Princess Sumaya جامعـــة
University الأميـــرة سميّـــة
for Technology للتكنولوجيا

Information Security Fundamentals Project

Authors:

Leen Amr	20210258
Mohammad Abdalaziz	20200168
Bahaa Qabbani	20220106
Osama Abughali	20220083

Supervisor:

Dr. Haitham Al-ani

May 24, 2024

Table of Contents

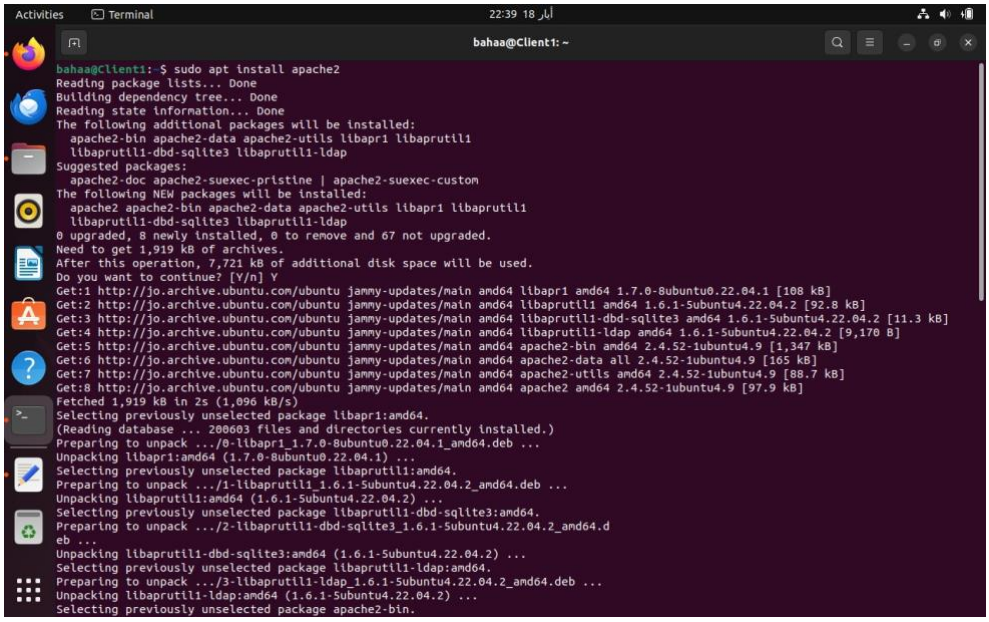
Introduction

This project dives into cybersecurity by setting up and securing a personal web server, checking for weaknesses through a simulated Man-in-the-Middle (MITM) attack, and exploring password cracking techniques. The first part focuses on creating a safe web server, hosting a basic webpage, and adding SSL encryption. The second part sets up a controlled environment to mimic a MITM attack, capturing unencrypted data and applying filters to manipulate it. Finally the third part examines password cracking methods like SSH dictionary attacks and hash cracking. Through these tasks, we gain practical knowledge about cybersecurity principles and defense strategies.

Part 1: Setting Up A Secured Webserver

1.1 Set Up a Web Server

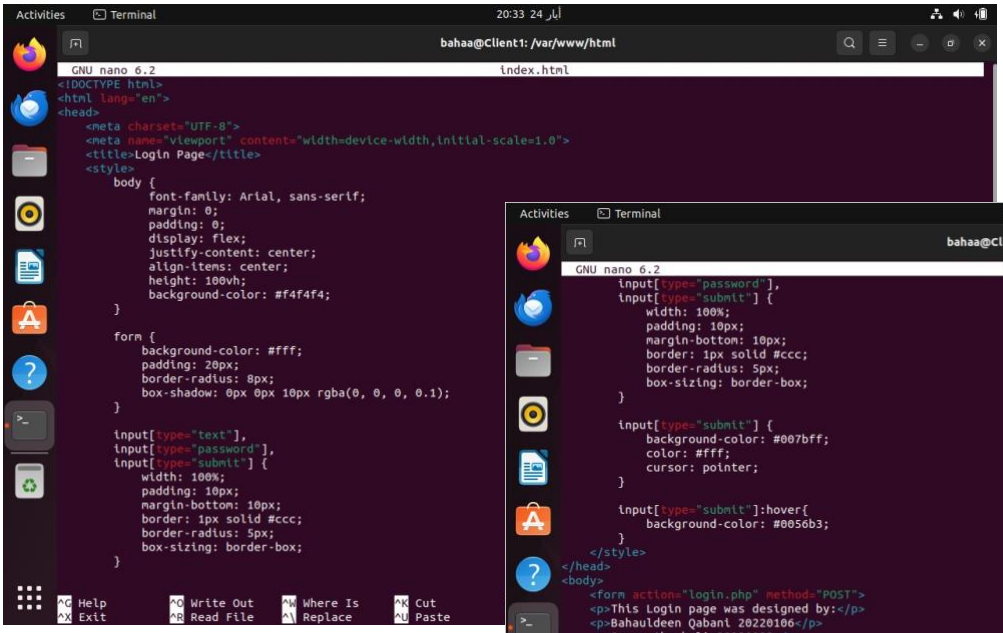
We successfully configured a web server using Apache on an Ubuntu server environment, enabling efficient hosting and management of web content.

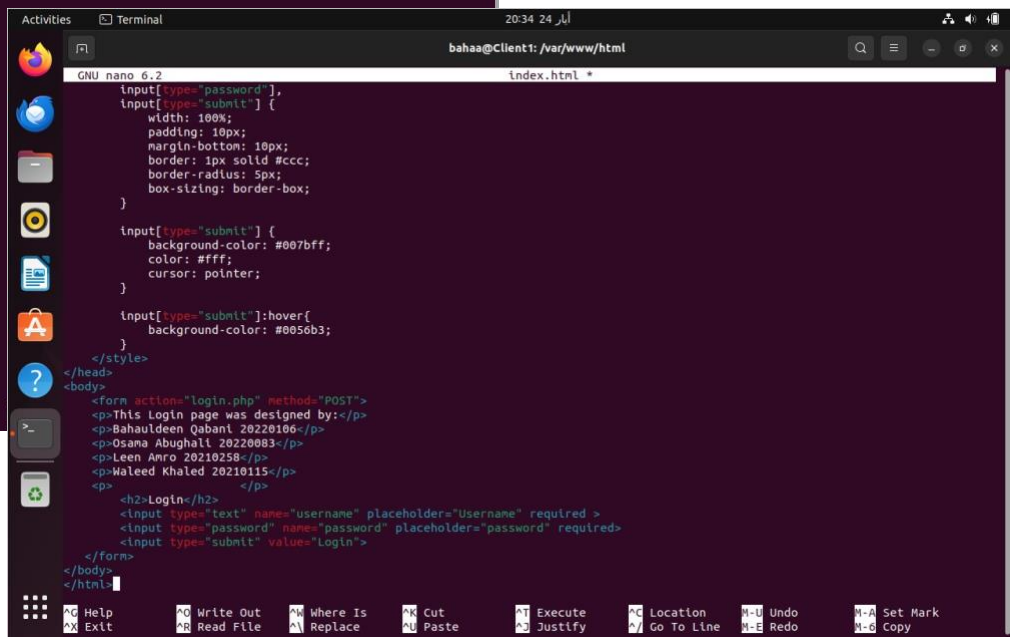


1.2 Host a Simple Web Page

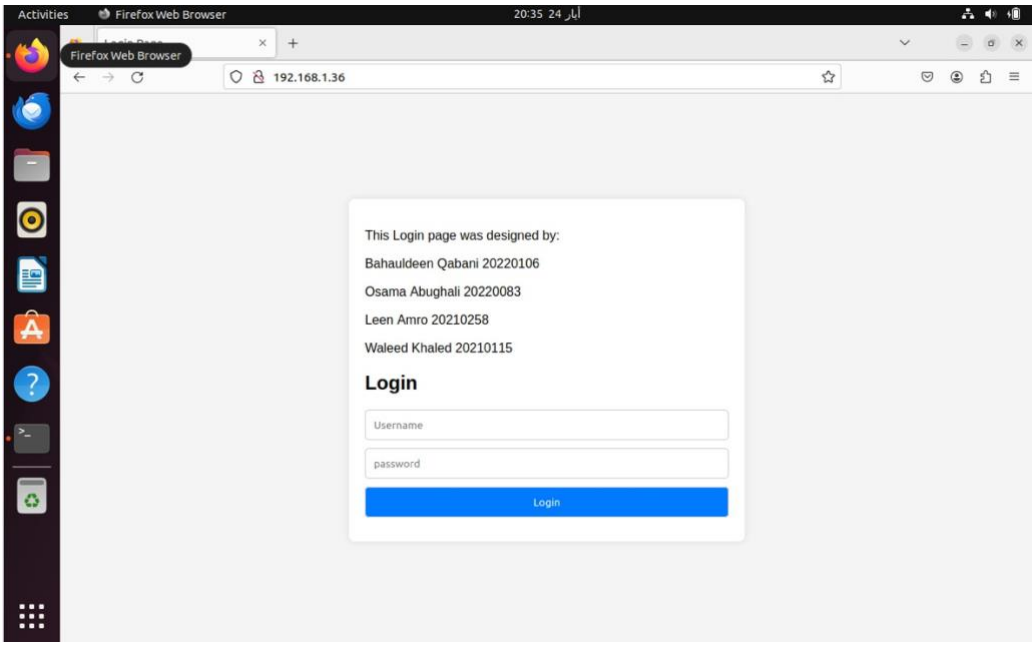
We asked chatgpt to write us a simple html code to set up our web page.

Here is the code:



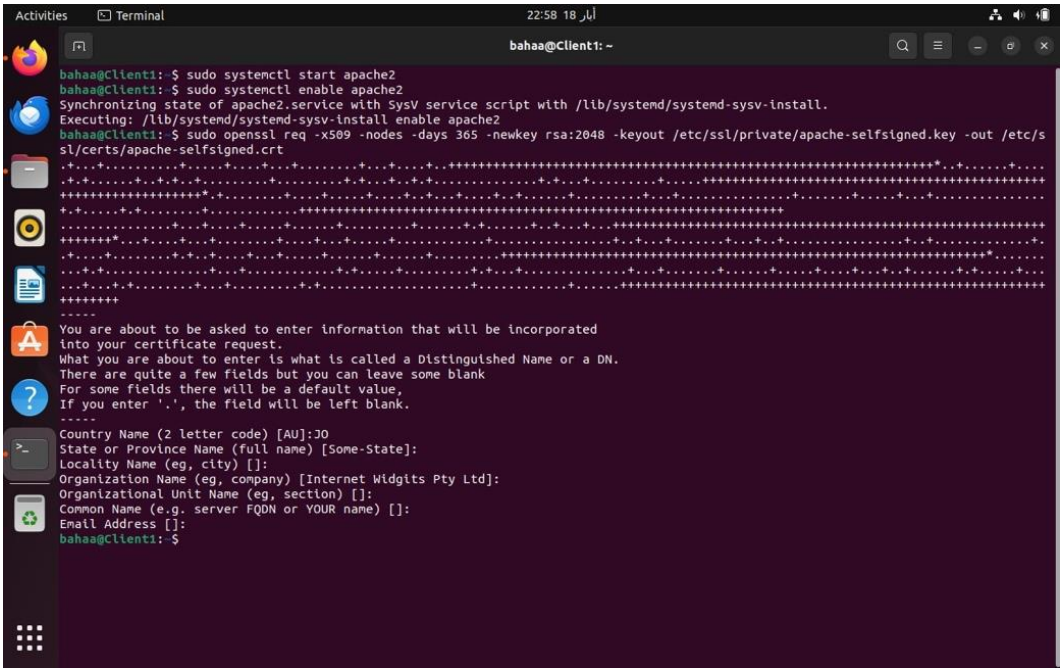


Here is a preview of our web page:

