

# PAROLA KIRMA SALDIRILARI

Eda Coşkun



# PAROLA MI, ŞİFRE Mİ?

## PAROLA

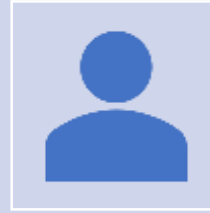
- Kimlik doğrulama yöntemidir.
- Bir sisteme giriş sağlamak amacıyla kullanılır.
- Harf, rakam ve özel karakterlerden oluşan metindir.
- Açık metindir, okunduğunda anlam ifade eder.

## ŞİFRE

- Parolanın bir algoritma aracılığı ile yeni bir formata dönüştürülmüş halidir.
- Metin, sözcük veya karakter dizisidir.
- Çözüm anahtarını bilmeyen kişiler tarafından okunamayacak şekildedir.
- Geri dönüştürülebilir veya dönüştürülemez.



# PAROLA KIRMA SALDIRISI



Kullanıcı hesaplarının kimlik doğrulamasını atlamak veya bunlardan yararlanmak için kullanılan yaygın bir saldırı vektörüdür.



Parolaların tahmin edilmesini ve kırılmasını hızlandıran otomatik parola saldırı araçlarıyla birlikte sistemdeki bozuk bir yetkilendirme güvenlik açığından yararlanmayı içerir.

# SALDIRI TÜRLERİ

Bilgisayar korsanları, genellikle meşru bir kullanıcının parolasını elde etmek ve parolasıyla kimlik doğrulaması yapmak için farklı tekniklere başvurur.

Parolayı ele geçirme amaçlı kullanılan saldırılar, türlerine göre iki ana gruba ayrılabilir. Bunlar:

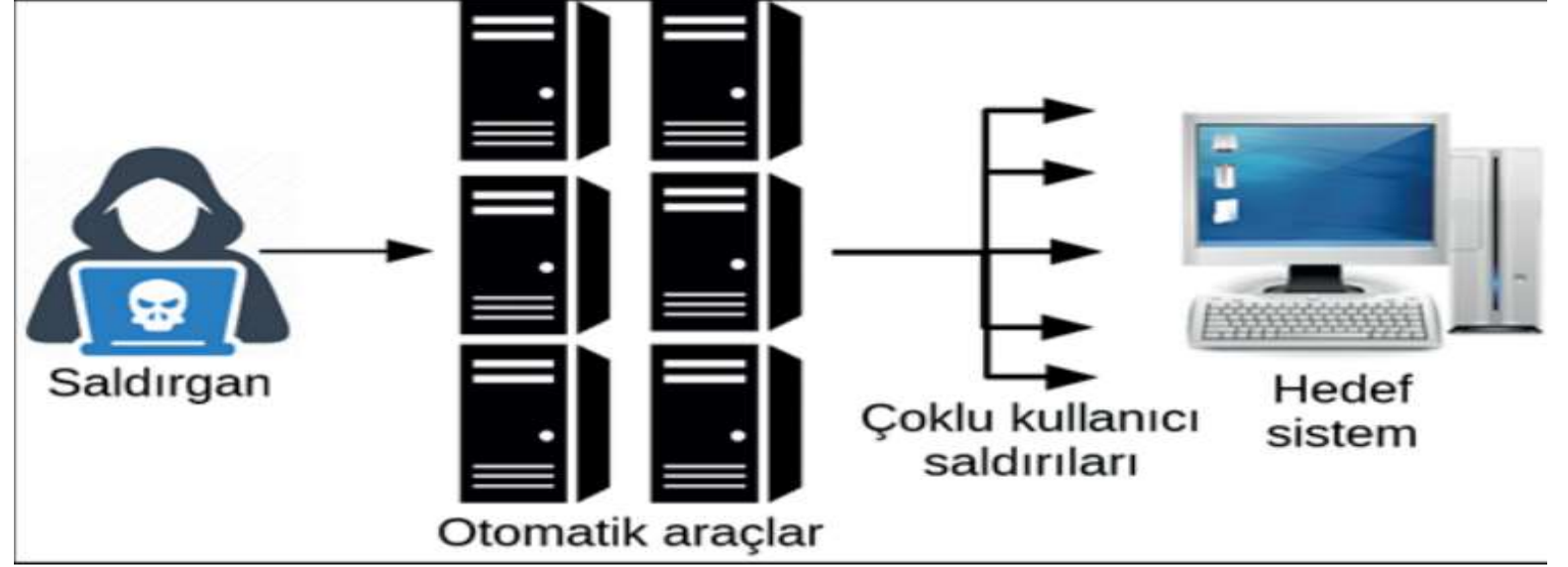
- Aktif Saldırılar
- Pasif Saldırılar

# AKTİF SALDIRILAR

Hedef bilgi sistemine veya veri dosyalarına çevrimiçi (anlık) olarak saldırılar gerçekleştirilmesidir.

- Kaba Kuvvet Saldırısı (Brute Force Attack)
- Parola Püskürtme Saldırısı (Password Spraying Attack)

## Kaba Kuvvet Saldırısı (Brute Force Attack)



- Çalışma Mantığı: Hedef sistemdeki parolayı deneme-yanılma yöntemleriyle kırmak  
Bu amaçla oluşturulan harfler ve özel karakterler içeren bir liste (**Pass List**) hazırlanır.
- Başarı Süresi: Hedef sistemdeki parolanın karmaşıklığına ve saldırıda kullanılan sistemin donanım gücüne bağlıdır.

