MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

WIRELESS SECURITY AUDIT: ASSESS THE SECURITY OF WIRELESS NETWORKS AND DEVICES WITHIN AN ORGANIZATION

"Securing the Airwaves – Audit, Analyze, and Protect Your Organization's Wireless Infrastructure"

Schedule

Date	Venue	Fees (Face-to-Face)
10 – 14 Aug 2026	London, UK	USD 3495 per delegate

► **Available delivery methods:** Face-to-Face & Online Training

Introduction

In today's mobile-first world, wireless networks are integral to business operations—but they also present unique vulnerabilities that cybercriminals actively exploit. This 5-day intensive training empowers IT auditors, cybersecurity professionals, and network engineers with the skills and methodologies to assess, audit, and secure wireless networks across enterprise environments.

The course blends practical hands-on techniques with structured audit approaches to identify wireless threats, evaluate access controls, analyze device configurations, and ensure compliance with leading cybersecurity standards. Participants will walk away with actionable tools and insights to conduct thorough wireless security assessments

Objectives

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

- Understand wireless networking architectures, protocols, and threats
- Identify and mitigate vulnerabilities in Wi-Fi configurations and connected devices
- Conduct a full wireless audit using industry-standard tools and checklists
- Assess encryption standards, rogue access points, and authentication method

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Why Attend

- Learn how to identify wireless attack vectors and insecure configurations
- Perform real-world assessments using open-source and commercial tools
- Enhance your organization\'s cybersecurity posture by closing wireless gaps
- Stay current with evolving wireless standards and audit techniques
- Receive a structured audit framework tailored for wireless environments

Target Audience

This program is designed for:

- IT auditors and information security professionals
- Network and wireless engineers
- Internal audit and compliance staff
- Penetration testers and cybersecurity analysts
- Anyone responsible for securing or assessing enterprise wireless environments

Individual Benefits

Key competencies that will be developed include:

- Wireless auditing methodologies and reporting
- Identification and remediation of vulnerabilities in Wi-Fi infrastructure
- Configuration assessment of access points, clients, and network segregation
- Hands-on use of audit and monitoring tools like Aircrack-ng, Kismet, and Wireshark
- Interpretation of audit results and regulatory mapping

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- Strengthened defenses against wireless attacks and unauthorized access
- Improved compliance with cybersecurity standards and frameworks
- Enhanced wireless infrastructure visibility and monitoring
- Standardized wireless audit processes across departments
- Reduced risk of data leakage or compromise through unsecured wireless paths

Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Deep dive into wireless technologies, audit frameworks, and security protocols
- Case Studies – Real-world breaches and lessons learned from wireless attacks
- Workshops – Hands-on auditing exercises using wireless testing tools
- Peer Exchange – Discussions on organizational challenges and mitigation strategies
- Tools – Templates for audit checklists, security assessment reports, and compliance mappings

MAWA EVENTS

Address: No. 857, Block A2. Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

Phone: +601116373203 | **Email:** info@mawaevents.net

Course Outline

Detailed 5-Day Course Outline

Training Hours: 7:30 AM – 3:30 PM **Daily Format:** 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

Day 1: Foundations of Wireless Networking and Security

- Module 1: Wireless Technology Overview (07:30 – 09:30)
- Wi-Fi architectures, standards (802.11), and frequencies
- Components of a wireless network (APs, controllers, clients)
- Common wireless vulnerabilities
- Module 2: Wireless Threat Landscape (09:45 – 11:15)
- Types of wireless attacks (e.g., eavesdropping, DoS, man-in-the-middle)
- Rogue devices, Evil Twin APs, and social engineering via Wi-Fi
- Case studies of recent wireless breaches
- Module 3: Compliance Standards and Wireless Controls (11:30 – 01:00)
- NIST 800-153, ISO 27001, PCI DSS wireless requirements
- Security controls for authentication, encryption, and segmentation
- Policy and procedure frameworks

Day 2: Wireless Audit Planning and Tool Familiarization

- Module 4: Audit Methodology and Scope Definition (07:30 – 09:30)
- Establishing wireless audit objectives and audit checklists
- Identifying target networks and defining success criteria
- Planning for onsite/offsite assessments
- Module 5: Wireless Audit Tools and Setup (09:45 – 11:15)
- Introduction to tools: Aircrack-ng, Kismet, NetStumbler, Wireshark
- Hardware requirements and configuration setup
- Legal and ethical considerations in wireless testing
- Module 6: Packet Capturing and Analysis (11:30 – 01:00)
- Sniffing traffic and detecting unsecured communications
- Identifying SSIDs, MAC addresses, and channel use
- Analyzing captured data for threats and anomalies

Day 3: Wireless Vulnerability Assessment

- Module 7: Network Discovery and Mapping (07:30 – 09:30)
- Detecting wireless devices and hidden networks
- Locating rogue APs and unauthorized clients
- Heat mapping and signal analysis
- Module 8: Security Configuration Auditing (09:45 – 11:15)
- Evaluating AP configuration (SSID, broadcast, encryption)
- Reviewing WPA2/WPA3, EAP, and captive portal settings
- Identifying weak passwords and legacy protocols
- Module 9: Authentication and Access Control Testing (11:30 – 01:00)
- Assessing 802.1X, MAC filtering, and VLAN segmentation
- Testing for bypass techniques and session hijacking
-

Credential capture and password cracking basics

Day 4: Advanced Wireless Testing Techniques

- Module 10: Simulating Wireless Attacks (07:30 – 09:30)
- Deauthentication and Evil Twin simulations
- Rogue AP injection and DNS spoofing
- Analyzing results and containment strategies
- Module 11: Wireless IoT Device Audit (09:45 – 11:15)
- Risks and vulnerabilities in connected devices
- Firmware analysis and hardcoded credential detection
- Isolation and secure configuration best practices
- Module 12: Physical Security and Signal Management (11:30 – 01:00)
- Signal leakage, placement of APs, and antenna tuning
- Wardriving, geolocation risks, and wireless zoning
- Shielding and wireless access control

Day 5: Reporting, Remediation, and Future Trends

- Module 13: Wireless Audit Reporting (07:30 – 09:30)
- Documenting findings and severity classification
- Creating actionable recommendations and risk summaries
- Mapping results to compliance frameworks
- Module 14: Remediation Planning (09:45 – 11:15)
- Short-term vs. long-term security enhancements
- Policy updates and employee awareness programs
- Integration with broader IT security strategies
- Module 15: Future of Wireless Security (11:30 – 01:00)
- Emerging threats: 5G, Wi-Fi 7, and SDR-based attacks
- Artificial intelligence in wireless monitoring
- Preparing for zero-trust wireless environments

Certification

Participants will receive a Certificate of Completion in Wireless Security Auditing, validating their technical and strategic proficiency in assessing and protecting wireless networks against modern cybersecurity threats.

Why Choose MAWA Events

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation’s unique goals.

In-House / Customized Training Interested in running this course for your team? Please contact us:	TEL: **+601116373203**	EMAIL: **info@mawaevents.net**