Capture the Flag

Comprehensive summary of each task in CTF exercise, detailing the steps taken, commands used, and challenges faced along the way.

Task 1: Compromise the Target Host

Objectives:

- Identify vulnerabilities in the target host.

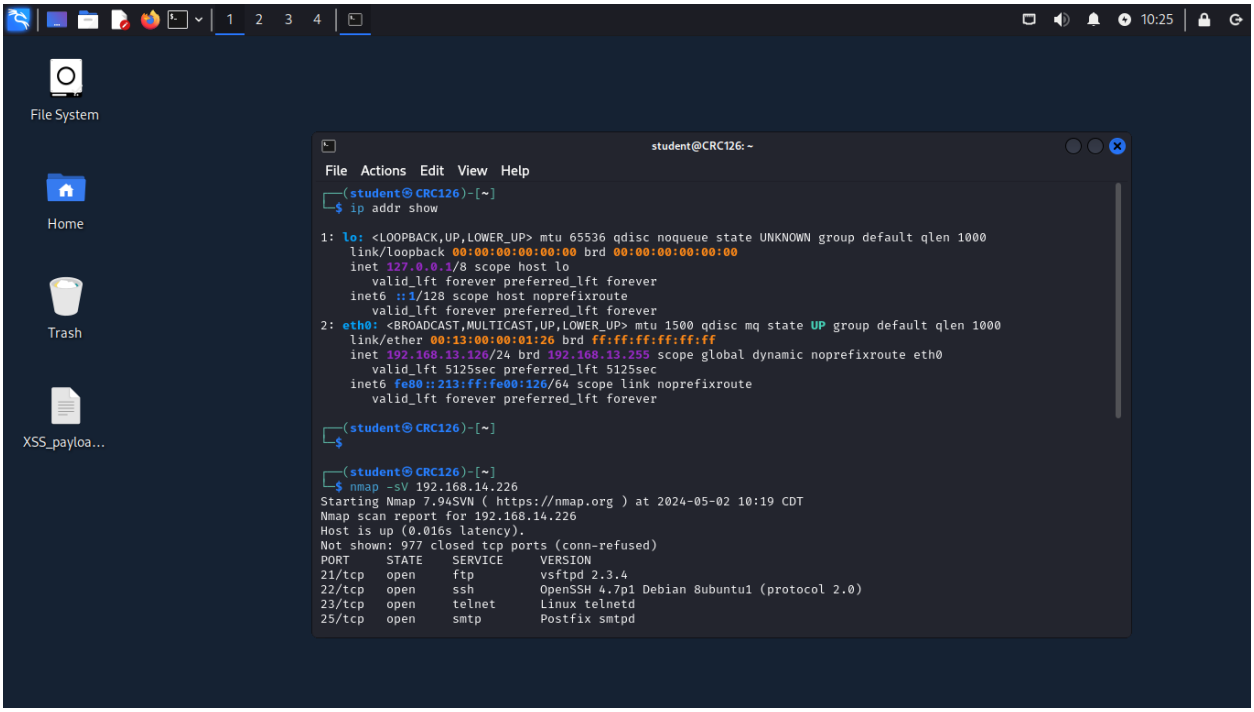
- Exploit a known vulnerability to gain filesystem access.

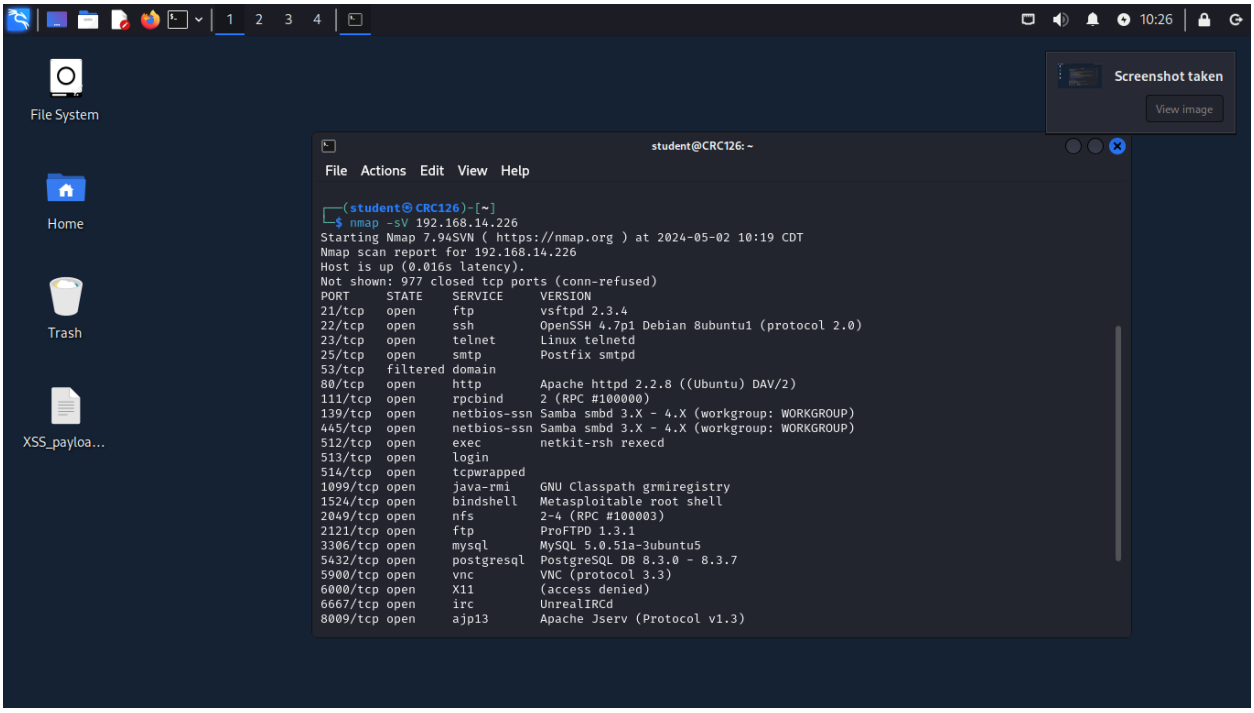
Steps and Commands:

