THE
ASCENDANCY
GROUP

ACTIVE AND PASSIVE WI-FI COURSE

COURSE OVERVIEW

This 5-day instructor led course prepares students for wireless (WiFi and Bluetooth) penetration testing engagements. We begin with radio frequency and propagation theory, then introduce the 802.11 standards and protocols. We then develop an understanding and exploitation of each type of wireless network implementation. We teach students how to identify and locate Wi-Fi emitters (access points, laptops, mobile phones), break or bypass the encryption, collect and analyze, and exploit the network. Finally, students write a comprehensive report summarizing results in a meaningful manner. This course culminates with a full mission profile (FMP) exercise and includes offensive security wireless professional certification coursework and exam vouchers. Exam mentorship is included; certification is guaranteed.

COURSE OBJECTIVES

- Legal brief and disclosures
- Introduction to radio-wave propagation and radio frequencies
- Introduction to 802.11 theory, standards, and protocols
- Setting up a wireless environment
- Planning a wireless penetration testing engagement
- Surveying wireless environments
- Identifying target emitters and disregarding/ not logging non-targets
- Locating target emitters
- Bypassing wireless security protocols (passive and active) WEP, WPA-PSK, WPS
- Bruteforce / rainbow Tables
- Scanning and enumerating the network
- Monitoring and analyzing the network
- Exploiting the router / clients
- Writing a comprehensive report
- Exam preparation