

### Course Overview:

The **Organizational Systems Wireless Auditor<sup>®</sup>** (OSWA<sup>™</sup>) is an international practical technical wireless security auditing certification designed for those who want to learn more about the various ways to professionally perform a wireless security audit or penetration test, with the aim of identifying weaknesses in wireless deployments. With many organizations using wireless technologies and many countries announcing wireless internet access initiatives, attending the OSWA<sup>™</sup> will give you a solid grounding in how to audit the security of wireless networks and clients.

The OSWA<sup>™</sup> focuses primarily on providing attendees with the technical knowledge, methodology and skills to execute a wireless audit/penetration test. Unlike other wireless courses which are limited to "administration"-style access-point-centric viewpoints or are not designed by wireless security professionals, the OSWA<sup>™</sup> is designed from the ground up to teach wireless security from the starting point of understanding the fundamentals of Radio Frequency (RF) and RF Spectrum Analysis, through to understanding the IEEE 802.11 specification and how to analyze information contained in 802.11 packet dumps before arriving at 802.11-based security concerns such as how to penetrate wireless LANs and going on to advanced methods of auditing wireless networks by targeting wireless clients, as well as how to build your own wireless hardware to augment your wireless auditing capabilities. In addition, it covers practical security issues affecting other wireless technologies such as Bluetooth and RFID.

This instructor-led, intensely practical, hands-on programme teaches a vendor-neutral approach to practical security testing of wireless networks and provides attendees with the correct balance of skill and ethics based on security best practices. By equipping attendees with the correct technical skillsets, as well as an understanding of legal issues involved in testing a target, the OSWA<sup>™</sup> will enhance the capability of professional security testers and provide beginners with the proper methodology, skills and tools to conduct consistent and comprehensive wireless security tests. Attendees will also learn how to hunt down and geographically locate wireless hackers and moochers on the fly and in real time using ThinkSECURE's MocherHunter<sup>™</sup> tool.

Attendees will also receive a laser-etched copy of the **OSWA-Assistant<sup>™</sup>**, ThinkSECURE's very own in-house developed wireless auditing toolkit with on-board software for auditing 802.11-, Bluetooth- and RFID-based networks, to enhance their wireless penetration-testing activities.

While the programme syllabus should be used to determine if this programme is appropriate for the attendee based on their current skills and requirements, all attendees will come away with the following:

- A solid understanding about Radio Frequency (RF) fundamentals and its impact on upper-layer protocols..
- The ability to isolate and analyze wireless networks from Layer 1 to Layer 3.
- The knowledge of what preparations have to be made prior to conducting a wireless security audit.
- Comprehensive technical understanding of how to practically execute a wireless security audit.
- Comprehensive technical understanding and ability to isolate and track down unauthorized wireless users.
- How to audit wireless networks using a variety of tools, including "Build-It-Yourself" hardware.
- The ability to recommend countermeasures based on wireless audit results.
- The legal implications of wireless security auditing.

With its wide variety of **practical classroom labwork** and a **practical certification exam**, the OSWA<sup>™</sup> wireless auditing and penetration-testing certification programme & exam are ideal complements to the defence-oriented OSWiSP<sup>™</sup> secure wireless deployment and administration training programme.

#### Technical Pre-Requisites:

- Understand basic networking principles
- Understand basic security principles and concepts
- Strong interest in wireless security

**Note: Though not strictly necessary, it is highly recommended that participants meet the above criteria in order to get the most benefit out of the course.**

#### Who Will Benefit From This Programme :

- Security Analysts / Consultants
  - Penetration Testers
  - Security Audit Teams
  - Network & System Administrators
  - Network & System Engineers
- and anyone who is looking to learn about how to conduct a technical vendor-neutral audit against wireless networks.

