About the Course

This course provides a comprehensive understanding of wireless and mobile security in modern enterprise environments. It explores the unique risks introduced by wireless communications and mobile devices. Students learn how radio frequency technologies, wireless networks, and mobile platforms operate.

The course explains security models of Apple iOS and Google Android systems at a conceptual level. Participants examine real-world attack techniques targeting wireless and mobile environments. Wireless authentication, encryption, and secure network design principles are covered. The course also introduces enterprise deployment models such as BYOD and corporate-managed devices.

Students learn how to implement mobile device management and wireless security controls.

Monitoring, detection, and incident response for mobile and wireless threats are discussed.

The course emphasizes governance, policy enforcement, and risk management. Hands-on labs demonstrate vulnerabilities and security controls using virtual environments. By the end, students will be able to design and manage secure wireless and mobile infrastructures.

Learning Objectives

1 Explain wireless and mobile security principles

2 Describe RF communication and wireless network operation

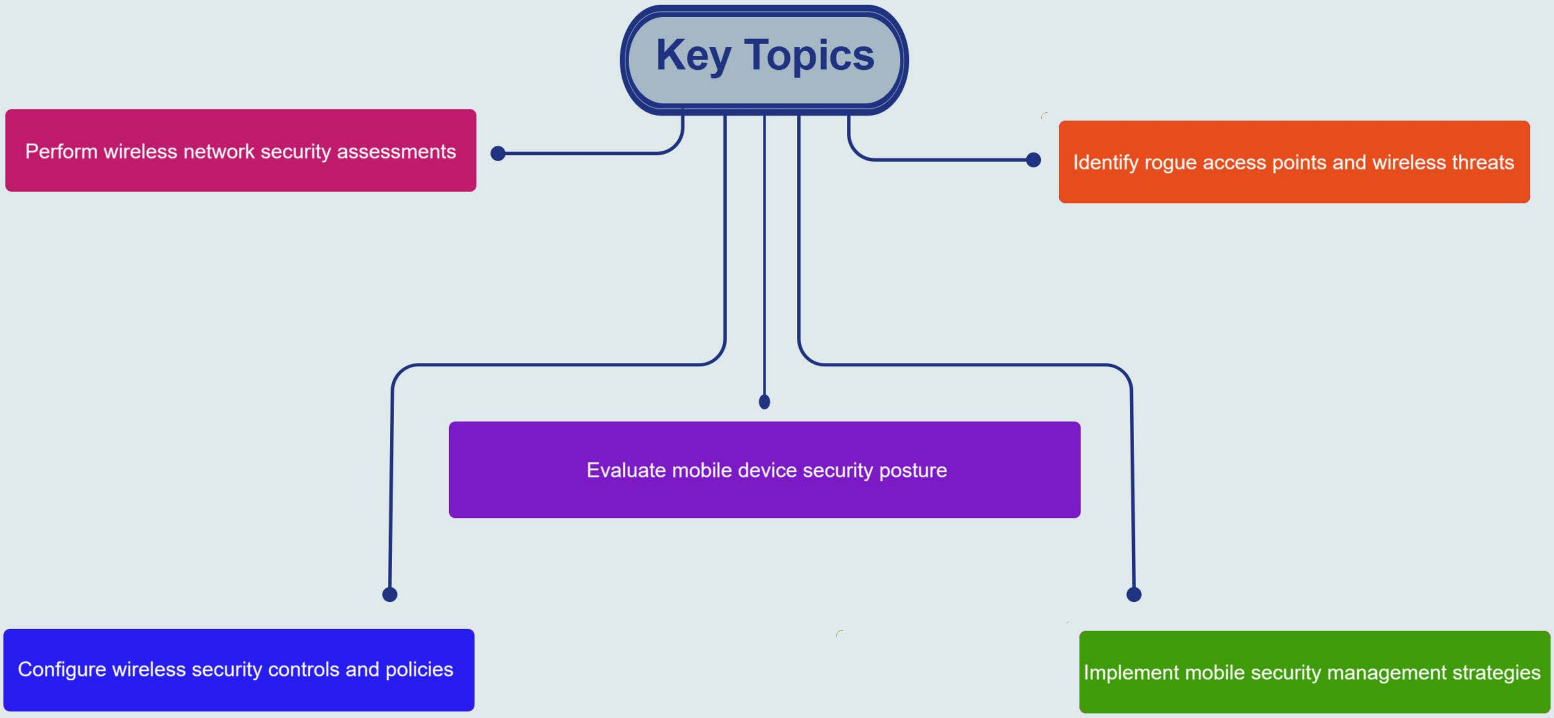
3 Identify wireless technologies, standards, and architectures

