**What WPA2/3 Pen Testing Is**

* **WPA2 (Wi-Fi Protected Access 2)**: Common Wi-Fi security standard using AES encryption (CCMP). Still widely deployed.
* **WPA3**: Newer, stronger uses **Simultaneous Authentication of Equals (SAE)** handshake instead of WPA2’s **4-way handshake**, making it more resistant to offline dictionary attacks.
* **Pen Testing Goal**: Try to capture authentication handshakes and test if weak passwords or misconfigurations can be exploited.

**Typical WPA2 Pen Testing Steps**

1. **Reconnaissance** – Identify Wi-Fi networks (airmon-ng, airodump-ng).
2. **Handshake Capture** – Disconnect a client, capture WPA2 handshake traffic (aireplay-ng).
3. **Password Cracking** – Use aircrack-ng or hashcat with a wordlist to attempt cracking captured hashes.
4. **Validation** – Confirm success, report vulnerabilities.

**WPA3 Changes (Harder to Attack)**

* WPA3 uses **SAE (Dragonfly handshake)** → resists offline dictionary attacks.
* Still possible to test for **implementation flaws** or weak configurations (e.g., transition mode where WPA2 + WPA3 coexist).

**Tools I’ll Likely Use**

* **Aircrack-ng suite** (Linux, very standard for Wi-Fi pen testing).
* **Wireshark** (packet analysis).
* **Hashcat** (GPU-based cracking if needed).

**Challenges & Considerations**

* WPA2: Plenty of existing tutorials (easy to replicate).
* WPA3: Fewer guides, more research — could make my tutorial unique.
* Ethics: Must test only on authorized labs/networks (e.g., WSU Cyber Lab, RADICL).

Starter Sources

**Aircrack-ng Documentation** (classic WPA2 attack steps) - <https://www.aircrack-ng.org/doku.php?id=cracking_wpa>

Wireshark WPA Handshake Analysis <https://wiki.wireshark.org/SampleCaptures#wpa_handshakes>

**Research Paper: Dragonblood (Vanhoef, 2019)** – WPA3 vulnerabilities - <https://wpa3.mathyvanhoef.com/>

**Next Steps :**

how do i pentest wpa 2/ 3 wireless network - research question 1

how do i map wireless networks – research question 2

how do i map databases on wireless networks – research question 3

learn wireshark, end map, sequal map before the next meeting as well as dissecting sources

begin with (mini tutorial WEP, WPA2, and after those are done, we can consider moving to WPA2-E

Should be able to use club AP adapter from Cybersecurity club