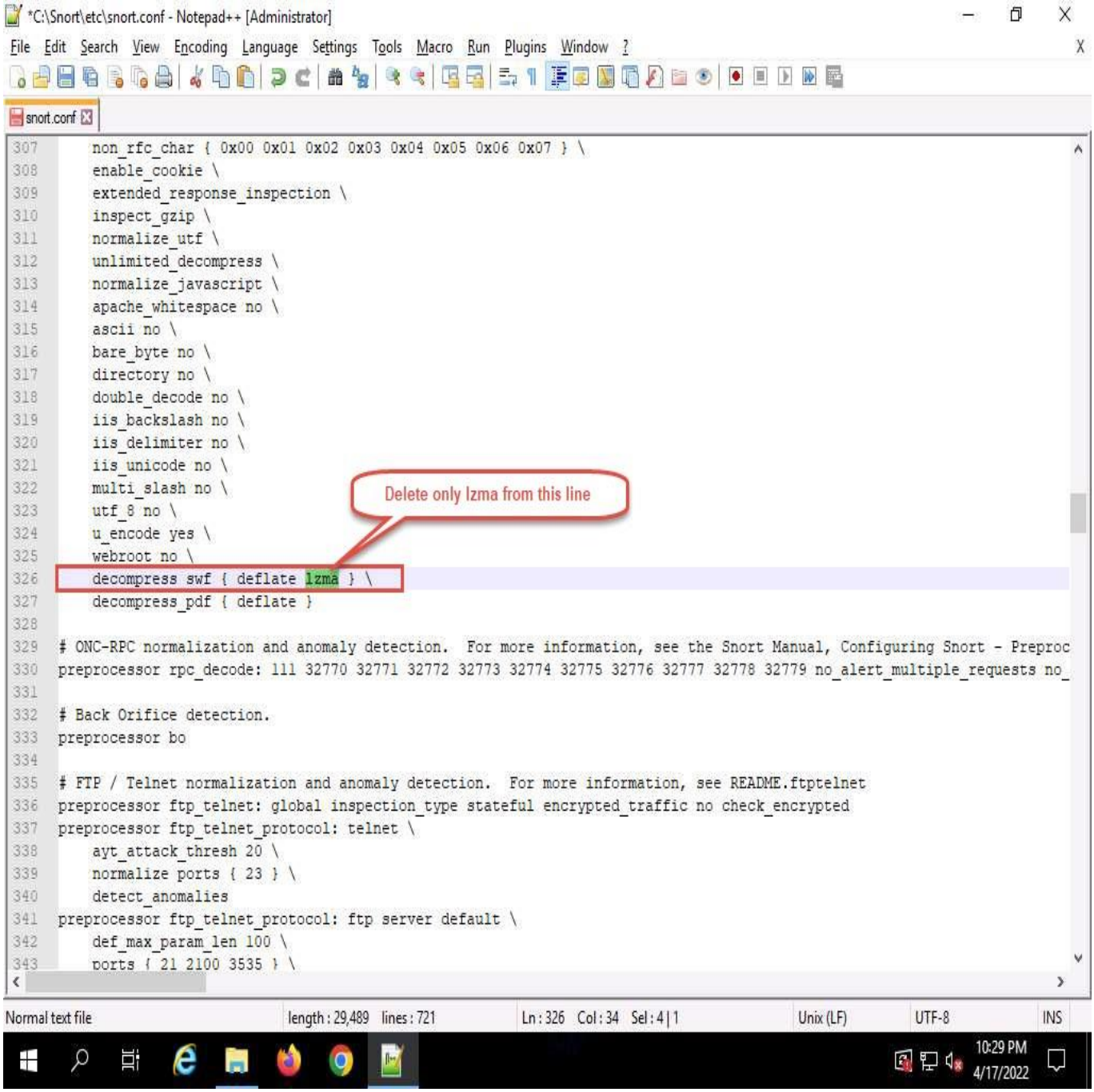
41. ☐ Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed preprocessor. This does nothing in IDS mode, however, it generates errors at runtime.

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

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

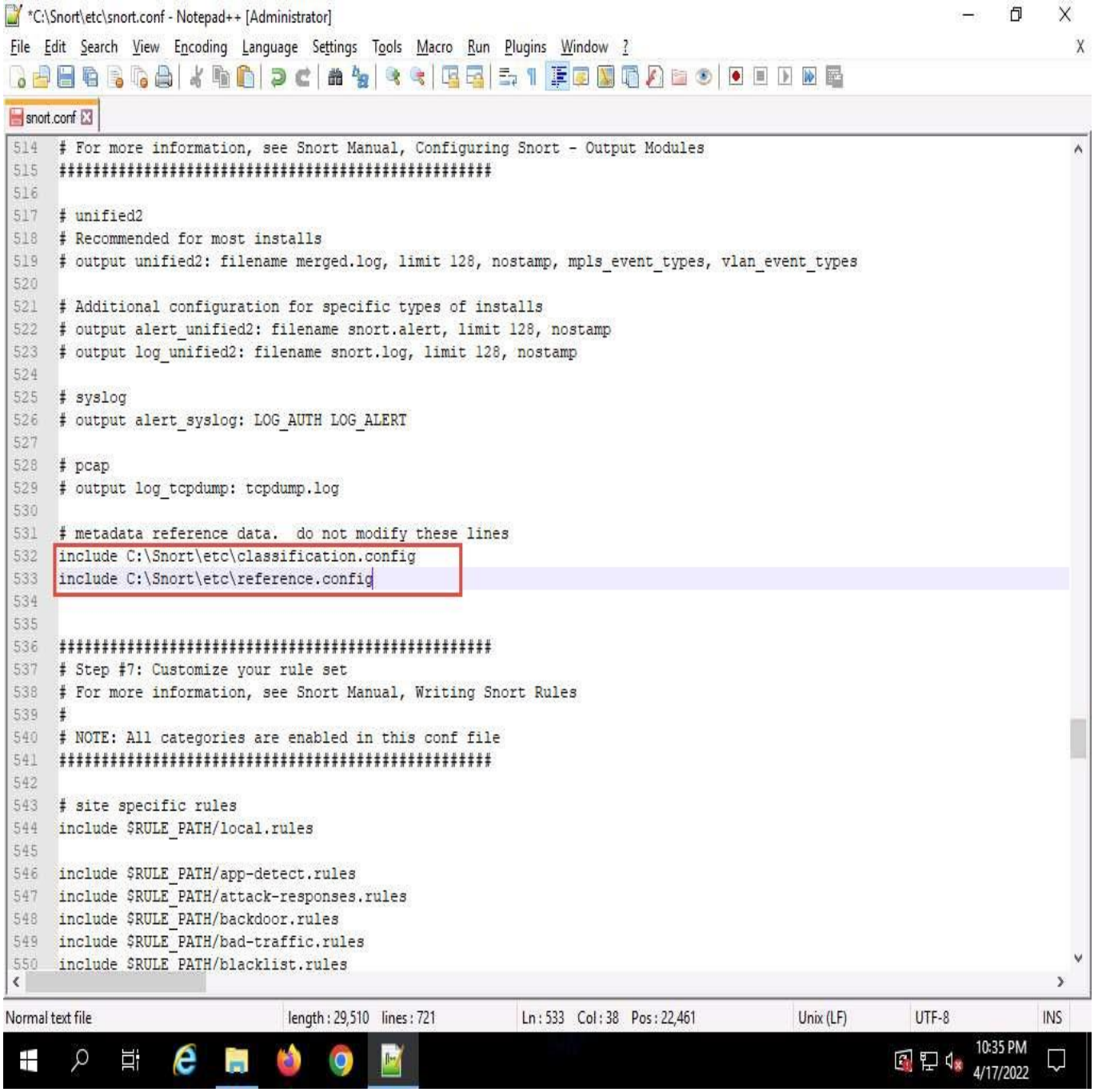


43. ☐ Scroll down to line 326 and delete **lzma** keyword and a (**space**).

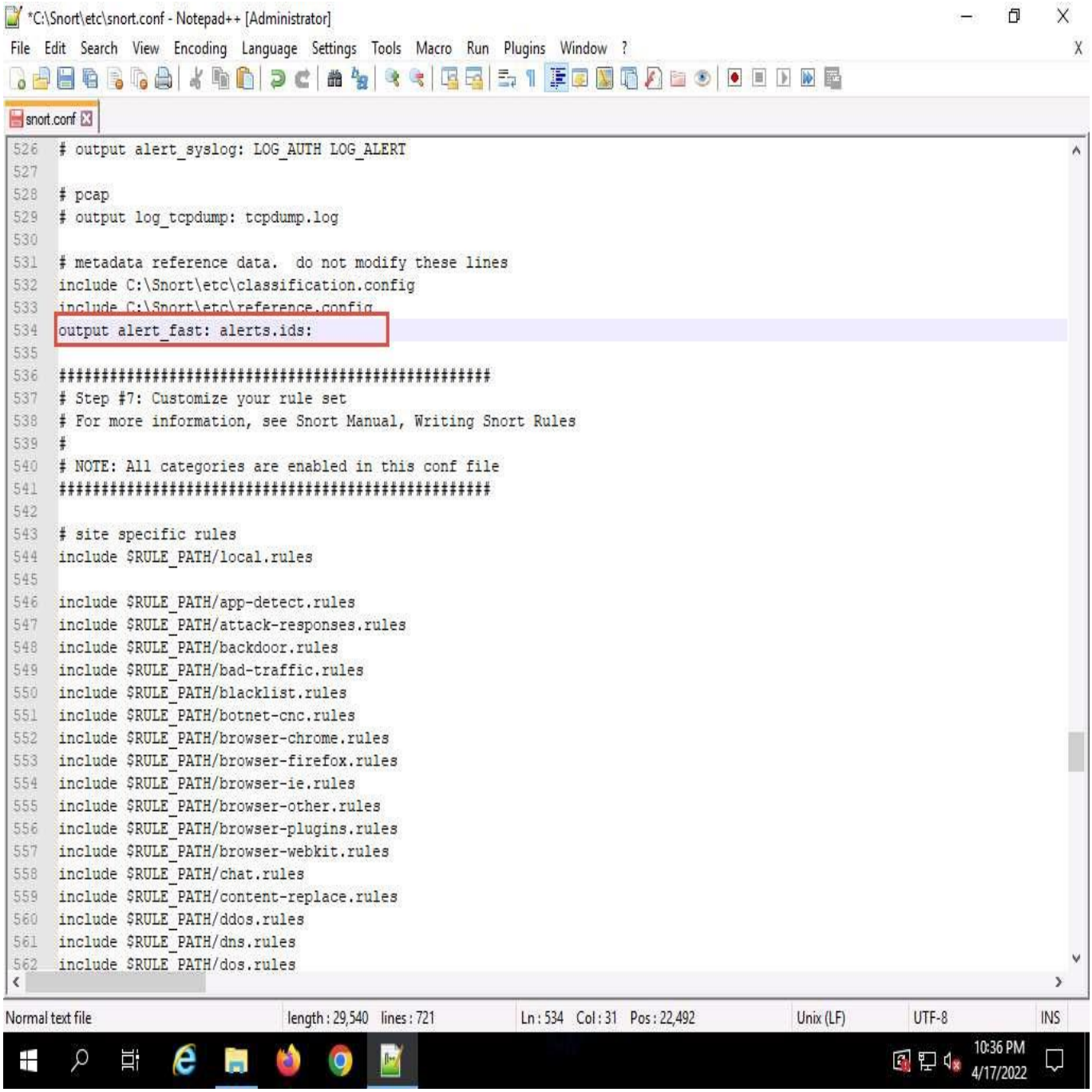


44. ☐ Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.

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.

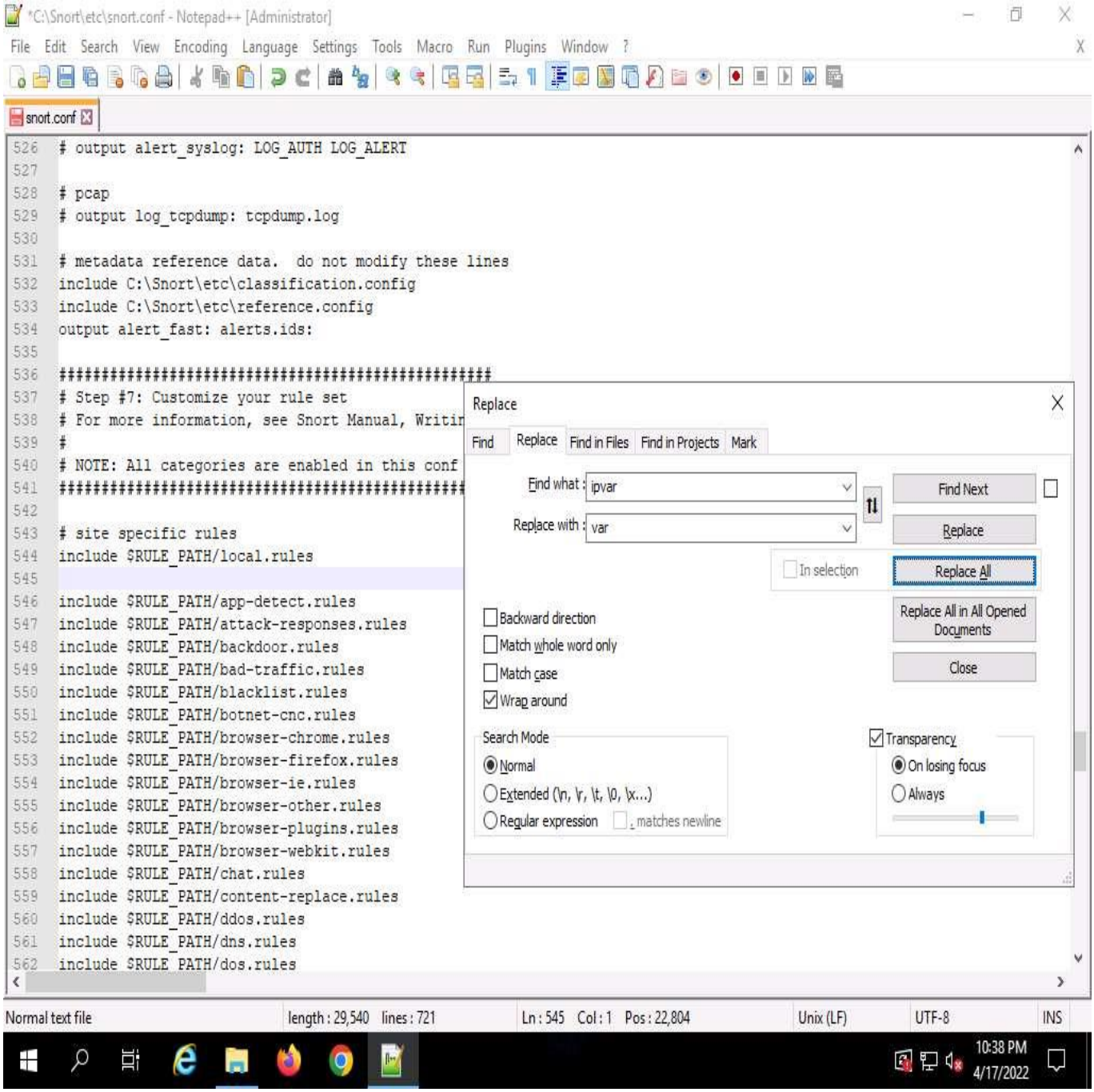


47. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To do this, press **Ctrl+H** on the keyboard. The **Replace** window appears; enter **ipvar** in the **Find what** : text field, enter **var** in the **Replace with** : text field, and click **Replace All**.

You will get a notification saying 11 occurrences were replaced.

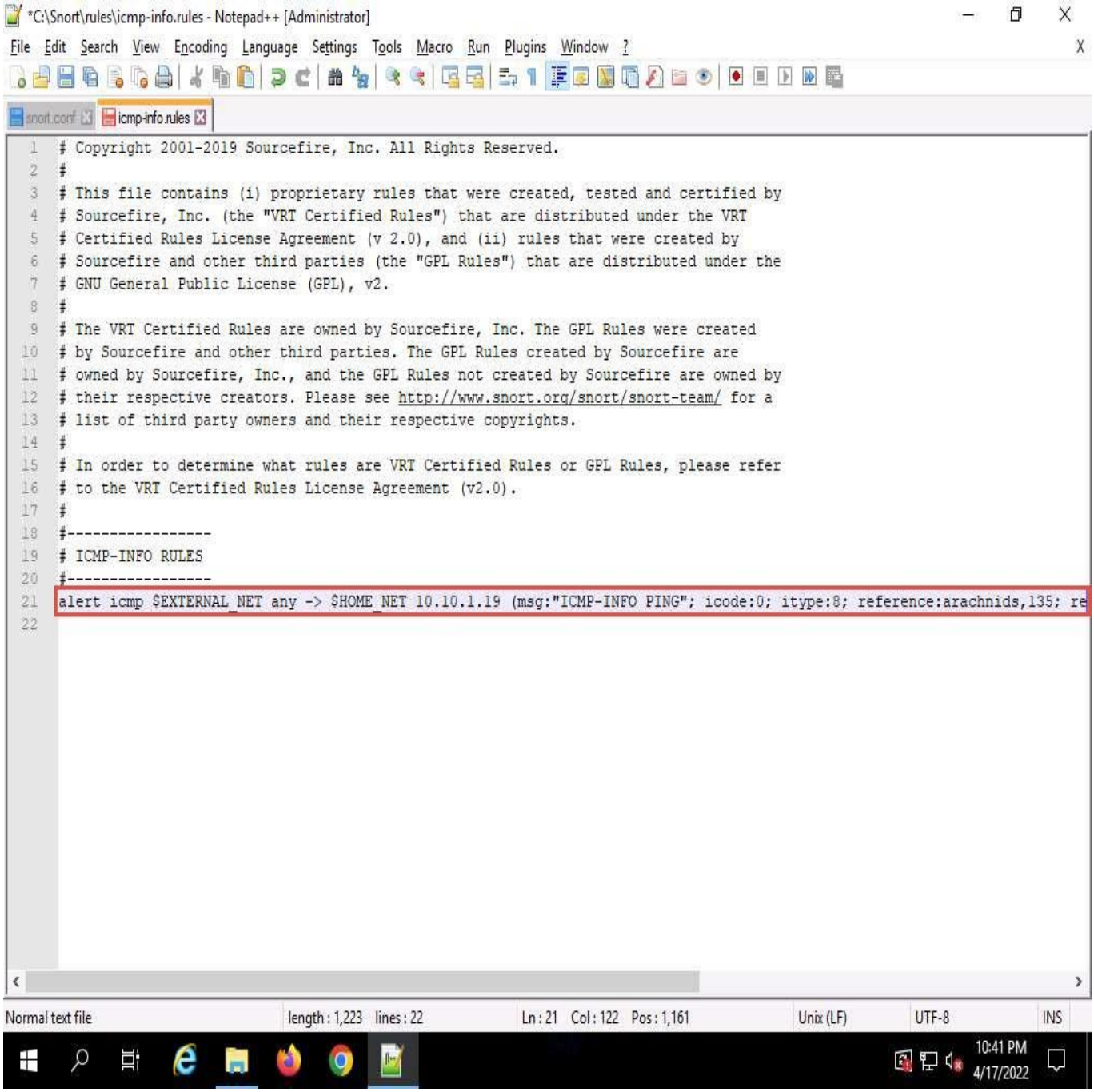
48. By default, the string is **ipvar**, which is not recognized by Snort: replace with the **var** string, and then **close** the window.

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.

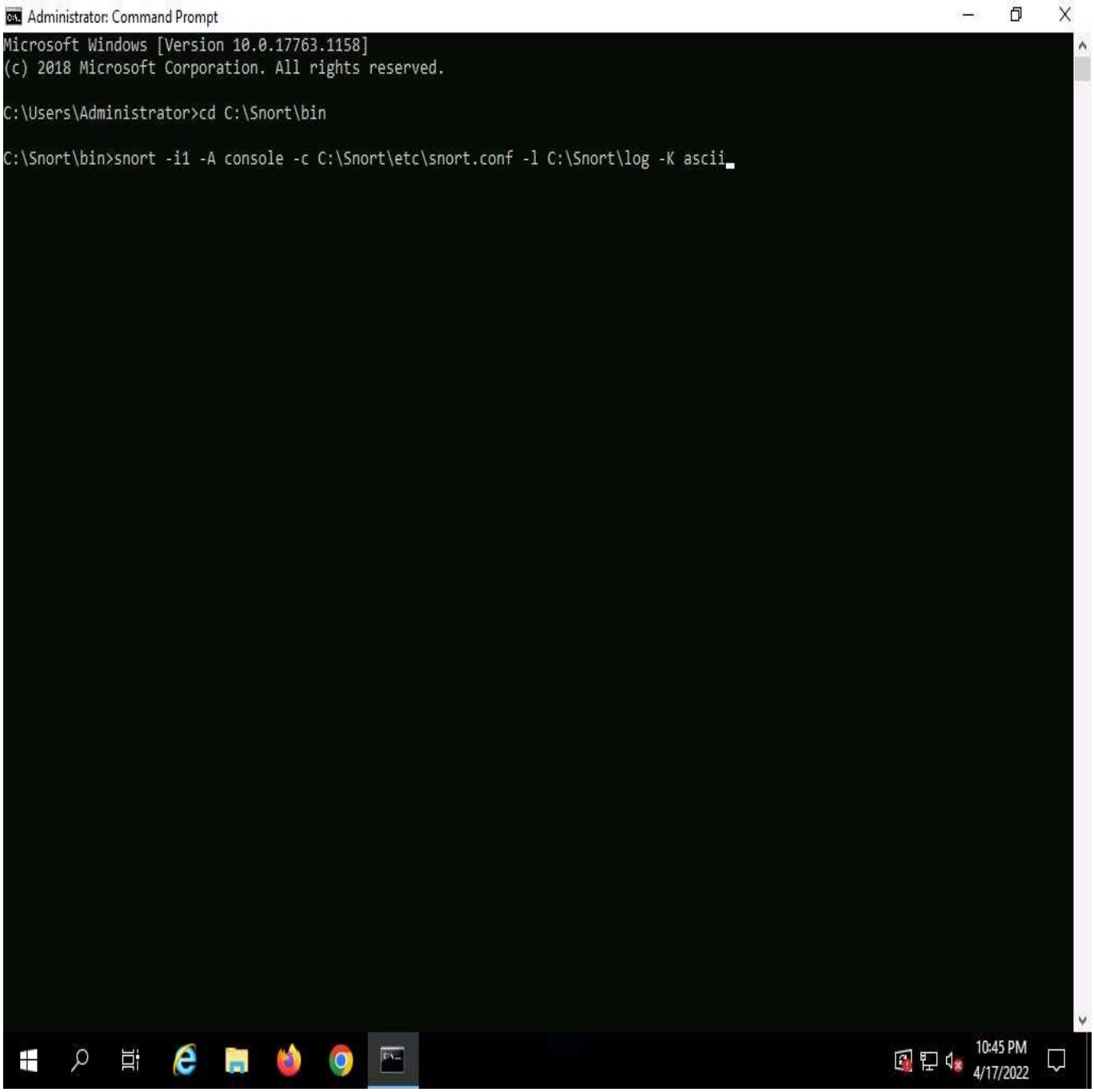


49. ☐ Click **Close** to close the **Replace** window.
50. ☐ Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.
51. ☐ Before running Snort, you need to enable detection rules in the Snort rules file. For this task, we have enabled the ICMP rule so that Snort can detect any 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.