4 Explain mobile platform security models and architecture

5 Analyze wireless and mobile threats, vulnerabilities, and attacks

6 Apply mobile device management and policy enforcement

Key Topics



Key Topics

Perform wireless network security assessments

Identify rogue access points and wireless threats

Evaluate mobile device security posture

Configure wireless security controls and policies

Implement mobile security management strategies

Pre Requisites

- **Basic knowledge of computer networking concepts (TCP/IP, WiFi basics)**
- **Familiarity with operating systems (Windows, Linux, or macOS)**
- **Introductory understanding of IT or cybersecurity concepts**
- **General user familiarity with mobile platforms such as Apple iOS or Google Android**

What You Will Receive

Course Presentation File

Complementary Files & Toolkit

Information Security Tactics eBook

Who Should Attend

- Network and Wireless Security Engineer / Administrator
- Cybersecurity Analyst / Security Operations (SOC) Specialist
- Security Engineer / Security Architect / Security Consultant
- Mobile Device and Enterprise Mobility Administrator (MDM/UEM)
- Risk, Compliance, and Information Security Officer / IT Auditor
- Incident Response and Digital Forensics Specialist

Syllabus

Foundations of Wireless & Mobile Security

- Wireless vs mobile risk models
- Security objectives and trust boundaries
- Enterprise security integration

RF and Wireless Communication Fundamentals

- RF fundamentals and propagation
- Spread spectrum and interference
- Broadcast communication risks

Wireless Technologies and Architecture

- WLAN, Bluetooth, NFC, RFID
- 802.11 standards overview
- Infrastructure vs ad-hoc networks
- WLAN architectures

Mobile Platforms and Security Architecture

- Mobile OS security models
- Sandboxing and permissions
- Secure boot and device trust

Wireless & Mobile Threat Landscape

- Threat actors and attack surface
- Rogue APs and malicious apps
- Ecosystem risks

Wireless and Mobile Attack Techniques

- Sniffing and MITM concepts
- Deauthentication and DoS attacks
- Rooting and jailbreaking concepts
- Credential capture attacks

Syllabus

Authentication, Encryption, and Access Control

- WPA/WPA2 and enterprise authentication
- 802.1X concepts
- Certificates and biometrics

Data Exposure and Device Security Risks

- Sensor risks and data leakage
- Storage security
- Lost device threats

Enterprise Deployment Models

- BYOD, COPE, CYOD
- Guest networks and segmentation
- Governance tradeoffs

Security Hardening and Policy Enforcement

- Secure configuration
- MDM/MAM/UEM
- Wireless hardening techniques

Monitoring and Incident Response

- Wireless IDS/IPS
- Mobile compliance monitoring
- Incident handling

Governance and Lifecycle Management

- Policy and compliance
- Security lifecycle
- Common failures

Hands-on Training

- Lab 1 — Wireless Signal & Network Discovery
- Lab 2 — Packet Capture and Traffic Analysis
- Lab 3 — Rogue Access Point Detection (Conceptual Simulation)
- Lab 4 — Wireless Authentication Comparison
- Lab 5 — Wireless Security Policy Design
- Lab 6 — Android Emulator Security Review
- Lab 7 — Mobile Application Permission Analysis
- Lab 8 — Mobile Data Storage Analysis
- Lab 9 — Mobile Device Hardening
- Lab 10 — BYOD Risk Assessment