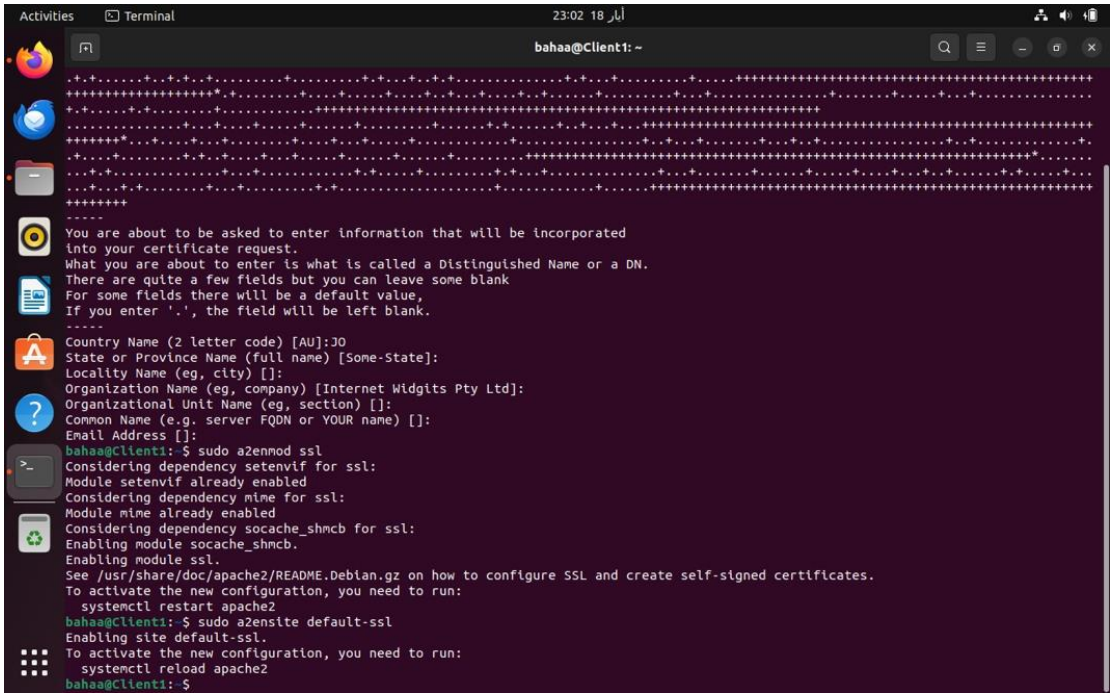


1.3 Create a Self-Signed SSL Certificate

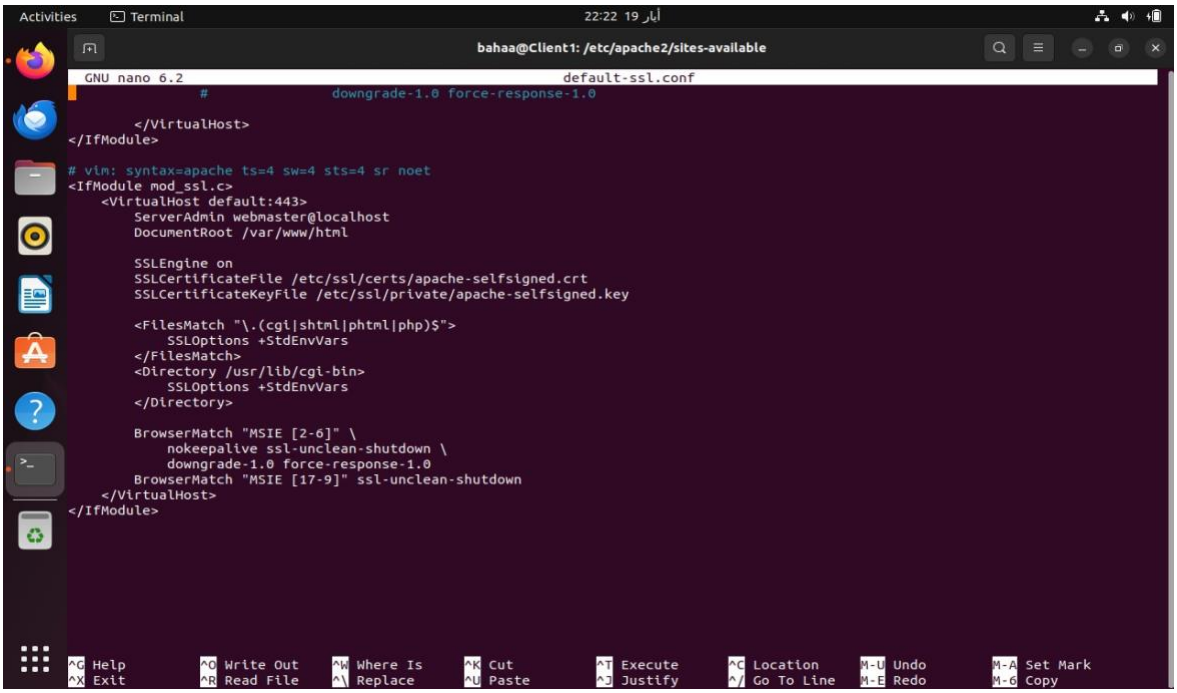
1- First, we created an RSA certificate.



2- We sent a signing request so we can be able to self-sign ourselves.

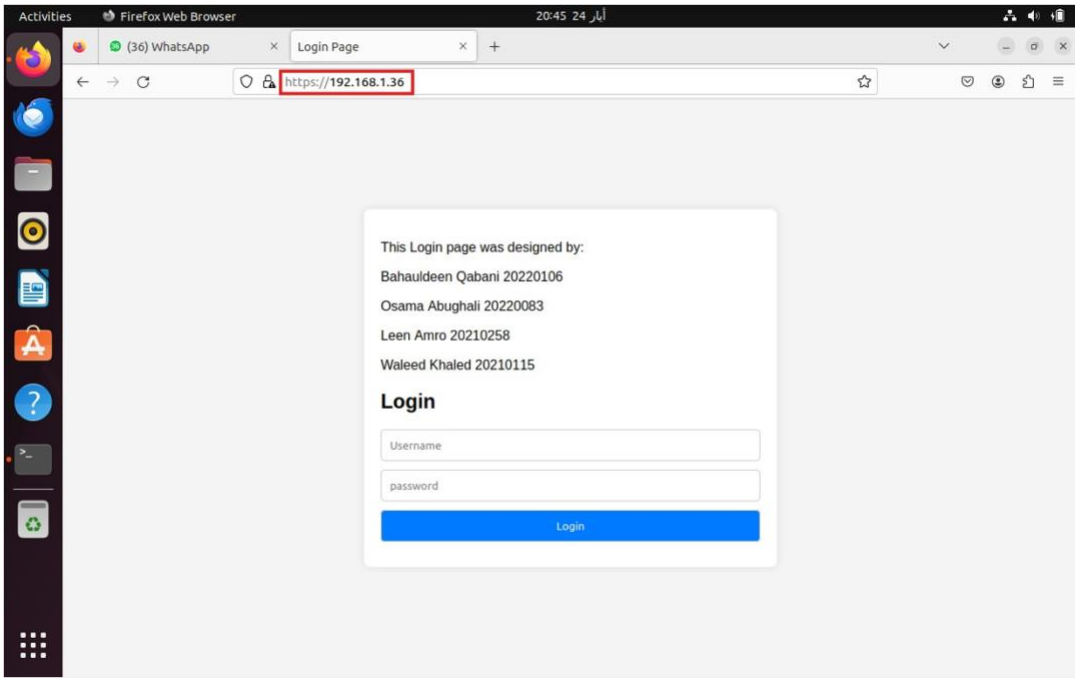


3- Configured the certificate to be used for SSL (Secure Sockets Layer), to enable secure communication over HTTP.



1.4 Testing

Here we tested our website by accessing it through a web browser using HTTPS.



* HTTP is already tested in objective 2.

Part 2: Man In The Middle Attack

2.1 Setup a Controlled Environment

We created two virtual machines:

1- Web Server

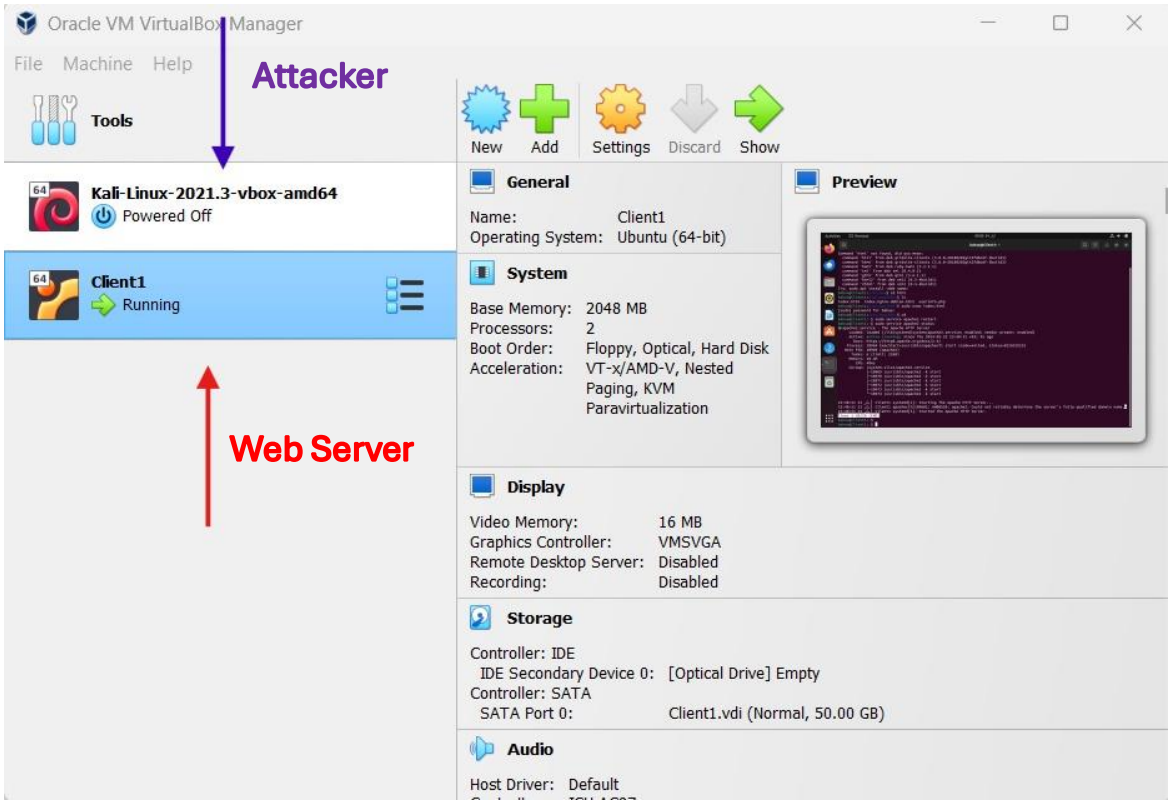
Purpose: Host the HTTP-based website created in Part 1.

Configuration: Install Ubuntu and set up Apache as shown in Part 1.

2- Attacker Machine

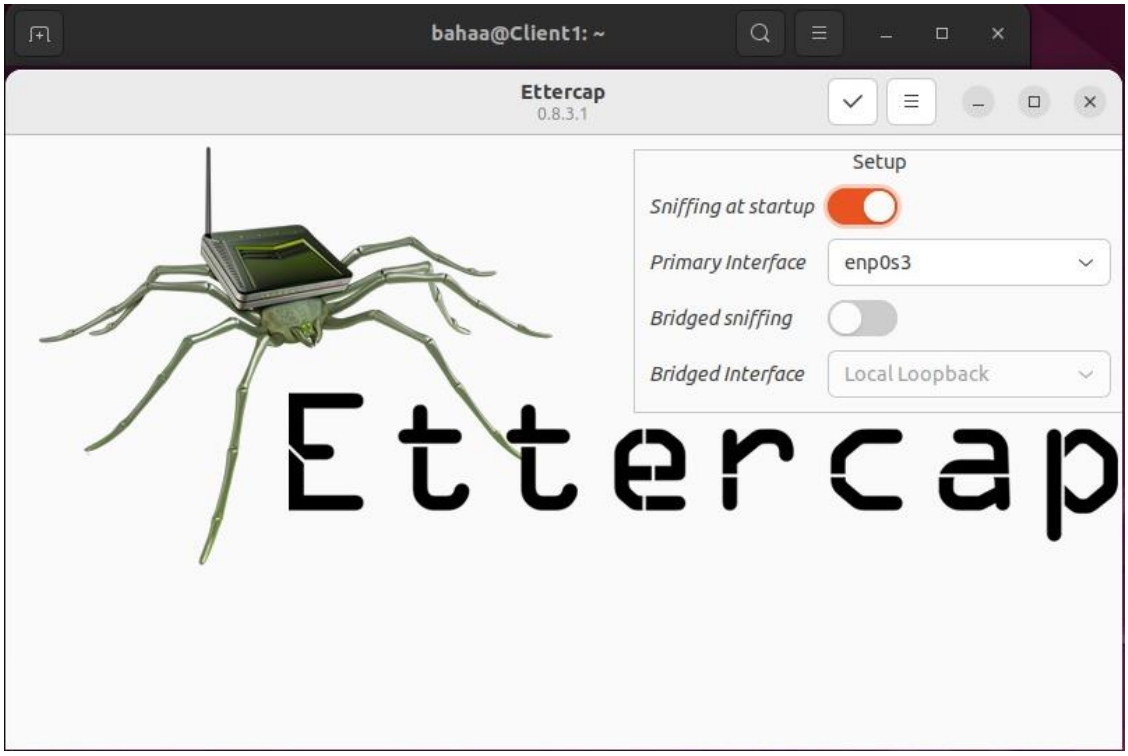
Purpose: Perform the MITM attack.

