



The Global Leader in Wireless Security

Managing WiFi Security Risks

Wireless Security Training Course

Incidents of WiFi hacking and malicious use are on the rise globally. WiFi, if not secured properly, can easily be hacked and misused. Unsecured WiFi provides an easy target for hit-and-run style attacks allowing hackers and criminals to cause severe damage while remaining invisible and undetected. For enterprises, this can lead to leakage of sensitive data, legal fees, fines and penalties, and brand erosion. Organizations without an official WiFi network are equally at risk.

Course Objectives:

The objective of this course is to help you:

- Understand the risks associated with wireless LANs
- Debunk common wireless security myths
- Learn about the vulnerabilities in WiFi networks and how hackers can exploit those vulnerabilities to breach your network security
- Learn techniques to manage and secure your network against wireless threats.

The course material will include a combination of tutorials, videos, and demonstrations of WiFi hacking and vulnerability assessment tools.

Who should attend:

Anyone interested in securing their corporate network against Wi-Fi cyber-attacks. Examples are:

- Network administrators, IT managers, Security officers
- Security consultants, security auditors
- Cyber law enforcement agents

Basic understanding of computer networking principles is a pre-requisite.

Course Content:

Day 1	Day 2
<p>Introduction</p> <ul style="list-style-type: none"> ○ Wireless LAN protocols and architectures <p>Wireless Security Challenges</p> <ul style="list-style-type: none"> ○ Paradigm shift from the traditional security model ○ Real world WiFi cyber crimes ○ Business risks <p>Authentication & Encryption I</p> <ul style="list-style-type: none"> ○ Wired Equivalent Privacy (WEP) and its drawbacks ○ WEP key cracking attacks: FMS, PTW, Café Latte ○ Countermeasures <p>Authentication & Encryption II</p> <ul style="list-style-type: none"> ○ WiFi Protected Access (WPA) ○ WPA dictionary attack; PEAP attack; WPA-TKIP vulnerability ○ WPA2 <p>Common Mistakes in WLAN configuration</p> <ul style="list-style-type: none"> ○ Hidden SSIDs, MAC filtering, and more <p>Case study: WiFi Security at Airports</p> <ul style="list-style-type: none"> ○ Viral SSIDs, Probing clients <p>Ad hoc networks</p> <ul style="list-style-type: none"> ○ Compromising Wi-Fi clients 	<p>Rogue APs</p> <ul style="list-style-type: none"> ○ Wired network exposure at layer 2 <p>Wi-Phishing</p> <ul style="list-style-type: none"> ○ Honeypot/Evil Twin, Multipot ○ Man-in-the-middle attacks: Trojan, Metasploit, Eavesdropping, Data modification <p>MAC Spoofing</p> <ul style="list-style-type: none"> ○ Bypassing access control <p>WiFi Denial of Service (DoS)</p> <ul style="list-style-type: none"> ○ Attacks by misusing 802.11 standard ○ RF jamming ○ Self DoS vulnerability in Cisco wireless LANs <p>New/upcoming standards</p> <ul style="list-style-type: none"> ○ 802.11e, 802.11n, 802.11w ○ Security implications <p>Case study: Securing WiFi Hotspots</p> <ul style="list-style-type: none"> ○ The Need for Open WiFi ○ Risks and security measures <p>Wireless Intrusion Prevention</p> <ul style="list-style-type: none"> ○ Core functions ○ What works, what doesn't?

Software:

Demonstrations will cover some of the most commonly used tools for WiFi hacking and vulnerability assessment.

Reconnaissance/ Decryption	NetStumbler, Kismet, Wireshark
Encryption Key Cracking	Aircrack-ng, Aircrack-ptw, coWPAtty, Café Latte
Packet Injection	Aireplay-ng, Tkiptun
Wi-Phishing/ Man-in- the-middle attacks	KARMA, Hotspotter, Delegated, Extreme Honeypot
Denial of Service	Void11, Wlanjack, Hunter-killer (over airjack), Zulu (over madwifi), RF jammer, FakeAP
Miscellaneous	Essidjack, Sidejacker, Cain abel, Nessus, Nmap