Detailed Plan for the Project

Objective

- To correctly identify and exploit vulnerabilities in a Windows VM Web Server.
- To highlight software issues and document each step while generating logs for analysis.

Tools To Use

Target Machine: Windows 10 VM (configured with XAMPP for the Web Server)

Attack Machine: Kali Linux VM

To Use:

- Nmap
- Nessus
- Nikto
- Gobuster
- Metasploit
- Wireshark
- Others (will adapt during Implementation phase)

Strategy and Steps

Setup

- Ensure Kali Linux is ready for Implementation.
- Configure XAMPP on Windows 10 VM.
- Enable Logging on the Windows VM to capture activity.
- Create three dummy files on the Windows VM for post-exploitation.

Reconnaissance

- Conduct the network scan on Nmap to identify open ports and active hosts.
- Use whois to obtain information about the domain.

Enumeration

- Run Nessus to find vulnerabilities in the target server.
- Run Nikto to scan the web server for vulnerabilities.
- Run Gobuster to enumerate directories and files.

Analyze Vulnerabilities

- Review the scan results from Nessus and cross-reference with the CVE databases.
- Determine the impact and severity of the vulnerabilities.
- Prioritization will be based on higher risk vulnerabilities.

Exploitation

- Run Metasploit to exploit the identified vulnerabilities.
- Continue documenting each step along the way.

- Provide evidence of the successful exploitation, using screenshots and captured footage.

Post-Exploitation

- Utilize Meterpreter to explore the web server.
- Extract information, providing proof by obtaining specific files I create on the target machine.
- Document my findings via screenshot and captured footage.

Documentation and Reporting

- Provide evidence, including logs and visual evidence provided, into a report.
- Include recommendations to fix the web server's vulnerabilities.

Expected Outcome

- Provide identification of the vulnerabilities.
- Provide evidence of the exploitation.
- Provide logs of all activity and document the process of the penetration test.
- Provide recommendations for the identified vulnerabilities.