

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.

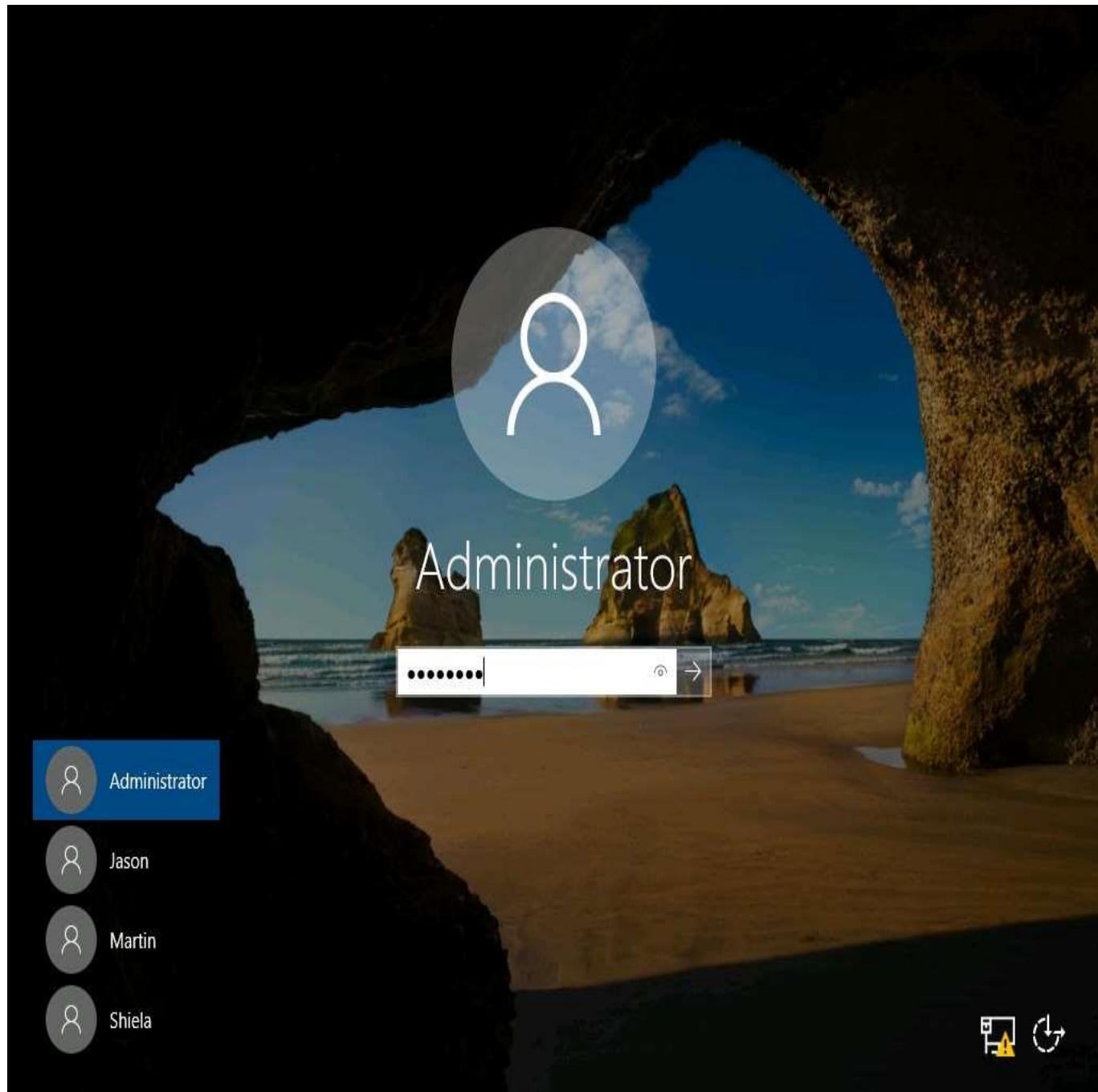
Uses of Snort:

- 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.

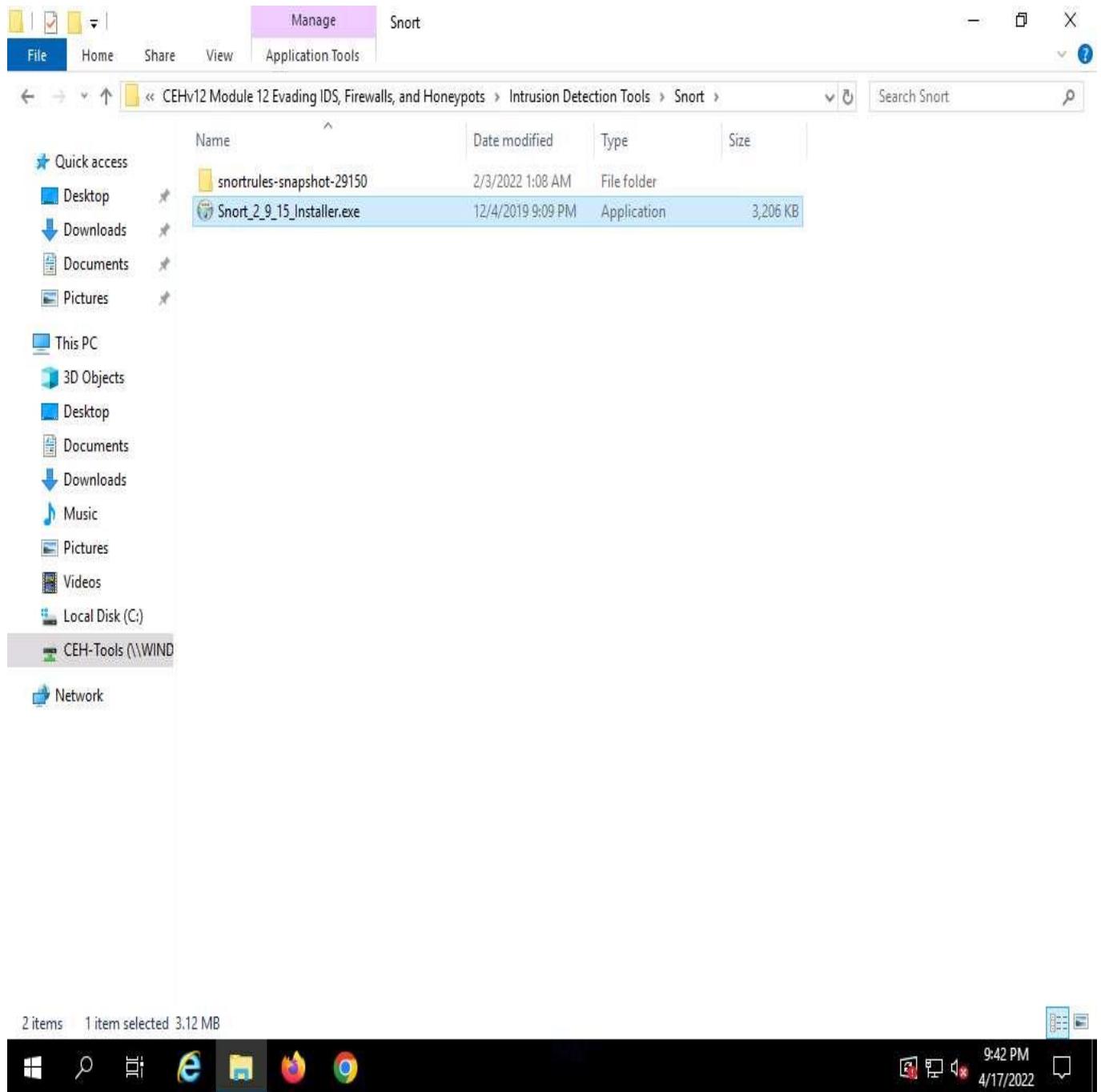
1. Click on **Windows Server 2019** to switch to **Windows Server 2019** machine. Click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** user profile is selected, click **Pa\$\$w0rd** to paste the password in the Password field and press **Enter** to login.

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.

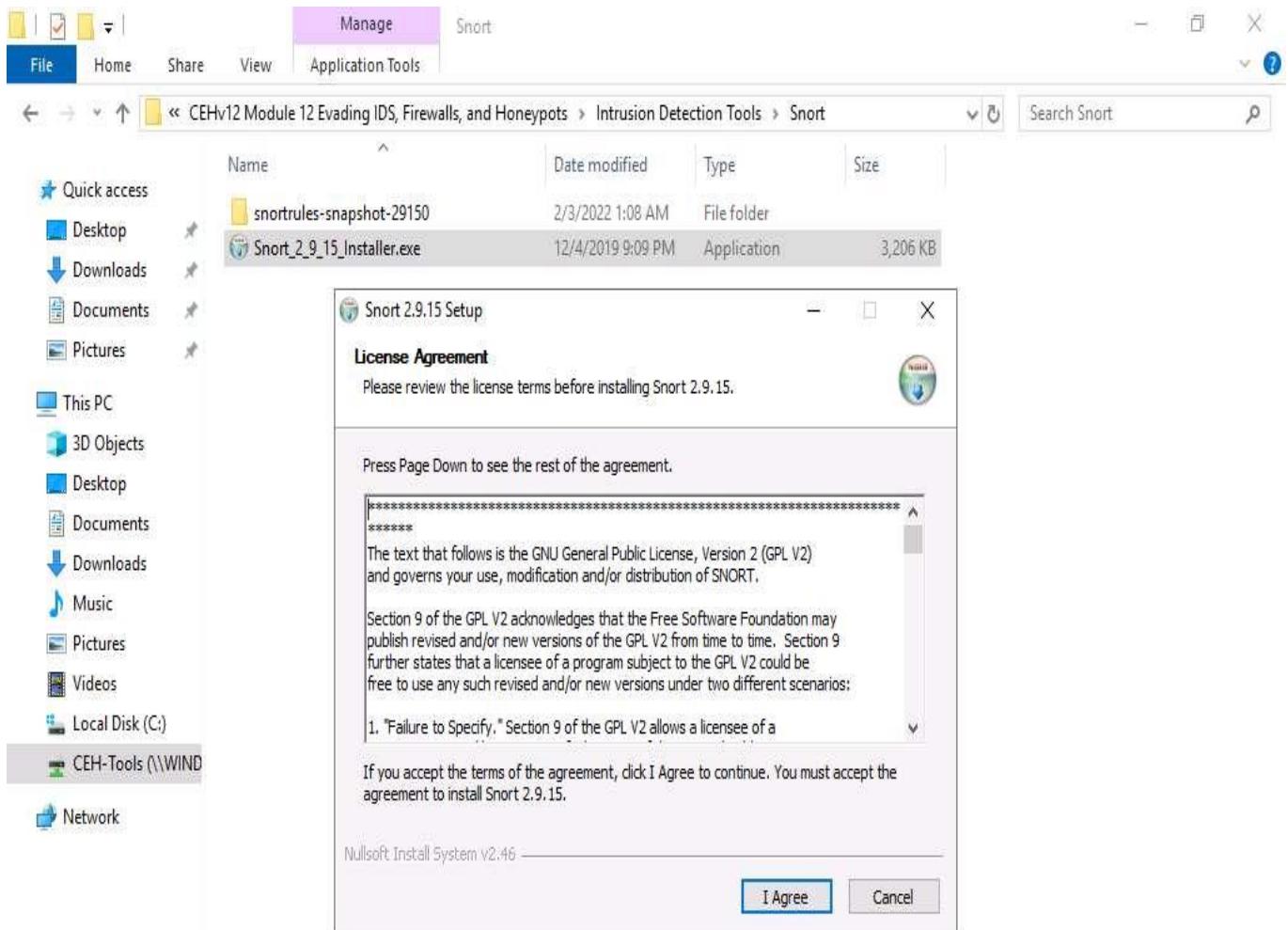


2. Navigate to Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort and double-click the Snort_2_9_15_Installer.exe file to start the Snort installation.

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

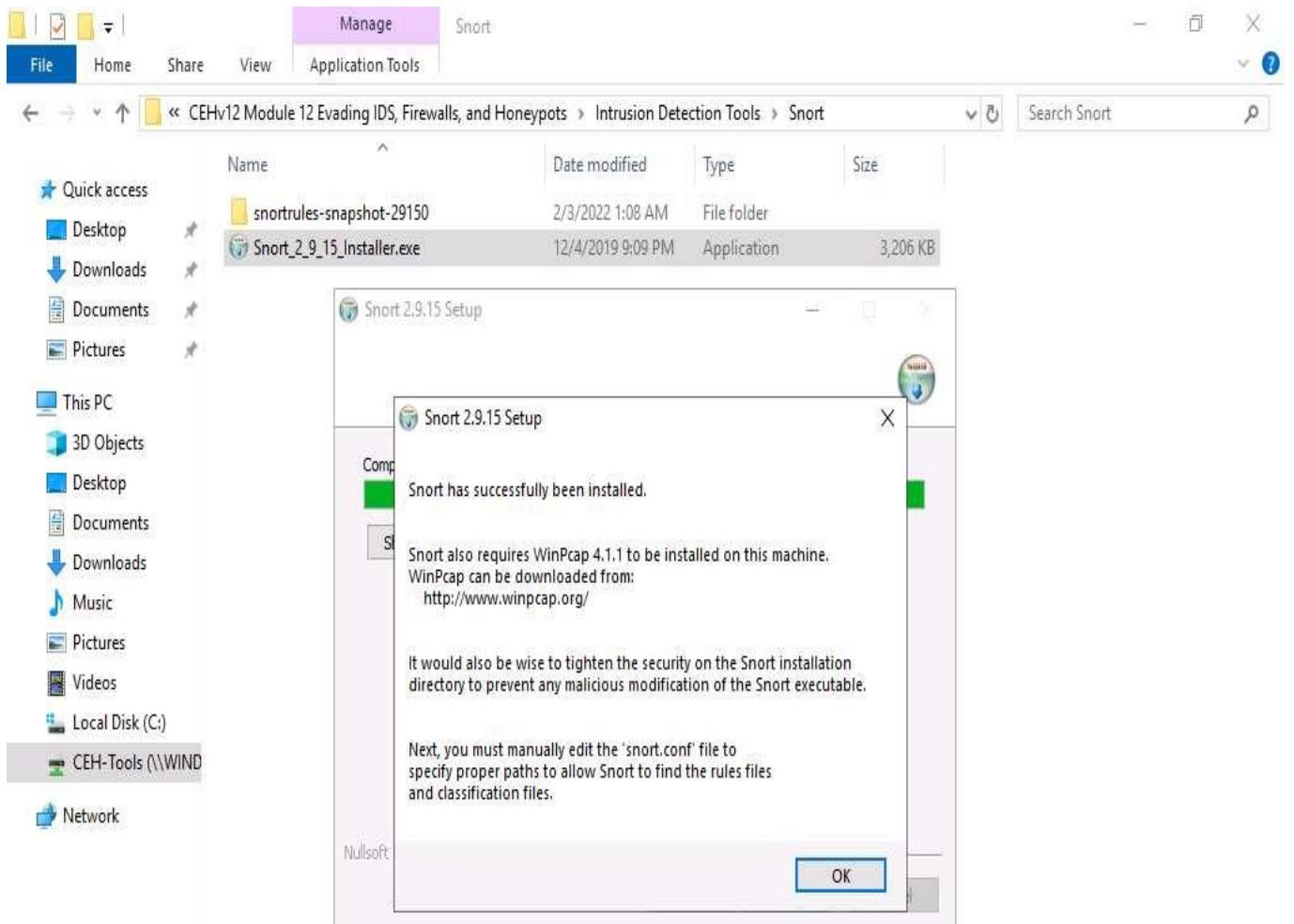


3. Accept the **License Agreement** and install Snort by selecting the default options that appear step by step in the wizard.

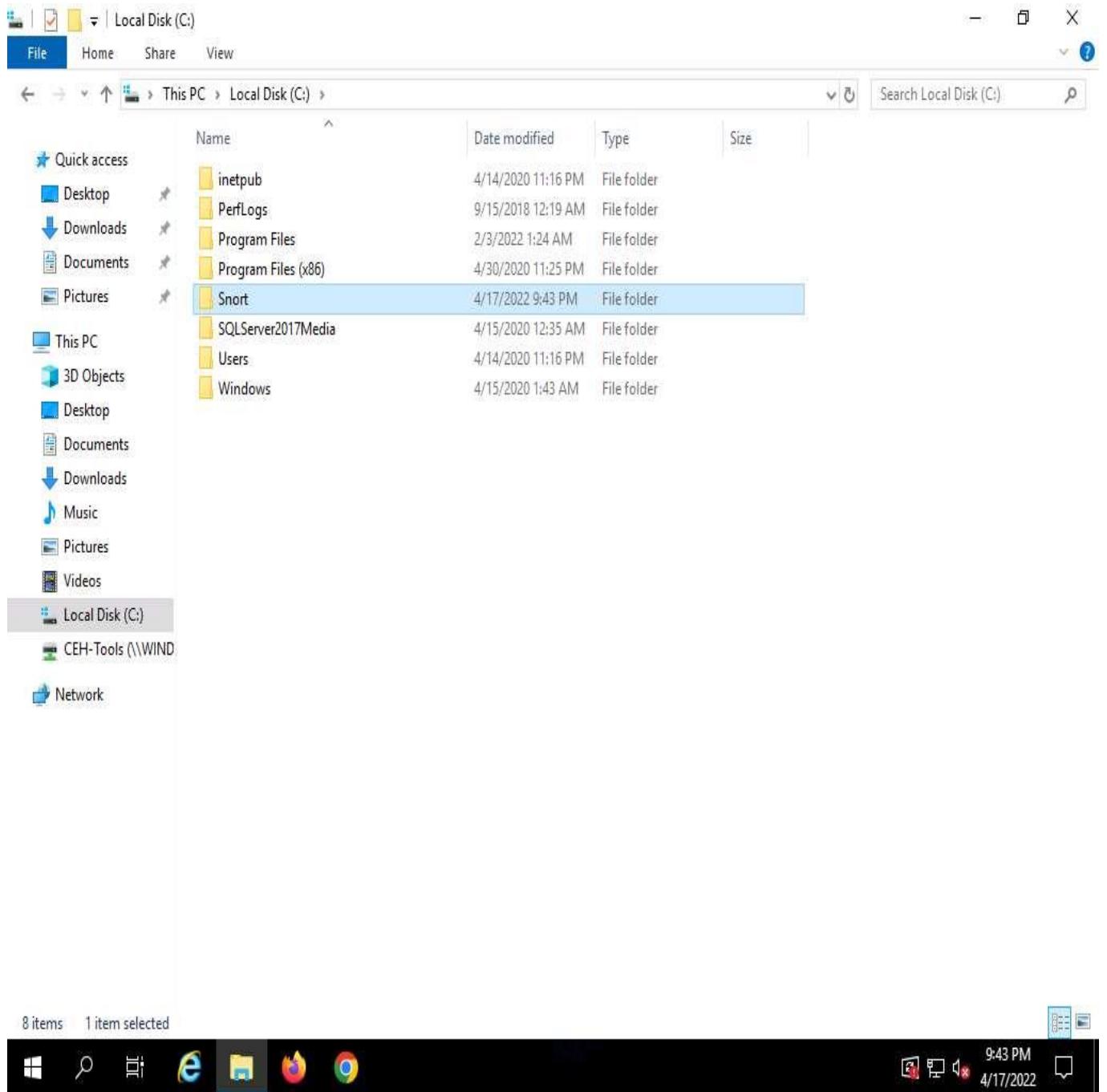


4. A window appears after the successful installation of Snort; click **Close**.
5. Click **OK** to exit the **Snort Installation** window.

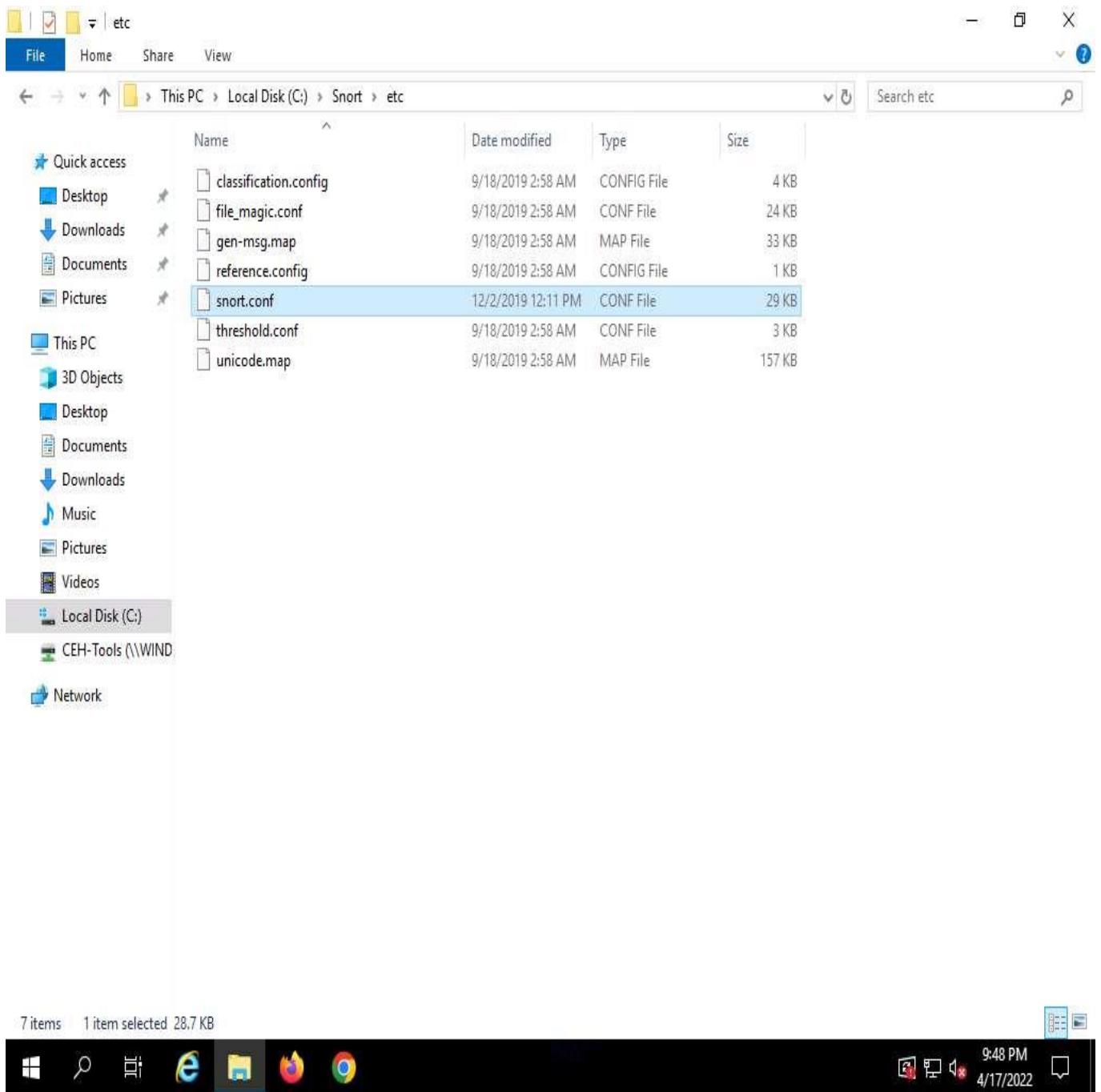
Snort requires **WinPcap** to be installed on your machine. In this task environment, we have already installed WinPcap drivers for packet capturing.



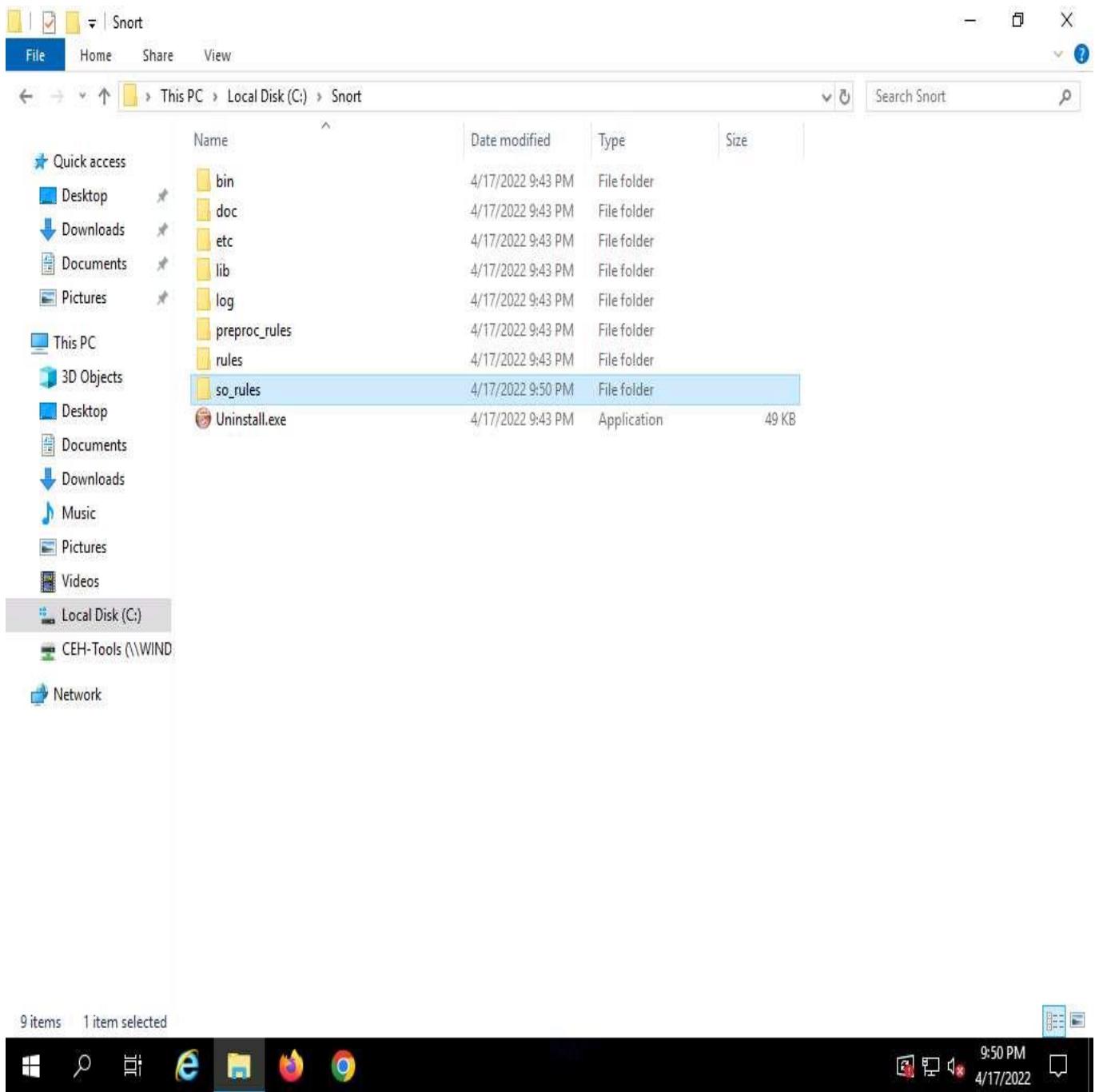
6. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).