## Programme Outline:

Practical coursework is interspersed throughout the OSWA™ programme and the following is a brief programme outline:

### Part 1: Why Audit Wireless Networks?

- The Need for Wireless Auditing
- The Law of the Land
- Legal & Best Practice compliance
- Introducing the 5E Attacker Methodology
- 5E: Exploration
- 5E: Enumeration
- 5E: Exploitation
- 5E: Embedding
- 5E: Egress

### Part 2: Radio Frequency (RF) Fundamentals

- The Concept of RF
- Wavelength
- Resonance
- Calculating Frequency Wavelengths
- Gain
- Power and Distance
- Attenuation
- Diffraction
- Interference
- RF Spectrum Analysis
- Understanding the Wireless Footprint : ThinkSECURE's MAX-SOIL & SR-SOIL Concepts
- Workbook Lab Exercises

### Part 3: Wireless 101

- Wireless Standards
- Bluetooth Security
- Bluetooth: Attacks
- Bluetooth: Threats to Companies and Individuals
- Bluetooth: Defences
- RFID
- RFID: History
- RFID: Privacy Issues
- RFID: Architecture
- RFID: Tag Characteristics
- RFID: Use Categories & Legislation
- RFID: Information Theft & Enumeration
- RFID: Deployer Security Measures
- RFID: Carrier Security Measures
- 802.11: Wireless Equipment
- 802.11: Wireless Chipsets
- 802.11: Selecting Wireless Chipsets
- 802.11: Master, Monitor & Frame-Injection
- 802.11 Accessories: Antennae
- 802.11 Accessories: Detection Tools
- 802.11 Frame Architecture
- 802.11 Frame Analysis
- Locking Down the Auditing Station
- Tool Selection
- The OSWA™-Assistant Auditing Toolkit
- Workbook Lab Exercises

### Part 4: Wireless Security Testing: Infrastructure

- Wireless Sniffing
- Understanding 802.11i : WEP, WPA-PSK & WPA/WPA2
- WEP Analysis
- Auditing WEP
- WPA/WPA2 & WPA-PSK/WPA2-PSK Analysis
- The 4-Way Handshake
- WPA Authentication Schema
- Auditing WPA/WPA2 & WPA2/WPA2-PSK
- 802.11-based Denial of Service
- Workbook Lab Exercises

### Part 5: Wireless Security Testing: Client

- Auditing the Wireless Client
- Discovering Wireless Clients
- Client Probing
- Probemapper™
- Mass Client Profiling
- Targeted Client Profiling
- Client Targeting
- The WCCD Vulnerability
- Workbook Lab Exercises

### Part 6: Testing with a Twist

- Ph00ling
- Why is Ph00ling possible?
- Ph00ling Technique
- Long Range Auditing
- Build Your Own Hardware: Antennas
- Antenna: Components
- Antenna: Assembly
- Antenna: Optimization
- Antenna: Benchmark Performance & Range Testing
- Build Your Own Hardware: NIC Jacks
- NIC Jack Construction & Assembly
- MocherHunter™: Introduction to Real Time Geo-Location of Hackers & Mochers
- MocherHunter™: Preparation
- MocherHunter™: Technique & Execution
- Concluding the Audit
- Workbook Lab Exercises

## Methodologies & Tools:

The following are just some of the Methodologies & Tools introduced during the OSWA™ programme:

- ◆ 5E Attacker Methodology
- ◆ MAX-SOIL / SR-SOIL
- ◆ OSWA-Assistant™ Wireless Auditing Software Toolkit
- ◆ Wireshark / Ethereal
- ◆ Kismet
- ◆ Airodump-ng / Aireplay-ng / Packetforge-ng
- ◆ Aircrack-ng / Aircrack-ptw
- ◆ CoWPAtty
- ◆ Probemapper™
- ◆ MDK3
- ◆ MocherHunter™:
- ◆ RF Spectrum Analyzer
- ◆ WiFi Finder
- ◆ Digital Hotspotter
- ◆ Yagi, Parabolics & Antennas
- ◆ Rfdump
- ◆ Bluetooth hacking tools

...and much more!



For more details regarding the availability, schedule and pricing for your country, please visit :

<http://oswa.securitystartshere.org>

Get your copy of our FREE

"Do You ThinkSECURE?" IT-security eNewsletter today !  
Our fortnightly eNewsletter contains news highlights from the IT-security world & a "Featured Tool" section !  
Signup at <http://DoYouThinkSECURE.securitystartshere.org>