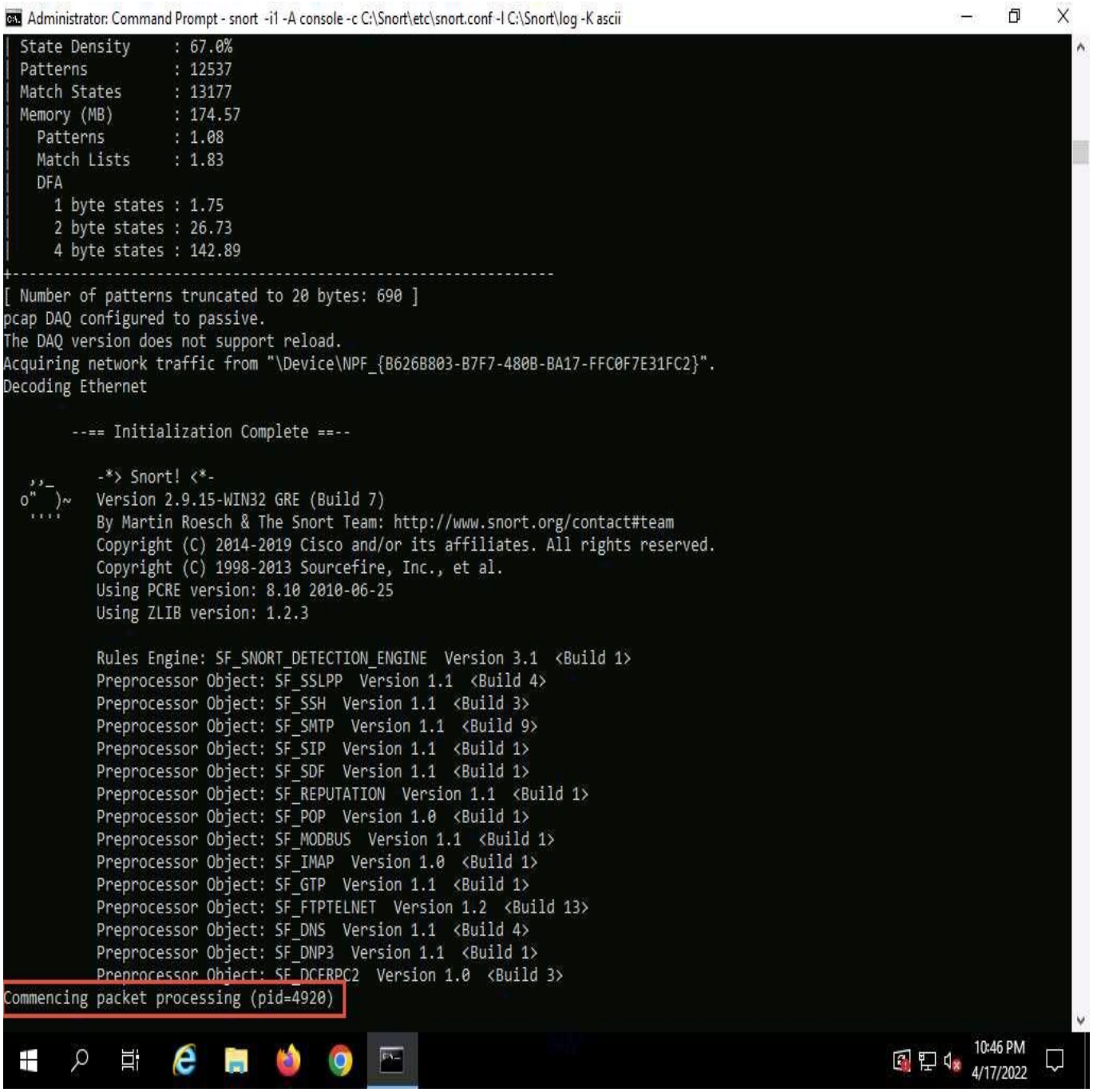
The IP address (10.10.1.19) mentioned in $HOME_NET may vary when you perform this task.



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.



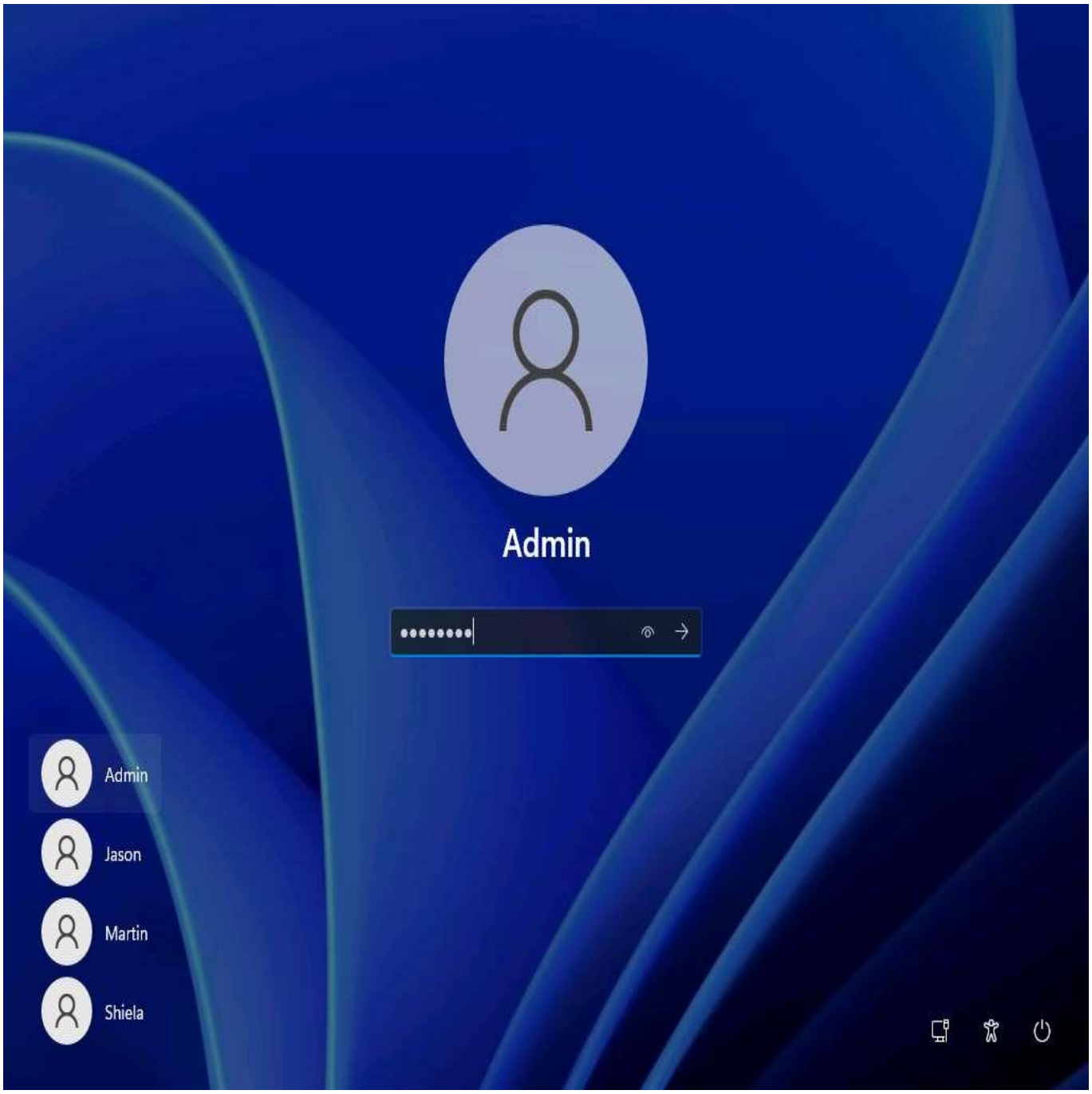
62. ☐ After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.
63. ☐ Leave the Snort command prompt running.
64. ☐ Attack your own machine, and check whether Snort detects it or not.
65. ☐ Now, click on Windows 11 to switch to the **Windows 11** machine (**Attacker Machine**).
Click Ctrl+Alt+Delete to activate the machine.

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

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

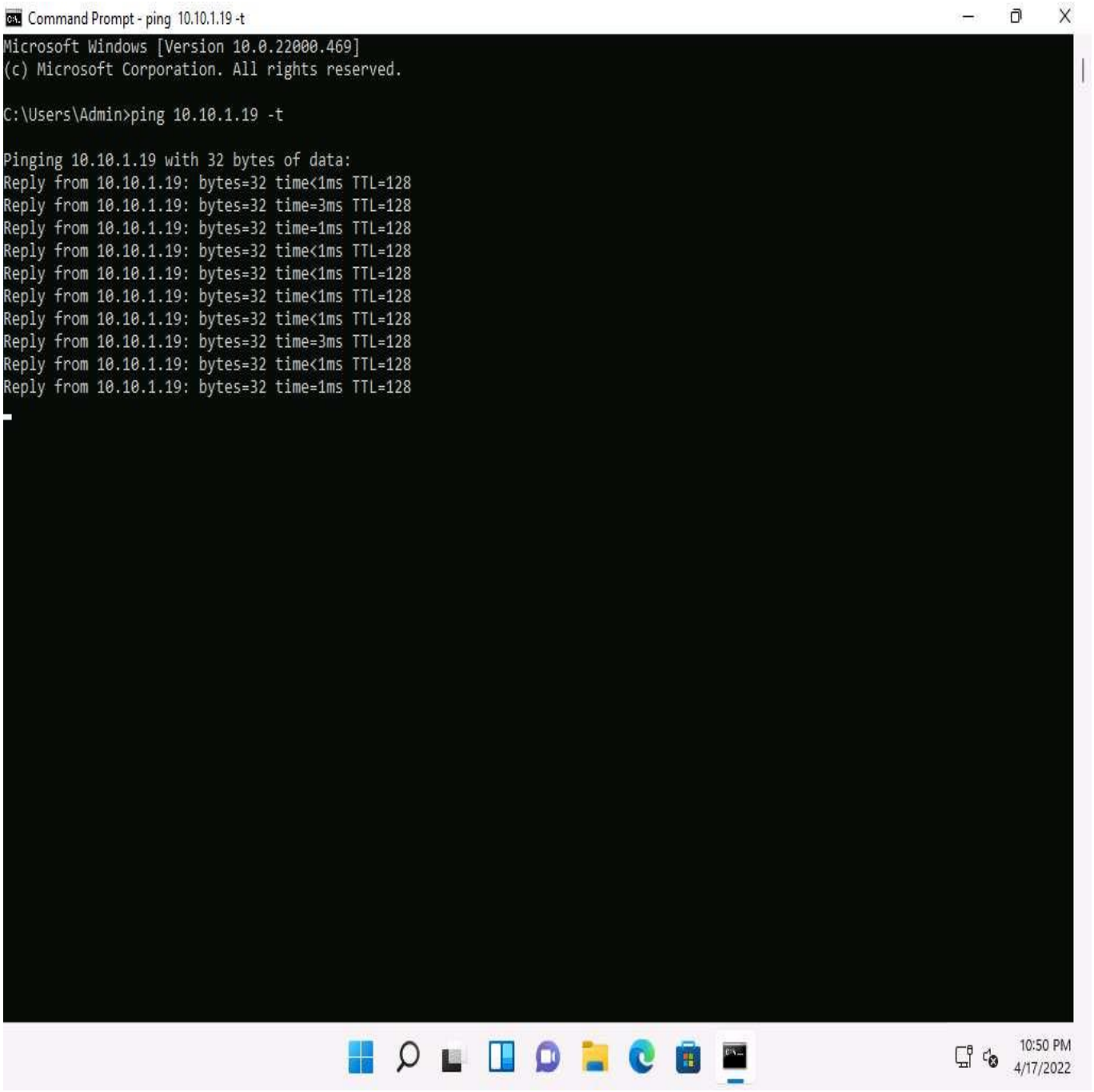
Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

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

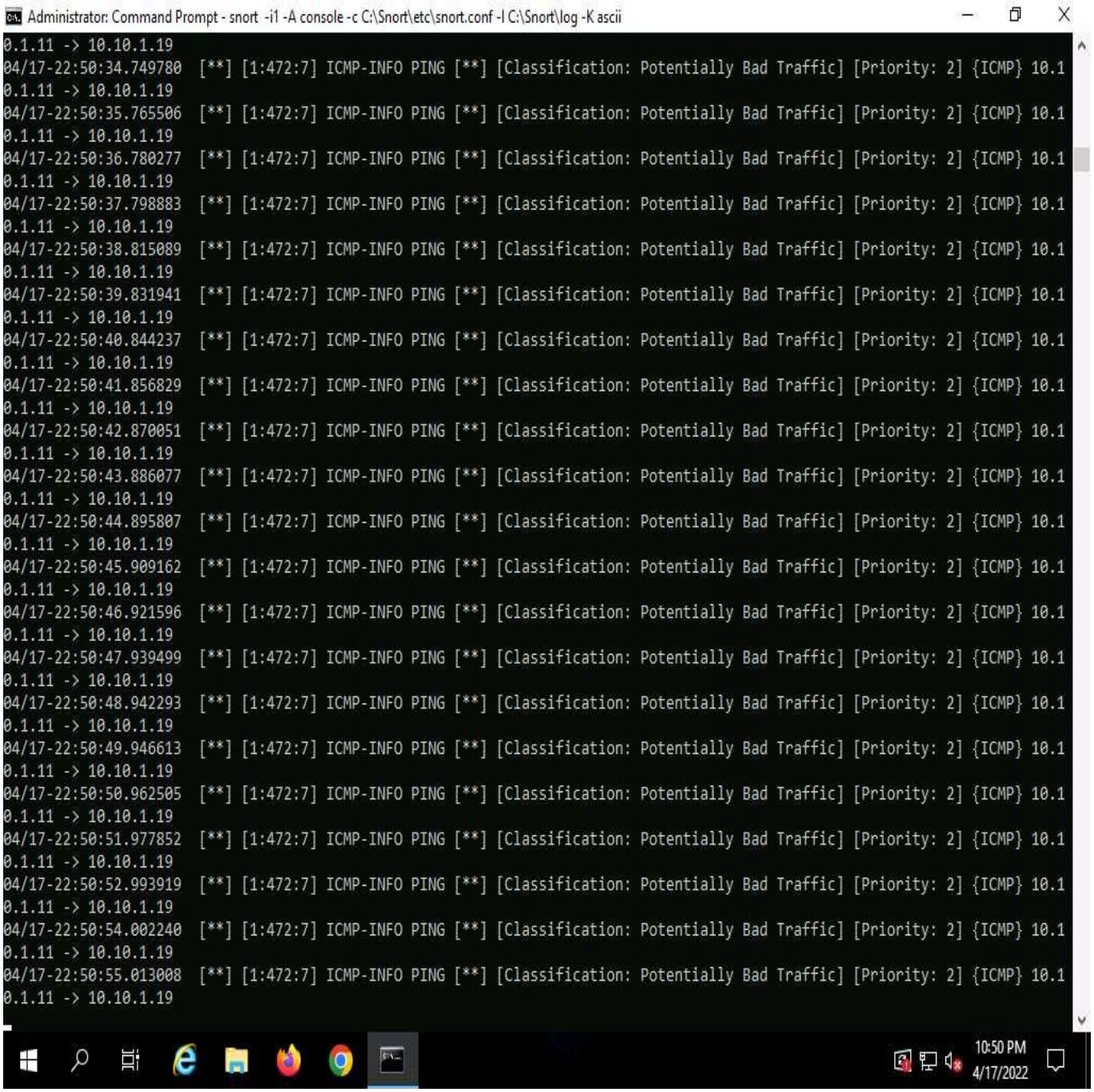


67. ☐ Open the command prompt and issue the command **ping 10.10.1.19 -t** from the **Attacker Machine**

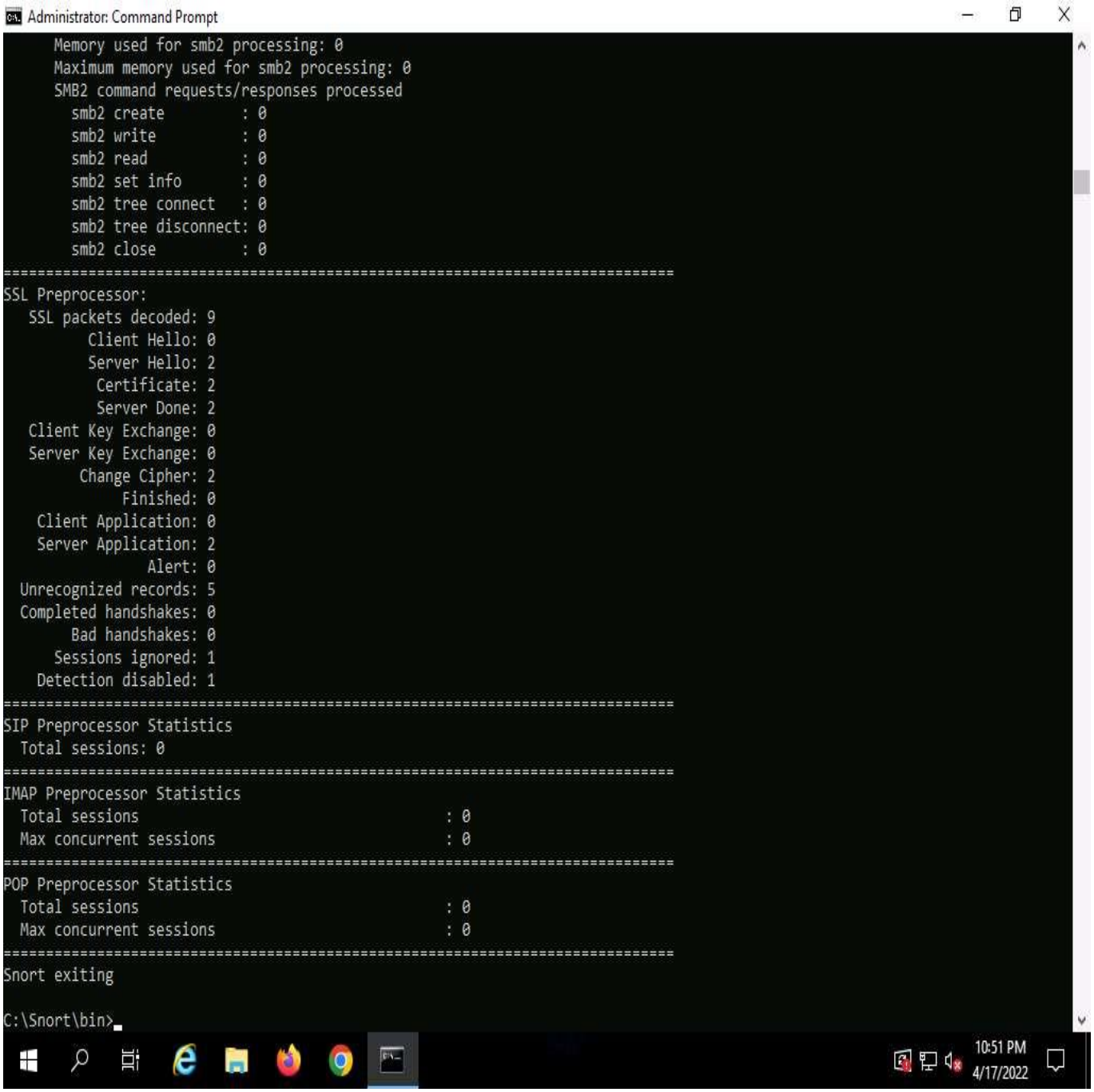
10.10.1.19 is the IP address of the Windows Server 2019. This IP address may differ when you perform the task.



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

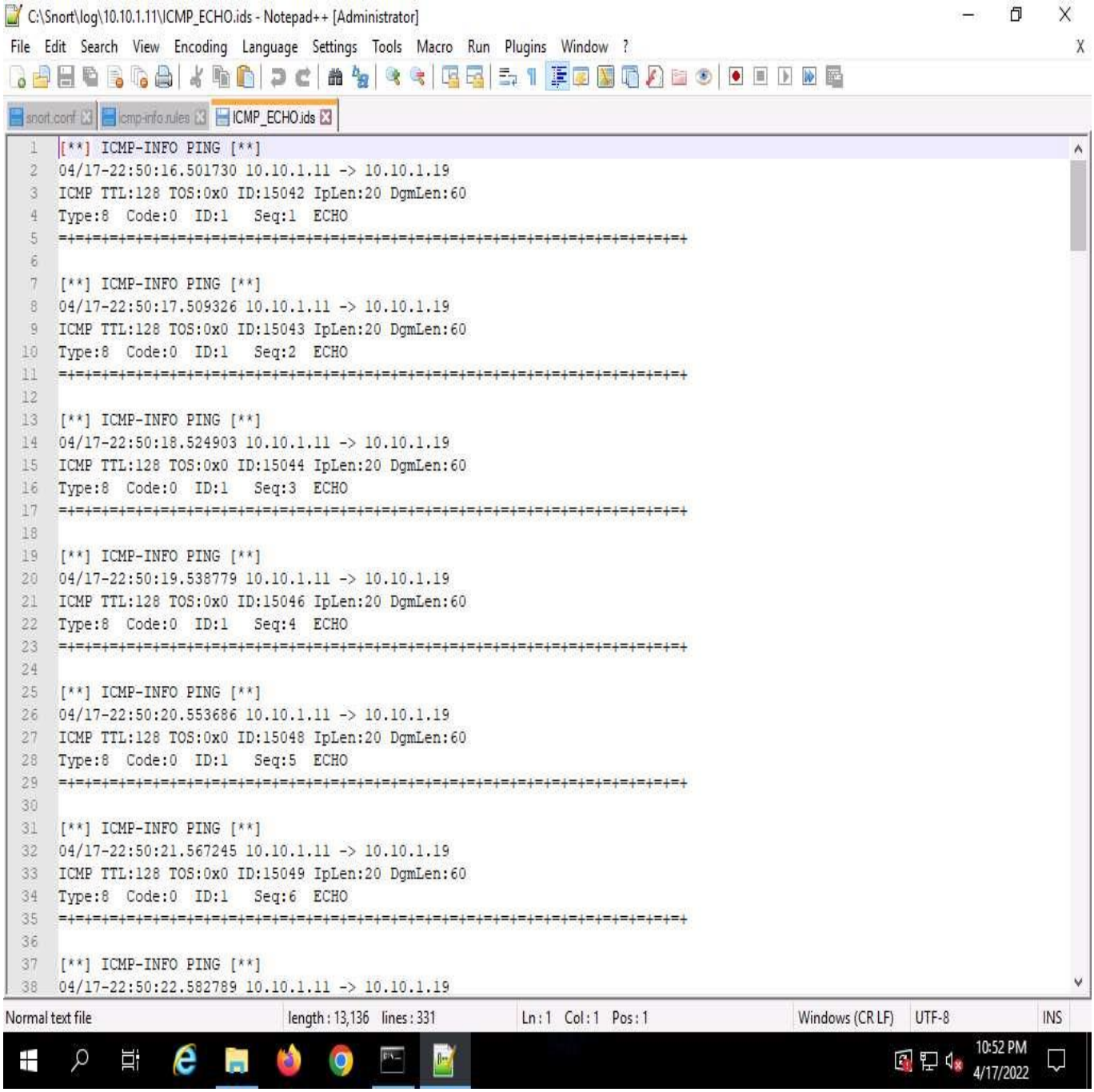


69. ☐ Press **Ctrl+C** to **stop** Snort; snort exits.