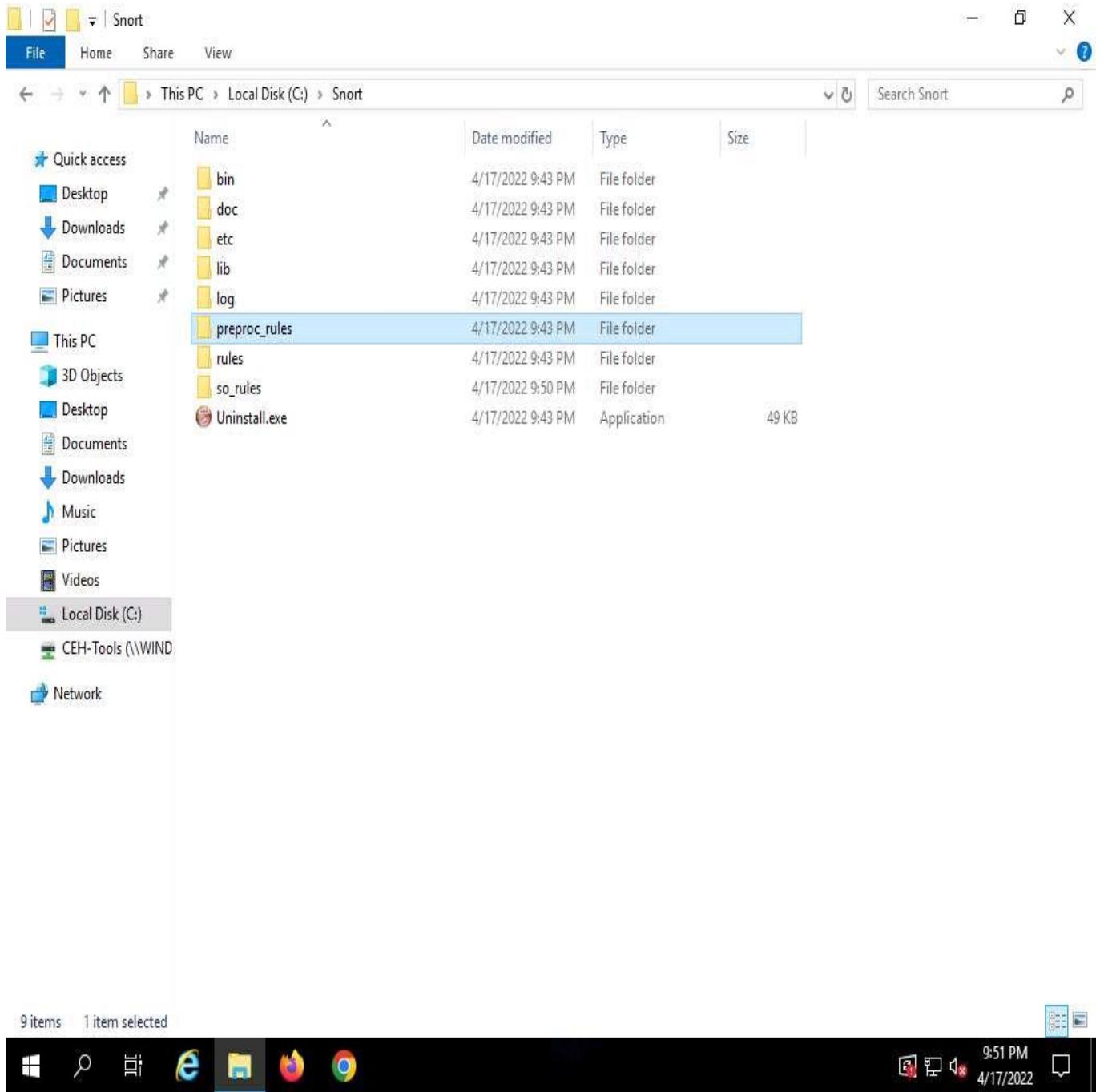
7. Navigate to the **etc** folder in the specified location, **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.
8. **snort.conf** is already present in **C:\Snort\etc**;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



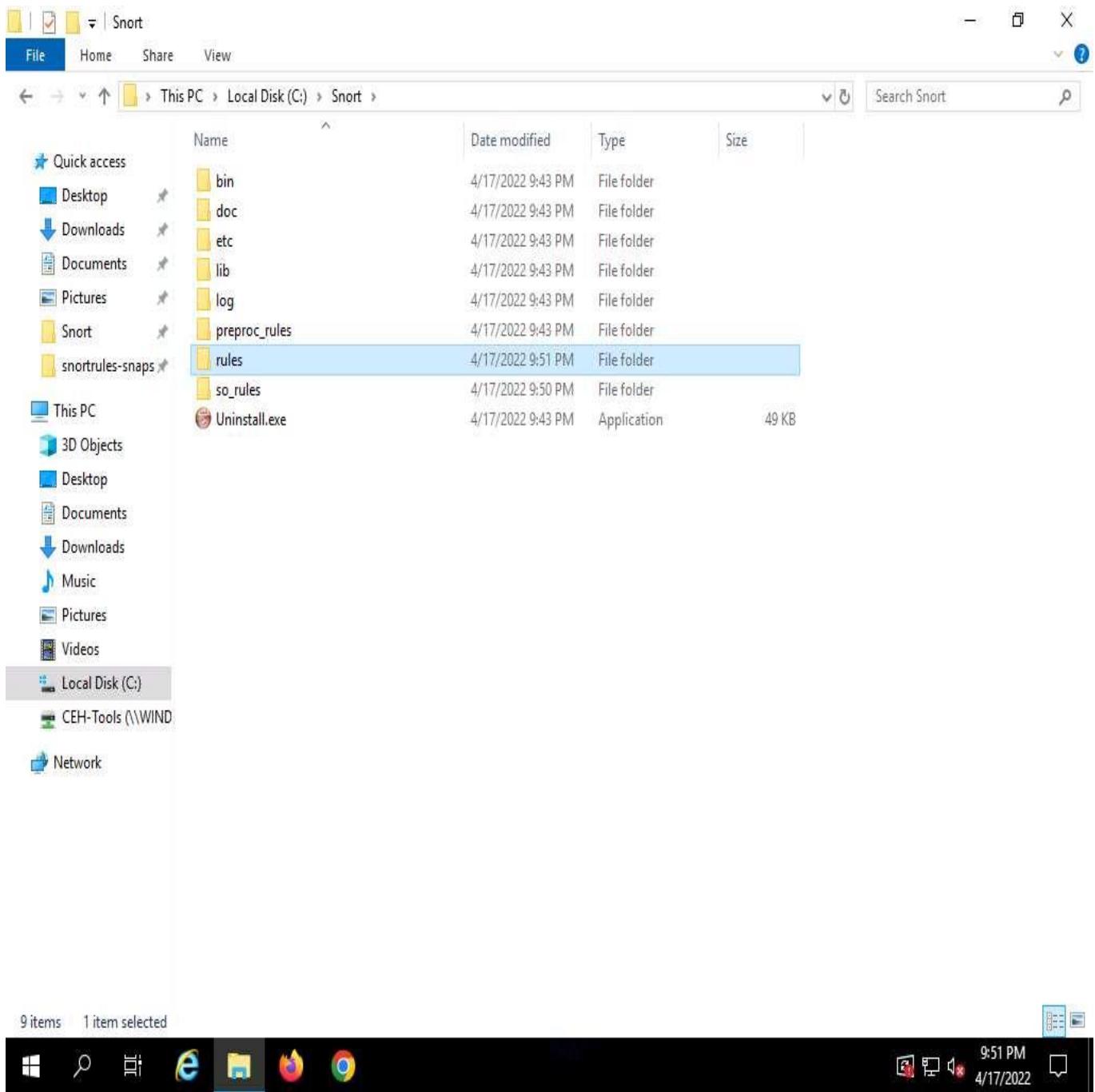
9. Copy the **so_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



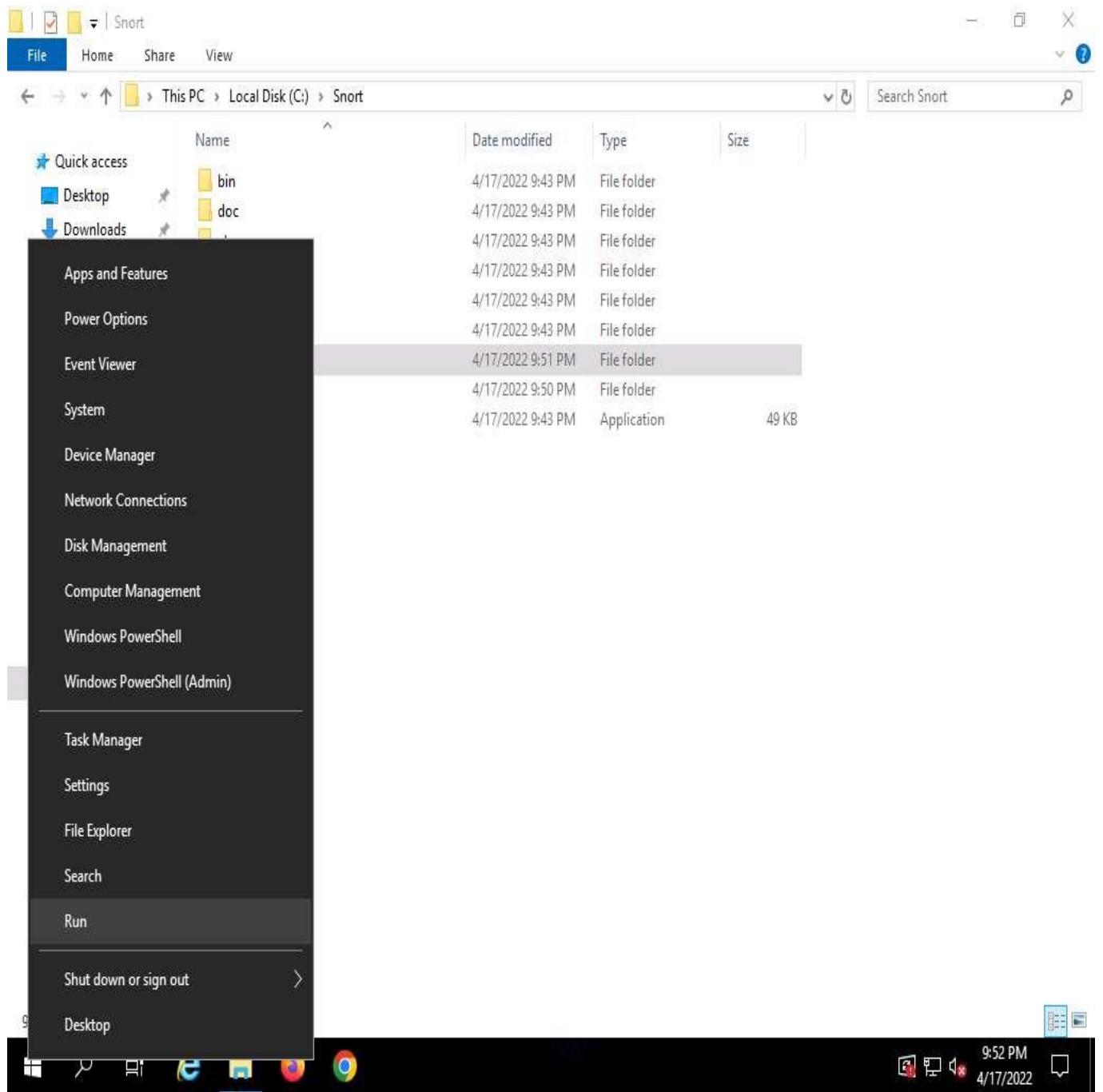
10. Copy the **preproc_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules**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



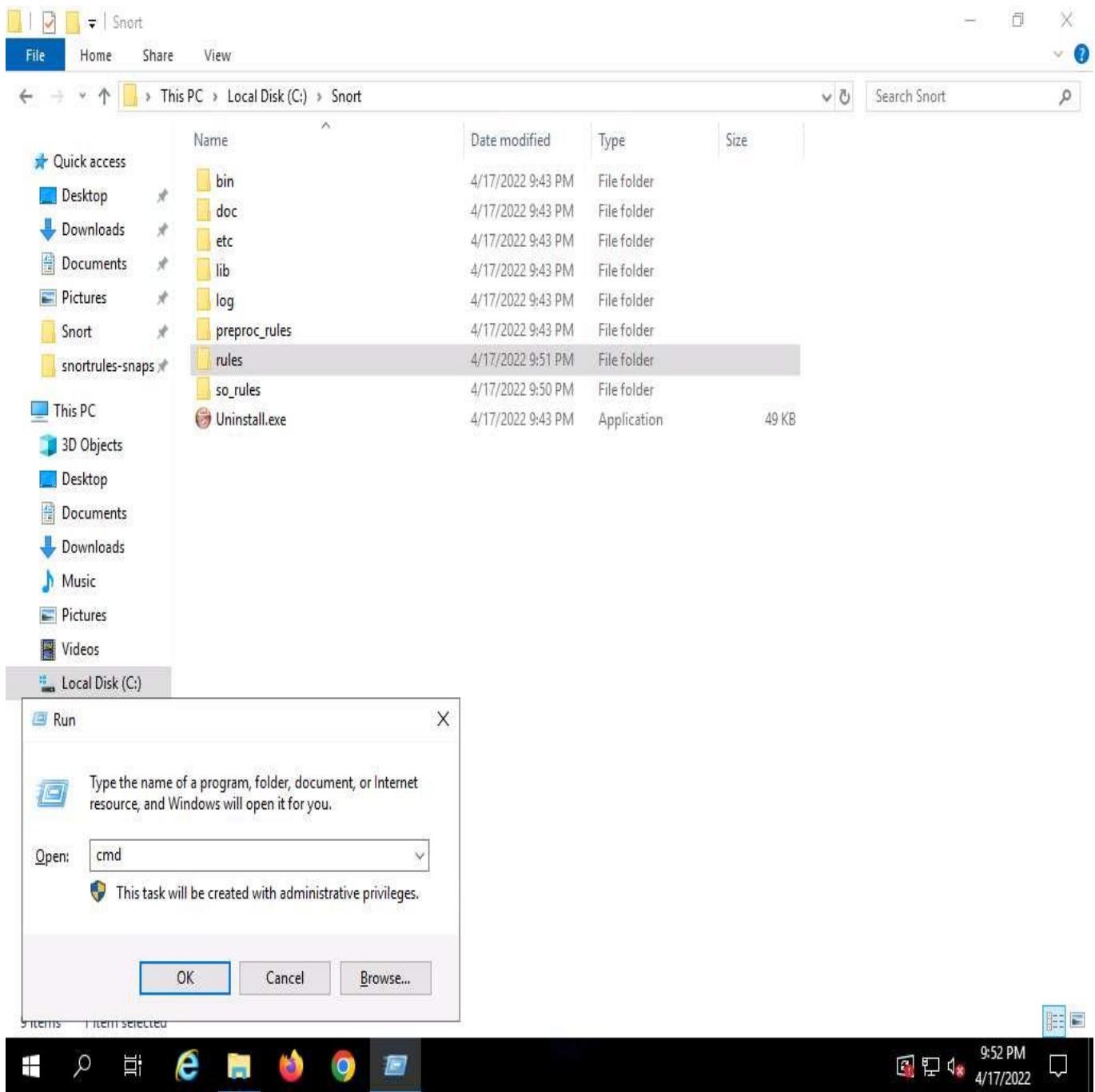
11. Using the same method, copy the **rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



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.

Administrator: C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Snort\bin

C:\Snort\bin>



9:53 PM
4/17/2022

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**.

```
Administrator: C:\Windows\system32\cmd.exe
IP6 Ext:      152 ( 95.597%)
IP6 Opts:      54 ( 33.962%)
Frag6:         0 ( 0.000%)
ICMP6:         66 ( 41.509%)
UDP6:          26 ( 16.352%)
TCP6:          6 ( 3.774%)
Teredo:        0 ( 0.000%)
ICMP-IP:       0 ( 0.000%)
EAPOL:         0 ( 0.000%)
IP4/IP4:       0 ( 0.000%)
IP4/IP6:       0 ( 0.000%)
IP6/IP4:       0 ( 0.000%)
IP6/IP6:       0 ( 0.000%)
GRE:           0 ( 0.000%)
GRE Eth:        0 ( 0.000%)
GRE VLAN:      0 ( 0.000%)
GRE IP4:        0 ( 0.000%)
GRE IP6:        0 ( 0.000%)
GRE IP6 Ext:    0 ( 0.000%)
GRE PPTP:       0 ( 0.000%)
GRE ARP:        0 ( 0.000%)
GRE IPX:        0 ( 0.000%)
GRE Loop:       0 ( 0.000%)
MPLS:           0 ( 0.000%)
ARP:            5 ( 3.145%)
IPX:            0 ( 0.000%)
Eth Loop:       0 ( 0.000%)
Eth Disc:       0 ( 0.000%)
IP4 Disc:       0 ( 0.000%)
IP6 Disc:       0 ( 0.000%)
TCP Disc:       0 ( 0.000%)
UDP Disc:       0 ( 0.000%)
ICMP Disc:      0 ( 0.000%)
All Discard:    0 ( 0.000%)
Other:          2 ( 1.258%)
Bad Chk Sum:    28 ( 17.610%)
Bad TTL:         0 ( 0.000%)
S5 G 1:          0 ( 0.000%)
S5 G 2:          0 ( 0.000%)
Total:          159
=====
Snort exiting
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.

Windows Select Administrator: C:\Windows\system32\cmd.exe

```
GRE VLAN:          0 (  0.000%)
GRE IP4:           0 (  0.000%)
GRE IP6:           0 (  0.000%)
GRE IP6 Ext:        0 (  0.000%)
GRE PPTP:           0 (  0.000%)
GRE ARP:            0 (  0.000%)
GRE IPX:            0 (  0.000%)
GRE Loop:           0 (  0.000%)
MPLS:               0 (  0.000%)
ARP:                5 ( 3.145%)
IPX:                0 (  0.000%)
Eth Loop:           0 (  0.000%)
Eth Disc:           0 (  0.000%)
IP4 Disc:           0 (  0.000%)
IP6 Disc:           0 (  0.000%)
TCP Disc:           0 (  0.000%)
UDP Disc:           0 (  0.000%)
ICMP Disc:          0 (  0.000%)
All Discard:         0 (  0.000%)
    Other:            2 ( 1.258%)
Bad Chk Sum:         28 ( 17.610%)
    Bad TTL:          0 (  0.000%)
    S5 G 1:           0 (  0.000%)
    S5 G 2:           0 (  0.000%)
    Total:             159
=====
Snort exiting
```

C:\Snort\bin>snort -W

```
,,,-> Snort! <*-  
o"~ Version 2.9.15-WIN32 GRE (Build 7)  
... By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using PCRE version: 8.10 2010-06-25  
Using ZLIB version: 1.2.3
```

Index	Physical Address	IP Address	Device Name	Description
1	00:00:00:00:00:00	0000:0000:fe80:0000:0000:0000:c9b9:9124	\Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}	Microsoft Corporation

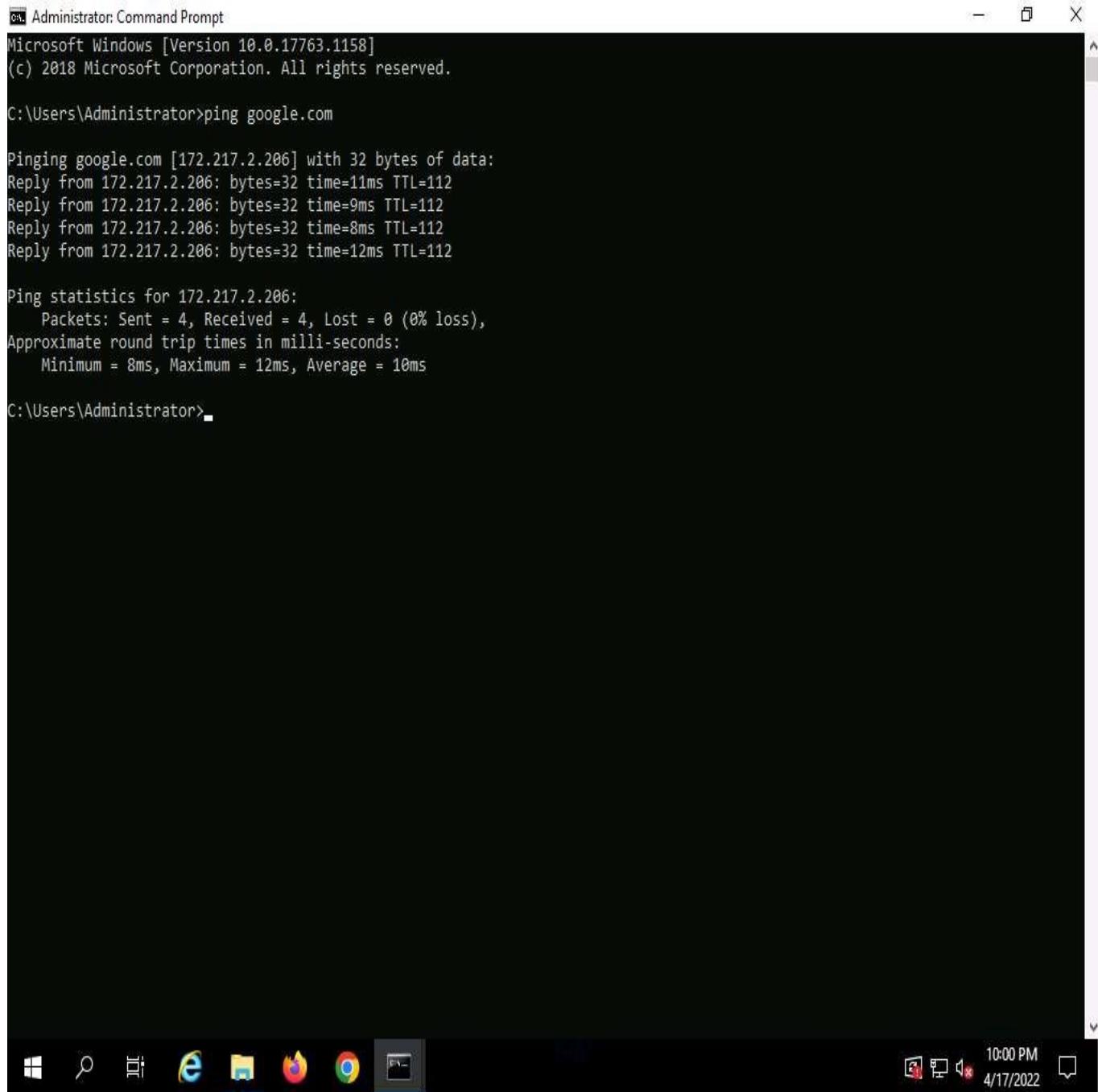
C:\Snort\bin>



9:55 PM
4/17/2022

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**.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [172.217.2.206] with 32 bytes of data:
Reply from 172.217.2.206: bytes=32 time=11ms TTL=112
Reply from 172.217.2.206: bytes=32 time=9ms TTL=112
Reply from 172.217.2.206: bytes=32 time=8ms TTL=112
Reply from 172.217.2.206: bytes=32 time=12ms TTL=112

Ping statistics for 172.217.2.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 12ms, Average = 10ms

C:\Users\Administrator>
```

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++**.

