Cyber Security Base – Module 5.1 – Project Report

Student: Mahmoud Sakr
Course: Cyber Security Base – Module 5.1
Environment: Kali Linux + Metasploitable3 (VMware)

---

1. Project Overview

The purpose of this project is to demonstrate practical cybersecurity attacks on a controlled virtual environment. The project uses **DVWA (Damn Vulnerable Web Application)** hosted on **Metasploitable3**, with **Kali Linux** as the attacker machine. The main objective is to identify, exploit, and document **common vulnerabilities** while applying **Threat Modeling techniques** such as **STRIDE** and **OWASP Top 10**.

The attacks cover both **web-based vulnerabilities** (SQL Injection, XSS, Command Injection) and **service-based attacks** (SSH and Telnet weak authentication). All actions were executed in a **virtual lab** environment, ensuring no impact on real systems. Screenshots and log files were captured as **evidence of exploitation**.

---

2. Environment Setup

- **Attacker VM:** Kali Linux
- **Target VM:** Metasploitable3
- Both VMs are configured on a **Host-Only network**.
- DVWA security level set to **Low**.
- Tools used: Nmap, Dirb/Gobuster, Snort, Excel, Python (optional for analysis)

---

3. Reconnaissance and Scanning

3.1 Host and Port Scanning

Command: `sudo nmap -sV -p- 192.168.x.x -oN scans/nmap_full.txt`
Output saved in `scans/nmap_full.txt`. Shows open ports for HTTP, SSH, Telnet, FTP, MySQL.

3.2 Web Content Discovery

Command: `dirb http://192.168.x.x /usr/share/wordlists/dirb/common.txt -o scans/dirb.txt`
Output saved in `scans/dirb.txt`. Discovered DVWA endpoints for SQLi, XSS, Command Injection.

---

4. Exploitation – Proof of Concept

4.1 SQL Injection

- **Vulnerability:** SQL Injection
- **Component:** DVWA SQL Injection page
- **Execution:** Inputted `' OR '1'='1` to bypass authentication.
- **Impact:** Extracted user credentials.

4.2 XSS Reflected

- **Vulnerability:** Cross Site Scripting (Reflected)
- **Component:** DVWA XSS page
- **Execution:** `<script>alert('XSS')</script>`
- **Impact:** Code executed on client browser.

4.3 Command Injection

- **Vulnerability:** Command Injection
- **Component:** DVWA Command Injection page
- **Execution:** `whoami` command executed.
- **Impact:** Commands executed with web server privileges.

4.4 SSH Weak Authentication

- **Vulnerability:** Weak Authentication
- **Component:** SSH on Metasploitable3
- **Execution:** Default credentials `msfadmin:msfadmin`.
- **Impact:** Remote access gained.

4.5 Telnet Weak Authentication

- **Vulnerability:** Weak Authentication
- **Component:** Telnet on Metasploitable3
- **Execution:** Default credentials `msfadmin:msfadmin`.
- **Impact:** Command line access gained.

---

5. Threat Modeling

PoC	Vulnerability	STRIDE	OWASP Top 10	Notes
SQL Injection	Injection	Tampering, Info Disclosure	A03	Extracted user data
XSS Reflected	XSS	Elevation of Privilege	A05	Alert may not show

PoC	Vulnerability	STRIDE	OWASP Top 10	Notes
Command Injection	Command Injection	Tampering, Elevation	A03	whoami → www-data
SSH Attack	Weak Authentication	Elevation of Privilege	A01	Default credentials login
Telnet Attack	Weak Authentication	Elevation of Privilege	A02	Default credentials login

Diagram Suggestion:

```
[User Input] --> [DVWA Page] --> [SQLi/XSS/Command Injection] --> [Data/Code Execution]
[Attacker] --> [SSH/Telnet] --> [System Access]
```

6. Conclusion

- Successfully exploited 5 attacks on DVWA and Metasploitable3.
- Threat Modeling completed for all attacks using STRIDE and OWASP Top 10.
- Demonstrates practical application of cybersecurity concepts in a controlled lab.