
## Why WiFi Security?

WiFi networks are ubiquitous. On one hand, a "wireless" connection makes life easier, but on other hand, it adds a whole new set of security concerns. In early days of WiFi security, the prime focus was on defending enterprise WiFi networks, but now, with the widespread use of WiFi, there have been cases where the attacker first penetrated the home WiFi network of an employee, broke into his work laptop and installed a backdoor which eventually got him inside the enterprise network. Hence, understanding WiFi security for both personal and enterprise networks, and being able to audit these networks is a critical skill that all security professionals should possess.

# Prerequisites

- Basic knowledge of computers and networking
- Familiarity with the Linux operating system

# What will you learn?

This section will familiarize you with WiFi security and pentesting. We will go through important concepts and how to use various tools/techniques to attack different WiFi security schemes. Starting with the basics of the WiFi networks and security, you will perform activities like sniffing and cracking passwords and then perform attacks on APs (Access Points)/client devices. In this section, we will also cover the WPA3 standard.

### Basics

#### Traffic Analysis

Traffic analysis refers to inspecting the captured/stored WiFi traffic to gather information regarding clients, access points and their activities. The labs in this section provide the user with traffic capture PCAPs and suitable tools for analysis.

#### Recon

Reconnaissance refers to the activity of finding/locating WiFi devices (APs and clients) present in the vicinity. It can also reveal information about the client device/owner and its behavior. The labs provided in this section provide the users with an emulated WiFi environment and monitor mode capable WiFi cards for sniffing. The objective is to use airodump-ng and other tools to find information about WiFi devices.

#### AP Client Basics

The labs in this section cover basic commands/tools that can be used to connect to an existing WiFi network, create WiFi networks of different types of security schemes and bypass the MAC filter.

#### OpenWRT Router

OpenWRT is the most popular open source OS for WiFi routers. OpenWRT allows technical users to compile custom firmware for their devices. The labs in this section are to provide the user CLI and Web UI access to an emulated OpenWRT WiFi router to familiarize the user with OpenWRT.

#### Tools

- Wifite
- termshark
- bettercap
- MDK4
- EAPHammer

## Personal Networks

### Offline Cracking

Personal WiFi network security schemes are the ones usually deployed at home or in personal spaces. Examples of such schemes include WEP, WPA-PSK, WPA2-PSK. This section covers the offline cracking labs for personal networks. A traffic capture PCAP is provided to the user along with the required tools.

### Live Cracking

This section covers the live attack/cracking labs for personal networks protected by personal WiFi security schemes such as WEP, WPA-PSK and WPA2-PSK. An emulated WiFi environment and monitor mode capable wlan0 is provided to users.

## Enterprise Networks

### Offline Cracking

Enterprise WiFi network security schemes are the ones usually deployed in company offices and other non-personal spaces. Examples of such schemes include WPA-EAP PEAP-MSCHAP2 and PEAP-TTLS. This section covers the cracking attacks on the MSHCAPv2 hash of user passwords using Asleap.

### Live Cracking

This section covers luring the client using honeypot (or evil twin) and recovering the correct user credentials from WiFi networks protected by enterprise WiFi networks security schemes like WPA-EAP, PEAP-MSCHAP2 and PEAP-TTLS.

### WiFi Pivoting

WiFi Pivoting refers to the approach where the attacker first gets access to the WiFi network and then attacks the machines on the wired LAN. This section covers attacks on the WPA enterprise network including the PEAP Relay attack. In each lab the user has to first get access to the protected WiFi network and then target the machines running on the wired LAN side of the network.

## Advanced Labs

### Python Scripting

This section covers different scripting labs where the user has been provided with an emulated WiFi environment. Python and the scapy library are installed on the machine. The user has to write the Python program to complete the given task.

### AP Backdoor

This lab teaches the creation of an AP Backdoor. In the lab, the user has to create a malicious .ko module on the development machine, transfer it to the test machine and then observe it in action. The infrastructure to develop and test a kernel module based backdoor is provided.

### Custom Firmware

Custom-compiled OpenWRT firmware is used by pentesters to create sniffer or hacking/pentesting platforms. The labs in this section teach you how to compile OpenWRT firmware and interact with emulated OpenWRT machines.

## Forensics

### Basic

The massive increase in WiFi devices in both enterprises and homes has made the WiFi aspect important for incident response. Most organizations store WiFi authentication/access logs and traffic captures in case of attacks and anomalies. These can later be analyzed to reconstruct the chain of events. In each lab in this section, the user is provided with a case scenario, WiFi traffic captures and other relevant information. The user has to use Wireshark and other tools to analyze the traffic and solve the scenarios.