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.

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



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

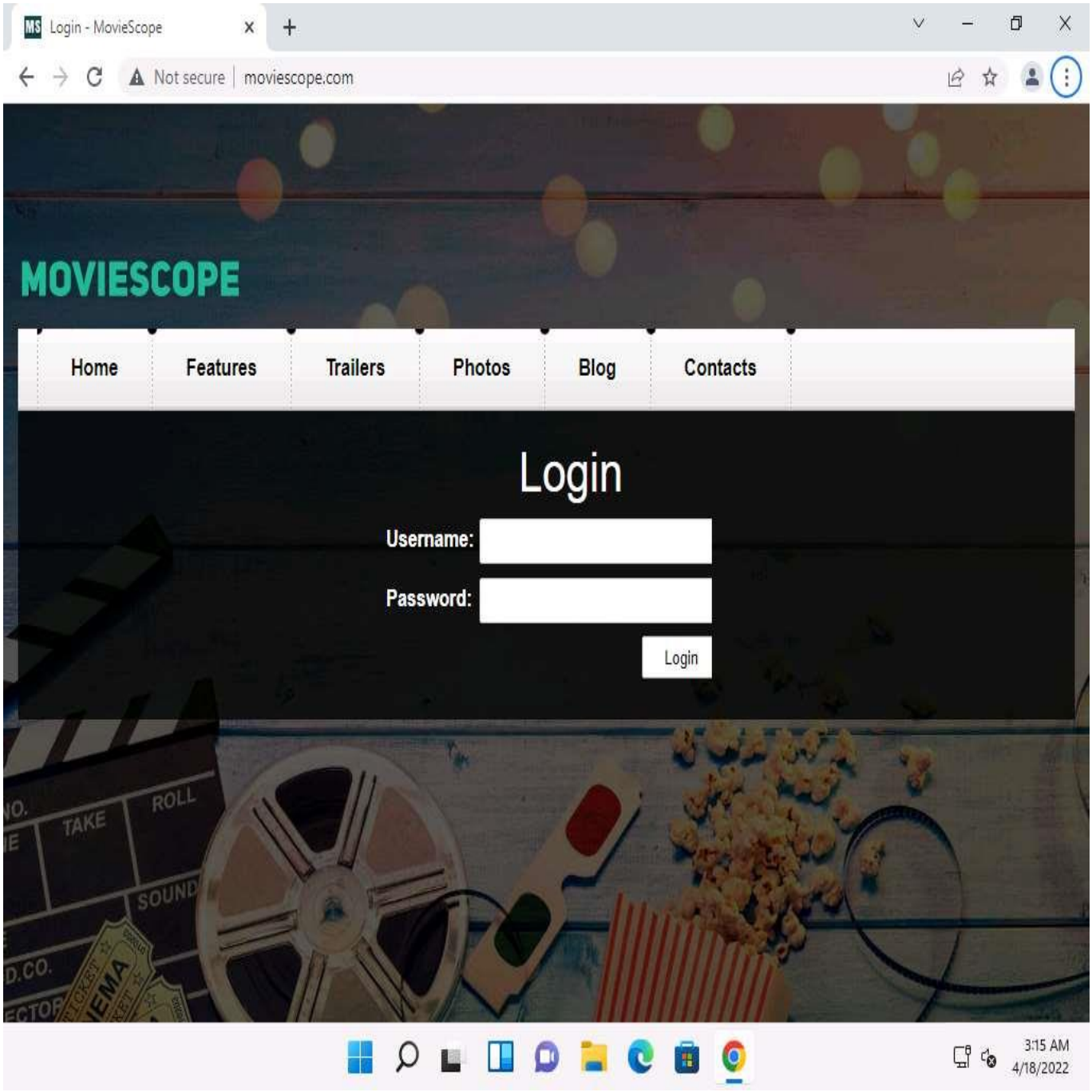
ZoneAlarm FREE Firewall blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting 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.

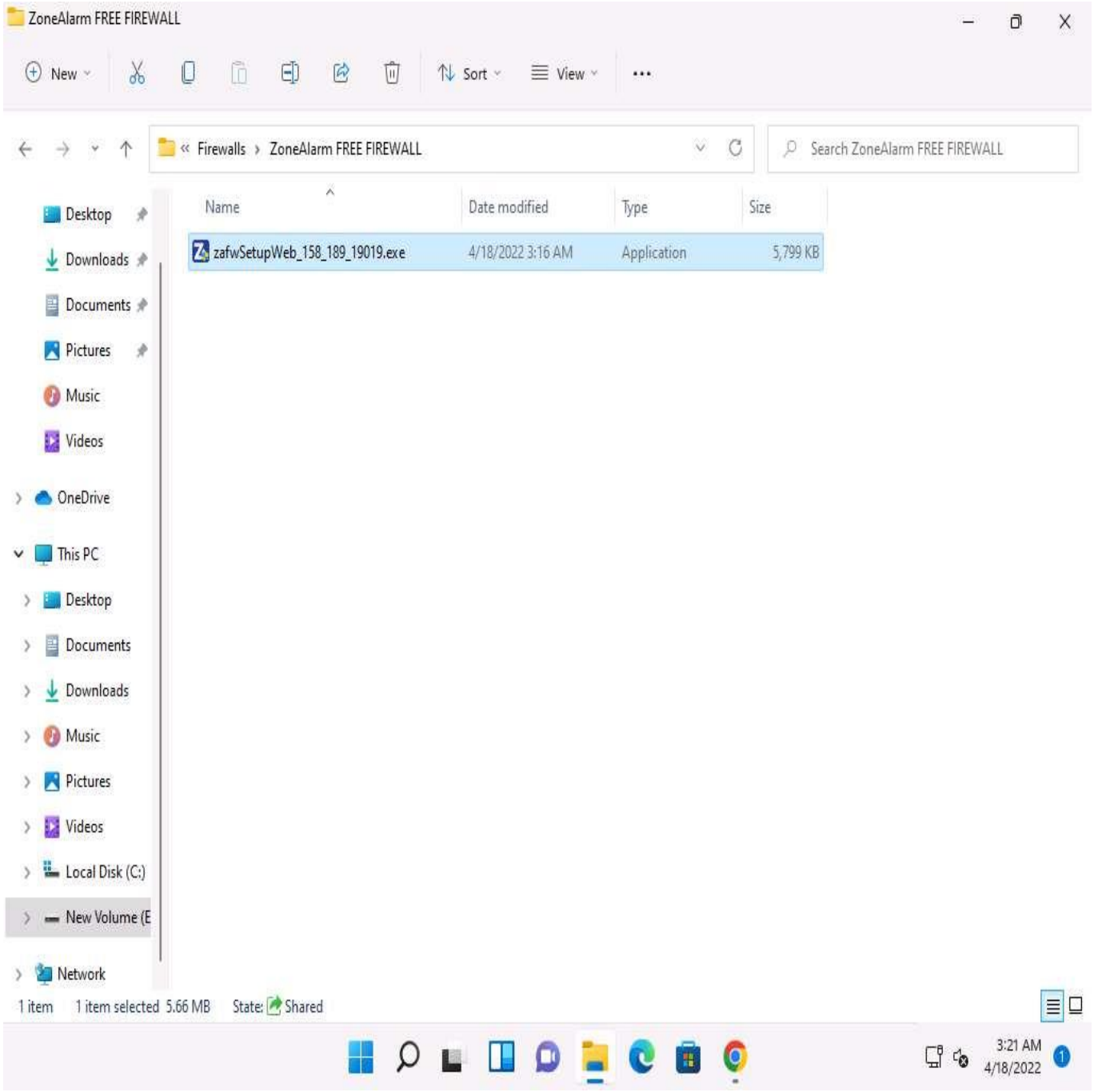
1. Before starting this task, we will browse an unwanted website in the **Windows 11** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

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

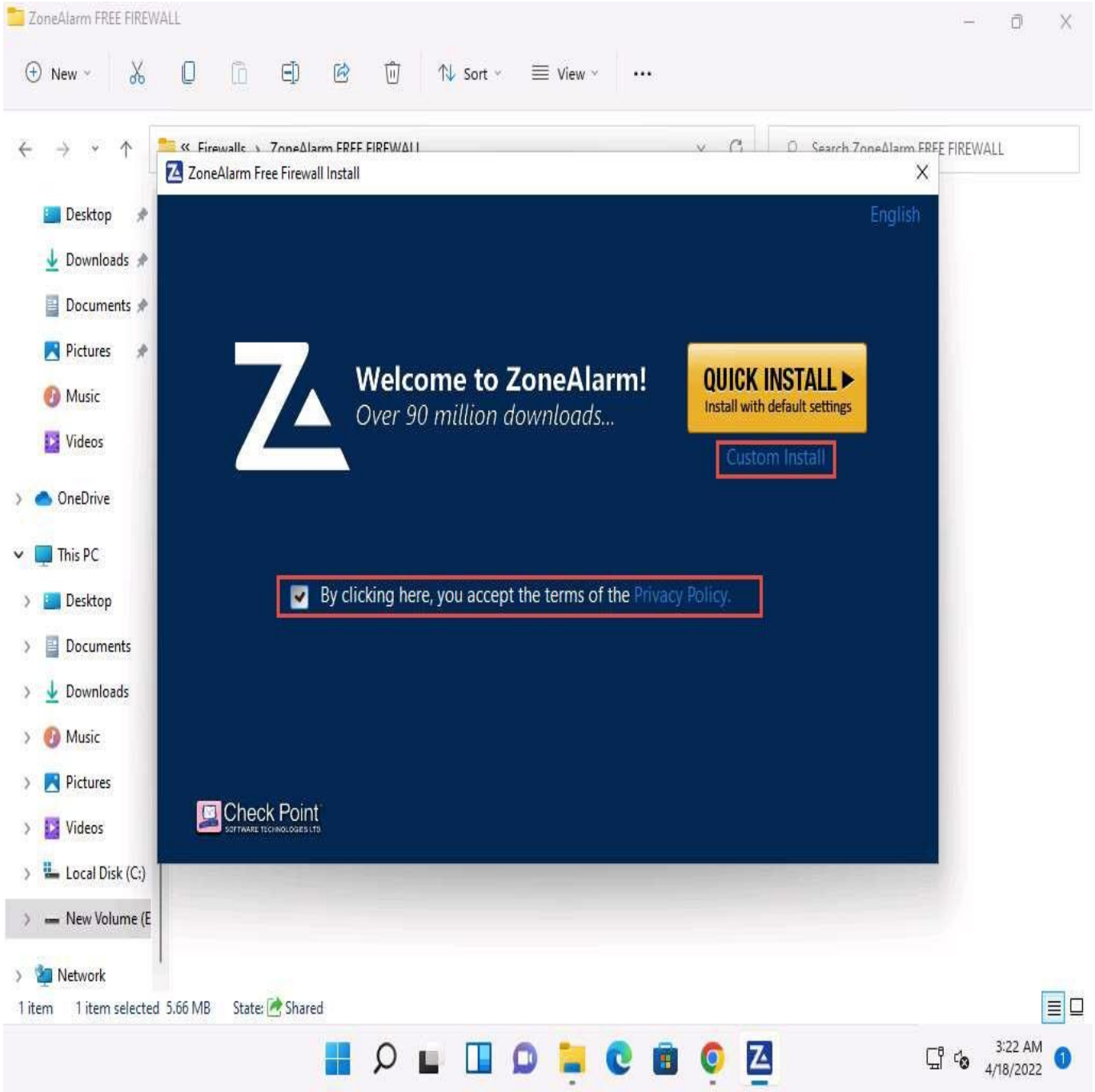
2. Click Windows 11 to switch to the **Windows 11** machine.
3. Open any browser (here, **Google Chrome**) and place the cursor in the address bar, type **www.moviescope.com** and press **Enter**.
4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 11** machine.
5. In this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



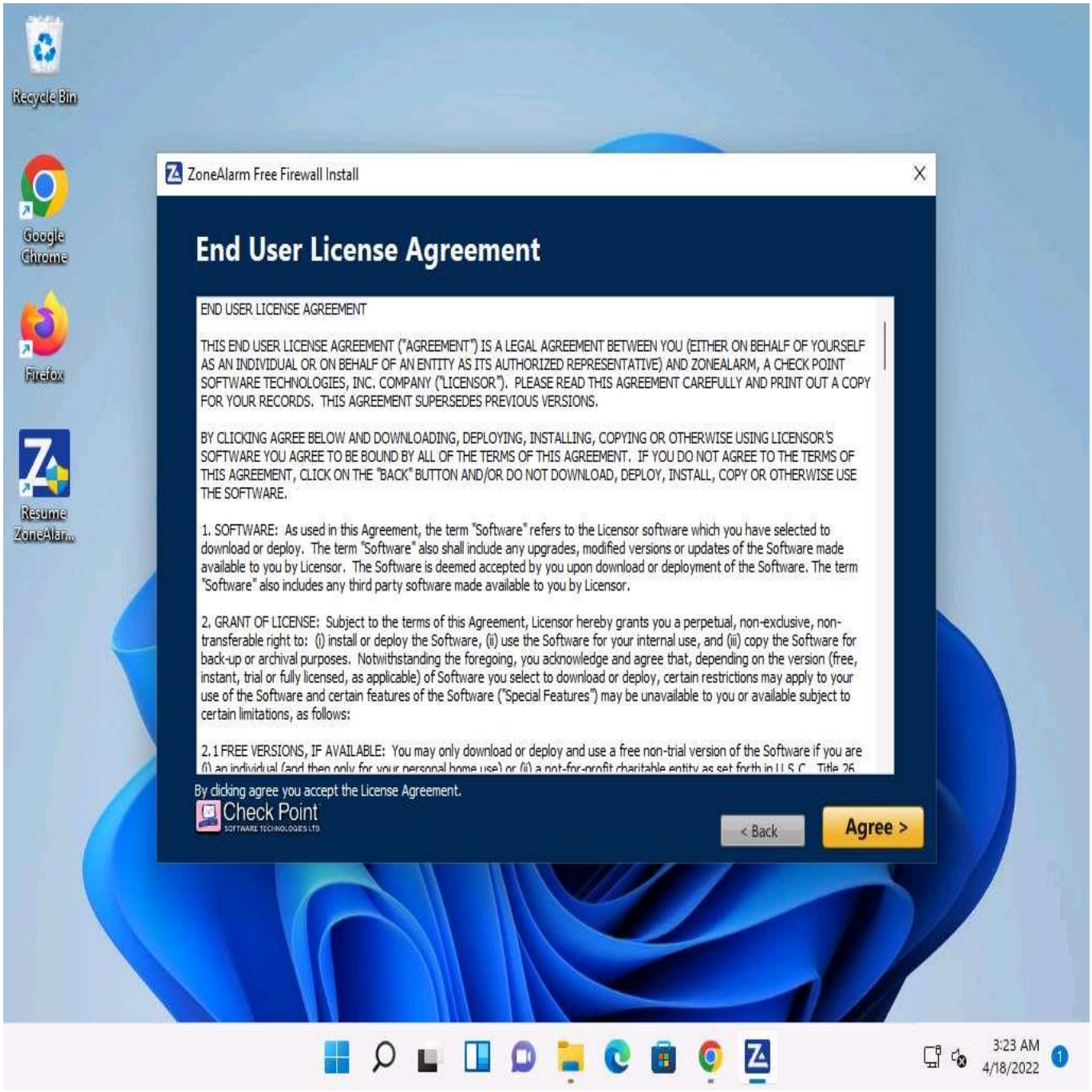
6. ☐ In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL** and double-click **zafwSetupWeb_158_189_19019.exe** to install ZoneAlarm FREE FIREWALL.



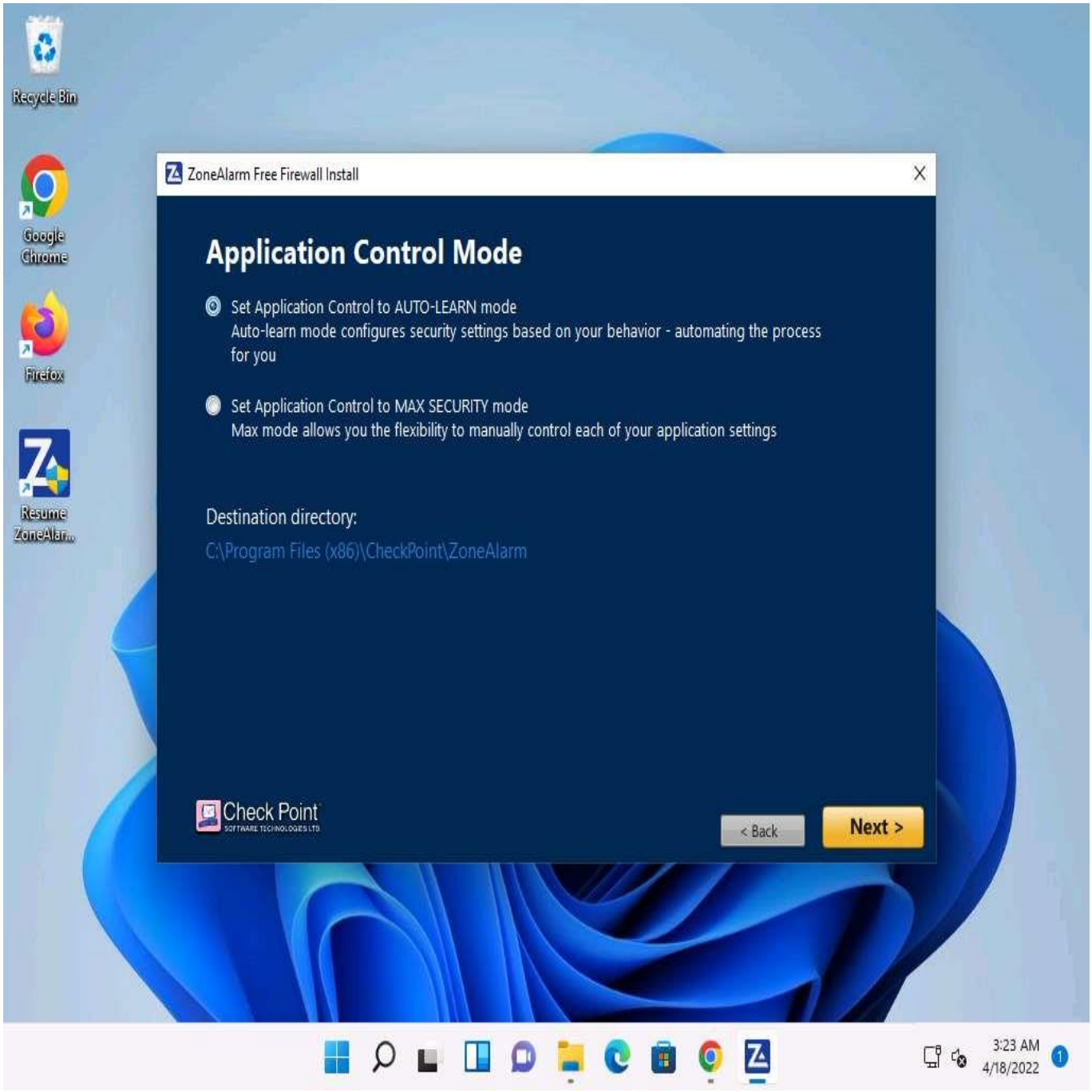
7. ☐ If the **User Account Control** pop-up appears, click **Yes**.
8. ☐ The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.



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

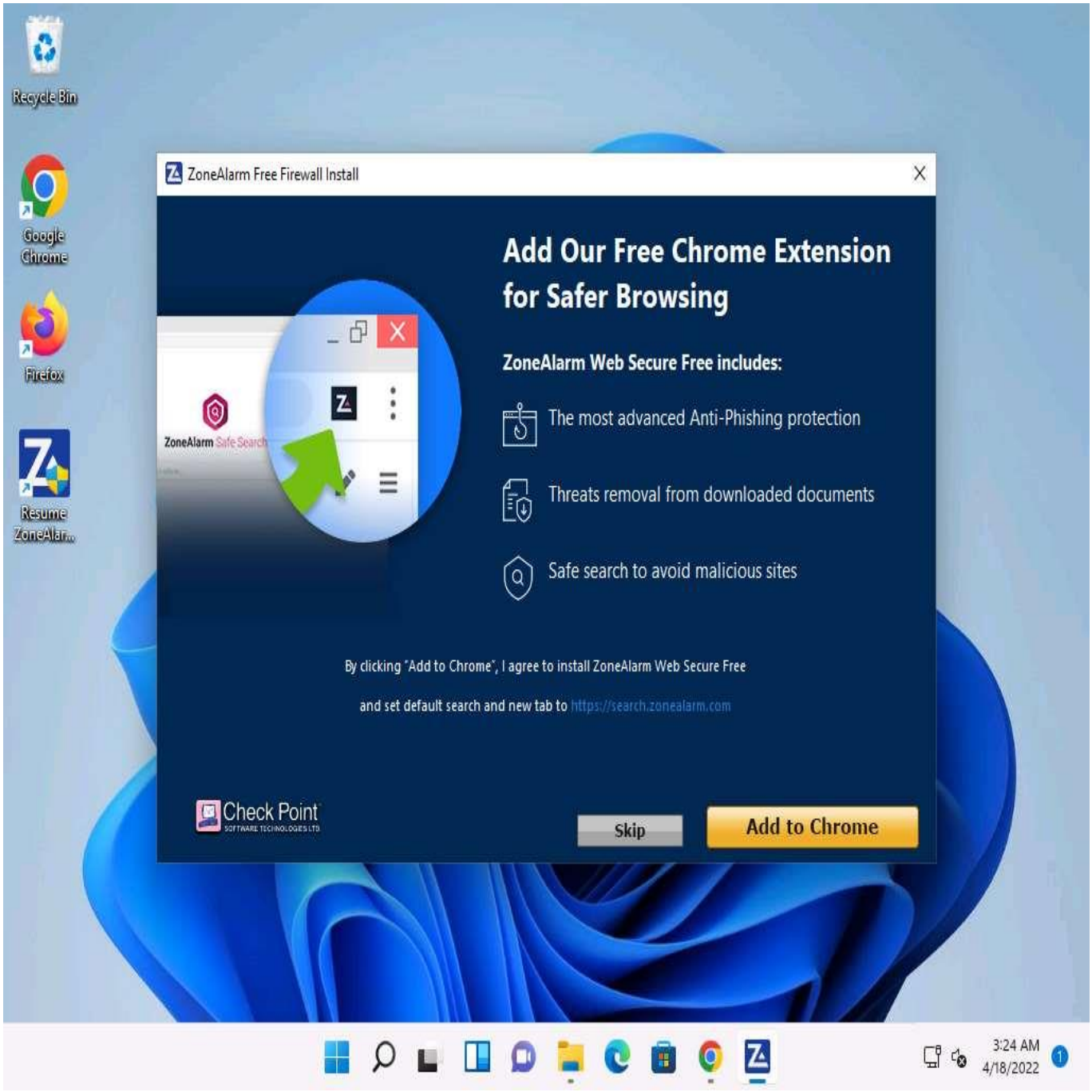


10. ☐ In the **Application Control Mode** wizard, ensure that the **Set Application Control to AUTO-LEARN mode** option is selected, and click **Next >**.
11. ☐ By choosing this mode, Zone Alarm Firewall configures the security settings based on behavior and automates this process for your network.

