Web Application Penetration Testing with Kali Linux

Module 1: Introduction to Penetration Testing & Setup

- Web Application Penetration Testing Concepts
- Penetration Testing Terminology
- Penetration Testing Methodology
- Kali Penetration Testing Concepts
    - Reconnaissance
    - Target Evaluation
    - Exploitation
    - Privilege Escalation
- Introduction to Kali Linux
- Kali System Setup
    - Running Kali Live from external media
    - Installing Kali Linux
- Kali Toolset Overview

Module 2 : Reconnaissance

- Company Website
- Website history/ archive.org
- Social Media Resources
- Shodan
- Google Hacking
- Researching Network
    - HTTrack – Website Mirroring
    - ICMP Reconnaissance Technique
    - DNS Reconnaissance Technique
    - Maltego
- Nmap

Module 3 : Server-side-Attacks

- Vulnerability Assessment
    - Webshag
    - Skipfish
    - ProxyStrike

    - OWASP-ZAP
    - Websploit
- Exploitation
    - Metasploit
    - W3af
- Exploiting E-mails
- Brute-force attack
    - Hydra
    - DirBuster
    - Webslayer
- Kali Password Cracking Tools
    - John the Ripper
    - Ophcrack
    - L0phcrack
- Man-In-The-Middle
    - SSL Stripping
    - Subterfuge
    - Cain &Able

Module 4: Client Side Attacks

- Social Engineering
- Social Engineering Toolkit
- Host Scanning
    - Host Scanning With Nessus
    - Installing Nessus
    - Using Nessus
- Obtaining & Cracking User Passwords
    - Default/Guessable Passwords
    - Dictionary Attack
    - Brute-force Attack
    - Hybrid Attack
    - Rainbow Tables
    - Crunch
    - Cupp

Module 5 : Attacking Authentication

- Attacking Session Management

- ClickJacking
- Hacking Web-session Cookies
    - Cookie Manager+
- Web Session Tools
    - Firesheep - Firefox Plugin
    - Web Developer – Firefox Plugin
    - GreaseMonkey
    - Cookie Injector
    - Wireshark
    - Burp Suite
    - Webscarab
    - Ettercap
- SQL Injection
    - SQL map
    - SQLi
    - SQL Ninja
    - SQLmap-gui
- Cross Site Scripting(XSS)
- XSS cookie stealing / Authentication Hijacking

Module 6 : Web Attacks

- Browser Exploitation Framework - BeEF
- Burp Proxy
- OWASP ZAP
- SET Password harvesting
- Denial-of-Service (DOS) Attack
    - Low Orbit Ion Cannon - L0IC
    - Hulk
    - Slowloris
    - Scapy
- Directory Traversal
- Injection Flaws
    - SQL Injection
    - Command Injection
    - HTML Injection
- Cross Site Request Forgery(CSRF)
- Insecure Redirect and Forward
- Force Browsing

- File Injection
- Buffer Overflow
- Format String
- Session Fixation Attack
- Session Hijacking
- XML Injection
- XML Poisoning
- Cookie Poisoning
- Authorization Bypass
- Privilege Escalation
- Malicious File Uploads
- HTTP Request & Response Tampering
- Web Services Testing
    - XML
    - SOAP
    - UDDI
    - WSDL
    - WSDL Information Gathering
    - Using Unauthorized Web Services
- SMTP injection
- Broken Authentication & Session Management
- Insecure Object Reference
- HTML Code Injection
- Insecure Cryptographic Storage
- Phishing Attack
- Log Tampering

Module 7 : Web Application Firewalls & IDS

- Mod Security
    - Installation
    - Writing Rules
    - Checking Logs
- Snort
    - Installation
    - Writing Rules

    - Analyzing Logs

Module 8 : Defensive Countermeasures

- SSL Defence
    - Checking Version of SSL
    - Giving Recommendation
- Error & Exception Handling
- SQL Injection Countermeasures
    - Writing Parameterized Queries
    - Using Stored Procedures
    - Least user Privileges
- XSS Countermeasures
- Cookie Poisoning defense
- Session management Countermeasures
- Broken Authorization Countermeasures
- Input Validation And Recommendation
- Password Policies

Module 9 : Penetration Testing & Reporting

- Report Format
- Report Writing & Documentation
- Best Practice For Penetration Testers
- Writing Reports using Nessus
- Writing Reports using Accunetix
- Kali reporting Tools
    - Dradis
    - Maltego Case File
    - Sample Reports