**ÇALIŞMASI GARANTİ EDİLİR ANCAK  
EN VERİMSİZ VE UZUN SÜREN SALDIRI TÜRÜDÜR.**

## Parola Püskürtme Saldırısı (Password Spraying Attack)

- Çalışma Mantığı: Mevcutta bulunan binlerce standart parolanın belirli zaman aralıklarıyla denenmesi
- Aynı anda binlerce cihaza yapılabileceği gibi farklı zamanlarda da kontrollü olarak yapılabilmektedir.
- Birçok firmanın belirlediği «Aktif Dizin» kurallarına göre, belli bir süre aralığında, belli bir deneme sayısından sonra hesap kilitlendiği için **tekrar sayısı** ve **tekrar süresi** önemli iki kavramdır.
- Hedef: Single-Sign-On (SSO) yöntemi ile giriş yapılan sistemler ve iki aşamalı doğrulama (Two-Factor Authentication) kullanılmayan kurumlar

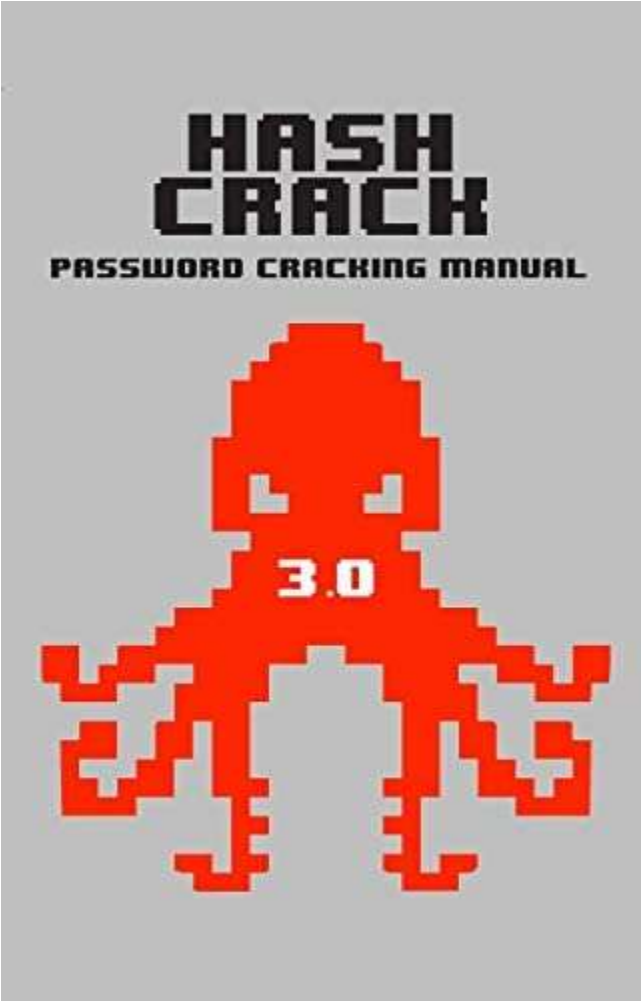
The screenshot shows a login page for 'www.lordiz.com' with the title 'Üye Giriş' (User Login) and 'TekŞifre ile Giriş Yap' (Login with Single-Sign-On). The page features a large input field for 'Cep Telefonu veya E-posta Adresi' (Mobile Phone or Email Address) and a 'Beni Hatırla' (Remember Me) checkbox. Below this is a 'Şifre' (Password) input field with a 'Şifremi Unuttum' (Forgot My Password) link. At the bottom, there are two buttons: 'TekŞifre Al' (Get Single-Sign-On) and 'Giriş Yap' (Login).

# PASİF SALDIRILAR

Çevrimdışı ortamlarda önceden hazırlanan tahmini parolalar kullanılarak veya incelemeler sonucunda ele geçirilen parolalar denenerek saldırı gerçekleştirilmektedir.

- Hash Kırma Saldırısı (Hash Crack Attack)
- Gökkuşáğı Tablo Saldırısı (Rainbow Table Attack)

