==

PHASE 3 – EXPLOITATION
VAPT PRACTICAL REPORT

==

Analyst Name :priyank
Phase   : Exploitation
Environment : Kali Linux
Target Type : Vulnerable Test Machine (Lab Environment)

==

1. INTRODUCTION

==

The objective of the exploitation phase is to validate identified vulnerabilities by safely exploiting them in a controlled lab environment. This phase confirms whether vulnerabilities can be used to gain unauthorized access, execute commands, or extract sensitive information.

The exploitation was performed using three industry-standard tools: Metasploit Framework, sqlmap, and Exploit-DB (PoC validation).

==

2. TOOL 1: METASPLOIT FRAMEWORK

==

Tool Name   : Metasploit Framework
Purpose   : Exploit known vulnerabilities and gain remote access

----

2.1 Vulnerability Exploited

Service   : FTP
Vulnerability : vsftpd 2.3.4 Backdoor
Target IP   : 192.168.79.129
Port   : 21

2.2 Exploit Used

Module Name:
exploit/unix/ftp/vsftpd_234_backdoor

2.3 Result

The exploit successfully spawned a backdoor shell on the target system. Root-level access was obtained, confirming that the vulnerability is critical and easily exploitable.

2.4 Impact

An attacker can gain full system control without authentication, leading to data theft, service disruption, or further lateral movement.

3. TOOL 2: SQLMAP

Tool Name : sqlmap
Purpose : Automated SQL Injection exploitation

3.1 Vulnerability Exploited

Vulnerability Type : SQL Injection
Application : DVWA (Damn Vulnerable Web Application)
Attack Vector : HTTP GET/POST parameter

3.2 Command Used

```
sqlmap -u "http://127.0.0.1/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
--cookie="security=low; PHPSESSID=XXXX"
--dbs
```

3.3 Result

sqlmap successfully identified the SQL injection vulnerability and extracted database names from the backend database.

3.4 Impact

Successful SQL injection allows attackers to read, modify, or delete database data, potentially leading to credential compromise and complete application takeover.

4. TOOL 3: EXPLOIT-DB (PoC VALIDATION)

Tool Name : Exploit-DB
Purpose : Vulnerability proof-of-concept validation

4.1 Activity Performed

Public exploit code related to the identified vulnerabilities was searched and reviewed on Exploit-DB.

4.2 Validation

The vulnerabilities exploited using Metasploit and sqlmap were found to have publicly available proof-of-concept exploits, confirming that these issues are well-known and actively exploitable.

4.3 Impact

Availability of public exploits significantly increases real-world attack risk, as attackers require minimal skill to compromise the target.

5. EXPLOITATION SUMMARY TABLE

Exploit ID	Tool	Vulnerability	Target IP	Status
003	Metasploit	vsftpd Backdoor RCE	192.168.79.129	Success

6. CONCLUSION

The exploitation phase successfully validated critical vulnerabilities identified during scanning. All three tools demonstrated that the target systems are highly vulnerable and susceptible to real-world attacks. Immediate remediation and secure configuration changes are recommended to reduce risk.

==

END OF REPORT

=======================================