Configuration: Install Kali Linux, a distribution tailored for penetration testing.



2.2 Configuring the Tools

We installed Ettercap using the command: `sudo apt update && sudo apt install ettercap-graphical`.



2.3 Sniffing and Capturing Data

- ARP Poisoning and Sniffing using Ettercap and Wireshark:

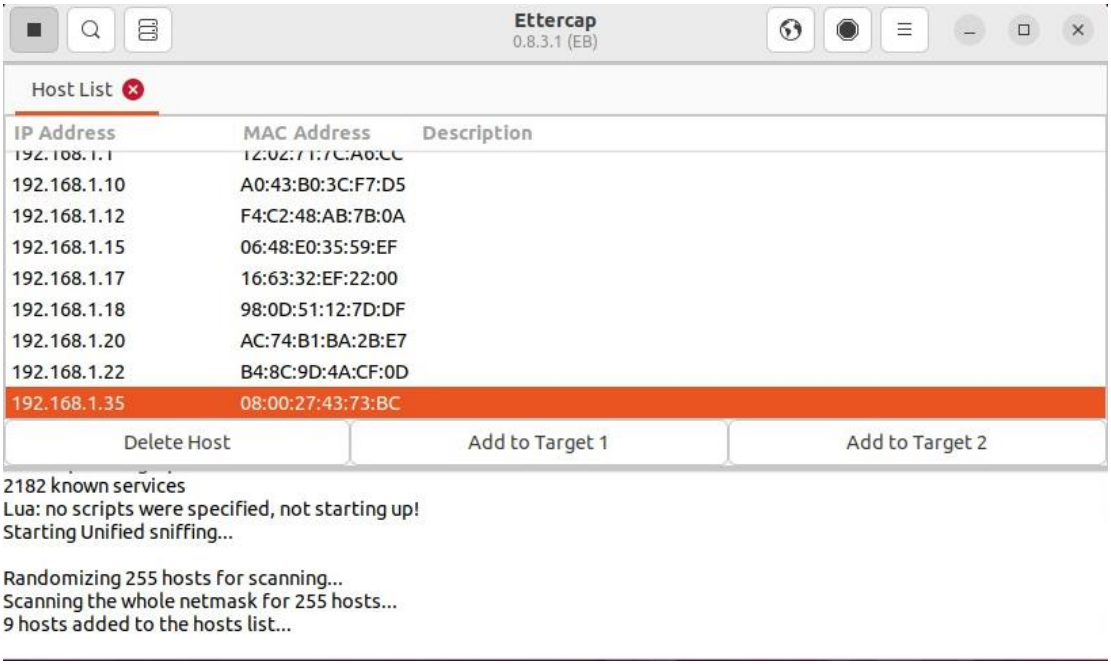
1- Opened Ettercap and started ARP poisoning targeting our website.

2- Started a unified sniffing session in Ettercap to monitor network traffic.

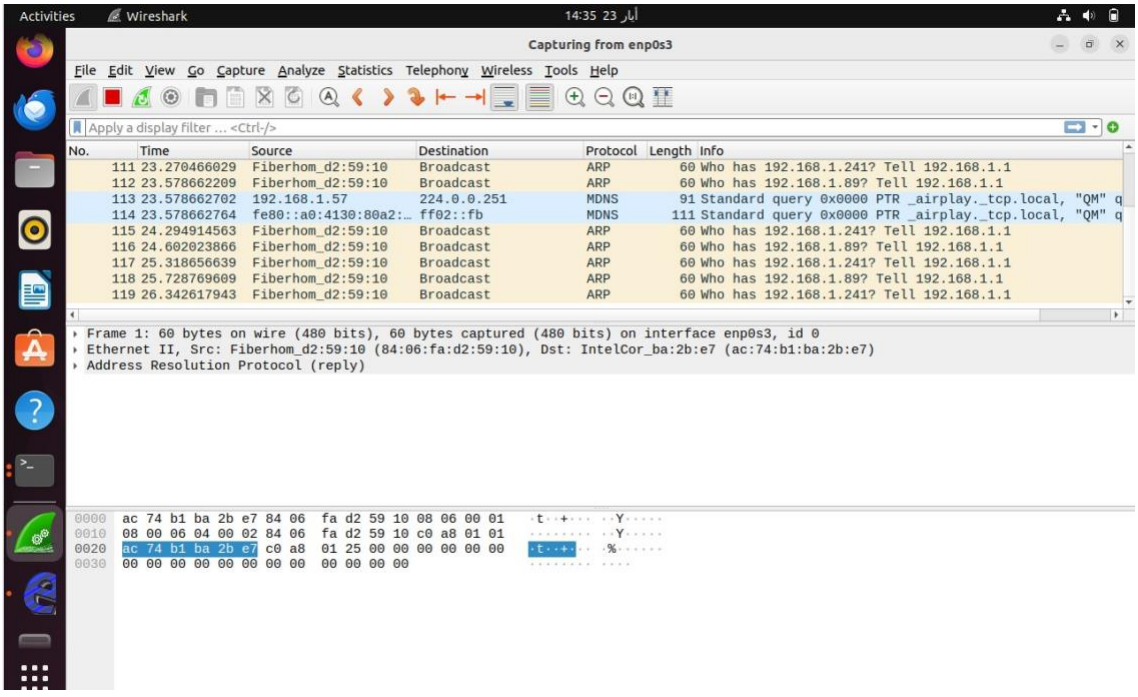
3- Scan for active hosts on the network using Ettercap.

4- Searched for our target host in the list of scanned hosts.

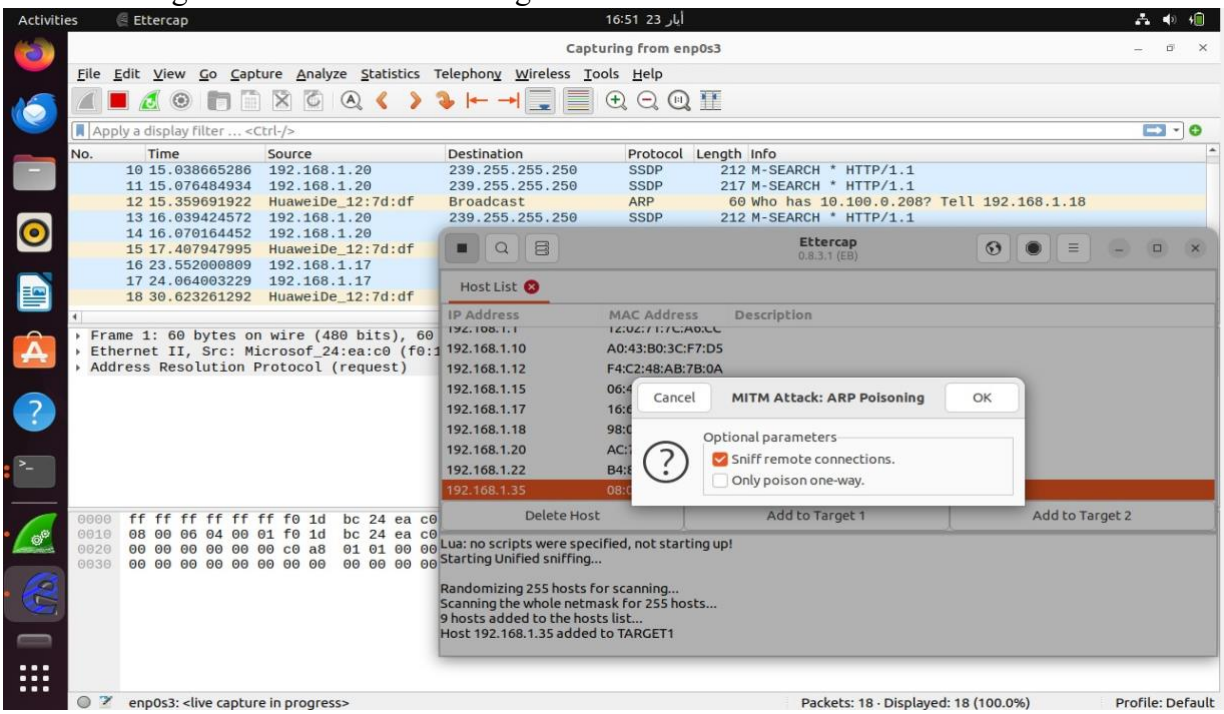
5- Added the target to Target 1 in Ettercap.



6- Launch Wireshark to capture network traffic.



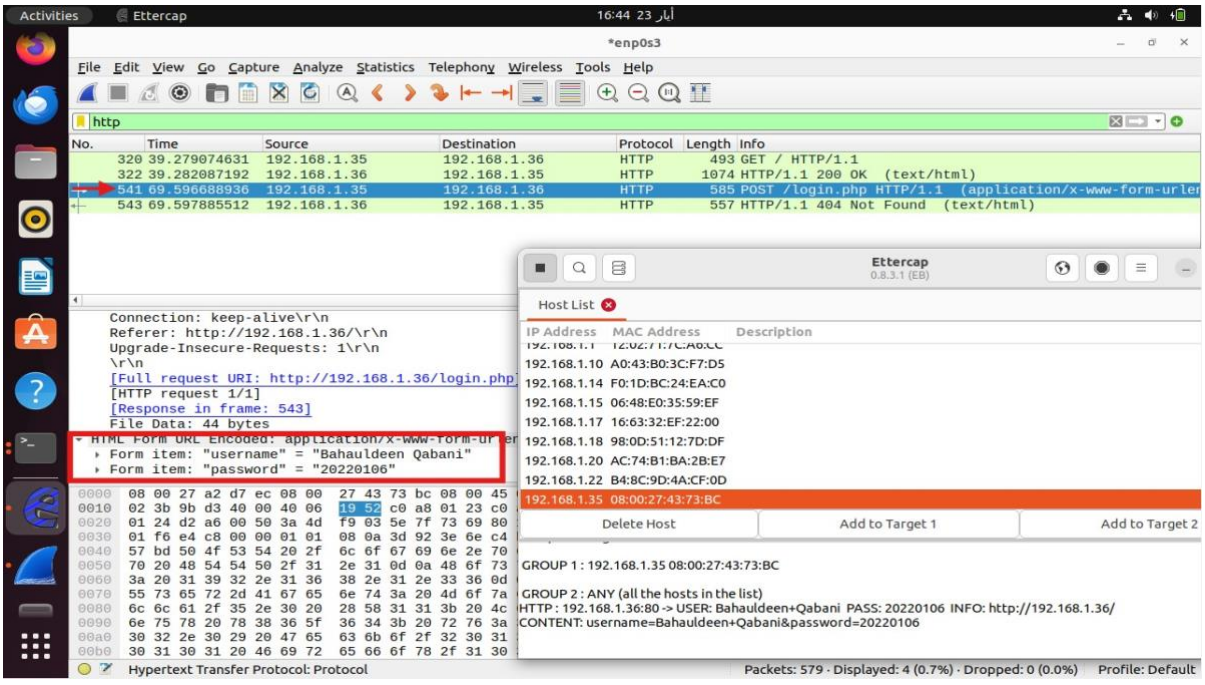
7- From the “MITM” menu in Ettercap, we chose the “Sniff remote Connections” parameter to enable sniffing of traffic between our traget and other hosts.



