



CWSA Wireless Security: Hands-On

7safe training

Course Outline



ISO 27001
BUREAU VERITAS
Certification



ISO 9001
BUREAU VERITAS
Certification



❖ CWSA Wireless Security: Hands-on



❖ What you will learn

- † Discover the latest security standards and practices in WiFi
- † Familiarise yourself with the various hardware and software components of a wireless network
- † Understand the threats to wireless networks, including rogue access points, denial of service (DoS) attacks and eavesdropping
- † In-depth coverage of a comprehensive series of wireless security measures, including WEP, WPA/ WPA2 and 802.11i
- † Learn how hackers and auditors test wireless networks for security related issues
- † Explore how an attacker might attempt to subvert and bypass each type of security control

❖ Benefits

- † Understand how a hacker can break into both unsecured and secured wireless networks
- † Our state-of-the-art class environment provides delegates with a first-hand opportunity to experiment with wireless devices and the tools used to break into wireless networks
- † The course culminates in a hands-on exercise to create a secure wireless network using digital certificates
- † The course is designed to educate for the purpose of properly defending wireless systems from unauthorised access

❖ Who should attend

- † Those responsible for the security of IT systems within an organisation, including but not limited to: IT Managers, Systems/Network Administrators, Systems Analysts, IT Security Professionals and Forensic/Network Investigators

- † Those interested in understanding the risks associated with wireless networks and how best to protect them

❖ Course style

This course is hands-on. Delegates learn how to secure wireless networks and then test them for vulnerabilities, adopting the mindset of an attacker. Open group discussion is strongly encouraged.

❖ Level & Prerequisites

Basic understanding of TCP/IP networking.

❖ Course content highlights

WIRELESS NETWORK SECURITY INTRODUCTION

- † A background into wireless networks and the security issues associated with a Wireless Local Area Network (WLAN)
- † Overview of wireless technologies (e.g. Bluetooth, WiFi, WiMax)

HARDWARE

- † Identification of wireless hardware components and their functionality
- † 802.11 architecture and commonly used terminology

TESTING FOR WIRELESS VULNERABILITIES

- † An overview of war driving and Wifi security auditing
- † Practical exercises on the equipment/tools used to gain access