The screenshot shows the Notepad++ application window with the file 'snort.conf' open. The file contains the Snort configuration code. The code includes sections for VRT Rule Packages, mailing lists, compatible versions, build options, and a sample configuration section. The Notepad++ interface shows standard menu bars, toolbars, and status bars at the bottom.

```
1 #-----  
2 # VRT Rule Packages Snort.conf  
3 #  
4 # For more information visit us at:  
5 # http://www.snort.org Snort Website  
6 # http://vrt-blog.snort.org/ Sourcefire VRT Blog  
7 #  
8 # Mailing list Contact: snort-sigs@lists.sourceforge.net  
9 # False Positive reports: fp@sourcefire.com  
10 # Snort bugs: bugs@snort.org  
11 #  
12 # Compatible with Snort Versions:  
13 # VERSIONS : 2.9.15.0  
14 #  
15 # Snort build options:  
16 # OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --ena  
17 #  
18 # Additional information:  
19 # This configuration file enables active response, to run snort in  
20 # test mode -T you are required to supply an interface -i <interface>  
21 # or test mode will fail to fully validate the configuration and  
22 # exit with a FATAL error  
23 #-----  
24  
25 #####  
26 # This file contains a sample snort configuration.  
27 # You should take the following steps to create your own custom configuration:  
28 #  
29 # 1) Set the network variables.  
30 # 2) Configure the decoder  
31 # 3) Configure the base detection engine  
32 # 4) Configure dynamic loaded libraries  
33 # 5) Configure preprocessors  
34 # 6) Configure output plugins  
35 # 7) Customize your rule set  
36 # 8) Customize preprocessor and decoder rule set  
37 # 9) Customize shared object rule set
```

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**.

```
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf X
34  # 6) Configure output plugins
35  # 7) Customize your rule set
36  # 8) Customize preprocessor and decoder rule set
37  # 9) Customize shared object rule set
38 #####
39
40 #####
41 # Step #1: Set the network variables. For more information, see README.variables
42 #####
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 10.10.1.19
46
47 # Set up the external network addresses. Leave as "any" in most situations
48 ipvar EXTERNAL_NET any
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS 8.8.8.8
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
62 # List of telnet servers on your network
63 ipvar TELNET_SERVERS $HOME_NET
64
65 # List of ssh servers on your network
66 ipvar SSH_SERVERS $HOME_NET
67
68 # List of ftp servers on your network
69 ipvar FTP_SERVERS $HOME_NET
70
```

Normal text file length: 29,457 lines: 721 Ln:45 Col:7 Pos:1,845 Unix (LF) UTF-8 INS

10:05 PM 4/17/2022

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**.

```
79
80 # List of ports you might see oracle attacks on
81 portvar ORACLE_PORTS 1024;
82
83 # List of ports you want to look for SSH connections on:
84 portvar SSH_PORTS 22
85
86 # List of ports you run ftp servers on
87 portvar FTP_PORTS [21,2100,3535]
88
89 # List of ports you run SIP servers on
90 portvar SIP_PORTS [5060,5061,5600]
91
92 # List of file data ports for file inspection
93 portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386]
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH C:\Snort\rules
105 var SO_RULE_PATH C:\Snort\so_rules
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules
107
108 # If you are using reputation preprocessor set these
109 var WHITE_LIST_PATH ..\rules
110 var BLACK_LIST_PATH ..\rules
111
112 #####
113 # Step #2: Configure the decoder. For more information, see README.decode
114 #####
115
```

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

```
79
80 # List of ports you might see oracle attacks on
81 portvar ORACLE_PORTS 1024;
82
83 # List of ports you want to look for SSH connections on:
84 portvar SSH_PORTS 22;
85
86 # List of ports you run ftp servers on
87 portvar FTP_PORTS [21,2100,3535];
88
89 # List of ports you run SIP servers on
90 portvar SIP_PORTS [5060,5061,5600];
91
92 # List of file data ports for file inspection
93 portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143];
94
95 # List of GTP ports for GTP preprocessor
96 portvar GTP_PORTS [2123,2152,3386];
97
98 # other variables, these should not be modified
99 ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24];
100
101 # Path to your rules files (this can be a relative path)
102 # Note for Windows users: You are advised to make this an absolute path,
103 # such as: c:\snort\rules
104 var RULE_PATH C:\Snort\rules;
105 var SO_RULE_PATH C:\Snort\so_rules;
106 var PREPROC_RULE_PATH C:\Snort\preproc_rules;
107
108 # If you are using reputation preprocessor set these
109 var WHITE_LIST_PATH C:\Snort\rules;
110 var BLACK_LIST_PATH C:\Snort\rules;
111
112 #####
113 # Step #2: Configure the decoder. For more information, see README.decode
114 #####
115
```

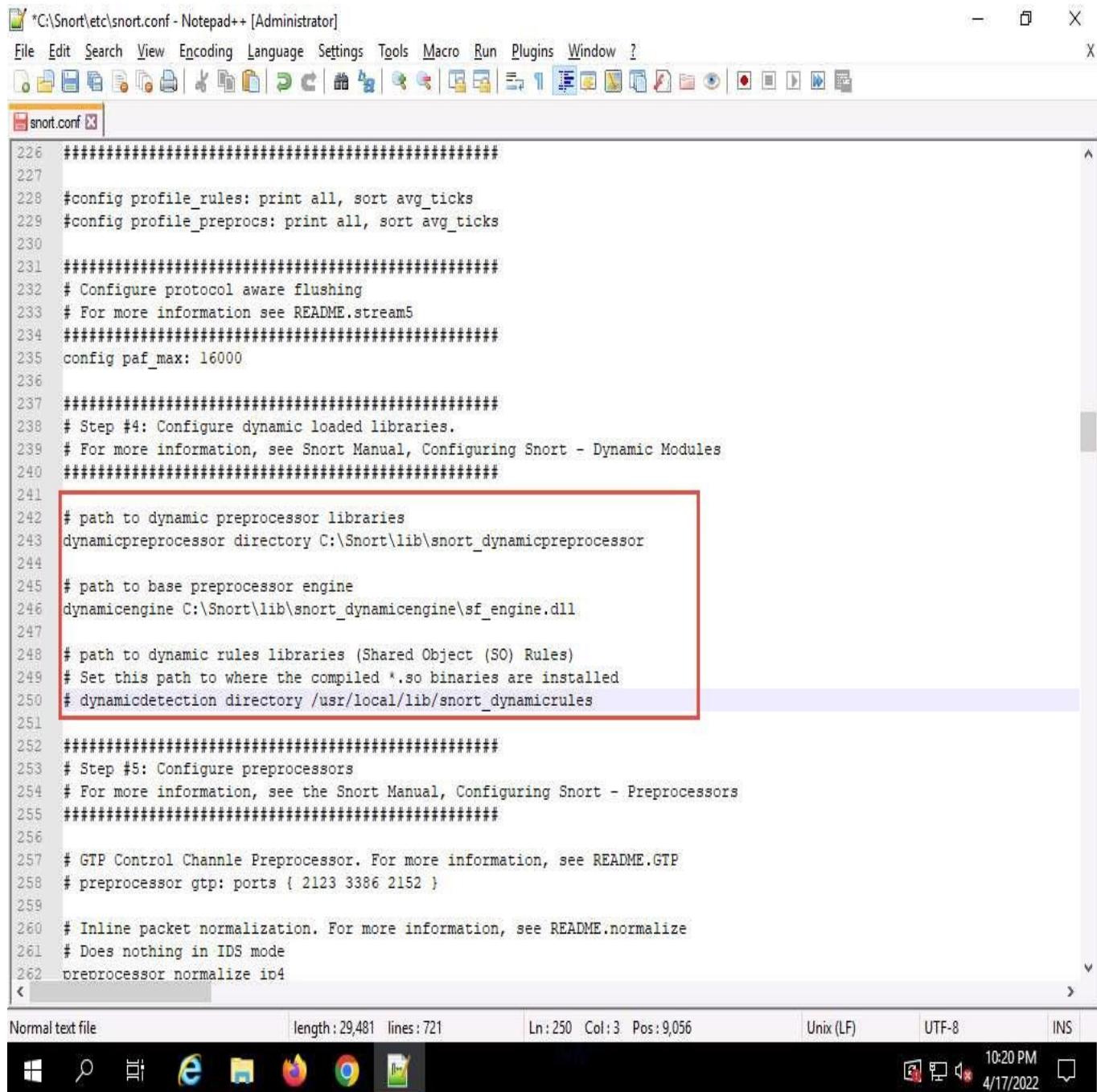
34. Navigate to **C:\Snort\rules**, and create two text files; name them **white_list** and **black_list** and change their file extensions from **.txt** to **.rules**.

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).



```

226 #####
227
228 #config profile_rules: print all, sort avg_ticks
229 #config profile_procs: print all, sort avg_ticks
230
231 #####
232 # Configure protocol aware flushing
233 # For more information see README.stream5
234 #####
235 config paf_max: 16000
236
237 #####
238 # Step #4: Configure dynamic loaded libraries.
239 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
240 #####
241
242 # path to dynamic preprocessor libraries
243 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
244
245 # path to base preprocessor engine
246 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
247
248 # path to dynamic rules libraries (Shared Object (SO) Rules)
249 # Set this path to where the compiled *.so binaries are installed
250 # dynamicdetection directory /usr/local/lib/snort_dynamicrules
251
252 #####
253 # Step #5: Configure preprocessors
254 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
255 #####
256
257 # GTP Control Channle Preprocessor. For more information, see README.GTP
258 # preprocessor gtp: ports { 2123 3386 2152 }
259
260 # Inline packet normalization. For more information, see README.normalize
261 # Does nothing in IDS mode
262 preprocessor normalize ip4
<
```

Normal text file length: 29,481 lines: 721 Ln: 250 Col: 3 Pos: 9,056 Unix (LF) UTF-8 INS

10:20 PM 4/17/2022

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).

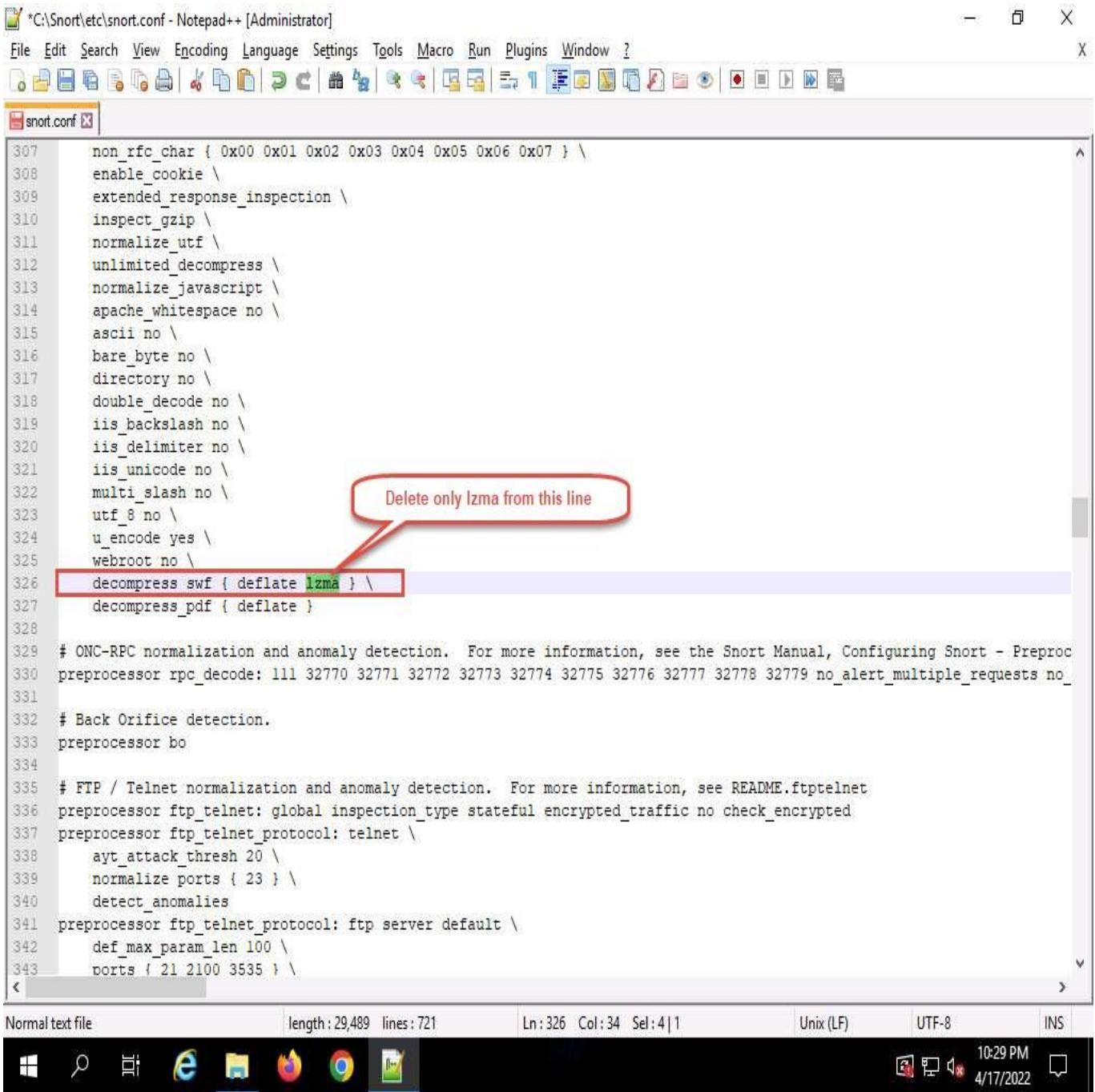
To 'comment out' is to render a block of code inert by turning it into a comment.

```
241
242 # path to dynamic preprocessor libraries
243 dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
244
245 # path to base preprocessor engine
246 dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
247
248 # path to dynamic rules libraries (Shared Object (SO) Rules)
249 # Set this path to where the compiled *.so binaries are installed
250 # dynamicdetection directory /usr/local/lib/snort_dynamicrules
251
252 #####
253 # Step #5: Configure preprocessors
254 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
255 #####
256
257 # GTP Control Channle Preprocessor. For more information, see README.GTP
258 # processor gtp: ports { 2123 3386 2152 }
259
260 # Inline packet normalization. For more information, see README.normalize
261 # Does nothing in IDS mode
262 # processor normalize_ip4
263 # processor normalize_tcp: block, rsv, pad, urp, req_urg, req_pay, req_urp, ips, ecn stream
264 # processor normalize_icmp4
265 # processor normalize_ip6
266 # processor normalize_icmp6
267
268 # Target-based IP defragmentation. For more inforation, see README.frag3
269 processor frag3_global: max_frags 65536
270 processor frag3_engine: policy windows detect_anomalies overlap_limit 10 min_fragment_length 100 timeout 180
271
272 # Target-Based stateful inspection/stream reassembly. For more inforation, see README.stream5
273 processor stream5_global: track_tcp yes, \
274     track_udp yes, \
275     track_icmp no, \
276     max_tcp 262144, \
277     max_udp 131072. \
<      
```

Normal text file length:29,489 lines:721 Ln:266 Col:3 Pos:9,744 Unix (LF) UTF-8 INS

10:22 PM 4/17/2022

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



*C:\Snort\etc\snort.conf - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

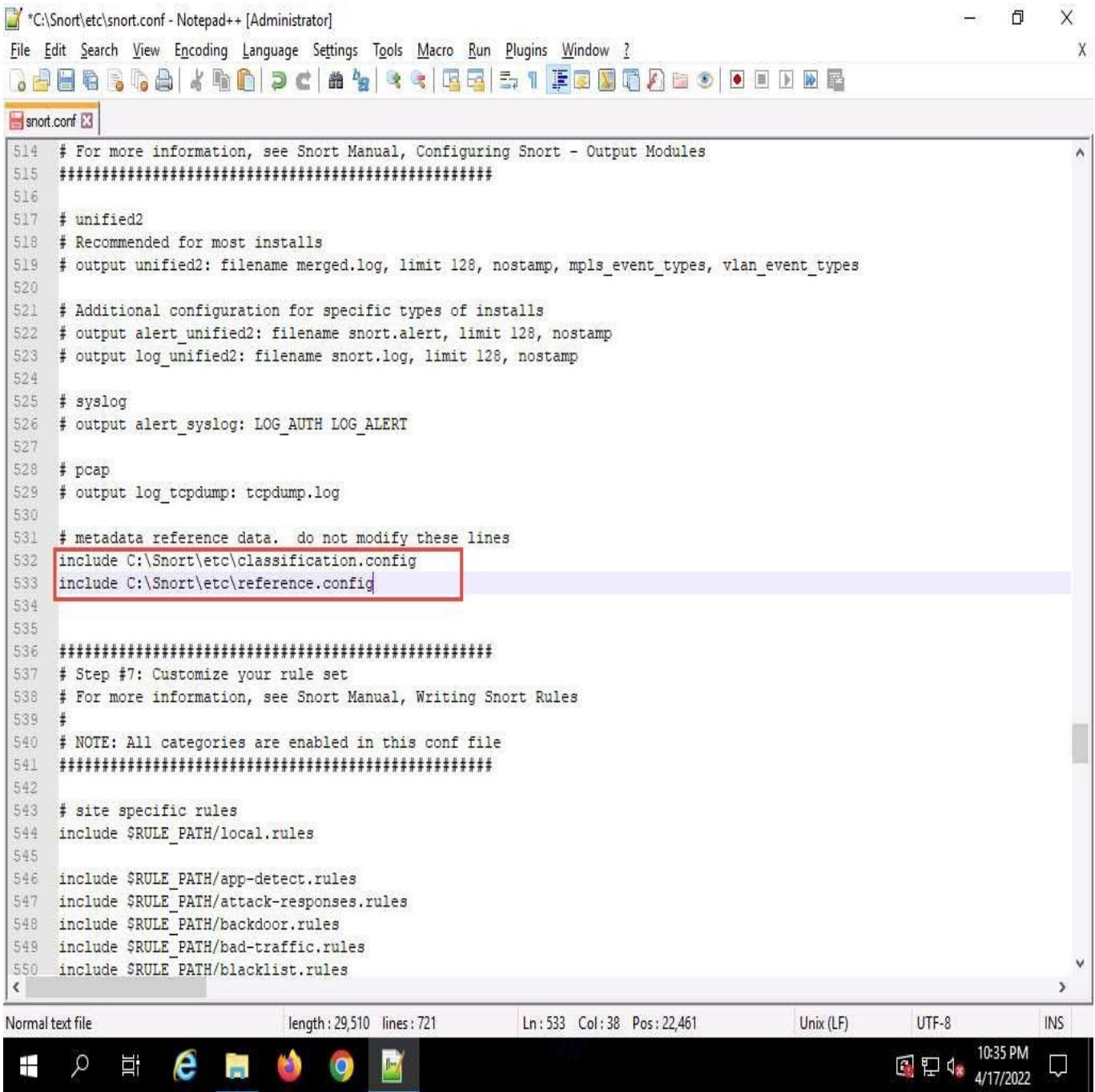
snort.conf

```
307     non_rfc_char { 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 } \
308     enable_cookie \
309     extended_response_inspection \
310     inspect_gzip \
311     normalize_utf \
312     unlimited_decompress \
313     normalize_javascript \
314     apache_whitespace no \
315     ascii no \
316     bare_byte no \
317     directory no \
318     double_decode no \
319     iis_backslash no \
320     iis_delimiter no \
321     iis_unicode no \
322     multi_slash no \
323     utf_8 no \
324     u_encode yes \
325     webroot no \
326     decompress_swf { deflate lzma } \
327     decompress_pdf { deflate } \
328
329 # ONC-RPC normalization and anomaly detection. For more information, see the Snort Manual, Configuring Snort - Preproc
330 preprocessor rpc_decode: 111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779 no_alert_multiple_requests no_
331
332 # Back Orifice detection.
333 preprocessor bo
334
335 # FTP / Telnet normalization and anomaly detection. For more information, see README.ftptelnet
336 preprocessor ftp_telnet: global inspection_type stateful encrypted_traffic no check_encrypted
337 preprocessor ftp_telnet_protocol: telnet \
338     ayt_attack_thresh 20 \
339     normalize_ports { 23 } \
340     detect_anomalies
341 preprocessor ftp_telnet_protocol: ftp server default \
342     def_max_param_len 100 \
343     ports { 21 2100 3535 } \
```

Normal text file length: 29,489 lines: 721 Ln:326 Col:34 Sel:4|1 Unix (LF) UTF-8 INS

Windows 10 taskbar icons: File Explorer, Edge, File Manager, Firefox, Google Chrome, File History, Task View, Power User, Taskbar settings, Date/Time (10:29 PM, 4/17/2022).

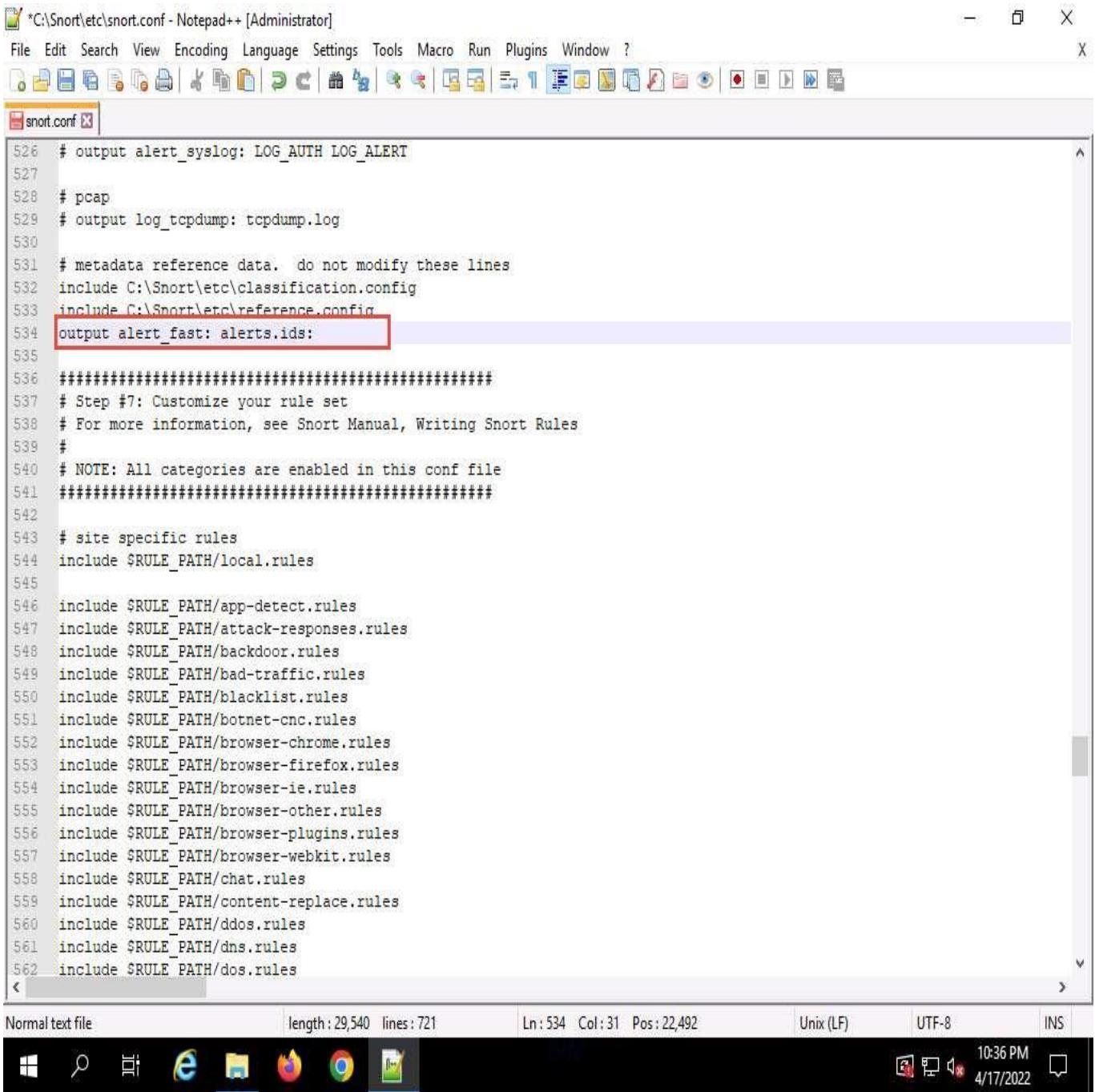
44. Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.
45. These two files are in **C:\Snort\etc**. Provide this location of files in the configure output plugins (in Lines 532 and 533) (i.e., **C:\Snort\etc\classification.config** and **C:\Snort\etc\reference.config**).



```
*C:\Snort\etc\snort.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf

514 # For more information, see Snort Manual, Configuring Snort - Output Modules
515 #####
516
517 # unified2
518 # Recommended for most installs
519 # output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
520
521 # Additional configuration for specific types of installs
522 # output alert_unified2: filename snort.alert, limit 128, nostamp
523 # output log_unified2: filename snort.log, limit 128, nostamp
524
525 # syslog
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527
528 # pcap
529 # output log_tcpdump: tcpdump.log
530
531 # metadata reference data. do not modify these lines
532 include C:\Snort\etc\classification.config
533 include C:\Snort\etc\reference.config
534
535
536 #####
537 # Step #7: Customize your rule set
538 # For more information, see Snort Manual, Writing Snort Rules
539 #
540 # NOTE: All categories are enabled in this conf file
541 #####
542
543 # site specific rules
544 include $RULE_PATH/local.rules
545
546 include $RULE_PATH/app-detect.rules
547 include $RULE_PATH/attack-responses.rules
548 include $RULE_PATH/backdoor.rules
549 include $RULE_PATH/bad-traffic.rules
550 include $RULE_PATH/blacklist.rules
```

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.



```
526 # output alert_syslog: LOG_AUTH LOG_ALERT
527
528 # pcap
529 # output log_tcpdump: tcpdump.log
530
531 # metadata reference data. do not modify these lines
532 include C:\Snort\etc\classification.config
533 include C:\Snort\etc\reference.config
534 output alert_fast: alerts.ids;
535
536 #####
537 # Step #7: Customize your rule set
538 # For more information, see Snort Manual, Writing Snort Rules
539 #
540 # NOTE: All categories are enabled in this conf file
541 #####
542
543 # site specific rules
544 include $RULE_PATH/local.rules
545
546 include $RULE_PATH/app-detect.rules
547 include $RULE_PATH/attack-responses.rules
548 include $RULE_PATH/backdoor.rules
549 include $RULE_PATH/bad-traffic.rules
550 include $RULE_PATH/blacklist.rules
551 include $RULE_PATH/botnet-cnc.rules
552 include $RULE_PATH/browser-chrome.rules
553 include $RULE_PATH/browser-firefox.rules
554 include $RULE_PATH/browser-ie.rules
555 include $RULE_PATH/browser-other.rules
556 include $RULE_PATH/browser-plugins.rules
557 include $RULE_PATH/browser-webkit.rules
558 include $RULE_PATH/chat.rules
559 include $RULE_PATH/content-replace.rules
560 include $RULE_PATH/ddos.rules
561 include $RULE_PATH/dns.rules
562 include $RULE_PATH/dos.rules
```

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.

The screenshot shows the Notepad++ interface with the file 'snort.conf' open. The 'Replace' dialog box is active, with 'Find what: ipvar' and 'Replace with: var'. The 'Replace All' button is highlighted. The main text area shows several 'include' statements for various rule sets like app-detect, attack-responses, and browser-chrome.

```

526 # output alert_syslog: LOG_AUTH LOG_ALERT
527
528 # pcap
529 # output log_tcpdump: tcpdump.log
530
531 # metadata reference data. do not modify these lines
532 include C:\Snort\etc\classification.config
533 include C:\Snort\etc\reference.config
534 output alert_fast: alerts.ids;
535
536 #####
537 # Step #7: Customize your rule set
538 # For more information, see Snort Manual, Writing Rules
539 #
540 # NOTE: All categories are enabled in this config
541 #####
542
543 # site specific rules
544 include $RULE_PATH/local.rules
545
546 include $RULE_PATH/app-detect.rules
547 include $RULE_PATH/attack-responses.rules
548 include $RULE_PATH/backdoor.rules
549 include $RULE_PATH/bad-traffic.rules
550 include $RULE_PATH/blacklist.rules
551 include $RULE_PATH/botnet-cnc.rules
552 include $RULE_PATH/browser-chrome.rules
553 include $RULE_PATH/browser-firefox.rules
554 include $RULE_PATH/browser-ie.rules
555 include $RULE_PATH/browser-other.rules
556 include $RULE_PATH/browser-plugins.rules
557 include $RULE_PATH/browser-webkit.rules
558 include $RULE_PATH/chat.rules
559 include $RULE_PATH/content-replace.rules
560 include $RULE_PATH/ddos.rules
561 include $RULE_PATH/dns.rules
562 include $RULE_PATH/dos.rules

```

- Click **Close** to close the **Replace** window.
- Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.
- 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.
- Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with **Notepad++**.
- 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.

```
1 # Copyright 2001-2019 Sourcefire, Inc. All Rights Reserved.
2 #
3 # This file contains (i) proprietary rules that were created, tested and certified by
4 # Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
5 # Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
6 # Sourcefire and other third parties (the "GPL Rules") that are distributed under the
7 # GNU General Public License (GPL), v2.
8 #
9 # The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
10 # by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
11 # owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
12 # their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
13 # list of third party owners and their respective copyrights.
14 #
15 # In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
16 # to the VRT Certified Rules License Agreement (v2.0).
17 #
18 #-----
19 # ICMP-INFO RULES
20 #
21 alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.1.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; re
```

- Now right-click on the **Windows Start** icon and click **Run** from the menu.
- In the **Run** window, type **cmd** in the **Open** field and press **Enter**: This will launch a command prompt window.
- In the command prompt window, type **cd C:\Snort\bin** and press **Enter**.
- Type **snort -iX -A console -c C:\Snort\etc\snort.conf -I C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this task: **X** is 1).

