

OFFSEC TRAINING

Foundational Wireless Network Attacks — WIFU (PEN-210) (OSWP) Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

ADVANCED

40 HOURS

5 DAYS

SECURITY

At a glance

COURSE	Foundational Wireless Network Attacks — WIFU (PEN-210) (OSWP)	WHAT IS INCLUDED
TRACK	OffSec Training	✓ Instructor-led delivery by practitioners who also work our SOC
DOMAIN	Cyber Security	✓ Hands-on lab access for the duration of the course
LEVEL	Advanced	✓ Course materials and lab guides
DURATION	40 hours (about 5 days)	✓ Hacky Security certificate of completion
DELIVERY	Classroom · Online live · On-site at your office	✓ Post-course support by email
LANGUAGE	English	
CLASS SIZE	Small cohorts — everyone gets lab time	

Who this is for

This is an advanced course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Sixteen modules, mapped one-for-one to the OffSec PEN-210 (Foundational Wireless Network Attacks) syllabus and taught in the same order, so nothing the exam draws on is left uncovered. PEN-210 is the course that leads to the OSWP; this is Hacky Security's own preparation for it, not OffSec courseware and not OffSec lab access.

The syllabus is foundational by design. It starts with the 802.11 standard and how wireless networks and their encryption actually work, moves through the Linux tooling and the frame analysis you need to see what is happening on the air, and then walks through the practical attacks: cracking authentication, WPS, rogue access points, WPA Enterprise and captive portals. The later modules cover the supporting tools — bettercap and Kismet — and the hardware realities of chipsets, drivers and manual connections.

Most of the work is hands-on and needs real radio hardware. Wireless attacks depend on a supported adapter and on getting the driver, the monitor mode and the capture right before any attack will run, so the course spends real time on the physical setup as well as the techniques. That reflects the exam, which is entirely practical.

Module 01 — IEEE 802.11

The standard underneath everything else: what Wi-Fi actually is at the protocol level.

- The 802.11 family of standards and how they evolved
- Bands, channels and the physical layer that carries the traffic
- Stations, access points and the roles devices take
- The management, control and data frame types
- How a client discovers, joins and stays associated to a network
- The vocabulary the rest of the course relies on

Module 02 — Wireless Networks

How wireless networks are built and behave, from the client's and the attacker's point of view.

- Infrastructure and ad-hoc network modes
- The association process from probe to authenticated, associated client
- SSIDs, BSSIDs and how networks advertise themselves
- Beacons, probes and the traffic a network emits even when idle
- What an attacker can learn simply by listening
- The behaviours later attacks exploit

Module 03 — Wi-Fi Encryption

The schemes meant to protect wireless traffic, and where each one is weak.

- WEP and why it fails
- WPA, WPA2 and WPA3 and how they differ
- Pre-shared-key versus enterprise authentication
- The four-way handshake and what it exposes
- Where each scheme's weaknesses actually lie
- Which attacks apply to which encryption

Module 04 — Linux Wireless Tools, Drivers, and Stacks

Getting a Linux machine to do wireless work at all, which is the prerequisite for everything.

- The Linux wireless stack and how the pieces fit together
- Drivers, and why the right one matters for attacks
- Putting an adapter into monitor mode
- The command-line tools for managing wireless interfaces
- Diagnosing why an interface will not cooperate
- Preparing a working attack platform

Module 05 — Wireshark Essentials

Reading wireless traffic, because you cannot attack what you cannot see.

- Capturing wireless traffic for analysis
- Filtering down to the frames that matter
- Reading 802.11 frames in the capture
- Following an association or a handshake through the packets
- Spotting the evidence an attack depends on
- Using capture analysis to confirm what is happening on the air

Module 06 — Frames and Network Interactions

The frame-level detail behind the attacks, and how devices actually talk.

- The structure of 802.11 frames in depth
- Management, control and data frames and what each carries
- How authentication and association exchanges look on the wire
- Deauthentication and disassociation frames and their effect
- The interactions that attacks manipulate
- Reading frame exchanges to understand a network's state

Module 07 — Aircrack-ng Essentials

The core toolkit for wireless attacks, used deliberately rather than by rote.

- The aircrack-ng suite and what each tool is for
- Capturing traffic with the suite's tools
- Injecting frames and forcing useful events
- Capturing a handshake for offline cracking
- Running the cracking step against captured material
- Fitting the suite into a full attack workflow

Module 08 — Cracking Authentication Hashes

Turning captured authentication material into a recovered key.

- What is captured during authentication and why it is crackable
- Dictionary attacks against captured handshakes
- Building and choosing wordlists for a target

- Using hardware acceleration where it helps
- The limits of cracking and what makes a key resistant
- Confirming a recovered key against the network

Module 09 — Attacking WPS Networks

Exploiting Wi-Fi Protected Setup, a convenience feature that undermines the encryption behind it.

