Web Application Exploitation & Network Traffic Analysis

Project-3: Web Login Exploitation & Network Traffic Monitoring

1. Objective

The objective of this project is to identify a vulnerable web application using network scanning, exploit web application vulnerabilities, and analyze the generated network traffic using packet capture tools.

2. Scope

Target Application: DVWA (Damn Vulnerable Web Application)
Testing Type: Black-box Testing
Environment: Local Virtual Lab

3. Tools Used

Tool	Purpose
Nmap	Network & service discovery
Metasploit Framework	Web exploitation
Wireshark	Traffic capture & analysis
Kali Linux	Attacking machine
DVWA	Vulnerable target application

4. Methodology

- Network Discovery using Nmap
- Web Service Enumeration
- Vulnerability Identification
- Web Exploitation using DVWA & Metasploit
- Network Traffic Capture using Wireshark
- Security Analysis & Reporting

5. Key Findings

Port	Service	Vulnerability	Severity
80	HTTP	Weak Authentication	High
80	HTTP	Command Injection	Critical

6. Network Traffic Analysis

Wireshark was used to capture HTTP traffic during the attack. Plain-text credentials, command injection payloads, and server responses were observed, demonstrating the risks of unencrypted web traffic.

7. Security Risks

- Credentials transmitted in plain text
- Remote command execution possible

- No intrusion detection mechanism
- Complete system compromise risk

8. Mitigation & Recommendations

- Enable HTTPS (TLS encryption)
- Implement strong input validation
- Use Web Application Firewall (WAF)
- Deploy IDS/IPS solutions
- Enforce strong authentication policies

9. Conclusion

This project successfully demonstrated how attackers can exploit vulnerable web applications and how network traffic analysis can be used to detect such attacks. Proper security controls are essential to protect against real-world threats.