1. Reconnaissance with Nmap:

   - Command: `nmap -sV 192.168.14.226`

   - Outcome: Discovered multiple open services including an FTP service running vsftpd 2.3.4, which is known for a backdoor vulnerability.

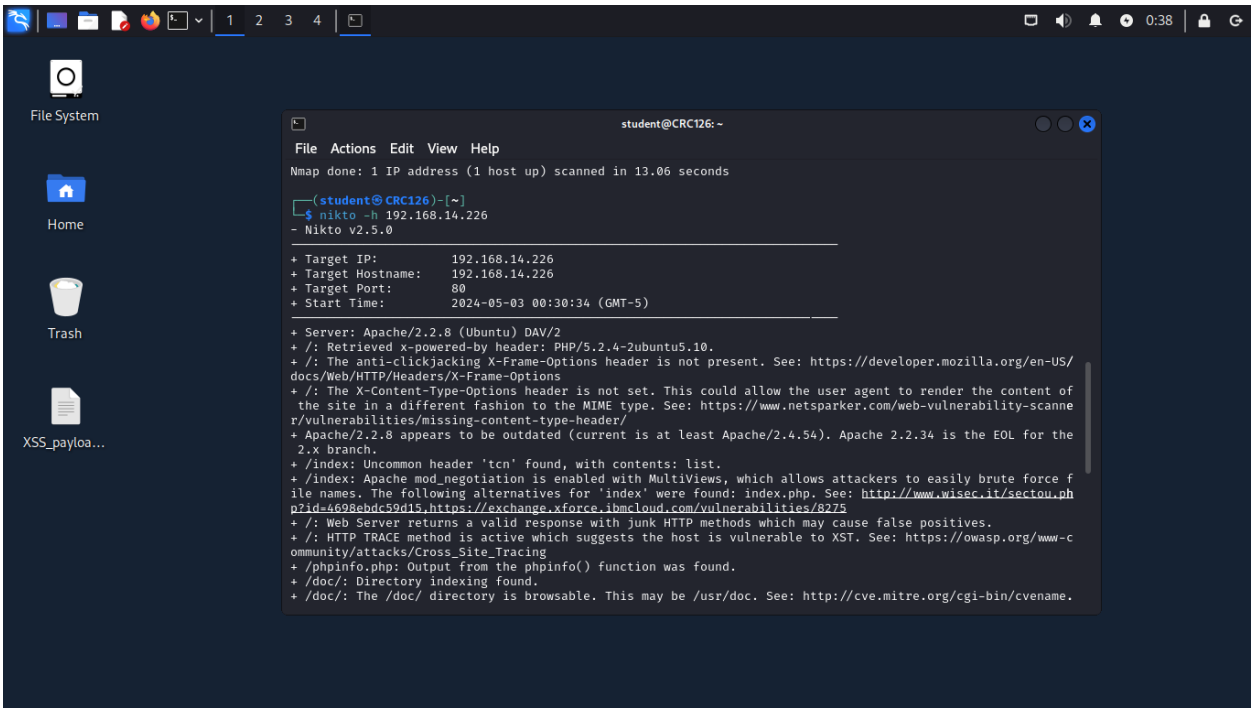




I have also used Nikto (specifically for web services) to scan for known vulnerability:

Installed Nikto with: sudo apt install nikto

Ran a web server scan: nikto -h 192.168.14.226.



