Wireless Network Security and Hacking Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Wireless network security is a critical component of modern cybersecurity frameworks, given the increasing reliance on Wi-Fi, mobile networks, and IoT connectivity. Vulnerabilities in wireless networks, if exploited, can lead to unauthorized access, data breaches, and critical service disruptions. Wireless Network Security and Hacking Training Course provides participants with in-depth knowledge of wireless network protocols, encryption standards, authentication mechanisms, and common attack vectors. Through practical exercises, participants will learn how to identify, prevent, and mitigate threats while strengthening the integrity, confidentiality, and availability of wireless systems.

The course also covers ethical hacking methodologies, penetration testing, and defensive strategies for securing enterprise and home wireless environments. Participants will gain hands-on experience in network scanning, intrusion detection, and vulnerability assessment using industry-standard tools and frameworks. Emphasis is placed on proactive risk management, policy implementation, and compliance with international cybersecurity standards. By the end of the training, learners will be equipped to safeguard networks against emerging wireless threats and enhance overall organizational cybersecurity posture.

Programme Curriculum

Wireless Network Security and Hacking Training Course

Introduction

Wireless network security is a critical component of modern cybersecurity frameworks, given the increasing reliance on Wi-Fi, mobile networks, and IoT connectivity. Vulnerabilities in wireless networks, if exploited, can lead to unauthorized access, data breaches, and critical service disruptions. Wireless Network Security and Hacking Training Course provides participants with in-depth knowledge of wireless network protocols, encryption standards, authentication mechanisms, and common attack vectors. Through practical exercises,

participants will learn how to identify, prevent, and mitigate threats while strengthening the integrity, confidentiality, and availability of wireless systems.

The course also covers ethical hacking methodologies, penetration testing, and defensive strategies for securing enterprise and home wireless environments. Participants will gain hands-on experience in network scanning, intrusion detection, and vulnerability assessment using industry-standard tools and frameworks. Emphasis is placed on proactive risk management, policy implementation, and compliance with international cybersecurity standards. By the end of the training, learners will be equipped to safeguard networks against emerging wireless threats and enhance overall organizational cybersecurity posture.

Course Objectives

1. Understand wireless network architectures and security protocols.
2. Identify vulnerabilities in Wi-Fi, Bluetooth, and IoT networks.
3. Apply encryption, authentication, and access control mechanisms.
4. Conduct ethical hacking and penetration testing for wireless systems.
5. Implement intrusion detection and prevention strategies.
6. Use vulnerability scanning and auditing tools effectively.
7. Understand rogue access points and man-in-the-middle attacks.
8. Design and enforce wireless network security policies.
9. Monitor and analyze network traffic for suspicious activity.
10. Respond to wireless network security incidents and breaches.
11. Evaluate emerging threats in wireless communications.
12. Integrate wireless security best practices into organizational operations.
13. Maintain compliance with cybersecurity standards and frameworks.

Organizational Benefits

- Enhanced protection against wireless network attacks
- Improved detection and response to security incidents
- Strengthened confidentiality, integrity, and availability of data
- Reduced risk of financial losses and reputational damage
- Improved compliance with regulatory and industry standards
- Increased staff expertise in wireless security and ethical hacking
- Reduced vulnerability to insider threats and rogue devices
- Enhanced operational resilience and business continuity
- Optimized security policy implementation and enforcement
- Better risk management and threat mitigation strategies

Target Audiences

- Network security administrators
- IT security analysts and engineers
- Ethical hackers and penetration testers
- Wireless network engineers
- IT auditors and compliance officers
- Security operations center (SOC) staff
- Cybersecurity consultants
- Technical managers and team leaders

Course Duration: 5 days

Course Modules

Module 1: Fundamentals of Wireless Networking

- Overview of wireless network types and standards
- Wireless protocols (Wi-Fi, Bluetooth, Zigbee)
- Wireless network topologies and infrastructure
- Understanding wireless signal propagation and coverage
- Security challenges in wireless communications
- Case Study: Network architecture review of a corporate Wi-Fi setup

Module 2: Wireless Threats and Vulnerabilities

- Common wireless attacks and exploitation techniques
- Rogue access points and unauthorized devices
- Packet sniffing and man-in-the-middle attacks
- Denial-of-service attacks on wireless networks
- Vulnerabilities in IoT and mobile networks
- Case Study: Security breach through rogue Wi-Fi hotspot

Module 3: Wireless Encryption and Authentication

- Wi-Fi security standards (WEP, WPA, WPA2, WPA3)
- Authentication mechanisms and key management
- Role of VPNs and secure tunneling protocols
- Implementing MAC filtering and network segmentation
- Evaluating encryption weaknesses and mitigation
- Case Study: Strengthening a corporate Wi-Fi network with WPA3

Module 4: Wireless Penetration Testing

- Ethical hacking principles and legal considerations
- Planning and executing wireless penetration tests
- Using industry-standard penetration testing tools
- Exploiting vulnerabilities in real-world scenarios
- Reporting and documenting findings
- Case Study: Penetration test on a university Wi-Fi network

Module 5: Intrusion Detection and Prevention

- Overview of wireless intrusion detection systems (WIDS)
- Network traffic monitoring and anomaly detection
- Preventive controls against wireless attacks
- Incident response procedures and protocols
- Integrating detection tools with SOC operations
- Case Study: Implementing WIDS in a high-risk enterprise network

Module 6: Security Policies and Best Practices

- Developing wireless security policies and guidelines
- Employee awareness and training programs
- Device management and access control policies

- Patch management and firmware updates
- Continuous monitoring and compliance checks
- Case Study: Policy rollout and enforcement in a multinational MFI

Module 7: Emerging Wireless Threats

- Threats in IoT, 5G, and mobile networks
- Cloud-based wireless security risks
- Zero-day exploits and advanced persistent threats (APTs)
- Future-proofing wireless network defenses
- Risk assessment and mitigation planning
- Case Study: Securing a 5G-enabled corporate campus

Module 8: Hands-On Wireless Security Labs

- Network scanning and vulnerability analysis exercises
- Simulated attack and defense scenarios
- Configuration of secure Wi-Fi networks
- Wireless traffic analysis and intrusion simulations
- Evaluating mitigation effectiveness
- Case Study: Lab-based simulated attack on a corporate wireless network

Training Methodology

- Instructor-led theoretical and practical sessions
- Hands-on labs and exercises for wireless security tools
- Scenario-based ethical hacking simulations
- Case study analysis from real-world breaches
- Group exercises and collaborative problem-solving
- Continuous assessment, feedback, and action plan development

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
02 Nov 2026	06 Nov 2026	Online	$1,000
02 Nov 2026	06 Nov 2026	Physical	$1,500
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$4,500
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com