ARMOURINFOSEC®

Hands-On Cyber Security Training · Indore, India

Wireless Security & WiFi Penetration Testing

Course Syllabus

Master wireless security testing, Wi-Fi attacks, WPA/WPA2 exploitation, WEP cracking, wireless reconnaissance, deauthentication attacks, MITM attacks, and advanced wireless penetration testing techniques using real-world practical labs.

// COURSE INFORMATION

Course Information

DURATION	1 Months / 4 Weeks / 30 Hours
LEVEL	Advanced
MODULES	14
FORMAT	Hands-on Labs / Hybrid (Online + Indore Classroom)

// COURSE OVERVIEW

Course Overview

The Advanced Wireless Networks Penetration Testing course is designed for ethical hackers, penetration testers, red team operators, wireless security analysts, and cybersecurity professionals who want to specialize in wireless network security assessments. This course covers wireless networking fundamentals, IEEE 802.11 standards, encryption mechanisms, wireless reconnaissance, DoS attacks, WEP exploitation, WPA/WPA2 attacks, Man-in-the-Middle attacks, packet injection, MAC spoofing, and advanced wireless cracking methodologies.

// LEARNING OBJECTIVES

Learning Objectives

- Assess wireless network security posture comprehensively
- Configure wireless adapters for penetration testing (monitor mode, injection)
- Discover hidden SSIDs and enumerate wireless infrastructure
- Perform wireless DoS and deauthentication attacks
- Crack WEP encryption using multiple attack techniques
- Capture and crack WPA/WPA2 handshakes
- Deploy evil twin and rogue access point attacks
- Conduct wireless Man-in-the-Middle attacks
- Perform advanced WPA/TKIP exploitation

- Provide wireless hardening and remediation recommendations

// PREREQUISITES
Prerequisites

- Basic networking knowledge
- Familiarity with Linux command line
- Understanding of TCP/IP networking
- Basic cybersecurity concepts
- Compatible wireless adapter for labs

// MODULE BREAKDOWN
Module Breakdown

01 Introduction to Wireless Networks

- Introduction to Wireless Networks
- Wireless Transmission Standards
- 802.11 Wireless Network Types (a/b/g/n/ac/ax)
- Wireless Architecture
- Wireless Communication Basics
- Frequency Bands and Channels

02 Wireless Encryption & Authentication

- Wireless Encryption Standards
- Wireless Authentication Methods
- WEP Encryption Mechanism
- WPA Encryption (TKIP)
- WPA2 Encryption (AES/CCMP)
- WPA3 Concepts
- Authentication Handshakes
- Four-Way Handshake Process

03 Wireless Network Cards in Linux

- Wireless Network Cards in Linux
- Wireless Interface Configuration
- Monitor Mode Activation
- Packet Injection Capabilities
- Wireless Adapter Compatibility
- Driver Configuration
- iwconfig and iw Commands

04 Wireless Security Measures & Bypass

- MAC Address Filtering
- MAC Address Spoofing (Macchanger)
- ESSID Broadcast Configuration
- Hidden SSID Discovery Techniques
- Wireless Coverage Limitation

- Security Misconfigurations
- Access Point Identification

05 Wireless Reconnaissance & Traffic Analysis

- Wireless Network Discovery
- Airodump-ng Packet Capture
- Access Point Enumeration
- Client Device Identification
- Signal Strength Analysis
- Channel Hopping
- Wireless Traffic Analysis
- Packet Capture and Filtering

06 Wireless Denial-of-Service Attacks

- RF Jamming Attacks
- CSMA/CA Jamming
- Deauthentication Attacks (Aireplay-ng)
- Network Traffic Disruption
- Channel Flooding
- Association Flooding
- Wireless DoS Mitigation

07 Wireless MITM & Rogue Access Points

- Wireless MITM Concepts
- Rogue Access Points (Airbase-ng)
- Evil Twin Attacks
- Traffic Interception
- Session Hijacking
- Captive Portal Attacks
- Client Isolation Bypass
- Credential Harvesting