2. Exploitation Using Metasploit:

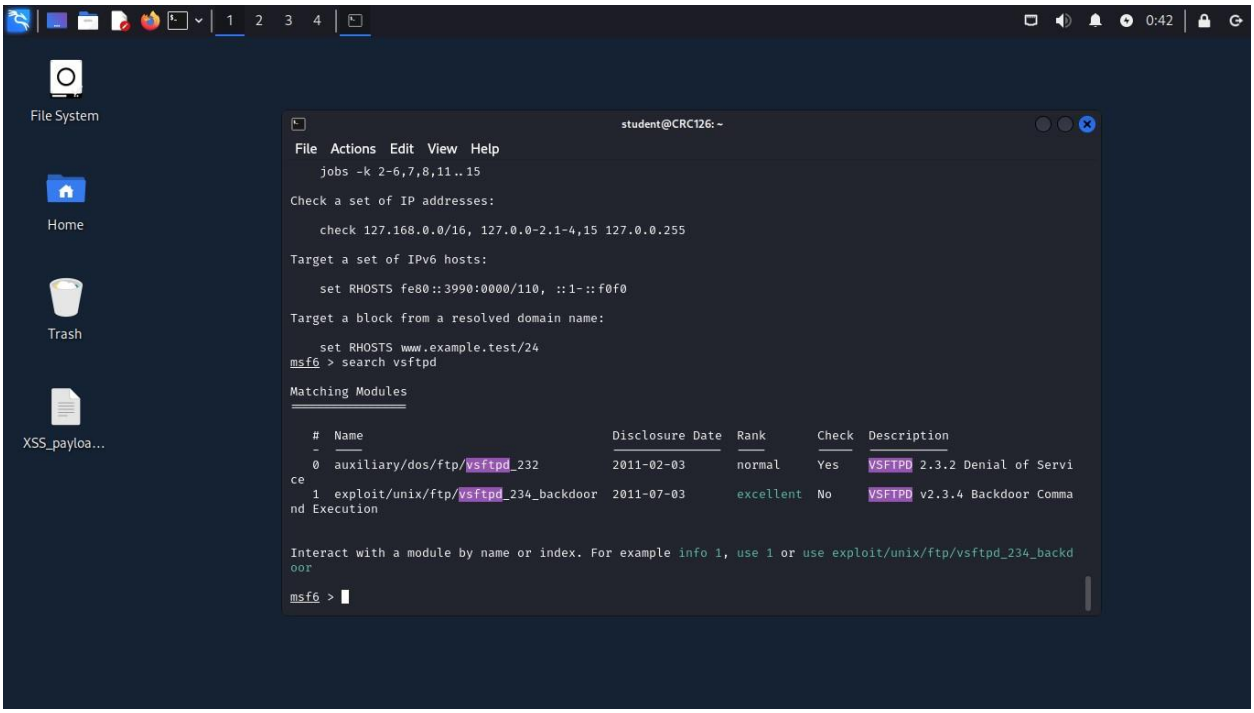
- Setup: Launched Metasploit using `msfconsole`.
- Exploit: Used the `exploit/unix/ftp/vsftpd_234_backdoor`.
- Commands:

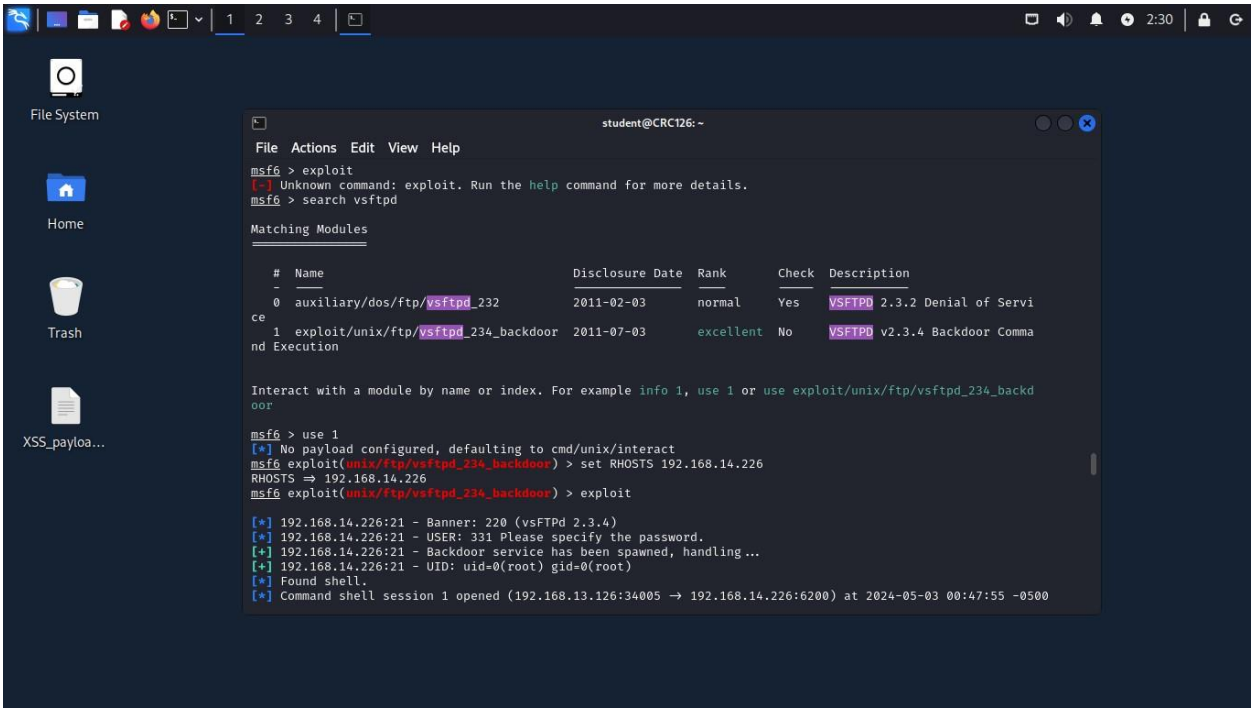
  use exploit/unix/ftp/vsftpd_234_backdoor

