BRUTE-FORCE ATTACKS
KABA KUVVET SALDIRILARI

YASİN MADEN

Kaba kuvvet saldırısı nedir?

Kaba kuvvet saldırısı, genellikle bir parola, URL veya şifreleme anahtarını bulmak için tüm kombinasyonları deneyerek gerçekleştirilen bir siber saldırı türüdür.

Tüm olası parola kombinasyonları sisteme sırayla denenebilir. Bu, herhangi bir parolanın uzunluğu veya karmaşıklığı ne olursa olsun, sonunda doğru parolayı bulma garantisi sağlar.

Bu tür saldırılar genellikle zaman alıcıdır ve geniş bir parola uzayını taramak için çok fazla hesaplama gücü gerektirebilir.

Kaba kuvvet saldırı çeşitleri

- Simple Brute-Force Attacks
- Dictionary Attacks
- Rainbow Table Attacks
- Credential Recycling
- Hybrid Brute Force Attack
- Reverse Brute Force Attack

Simple Brute-Force Attack

En ilkel kaba kuvvet saldırı çeşididir.

Belirlediğimiz şartlara göre tüm olasılıkları deneyerek hedefin şifresini bulmak için yapılan saldırı türüdür.

Şifre kırma işlemi parolanın karmaşıklık seviyesine göre günlerce, haftalarca hatta yıllarca sürebilir.

```python
from string import ascii_letters, digits, punctuation


#   4 Karakter  |   Rakamlar    |   Harfler (Büyük - Küçük) | Noktalama İşaretleri
for i in ascii_letters + digits + punctuation:
    for j in ascii_letters + digits + punctuation:
        for k in ascii_letters + digits + punctuation:
            for l in ascii_letters + digits + punctuation:
                print(i, j, k, l)
```

Credential Recycling

Daha önce ele geçirilen veya sızdırılan kullanıcı kimlik bilgilerinin tekrar kullanılması anlamına gelir.

Bu, saldırganın elindeki kullanıcı adı ve şifre kombinasyonlarını başka platformlarda veya hesaplarda kullanarak yetki elde etmeye çalıştığı bir siber saldırı türüdür.

Korunmak için şifrelerimiz güçlü ve benzersiz olmalıdır.

(Parola yöneticisi kullanabilirsiniz.)

★★★★★
Parola Yöneticisi

Facebook'un bir siber saldırı sonucunda bazı bilgilerimizi sızdırdığını varsayalım.

Facebook'tan sızdırılan bilgiler	
e-mail:	yasin.maden@ogr.dpu.edu.tr
password:	yasin123

Saldırganlar bu bilgileri kullanarak diğer popüler web sitelerindeki hesaplara giriş yapmaya çalışır.

Google, Instagram…

Rainbow Table Attack

Veri tabanlarında kullanıcı şifreleri çeşitli hash algoritmaları ile şifrelenip saklanır.

Bu hash değerleri geri döndürülemez ancak önceden hazırlanan hash listeleri ile karşılaştırma yapılabilir.

85d827d4dbb3d93690e834b8203281ecbe8db975b84fb9db34f483ca8ffb6f88

- (SHA-256) Bir saldırıda bu hash değerini ele geçirdiğimizi varsayalım.

Dictionary Attack

Saldırganlar önceden hazırlanmış bir "sözlük" veya kelime listesini kullanır ve şifre kombinasyonlarını deneyerek sisteme erişmeye çalışırlar.

Personalized Dictionary Attack

Kişiselleştirilmiş sözlük saldırısı, saldırganların hedefin kişisel bilgilerini içeren özel bir sözlük veya kelime listesi oluşturarak şifre kırma türünü ifade eder.

(Cupp, Crunch, Cewl, Dymerge… gibi araçlar kullanılarak sözlük oluşturulabilir.)

Teşekkürler...