**🔎 1. WEP Nedir?**

**WEP (Wired Equivalent Privacy)**, kablosuz ağları korumak için geliştirilen eski bir güvenlik protokolüdür.

* **RC4 algoritması** ile veri şifreler.
* **IV (Initialization Vector)** adı verilen rastgele sayı üreticisi kullanır.
* Ancak IV’ler kısa (24 bit) ve tekrarlıdır. Bu da şifrelemenin kırılmasını kolaylaştırır.
* Günümüzde güvensiz kabul edilir ve yerini **WPA/WPA2** almıştır.

**🎯 2. WEP’e Neden Saldırı Yapılır?**

* WEP, zayıf yapısından dolayı **kısa sürede kırılabilir**.
* Gerçek saldırganlar tarafından kötüye kullanılabilir.
* Biz bu saldırıyı **eğitim amacıyla**, şifreleme teknolojilerinin evrimini anlamak için inceliyoruz.

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

* airmon-ng → Kablosuz kartı monitor moduna alır.
* airodump-ng → Ağları ve trafiği izler.
* aireplay-ng → Paket enjeksiyonu ile veri üretir.
* aircrack-ng → Toplanan verilerden WEP şifresini kırar.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

metin, ekran görüntüsü, yazı tipi, doküman, belge içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Örnek komut

**🧪 6. Uygulama Senaryosu (Sınıf Ortamı)**

1. **Test amacıyla WEP şifreli bir ağ kurulur.**
2. Öğrenciler yukarıdaki adımları uygular.
3. WEP şifresi çözülür.
4. WEP’in neden artık kullanılmadığı teknik olarak gösterilir.

**🎓 8. Sonuç**

* WEP artık güvensizdir ve kullanılmamalıdır.
* Zayıf şifreleme yöntemleri hızla kırılabilir.
* Öğrenciler uygulama ile WEP’in zaaflarını deneyimler.
* Modern güvenlik protokollerinin (WPA2, WPA3) önemini kavrar.