  set RHOSTS 192.168.14.20x

  exploit

- Outcome: Successfully exploited the service, gained root access.





Challenges:

- Initially identifying the correct IP and service to target.

- Ensuring the Metasploit module matched the identified vulnerability.

In Task 1, our objective was to identify and exploit vulnerabilities on a designated target host to gain filesystem access. I initiated this process with a thorough reconnaissance phase using Nmap to scan for open ports and services, where I discovered several potential vulnerabilities, including a notable vsftpd 2.3.4 service known for its exploitable backdoor. Utilizing Metasploit, I targeted this vulnerability specifically, successfully exploiting it to gain root access to the machine. This first task required precision in matching the identified services with known exploits and demonstrated the critical importance of accurate vulnerability assessment in cybersecurity.

Task 2: Extract the Password from the Email File

Objectives:

- Locate an email file within the compromised host.

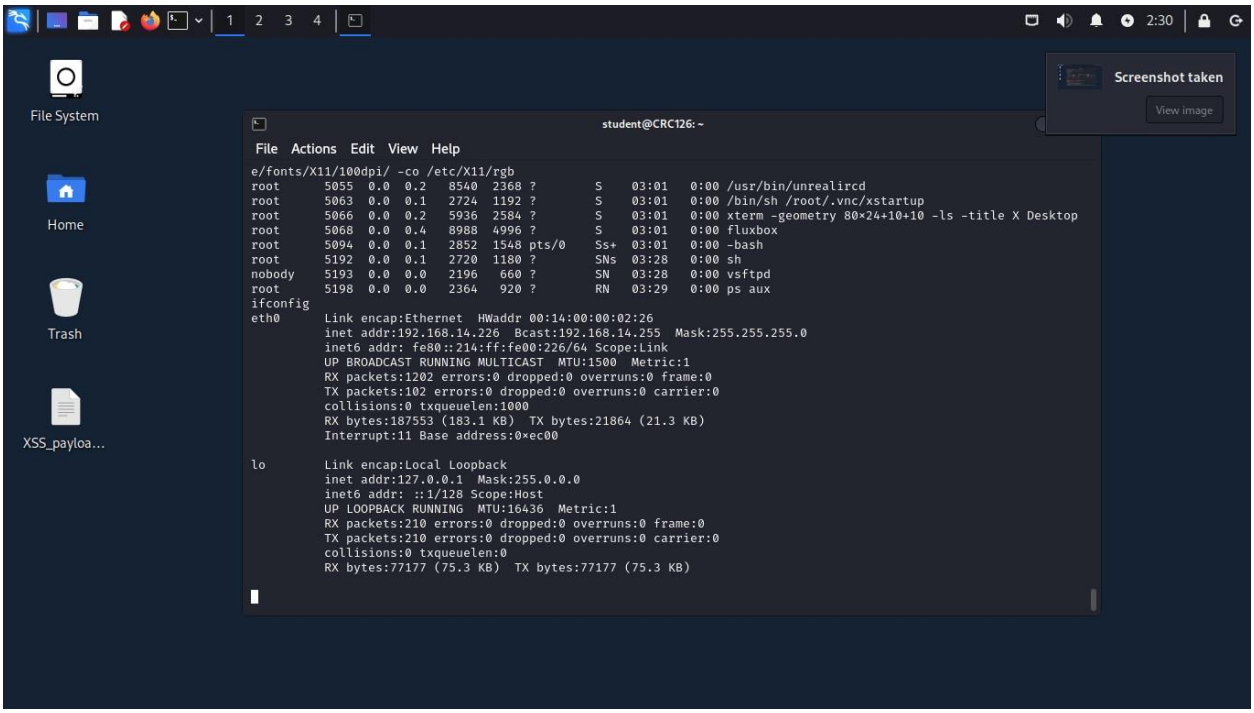
- Extract the password from the email file.

