OffSec

PEN-210

Wireless Network Attacks

OSWP

PEN-210 (Wireless Attacks) introduces the foundations of wireless network security, exploring common vulnerabilities and exploitation techniques. The course prepares learners in skills related to different types and architectures of Wi-Fi networks, wireless reconnaissance, and exploiting vulnerabilities in WPS.

IEEE 802.11	Gain a deep understanding of the IEEE 802.11 wireless networking standards that form the foundation of Wi-Fi technology
Wireless Networks	Explore the architecture, components, and security challenges of wireless networks, including both infrastructure and ad-hoc modes
Wi-Fi Encryption	Learn about the various encryption protocols used in wireless networks, such as WEP, WPA, and WPA2, and their vulnerabilities
Linux Wireless Tools, Drivers, and Stacks	Master essential Linux tools and drivers used for wireless network configuration, monitoring, and troubleshooting
Wireshark Essentials	Learn how to analyze wireless network traffic using Wireshark, a powerful packet capture and analysis tool
Frames and Network Interactions	Gain insights into wireless frame structure, network interactions, and protocols to understand the inner workings of wireless communications
Aircrack-ng Essentials	Familiarize yourself with Aircrack-ng, a versatile suite of tools for wireless security assessment, including capturing packets, cracking passwords, and deauthenticating clients
Cracking Authentication Hashes	Learn how to crack various wireless authentication hashes, such as WPA/WPA2 PSKs, to gain access to secured networks
Attacking WPS Networks	Explore vulnerabilities in Wi-Fi Protected Setup (WPS) and learn how to exploit them to compromise wireless networks
Rogue Access Points	Understand the risks posed by rogue access points, learn how to detect them, and implement mitigation measures

OffSec

PEN-210

Wireless Network Attacks

OSWP

Attacking WPA Enterprise	Discover vulnerabilities in Wi-Fi Protected Access (WPA) for and learn how to exploit them to compromise wireless enterprise networks
Attacking Captive Portals	Learn how to exploit and bypass the login restrictions of a Wi-Fi network
bettercap Essentials	Gain insight on the installation, execution, and interaction with Bettercap to implement effective security measures to defend against vulnerabilities and man-in-the-middle techniques
Kismet Essentials	Learn how to install Kismet, configure files, detect rogue devices and unauthorized access points while monitoring real-time network traffic
Determining Chipsets and Drivers	Identify vulnerabilities tied to specific chipsets or drivers, and choose the right tools for detecting and defending against wireless network attacks
Manual Network Connections	Spot suspicious behavior, avoid insecure automatic connections, and configure connections securely to reduce the risk of wireless network attacks