**Hedefe Özel Şifre Listeleri Oluşturmanın Sanatı: CeWL Nedir ve Nasıl Kullanılır?**

Siber güvenlikte kaba kuvvet (brute-force) saldırıları denince akla genellikle rockyou.txt gibi milyonlarca genel şifre içeren devasa listeler gelir. Peki ya hedefinizdeki kişinin veya şirketin bu listelerde olmayan, tamamen kendilerine özgü bir şifre kullanma ihtimali? Belki şirketlerinin adı, sevdikleri bir proje, evcil hayvanlarının ismi veya çalıştıkları departmanla ilgili bir kelime... İşte bu "hedefe özel" kelimeleri keşfedip onlardan bir şifre listesi oluşturmanın en akıllı yolu, **CeWL** (Custom Word List Generator) aracıdır.

Bu yazıda, CeWL'ün ne olduğunu, neden standart kelime listelerinden çok daha etkili olabildiğini, nasıl kurulduğunu ve bu aracı bir sosyal mühendislik ustası gibi kullanarak hedefe yönelik güçlü şifre listeleri nasıl oluşturabileceğinizi pratik örneklerle ele alacağız.

**1. CeWL Aracı Nedir?**

**CeWL**, belirli bir web sitesini bir örümcek gibi tarayarak, site içeriğinde geçen kelimelerden özel bir kelime listesi (wordlist) oluşturan, Ruby tabanlı bir komut satırı aracıdır. "Custom Word List Generator" (Özel Kelime Listesi Oluşturucu) adının hakkını veren CeWL, bir şirketin "Hakkımızda", "Projelerimiz", "Blog" gibi sayfalarını gezer ve burada tekrar eden kelimeleri toplayarak size sunar.

CeWL'ün temel mantığı, insanların genellikle kendileriyle veya çalıştıkları ortamla ilgili kelimeleri şifre olarak seçme eğilimine dayanır. Örneğin, "HedefSirket" adlı bir şirketin web sitesinde sıkça "ProjeX", "Inovasyon2023", "TakimLideri" gibi kelimeler geçiyorsa, çalışanların "ProjeX123", "Inovasyon!", "TakimLideri23" gibi şifreler kullanma olasılığı yüksektir. CeWL, bu potansiyel şifre köklerini sizin için otomatik olarak toplar.

**2. Neden Kullanılır?**

CeWL, standart kelime listelerine göre birçok avantaja sahiptir ve bu yüzden sızma testlerinin önemli bir parçasıdır:

* **Hedefe Odaklıdır:** Milyonlarca alakasız kelimeyi denemek yerine, doğrudan hedefle ilgili, başarı olasılığı çok daha yüksek olan küçük ve etkili bir liste oluşturur.
* **Zaman Kazandırır:** Devasa listelerle yapılan kaba kuvvet saldırıları günler sürebilir. CeWL ile oluşturulan odaklı bir liste, sonuçları saatler hatta dakikalar içinde verebilir.
* **Sosyal Mühendislik Boyutu:** Bir şirketin web sitesinden toplanan kelimeler, o şirketin kültürü, projeleri ve çalışanları hakkında ipuçları verir. Bu, sadece şifre kırma değil, aynı zamanda diğer sosyal mühendislik saldırıları için de değerli bir bilgi kaynağıdır.
* **Fark Edilmeme Olasılığı:** Çok sayıda başarısız giriş denemesini izleyen sistemler, küçük ve hedefe yönelik bir liste ile yapılan denemeleri fark etmeyebilir.
* **Standart Listelerin Dışına Çıkar:** password123, 123456 gibi herkesin bildiği şifrelerin ötesinde, sadece o hedefe özgü kelimeleri bulur.

**3. Nasıl Kurulum Yapılır?**

CeWL, Ruby ile yazıldığı için sisteminizde Ruby'nin kurulu olması gerekir.

**Yöntem 1: Gem ile Kurulum (Ruby'nin Paket Yöneticisi)**

Bu en standart ve kolay kurulum yöntemidir.

# Ruby kurulu değilse önce onu ve gerekli geliştirme araçlarını kurun

# Ardından gem ile CeWL'ü kurun

sudo gem install cewl

**Yöntem 2: Kali Linux (Zaten Kurulu Gelir)**

Eğer sızma testleri için popüler bir dağıtım olan Kali Linux kullanıyorsanız, CeWL sisteme önceden yüklenmiş olarak gelir. Terminale cewl yazarak doğrudan kullanmaya başlayabilirsiniz.