Steps and Commands:

1. Search for Email Files:

   - Command: `find /home/ -name ".eml"`

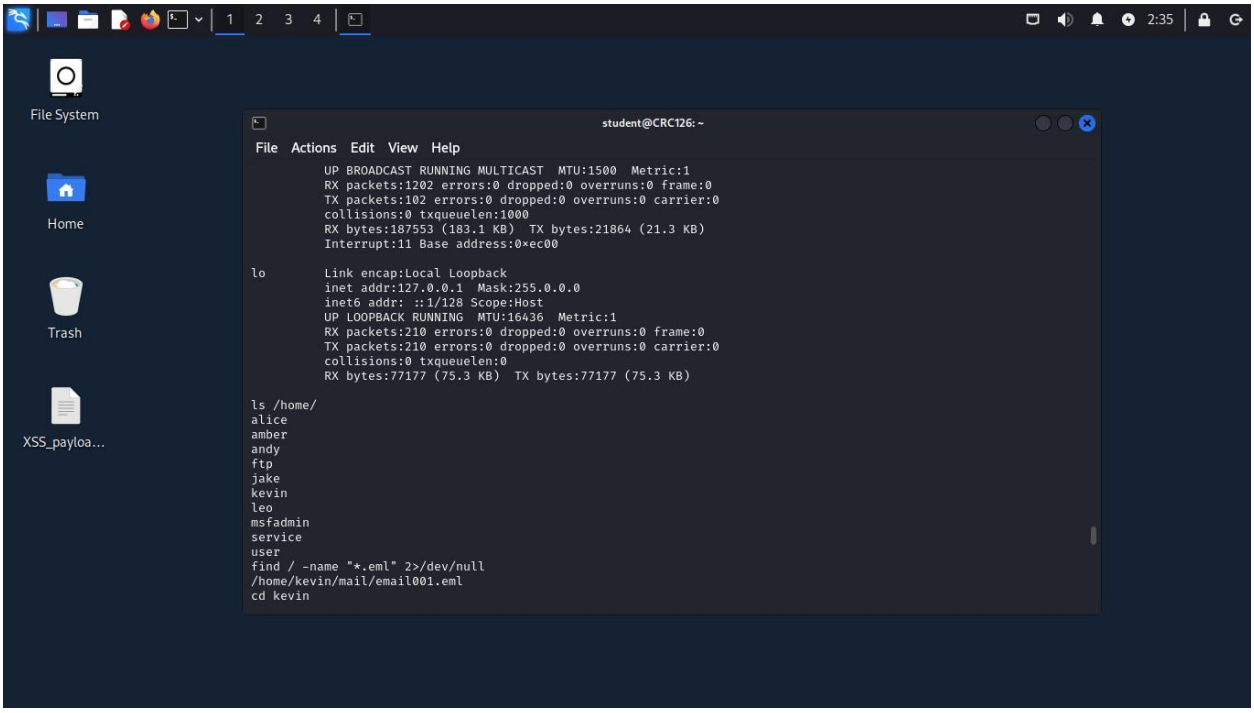
   - Outcome: Found `/home/kevin/mail/email001.eml`.



2. Extracting Information:

   - Command: `cat /home/kevin/mail/email001.eml`

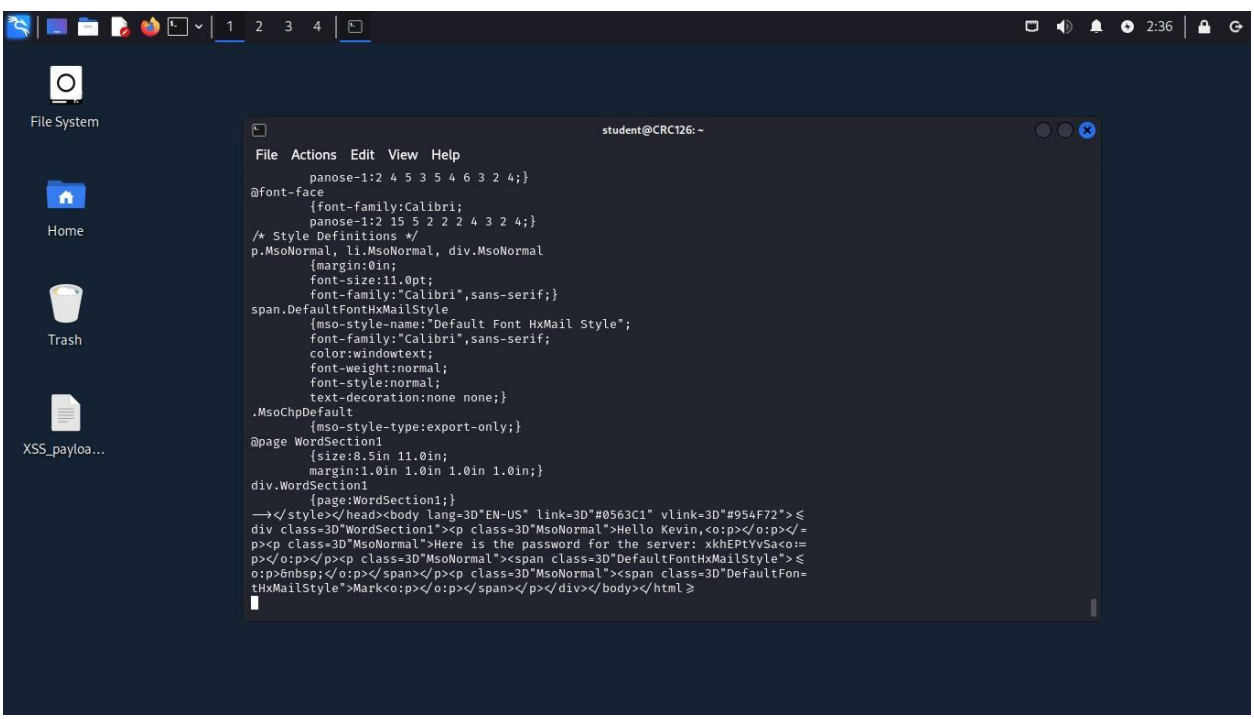
   - Outcome: Extracted sender and receiver's email addresses and the password.



