



---

## Art of Exploitation – WIRELESS Edition

CSRgroup and our partner Solvern Innovations are proud to present the newest offering in the Art of Exploitation series of Computer Exploitation courses.

The emergence of wireless networks as a primary means of communications and internet access has been a bonanza for the hacker. Interception of your wireless communications by Man-in-the-middle attacks, spoofing MAC addresses to gain access to supposedly “secure” wireless access points and bypassing weak encryption are just some of the techniques that hackers use to exploit your wireless communications.

This class is designed to provide the Computer Security Operator with the knowledge, tactics, techniques and procedures that are used by wireless hackers. By focusing primarily on the discovery, analysis and exploitation of Wireless Networks, not on securing them, the Art of Exploitation – Wireless Edition, provides a unique training experience not found in other commercial “Wireless Security” courses. After five days of intense study, the student will be able to go back to their organization armed with the essential information they need so they can perform Wireless Security Assessments and Wireless Exploitation.

### About AOE Courses

The Art of Exploitation is a series of courses on various segments of computer exploitation. All of the courses are modular, allowing portions to be moved, subtracted, added, or even combined with other AOE courses to create a custom offering specific to the needs of the target audience. All AOE courses are built on the “Practice by Doing” method of instruction and contain many practical application labs. All AOE courses share the same philosophy; Focus on Methodology and Techniques instead of “Toolology”. Tools come and go, but if the student can learn the proper techniques and methodology, they can use many different tools to accomplish their goals and objectives.

### Pre Requisites

This course does not cover the basics of 802.11, RF or TCP/IP, so the student should already have a basic understanding of these protocols and should also be familiar with the Linux operating system.

### Exercises

The five day course includes over 20 practical application exercises allowing the student to put into practice the skills they are being taught.

### Target Audience

Individuals involved in Computer Network Operations, Computer and Network Security, auditors, network and system administrators should benefit from attending this course.

### Contact

Phone: 410-609-3157  
email: [wireless@csr-group.com](mailto:wireless@csr-group.com)  
[www.csr-group.com](http://www.csr-group.com)



---

## DETAILED OUTLINE

### Module 1 – Wireless Overview/Basics

- Wireless Hardware Review
- Antenna selection, driver selection and chipsets.
- Authentication, Association and Authentication Schemes (WEP, WPA, EAP, 802.1X).
- 802.11 packet structure, frames, fields, and types.
- Basic wireless tools (iwconfig, iwlist, wpa\_supplicant, wlanconfig and their usage.
- Creating, modifying and destroying Virtual Access Points for wireless surveys and assessments.

### Module 2 – Wireless Methodology

- Planning a Wireless Assessment/Operation
- Wireless Survey Methodology
- Open Source Research/Collection
- Site Survey and survey steps

### Module 3 – Reconnaissance

- Site Surveys – in detail
- Physical Topology and Security
- Passive Collection Techniques
- Kismet usage
- Gps mapping
- Wireless DF Techniques

### Module 4 – Wireless Analysis

- Analyzing Site Survey Results
- Wireshark usage
- Creating and using display filters in Wireshark
- Decrypting WEP/WPA Packets in Wireshark
- Plotting and Mapping using gpsmap
- Plotting and Mapping using Googleearth
- Combining and merging multiple surveys and captures using kismet tool suite and other tools.
- Network mapping and session reconstruction with wifizoo, scapy and perl scripts



---

## Module 5 – Other Wireless Technologies

- Exploiting Mobile Devices Overview
- Cell Technologies
- EvDO/EDGE/GSM
- Blackberry
- Bluetooth stack, Packet Structure, addressing, security, pico and scatternets
- Bluetooth packet capture and analysis
- Bluecasing (Bluetooth survey)
- Bluetooth Hardware and antennas
- Bluetooth scanning with BTscanner and hcitools
- Querying Bluetooth services with sdptool and other tools
- Bluesnarfing and Bluebugging mobile devices
- RFID security
- Reading, Writing and Modifying RFID devices using the RFIDiot tools
- Emerging wireless technologies (802.11n, WiMax etc)

## Module 6 – Wireless Exploitation

- Accessing Open Networks & Discovering Hidden SSIDs
- Spoofing and bypassing MAC filtering using the aircrack-ng suite of tools
- Cracking WEP actively and passively
- Spoofing Wireless Packets
- Cracking WPA and WPA2 PSK/AES
- Performing Wireless Man-in-the-Middle and SSL MiTM operations using fragrouter and the dsniiff tool suite
- Setting up and using Rogue Access Points
- Bridging wired and wireless networks together for covert access
- Attacking EAP/RADIUS
- Performing Client Side Wireless Attacks
- Automated wireless discovery and exploitation using the SILICA device