Ethical Hacking with Kali Linux

Lecture and Demonstration: 10 Days
Daily Classes **:** 02 Hours

1. Introduction to Kali Linux

- Introduction to Kali Linux
- Unix vs Linux
- Different Desktop Environment
- Installation and Configuration

2. Basics of Terminal

- Basic Commands
- Different types of Users
- Some Shortcuts

3. Anonymity

- What is Proxy?
- Introduction to VPNs
- What is Tor?
- How to hide IP?
- How to change MAC Address?
- What is ProxyChains?

4. Footprinting and Reconnaissance

- Gather information about a host
- DNS enumeration
- Brute forcing subdomains against a target host
- Trace Domain Name Server
- Network Mapping
- Port Scanning
- How to search Exploits?
- Route Mapping
- Recognising Web Technologies
- Identify Domain Information
- How to find hidden objects, files and directories on a website?

5. Vulnerability Assessment

- Webserver and Web Application Assessment
- Web Server Detection
- CMS Detection
- Cloudflare Detection
- Recon and mapping out the target
- Find websites and web applications for security issues
- Unix and Linux Security Check

6. Web Application Penetration Testing

- SQL injection vulnerability scanning
- Vulnerability Scanning of Web Applications
- Fuzzing
- Scripting
- Spidering
- Website Cloning
- Fake Website for Phishing
- WordPress CMS Analysis

7. Database Assessment

- SQL Injection to Google Dorks
- SQL Injection Automation
- Mimic a MySQL Console

8. Password Attacks

- Identify the different types of Hashes
- Crack Encrypted Passwords or Data
- Create Custom Wordlists
- Offline Password Cracking
- Auto-detection Password Hash Types
- Customized Password Cracking
- Online Password Cracking
- Bruteforce Password Cracking

9. Wireless Attacks

- Packet Sniffing
- WEP Cracking
- WPA/WPA2-PSK Cracking
- Wifi Jamming
- DoS & DDoS Attack

10. Exploitation Tools

- Buffer Overflow
- Honeypot
- Android Hacking
- Browser Exploitation

11. Sniffing & Spoofing

- Network Analysis
- Packet Capture and Analysis
- MITM Attacks against a Network