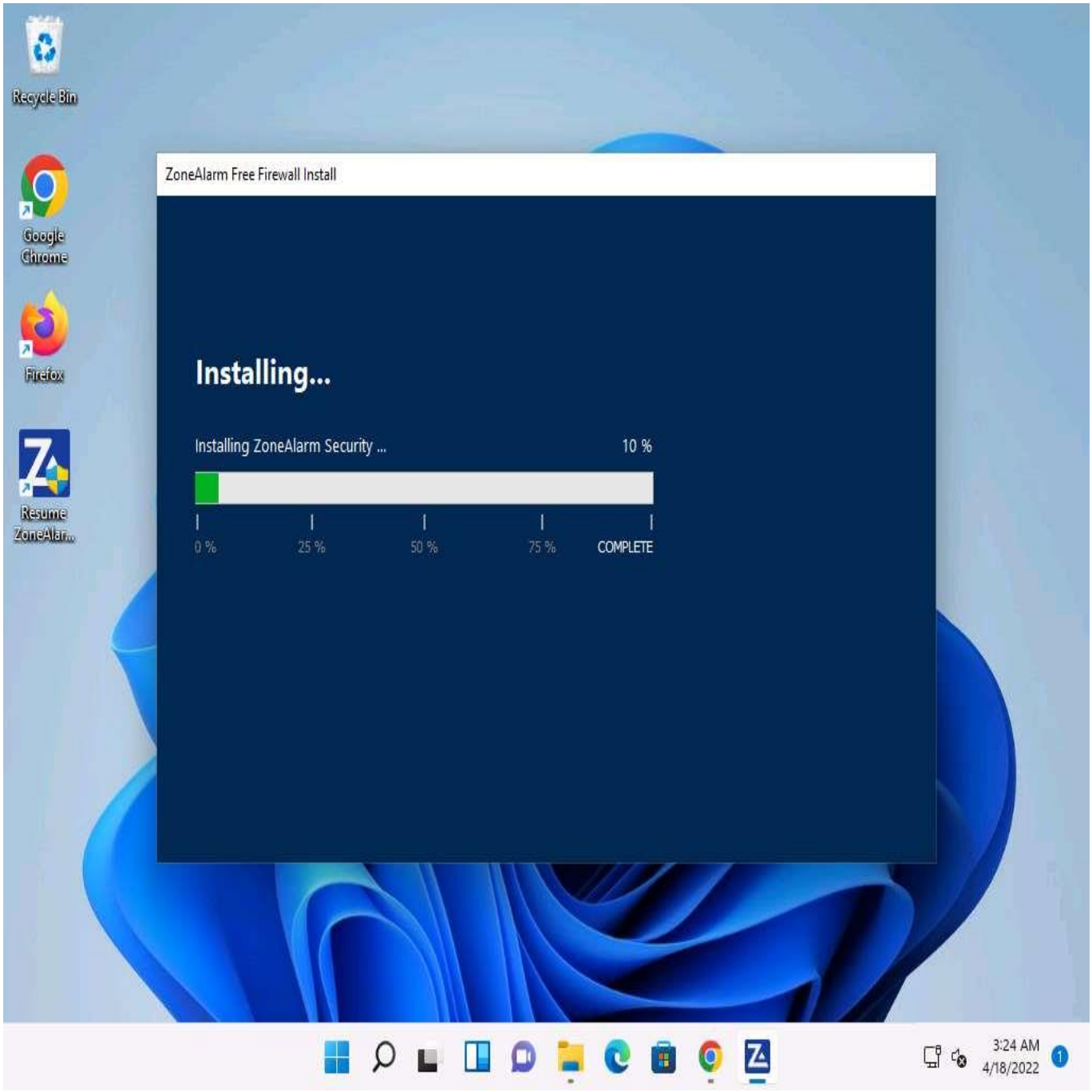


12. ☐ Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

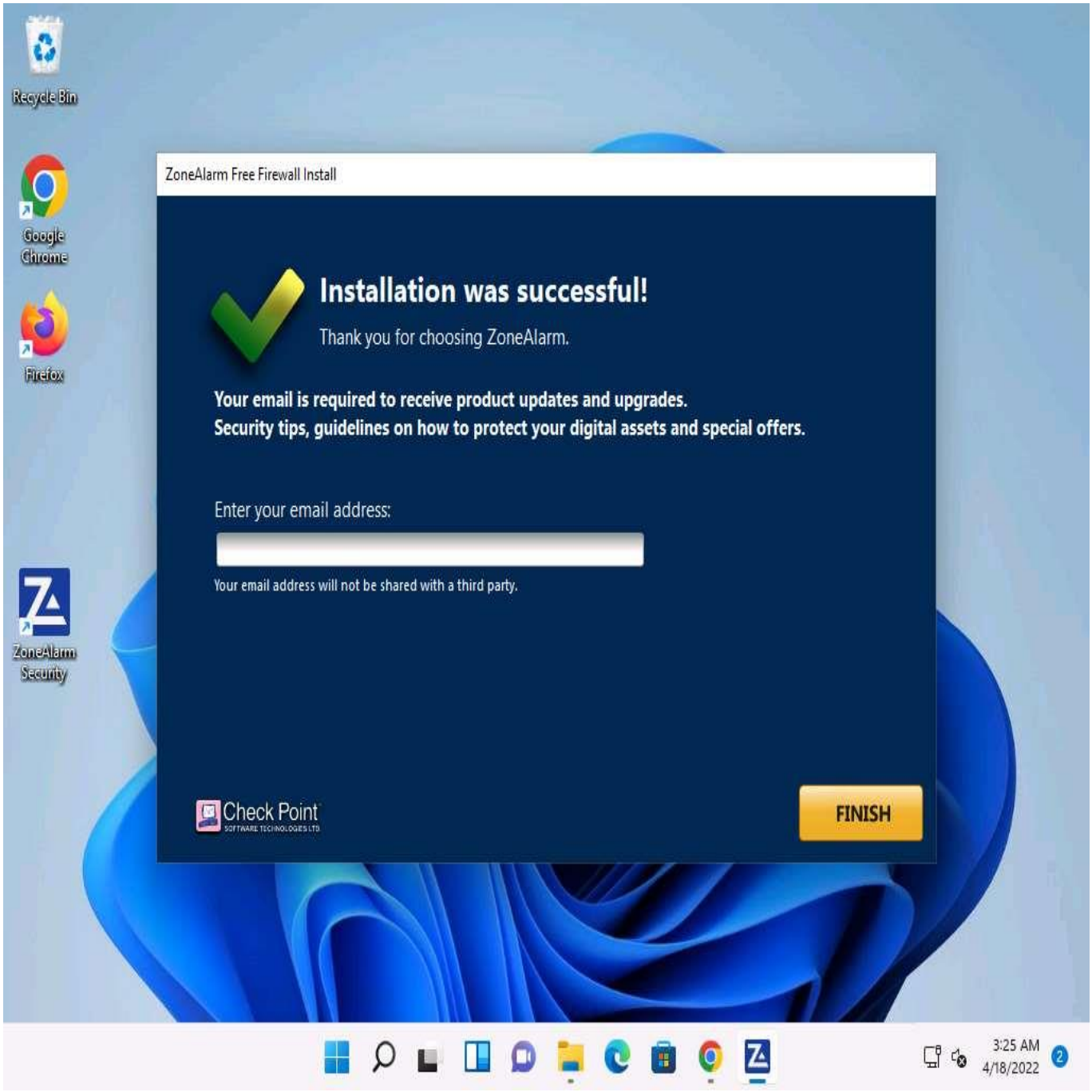
If you wish to enable this option, click Add to Chrome. In this task, we are choosing to skip this option.



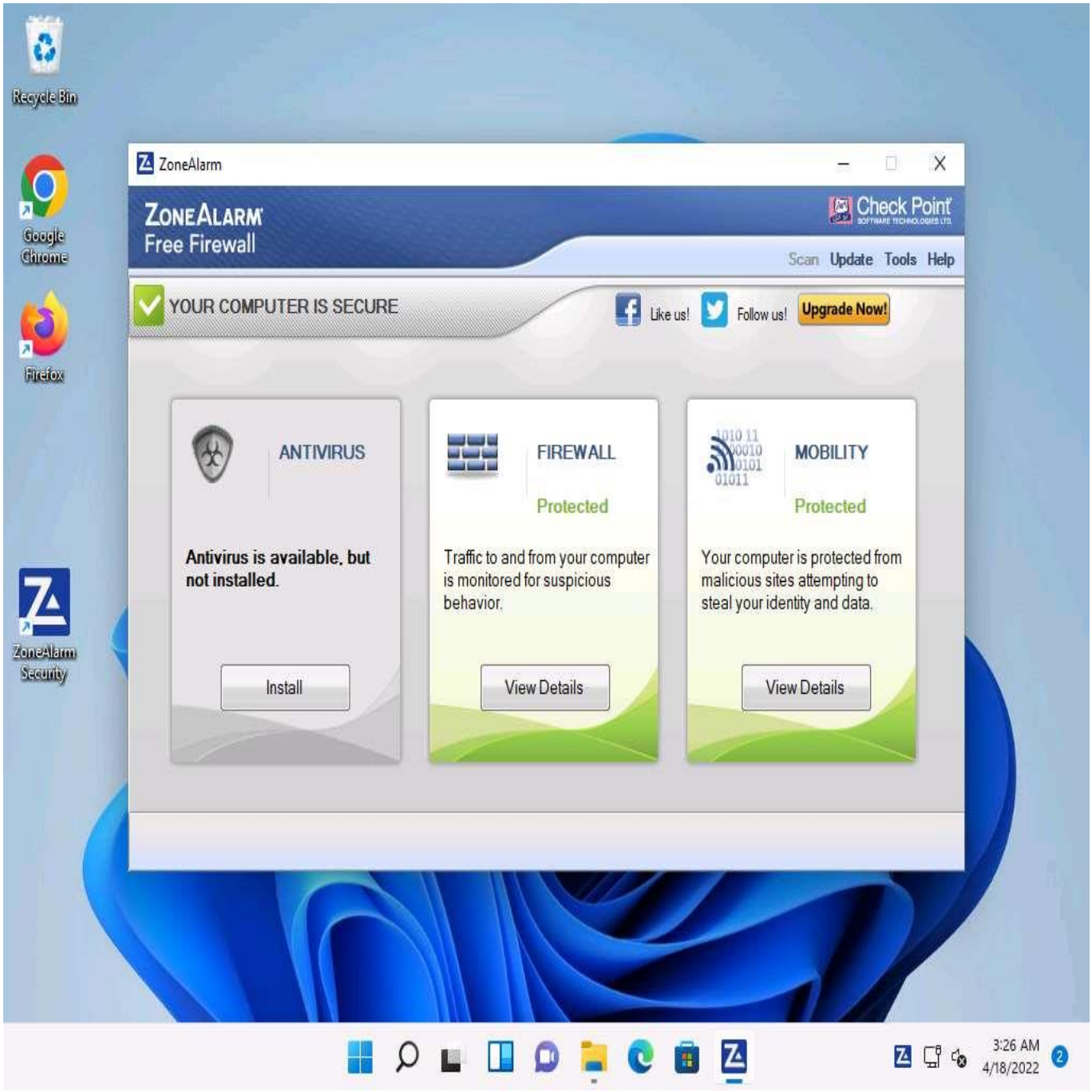
13. ☐ ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.
14. ☐ Wait until the installation is completed: this may take a few minutes to install.



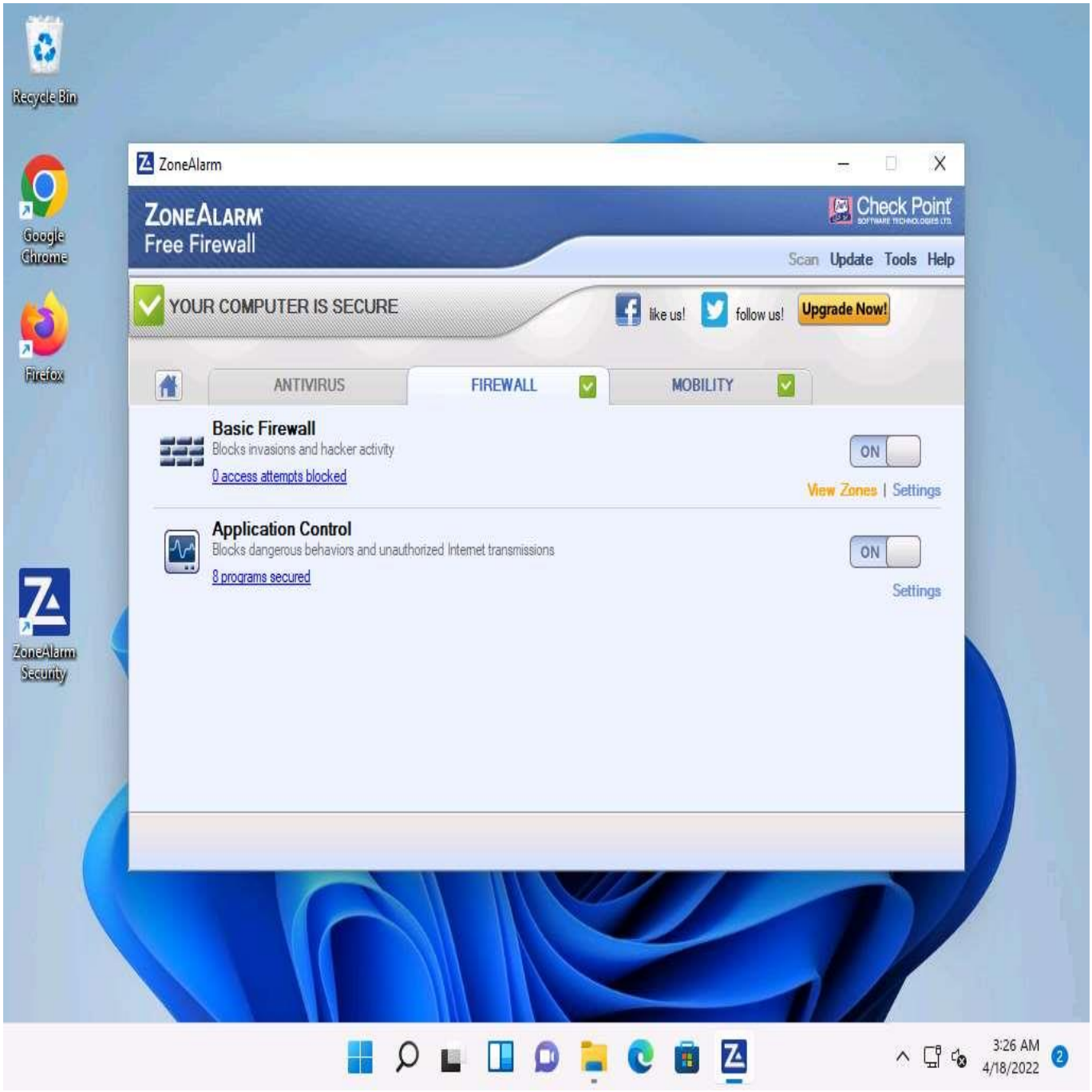
15. ☐ The **Installation was Successful!** wizard appears; click **FINISH**.
16. ☐ As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.



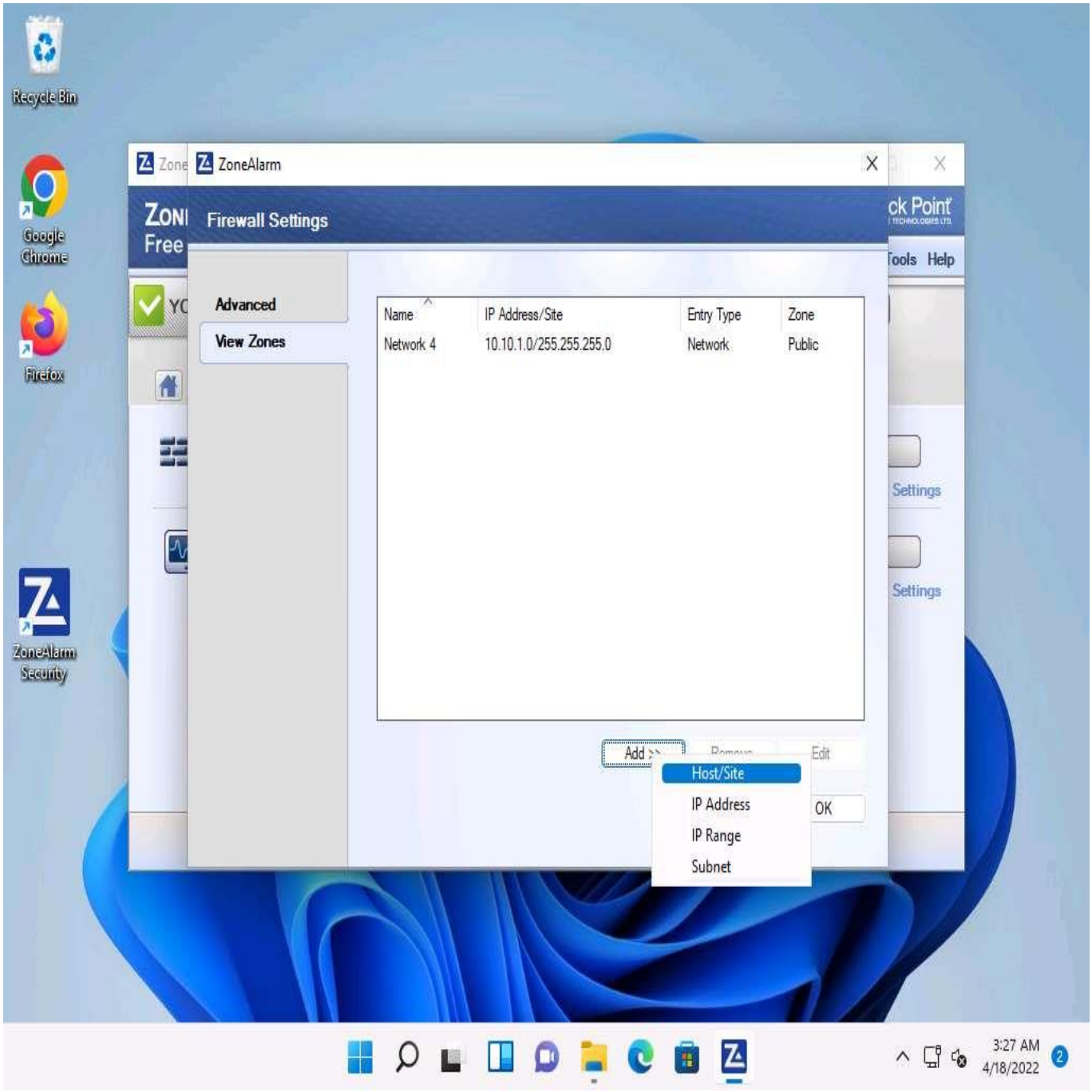
17. ☐ The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.



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

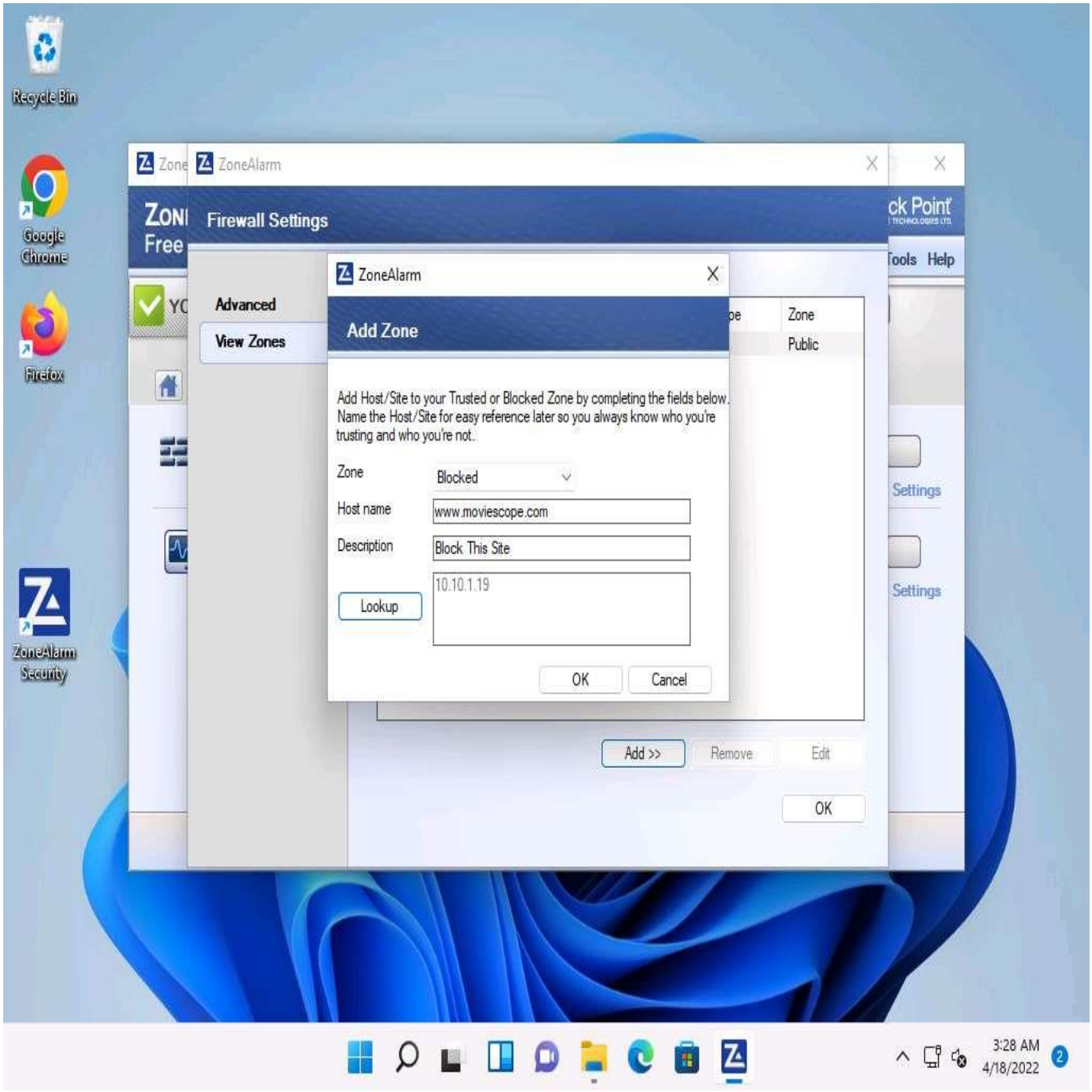


19. ☐ The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.