**Yöntem 3: GitHub'dan Klonlama**

Aracın en güncel halini doğrudan kaynaktan almak isterseniz:

git clone https://github.com/digininja/CeWL.git

cd CeWL

# Bu dizindeyken aracı "ruby cewl.rb" komutuyla çalıştırabilirsiniz.

**4. Kullanım Parametreleri Nedir?**

CeWL'ün kelime listenizi özelleştirmenize olanak tanıyan birçok kullanışlı parametresi vardır:

* <url>: Aracın tarayacağı hedef web sitesinin URL'si. (Temel parametre)
* -d <sayı> veya --depth <sayı>: Örümceğin ne kadar derine ineceğini belirtir. Örneğin, -d 2 ana sayfadan bir linke tıklar ve o linkin içindeki linklere de gider.
* -m <sayı> veya --min\_word\_length <sayı>: Listeye eklenecek kelimelerin minimum uzunluğunu belirtir. "ve", "bir" gibi kısa ve alakasız kelimeleri elemek için kullanışlıdır.
* -w <dosya> veya --write <dosya>: Oluşturulan kelime listesini belirtilen dosyaya yazar.
* -c veya --count: Her kelimenin sitede kaç kez geçtiğini gösterir. En sık kullanılan kelimeleri bulmak için harikadır.
* -e veya --email: Sitede bulunan e-posta adreslerini de toplar.
* --email\_file <dosya>: Bulunan e-postaları ayrı bir dosyaya yazar.
* --with-numbers: Kelimelerin hem harfli hem de sayı içeren versiyonlarını listeye ekler (örneğin "kelime" ve "kelime123").
* --auth\_user ve --auth\_pass: Kimlik doğrulaması gerektiren siteleri taramak için kullanıcı adı ve şifre belirtir.

**5. Etkili Kullanım İçin 5 Örnek ve Açıklamaları**

Şimdi CeWL'ü bir siber güvenlik analisti gibi nasıl kullanacağımıza bakalım.

**Örnek 1: Temel Kelime Listesi Oluşturma**

Bu, bir şirketin web sitesinden hızlıca bir kelime listesi çekmenin en basit yoludur.

cewl https://hedefsirket.com -m 6 -w hedefsirket\_wordlist.txt

* **Açıklama:**
  + https://hedefsirket.com: Taranacak hedef siteyi belirtir.
  + -m 6: Sadece 6 veya daha fazla karakter uzunluğundaki kelimeleri listeye dahil eder. Bu, "a", "ile", "ve" gibi anlamsız kelimeleri filtreler.
  + -w hedefsirket\_wordlist.txt: Çıktıyı hedefsirket\_wordlist.txt adlı bir dosyaya kaydeder. Bu dosya artık Hydra veya Hashcat gibi araçlarda kullanılmaya hazırdır.

**Örnek 2: Derinlemesine Tarama ve En Popüler Kelimeleri Bulma**

Sitenin sadece ana sayfasını değil, alt sayfalarını da tarayarak daha kapsamlı bir liste oluşturalım.

cewl https://hedefsirket.com -d 3 -c

* **Açıklama:**
  + -d 3: CeWL'e ana sayfadan başlayarak 3 seviye derine inmesini söyler. Bu, blog yazıları, proje detay sayfaları gibi daha zengin içerikli sayfalara ulaşmasını sağlar.
  + -c: Çıktıda her kelimenin yanında o kelimenin sitede kaç kez geçtiğini gösterir. Örneğin Inovasyon: 45. Bu, şirketin en çok vurguladığı ve dolayısıyla çalışanların şifre olarak seçme ihtimali en yüksek olan kelimeleri belirlemenize yardımcı olur.

**Örnek 3: E-posta Adreslerini ve Kullanıcı Adlarını Toplama**

Şifreleri kırmak için önce geçerli kullanıcı adlarına ihtiyacımız var.

cewl https://hedefsirket.com -e --email\_file emails.txt

* **Açıklama:** -e ve --email\_file emails.txt parametreleri, CeWL'ün siteyi tararken isim.soyisim@hedefsirket.com formatındaki tüm e-posta adreslerini bulup emails.txt dosyasına kaydetmesini sağlar. E-postaların @ işaretinden önceki kısmı (isim.soyisim) genellikle o şirketin kullanıcı adı formatıdır. Bu, kaba kuvvet saldırısı için hem kullanıcı adı hem de e-posta listesi elde etmenizi sağlar.

**Örnek 4: Kimlik Doğrulaması Gerektiren Bir Intranet Sitesini Tarama**

Bazen hedef, sadece şirket çalışanlarının erişebildiği bir iç ağ (intranet) sitesi olabilir.

cewl https://intranet.hedefsirket.com --auth\_user testkullanici --auth\_pass test123 -w intranet\_words.txt

* **Açıklama:** Eğer elinizde düşük yetkili bir kullanıcı hesabı varsa, --auth\_user ve --auth\_pass parametreleriyle bu hesabı kullanarak intranet sitesinde oturum açabilir ve sadece giriş yapmış kullanıcıların görebileceği sayfalardan (departman isimleri, iç projeler, personel adları vb.) kelimeler toplayabilirsiniz. Bu, çok daha değerli ve hedefe yönelik bir kelime listesi oluşturur.