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Snort\bin

C:\Snort\bin>snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii.
```

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.

```
Administrator: Command Prompt - snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii
State Density      : 67.0%
Patterns          : 12537
Match States      : 13177
Memory (MB)       : 174.57
  Patterns        : 1.08
  Match Lists     : 1.83
DFA
  1 byte states  : 1.75
  2 byte states  : 26.73
  4 byte states  : 142.89
[ Number of patterns truncated to 20 bytes: 690 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}".
Decoding Ethernet

    === Initialization Complete ===

  -*> Snort! <*-
Version 2.9.15-WIN32 GRE (Build 7)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.3

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=4920)

 10:46 PM
 4/17/2022
```

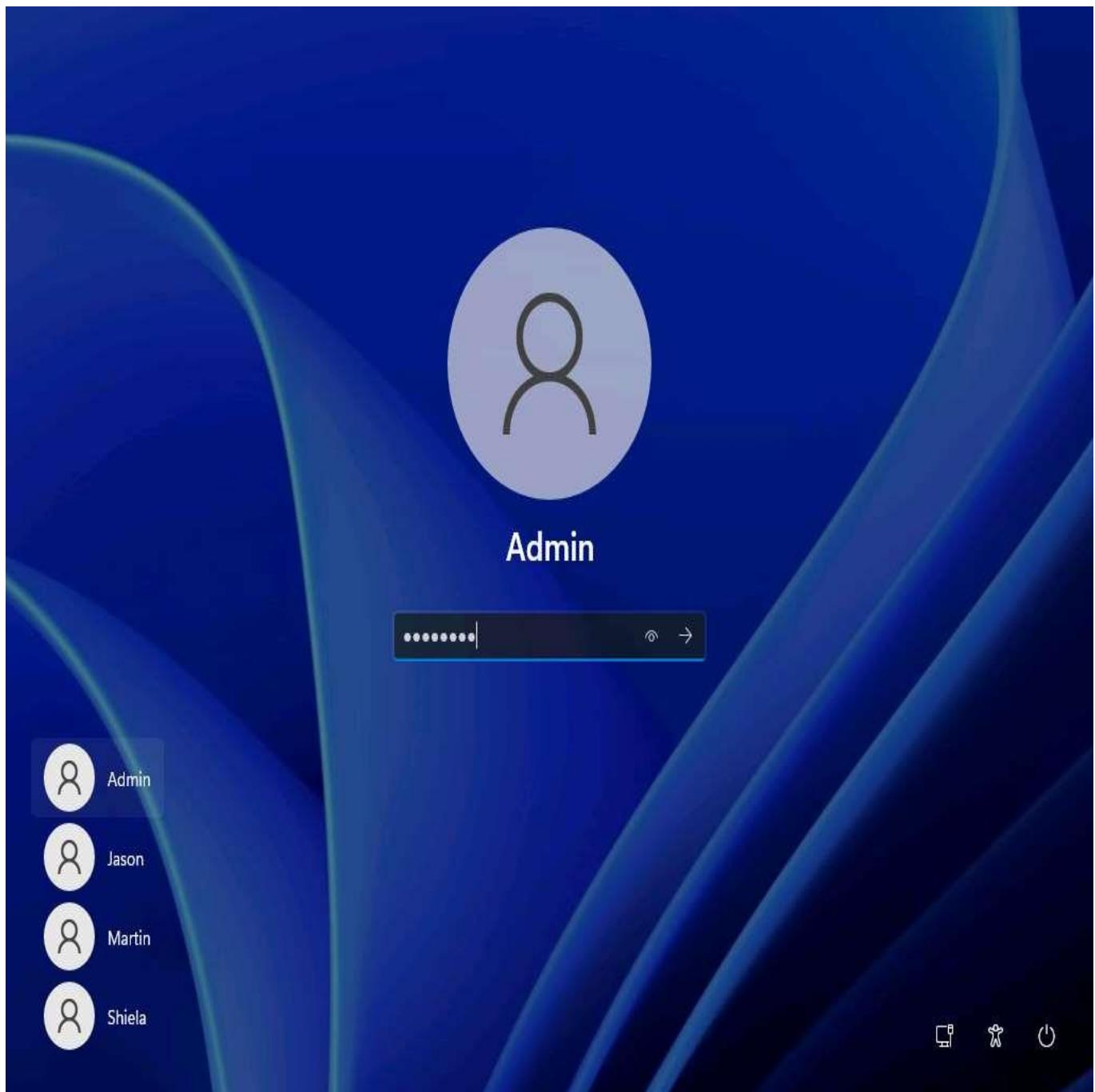
62. After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.
63. Leave the Snort command prompt running.
64. Attack your own machine, and check whether Snort detects it or not.
65. Now, click on **Windows 11** to switch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

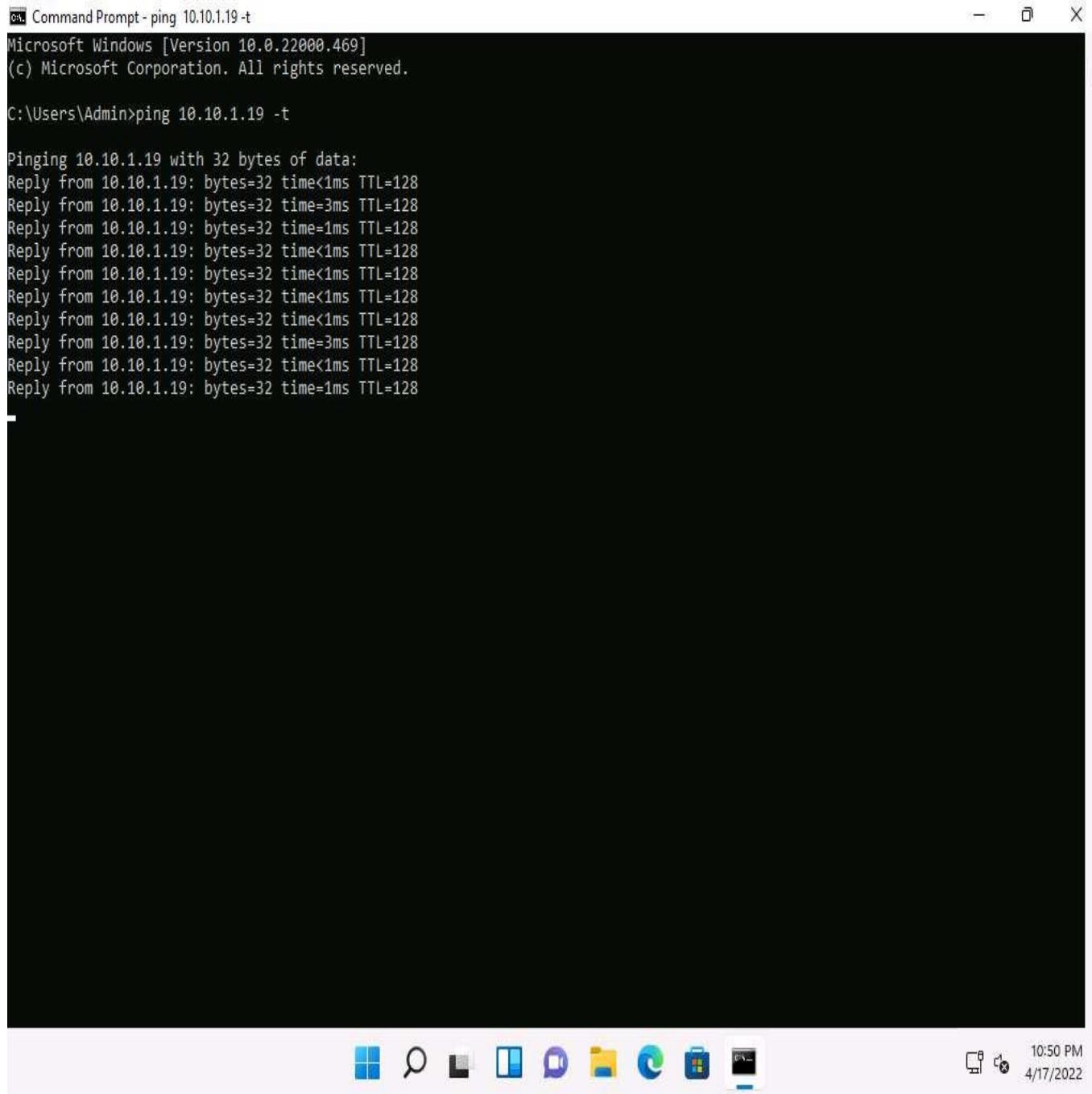
Alternatively, you can also click **Pa\$\$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

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.



Command Prompt - ping 10.10.1.19 -t
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Admin>ping 10.10.1.19 -t

Pinging 10.10.1.19 with 32 bytes of data:
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time=3ms TTL=128
Reply from 10.10.1.19: bytes=32 time=1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time=3ms TTL=128
Reply from 10.10.1.19: bytes=32 time=1ms TTL=128
Reply from 10.10.1.19: bytes=32 time<1ms TTL=128
Reply from 10.10.1.19: bytes=32 time=1ms TTL=128

68. Click [Windows Server 2019](#) to return to the **Windows Server 2019** machine. Observe that Snort triggers an alarm, as shown in the screenshot:

```
Administrator: Command Prompt - snort -i1 -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii
0.1.11 -> 10.10.1.19
04/17-22:50:34.749780 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:35.785506 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:36.780277 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:37.798883 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:38.815089 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:39.831941 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:40.844237 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:41.856829 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:42.870051 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:43.886077 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:44.895807 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:45.909162 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:46.921596 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:47.939499 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:48.942293 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:49.946613 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:50.962505 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:51.977852 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:52.993919 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:54.002240 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
04/17-22:50:55.013008 [**] [1:472:7] ICMP-INFO PING [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 10.1
0.1.11 -> 10.10.1.19
```

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

```
Administrator: Command Prompt
Memory used for smb2 processing: 0
Maximum memory used for smb2 processing: 0
SMB2 command requests/responses processed
  smb2 create      : 0
  smb2 write       : 0
  smb2 read        : 0
  smb2 set info    : 0
  smb2 tree connect: 0
  smb2 tree disconnect: 0
  smb2 close       : 0
=====
SSL Preprocessor:
  SSL packets decoded: 9
    Client Hello: 0
    Server Hello: 2
    Certificate: 2
    Server Done: 2
  Client Key Exchange: 0
  Server Key Exchange: 0
    Change Cipher: 2
      Finished: 0
  Client Application: 0
  Server Application: 2
    Alert: 0
  Unrecognized records: 5
  Completed handshakes: 0
  Bad handshakes: 0
    Sessions ignored: 1
  Detection disabled: 1
=====
SIP Preprocessor Statistics
  Total sessions: 0
=====
IMAP Preprocessor Statistics
  Total sessions          : 0
  Max concurrent sessions: 0
=====
POP Preprocessor Statistics
  Total sessions          : 0
  Max concurrent sessions: 0
=====
Snort exiting
C:\Snort\bin>
```

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.

```
C:\Snort\log\10.10.1.11\ICMP_ECHO.ids - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf cmp-info.rules ICMP_ECHO.ids

