Network Penetration Testing Project Report

1. Introduction

This project demonstrates real-world penetration testing using DVWA (Damn Vulnerable Web Application) as the target system hosted on Metasploitable2, and Kali Linux as the attacking system. Various techniques such as scanning, enumeration, exploitation, and remediation have been performed using well-known tools.

2. Tools Used

- Kali Linux (Attacker Machine)
- Metasploitable2 with DVWA (Target Machine)
- Nmap
- Nikto
- Burp Suite
- Hydra
- John the Ripper

3. Tasks Performed

- Network Scanning using Nmap
- Web vulnerability scanning using Nikto and Burp Suite
- SQL Injection on DVWA
- Command Injection and File Upload exploits
- Brute Force attack using Hydra on login forms
- Password hash extraction and cracking using John the Ripper

4. Sample Commands

nmap -v -sV -O 192.168.1.101

hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.1.101 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^:Login failed"

john hash.txt

nikto -h http://192.168.1.101/dvwa

5. Findings

- Found SQL Injection vulnerability in DVWA
- Found hidden ports with services using Nmap (-p-)
- Successfully cracked password hashes using John

6. Remediation

- Update DVWA and Apache to the latest version to patch known vulnerabilities
- Disable unused services and close unnecessary ports
- Implement strong password policies to resist brute-force attacks
- Monitor and log suspicious access attempts

7. Major Learning Outcomes

Through this project, I have learned how to set up a lab for penetration testing, perform vulnerability scanning, exploit web vulnerabilities, and understand the importance of patch management and securing web applications.