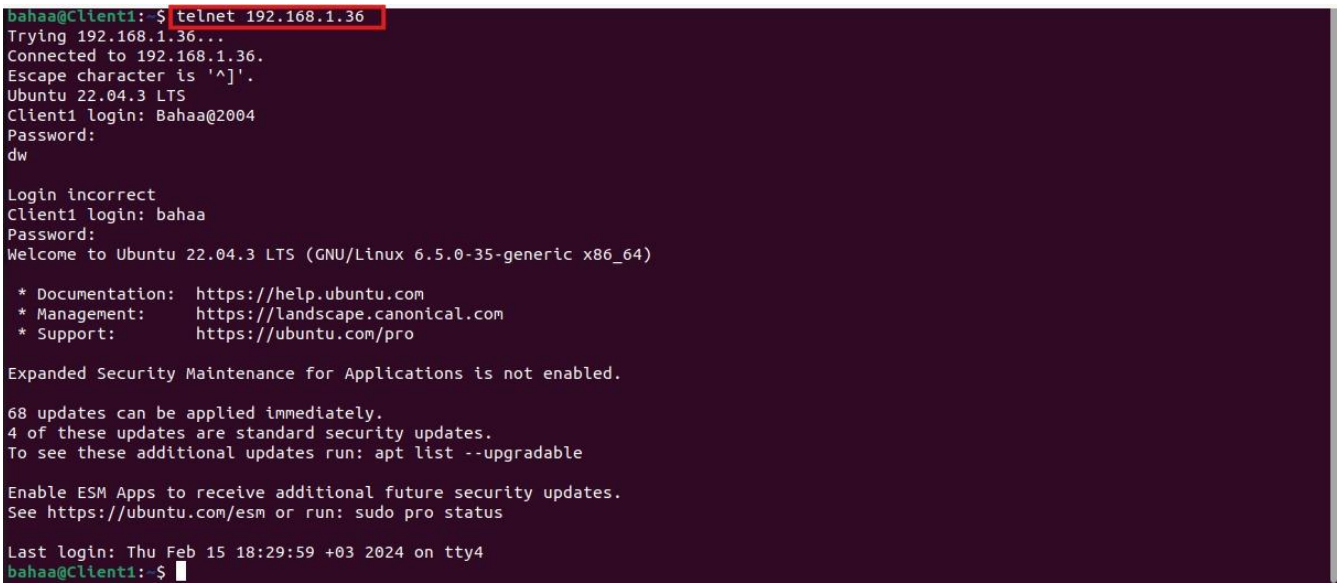
8- Performed ARP poisoning to intercept traffic between the target and the gateway.

9- Used Wireshark to capture the network traffic generated during the ARP poisoning attack.

10- Looked for sensitive information in the captured traffic, such as usernames and passwords.

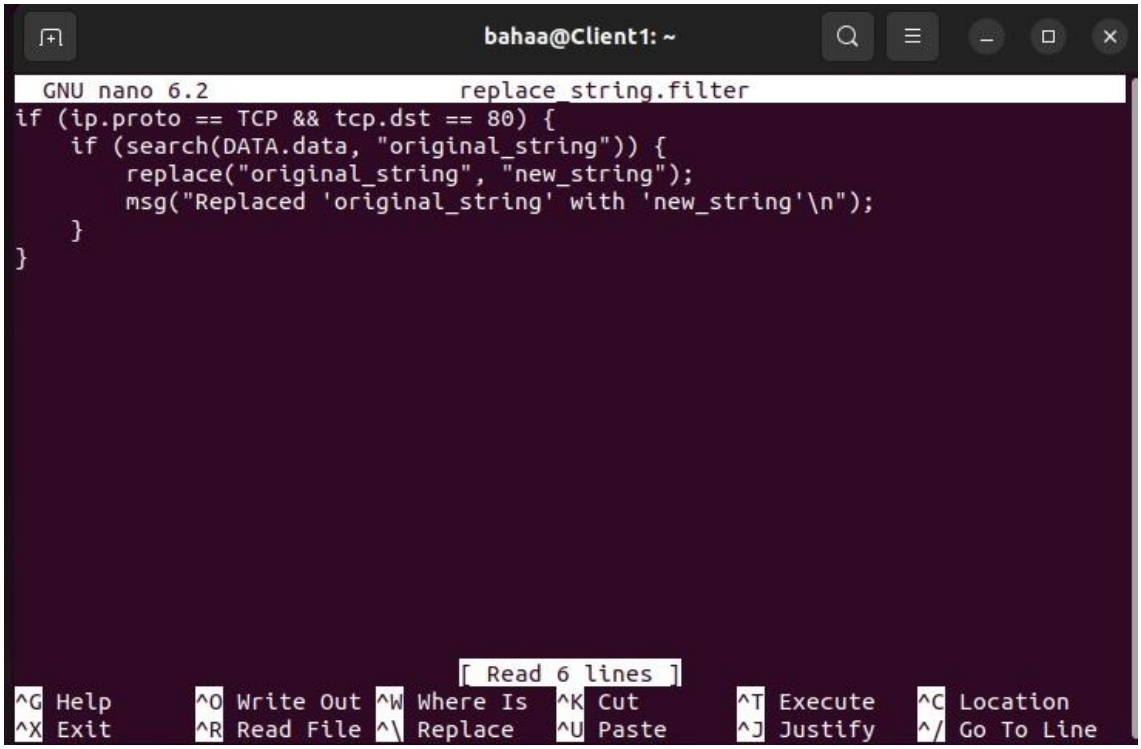


11- Finally we captured Telnet traffic to retrieve the credentials.

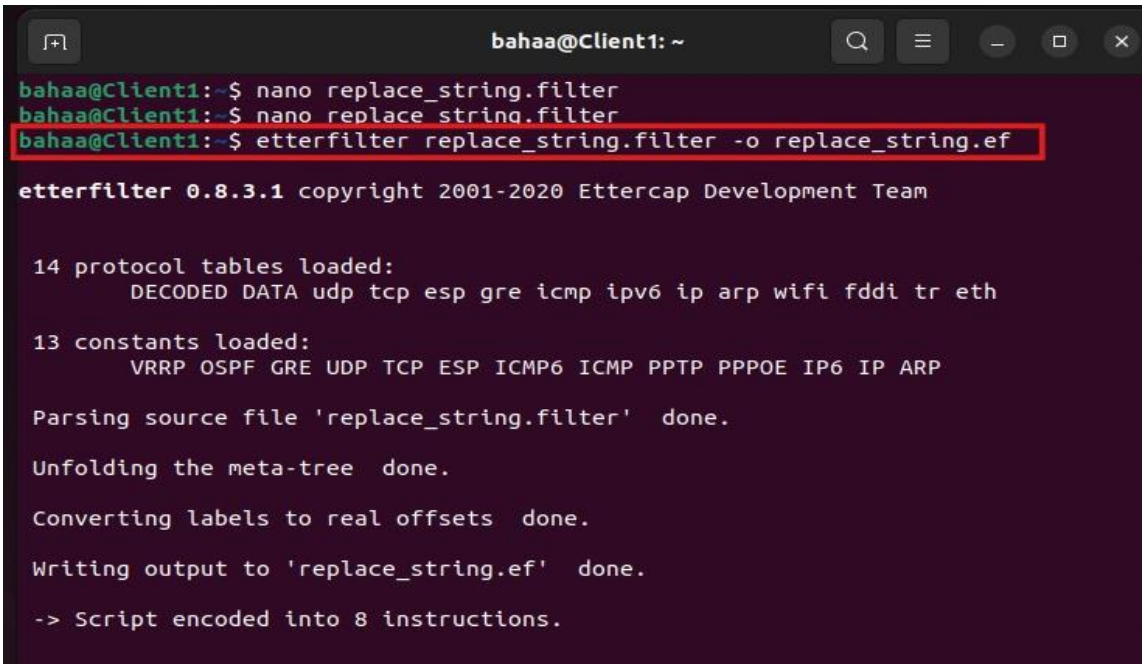


2.4 Using Filters in Ettercap for MITM

1- First we created a new filter file named `'replace_string.filter'`.
2- We wrote this code inside the filter file.

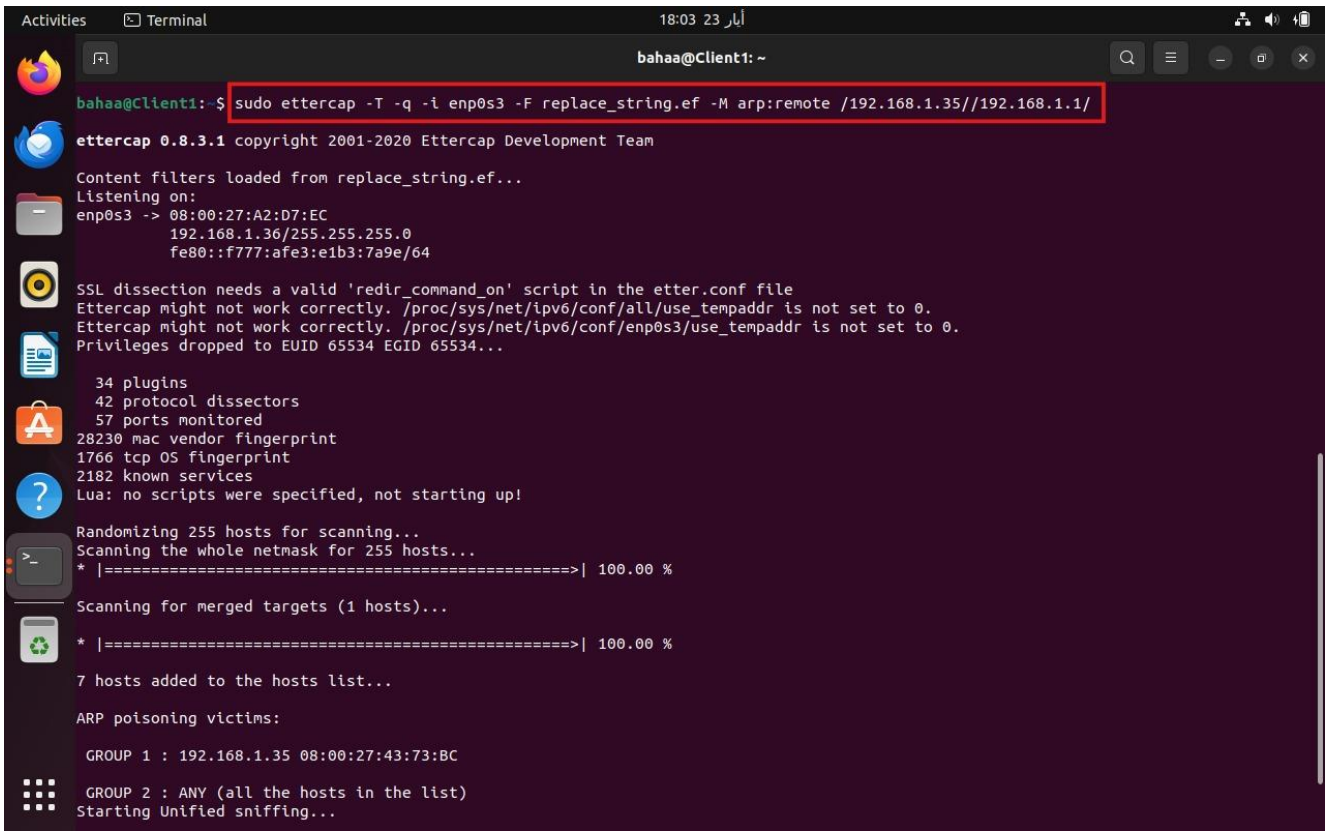


3- We compiled the filter using Ettercap's filter compiler.



4- Execute Ettercap with the compiled filter we coded to perform MITM attack (ARP poisoning).