1 [**] ICMP-INFO PING [**]
2 04/17-22:50:16.501730 10.10.1.11 -> 10.10.1.19
3 ICMP TTL:128 TOS:0x0 ID:15042 IpLen:20 DgmLen:60
4 Type:8 Code:0 ID:1 Seq:1 ECHO
5 ++++++=====
6
7 [**] ICMP-INFO PING [**]
8 04/17-22:50:17.509326 10.10.1.11 -> 10.10.1.19
9 ICMP TTL:128 TOS:0x0 ID:15043 IpLen:20 DgmLen:60
10 Type:8 Code:0 ID:1 Seq:2 ECHO
11 ++++++=====
12
13 [**] ICMP-INFO PING [**]
14 04/17-22:50:18.524903 10.10.1.11 -> 10.10.1.19
15 ICMP TTL:128 TOS:0x0 ID:15044 IpLen:20 DgmLen:60
16 Type:8 Code:0 ID:1 Seq:3 ECHO
17 ++++++=====
18
19 [**] ICMP-INFO PING [**]
20 04/17-22:50:19.538779 10.10.1.11 -> 10.10.1.19
21 ICMP TTL:128 TOS:0x0 ID:15046 IpLen:20 DgmLen:60
22 Type:8 Code:0 ID:1 Seq:4 ECHO
23 ++++++=====
24
25 [**] ICMP-INFO PING [**]
26 04/17-22:50:20.553686 10.10.1.11 -> 10.10.1.19
27 ICMP TTL:128 TOS:0x0 ID:15048 IpLen:20 DgmLen:60
28 Type:8 Code:0 ID:1 Seq:5 ECHO
29 ++++++=====
30
31 [**] ICMP-INFO PING [**]
32 04/17-22:50:21.567245 10.10.1.11 -> 10.10.1.19
33 ICMP TTL:128 TOS:0x0 ID:15049 IpLen:20 DgmLen:60
34 Type:8 Code:0 ID:1 Seq:6 ECHO
35 ++++++=====
36
37 [**] ICMP-INFO PING [**]
38 04/17-22:50:22.582789 10.10.1.11 -> 10.10.1.19
```

Normal text file length: 13,136 lines: 331 Ln:1 Col:1 Pos:1 Windows (CR LF) UTF-8 INS

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

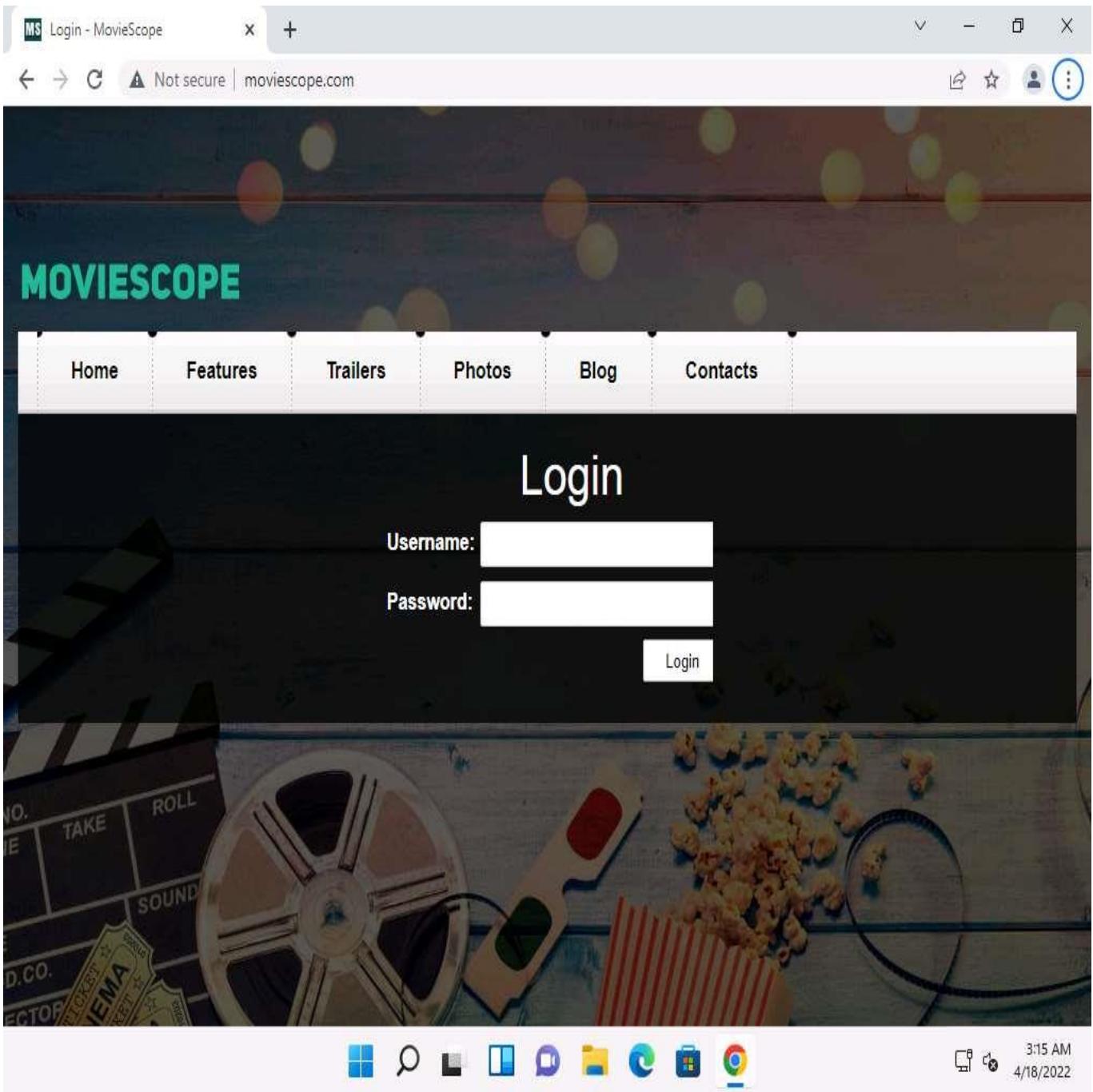
ZoneAlarm FREE Firewall blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting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

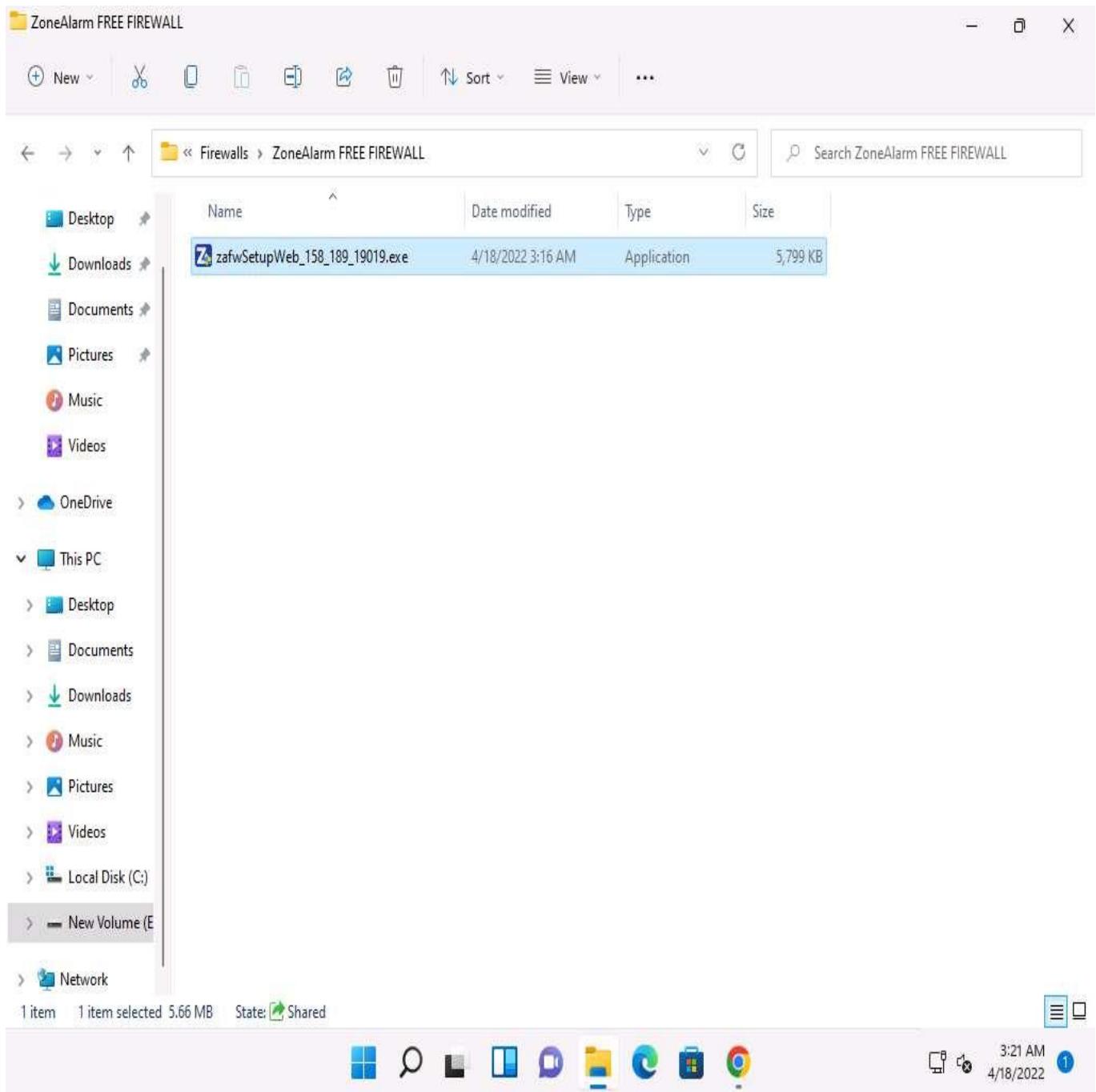
1. Before starting this task, we will browse an unwanted website in the **Windows 11** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

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

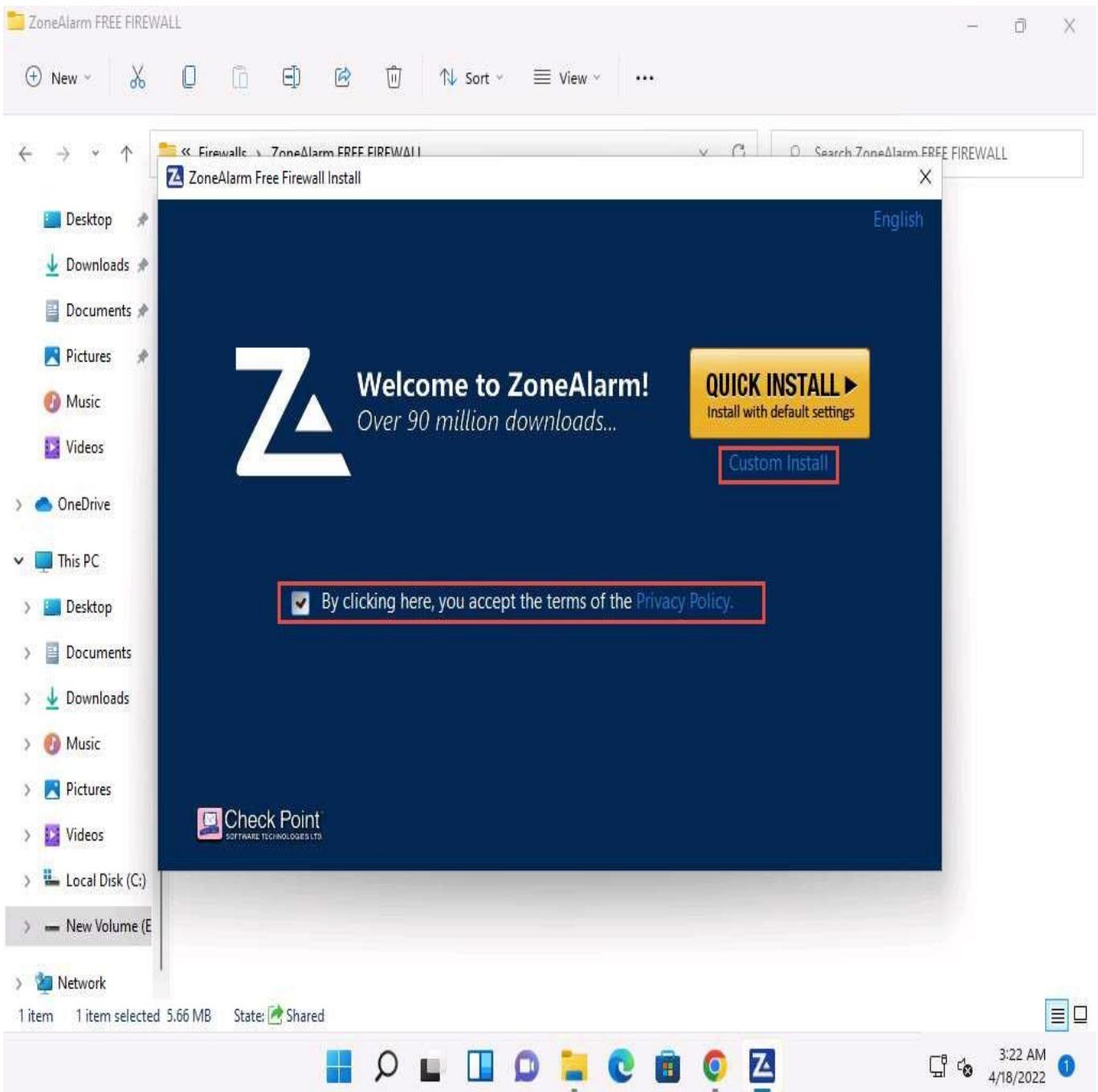
2. Click **Windows 11** to switch to the **Windows 11** machine.
3. Open any browser (here, **Google Chrome**) and place the cursor in the address bar, type **www.moviescope.com** and press **Enter**.
4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 11** machine.
5. In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



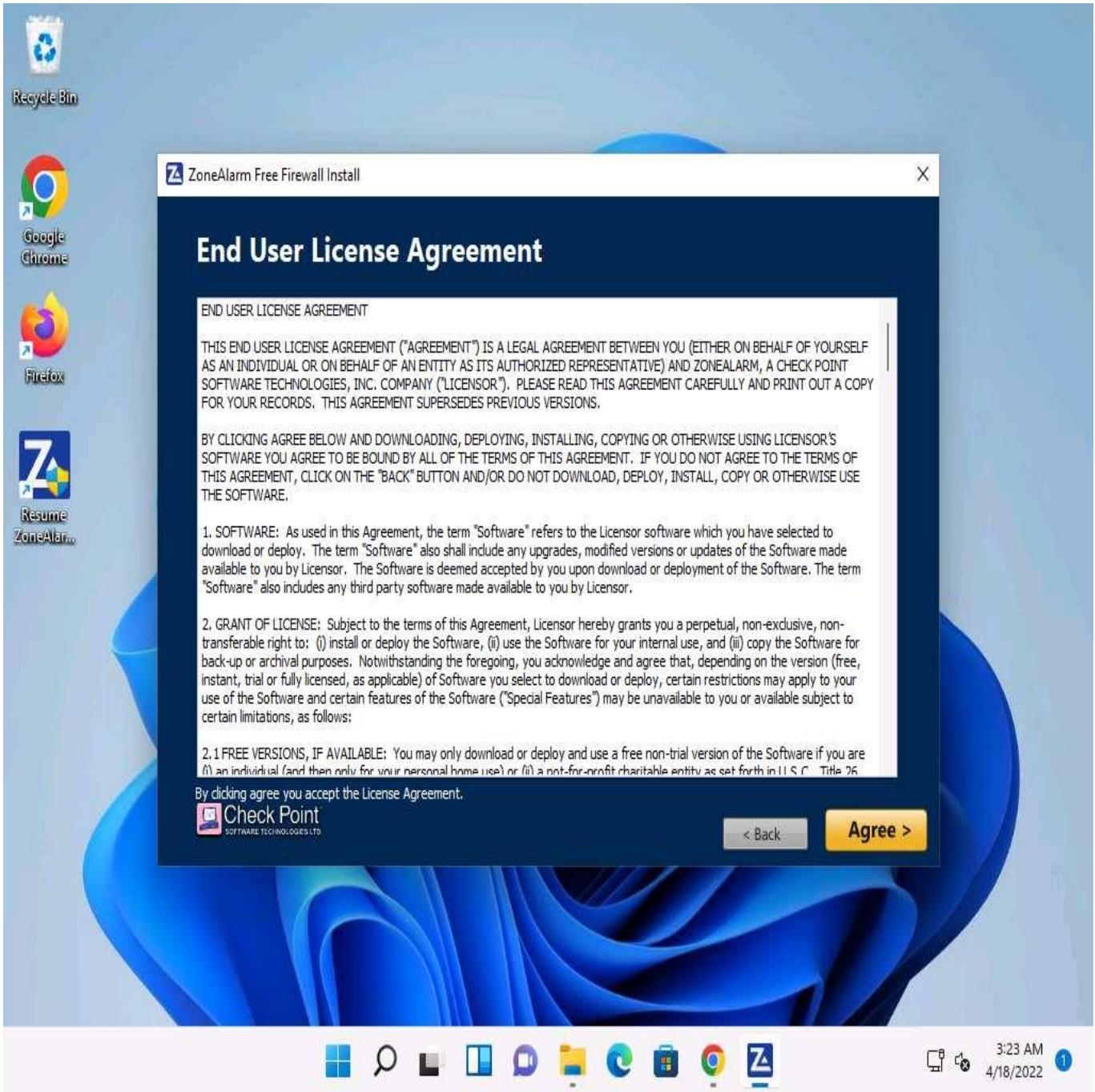
6. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL** and double-click **zafwSetupWeb_158_189_19019.exe** to install ZoneAlarm FREE FIREWALL.



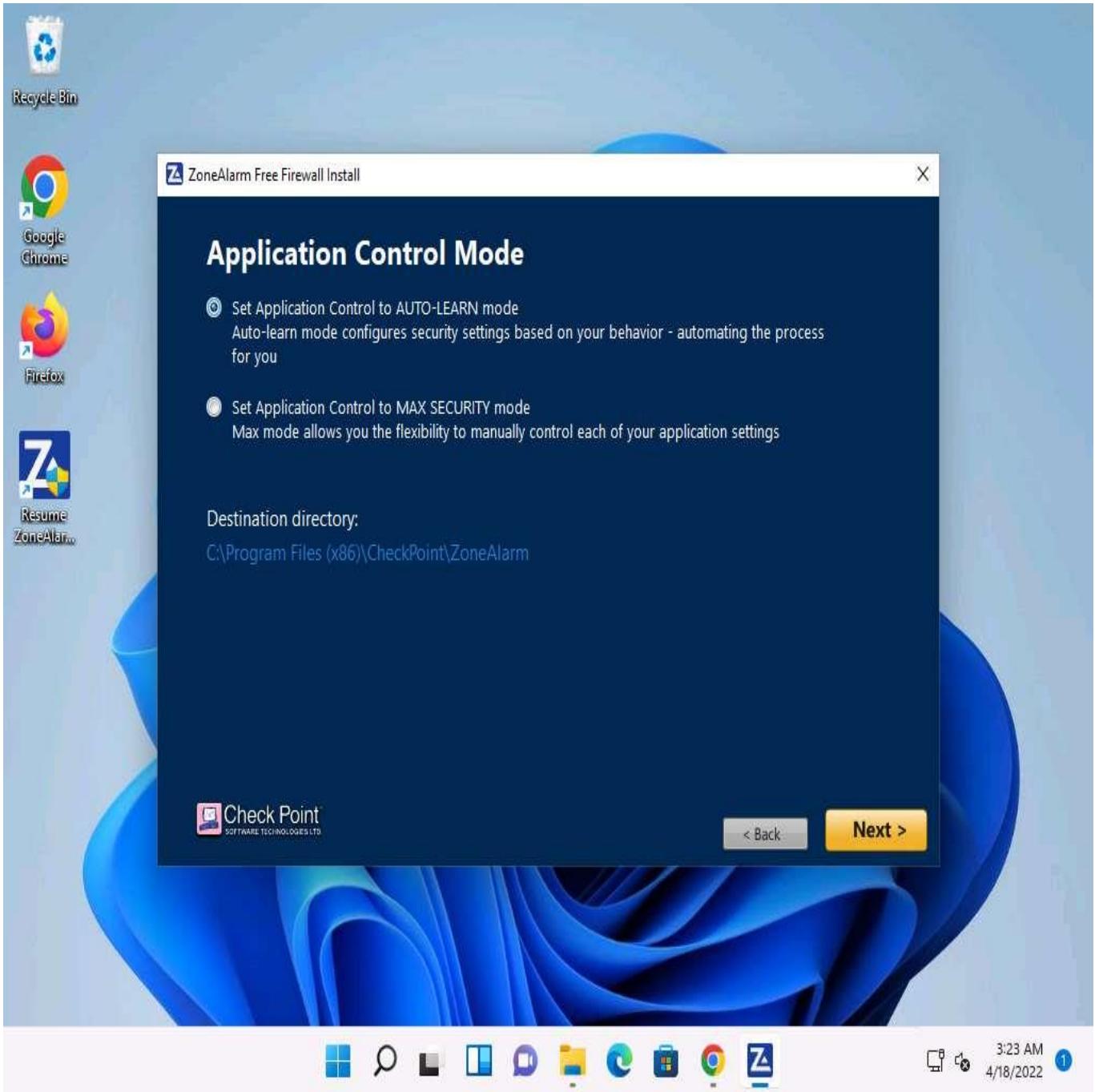
7. If the **User Account Control** pop-up appears, click **Yes**.
8. The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.