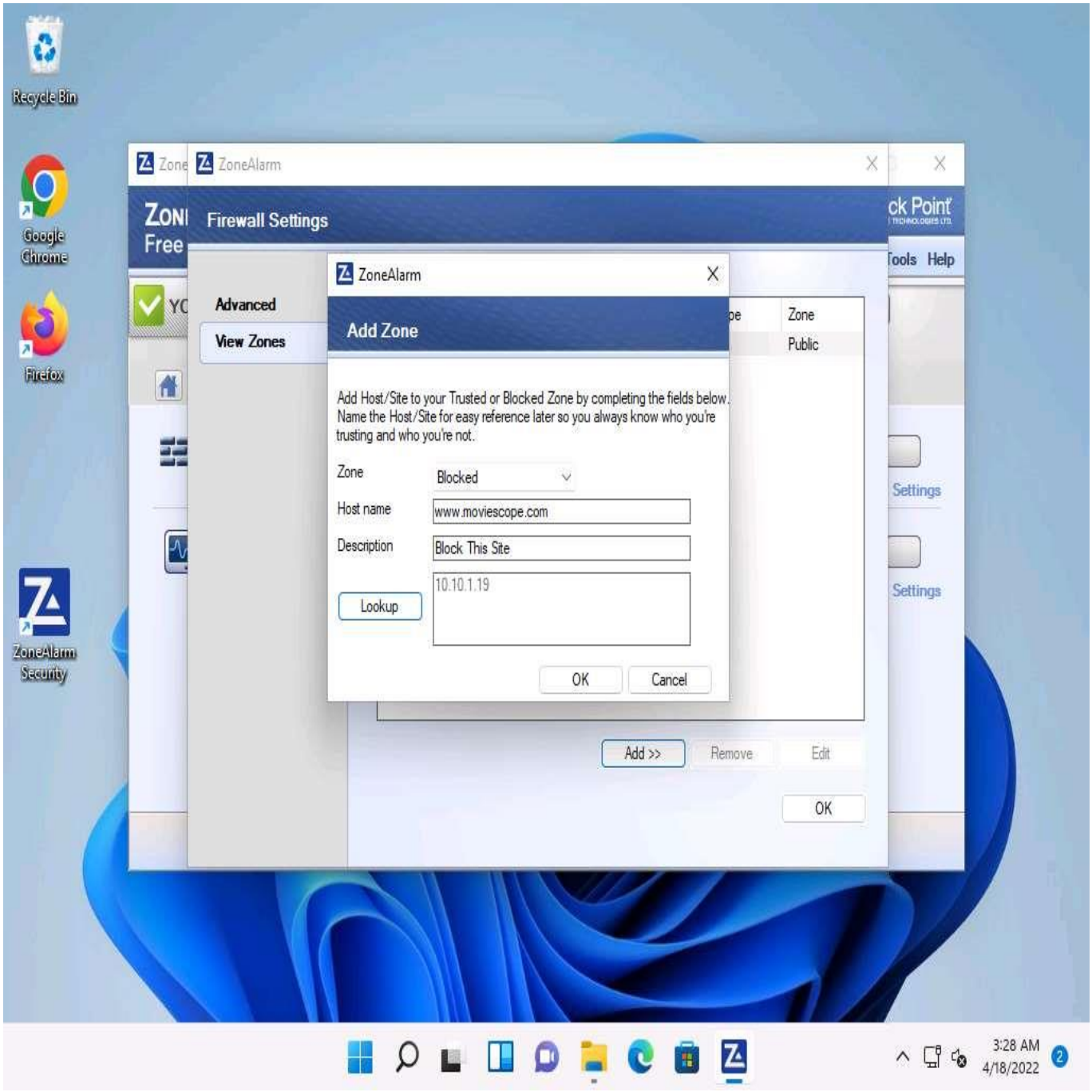


20. ☐ The **Add Zone** window appears; choose the following:
    - Zone: **Blocked**
    - Hostname: **www.moviescope.com**
    - Description: **Block This Site**
    - Click **Lookup**; by doing this, we are blocking unwanted sites from browsing
21. ☐ You can provide any site that you wish to block.

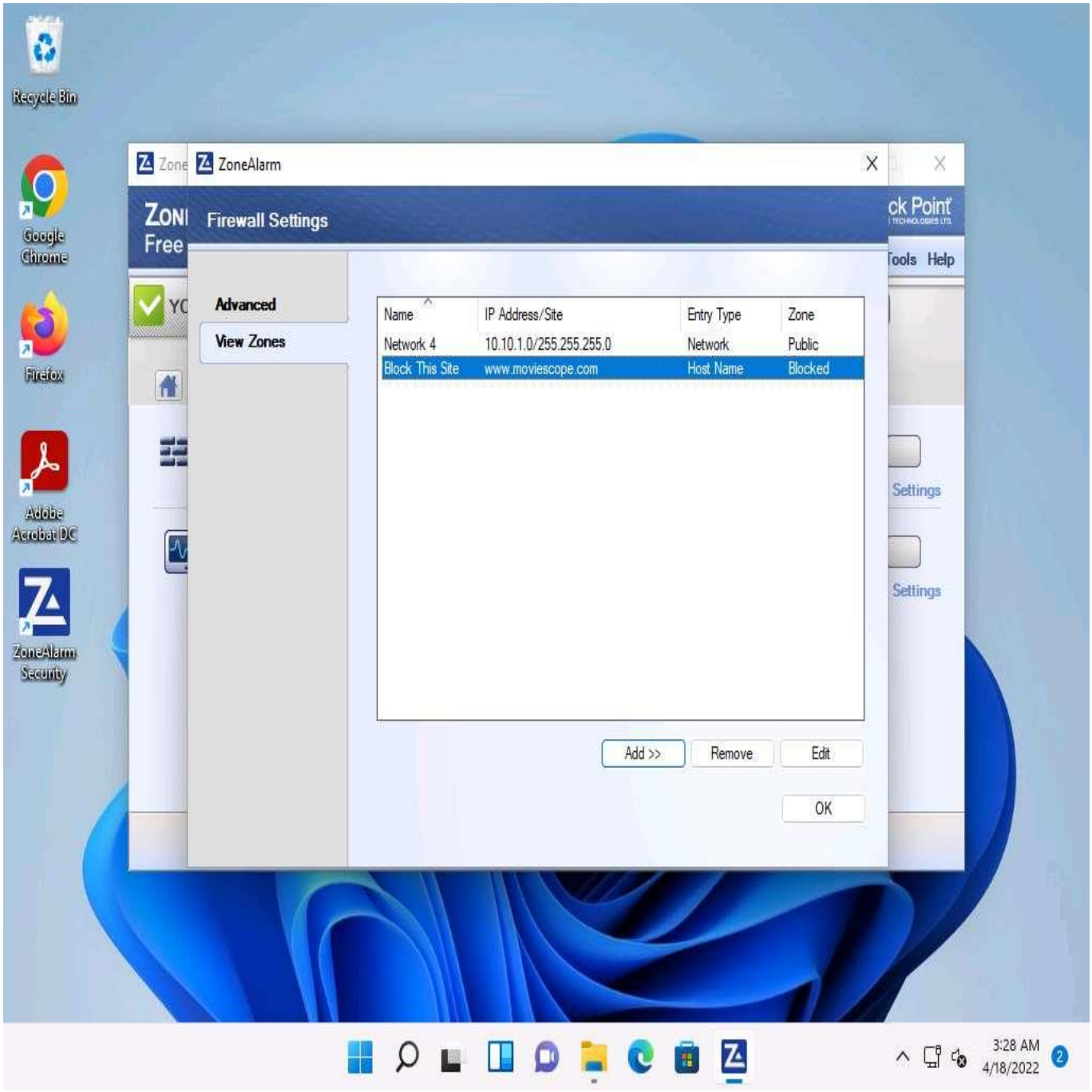
www.moviescope.com is the local website that is configured on Windows Server 2019.



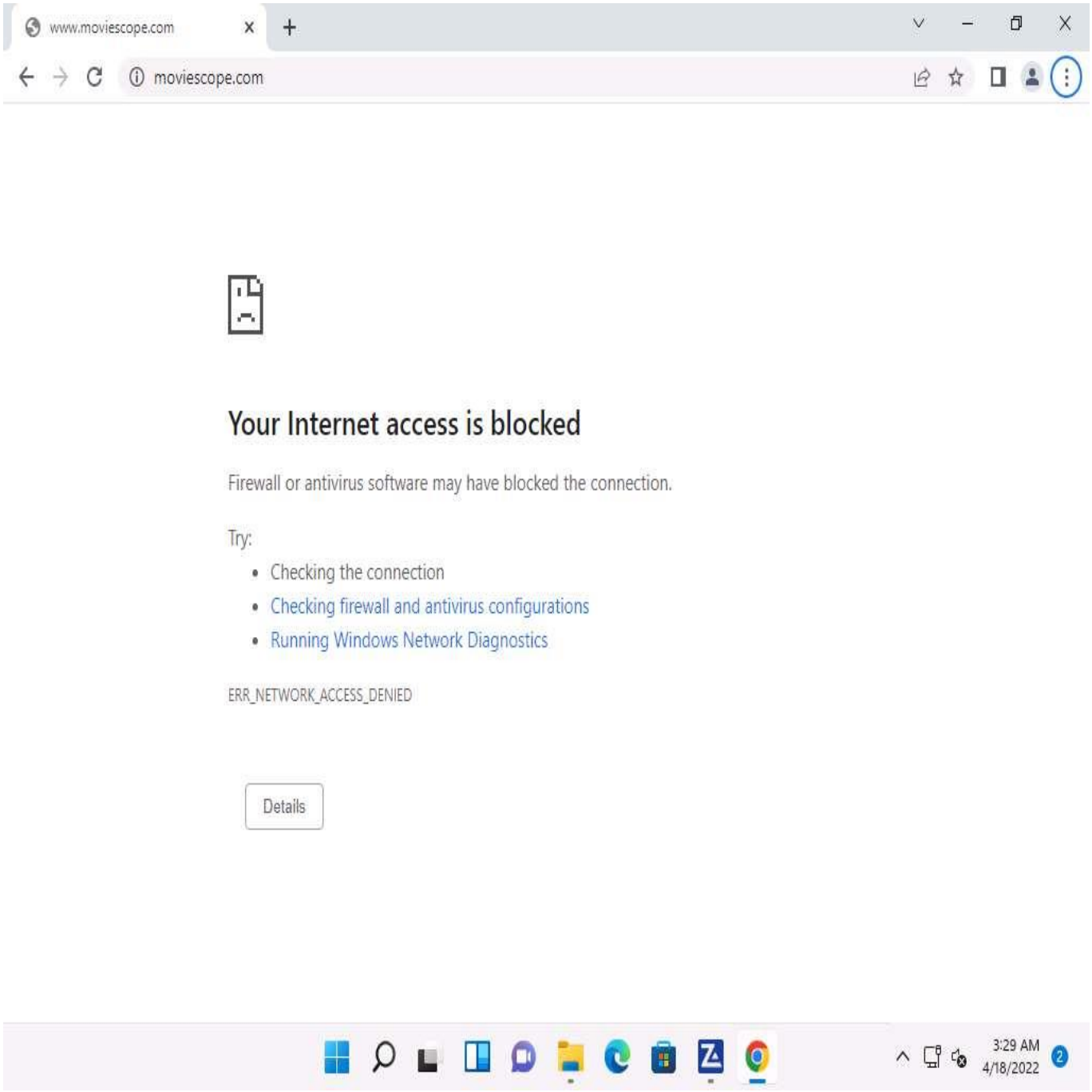
22. ☐ As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.



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**.

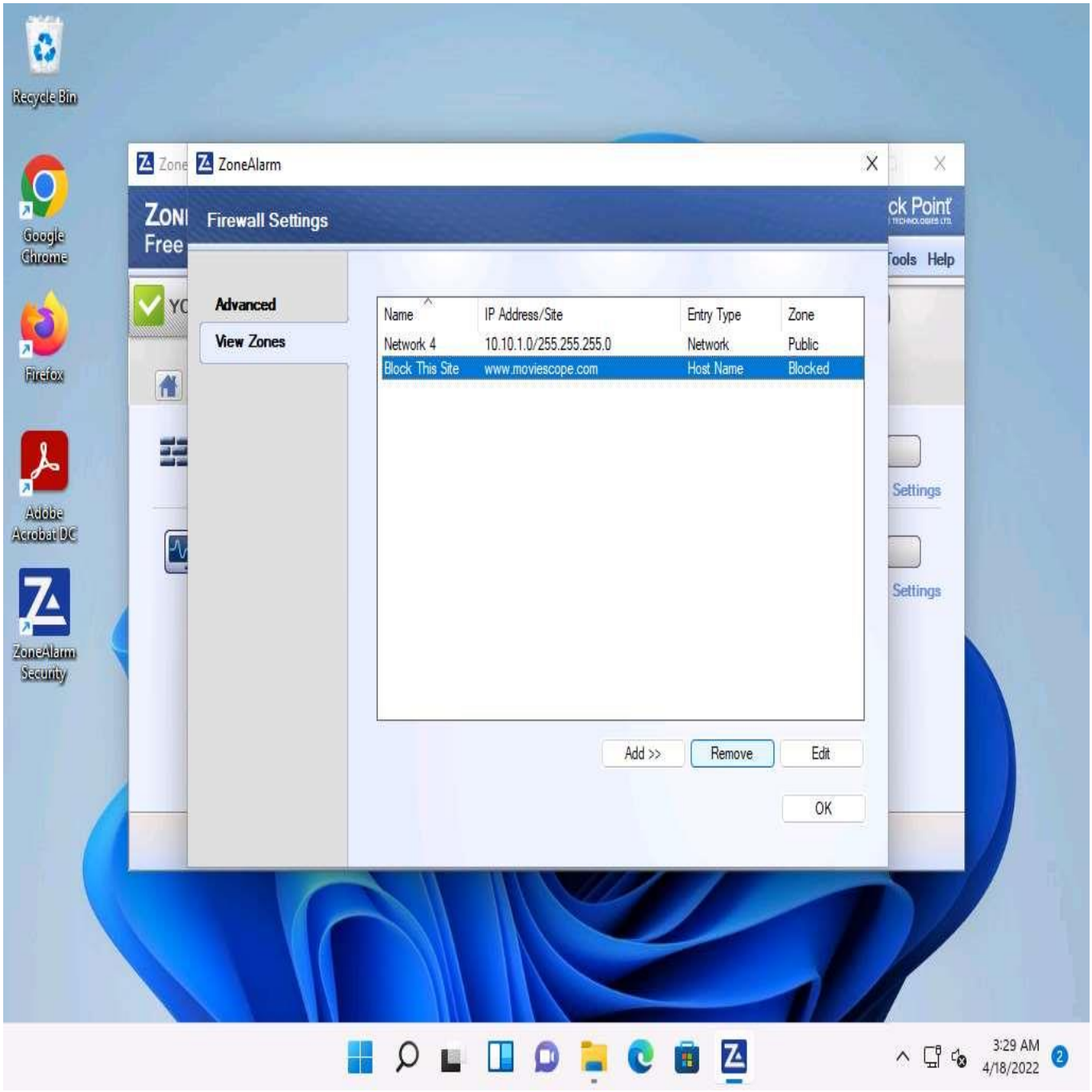


This is how you can block access for unwanted sites from browsing.

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**.

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

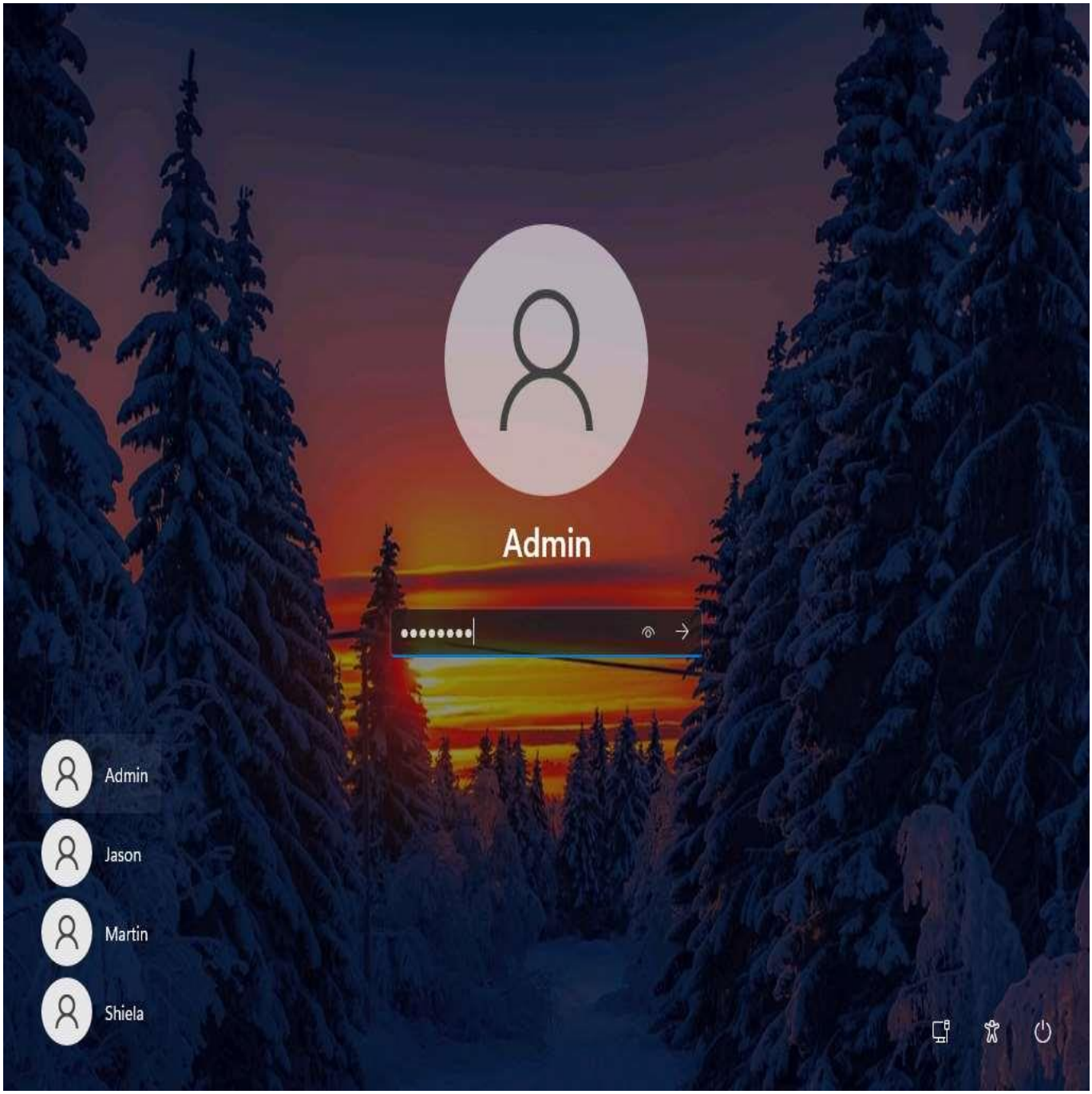
27. ☐ This will remove the block access for the **www.moviescope.com** site.



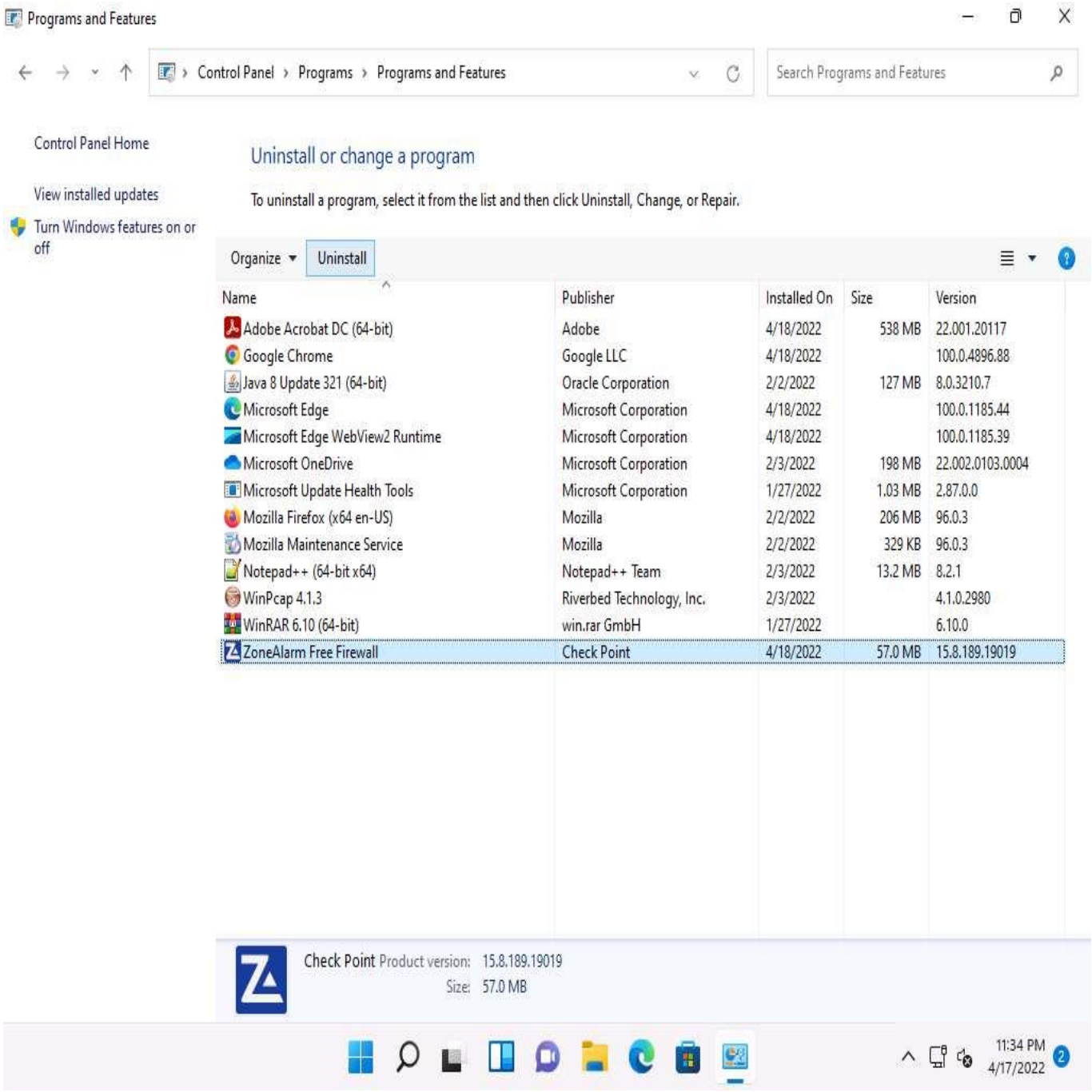
28. ☐ Close the ZoneAlarm main window.
29. ☐ Click **Show hidden icon** from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.

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

30. ☐ Restart the **Windows 11** machine.
31. ☐ After the system reboots, click Ctrl+Alt+Delete. By default, **Admin** user account is selected, click Pa$$w0rd to enter the password 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.

