Applied Wireless Network Security and Ethical Hacking Training Course

Ref: #TEL9960

Course Introduction / Overview:

This training course is designed to equip cybersecurity professionals, network administrators, and IT managers with the practical skills needed to secure and defend wireless networks from modern threats. The proliferation of Wi-Fi and other wireless technologies has introduced new vulnerabilities that require a specialized approach to security. This program, offered by BIG BEN Training Center, provides a comprehensive framework for understanding the core principles of wireless security, from various WLAN protocols and authentication methods to the techniques used in ethical hacking. We will explore key concepts such as denial-of-service attacks, man-in-the-middle attacks, and network reconnaissance. The curriculum is informed by the academic work of authors like William Stallings, whose books on network security provide a foundational and detailed understanding of the principles behind a secure network. This course goes beyond a simple overview of technology to provide a deep understanding of how to implement real-world solutions that ensure data privacy, network integrity, and operational continuity. We prepare participants to be leaders who can build more resilient and trusted wireless networks.

Target Audience / This training course is suitable for:

- Network administrators.
- Cybersecurity specialists.
- IT managers.
- Security analysts.
- Ethical hackers.
- Penetration testers.
- System administrators.
- Government agencies and equivalents.

Target Sectors and Industries:

- Telecommunications.
- IT and Managed Services.
- Corporate Enterprises.
- Healthcare.
- Financial Services.
- Government and Public Administration.
- Retail.
- Education.

Target Organizations Departments:

- Cybersecurity.
- IT and Network Operations.
- Information Security.
- Internal Audit.
- Compliance and Risk Management.
- Technical Services.
- Operations.
- Strategic Planning.

Course Offerings:

By the end of this course, the participants will have able to:

- Understand the key wireless security threats.
- Secure Wi-Fi networks and access points.
- Implement strong authentication protocols.
- Perform wireless network reconnaissance.
- Simulate common wireless attacks (ethical hacking).
- Conduct a wireless security audit.
- Develop a robust incident response plan.
- Mitigate denial of service attacks.

Course Methodology:

This training course uses a highly practical and hands-on methodology. The program is built on real-world examples of wireless security breaches and the techniques used to prevent them. Participants will work in a simulated lab environment to perform ethical hacking exercises, where they will learn how to identify and exploit vulnerabilities. We will use interactive workshops to practice skills like packet analysis and intrusion detection. The curriculum is designed to be a collaborative experience where participants can share their unique challenges and innovative solutions. Our trainers, with extensive experience in the field, will provide direct feedback and guidance throughout the course. BIG BEN Training Center is committed to providing a dynamic and practical learning environment, ensuring that participants leave with the skills and confidence to effectively secure wireless networks.

Course Agenda (Course Units):

Unit One: Foundations of Wireless Security

- Introduction to wireless network security.
- WLAN standards and protocols.
- WPA2 vs. WPA3.
- Authentication methods.
- Encryption protocols.
- Common wireless vulnerabilities.
- The role of ethical hacking.

Unit Two: Wireless Network Reconnaissance

- Introduction to network reconnaissance.
- Passive scanning and data collection.
- Active scanning techniques.
- Using network analysis tools.
- Packet sniffing.
- Identifying hidden networks.
- Mapping the wireless landscape.

Unit Three: Common Wireless Attacks

- Deauthentication attacks.
- Man-in-the-middle attacks.
- Evil Twin attacks.
- Denial of Service (DoS) attacks.
- WPA2 and WPA3 cracking techniques.
- Eavesdropping and data interception.
- Simulating wireless attacks.

Unit Four: Securing Your Wireless Network

- Configuring a secure WLAN.
- Implementing WPA3 Enterprise.
- Network segmentation.
- Intrusion detection systems (IDS).
- Access control and user policies.
- Secure guest network design.
- Monitoring and logging.

Unit Five: Security Auditing and Incident Response

- Conducting a wireless security audit.
- Penetration testing methodology.
- Developing an incident response plan.
- Forensic analysis of a security breach.
- Remediation and hardening.
- Risk management.
- The future of wireless security.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

How can a deeper understanding of wireless network security and the mindset of an ethical hacker empower professionals to build a more resilient and proactive defense against the ever-evolving landscape of digital threats?

What unique qualities does this course offer compared to other courses?

This training course is unique because it provides a dedicated, strategic focus on wireless network security through the lens of an ethical hacker. While other programs may cover general cybersecurity, our curriculum is designed to empower professionals with the specific skills needed to address the unique vulnerabilities of wireless networks. The program is a hands-on experience, with exercises that directly simulate the challenges and decisions involved in a real-world penetration test or incident response scenario. We go beyond theoretical concepts to provide a clear, actionable roadmap for balancing the need for convenient wireless access with the imperative of delivering a secure and trusted environment. This course is for professionals who want to lead their organizations toward a more secure, resilient, and protected future.