# Wireless Penetration Testing & Ethical Hacking

Duration: 40 hrs

**Module 1: Introduction to Wireless Penetration Testing**

- Understanding Wireless Security Threats
- Overview of IEEE 802.11 Standards
- Wireless Security Mechanisms (WEP, WPA, WPA2, WPA3)
- Role of Wireless Penetration Testing in Cybersecurity

**Module 2: Wireless Networking Basics & Attack Surface**

- Wireless Communication Fundamentals
- SSIDs, BSSIDs, and ESSIDs
- Packet Analysis & Sniffing Fundamentals
- Identifying Attack Vectors in Wireless Networks

**Module 3: Setting Up the Wireless Penetration Testing Lab**

- Required Hardware: Wireless Adapters & Chipsets
- Configuring Kali Linux for Wireless Testing
- Essential Open-Source Tools for Wireless Attacks
- Legal & Ethical Considerations

**Module 4: Wireless Reconnaissance & Scanning**

- Passive vs. Active Wireless Reconnaissance
- Discovering Wireless Networks (Airodump-ng, Kismet)
- Identifying Hidden SSIDs
- Mapping Wireless Network Infrastructure (WiGLE, Netdiscover)

**Module 5: Wireless Packet Sniffing & Traffic Analysis**

- Capturing Wireless Packets (Wireshark, Tcpdump)
- Analyzing Wireless Traffic for Weaknesses
- Detecting Rogue Access Points
- Man-in-the-Middle (MITM) Attack Detection

**Module 6: Attacking WEP-Protected Networks**

- Understanding WEP Encryption Weaknesses
- Cracking WEP Encryption (Aircrack-ng, Wireshark)

- Replay and FMS Attacks
- Mitigation Techniques for WEP Exploits

**Module 7: Attacking WPA/WPA2 Networks**

- WPA/WPA2-PSK & Enterprise Security Overview
- Capturing WPA Handshakes (Airodump-ng, Hcxdumptool)
- Dictionary & Brute-Force Attacks (Hashcat, John the Ripper)
- Evil Twin Attack & Rogue AP Exploitation (Airbase-ng)
- WPS Attacks & Exploiting Weak Configurations (Reaver, Bully)

**Module 8: Advanced Wireless Attacks**

- Deauthentication & Disassociation Attacks (MDK3, Aireplay-ng)
- Honeypots & Fake Access Points (Mana Toolkit, Fluxion)
- Credential Harvesting via Captive Portals (WiFi-Pumpkin, Bettercap)
- Wireless Social Engineering Attacks

**Module 9: Bluetooth & RFID Security Testing (Concepts)**

- Bluetooth Reconnaissance & Enumeration
- Bluetooth MITM & Sniffing
- RFID Cloning & Spoofing
- Attacking NFC Systems

**Module 10: Wireless Intrusion Detection & Prevention**

- Wireless IDS/IPS Concepts
- Identifying & Blocking Rogue Access Points
- Monitoring Wireless Traffic for Threats (Kismet, Snort)
- Implementing Security Best Practices

**Module 11: Reporting & Remediation**

- Documenting Findings & Exploits
- Creating Professional Penetration Testing Reports
- Remediation Strategies & Hardening Wireless Networks
- Post-Engagement Best Practices