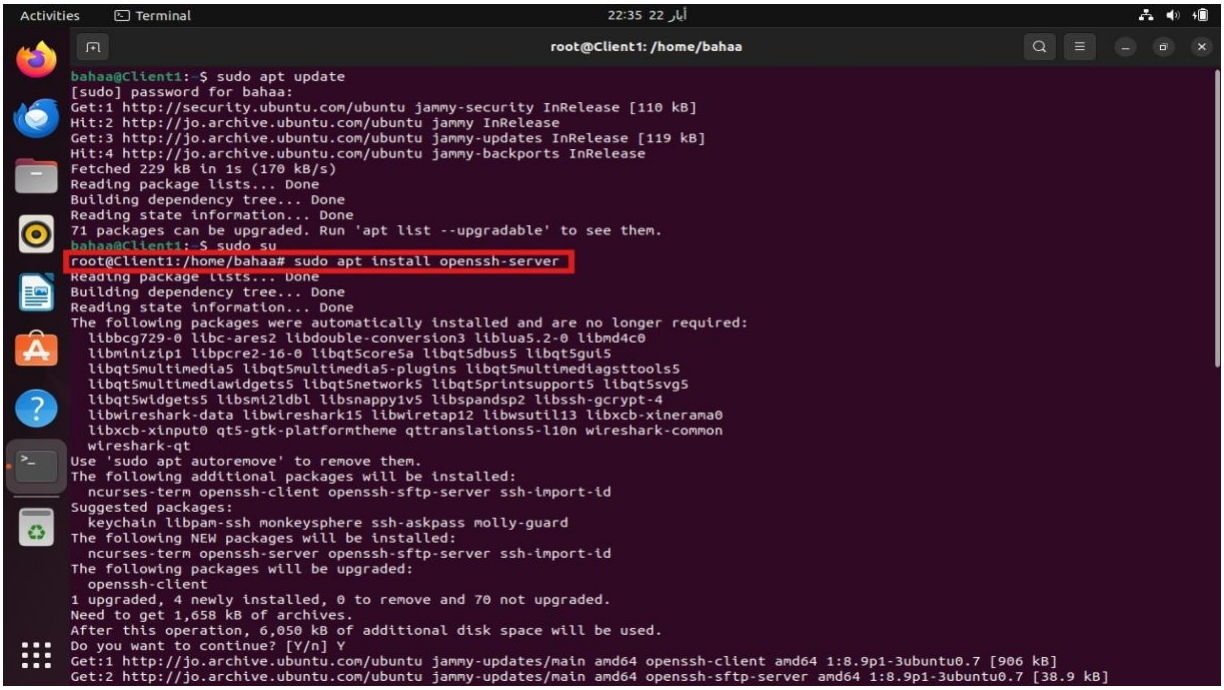
5- Replace `<network_interface>`, `<target_ip>`, and `<gateway_ip>` with the appropriate values for our setup.



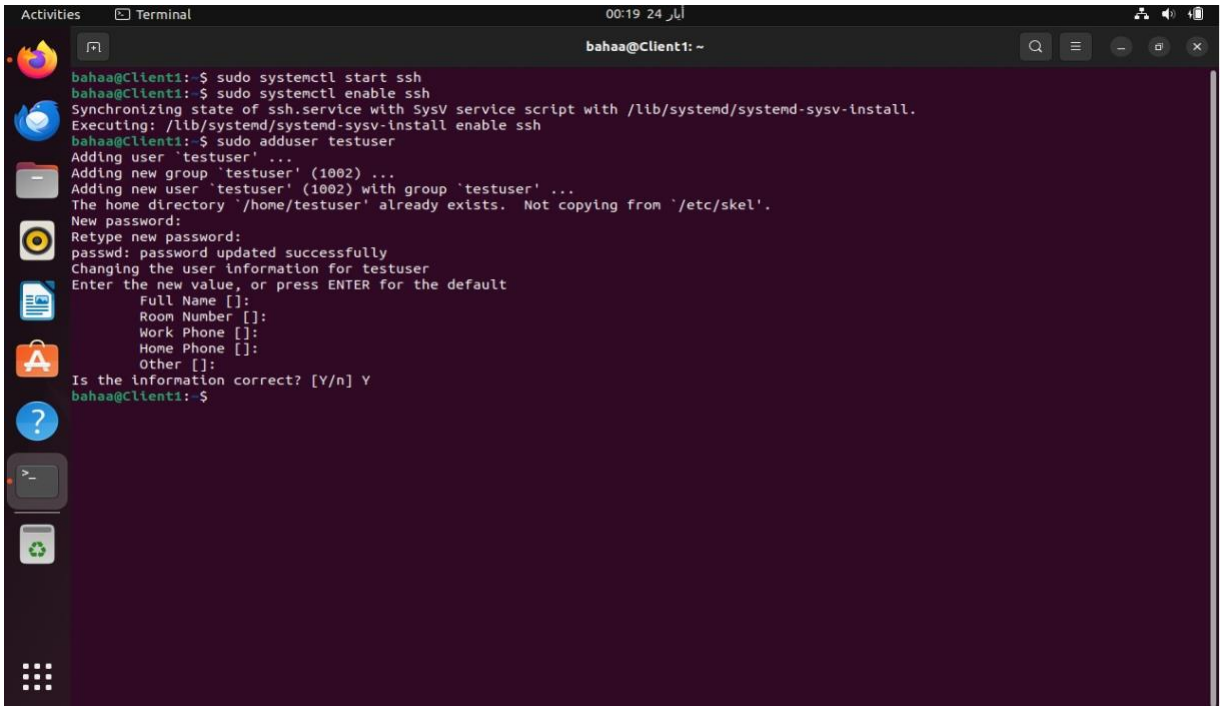
Part 3: Password Cracking

3.1 SSH Dictionary Attack

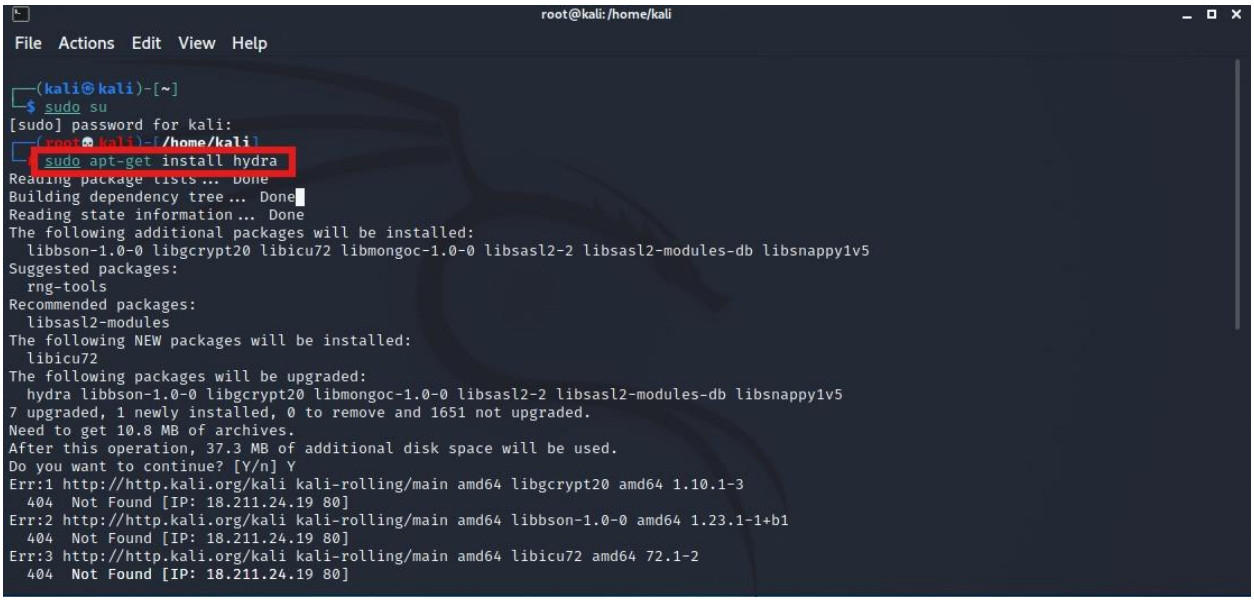
1- First we downloaded openssh-server



2- We created a user named ‘testuser’ with a known password on the target machine.

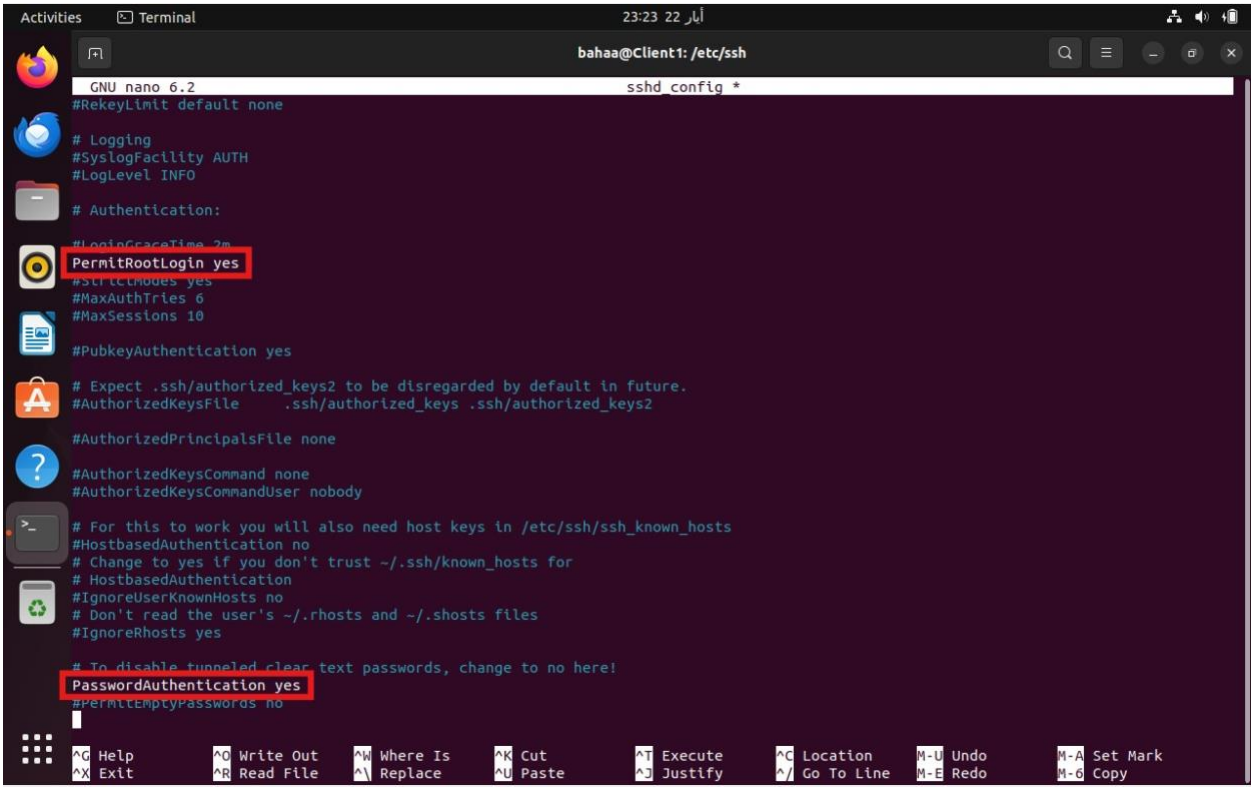


3- Installed Hydra on the attacker machine



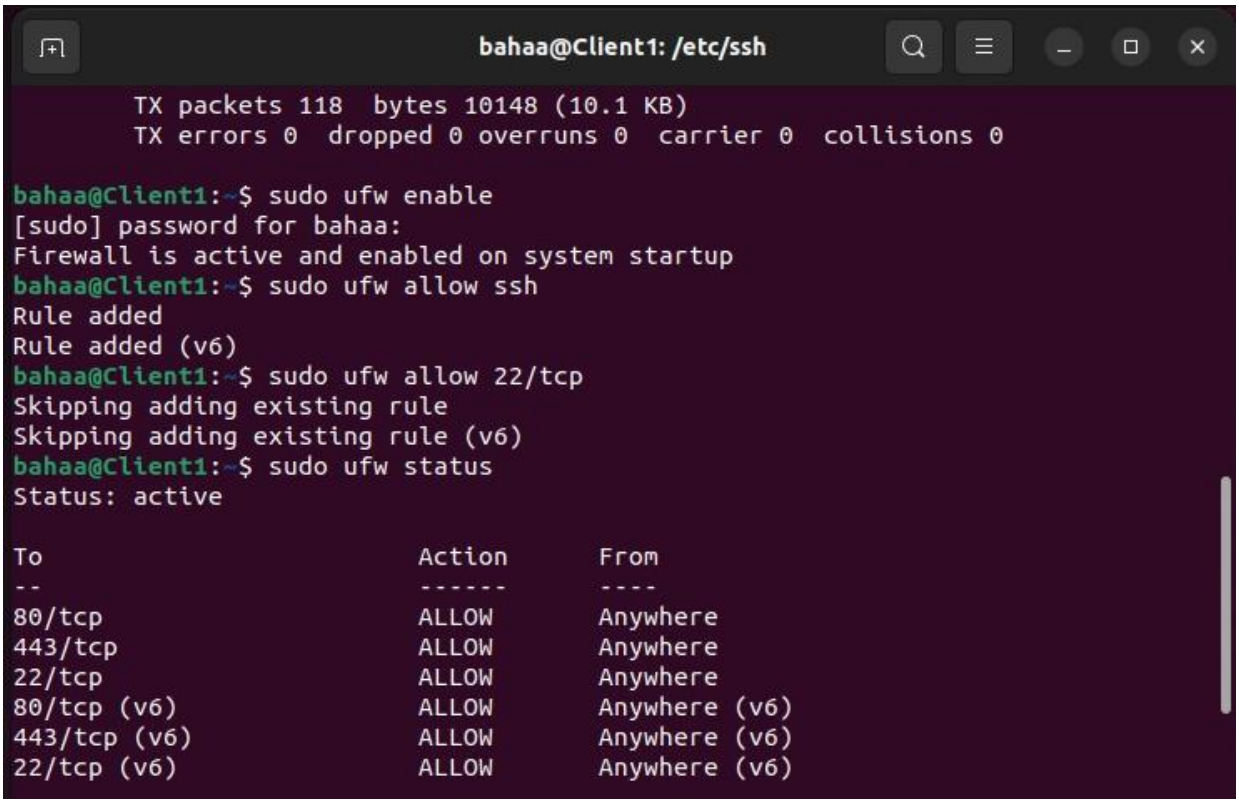
4- Opened the SSH configuration file `'/etc/ssh/sshd_config'`