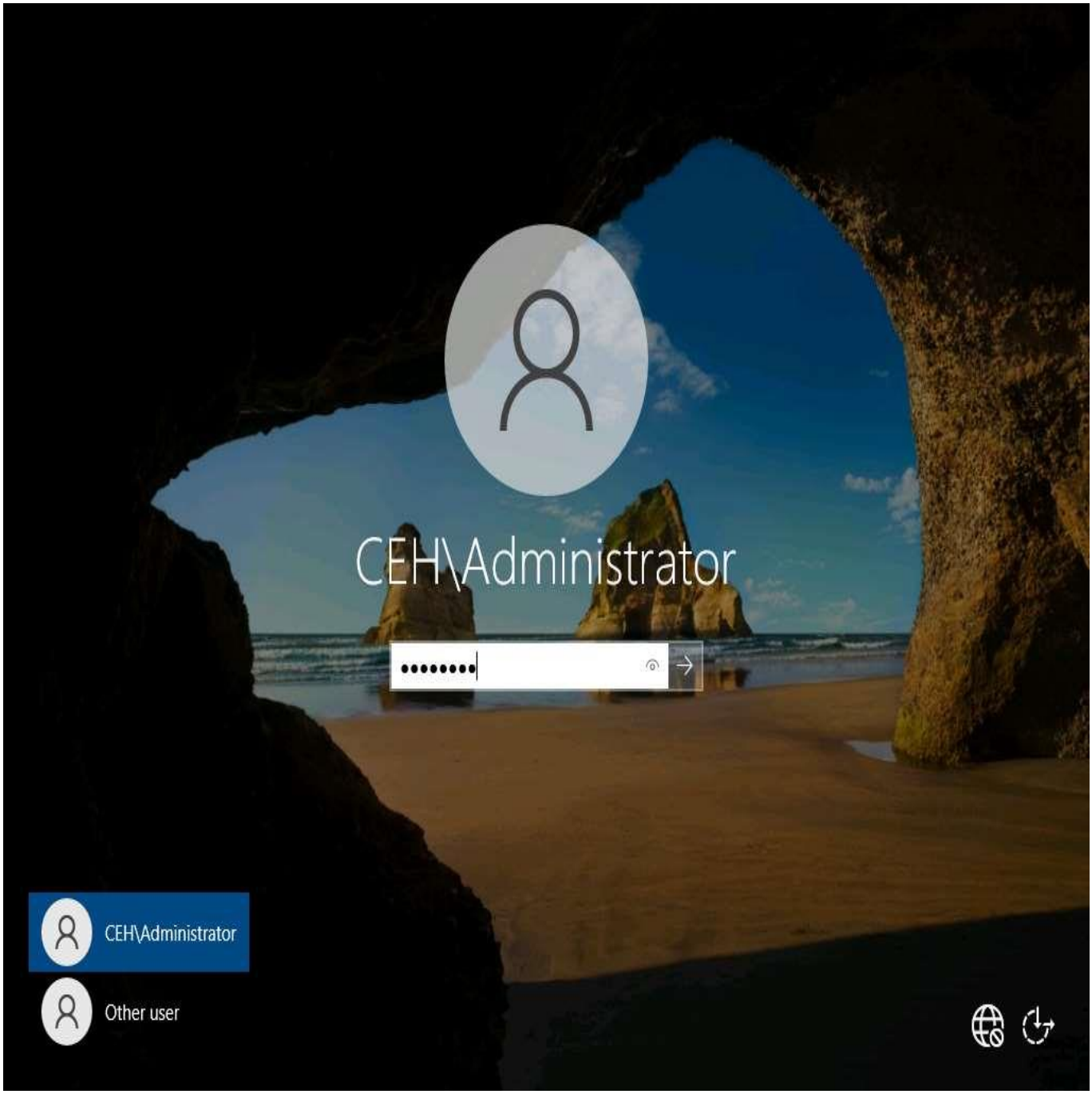
Task 3: Detect Malicious Network Traffic using HoneyBOT

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.

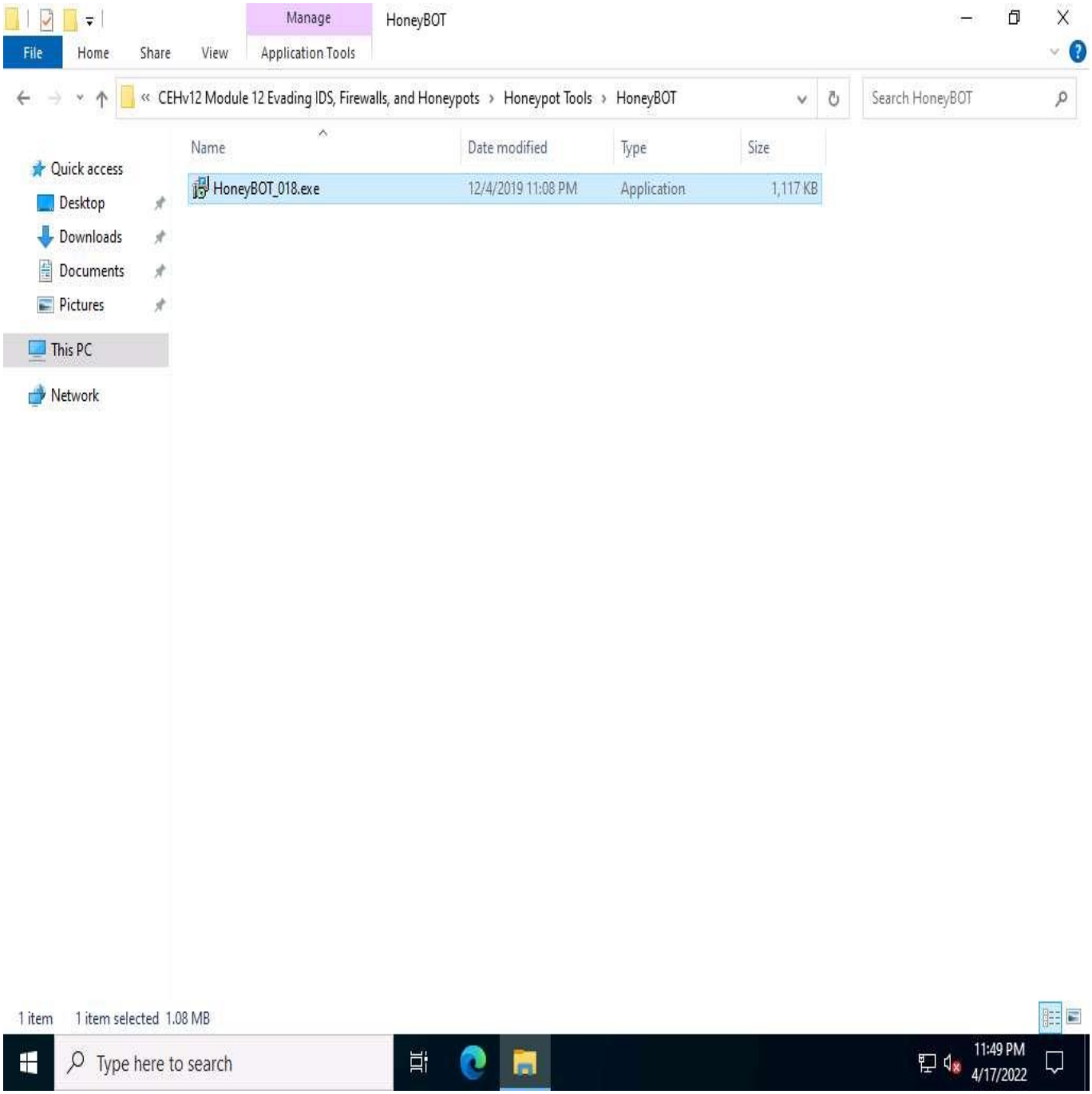
1. Click Windows Server 2022 to switch to the **Windows Server 2022** machine. Click Ctrl+Alt+Delete to activate the machine. By default, **CEH\Administrator** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

   Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2022** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

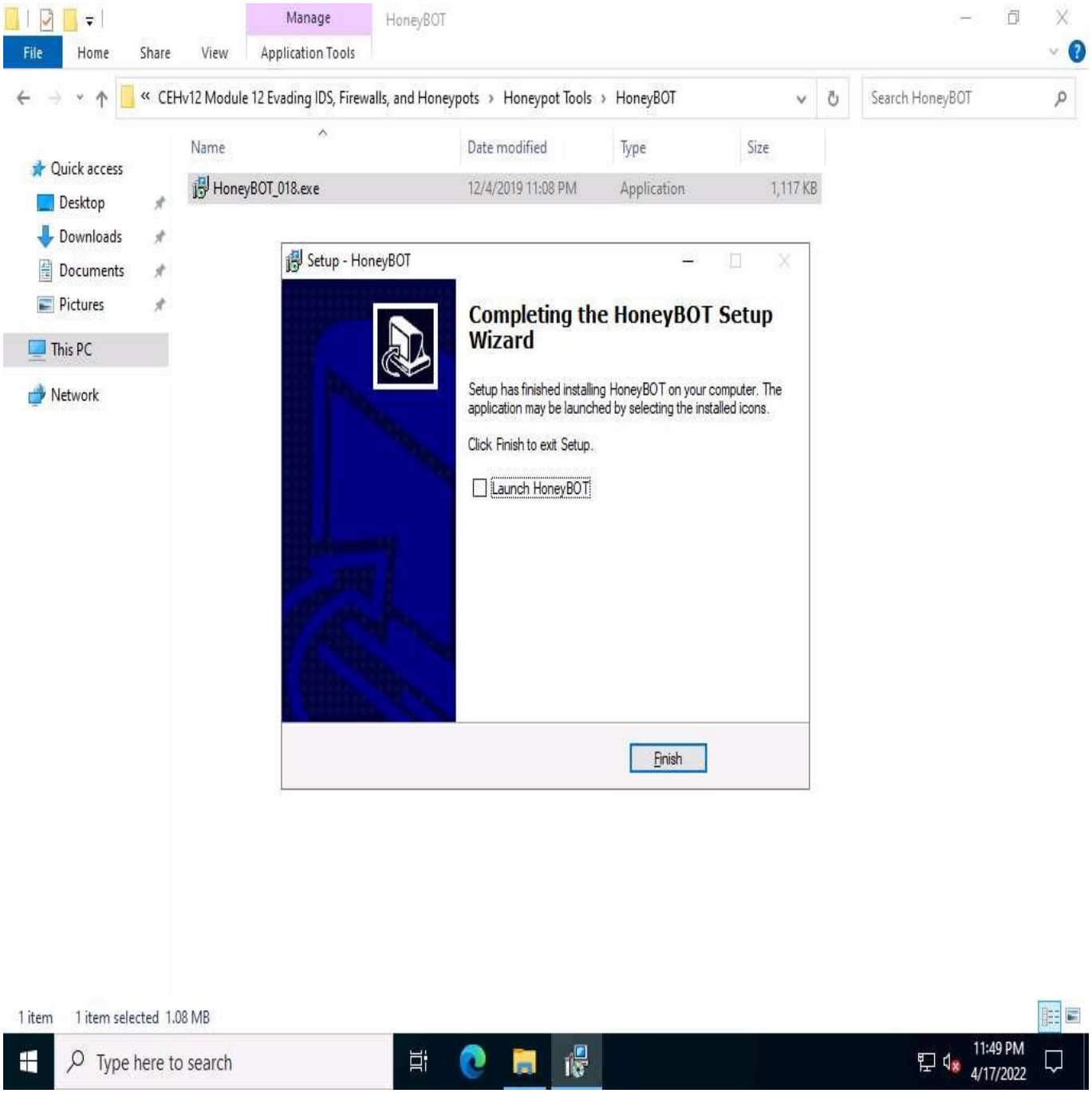


2. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

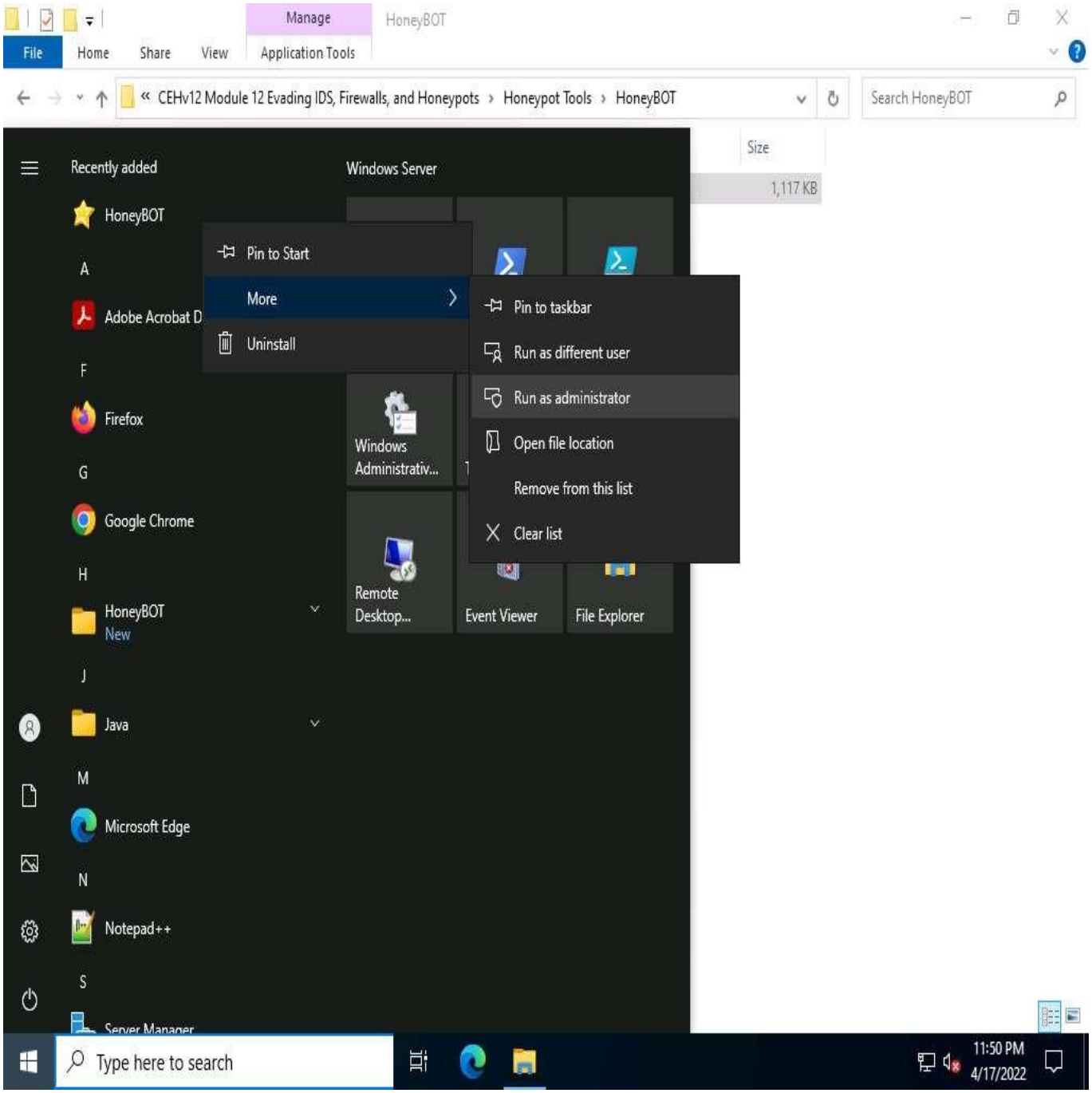
if the **User Account Control** window appears, click **Yes**.



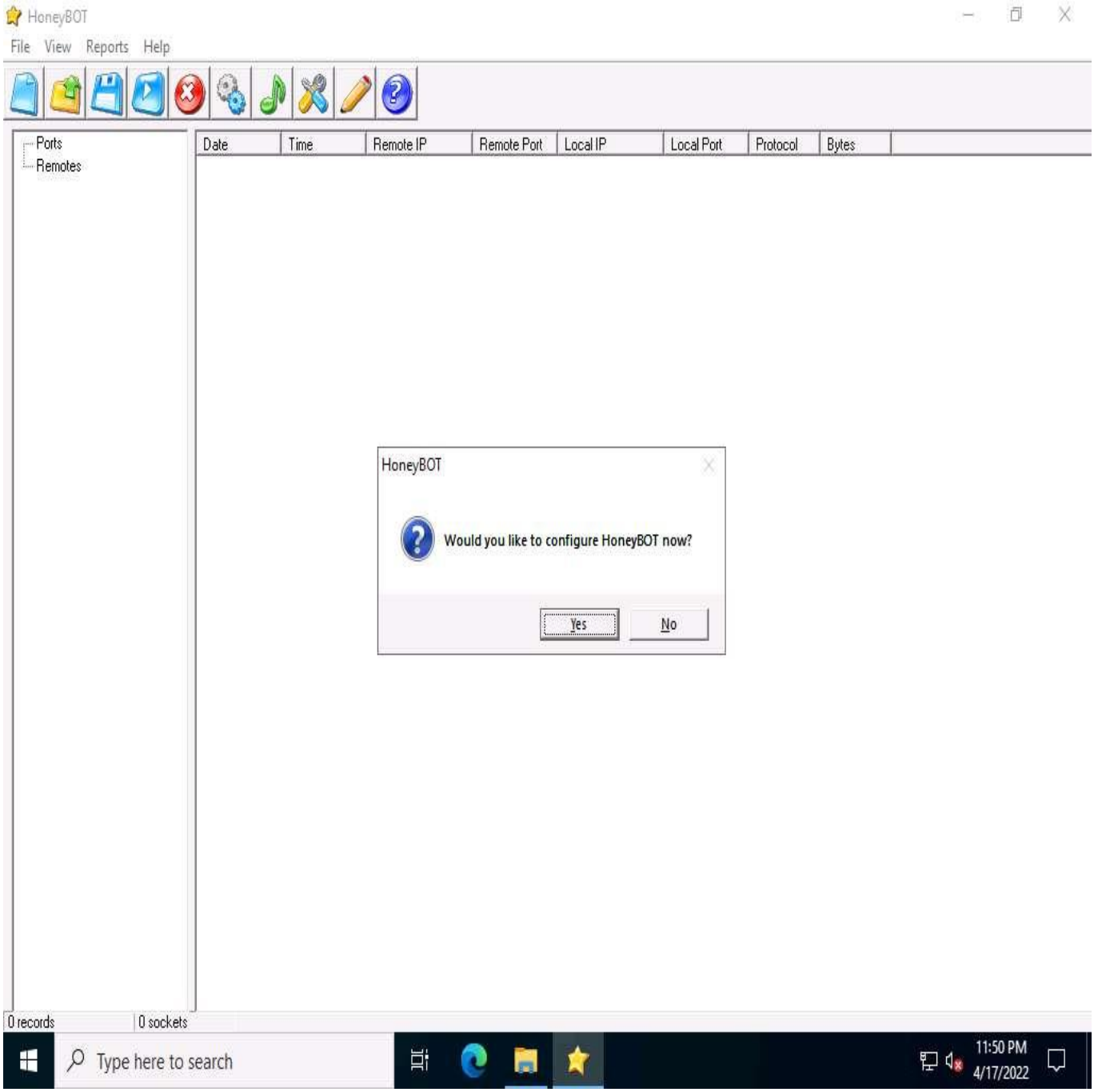
3. ☐ Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.



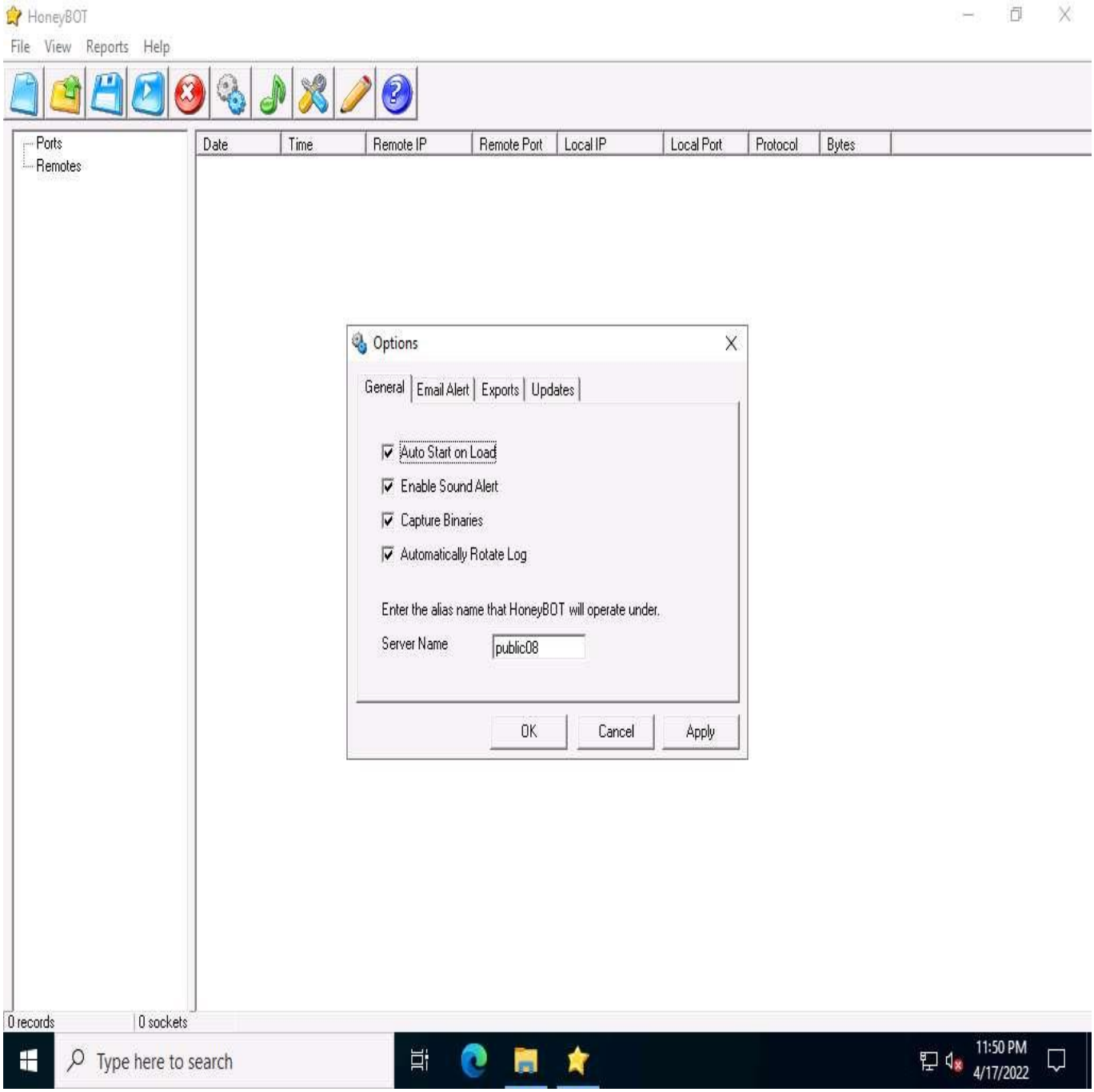
4. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT** --> **More** --> **Run as administrator**, as shown in the screenshot.



