**🔍 1. Gizli Ağ (Hidden SSID) Nedir?**

* Normalde kablosuz ağlar (Wi-Fi), SSID (ağ adı) bilgisini herkese **yayınlar**.
* Ancak bazı kullanıcılar veya sistem yöneticileri güvenlik gerekçesiyle bu bilgiyi **gizler**.
* Bu durumda ağ ismi (SSID) görünmez olur ve sadece manuel olarak bağlanılabilir.
* **Ama:** Gizli olması, güvenli olduğu anlamına **gelmez**.

**🧠 2. Gizli Ağlar Nasıl Yakalanır?**

Gizli bir ağ SSID’sini yayınlamasa bile, istemciler (bağlanmış cihazlar) o ağa bağlanmaya çalışırken **ağ ismini açığa çıkarırlar**.  
Bu davranış analiz edilerek gizli ağlar tespit edilebilir.

**🛠️ 3. Gerekli Araçlar (Kali Linux)**

* **airmon-ng** → Kablosuz adaptörü monitör moduna almak için
* **airodump-ng** → Paketleri dinleyip ağları analiz etmek için

🌐 **4. Adım Adım Gizli Ağ Bulma**

✅ **1. Kablosuz adaptörü monitör moduna al:**

sudo airmon-ng start wlan0

wlan0 yerine senin adaptör ismin farklı olabilir (iwconfig ile bakabilirsin).

✅ **2. Tüm ağları ve cihazları izle:**

sudo airodump-ng wlan0mon

Bu ekranda SSID kısmı boş olan satırlar, gizli ağları gösterir.

**✅ 3. İstemcisi olan gizli ağı hedefle:**

Gizli ağa bağlı bir cihaz varsa, o cihazın MAC adresi görünür. Onu hedefleyip “deauth” saldırısı yapılır:

**sudo aireplay-ng -0 10 -a GIZLI\_AG\_BSSID -c KULLANICI\_MAC wlan0mon**

* -0 10 → 10 kez bağlantıyı kes
* -a → hedef ağın BSSID’si
* -c → istemcinin MAC adresi

**✅ 4. SSID yakala:**

* Deauthentication saldırısı sonrası, istemci yeniden bağlanmaya çalışır
* Bu sırada airodump-ng ekranında SSID (ağ adı) **anlık olarak görünür**

📷 5. Örnek Terminal Ekranı

metin, ekran görüntüsü, yazı tipi, yazılım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🎯 6. Öğrenim Çıktıları**

* SSID yayını nedir, nasıl gizlenir
* Gizli ağlar nasıl tespit edilir
* Paket dinleme ve istemci ilişkisini analiz etme
* Deauthentication saldırısının nasıl işlediği
* Pasif bilgi toplama tekniklerinin mantığı