5- Ensure that PermitRootLogin and PasswordAuthentication settings are enabled



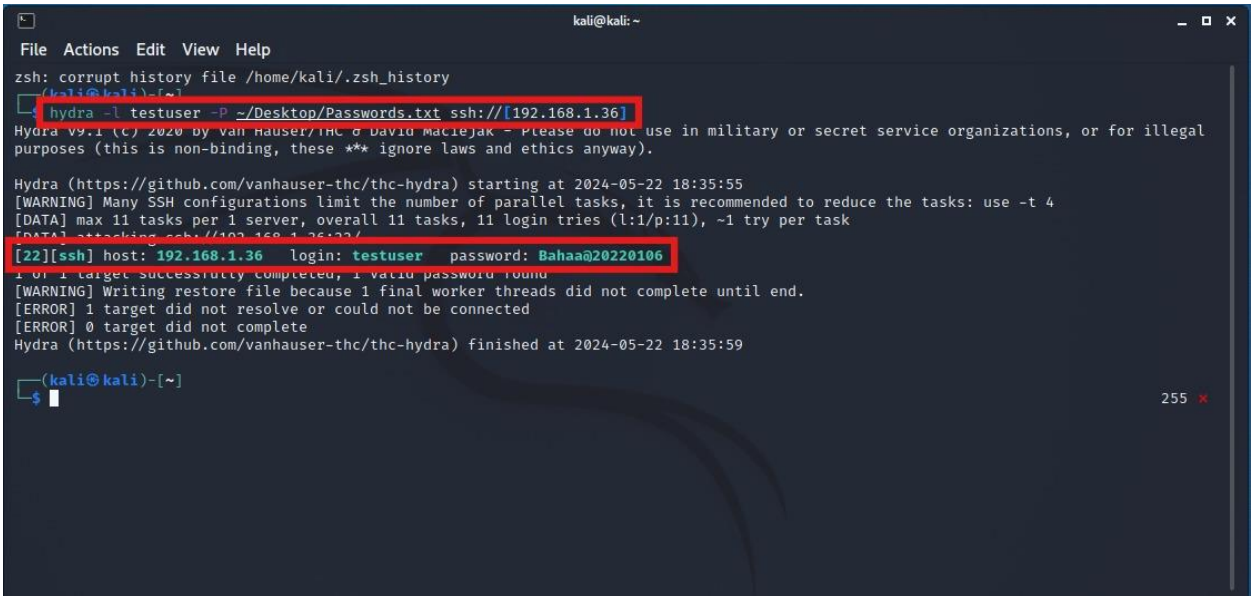
6- Created a password dictionary file named it ‘password.txt’ that contains random passwords including the actual password of the user ‘testuser’.

7- We faced multiple problems getting access to the user, then we figured out that port 22 wasn’t opened, so we opened the port and made it accessible which made it successfully work.



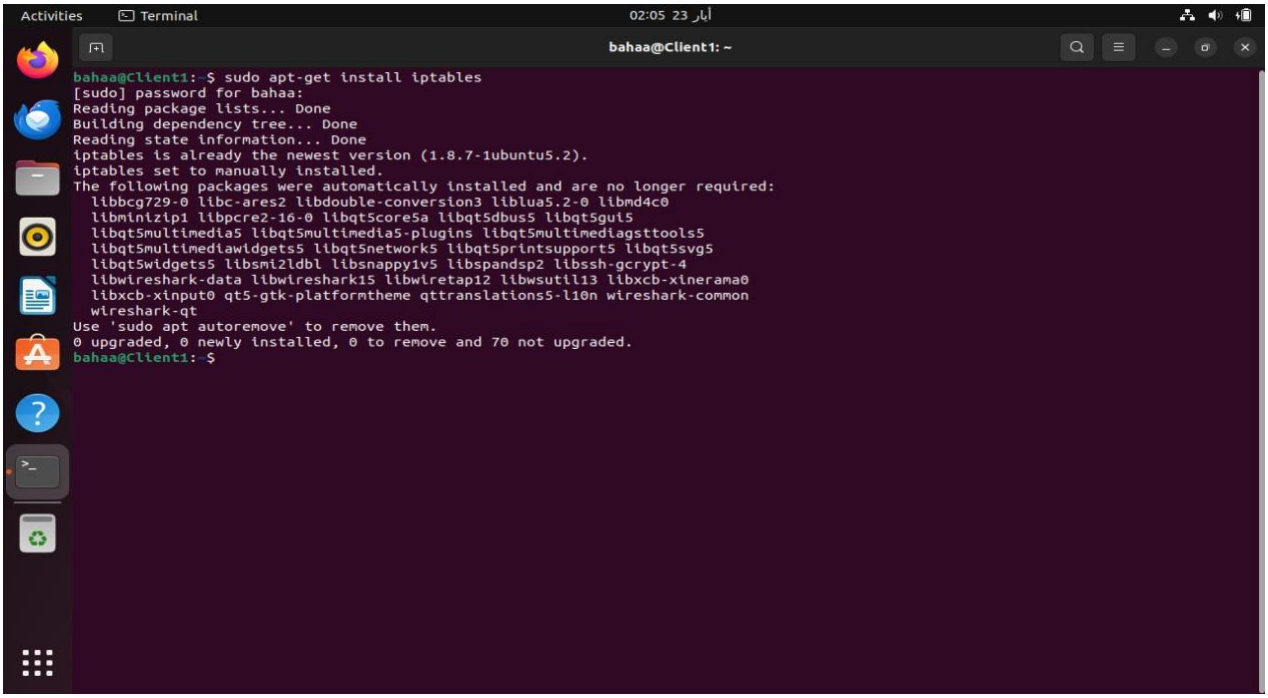
8- After running Hydra to perform the dictionary attack, we replaced `<target_ip>` with the IP address of the target machine.

9- Finally we were able to identify the password of the user ‘testuser’.



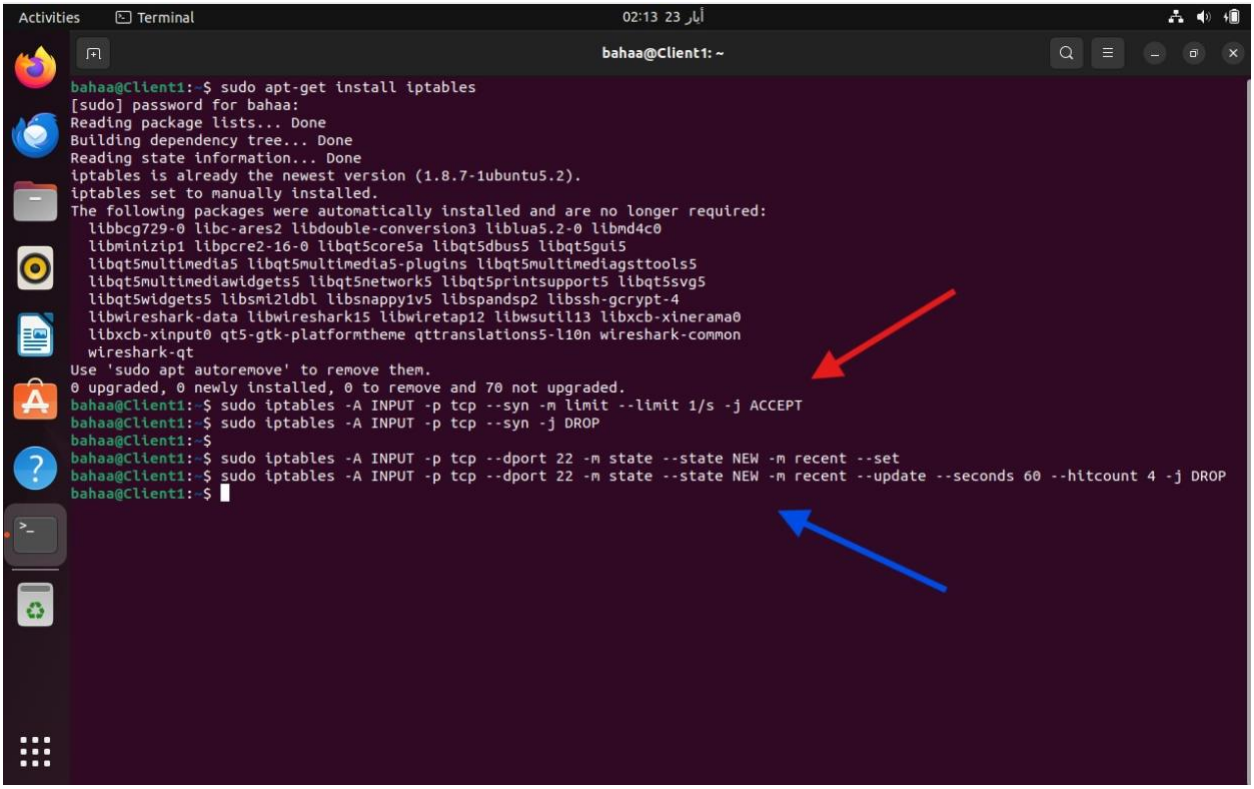
3.2 Firewall Setup

1- First we installed iptables on the system



2- Blocked half-open scans (SYN scans) using the first two commands (the red arrow shown in the figure below), enhancing network security.

3- Blocked full-open scans using the other two commands (the blue arrow shown in the figure below), fortifying the network against potential threats.



4- Flushed any exisitng iptable rules to make sure that the slate is clean for the new configuration(the red arrows).