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.

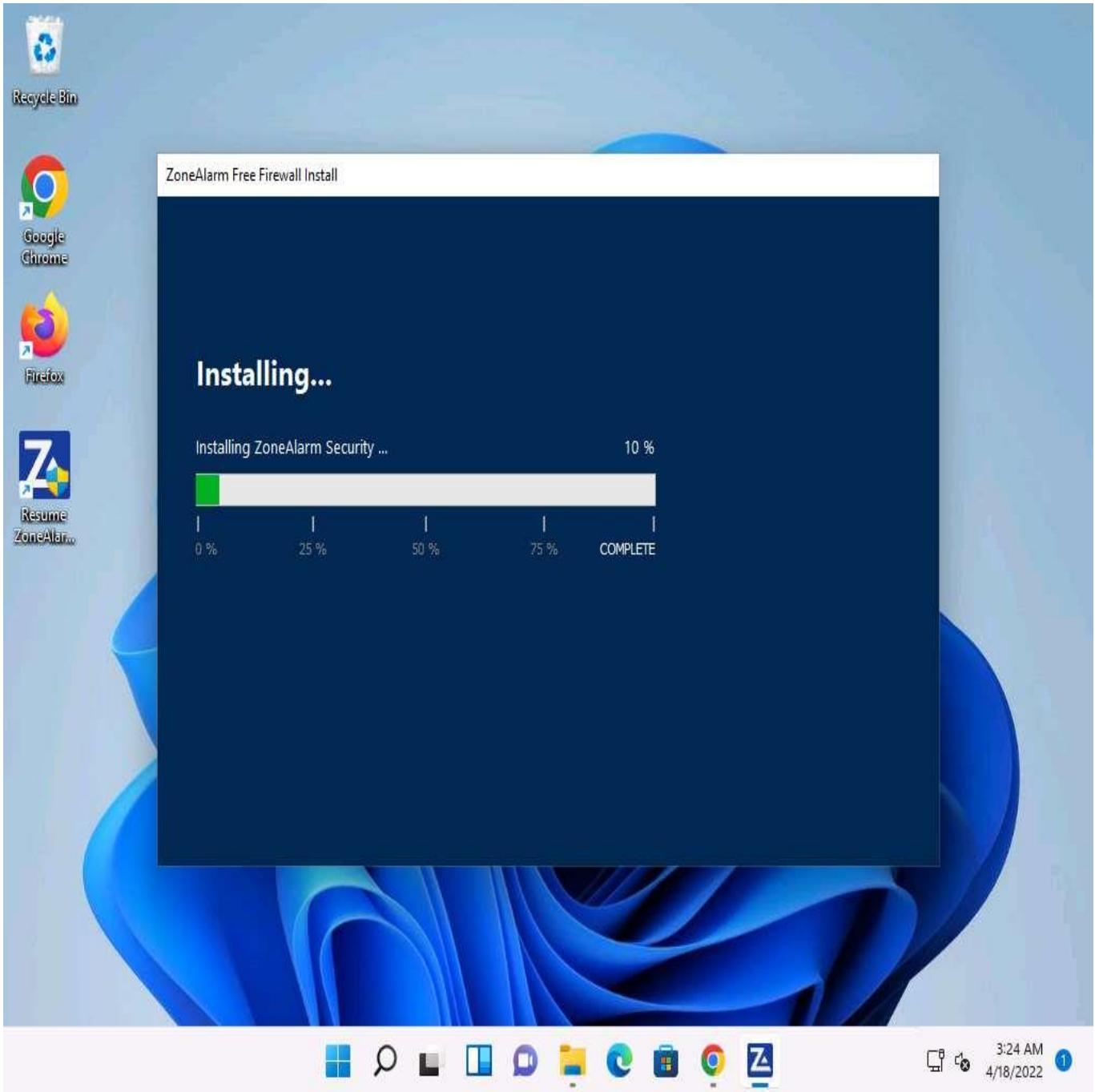


12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

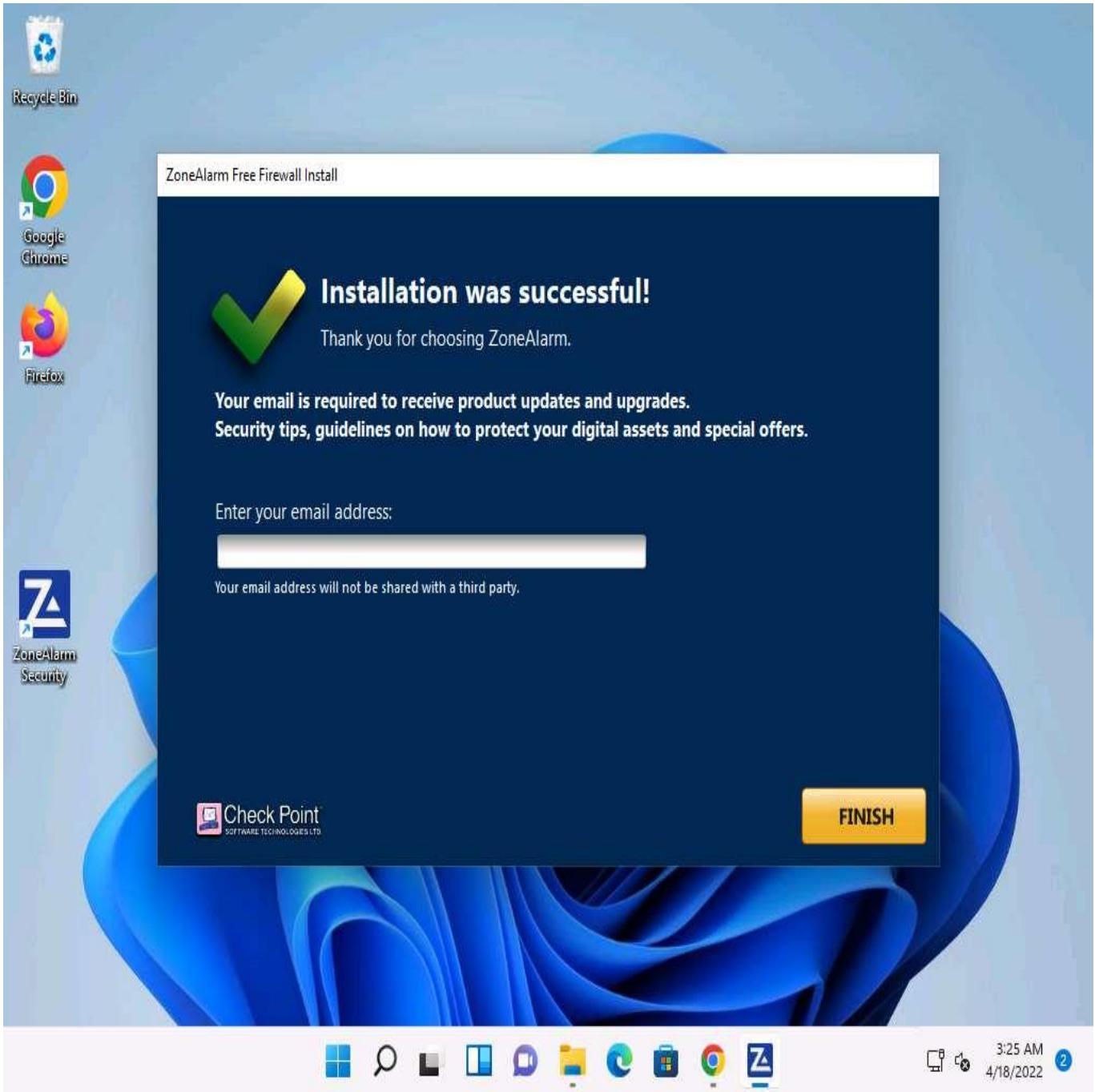
If you wish to enable this option, click Add to Chrome. In this task, we are choosing to skip this option.



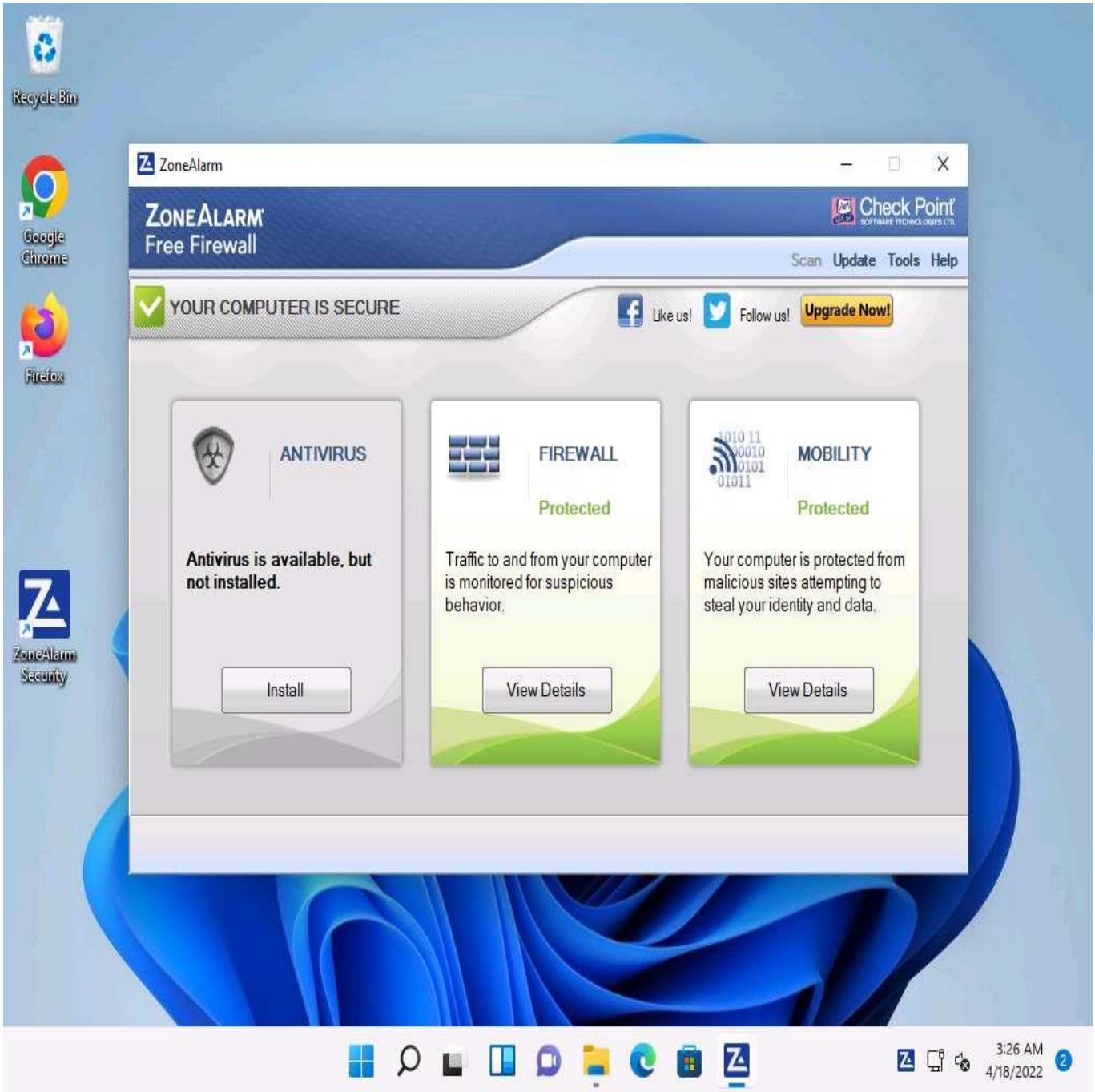
13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.
14. Wait until the installation is completed: this may take a few minutes to install.



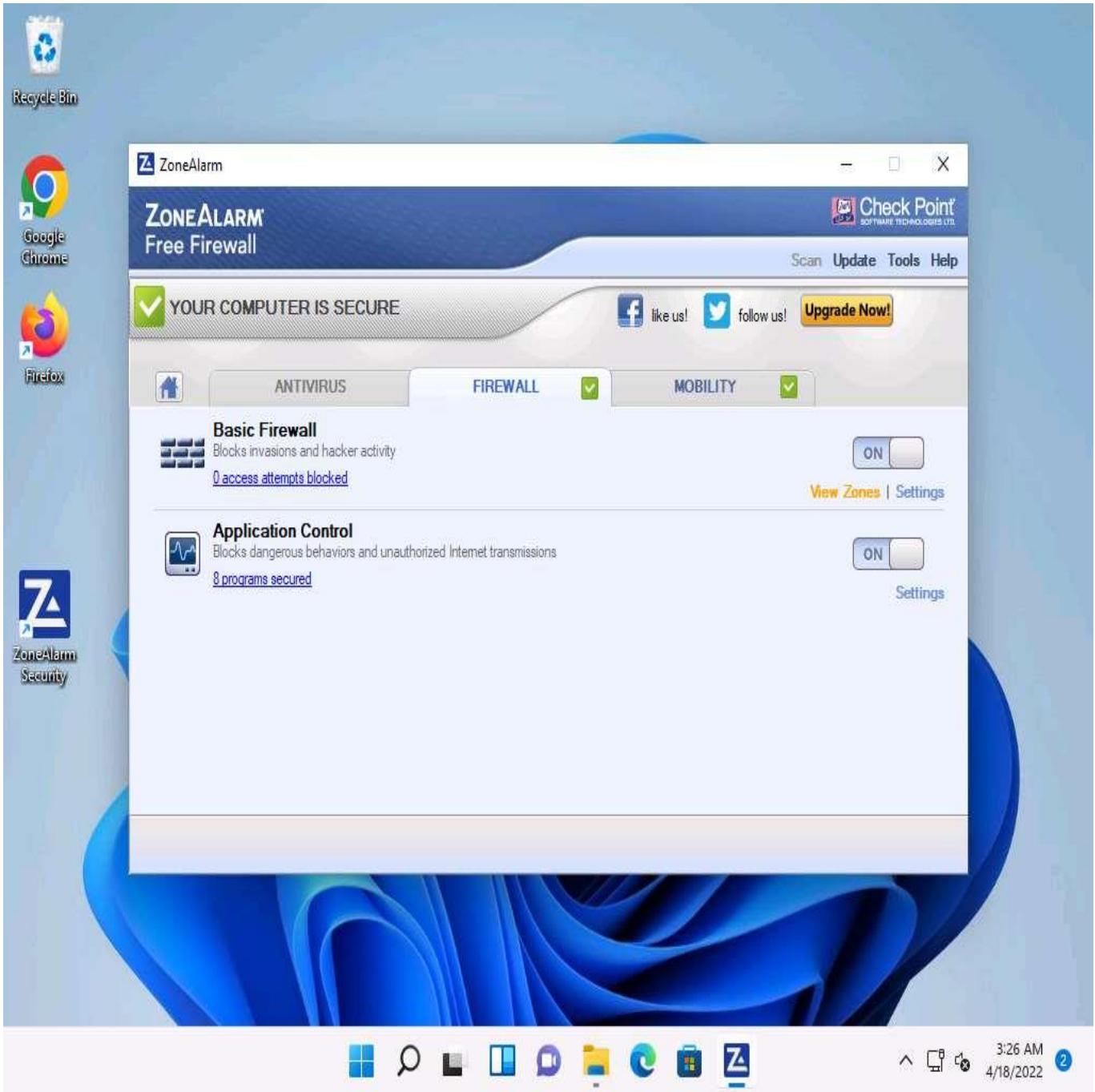
15. The **Installation was Successful!** wizard appears; click **FINISH**.
16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.



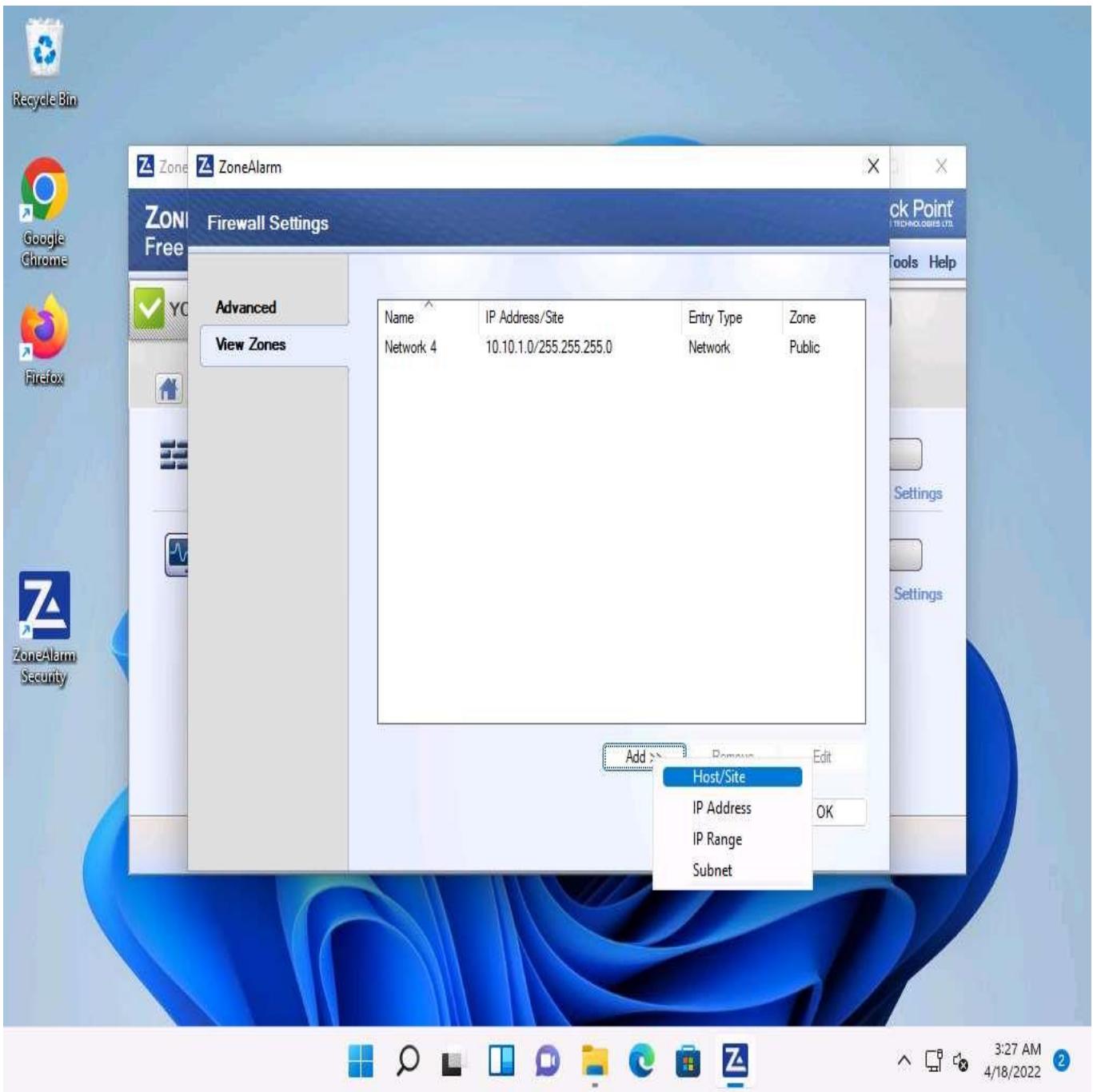
17. The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.



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

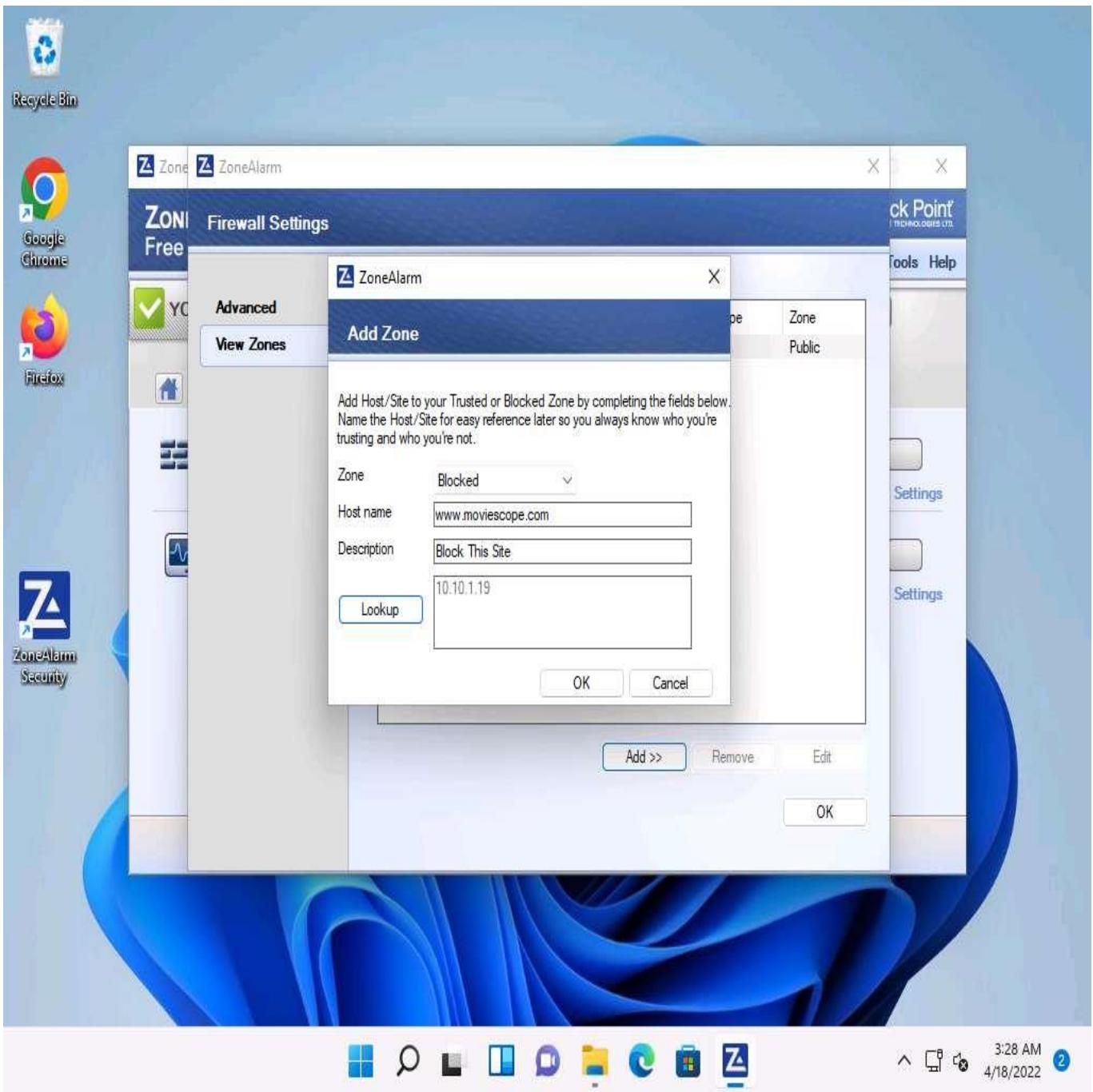


19. The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.

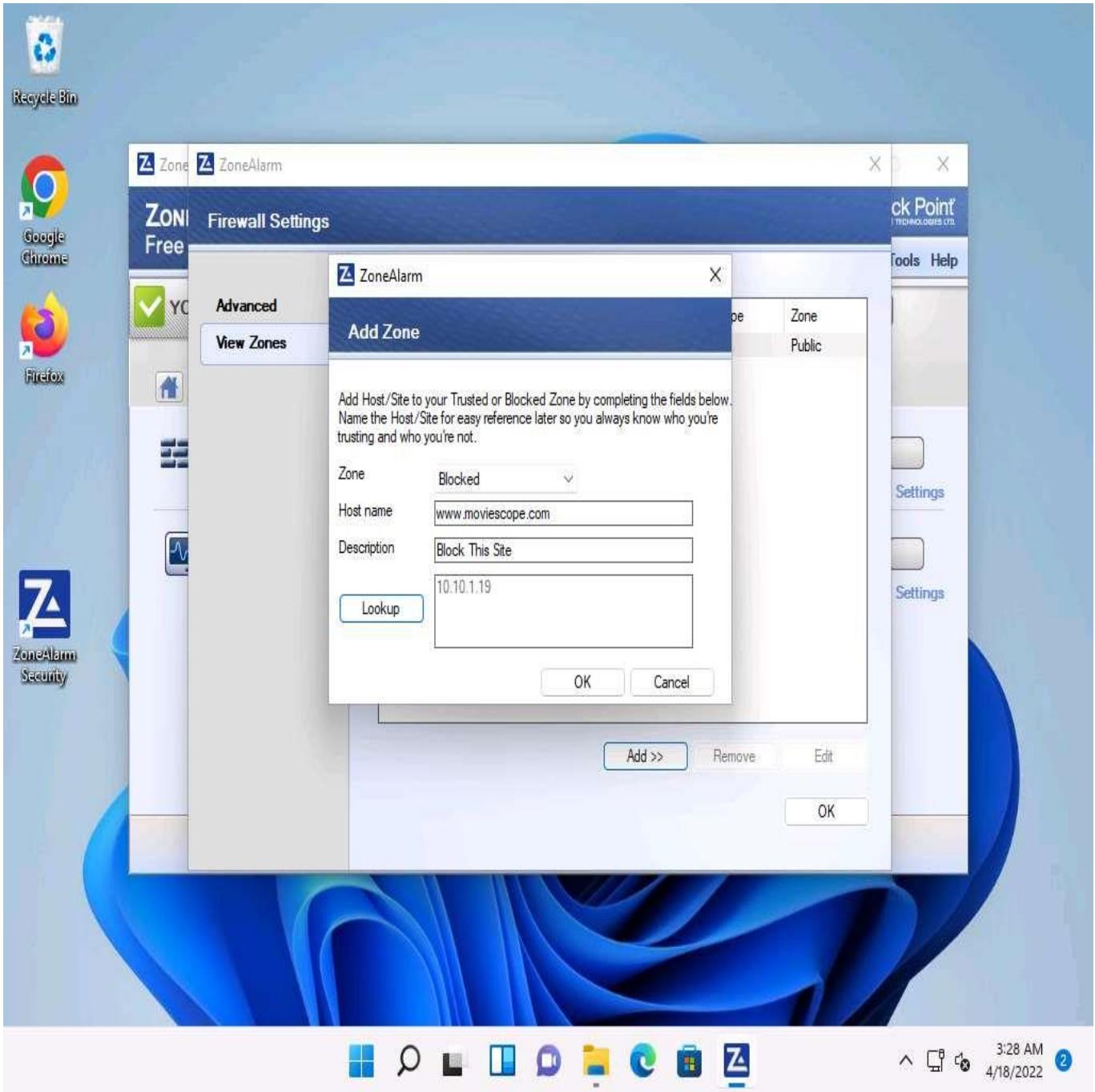


20. The **Add Zone** window appears; choose the following:
 - o Zone: **Blocked**
 - o Hostname: **www.moviescope.com**
 - o Description: **Block This Site**
 - o Click **Lookup**; by doing this, we are blocking unwanted sites from browsing
21. You can provide any site that you wish to block.

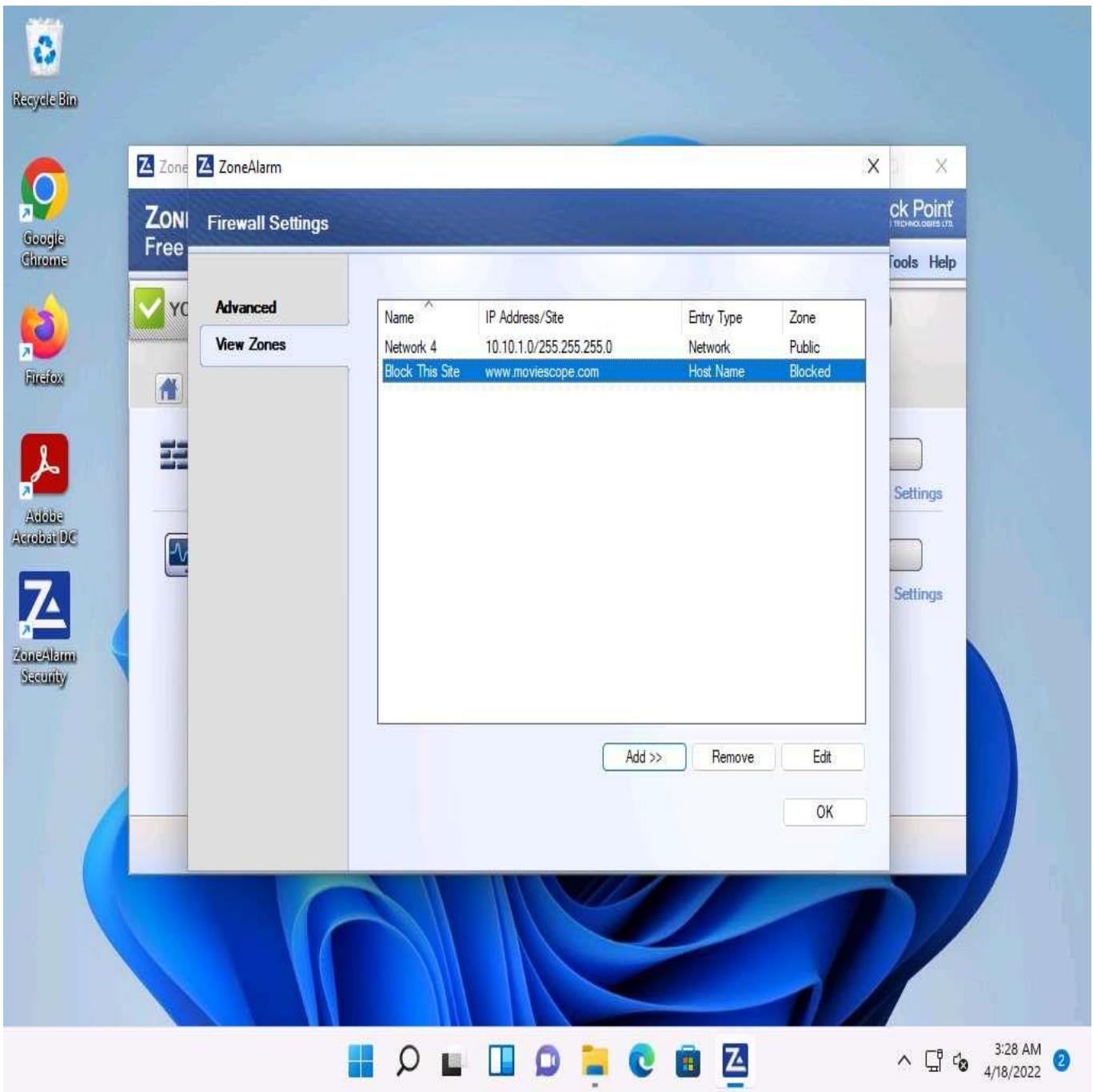
www.moviescope.com is the local website that is configured on Windows Server 2019.



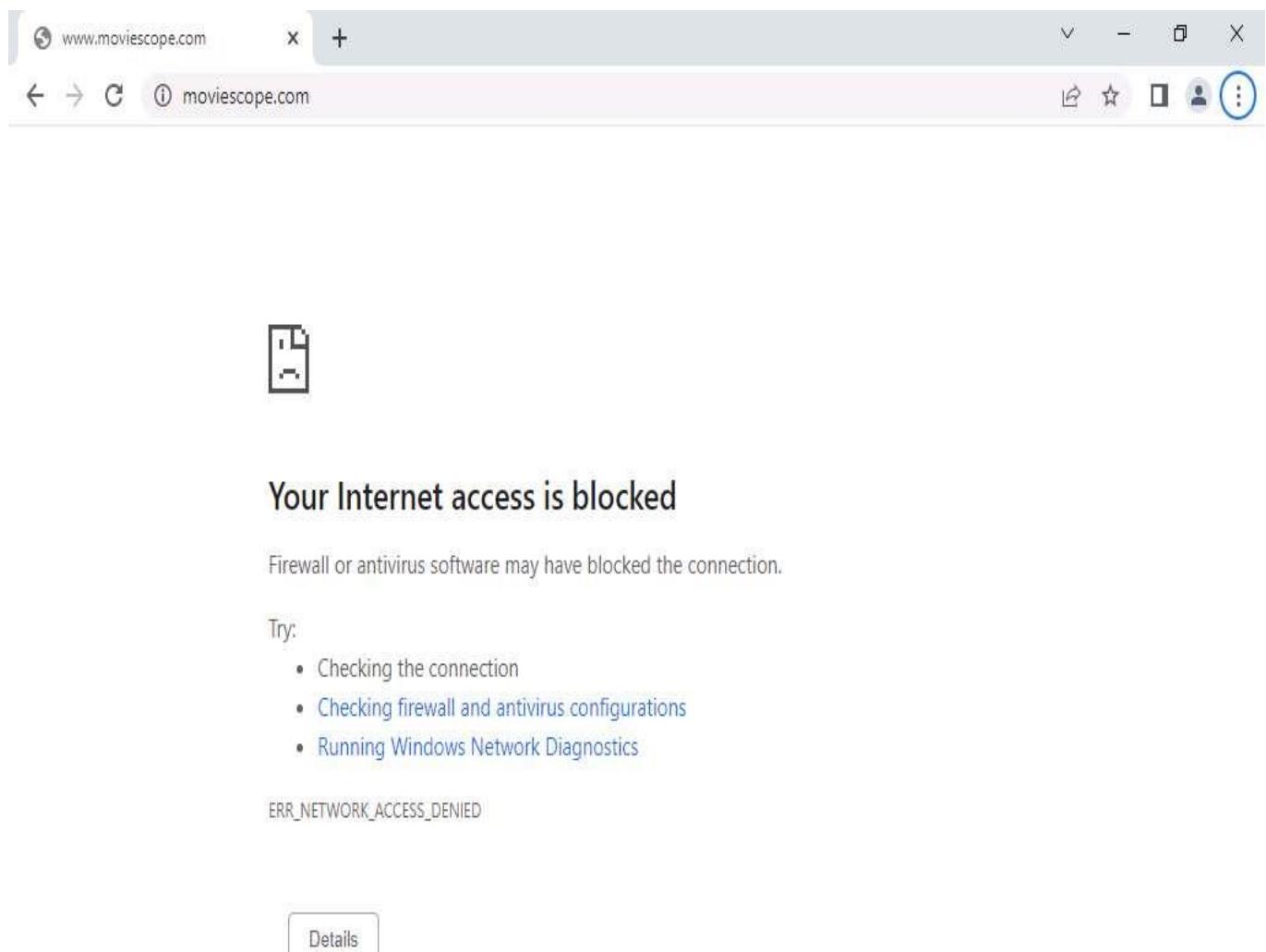
22. As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.



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**.

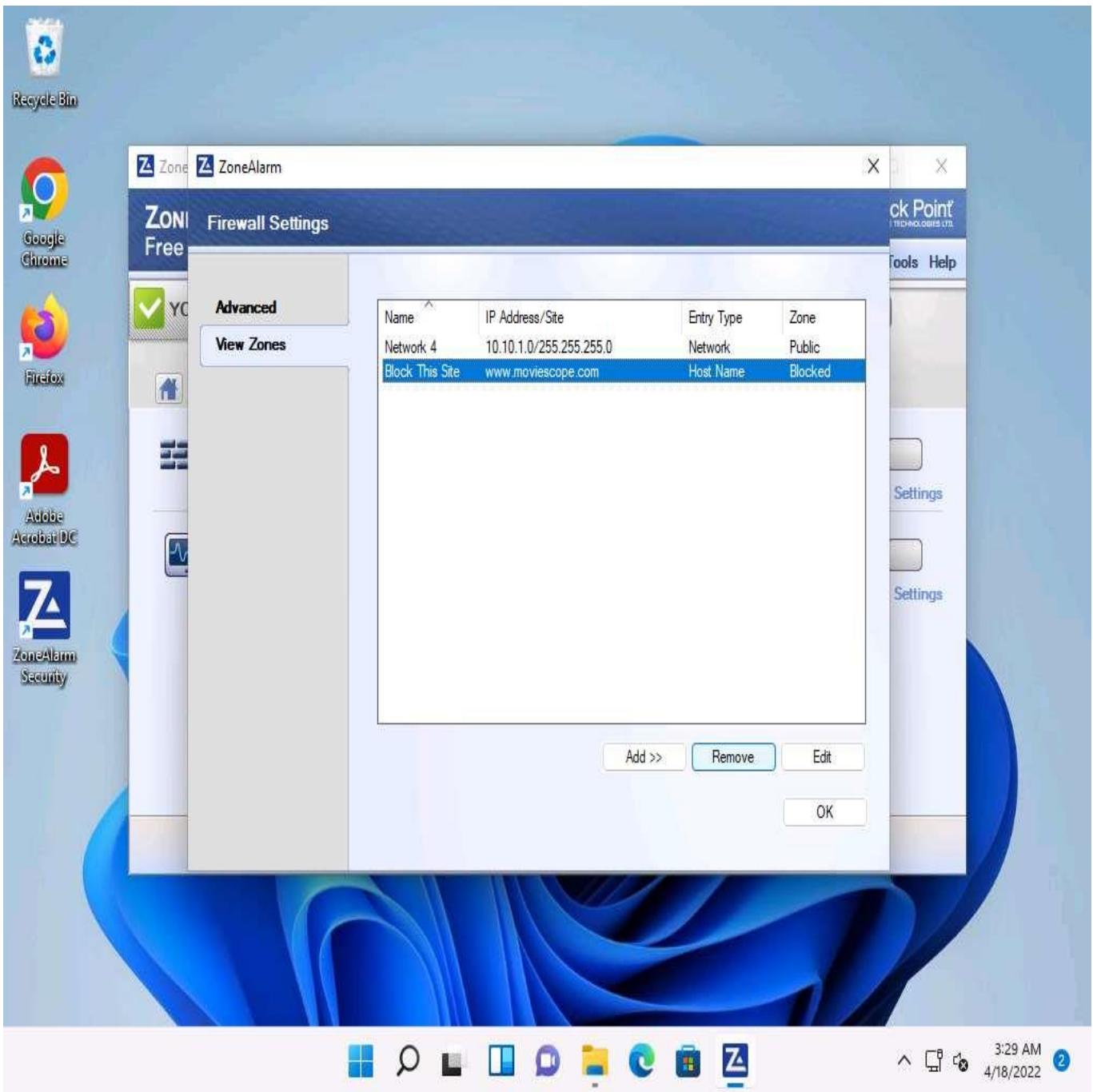


This is how you can block access for unwanted sites from browsing.

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.

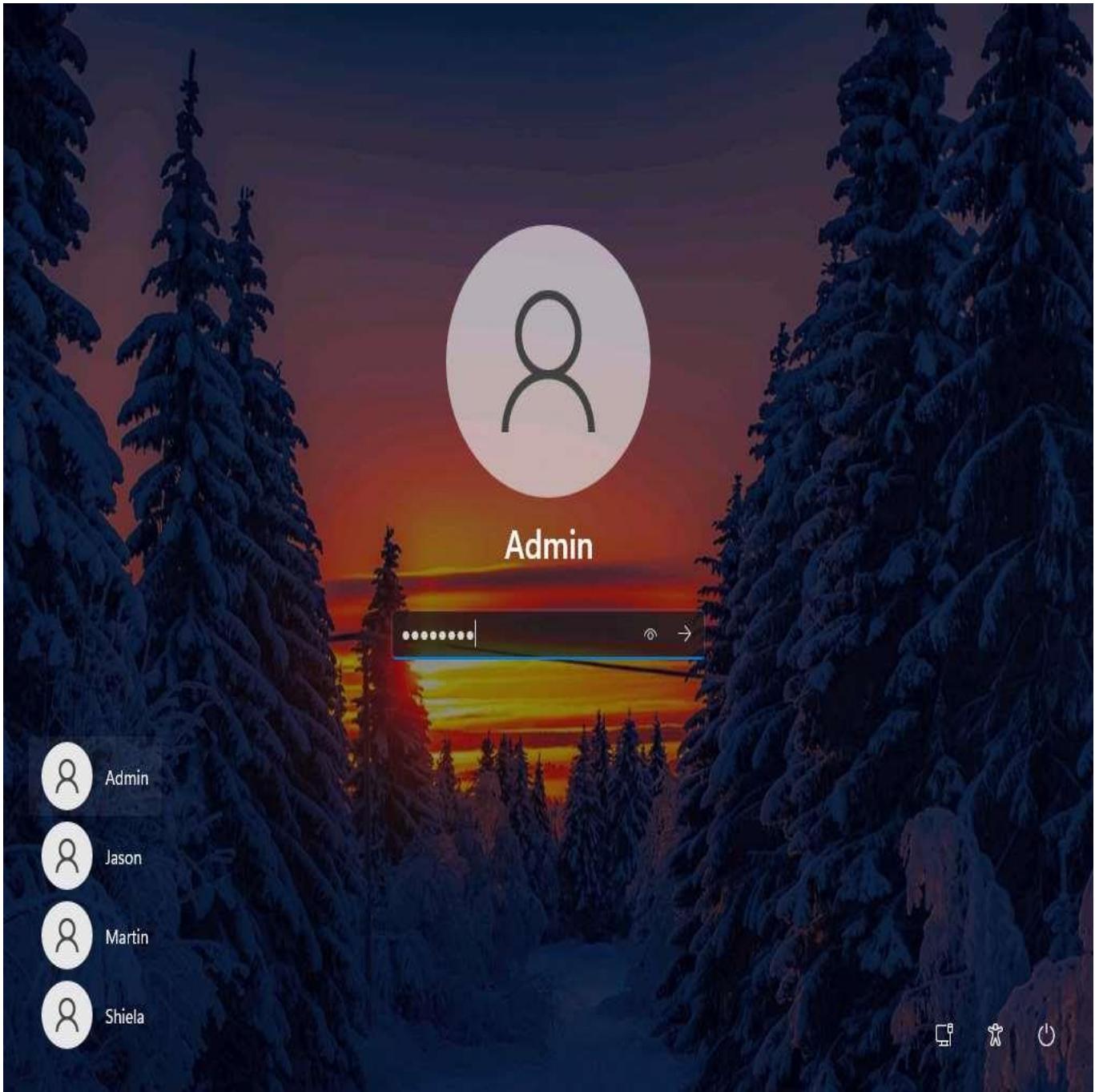


28. Close the ZoneAlarm main window.
29. Click **Show hidden icon** from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.

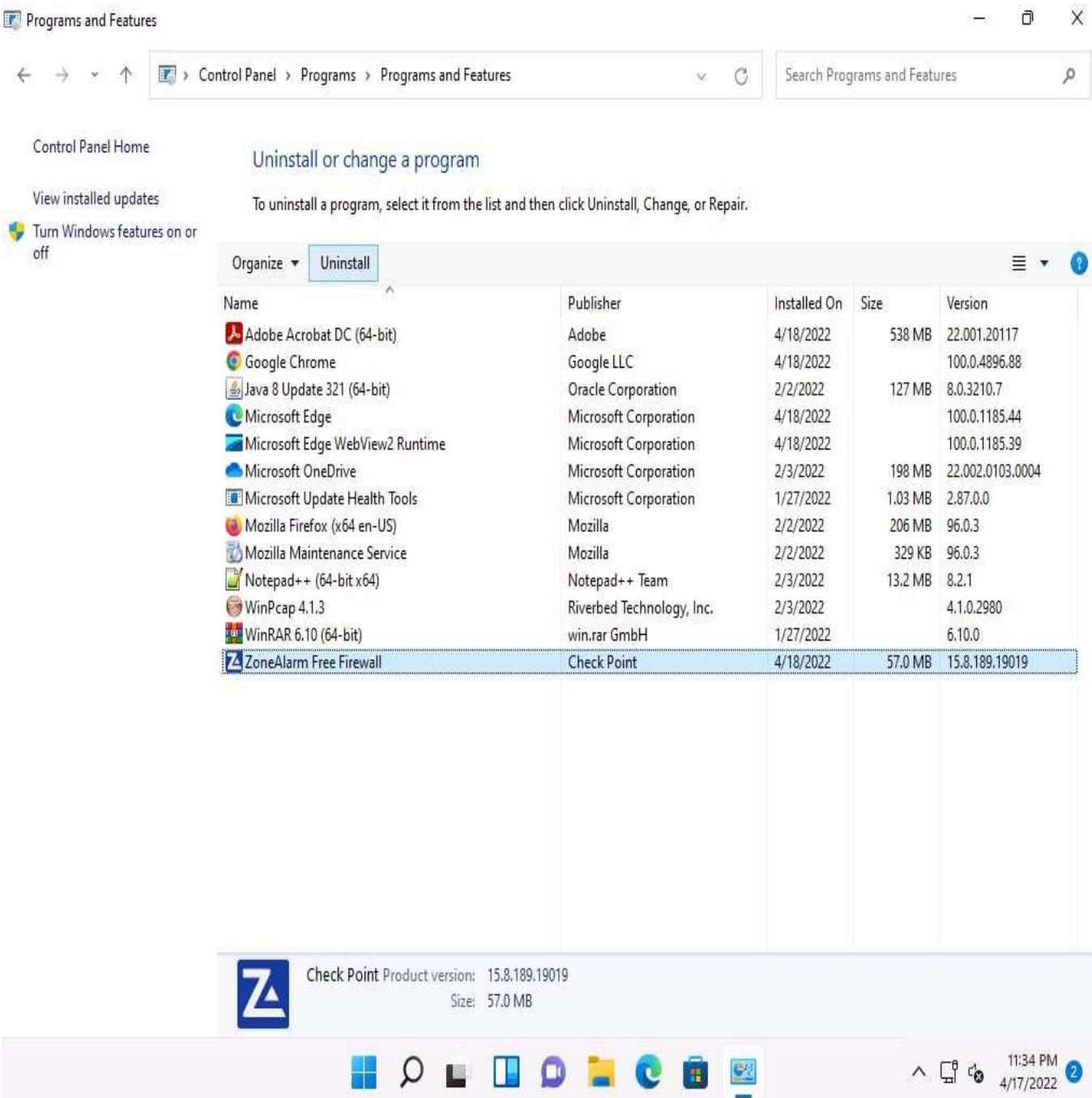


If a **Shut down** pop-up appears, click **Yes**.

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**.
 - o In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left pane of the window
 - o 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**
 - o Again, in the **Windows Defender Firewall** window, click **Advanced settings** link in the left pane
 - o Once the **Windows Defender Firewall with Advanced Security** appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section
