WiFi Pentesting Bootcamp

Objective: WiFi networks are widely used and they're getting better all the time. To stay relevant as a security professional, you need an in-depth understanding of WiFi security and be able to audit a WiFi network.

In this bootcamp, you will learn WiFi protocol basics, security standards, limitations and attacks. Along with the instructor sessions, you will practice your skills in the cloud-based labs that use WiFi emulation to create real-world scenarios.

Our teaching methodology focuses on helping students learn essential concepts through tackling attacks in our purpose-built labs. At the end of this bootcamp, you will have job-ready skills to begin your journey as a WiFi pentester.

Module I: Protocol Basics, Traffic Sniffing, and Recon

Objective: Learn the basics of WiFi protocol and how the devices communicate through WiFi using different packets, protocols, layers, clients, and access point components. Learn about traffic sniffing and capture, and how to process captured traffic to find WiFi components operating in the vicinity.

1. WiFi standard basics
    a. Bands
    b. Channels
    c. SSID
    d. BSSID
    e. Frame structure and header
2. Transmission basics
3. Basic commands to interact with WiFi interface
4. Traffic sniffing
5. WiFi traffic sniffing
    a. Monitor mode
    b. Remote sniffing
6. Capturing and storing traffic
7. Discovering wireless networks and clients
8. Analyzing WiFi traffic (header/packet analysis)

Module II: Attacking Personal Networks

Objective: Understand the need to secure WiFi networks and learn how personal WiFi network security standards work. Learn about the shortcomings of these standards and how to overcome them. Practice attacks to crack secured networks.

1. Introduction to WiFi security schemes
    a. WEP
        i. WEP-40
        ii. WEP-104
    b. Encryption-based
        i. WPA (TKIP)
        ii. WPA2 (CCMP)
    c. Management modes
        i. Personal Network (PSK)
        ii. Enterprise network (EAP or MGT)
    d. Observing the difference in packets
        i. Lab 3 mentioned in module I
2. Cracking WEP
    a. Theory and explanation
    b. Live WEP cracking
    c. Decrypting WEP traffic
3. Cracking WPA/WPA2-PSK
    a. Theory and explanation
    b. Live WPA-PSK cracking
    c. Decrypting WPA-PSK traffic
4. AP-less Attacks

Module III: Attacking Enterprise Networks

Objective: Understand how security requirements for enterprise networks differ from that of personal WiFi networks, how enterprise WiFi network security standards work, their shortcomings and how to overcome them. Practice honeypot attacks to break into secure networks.

1. Understanding WPA/WPA2-EAP
    - PEAP
        i. GTC

        ii. MSCHAPv2
    - TTLS
        i. PAP
        ii. MSCHAPv2
2. Honeypot attacks
    - Creating fake networks
    - Evil twin attack
    - Karma attacks
3. Attacking WPA/WPA2-PEAP
    - Theory and explanation
    - PEAP-GTC
    - PEAP-MSCHAPv2
4. Attacking WPA/WPA2-TTLS
    - Theory and explanation
    - TTLS-PAP
    - TTLS-MSCHAPv2

Module IV: Advanced Attacks and WPA3

Objective: Understand WPA3, the latest WiFi security standard, and learn some advanced attacks on enterprise WiFi networks.

- PEAP-relay attack
- WiFi pivoting
- Introduction to WPA3
    - WPA3-OWE (Opportunistic Wireless Encryption)
    - WPA3-SAE (Simultaneous Authentication of Equals)
    - WPA3-SAE Transition Mode
    - WPA3-Enterprise
- Proposed attacks on WPA3