08 WEP Cracking Techniques

- WEP Encryption Weaknesses
- Initialization Vectors (IVs)
- IV Collection Techniques
- ARP Replay Attack
- Packet Injection for IV Generation
- Keystream Reuse Exploitation
- Aircrack-ng WEP Cracking
- Fragmentation Attack

09 Chop-Chop & Packet Replay Attacks

- Chop-Chop Attack Methodology
- PTW Attack
- KoreK Attack
- Packet Replay Techniques

- Interactive Packet Replay
- Traffic Manipulation
- Generating Packets Without Key Knowledge

10 Caffe Latte Attack

- Fake Access Point Creation
- Client-Side Wireless Attacks
- Caffe Latte Attack Methodology
- Wireless Client Exploitation
- Attacking Disconnected Clients
- Gratuitous ARP Generation

11 WPA/WPA2 Cracking

- WPA/WPA2 Encryption Analysis
- Four-Way Handshake Capture
- Dictionary Attacks
- Hash Cracking with Aircrack-ng
- Hashcat for WPA Cracking
- Rainbow Table Attacks
- MIC Failure Exploitation
- PMKID Attack Technique

12 Cowpatty & Hash Table Attacks

- Cowpatty Attack Methodology
- Pre-Computed Hash Tables
- Rainbow Table Generation
- Offline WPA Cracking
- Optimized Cracking Performance
- Custom Wordlist Generation

13 Advanced WPA/TKIP Attacks

- WPA TKIP Attack Methodology
- Beck-Tews Attack
- Michael Reset Attack
- TKIP Weaknesses Exploitation
- Advanced Wireless Exploitation
- KRACK Attack Concepts
- WPA3 Dragonblood Vulnerabilities

14 Enterprise Wireless Security & Reporting

- Enterprise WPA Attacks (EAP)
- RADIUS Server Assessment
- Wireless Intrusion Detection Systems
- Wireless Hardening Best Practices
- Penetration Test Reporting
- Remediation Recommendations
- Wireless Security Policy Development

// TOOLS & HANDS-ON LABS

Tools & Hands-On Labs

- Dedicated wireless penetration testing lab
- Multiple access points with various encryption (WEP, WPA, WPA2)
- Enterprise wireless with RADIUS server
- Compatible wireless adapters (monitor mode + injection)
- Isolated RF environment for safe testing
- Packet capture and analysis stations
- Rogue AP simulation environment

// TRAINING MODE

Training Mode

Every Armour Infosec course runs as a unified programme delivered in two parallel modes — the same curriculum, the same trainers, the same certification, regardless of how you join.

- ✓ Online Live Classes — real-time, instructor-led, fully interactive sessions
- ✓ On-Premise Classroom Training — in-person at our Indore centre (Sudama Nagar)
- ✓ Both modes run concurrently in every batch; switch between them as your schedule needs
- ✓ Same syllabus, lab access, and certification track for online and on-premise students

// CERTIFICATIONS & CAREER OUTCOMES

Certifications & Career Outcomes

This course aligns with industry-recognised certifications and prepares graduates for offensive-security, application-security, and infrastructure-security roles.

- OSWP (Offensive Security Wireless Professional)
- CEH Wireless module
- CompTIA Security+ wireless domain
- CWSP (Certified Wireless Security Professional)

// ENROL WITH ARMOUR INFOSEC

Enrol With Armour Infosec

Reach out to discuss enrolment, batch schedule, and lab access. Our Indore training centre runs both in-person and live online cohorts with placement assistance.

PHONE	+91 99777 47168
EMAIL	info@armourinfosec.com
ADDRESS	674, Sudama Dwar, Narendra Tiwari Marg, Sudama Nagar, Indore, Madhya Pradesh 452009
WEBSITE	https://armourinfosec.com

Scan to View Course Online

https://www.armourinfosec.com/training/wireless-security/