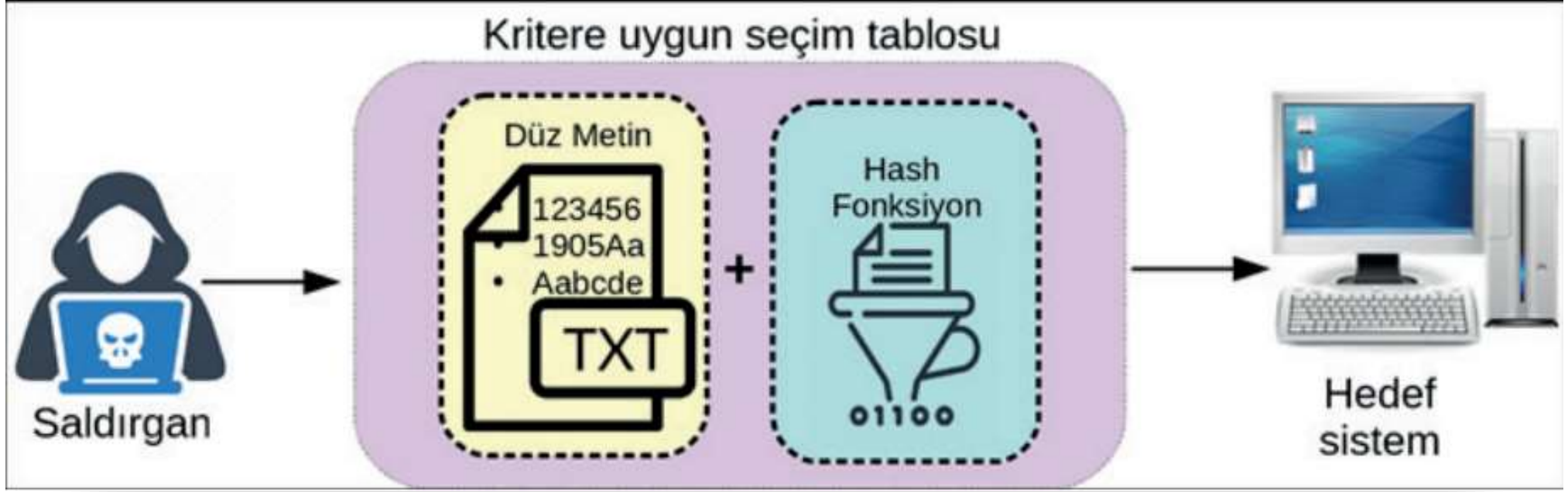




## Hash Kırma Saldırısı (Hash Crack Attack)

- Saldırgan, yaygın olarak kullanılan parola dizelerinden oluşan bir sözlükten hashler oluşturabilir.
- Hash parolalardan oluşan bir veri tabanına erişirse veri tabanındaki her dize için hash kodu hesaplayabilir ve geçerli hash kodla eşleştirebilir.
- Bir eşleşme gerçekleştiğinde bu hashin düz metin parolası bilinir.

Dezavantajı: Veri tabanındaki her dize için hash kodunu hesaplamak **zaman alıcıdır** ve parola olarak kullanılan büyük hacimli dizeler için **çok fazla alan** gerektirir.



## Gökkuşağı Tablo Saldırısı (Rainbow Table Attack)

- Çalışma Mantığı: Belirli bir ölçüte göre seçilen içerisinde düz ve hash fonksiyonlarını içeren bir tablo (**Rainbow Table**) ile hedef sistemdeki parolayı kırmak
- Tablo, sızdırılmış ya da daha önce kırılmış parolaları içerir.
- Açık kaynak araması ile kullanıcıların en çok tercih ettiği parola örnekleri ve özel servislerin (rockyou wordlist gibi) hazırladığı listeler kullanılmaktadır.

Kaba kuvvet saldırısından farkı: Denenen parolaları belirli bir düzene (düz karşılığı olan hash edilmiş parolalara) dayalı olarak seçmek



# EN YAYGIN PAROLA KIRMA SALDIRILARI

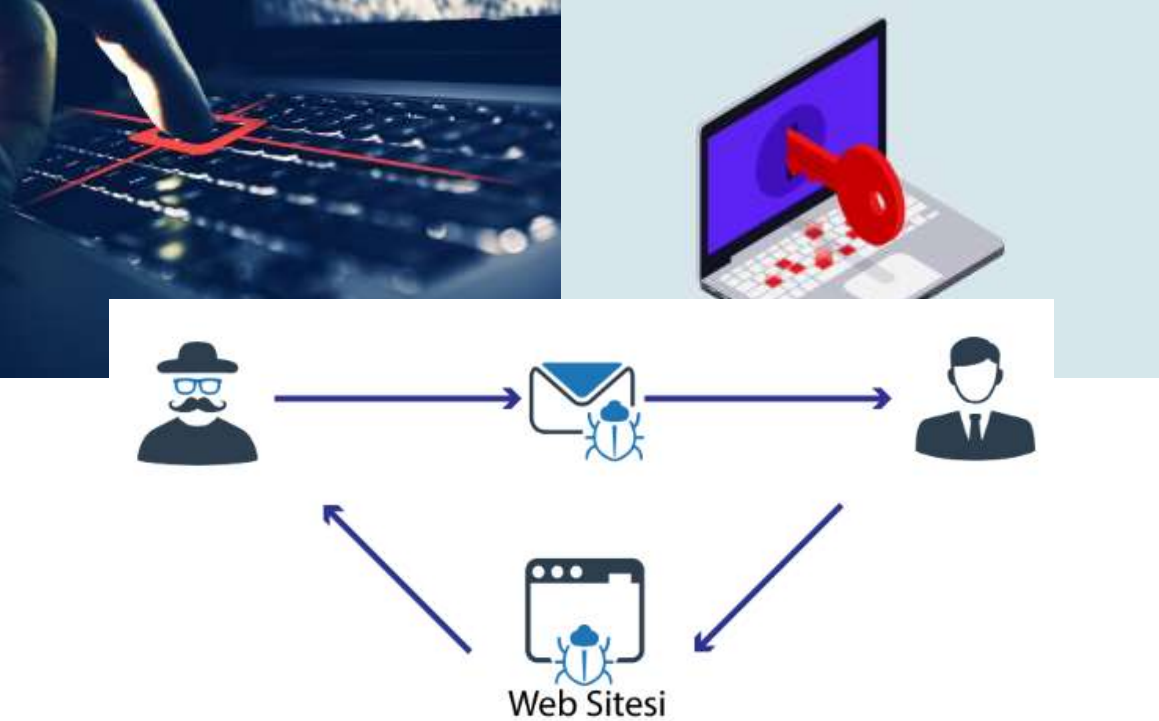
---

Siber saldırganlar tarafından kullanılan en yaygın parola kırma saldırıları:

- Keylogger Yöntemi
- Sosyal Mühendislik Yöntemi
- Sözlük (Dictionary) Yöntemi
- Kaba Kuvvet (Brute-Force) Yöntemi
- Gökkuşaağı Tablo (Rainbow Table) Yöntemi
- Kimlik Bilgilerini Doğrulama (Credential Stuffing) Yöntemi

## Keylogger Yöntemi

Bir saldırgan, kullanıcının klavyesi ile yazdığı tüm yazıları izleyen bir yazılım yüklemeyi başarır ve kimlik bilgileriyle hangi web sitesine veya uygulamaya giriş yaptığını toplamasına olanak tanır. Bu tür saldırılar, kullanıcının kötü amaçlı keylogger yazılımını makinelerine yükleyen başka bir saldırıya dayanır.