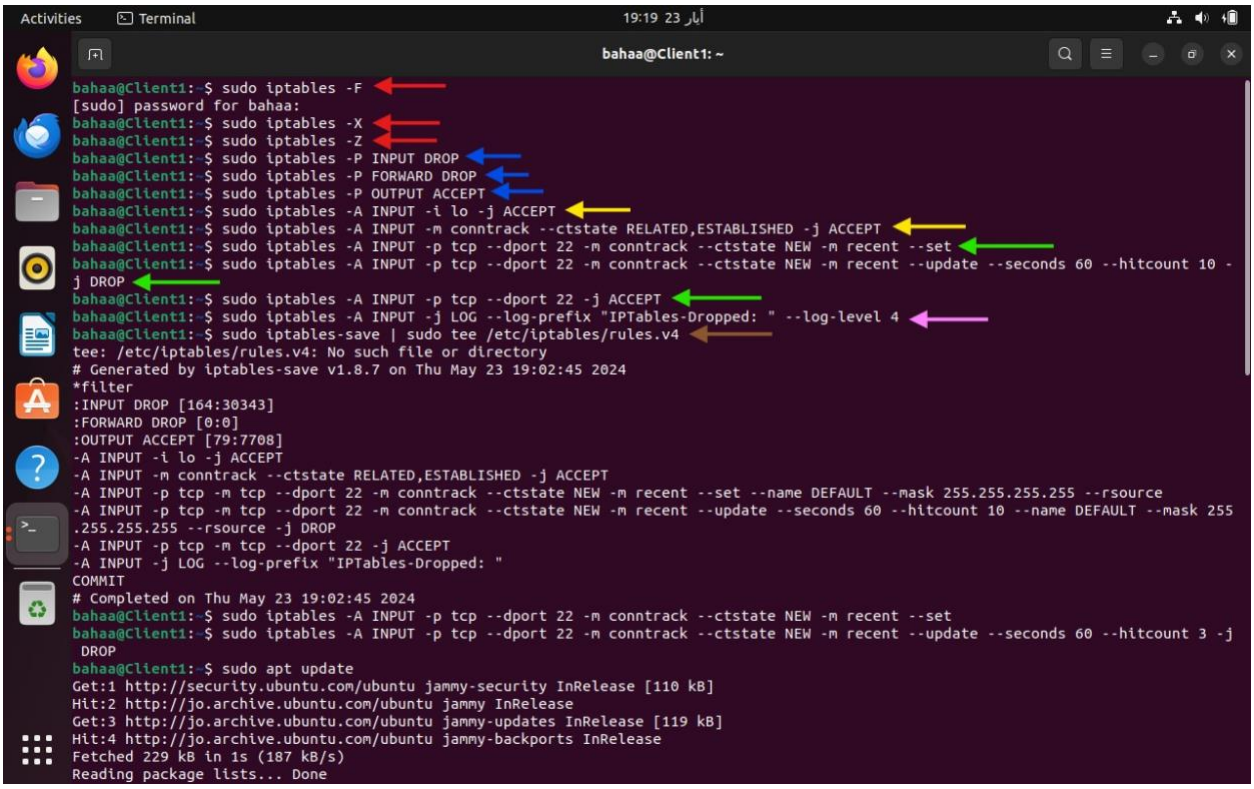
5- Set default policies within the iptables to define how packets should be handled by default(the blue arrows).

6- Allowed loopback and established connections to ensure essential network functionality(the yellow arrows).

7- Allowed SSH traffic with rate limiting to prevent brute force attacks(the green arrows).

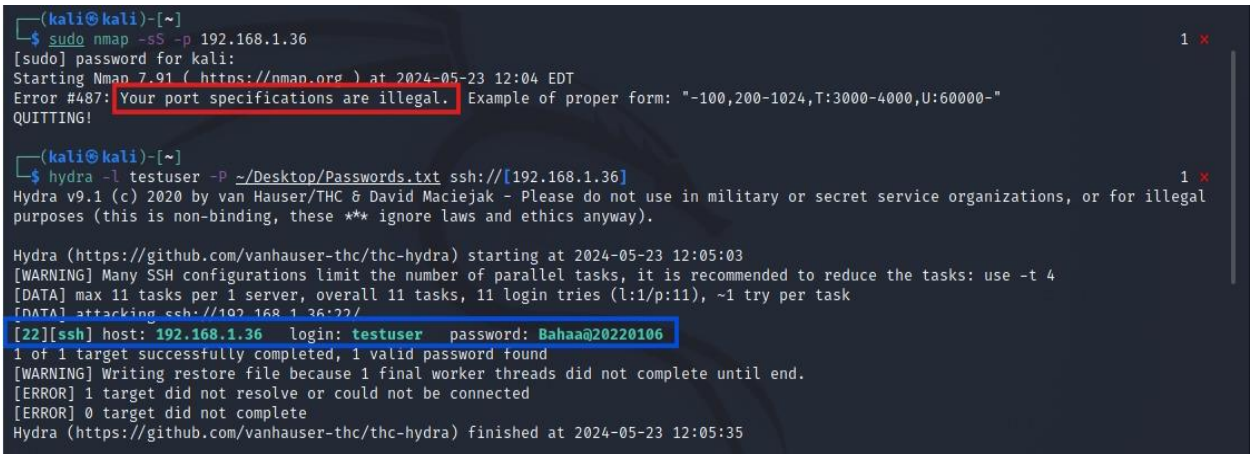
8- Configured iptables to log dropped packets, providing visibility into potential malicious activity(the pink arrow).

9- Saved the configured iptables rules to ensure they presist across reboots(the brown arrow).



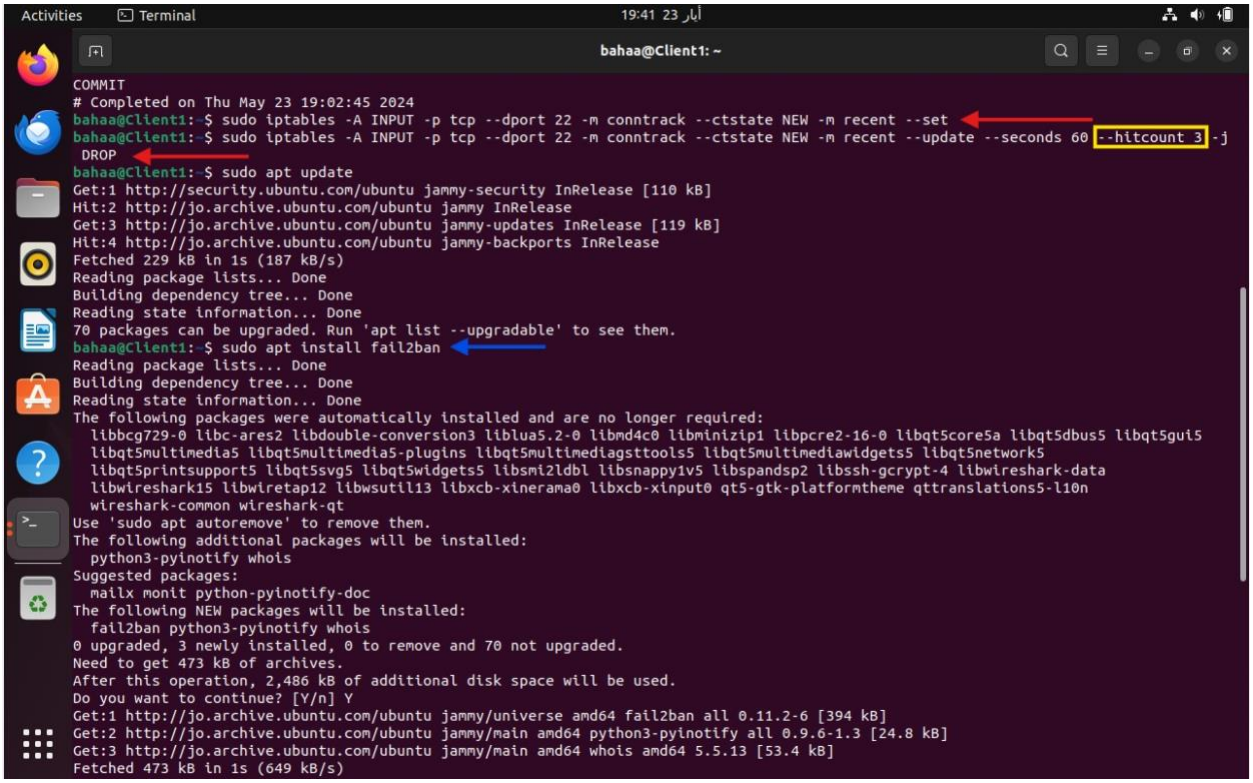
10- We proceed to the other machine to check if the ports are visible and conducted a dictionary attack to test security measures.

11- Luckily the ports were blocked (outlined with red), but a successful dictionary attack can be performed (otlined with blue) so this is a potential vulnerability.

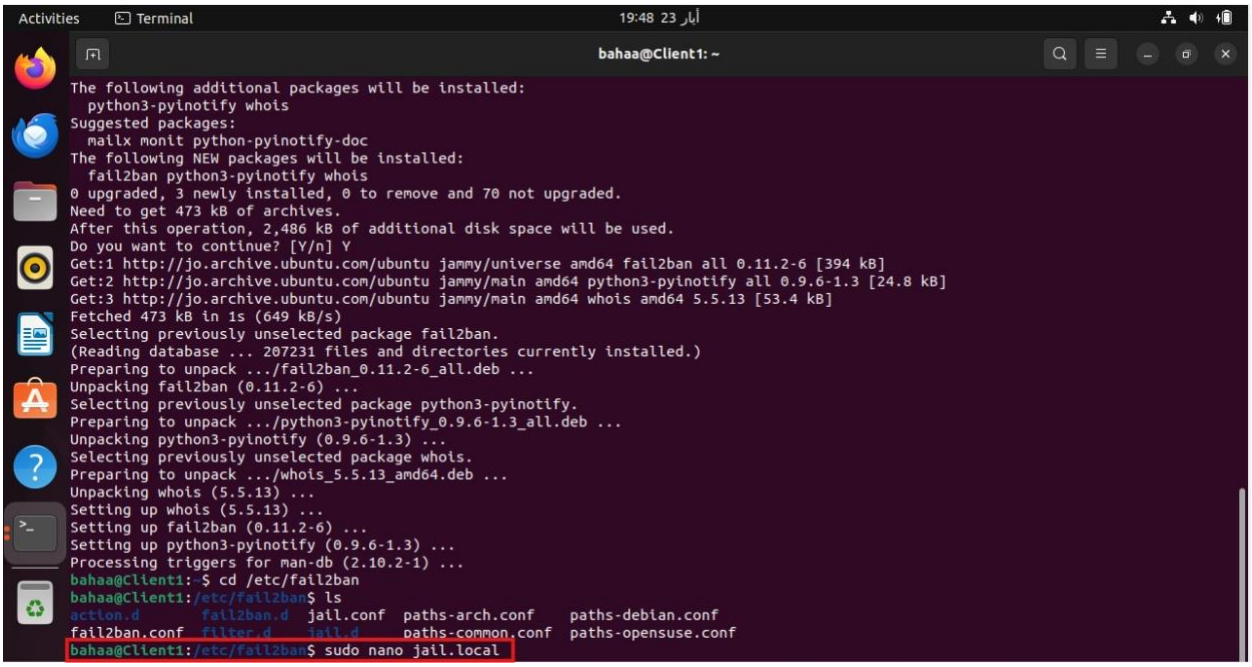


12- Went back to modify rate limiting (the red arrow) , limit the hit count to 3 attempts (outlined with yellow), enhancing security against brute force attacks.

13- We installed fail2ban, this is a tool to monitor log files and automatically ban IP adresses that make multiple failed logins(the blue arrow).



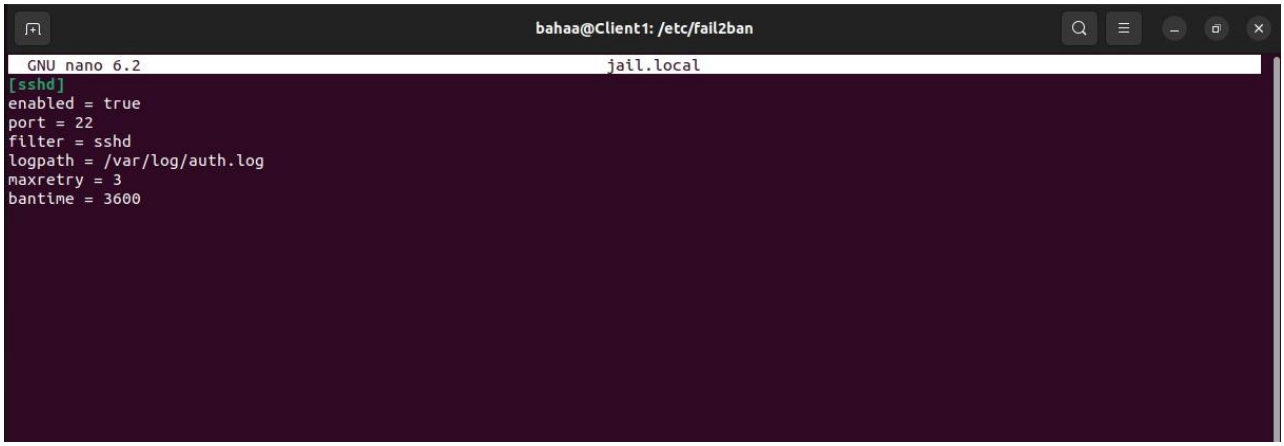
14- Configured the jail.local file.



15- Then we implemented the following:

- enable: enables jail
- port: specifies port
- filter: filter used
- logpath: log file to monitor
- maxretry: max changes
- bantime: duration of ban in seconds

Then restarted fali2ban service to apply and save the new configuration settings and enable it.