Challenges:

- Searching through the filesystem without knowing the exact location of the email.

- Reading and interpreting the contents of the email correctly.



Upon gaining access to the target host's file system in Task 2, I proceeded to locate an email file that contained the password needed for the next task. Using standard command-line tools, I found an email file in the user Kevin's mail directory and extracted critical information, including the sender and receiver’s email addresses and a password. This task underscored the value of effective navigation and command utility within a Linux environment and highlighted the importance of sensitive information management within corporate or secured environments.

Task 3: Download the Top-Secret Image

Objectives:

- Identify the webserver hosting the top-secret image.

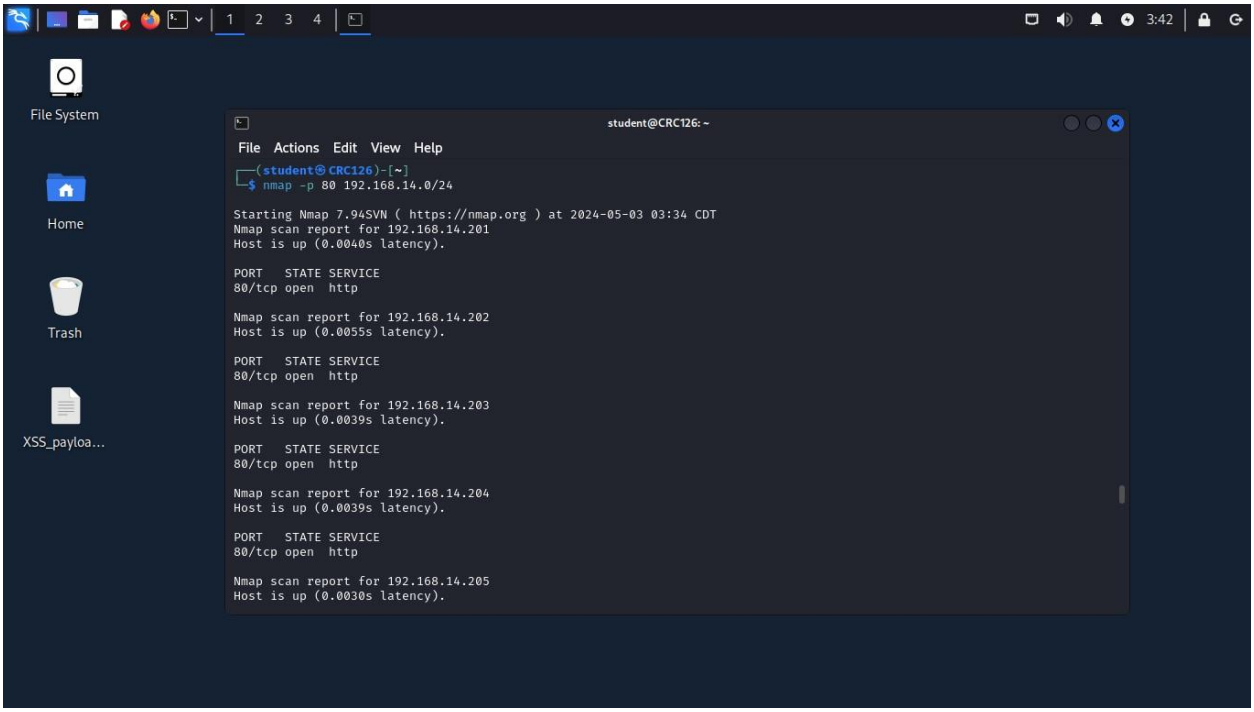
- Use the extracted password to access and download the image.

Steps and Commands:

1. Network Scanning with Nmap:

   - Command: `nmap -p 80 192.168.14.0/24`

   - Outcome: Identified multiple hosts with open HTTP ports.