## Sosyal Mühendislik Yöntemi

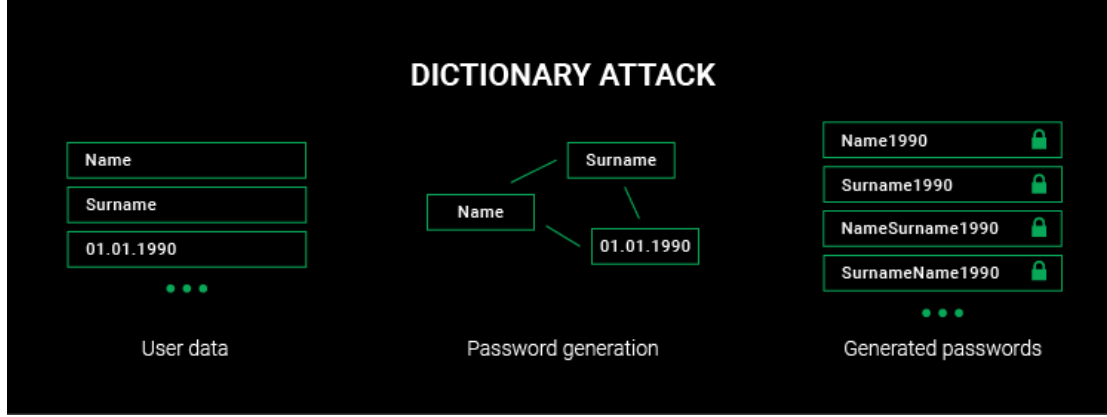


Bu yaklaşım, her biri insanları aldatarak bilgilerini ifşa etme veya belirli bir eylemde bulunmaları için kandırma fikrine dayanan bir dizi stile sahiptir.

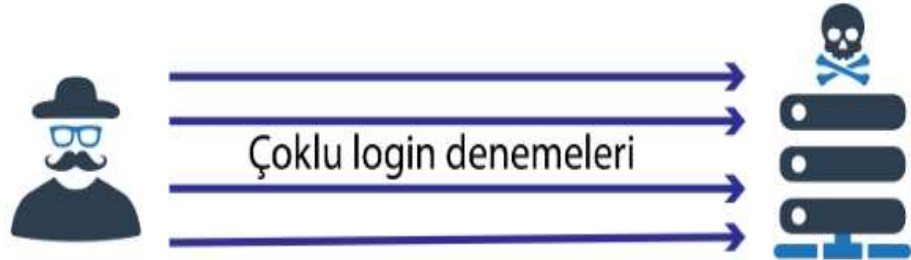
Yaygın yöntemler:

- Kimlik Avı Saldırısı
- Truva Atı Saldırısı

## Sözlük (Dictionary) Yöntemi



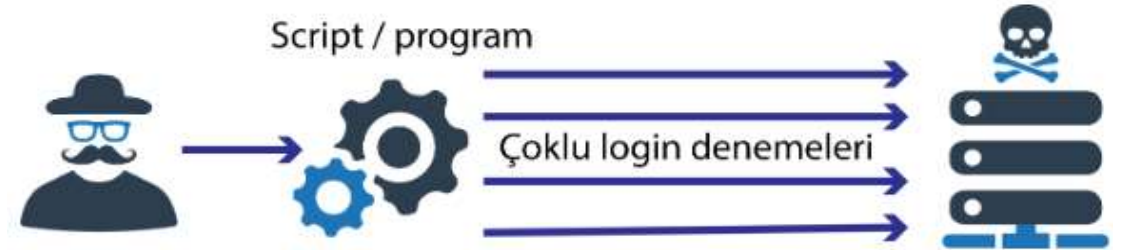
Saldırgan, belirlenen kelimelerin ya da harflerin kombinasyonundan oluşan bir kelime listesi (**dictionary**) hazırlar. Bulmaya çalışılan **parolanın karakteristiği** ile ilgili ne kadar çok şey biliyorsa sözlük dosyası o kadar küçük, kırmak da o kadar kolay olur. Daha sonra oluşturulan bu sözlük ile parola denemeleri yapmaya başlar.



## Kaba Kuvvet (Brute-Force) Yöntemi



Saldırganlar, parola kırılıncaya kadar olası her harf, sayı ve simge parola kombinasyonunu tekrar tekrar denemek için araçlar kullanmaktadır.