- What WPS is and why it exists
- The weaknesses in the WPS PIN mechanism
- Online brute-force attacks against WPS
- Offline attacks where they apply
- Recovering the network key through WPS
- Recognising when a target exposes this route

Module 10 — Rogue Access Points

Standing up an access point of your own to attract and attack clients.

- What a rogue access point is and how clients are lured to it
- Impersonating a legitimate network
- Getting clients to associate with your access point
- Positioning the rogue AP within a larger attack
- The client behaviours that make this work
- Handling traffic once a client connects

Module 11 — Attacking WPA Enterprise

Attacking the enterprise authentication model, which behaves very differently from a pre-shared key.

- How WPA Enterprise and 802.1X authentication work
- The role of the RADIUS server and the EAP methods
- Setting up to intercept enterprise authentication
- Capturing and attacking enterprise credentials
- The weaknesses specific to enterprise deployments
- Where this differs from attacking a pre-shared-key network

Module 12 — Attacking Captive Portals

Getting past — and abusing — the login pages that gate many public networks.

- How captive portals intercept and redirect clients
- The mechanisms that enforce the portal
- Bypassing a captive portal's controls
- Combining a portal attack with a rogue access point
- Capturing what a portal collects from clients
- Recognising the portal's weak points

Module 13 – bettercap Essentials

A second core tool, for the interception and manipulation side of wireless attacks.

- What bettercap does and where it fits
- Driving bettercap for wireless work
- Reconnaissance and monitoring with the tool
- Manipulating traffic and clients
- Combining bettercap with the aircrack-ng workflow
- Using it within the exam's practical tasks

Module 14 – Kismet Essentials

Detection and monitoring across the wireless environment.

- What Kismet is and what it detects
- Discovering networks and devices passively
- Monitoring the wireless environment over time
- Reading Kismet's output
- Using detection to plan an attack
- Fitting Kismet into the wider workflow

Module 15 – Determining Chipsets and Drivers

The hardware groundwork that decides whether any of this works at all.

- Why the adapter's chipset determines what attacks are possible
- Identifying the chipset in a given adapter
- Matching a chipset to a supported driver
- Confirming that monitor mode and injection actually work
- Choosing hardware suited to wireless attacks
- Troubleshooting an adapter that will not perform

Module 16 – Manual Network Connections

Connecting to wireless networks by hand, without the graphical helpers, when you need full control.

- Connecting to a network from the command line
- Working with wireless configuration directly
- Connecting to open, WPA and enterprise networks manually
- Diagnosing a connection that fails
- The control manual connection gives over the process
- Building the confidence to work without a GUI

Who should take this

Penetration testers who need to add wireless to their assessments, network and security administrators responsible for Wi-Fi they want to test themselves, and security enthusiasts who want a grounded, practical introduction to wireless attacks. It is a focused, foundational course rather than a broad one.

The course is foundational and reachable for a motivated beginner, but it is not effortless. You will want basic comfort with the Linux command line and a willingness to deal with hardware: wireless work lives and dies on

having a supported adapter and getting the driver and monitor mode right. Expect to spend real time on setup. There is no assumed prior wireless experience, but the people who pass are the ones who put the radio hardware in front of them and practise.

The exam

The OSWP exam is set and awarded by OffSec. It is entirely practical: you connect to a wireless lab environment and have to attack the networks and prove your access.

- A proctored, hands-on assessment lasting 3 hours and 45 minutes
- A further 24 hours afterwards to write and submit a professional report
- Three network scenarios are available; you must recover proof from two of them, one of which is mandatory
- Each attacked scenario must be evidenced in the report, including the recovered key and proof
- Delivered over VPN, with proctoring throughout

The exam voucher is purchased separately from OffSec, along with any lab access, which is part of their product rather than ours. We prepare you for the exam; you book and sit it through OffSec directly.

How we deliver it

Classroom or online live, or at your office for a private group. The work is hands-on against wireless networks we run for practice, using supported adapters, so you spend your time doing the captures and attacks rather than watching them. Small cohorts, so everyone gets radio hardware and instructor time. The hardware and driver setup is treated as part of the skill, because on the exam a misconfigured adapter costs you the attack.

Mapped to the OffSec PEN-210 syllabus and taught from Hacky Security's own curriculum and lab estate by instructors who do offensive work for a living. This is preparation for the OSWP; the certification, voucher and any official lab access come from OffSec.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 · info@hackysecurity.com

<https://hackysecurity.com/courses/hacky-wifi-hacking-training/>

CHANDIGARH · SHIMLA · DELHI · DUBAI · LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.