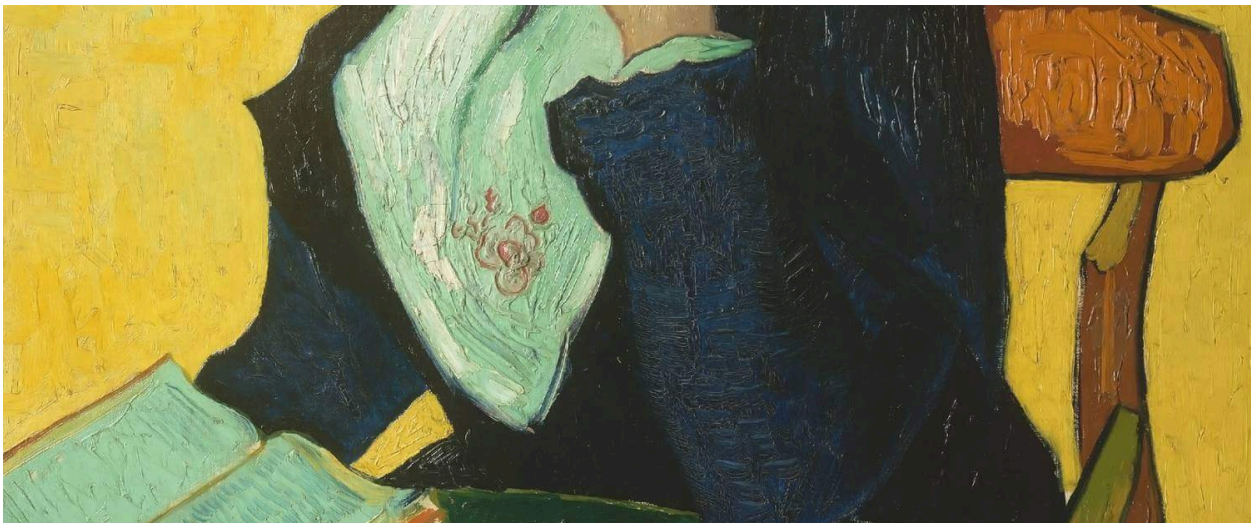


WiFi hacking Basic inro

Full Roadmap: Zero → Hero (Wi-Fi Security)

Phase 1 — Absolute Basics (Foundation)

Learn how networks function before touching security.

Topics:

- IP address
- subnet
- gateway
- DNS
- DHCP
- NAT

Core concepts:

- Internet Protocol
- Dynamic Host Configuration Protocol

You should understand:

- why devices get private IPs

- how your router assigns addresses
- why internet still works through one public IP

Phase 2 — Wireless Fundamentals

Now learn Wi-Fi architecture.

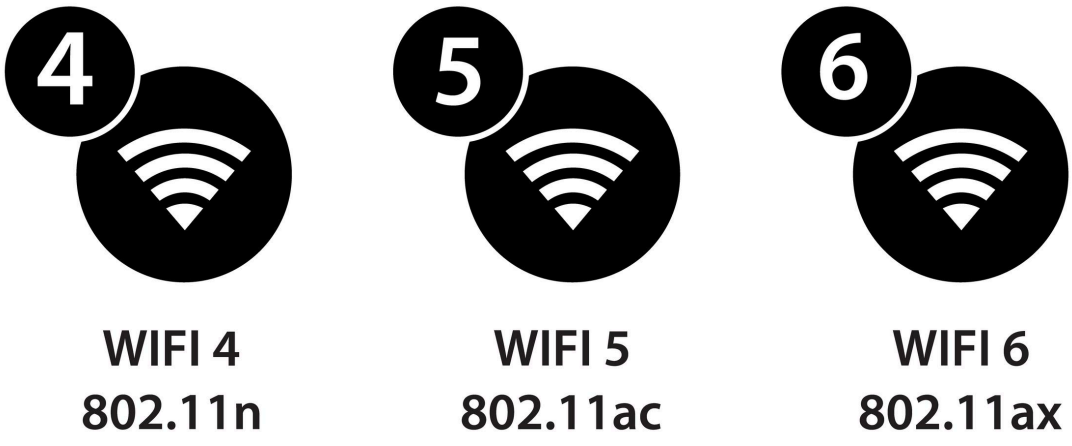
Topics:

- SSID
- BSSID
- channels
- RSSI
- roaming
- 2.4 GHz vs 5 GHz vs 6 GHz

Main wireless standard:

- IEEE 802.11

Visual difference helps here:



Phase 3 — Encryption and Authentication

This is the heart of Wi-Fi security.

Learn:

- WEP
- WPA
- WPA2
- WPA3
- AES
- handshake concept
- PMK / PTK basics

Important cryptography:

- Advanced Encryption Standard

Know clearly:

- WEP = obsolete
- WPA2 = still common
- WPA3 = strongest consumer standard

Phase 4 — Router Hardening (Immediate Real Protection)

This gives the biggest real-world benefit.

Checklist:

- change admin password
- disable WPS
- firmware updates
- separate guest network

- disable remote management
- use WPA3/WPA2-AES only
- monitor connected devices

Router examples:

- TP-Link
- Netgear

Phase 5 — Packet Analysis (Professional Skill)

Learn how packets move.

Best tool:

- Wireshark

Use it to inspect:

- DHCP exchange
- DNS queries
- ARP traffic
- TCP sessions

This turns theory into real visibility 🔍

Phase 6 — Linux for Wireless Work

Mandatory because most advanced wireless analysis uses Linux.

Best beginner:

- Ubuntu

Later:

- Kali Linux

Learn:

- terminal

- network interfaces
- permissions
- package install

Phase 7 — Wireless Threat Models (Conceptual)

Understand how Wi-Fi is attacked conceptually:

- evil twin access points
- rogue AP
- weak password exposure
- deauthentication abuse
- MAC spoofing
- captive portal deception

⚠️ Study the concepts, not offensive misuse.

Phase 8 — Home Lab (Very Important)

Build your own legal lab 🧪

You need:

- spare router
- old laptop
- isolated test network

Practice:

- change security modes
- compare WPA2 vs WPA3
- inspect traffic
- test signal leakage

Phase 9 — Advanced Wireless Topics

When strong enough, learn:

- enterprise Wi-Fi
- RADIUS
- 802.1X authentication
- VLAN separation

Important enterprise concept:

- IEEE 802.1X

Phase 10 — Become Expert-Level

Read:

- RFCs
- vendor security docs
- router firmware release notes

Follow companies:

- Cisco
- Ubiquiti

Professional Wi-Fi security roadmap used by cybersecurity engineers 🚀