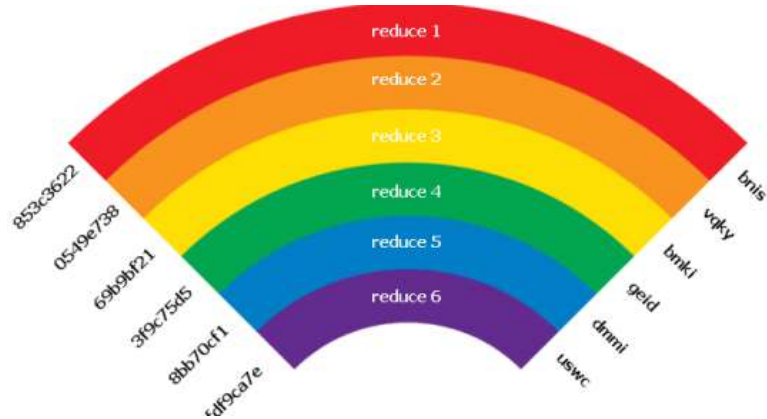


# Gökuşağı Tablo (Rainbow Table)

## Yöntemi

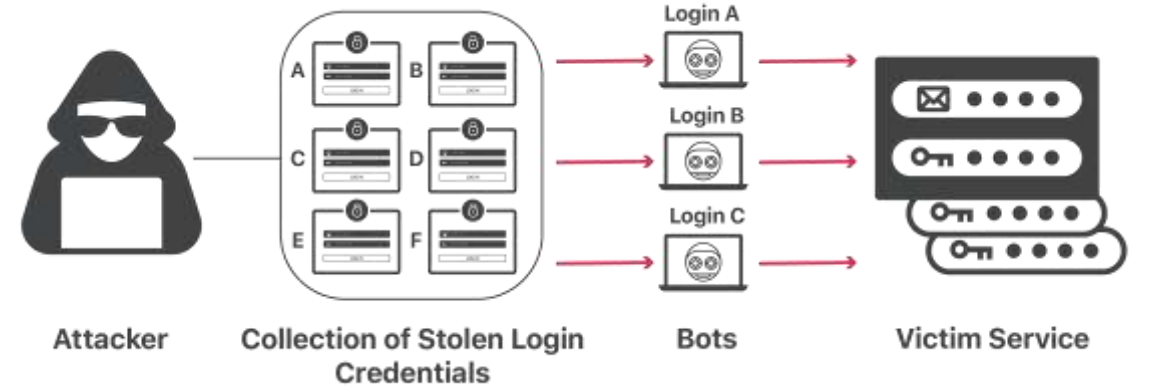


Bu yöntem, veri tabanlarında depolanan parola hashlerini kırmak için kaba kuvvet veya sözlük saldırılarından daha verimli ve etkili olan gökuşağı tablosu adında bir kaynak kullanmaktadır.



# Kimlik Bilgilerini Doğrulama (Credential Stuffing) Yöntemi

Pek çok kişinin hesaplar arasında aynı parolaları veya parola çeşitlerini kullandığını bilen saldırganlar, veri sızıntılarından ve saldırı olaylarından toplanan çalıntı kimlik bilgileri ile bu şifreleri kırabilmektedir.



# SALDIRI ARAÇLARI

Ophcrack

Cain and  
Abel

Brutus

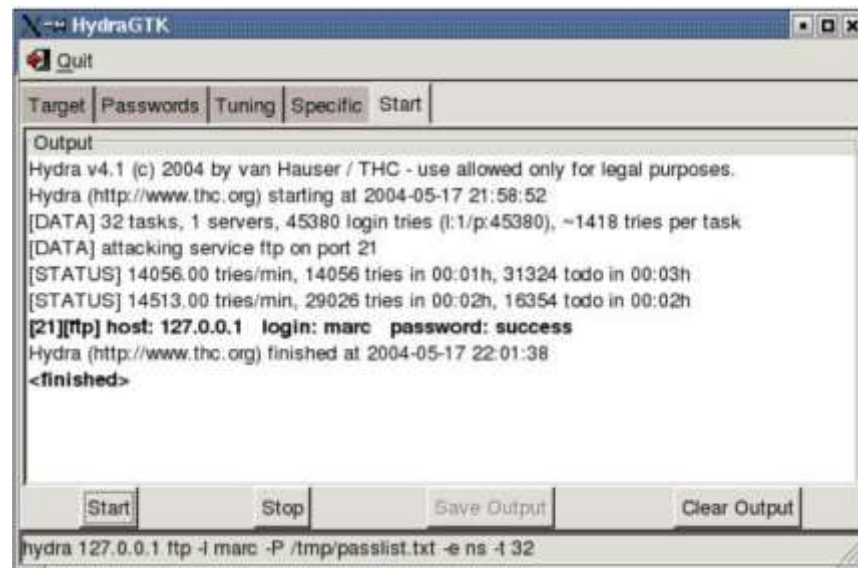
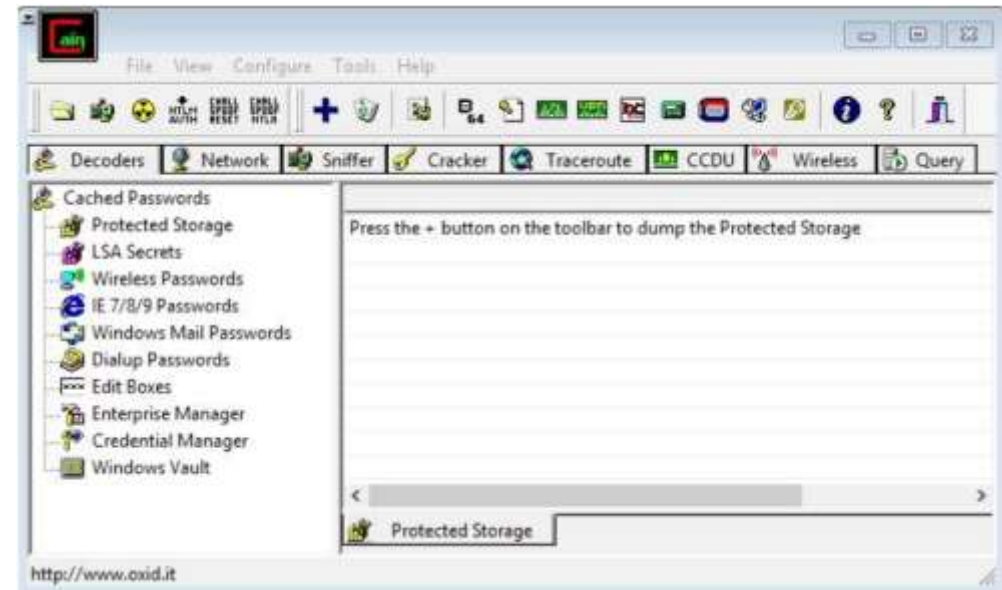
John the  
Ripper