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

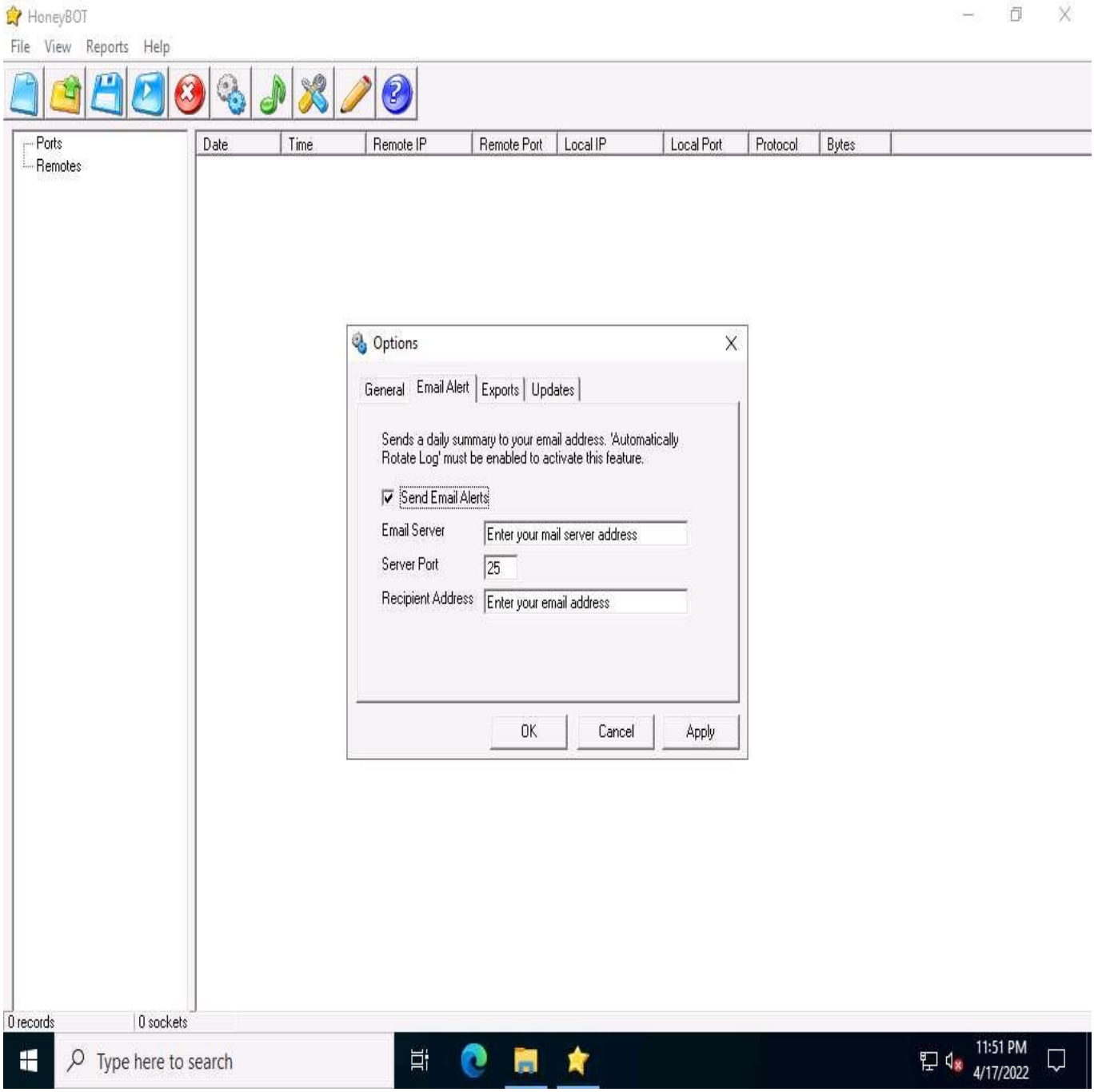


6. ☐ The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.
7. ☐ In this task, we are leaving the settings on default for the **General** tab in the **Options** window.

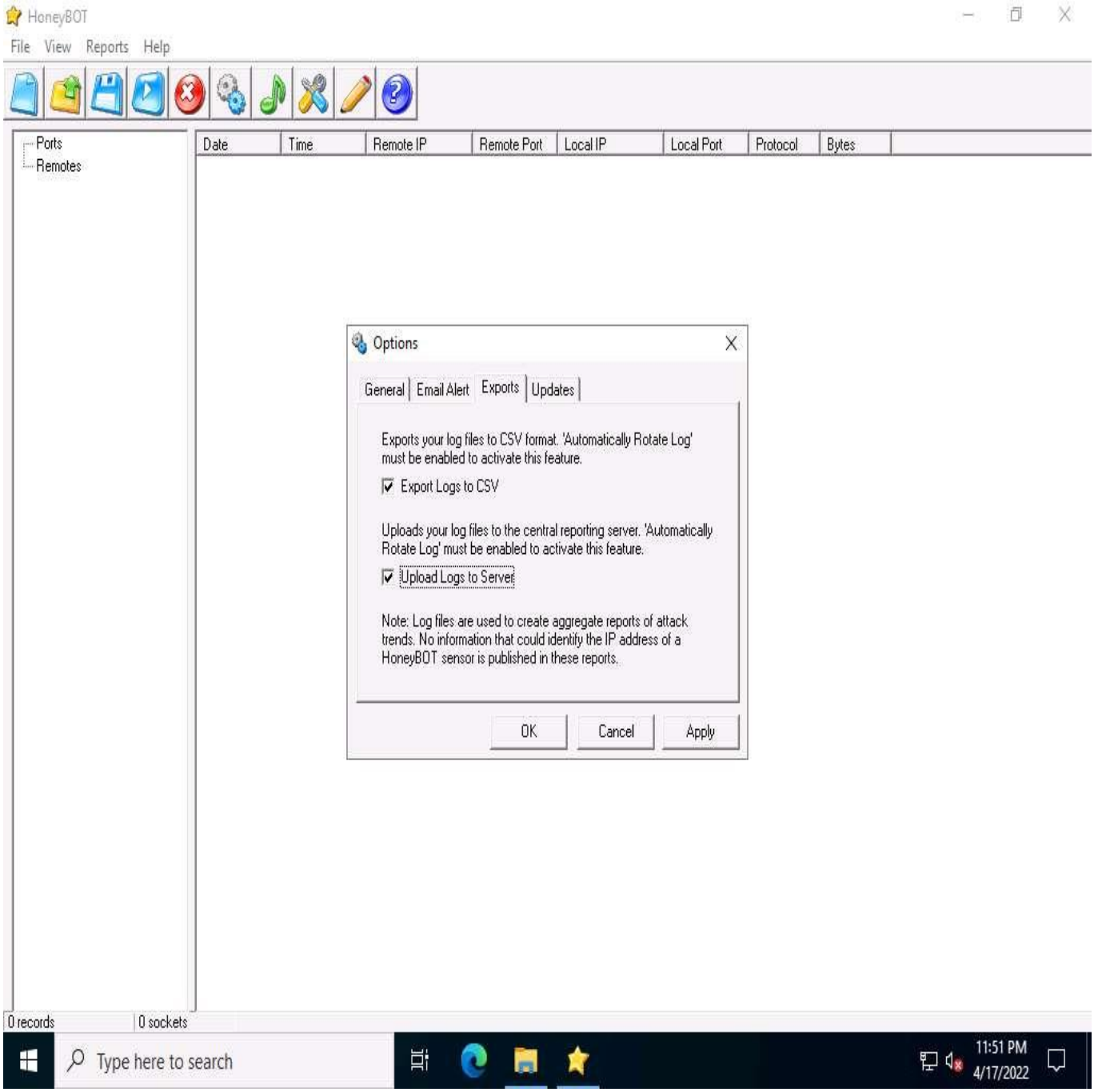


8. ☐ Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

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

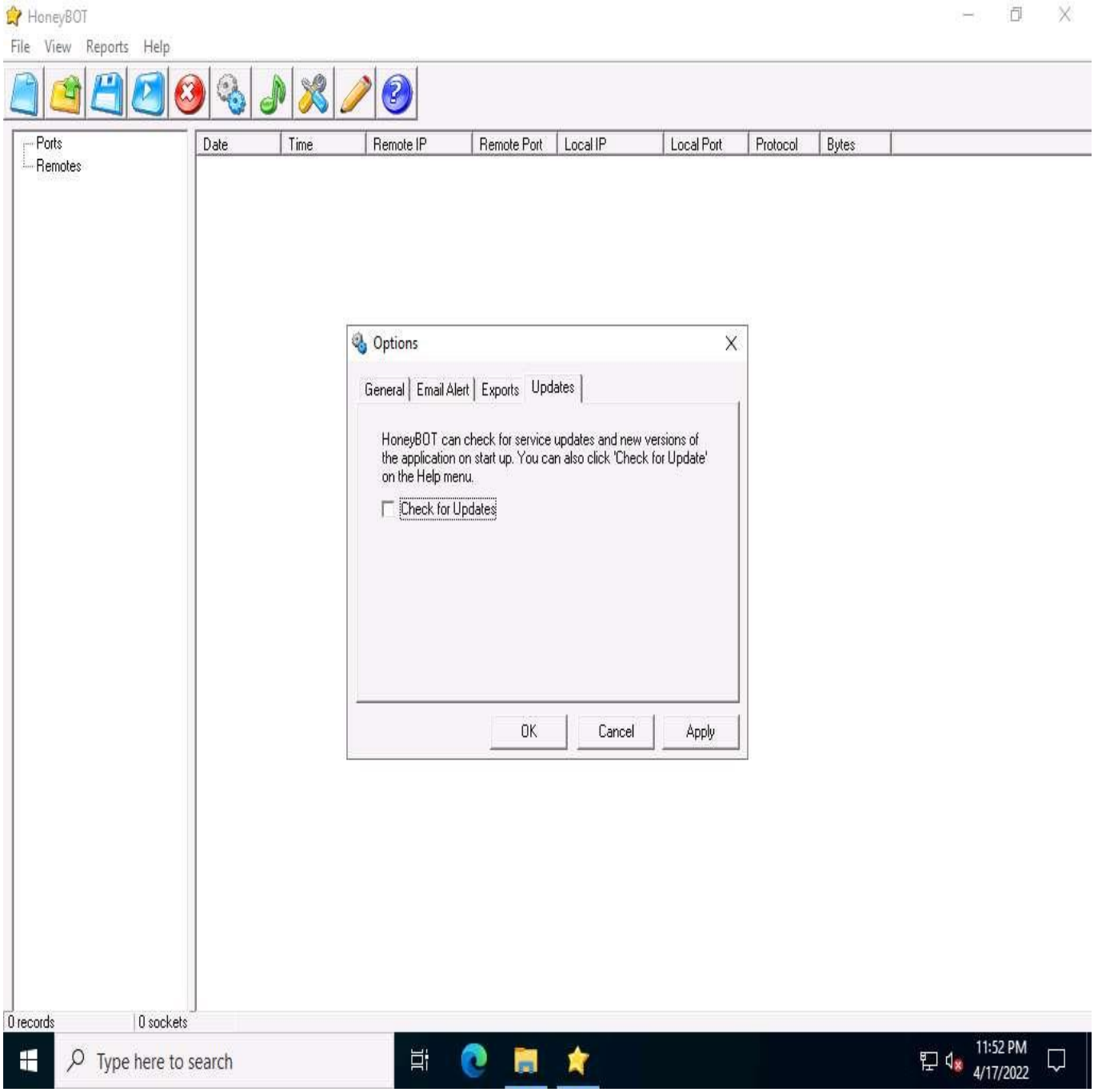


9. ☐ On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (here, **Export Logs to CSV** and **Upload Logs to Server** checkbox are selected)

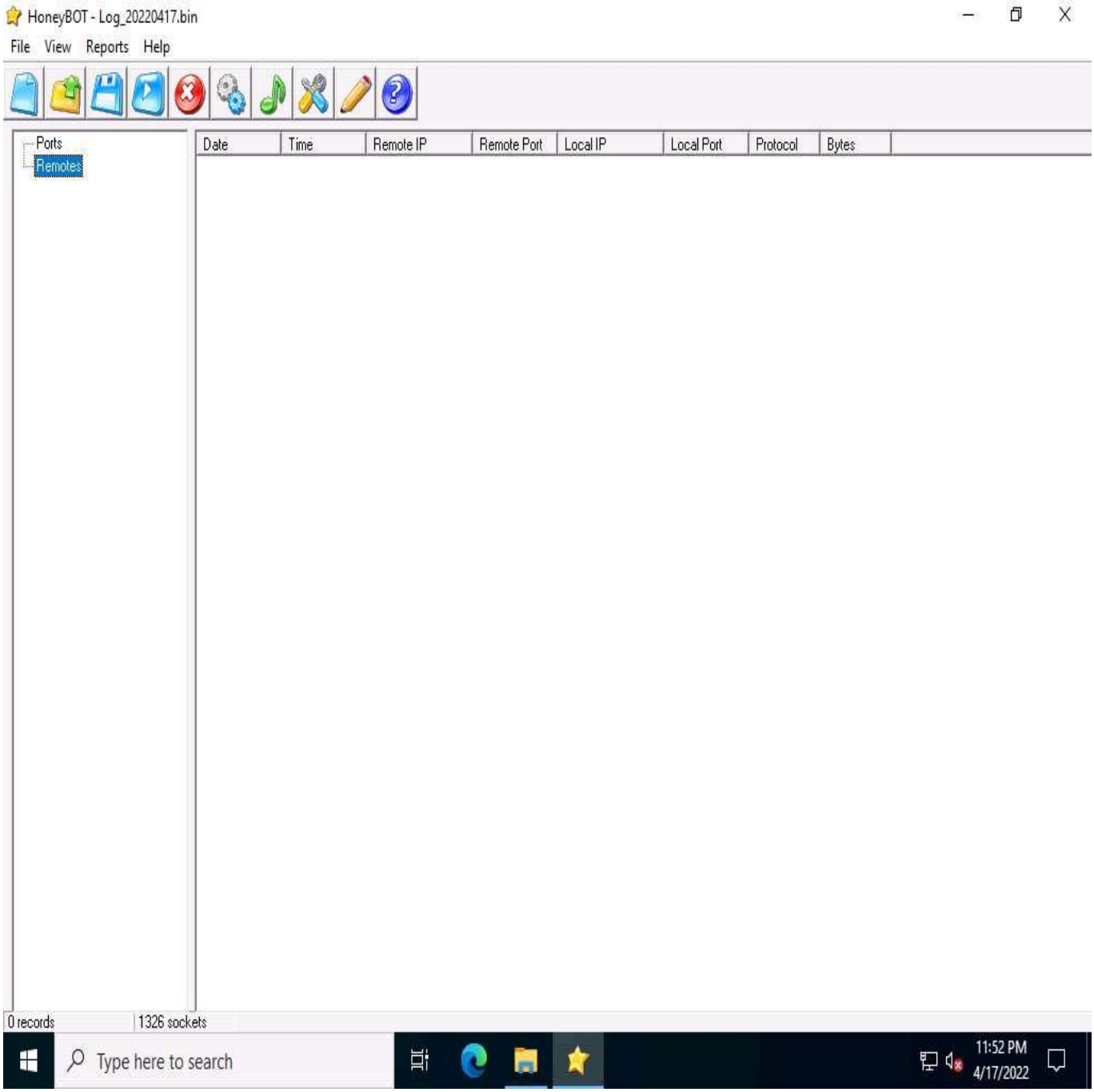


10. ☐ On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

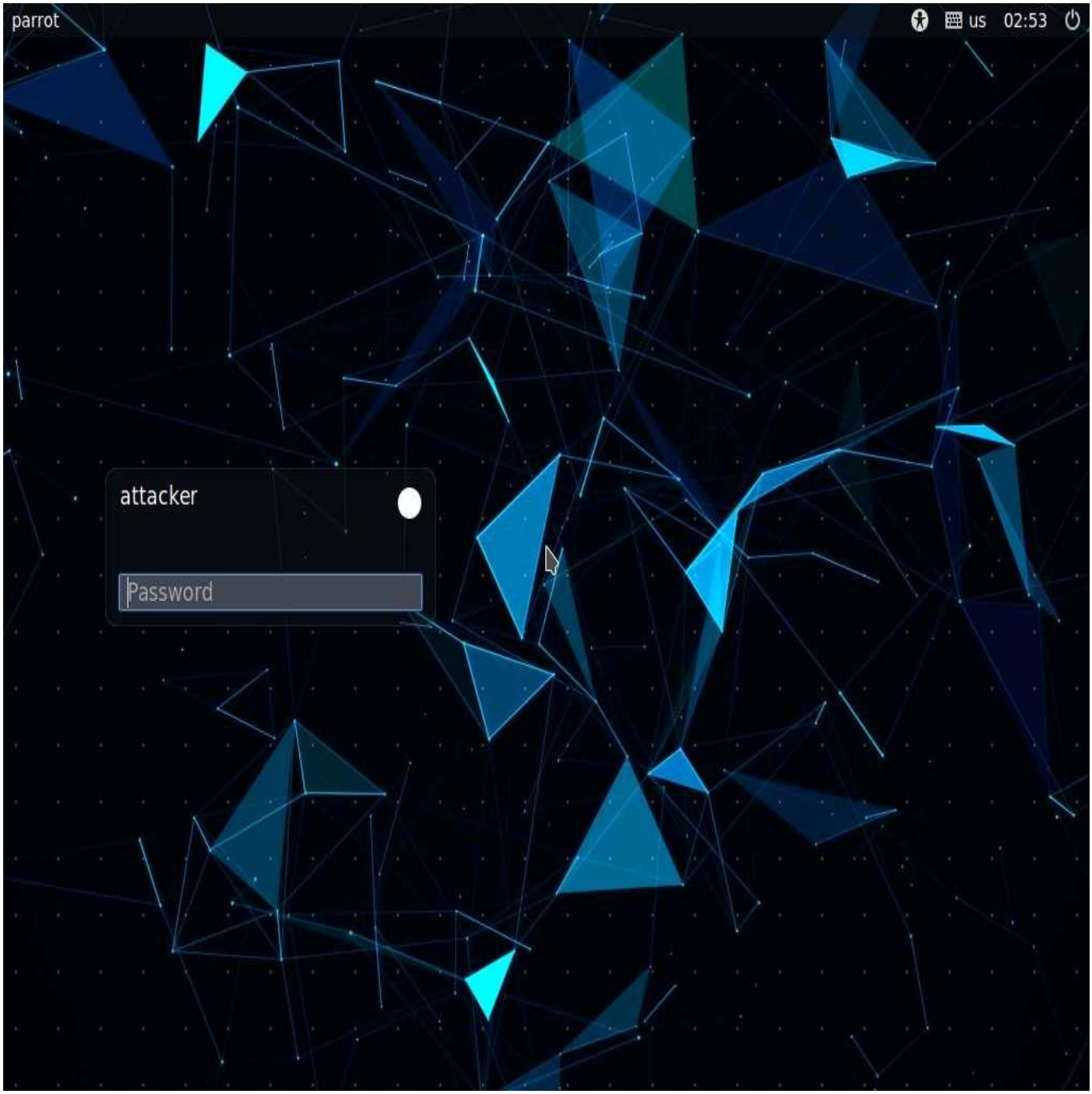
If a **Bindings** pop-up appears, click **OK** to continue.



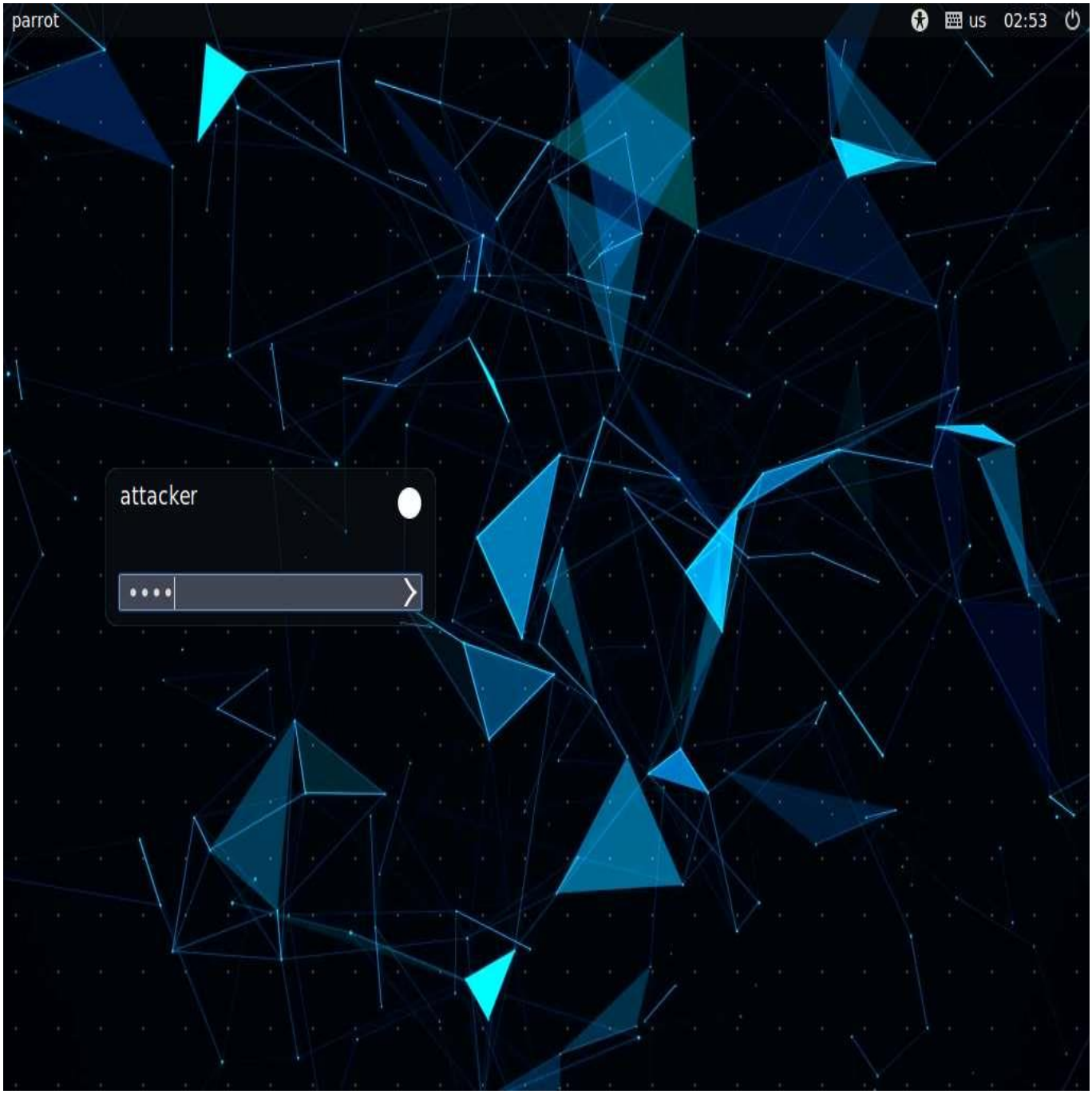
11. ☐ The **HoneyBOT** main window appears, as shown in the screenshot.



12. ☐ Now, leave the HoneyBOT window running on **Windows Server 2022**.
13. ☐ Click Parrot Security to switch to the **Parrot Security** machine.

