Offensive Security Wireless Attacks (OSWP) Syllabus

Course Summary and Organization of Content	
Course Summary	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
Organization of Content	Learning material is divided into **Learning Modules.** Each Learning Module has multiple **Learning Units**, which are digestible, atomic pieces of learning material designed for efficient comprehension and application. This structure allows learners to easily grasp key concepts and integrate them into their skillset, enabling them to progress smoothly through the course. Each Learning Unit is defined by several **Learning Objectives**: discreet and practical goals for the learner to strive for. Learning Objectives are assessed at the end of each Learning Unit via hands-on **Module Exercises**. Many exercises require the learner to show their skills by interacting with Offensive Security lab machines. Whenever a walkthrough is part of the course material, there are accompanying videos that correspond with the written content.

Who's This Course Designed For?
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.

What You'll Learn	
• 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

Learning Module	Learning Units
IEEE 802.11	IEEE
	802.11 Standards and Amendments
	Antenna Diversity vs MIMO
	Wrapping Up
Wireless Networks	Overview
	Infrastructure
	Wireless Distribution Systems
	Ad-Hoc Networks
	Mesh Networks
	Wi-Fi Direct

	Monitor Mode
	Wrapping Up
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
	Wrapping Up
Linux Wireless Tools, Drivers, and Stacks	Loading and Unloading Wireless Drivers
	Wireless Tools

	Wireless Stacks and Drivers
	Wrapping Up
Wireshark Essentials	Getting Started
	Wireshark Filters
	Wireshark at the Command Line
	Remote Packet Capture
	Advanced Preferences
	Wrapping Up
Frames and Network Interaction	Packets vs Frames
	802.11 MAC Frames
	Frame Types

	Interacting with Networks
	Wrapping Up
Aircrack-ng Essentials	Airmon-ng
	Airodump-ng
	Aireplay-ng
	Aircrack-ng
	Airdecap-ng
	Airgraph-ng
	Wrapping Up
Cracking Authentication Hashes	Aircrack-ng Suite

	Custom Wordlists with Aircrack-ng
	Hashcat
	Airolib-ng
	coWPAtty
	Wrapping Up
Attacking WPS Networks	WPS Technology Details
	WPS Vulnerabilities
	WPS Attack
	Wrapping Up
Rogue Access Points	The Basics of Rogue APs

	Discovery
	Creating a Rogue AP
	Wrapping Up
Attacking WPA Enterprise	Basics
	PEAP Exchange
	Attack
	Wrapping Up
Attacking Captive Portals	Basic Functionality
	The Captive Portal Attack
	Additional Behaviors Surrounding Captive Portals

	Wrapping Up
bettercap Essentials	Installation and Executing
	Modules vs. Commands
	Wi-Fi Module
	Additional Methods of Interacting with Bettercap
	Wrapping Up
Kismet Essentials	Installation
	Configuration Files
	Starting Kismet
	Web Interface
	Remote Capture

	Log Files
	Exporting Data
	Wrapping Up
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