1. Introduction

This report documents a penetration testing exercise conducted on **Metasploitable 2**, a deliberately vulnerable virtual machine designed for security training.

---

2. Scope & Environment

- Target: Metasploitable 2 (Lab environment)
- Attacker: Kali Linux
- Tools: Nmap, Searchsploit, Metasploit

---

3. Scanning & Enumeration

A service version scan was conducted using Nmap:

```
nmap -sV <target-ip>
```

Results revealed multiple exposed services including FTP (vsftpd 2.3.4), SSH, Telnet, and MySQL.

---

4. Vulnerability Identification

The FTP service running **vsftpd 2.3.4** was identified as vulnerable to a known backdoor vulnerability. Research was conducted using Searchsploit.

---

5. Exploitation

The vulnerability was exploited using Metasploit Framework, resulting in successful bind shell access to the target system.

---

6. Impact Assessment

- Remote unauthorized access
- High risk of data exposure and system compromise

---

7. Remediation & Recommendations

- Upgrade or remove vulnerable services
- Disable insecure protocols (FTP / Telnet)
- Enforce firewall and access control policies

---

9. Video Demonstration (Unlisted):

https://youtu.be/ZePNo5Xdfv8

---

9. Conclusion

This exercise demonstrates the importance of regular vulnerability scanning, patch management, and secure system configuration to reduce attack surfaces.