CUPP

Hydra

Cewl

Medusa

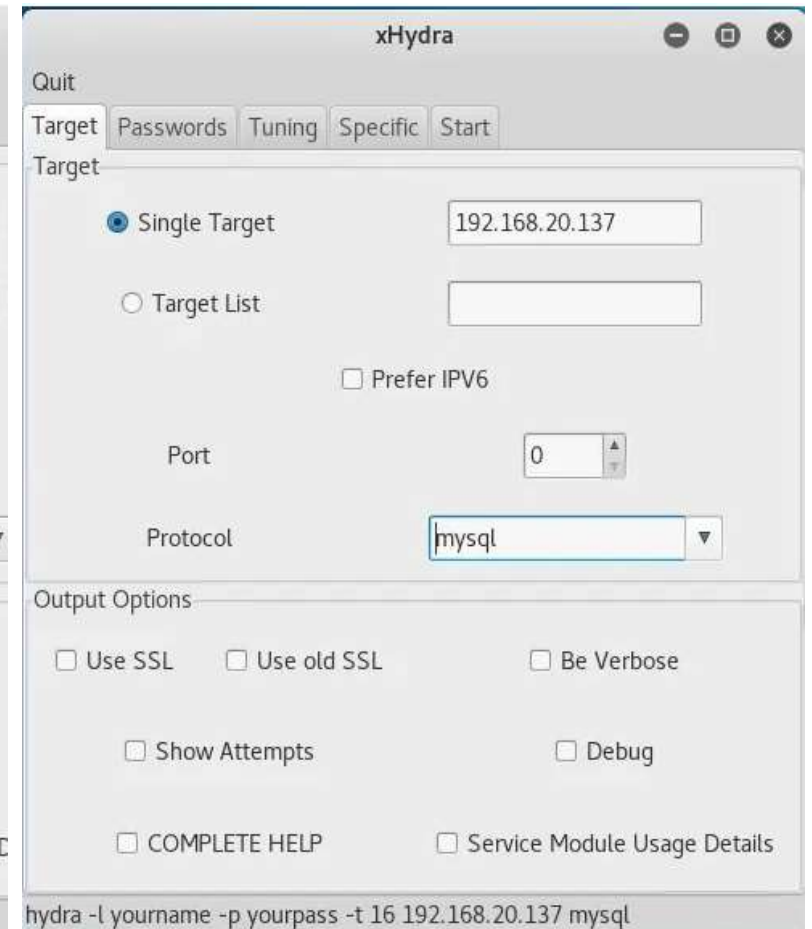
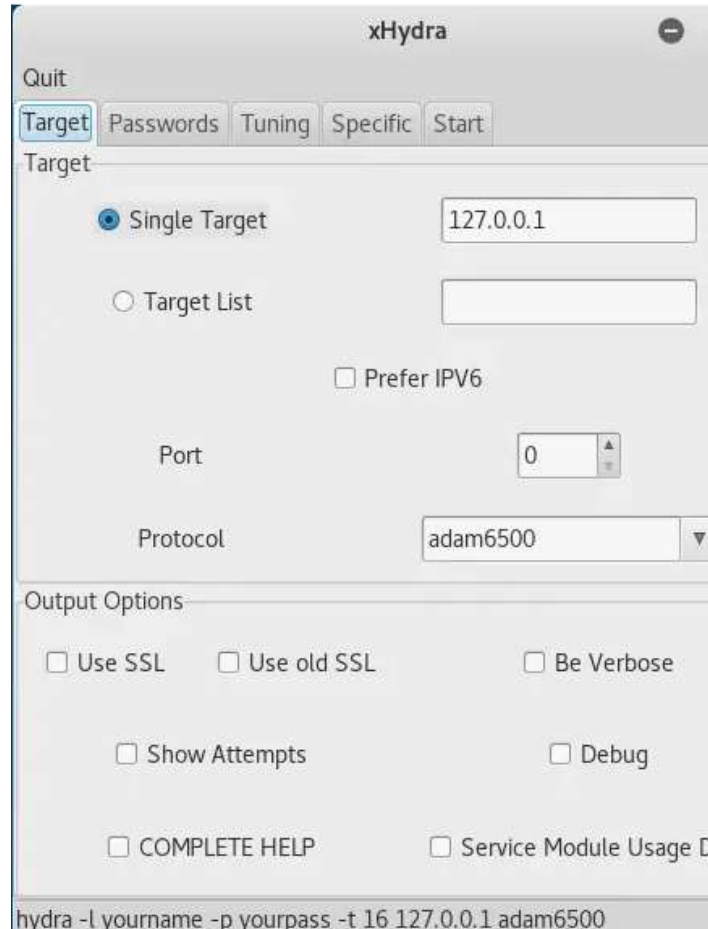