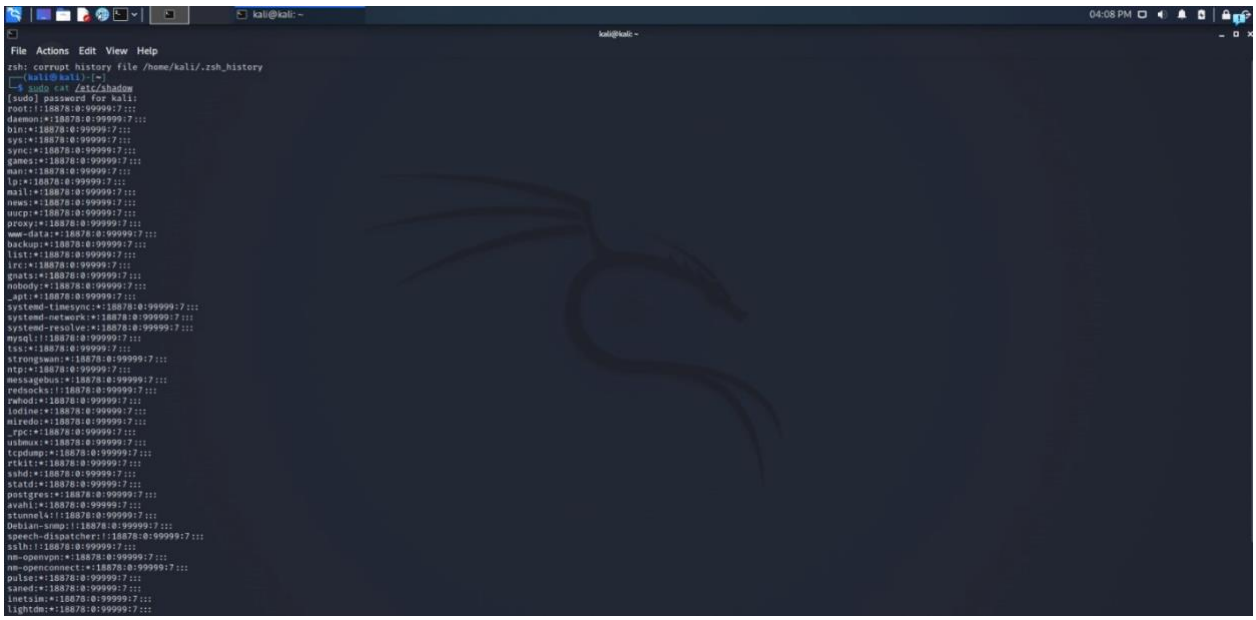


16- Finally we attempted the dictionary attack again to assess the effectiveness of the configured fail2ban settings in preventing unauthorized access.

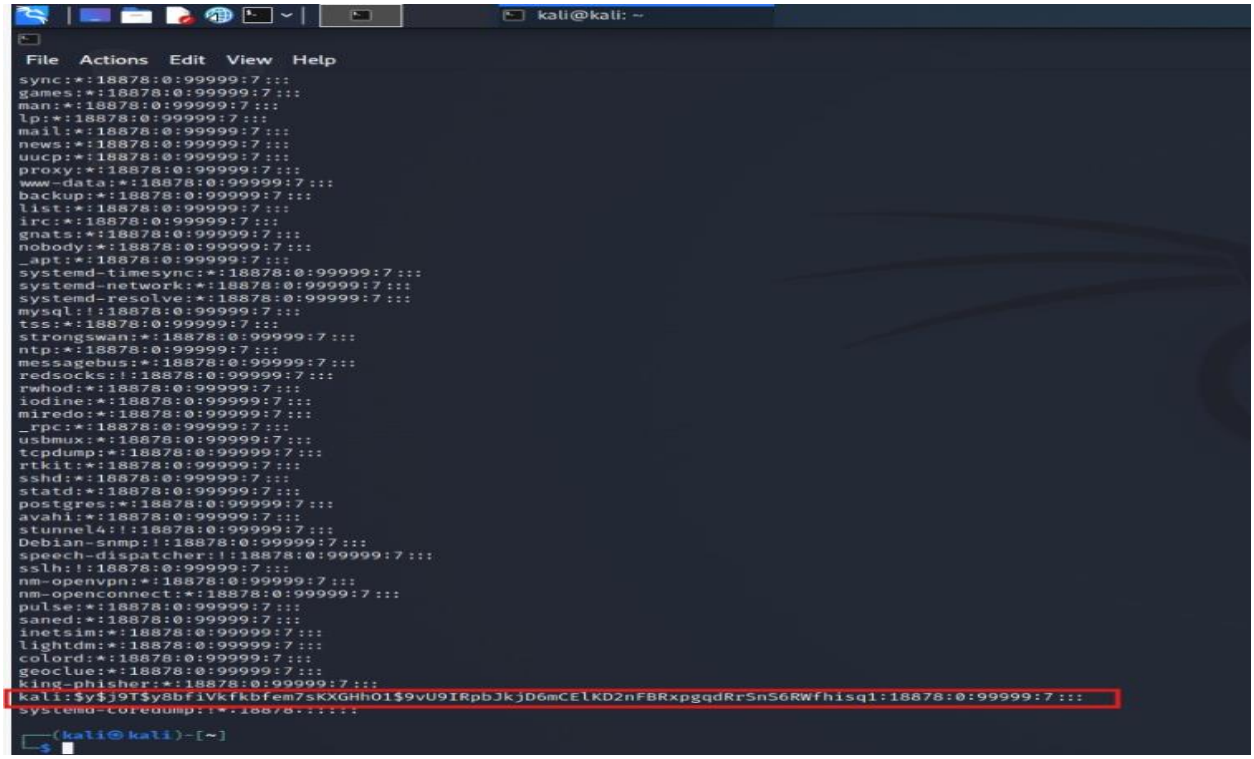
```
┌──(kali㉿kali)-[~]
└─$ hydra -l testuser -P ~/Desktop/Passwords.txt ssh://[192.168.1.36]                                    255 ✗
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-23 12:18:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 11 tasks per 1 server, overall 11 tasks, 11 login tries (l:1/p:11), ~1 try per task
[DATA] attacking ssh://192.168.1.36:22/
[ERROR] could not connect to ssh://192.168.1.36:22 - Connection refused
```

3.3 Hashing Cracking

1- First we started by accessing the shadow file that is located in /etc/shadow and scanned through the contents of the file searching for the user that we want to crack his password.

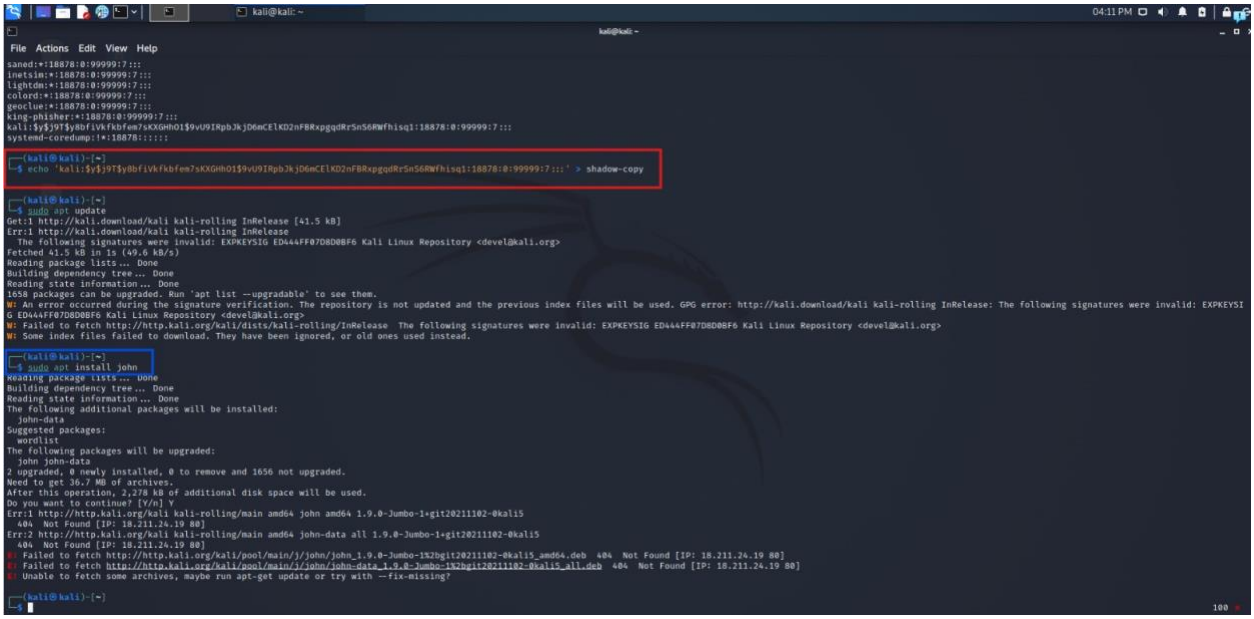


2- After we located the user that we want to hash crack his password, we copied the line containing the user's information from the shadow file, this line contains the hashed password(outlined with red).



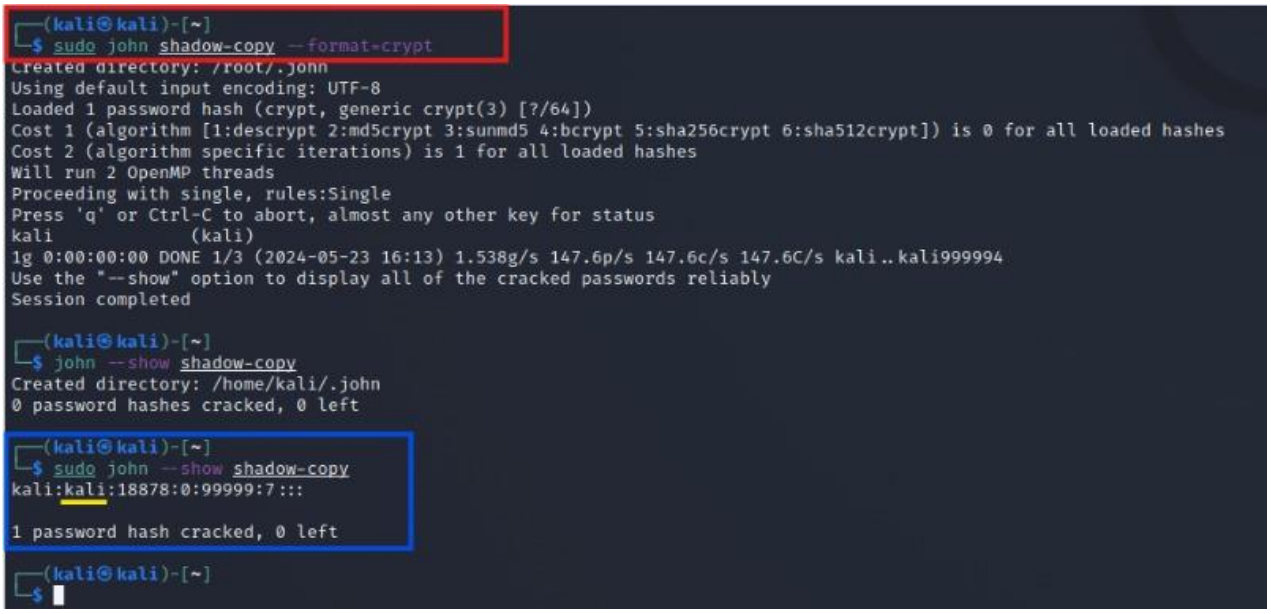
3- We created a shadow copy file named ‘shadow-copy’ to store the copied user entry, then pasted the copied line into this new file that will be used as input for John the Ripper(outlined with red).

4- Installed John the ripper, which is a popular password cracking tool, to use it for hash cracking(outlined with blue).



5- After running John the Ripper on the shadow-copy file, we were able to hash crack the password successfully.

6- Finally the cracked password was displayed, allowing us to access the user's account.



Conclusion

To sum up, this project thoroughly looked into cybersecurity ideas, starting from making secure web servers to practicing and shielding against possible attacks. We got practical experience in setting up servers, securing them with SSL encryption, and finding weak spots through simulated MITM attacks. We also learned about password cracking methods, emphasizing the need for strong security tools like firewalls and encryption. By doing these tasks, we are more prepared to handle real-world cybersecurity issues, making the digital world safer for everyone.