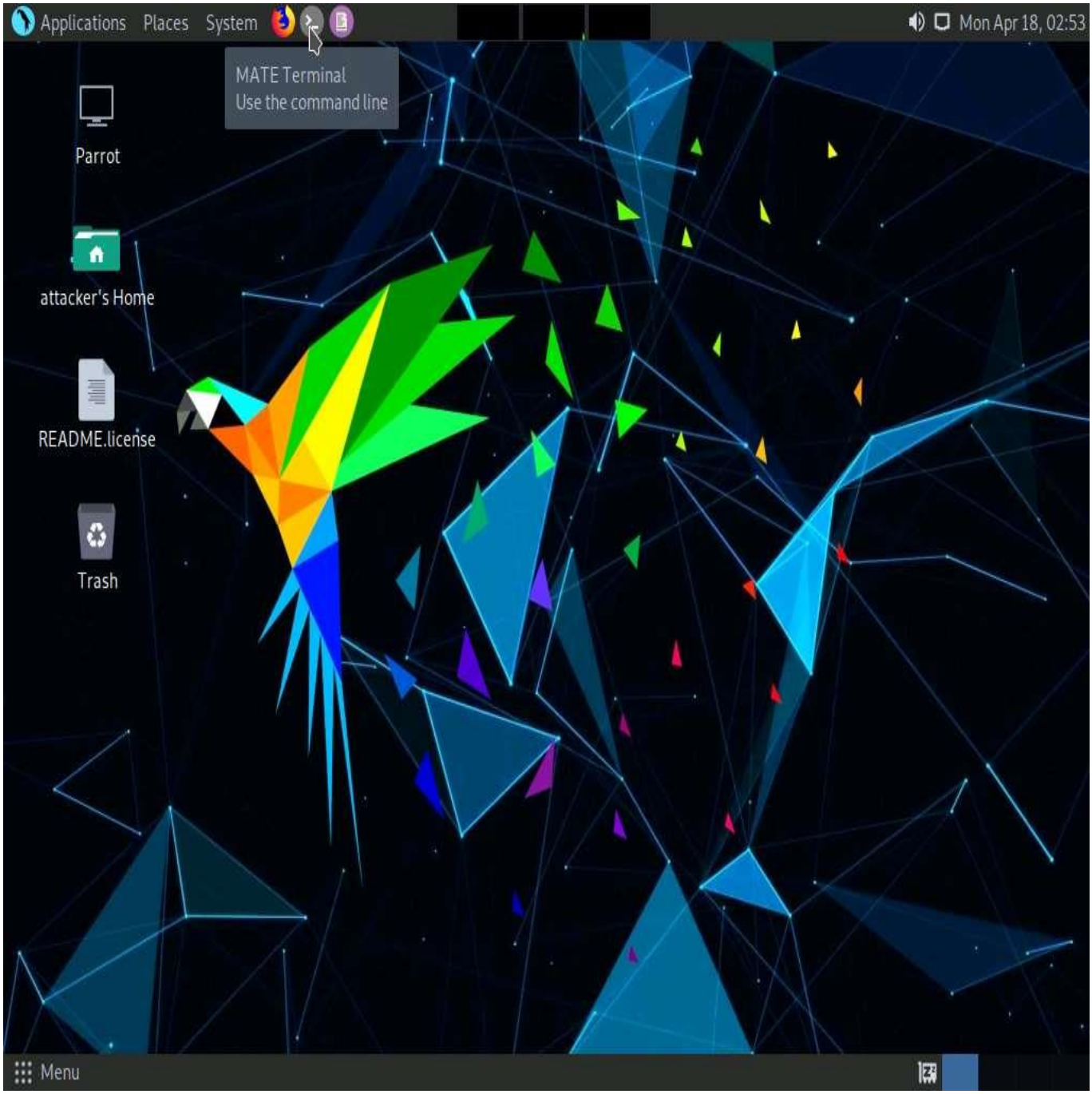


14. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



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

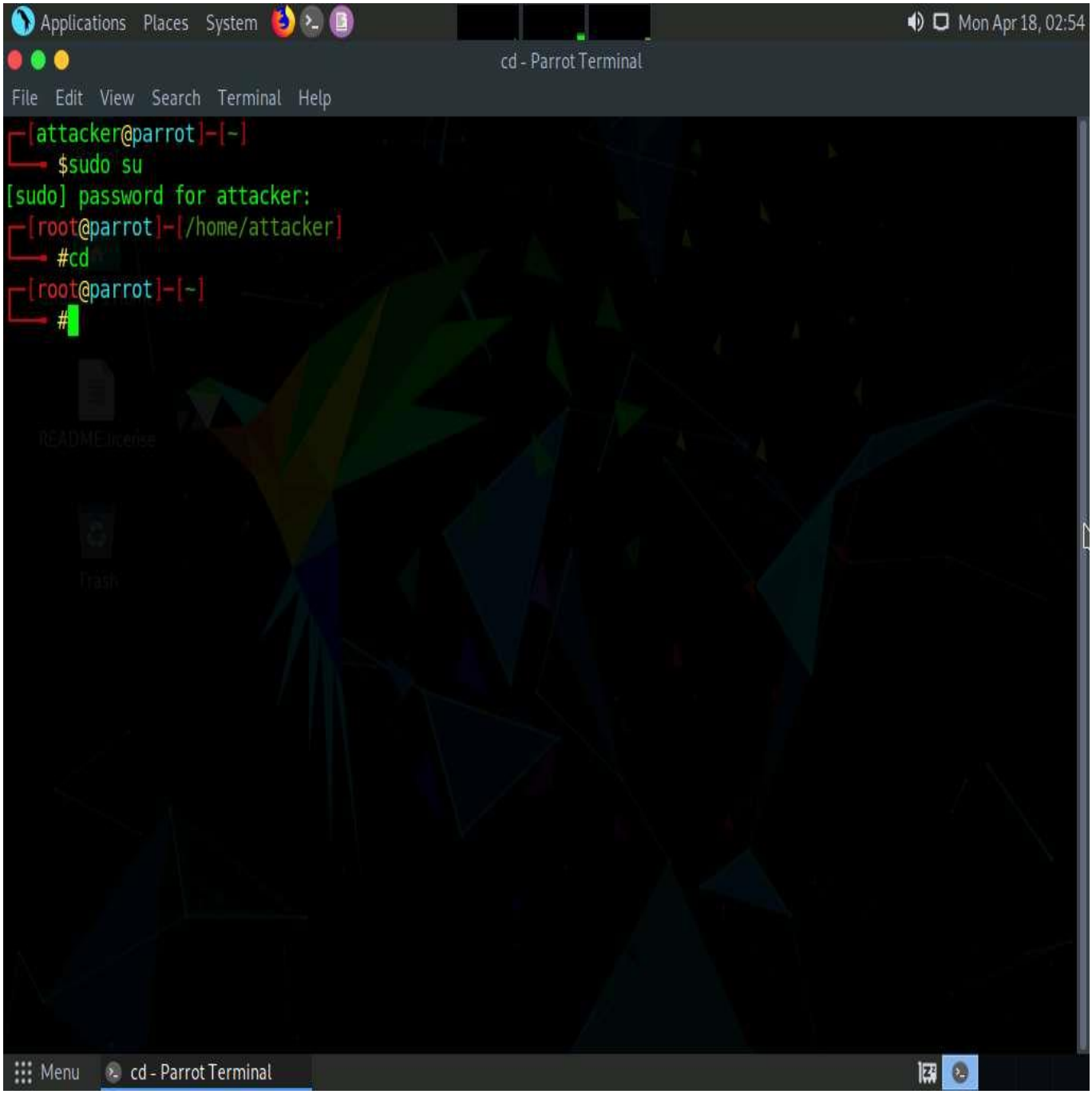
If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



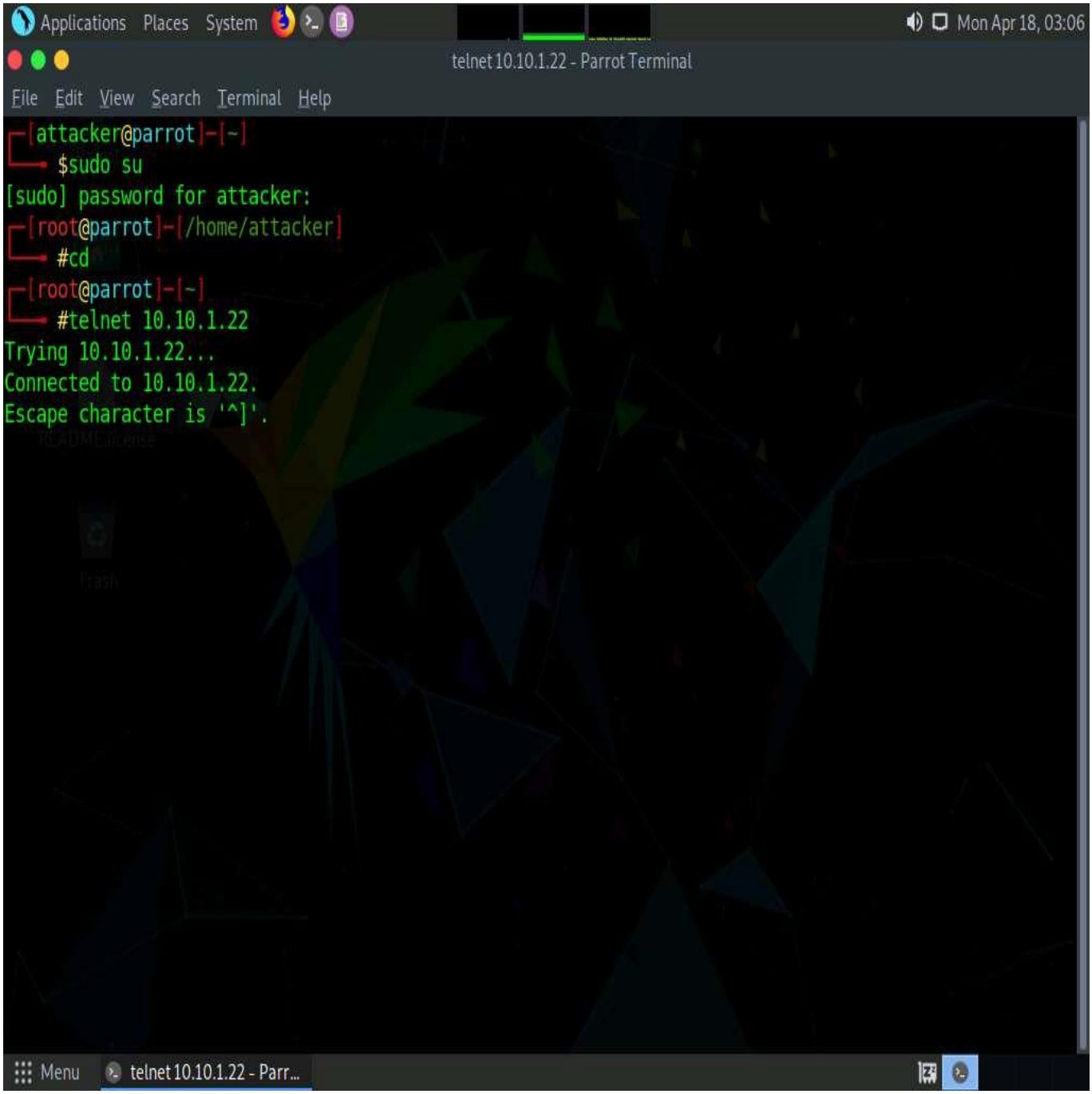
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
17. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

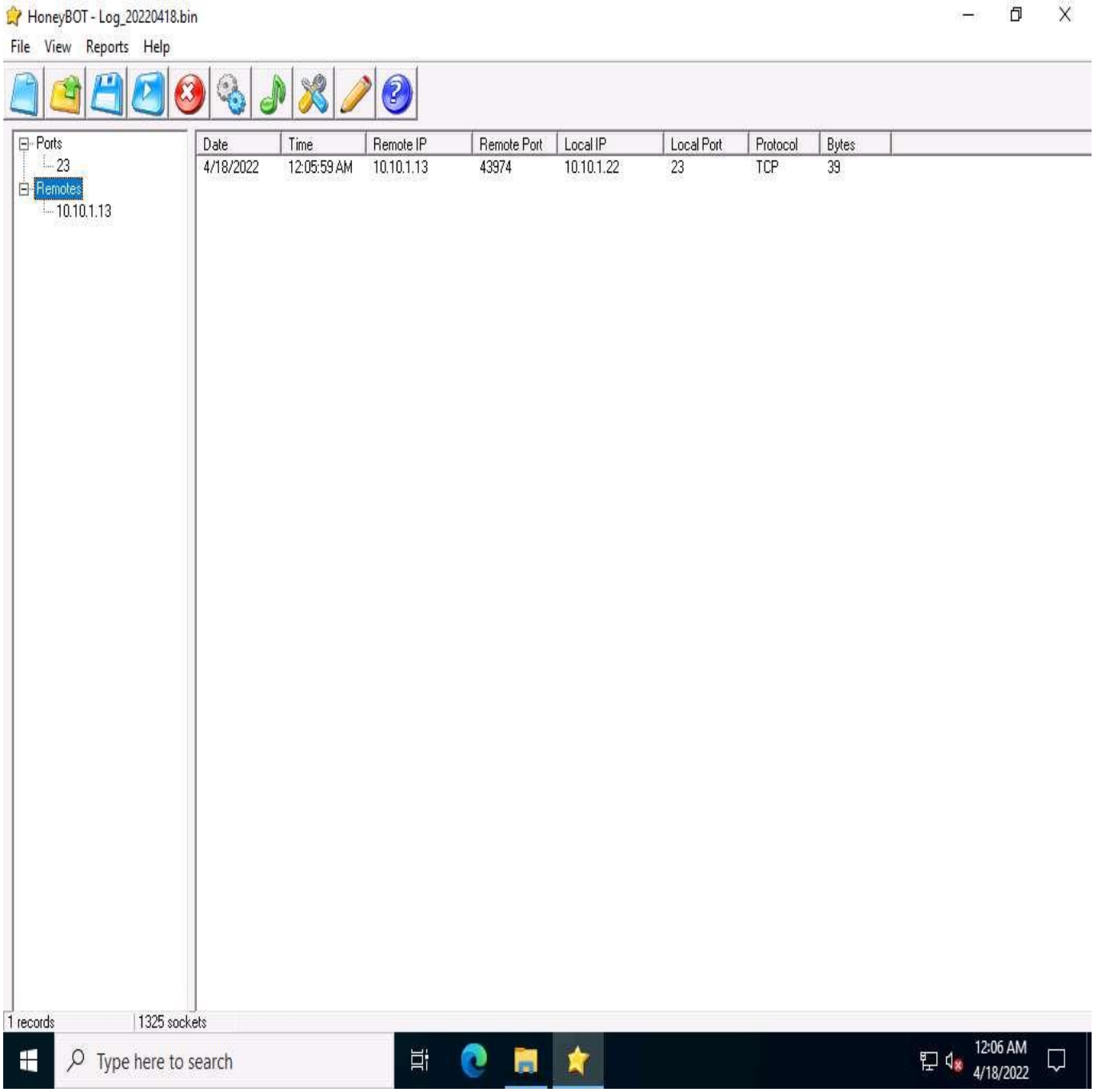
18. Now, type **cd** and press **Enter** to jump to the root directory.



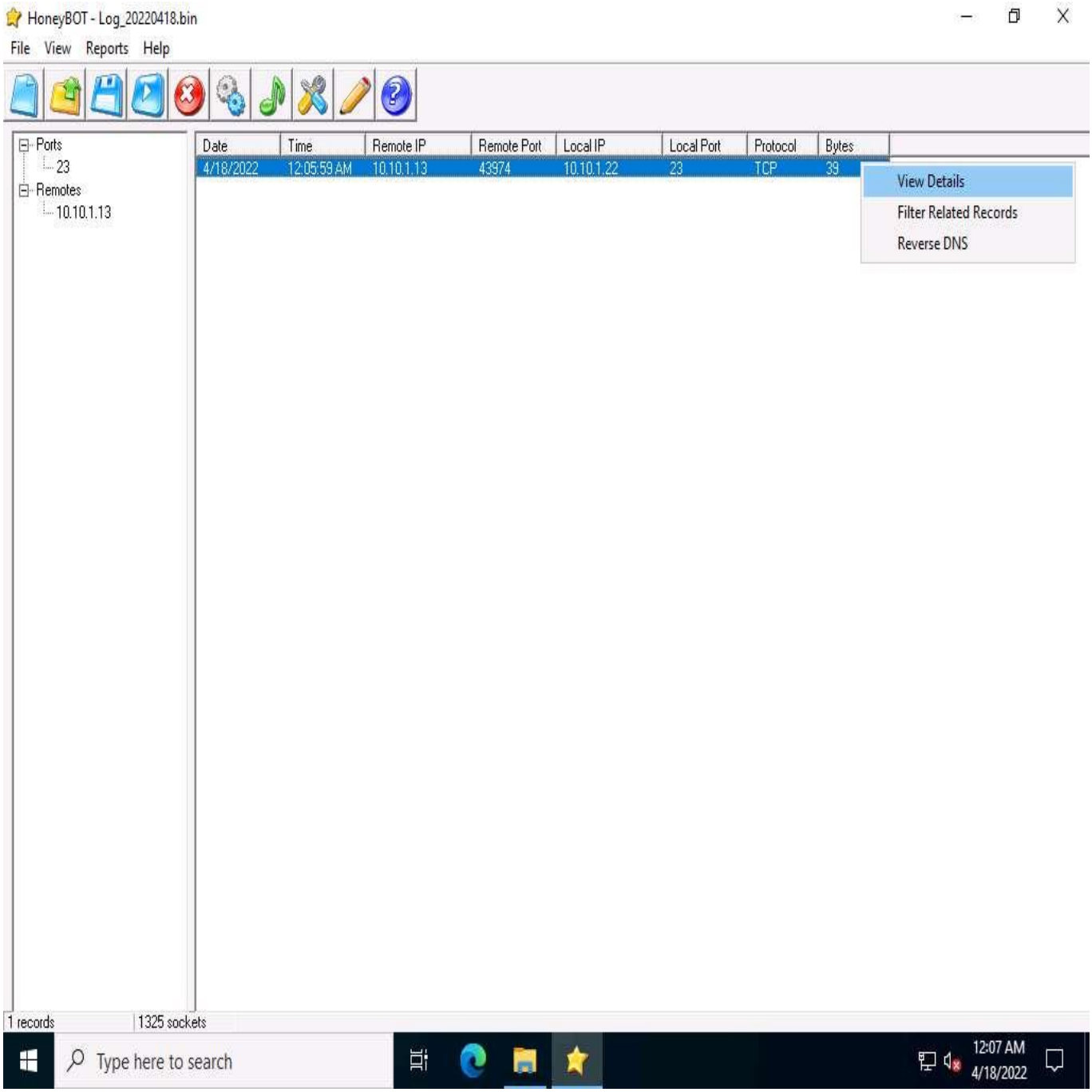
19. ☐ In the terminal window; type **telnet [IP Address of the Windows Server 2022 machine]** and press **Enter**.
20. ☐ You will be prompted for the telnet credentials of the **Windows Server 2022** machine.
21. ☐ In this task, the IP address of **Windows Server 2022** is **10.10.1.22**; this may differ when you perform this task.



22. ☐ Click 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.

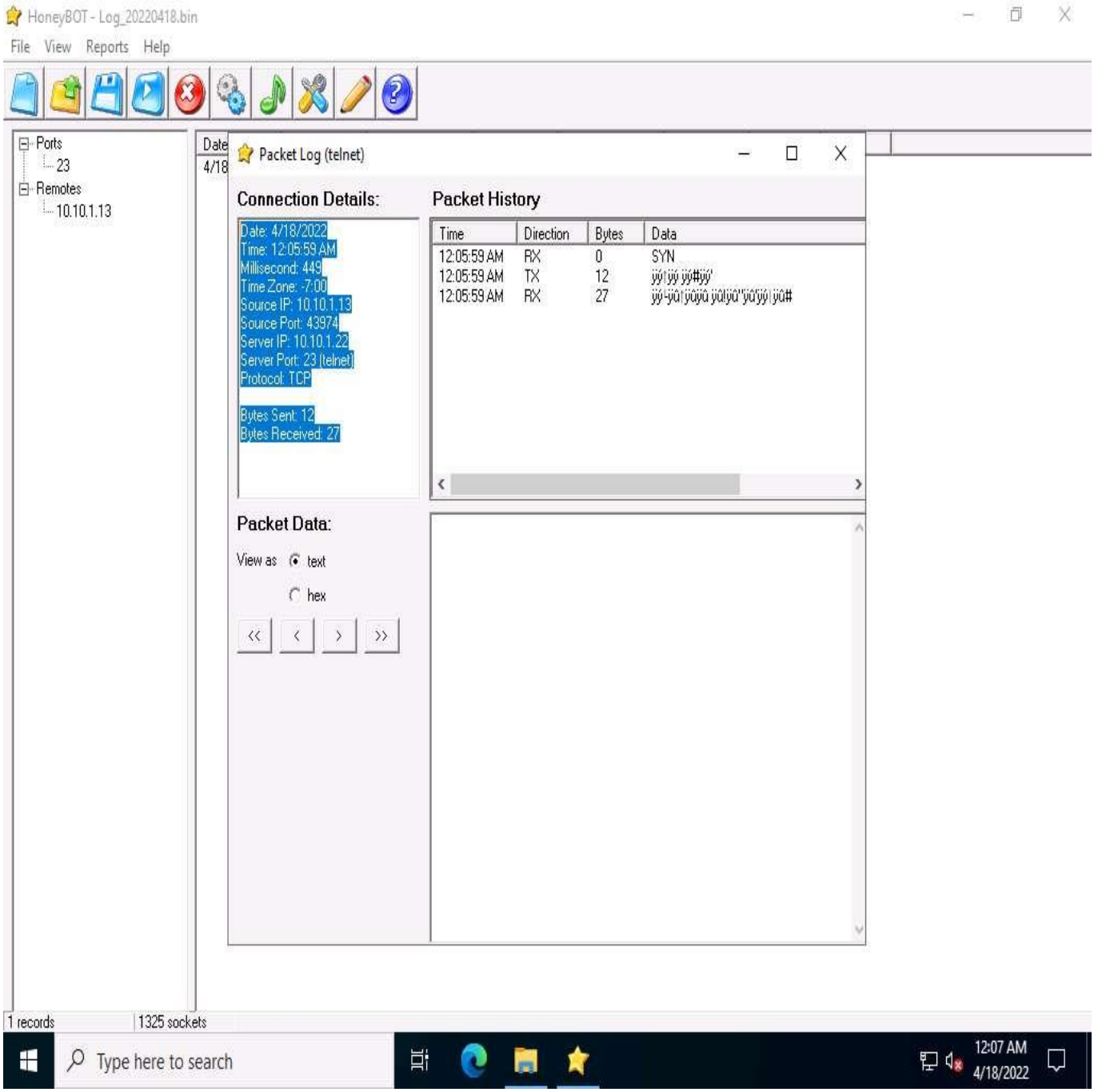


25. ☐ Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.



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.

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 and continue with the next lab.

To **End** the lab instance, click on the **Menu** icon from the top-right corner of the screen and click **End** from the options. In the **Are you sure you want to end this lab?**, click **Yes, end my lab**.