# Hydra ile Saldırı

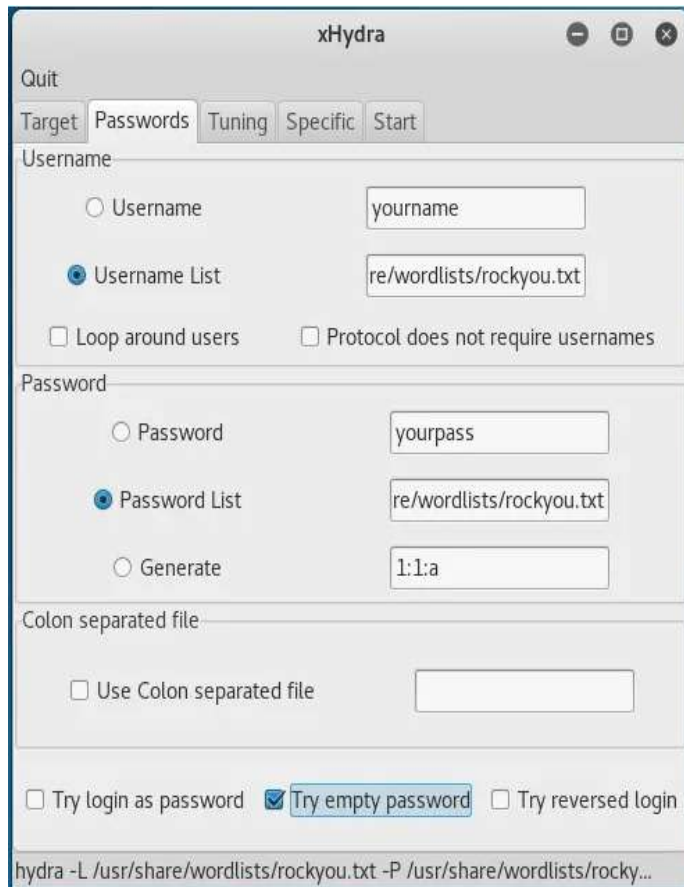


`gunzip /usr/share/wordlists/rockyou.txt.gz`



# Hydra ile Saldırı

File System-usr-share-wordlists



Quit

Target Passwords Tuning Specific Start

Username

☐ Username yourname

☒ Username List re/wordlists/rockyou.txt

☐ Loop around users ☐ Protocol does not require usernames

Password

☐ Password yourpass

☒ Password List re/wordlists/rockyou.txt

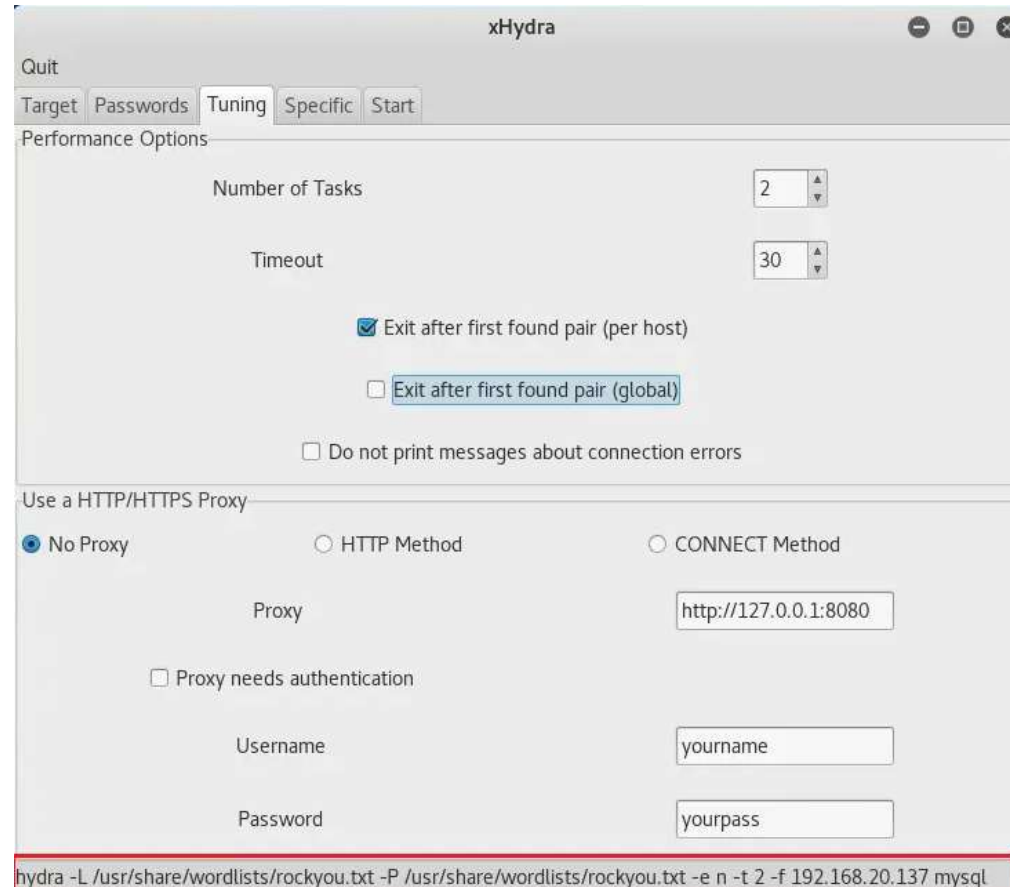
☐ Generate 1:1:a

Colon separated file

☐ Use Colon separated file

☐ Try login as password ☒ Try empty password ☐ Try reversed login

hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rocky...



Quit

Target Passwords Tuning Specific Start

Performance Options

Number of Tasks 2

Timeout 30

☒ Exit after first found pair (per host)

☐ Exit after first found pair (global)

☐ Do not print messages about connection errors

Use a HTTP/HTTPS Proxy

☒ No Proxy ☐ HTTP Method ☐ CONNECT Method

Proxy http://127.0.0.1:8080

☐ Proxy needs authentication

Username yourname

Password yourpass

hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt -e n -t 2 -f 192.168.20.137 mysql

# Hydra ile Saldırı



# SALDIRI ÖRNEKLERİ

- İlk saldırılar 90'lı yıllarda
- 2009 yılında o güne kadar yaşanmış en büyük kırma saldırısı olan “Rockyou.com” web hizmetinden 32 milyona yakın parola kırılarak piyasaya sürülmüştür.
- 2011 Haziran ayında NATO üyelerinin 11.000 kayıtlı kullanıcılarının meta-data bilgileri ele geçirildi.
- Temmuz ayında ise Amerika Birleşik Devletlerinde görev yapan özellikle askeri personellerine ve iç işleri çalışanlarına ait bilgilerin ele geçirilerek terör örgütlerine dağıtıldığı iddia edildi.

