Exploit Writing:
I studied how to take a proof-of-concept vulnerability and develop it into a working exploit. For example, using Python to write a script that triggers a buffer overflow, or using Metasploit's msfvenom to craft a reverse shell payload. I also learned that published exploits from Exploit-DB often serve as templates to understand exploit structure.

Mitigations:
I realized that modern systems use protections such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP), and Web Application Firewalls (WAFs). While these make exploitation harder, attackers often develop bypass techniques, which shows the importance of layered defenses.

Key Takeaways
From this study, I understood that:

- Exploits are built on deep technical knowledge of vulnerabilities and system internals.
- Writing even simple exploits requires safe practice in isolated labs.
- Defenses like ASLR and DEP exist to reduce the success of exploits, but attackers continuously look for ways around them.

Learning Resources
To strengthen my understanding, I studied proof-of-concept exploits on Exploit-DB, which helped me see how vulnerabilities are weaponized. I also explored TCM Security's exploit development guides. A notable case study I reviewed was EternalBlue (MS17-010), which was weaponized into the WannaCry ransomware showing how powerful exploit development can be when vulnerabilities are left unpatched.

Practical Applications.

1. **Vulnerability Scanning Lab**

   Summary of Findings.

   The Web Vulnerability Assessment and Penetration Testing (VAPT) conducted for the target organization Metasploit (192.168.56.104) yielding to important findings and insights. This summary provides an overview of the key results obtained during the assessment. It was observed that the application was exposed to a total of 21

security vulnerabilities during the given assessment tenure with 5 as Critical, 14 as High, and 2 as Medium Severity vulnerabilities

Scan ID	Vulnerability	CVSS Score	Priority	Host
001	vsftpd 2.3.4 Backdoor (FTP)	10.0	Critical	192.168.56.104
002	OpenSSH 4.7p1 (Outdated, Weak Algorithms)	7.5	High	192.168.56.104
003	Telnet Service Enabled	8.0	High	192.168.56.104
004	Postfix smtp (Potential Open Relay)	5.0	Medium	192.168.56.104
005	ISC BIND 9.4.2 (DoS/Cache Poisoning Vulns)	7.5	High	192.168.56.104
006	Apache httpd 2.2.8 (Multiple Vulns, CVE-2007-6750, CVE-2011-3192)	7.5	High	192.168.56.104
007	RPC services exposed (rpcbind, nfs)	6.5	Medium	192.168.56.104
008	Samba 3.x–4.x (Remote Code Execution, CVE-2007-2447)	9.3	Critical	192.168.56.104
009	rlogin service enabled (Cleartext Auth)	7.0	High	192.168.56.104
010	Netkit-rsh rexecd (Insecure Remote Exec)	7.5	High	192.168.56.104
011	Netkit rshd (Remote Shell, Cleartext)	7.5	High	192.168.56.104
012	Metasploitable root shell service	10.0	Critical	192.168.56.104
013	NFS (Unauthenticated Share Access)	7.8	High	192.168.56.104
014	ProFTPD 1.3.1 (Backdoor in Some Builds)	7.5	High	192.168.56.104
015	MySQL 5.0.51a (Weak Auth, Known Vulns)	7.5	High	192.168.56.104
016	PostgreSQL 8.3.x (Weak Auth, CVEs)	7.5	High	192.168.56.104
017	VNC (No Encryption, Default Password Risk)	7.5	High	192.168.56.104

Scan ID	Vulnerability	CVSS Score	Priority	Host
018	X11 Service Open (Unauthenticated Access)	7.5	High	192.168.56.104
019	UnrealIRCd (Backdoor, CVE-2010-2075)	10.0	Critical	192.168.56.104
020	Apache Jserv Protocol (AJP13) exposed	7.0	High	192.168.56.104
021	Apache Tomcat (5.5/6.0, Manager RCE Vulns)	9.0	Critical	192.168.56.104

Vulnerability Findings and Remediation:

1. vsftpd 2.3.4 Backdoor (FTP)

- **Finding:** This version contains a known backdoor that allows attackers to gain root access remotely.
- **Remediation:** Remove or disable vsftpd 2.3.4. Install the latest **secure FTP service** (vsftpd > 3.x or switch to SFTP).

2. OpenSSH 4.7p1 (Outdated, Weak Algorithms)

- **Finding:** Old version vulnerable to brute force and weak cipher attacks.
- **Remediation:** Upgrade to **latest OpenSSH**. Disable weak algorithms (e.g. DES, MD5). Use only strong ciphers (AES, ChaCha20).

3. Telnet Service Enabled

- **Finding:** Telnet transmits credentials in cleartext, making it easy to intercept.
- **Remediation:** Disable Telnet. Replace with **SSH** for secure remote management.

4. Postfix SMTP (Potential Open Relay)

- **Finding:** Misconfiguration can allow mail relay abuse for spam or phishing.
- **Remediation:** Configure Postfix to **disable open relay**. Restrict relaying to authenticated users only.