**🔍 1. WPA/WPA2 Nedir?**

* **WPA (Wi-Fi Protected Access)** ve **WPA2**, kablosuz ağlarda veri güvenliği sağlamak için kullanılan şifreleme protokolleridir.
* WPA2, WPA'nın daha güçlü bir sürümüdür ve genellikle **AES** (Advanced Encryption Standard) kullanır.
* Amaç: Kablosuz ağ üzerinden yapılan iletişimi **şifreleyerek** dış müdahalelere karşı korumak.

**⚔️ 2. WPA/WPA2’ye Yönelik Saldırı Türleri**

**✅ a) Handshake Yakalama**

* Kablosuz cihaz, modeme bağlanırken bir "handshake" (tokalaşma) süreci gerçekleşir.
* Bu handshake dosyası, parola kırma saldırıları için yakalanabilir.

**✅ b) Dictionary Attack / Wordlist Attack**

* Elde edilen handshake dosyası, sözlükteki şifrelerle eşleştirilerek çözülmeye çalışılır.
* Eğer şifre zayıfsa, kırılma ihtimali yüksektir.

**✅ c) Deauthentication (Bağlantı Kesme) Saldırısı**

* Hedef cihaz, ağdan zorla çıkarılır. Yeniden bağlanmaya çalışırken handshake alınır.
* Bu saldırı, aireplay-ng aracıyla yapılır.

**✅ d) PMKID Saldırısı (Modern WPA2 Yöntemi)**

* Cihaz bağlanmadan önce bile şifre çözümüne olanak sağlar.
* Özellikle bazı router modellerinde etkili olur.

**🧰 3. Kullanılabilecek Araçlar (Kali Linux)**

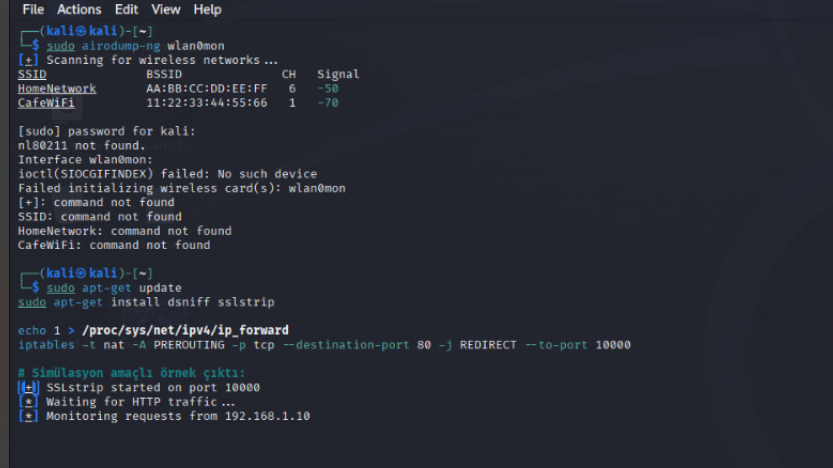
* airmon-ng → Kablosuz kartı monitor moduna almak için
* airodump-ng → Erişim noktalarını ve cihazları izlemek için
* aireplay-ng → Deauthentication saldırısı için
* aircrack-ng → Handshake dosyasını kırmak için
* hcxdumptool ve hashcat → PMKID saldırıları için

⚙️ 4. Kurulum (Kali’de genelde önceden yüklüdür)

metin, yazı tipi, makbuz, beyaz içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.





Örnekteki gibi

**🧪 7. Uygulama Senaryosu (Sınıf Ortamı İçin)**

1. Deneysel WPA2 ağı kurulur (basit parola ile).
2. Öğrenciler yukarıdaki adımları uygulayarak handshake dosyası elde eder.
3. aircrack-ng veya hashcat ile parola çözüm süreci başlatılır.
4. Öğrencilere güçlü ve zayıf şifreler arasındaki farklar açıklanır.

**🎯 9. Sonuç**

Bu eğitimle öğrenciler:

* Kablosuz ağ güvenliği temelini öğrenir,
* Handshake nedir, nasıl elde edilir kavrar,
* Zayıf şifrelerin ne kadar riskli olduğunu fark eder,
* WPA2 şifreleme ve saldırı yöntemlerine karşı savunma yollarını öğrenir.