Penetration Testing: Web Applications

Duration: 40 hrs (5days)

Module 1: Introduction to Ethical Hacking & Penetration Testing

- What is Penetration Testing?
- Difference Between Ethical Hacking & Cybercrime
- Pen Testing Methodologies (PTES, OWASP, NIST)
- Legal & Ethical Considerations

Module 2: **Introduction to tools useful for Web Application Pen testing**

- WHOIS, nslookup, Ping
- Nmap, Wireshark, Burp suite

Module 3: Vulnerability Assessment

- Understanding CVEs & Vulnerabilities
- Using Vulnerability Scanners (Nessus, OpenVAS)
- Introduction to Metasploit Framework

Module 4: **Exploitation & Gaining Access (Theory + Hands-on)**

- Exploiting Common Vulnerabilities
- SQL Injection (use cases: Data breaches, database access, account takeover)
- XSS (Reflected , Stored, DOM-based) Use case: Stealing cookies, session hijacking, phishing attacks
- OS Command Injection
- File Inclusion
- Cross-Site Request Forgery (CSRF)
- Hand on using the sample application using all common vulnerabilities

Module 5: OWASP Top 10 for web application (Theory+ Hands-on) – Top 5

- ***Explain the theory and use sample web applications to show the vulnerabilities, how to identify using tools, damages caused***
- Broken access control
- Cryptographic Failures

- Injections (only overview, already covered in module 4)
- Insecure Design
- Security misconfiguration

Module 6: OWASP Top 10 for web application

- ***Explain the theory and use sample web applications to show the vulnerabilities, how to identify using tools***
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery (SSRF)

Module 7: How to fix common web application pen test findings

(Examples given)

- Distributed Denial Of Service Attacks(DDoS)
- HTML Injection Validation (UI & API)
- Missing HTTP security headers
- Verbose errors with detailed backend information
- Cloud related: Removing public access for PaaS resources, WAF
- No sensitive information in URL/query params

Module 8: Pen test best practices for Thick clients

{Should include Tools used, penTest approach for the exploit and mitigation measures}

- Registry / File monitoring
- Privilege escalation
- DLL Hijacking / Remote Code Execution
- Reverse Engineering (considering C#/java as programming language)
- Tools: TCP View, CFF Explorer, Regshot, Winhex