 - o 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.
-

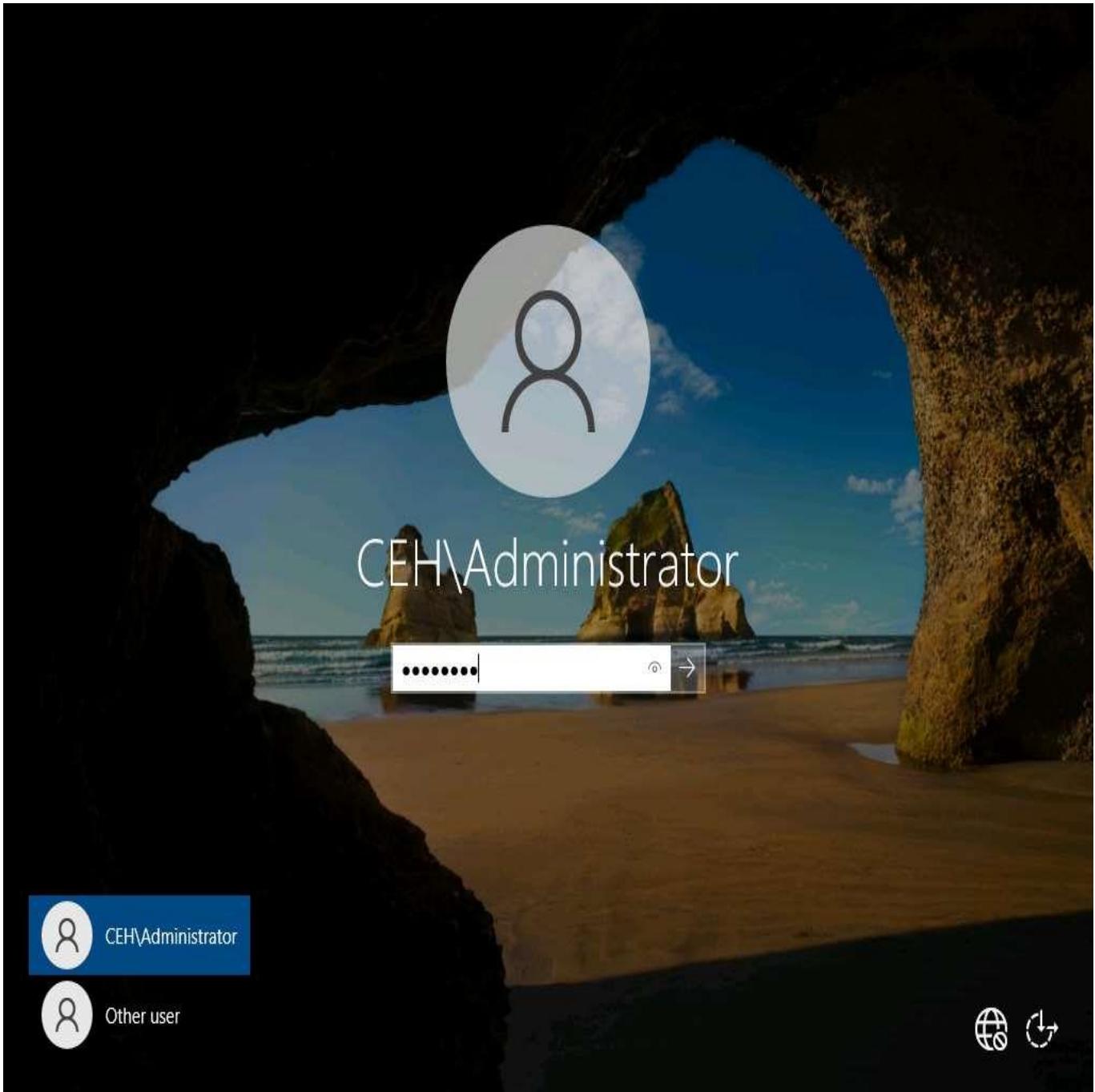
Task 3: Detect Malicious Network Traffic using HoneyBOT

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.

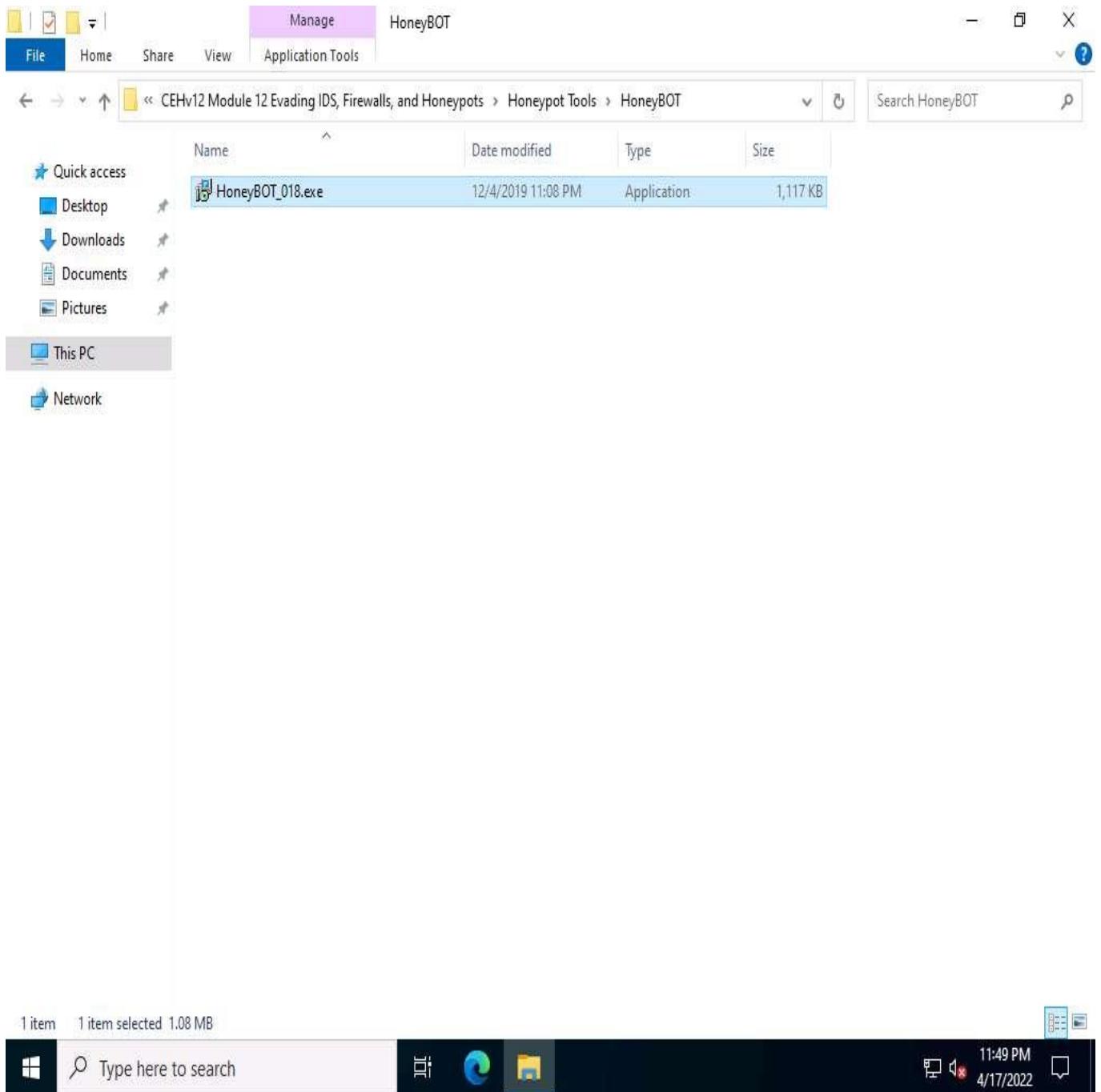
1. Click **Windows Server 2022** to switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Delete** to activate the machine. By default, **CEH\Administrator** user profile is selected, click **Pa\$\$w0rd** to paste the password in the Password field and press **Enter** to login.

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.

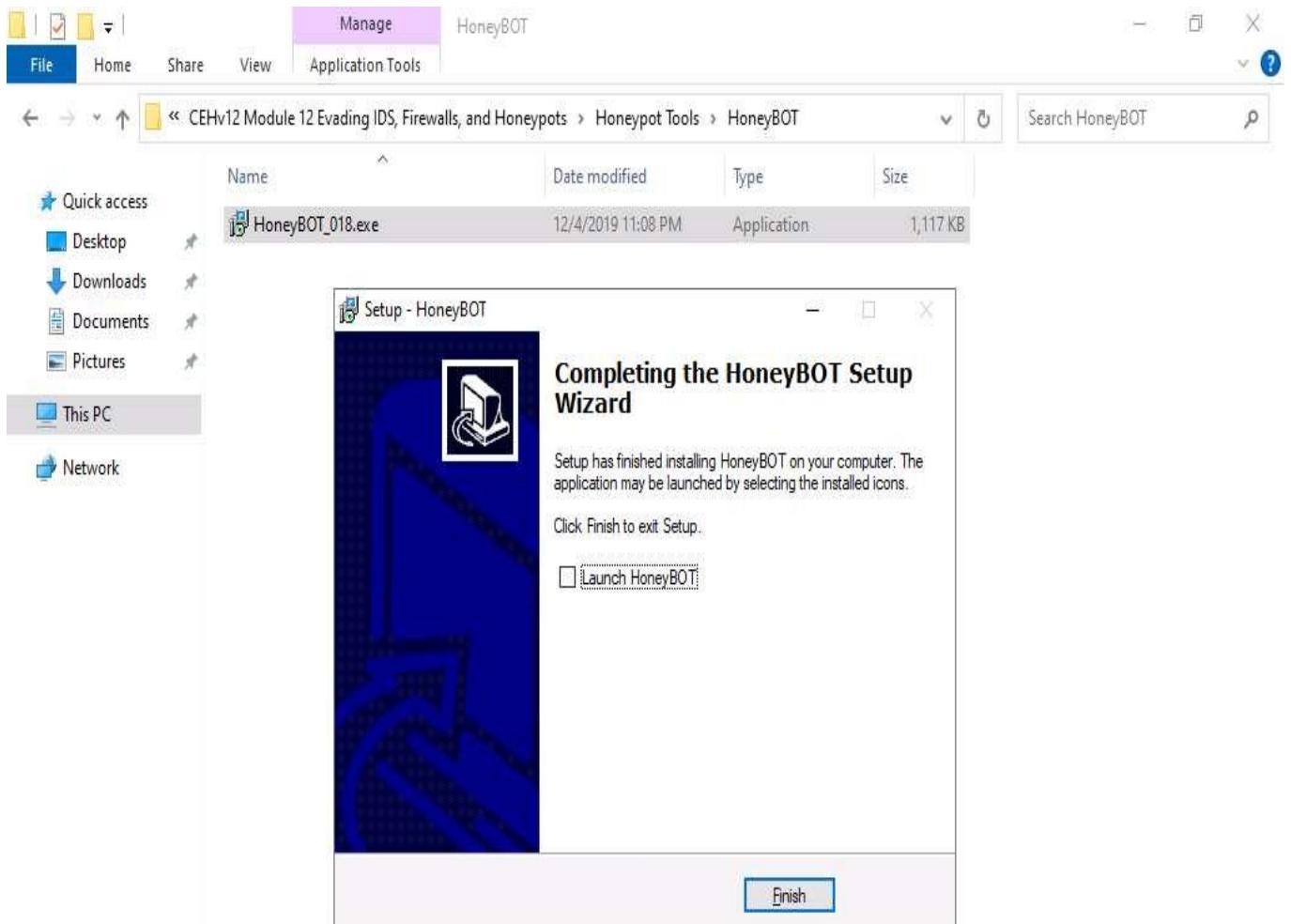


2. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

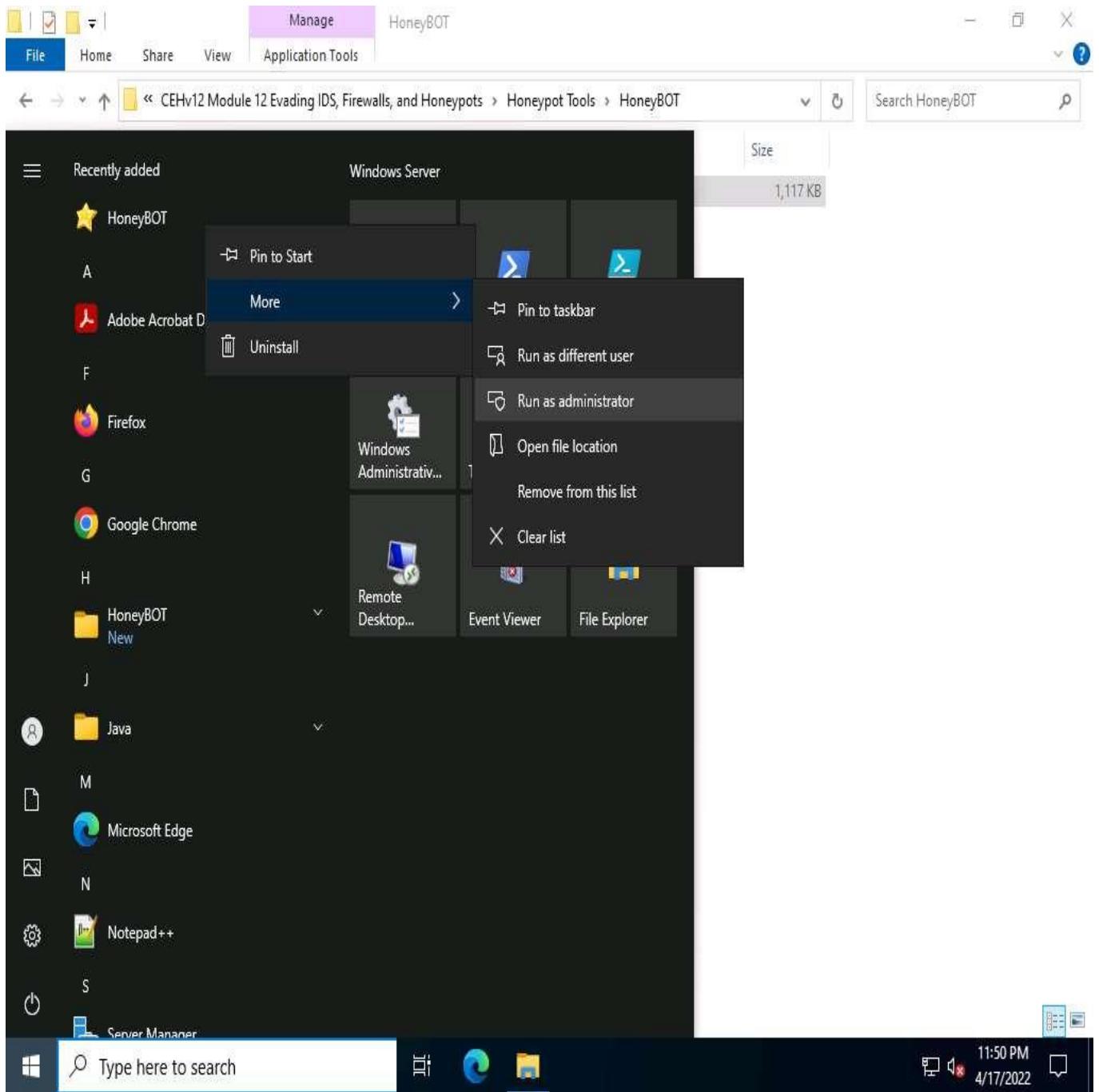
if the **User Account Control** window appears, click **Yes**.



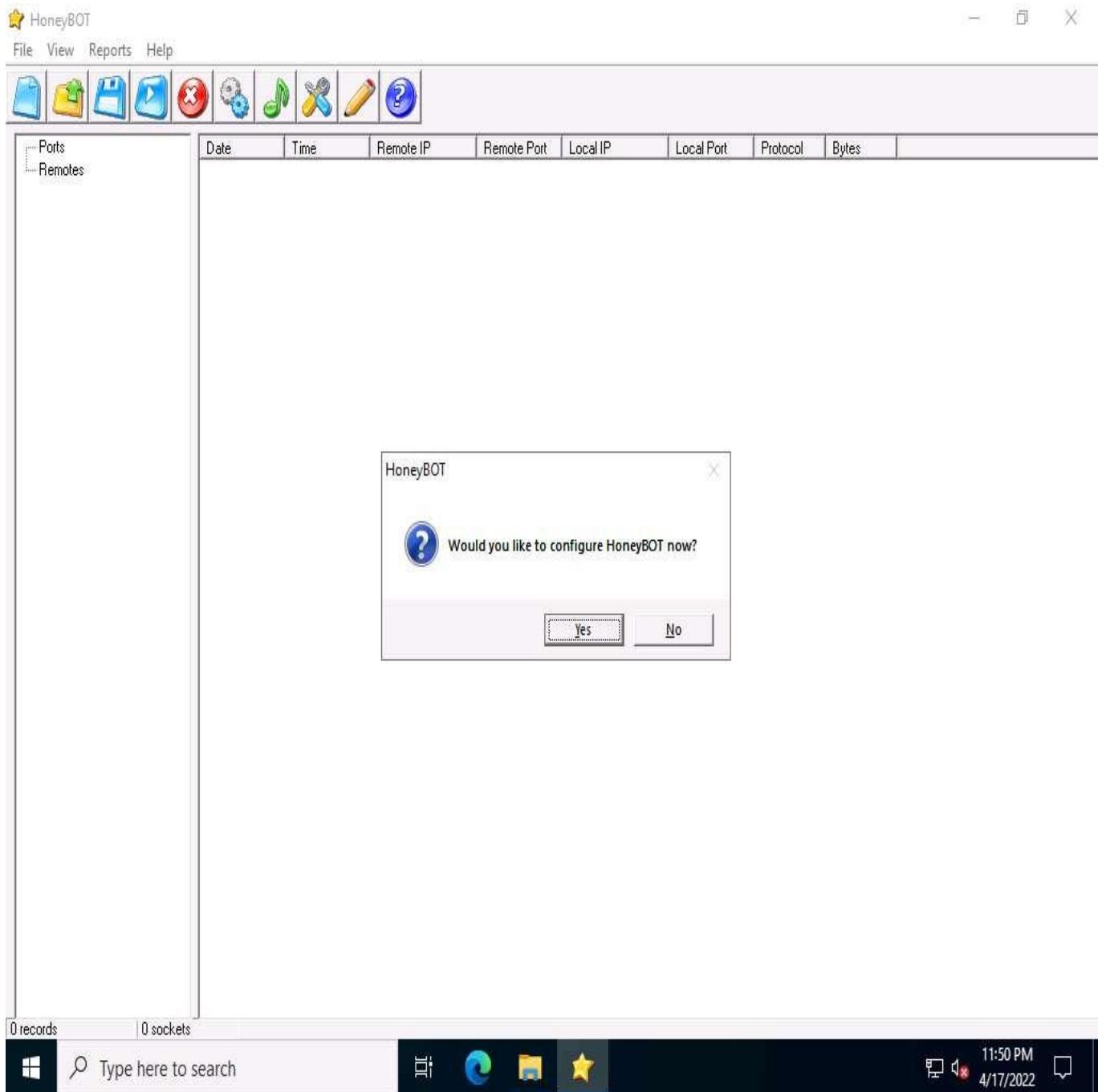
3. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.



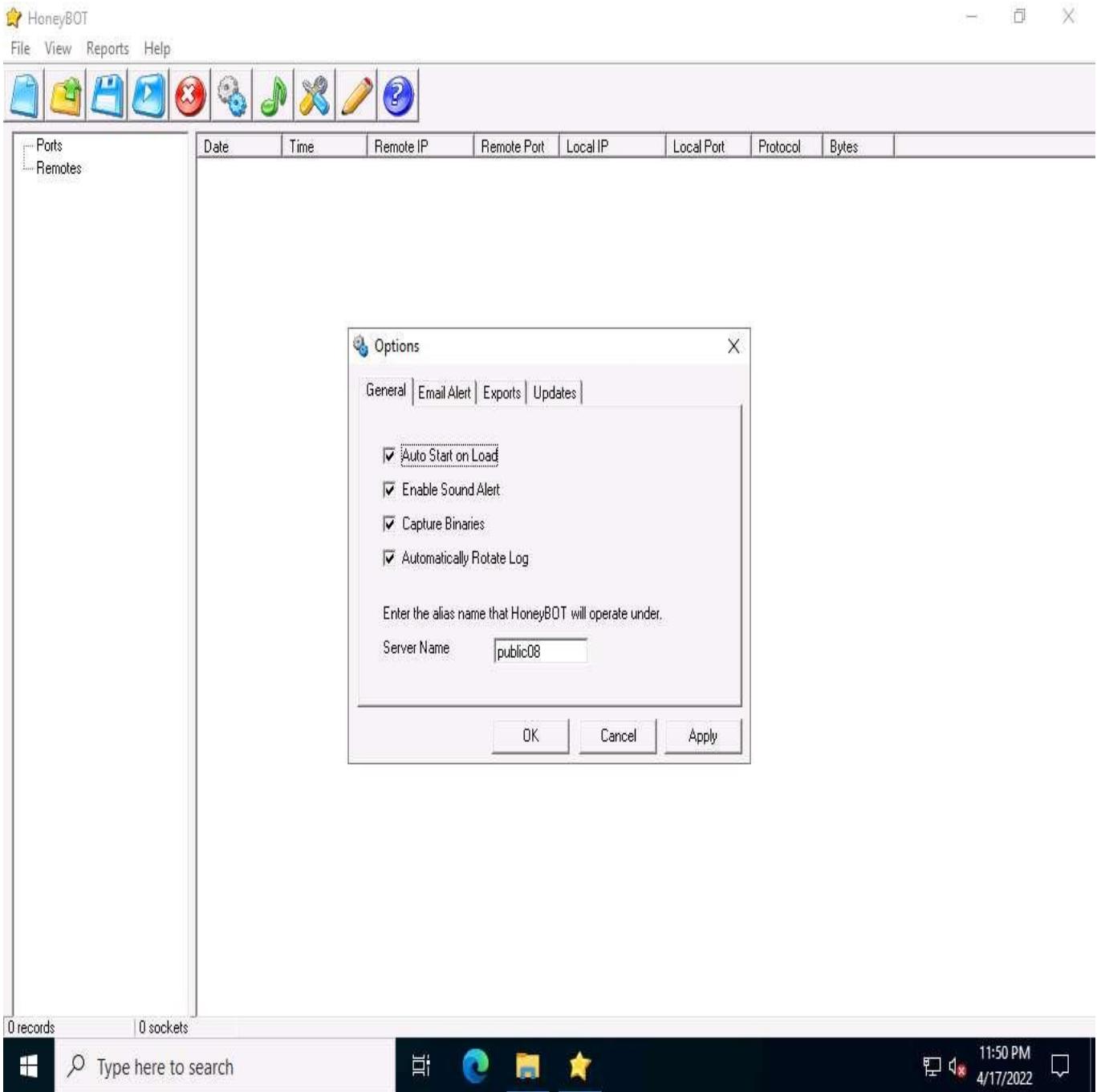
4. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT** --> **More** --> **Run as administrator**, as shown in the screenshot.



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

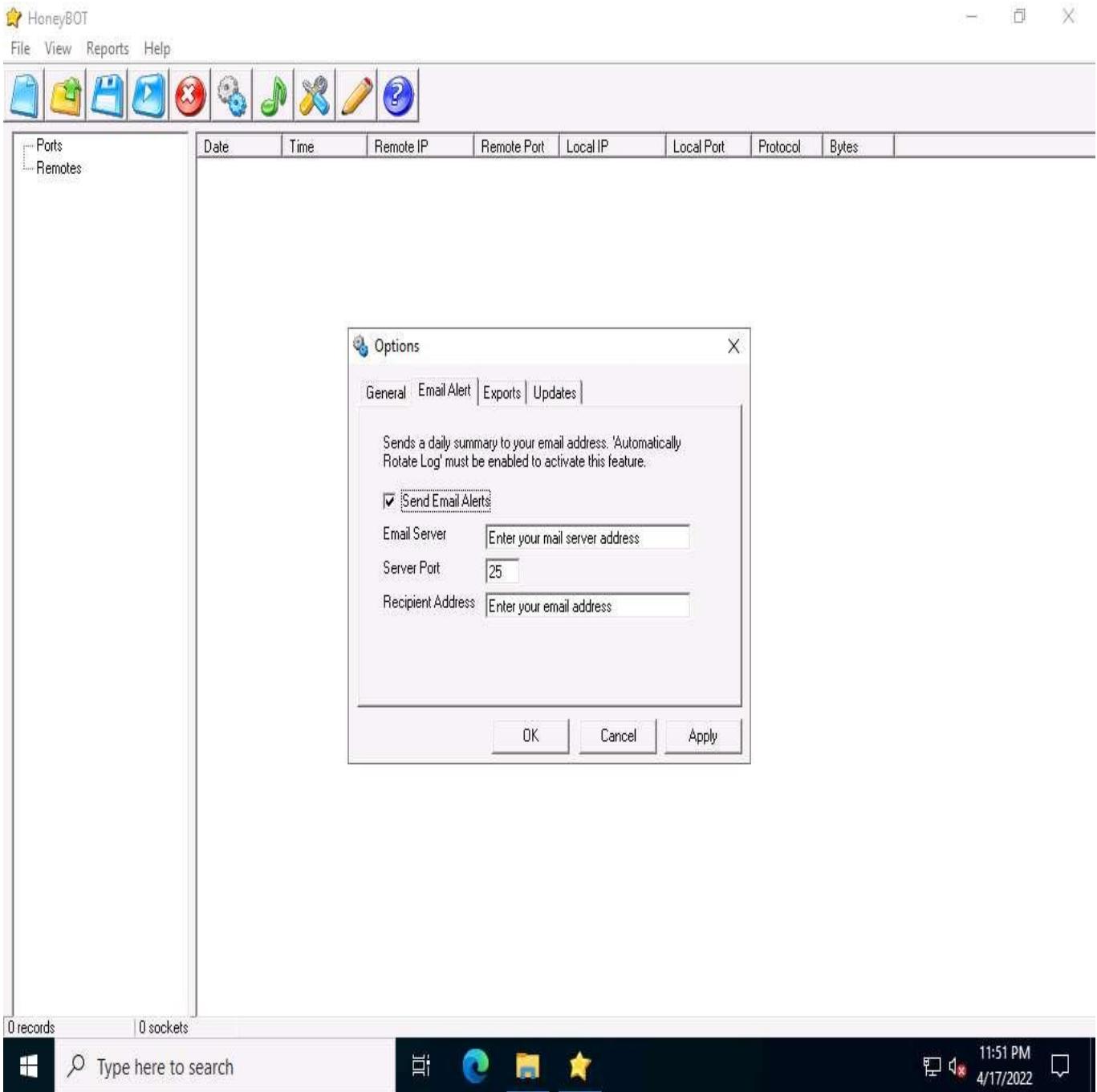


6. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.
7. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.

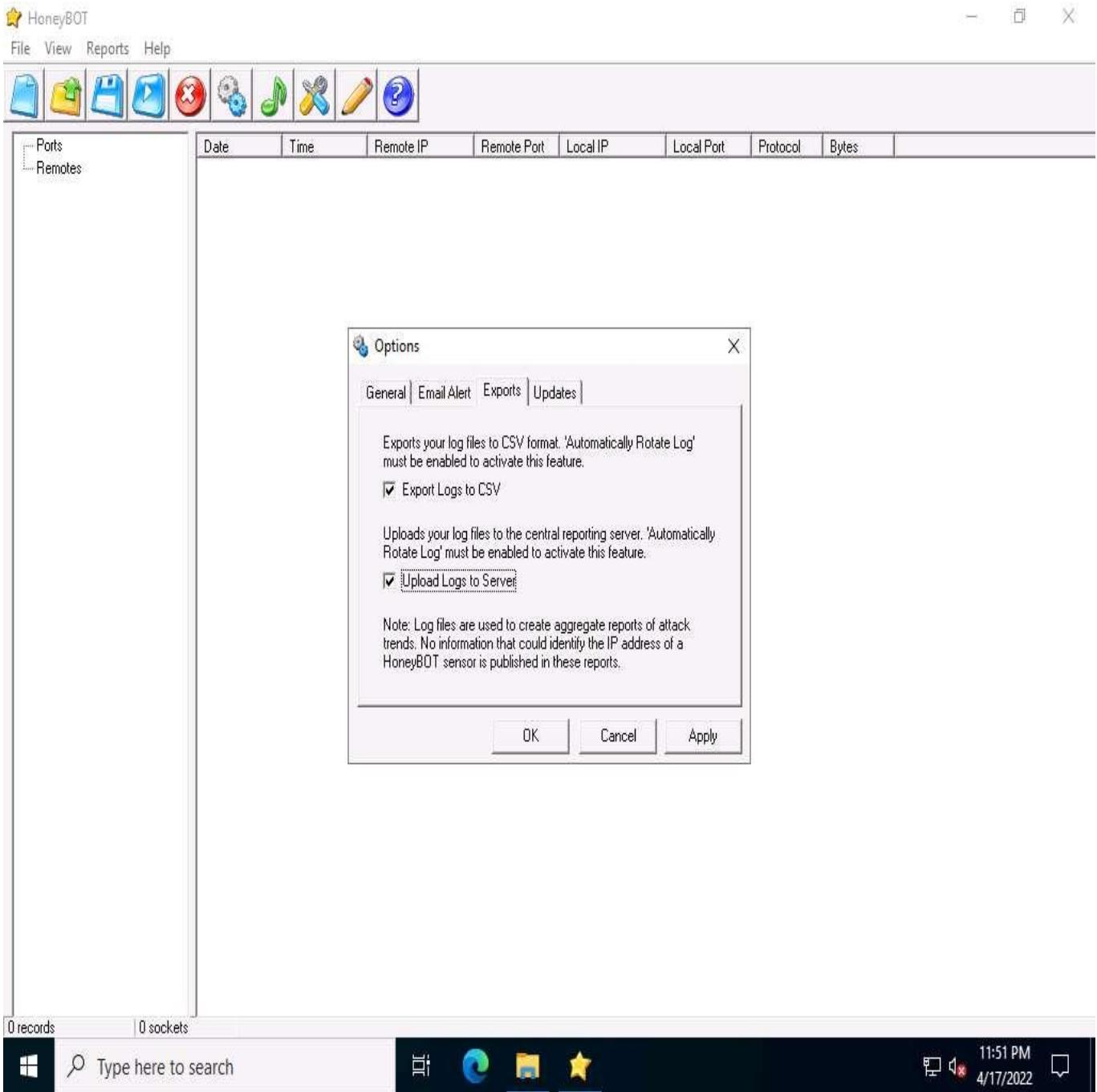


8. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

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

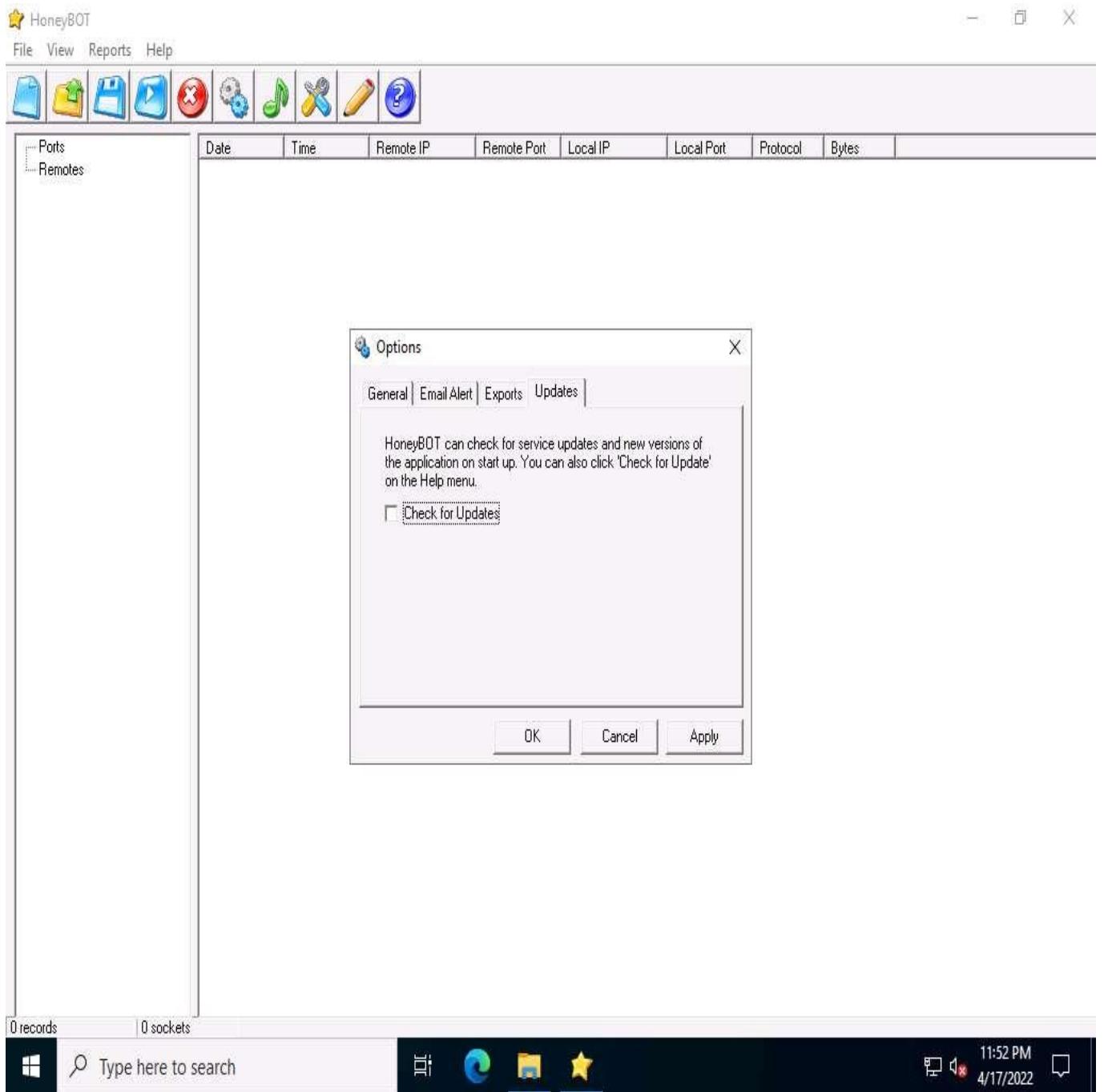


9. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (here, **Export Logs to CSV** and **Upload Logs to Server** checkbox are selected)



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.



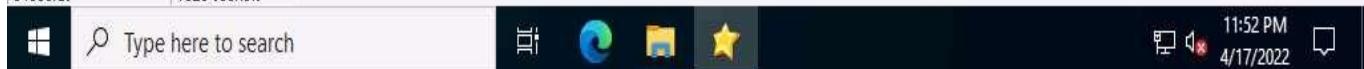
11. The **HoneyBOT** main window appears, as shown in the screenshot.

File View Reports Help

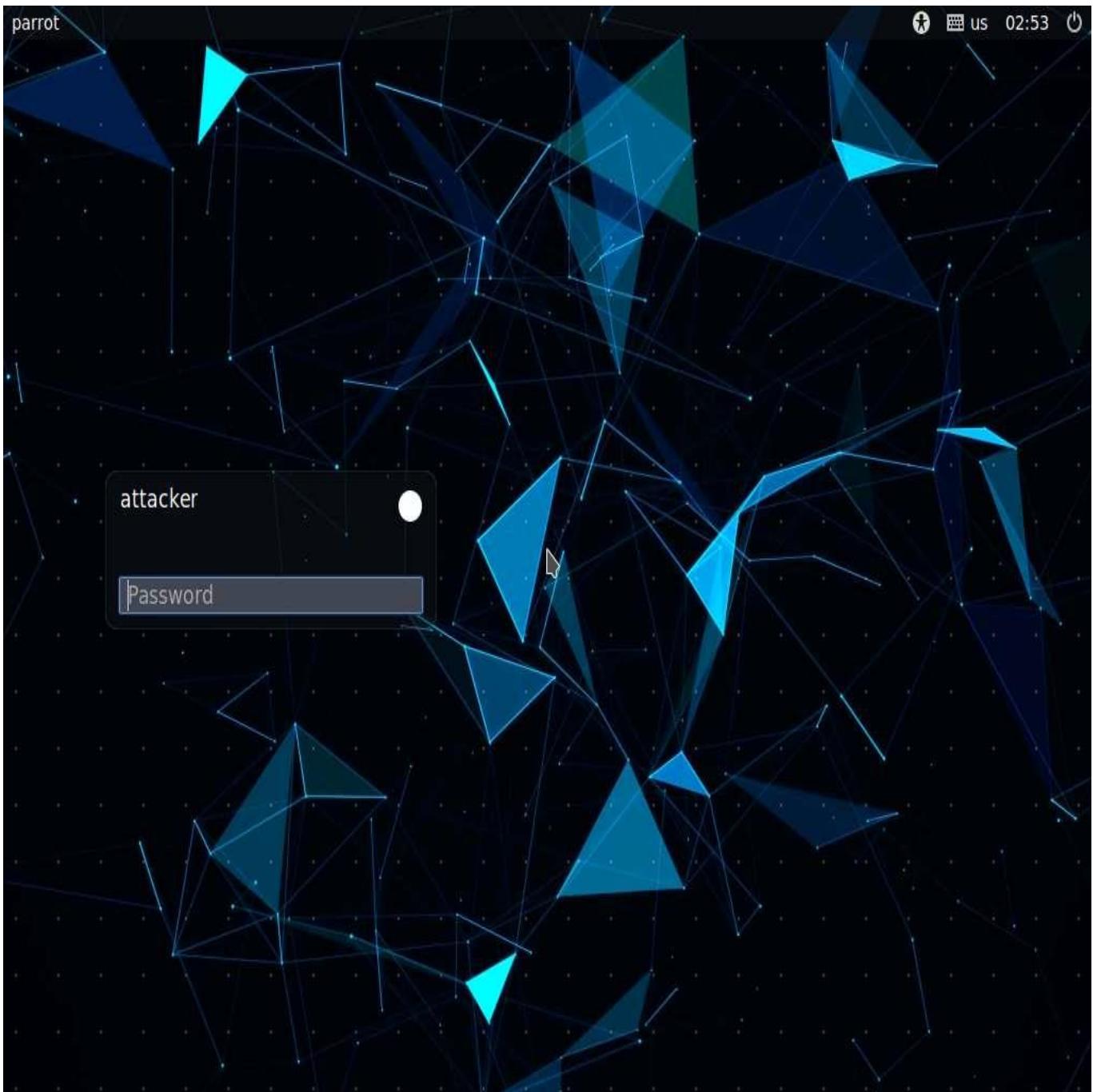


Ports	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes	
Remotes									

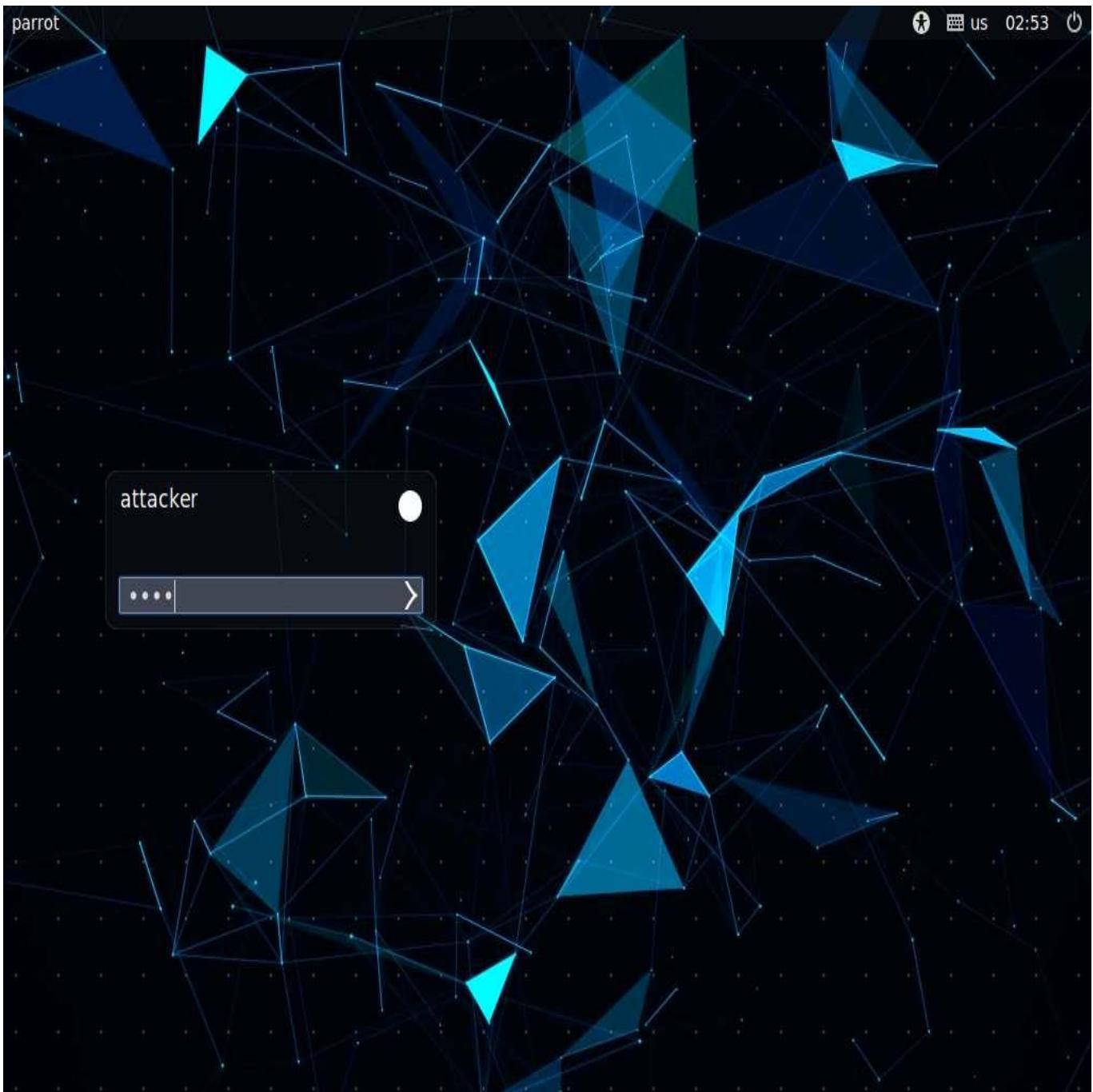
0 records | 1326 sockets



12. Now, leave the HoneyBOT window running on **Windows Server 2022**.
13. Click [Parrot Security](#) to switch to the **Parrot Security** machine.

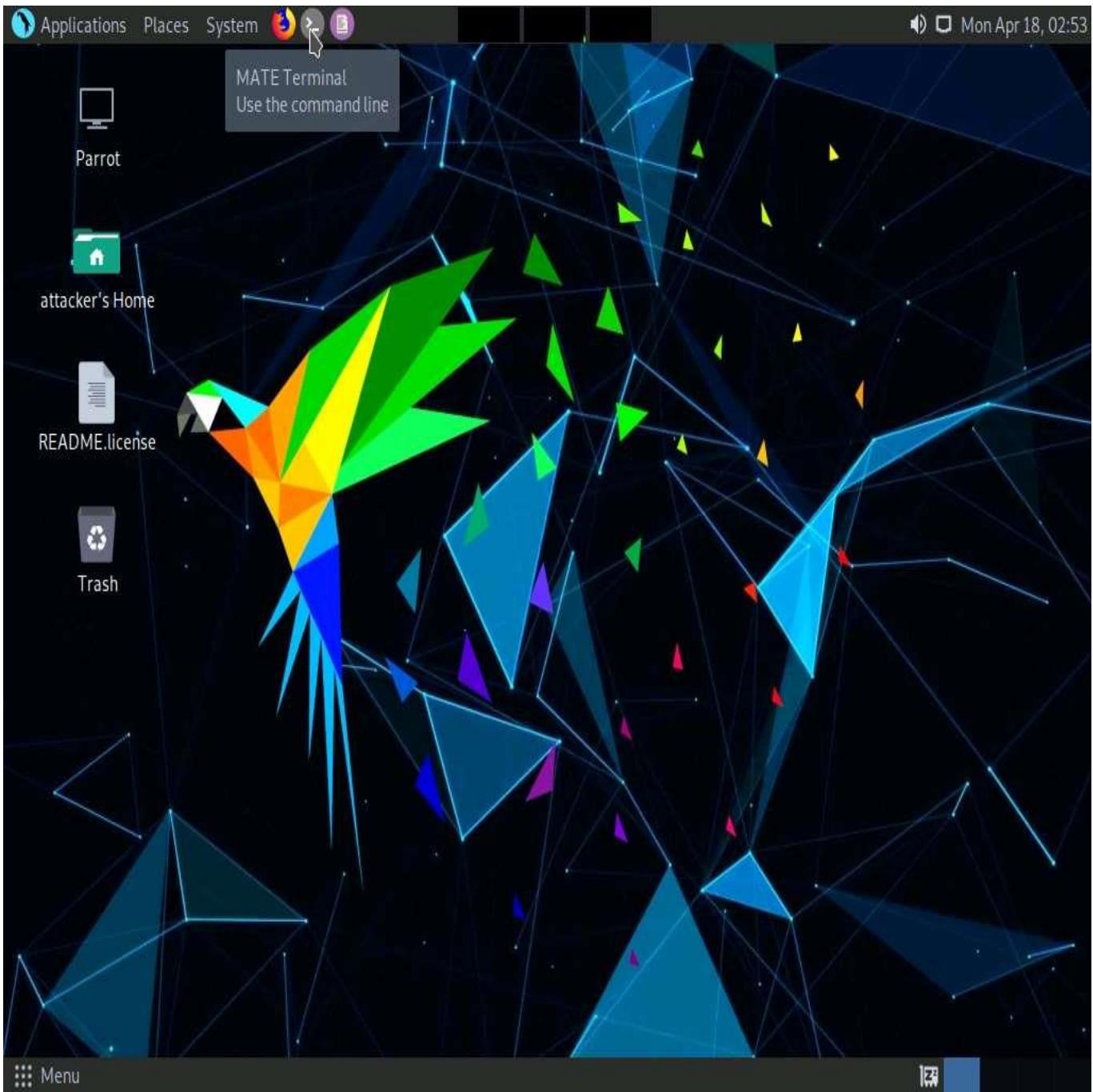


14. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



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.

Applications Places System cd - Parrot Terminal

File Edit View Search Terminal Help