Bu saldırılardan sonra birçok resmi kurum ve e-ticaret siteleri zayıf parola kullanımını (1234, abcd gibi) yasakladı ve güçlü parola algoritması (büyük harf simge içeren en az sekiz karakterden oluşan gibi) standartı kullanımını zorunlu hale getirmiştir.

# Parola Kirmak Ne Kadar Süre?

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %\$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

# SALDIRI ORANLARI

## Stolen or Weak Passwords



of breaches leveraged  
either stolen and/or  
weak passwords.

## Social Attacks Social attacks, such as phishing, accounted for



of attacks that resulted  
in a data breach.

## Credential-Stealing Software



of data breaches involved  
some form of credential-  
stealing malware.

# SALDIRILARA NEDEN OLAN EKSİKLİKLER

Birçok kurum/kuruluş ve kullanıcılar tarafından bu saldırılar için gerekli önlemler eksik kalmaktadır.

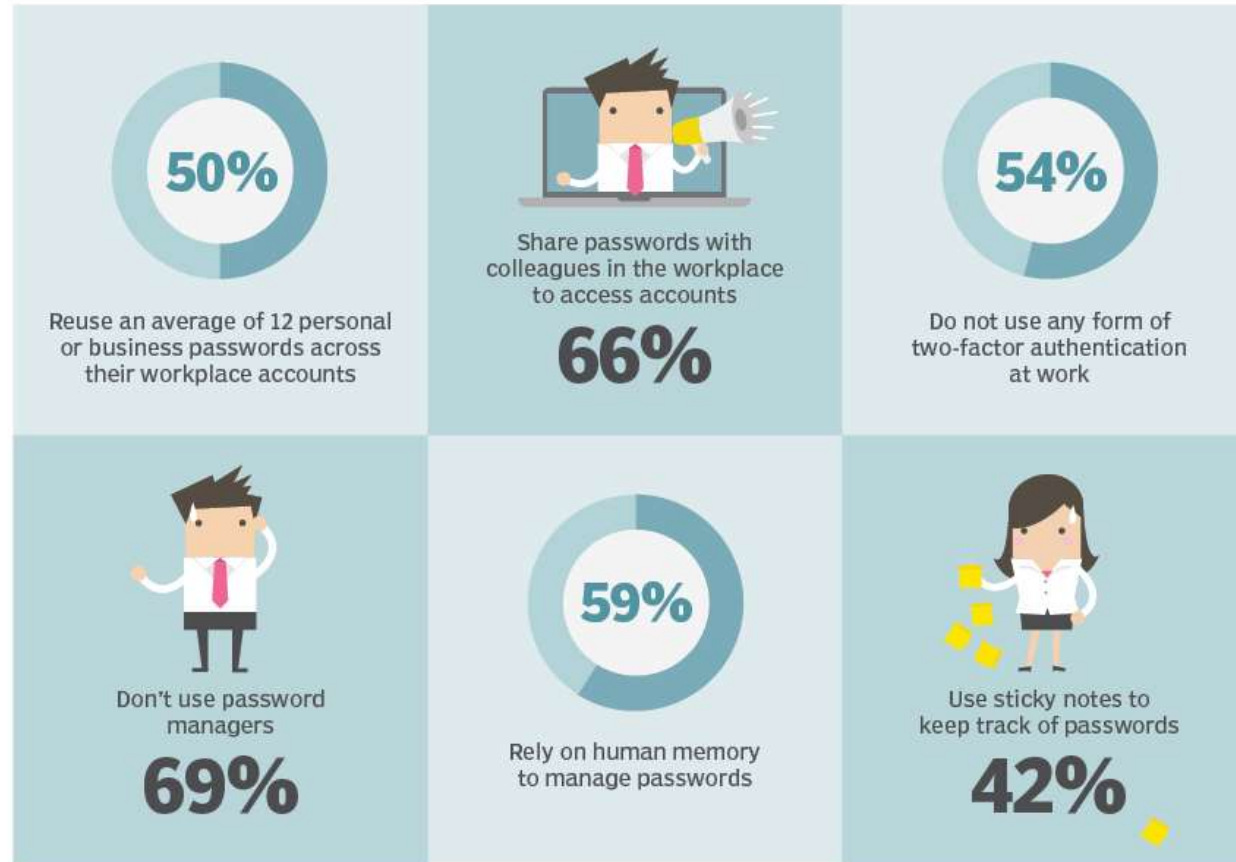
- Kurum içi gerekli parola politikalarının yetersiz olması,
- SIEM kullanılmaması,
- Hesap kilitleme politikalarının bulunmaması,
- Basit parola kullanımı,
- Aynı parolanın başka yerlerde kullanılması

gibi hatalar sebebiyle ciddi zararlar ortaya çıkabilir.



# Password hygiene shortcomings

The Ponemon Institute's latest research report on password practices reveals several areas where real-world practices fall short of password best practices.





# Parola Kırma Saldırıları Nasıl Önlenir?

Parola kırma saldırılarını önlemek için en iyi uygulamalardan birkaçı şunlardır:

- Güçlü parola politikaları uygulamak
- Kuruluş çapında parola güvenliği eğitimi
- Çok faktörlü kimlik doğrulamayı etkinleştirmek
- Her uygulama için farklı parola kullanmak
- SIEM (Güvenlik Bilgileri ve Olay Yönetimi) kullanılması

