PEN-210: Foundational Wireless Network Attacks

Duration: 90 Days

Course Description:

The Foundational Wireless Network Attacks (PEN-210) course introduces the foundations of wireless network security, exploring common vulnerabilities and exploitation techniques. Learners gain practical experience in a hands-on, self-paced environment allowing them to learn the principles of wireless security assessments.

Learners completing the online training course and passing the accompanying exam earn the OffSec Wireless Professional (OSWP) certification. This wireless security certification demonstrates a learner's ability to identify and exploit vulnerabilities in 802.11 networks. The OSWP equips penetration testers with specialized skills in wireless security assessment, complementing their knowledge base and making them a valuable asset for organizations.

Course Outlines:

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 Interaction

➢ 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.

REGISTER NOW!
training@trends.com.ph
(+632) 8863-2123
www.trendsacademy.com.ph