```
[attacker@parrot] ~ [-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] ~ [-]/home/attacker
└─# cd
[root@parrot] ~ [-]
└─#
```

README LICENSE

Trash

Menu cd - Parrot Terminal

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.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker]
└─# cd
[root@parrot]~[-]
└─# telnet 10.10.1.22
Trying 10.10.1.22...
Connected to 10.10.1.22.
Escape character is '^]'.
```

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.

★ HoneyBOT - Log_20220418.bin

File View Reports Help

Ports Remote 10.10.1.13

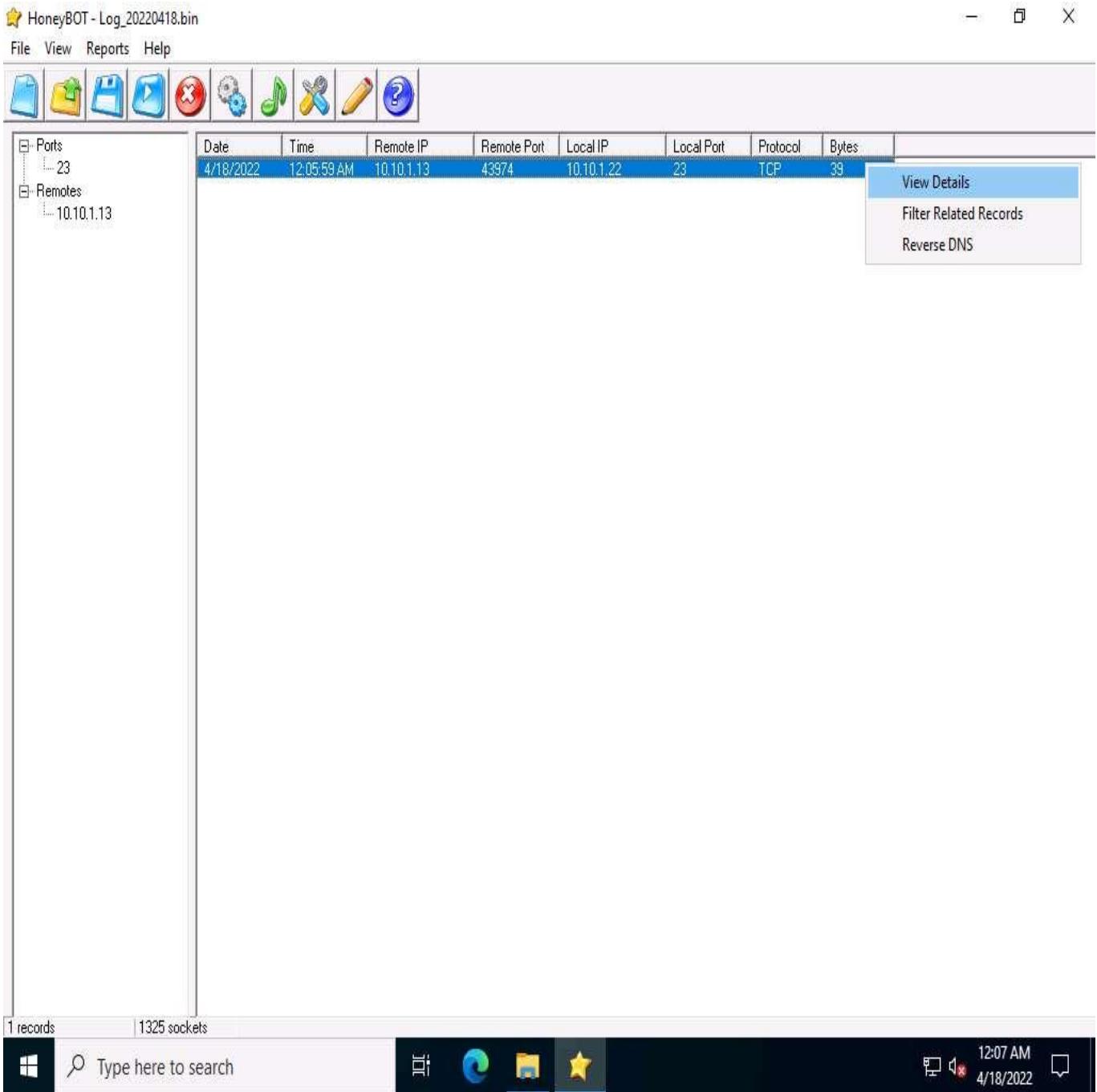
	Date	Time	Remote IP	Remote Port	Local IP	Local Port	Protocol	Bytes	
	4/18/2022	12:05:59 AM	10.10.1.13	43974	10.10.1.22	23	TCP	39	

1 records | 1325 sockets

Type here to search

12:06 AM
4/18/2022

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**.