2. Automated Script for Identifying Targets:

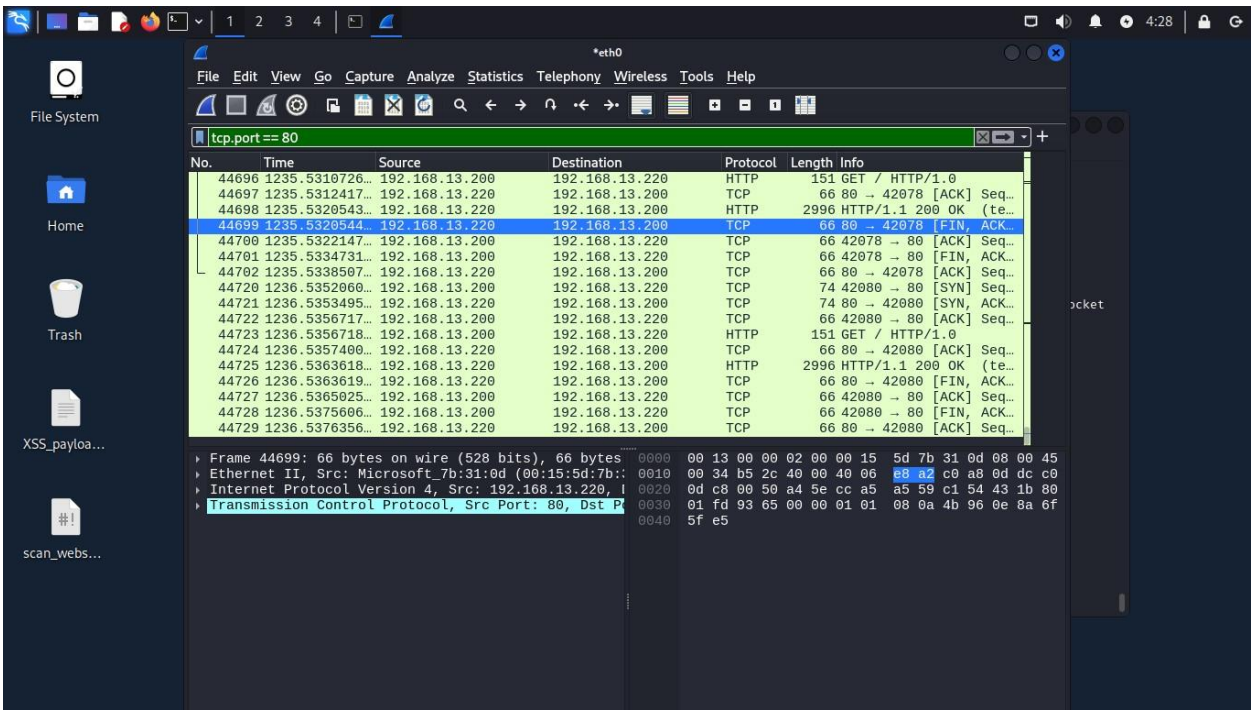
- Script Execution: `./scan_webservers.sh`

- Outcome: Script indicated multiple targets suggesting a login with "msfadmin/msfadmin".

3. Traffic Analysis with Wireshark:

- Filter Used: `tcp.port == 80`

- Outcome: Noticed frequent TCP FIN, ACK packets, which led to testing IP `192.168.13.220`.

