PEN-210: Foundational Wireless Network Attacks (OSWP)

Course Overview

PEN-210 is an in-depth wireless security and penetration testing course designed to provide learners with the knowledge and practical skills required to identify, exploit, and remediate vulnerabilities in wireless networks. The course covers a wide range of topics, including IEEE 802.11 standards, wireless network types, Linux wireless tools, Wireshark essentials, and advanced wireless network monitoring and analysis techniques.

Throughout the course, students will engage in interactive labs and exercises that simulate real-world scenarios, gaining valuable experience in conducting wireless network assessments and implementing effective security measures. By the end of PEN-210, learners will have a comprehensive understanding of wireless network security and the ability to conduct wireless penetration tests.

Duration: 5 Days (Lecture and Hands-On Labs)

Exam Reference: OffSec Wireless Professional Certification (OSWP)

Target Audience

PEN-210 is designed for cybersecurity professionals, network administrators, and IT professionals who want to expand their knowledge and skills in wireless network security and penetration testing. The course is particularly beneficial for individuals just beginning to pursue careers in cybersecurity or ethical hacking.

Course Objectives

- Comprehensive understanding of IEEE 802.11 standards and wireless network types
- Proficiency in using Linux wireless tools, drivers, and stacks
- Mastering Wireshark for packet
- Deploying and detecting rogue access points
- Attacking WPA Enterprise networks and captive portals
- Utilizing Bettercap and Kismet for wireless network monitoring and analysis

Duration

5 Days

Certifications

PEN-210

Contact Us

800.674.3550

2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

PEN-210: Foundational Wireless Network Attacks (OSWP)

APPLIED TECHNOLOGY ACADEMY

Course Outline

IEEE 802.11

- IEEE
- 802.11 Standards and Amendments
- Antenna Diversity vs MIMO

Wireless Networks

- Overview
- Infrastructure
- Wireless Distribution Systems
- Ad-Hoc Networks
- Mesh Networks
- Wi-Fi Direct
- Monitor Mode

Wi-Fi Encryption

- Open Wireless Networks
- Wired Equivalent Privacy
- Wi-Fi Protected Access
- Wi-Fi Protected Access 3
- Opportunistic Wireless Encryption
- 6 Wireless Protected Setup
- 802.11w

Linux Wireless Tools, Drivers, and Stacks

- Loading and Unloading Wireless Drivers
- Wireless Tools
- Wireless Stacks and Drivers

Wireshark Essentials

- Getting Started
- Wireshark Filters
- Wireshark at the Command Line
- Remote Packet Capture
- Advanced Preferences

Frames and Network Interaction

- Packets vs Frames
- 802.11 MAC Frames
- Frame Types
- Interacting with Networks

Aircrack-ng Essentials

- Airmon-ng
- Airodump-ng
- Aireplay-ng
- Aircrack-ng
- Airdecap-ng
- Airgraph-ng

Cracking Authentication Hashes

- Aircrack-ng Suite
- Custom Wordlists with Aircrack-ng
- Hashcat
- Airolib-ng
- coW Patty

Attacking WPS Networks

- WPS Technology Details
- WPS Vulnerabilities
- WPS Attack

Rogue Access Points

- The Basics of Rogue Aps
- Discovery
- Creating a Rogue AP

Attacking WPA Enterprise

- Basics
- PEAP Exchange
- Attack

Attacking Captive Portals

- Basic Functionality
- The Captive Portal Attack
- Additional Behaviors Surrounding Captive Portals

Bettercap Essentials

- Installation and Executing
- Modules vs Commands
- Wi-Fi Module
- Additional Methods of Interacting with Bettercap

Kismet Essentials

- Installation
- Configuration Files
- Starting Kismet
- Web Interface
- Remote Capture
- Log Files
- Exporting Data

Determining Chipsets and Drivers

- Determining the Wireless Chipset
- Determining the Wireless Driver
- Example: Alfa AWUS036AC

Manual Network Connections

- Connecting to an Access Point
- Setting up an Access Point

Prerequisites

All learners are required to have:

- Solid understanding of TCP/IP and the OSI model as well as familiarity with Linux
- A modern laptop or desktop that can boot and run Kali Linux
- Specific Hardware is required to complete course exercises