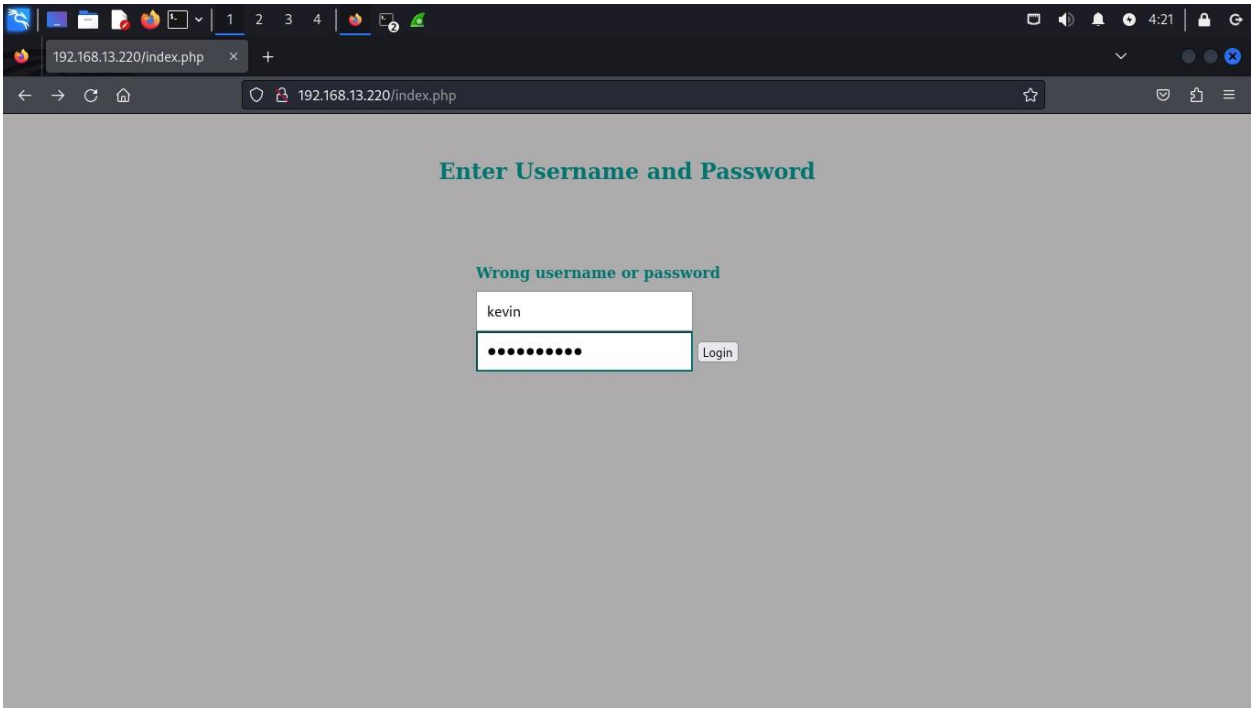


4. Accessing and Downloading the Image:

- Web Access: Visited `http://192.168.13.220` in a browser.

- Used Credentials: Username (kevin), Password (extracted from the email).

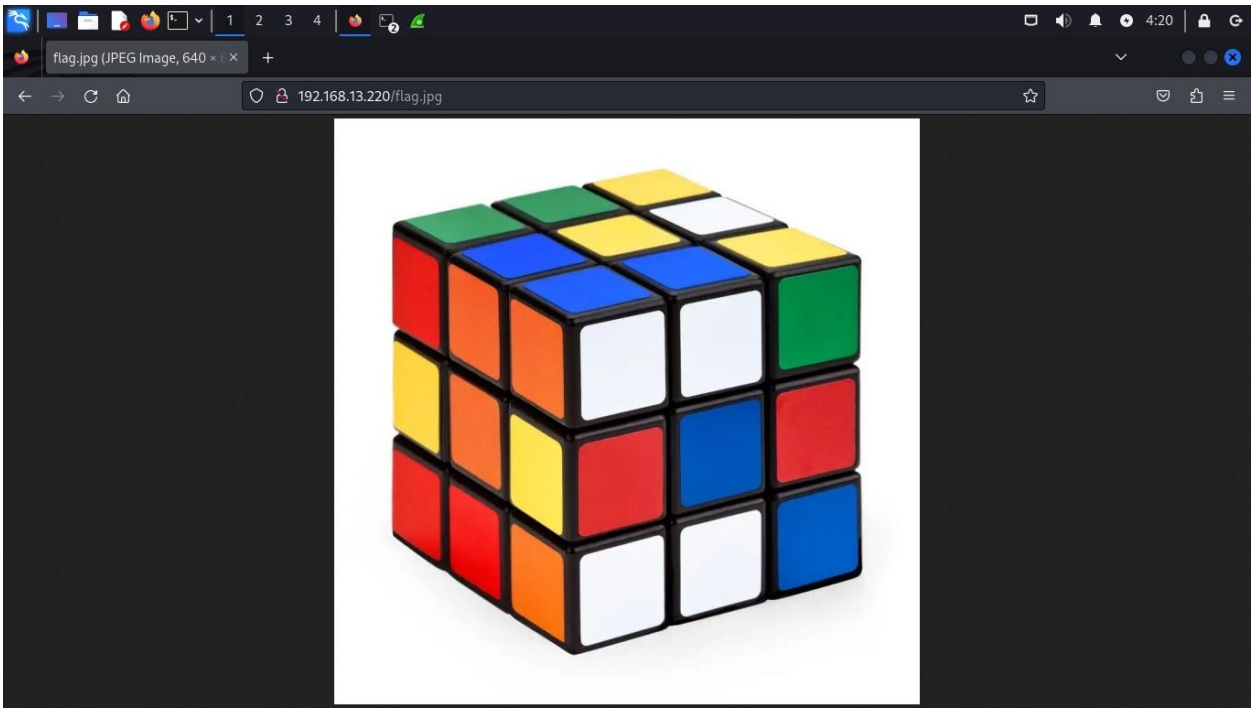
- Outcome: Successfully logged in and accessed the image.



Challenges:

- Determining the correct webserver among many.

- Initially using traffic analysis effectively to narrow down the target.



Task 3 centered on identifying and accessing a webserver within a network that hosted a top-secret image. An extensive scan of the network using Nmap revealed multiple hosts with open HTTP services. To refine search and pinpoint the exact server, I employed a custom script that identified potential servers suggesting a standardized login. Further analysis with Wireshark indicated significant traffic between hosts, leading to test specific IPs in a web browser. Upon accessing the server at IP 192.168.13.220 and using the credentials obtained from Task 2, I successfully logged in and accessed the top-secret image. This task demonstrated the integration of network traffic analysis, script automation, and practical application of extracted data to achieve a specified objective.

Conclusion

Throughout these tasks, I navigated complex cybersecurity challenges ranging from system exploitation to sensitive data extraction and secure web access. Each phase required a strategic approach, combining technical skills with critical thinking and problem-solving. This exercise not only reinforced foundational cybersecurity principles but also provided a hands-on experience in conducting thorough digital investigations and securing sensitive information against potential threats.