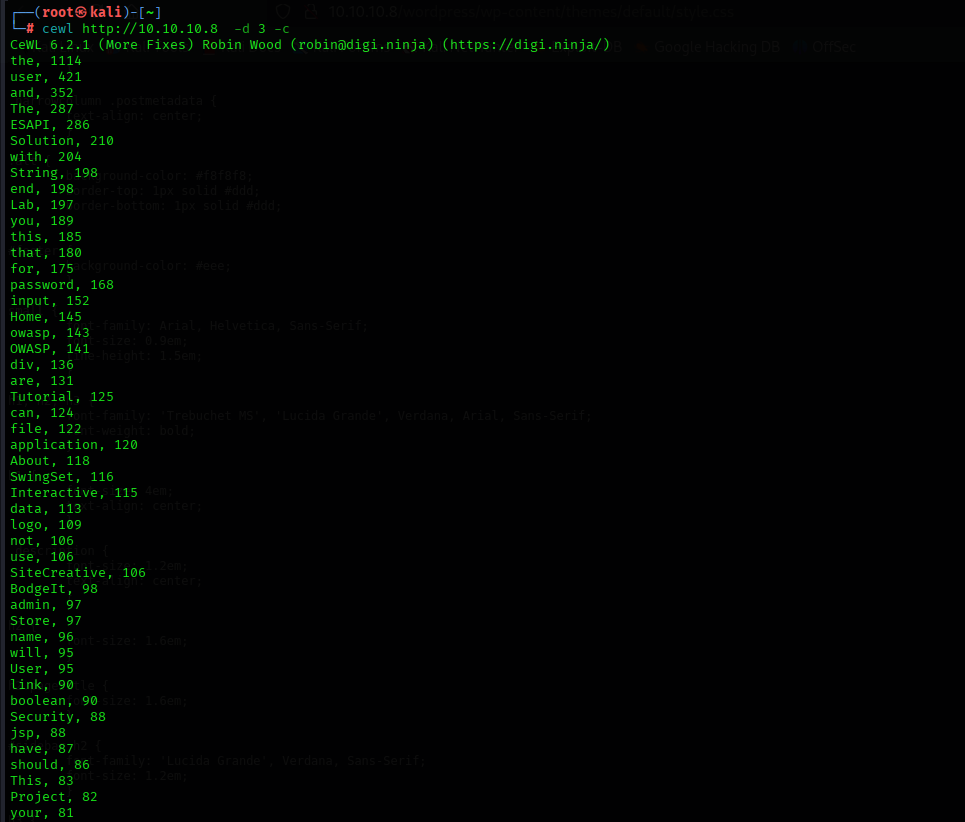
**Örnek 5: Sayısal Karakterler İçeren Potansiyel Şifreler Oluşturma**

İnsanlar genellikle şifrelerinin sonuna bir yıl veya sayı ekler (örn: Sirket2024).

cewl https://hedefsirket.com -m 8 --with-numbers -w hedefsirket\_numeric.txt

* **Açıklama:** --with-numbers parametresi, CeWL'ün bulduğu her kelimenin sonuna rakamlar ekleyerek listeyi zenginleştirmesini sağlar. Örneğin, "ProjeX" kelimesini bulduysa, listeye hem "ProjeX" hem de "ProjeX2023" gibi varyasyonları ekleyebilir. Bu, daha karmaşık şifre politikalarına sahip sistemlere karşı başarı şansını artırır.

**📄 Örnek: CeWL ile Özelleştirilmiş Wordlist (Kelime Listesi) Oluşturma**  
**CeWL** (Custom Word List generator), hedef bir web sayfasını tarayarak o sayfada geçen kelimelerden özelleştirilmiş bir **wordlist (kelime listesi)** oluşturmak için kullanılan bir bilgi toplama aracıdır. Bu wordlist, daha sonra parola tahmini (brute force) gibi saldırılarda kullanılabilir.

  
Komutta cewl http://10.10.10.8 -d 3 -c parametreleri kullanılmıştır. Bu parametrelerin anlamı:

* -d 3: Sayfa derinliği 3 olacak şekilde iç linkleri takip ederek tarama yapılır.
* -c: Çıktıda her kelimenin kaç kez geçtiği de gösterilir.

Elde edilen sonuçlar, web sitesindeki metin içeriklerinden çıkarılmış kelimeleri ve bu kelimelerin frekansını (kaç kez geçtiğini) listeler. Örneğin, “user”, “password”, “admin”, “application” gibi terimler oldukça sık tekrar etmektedir ve bu tür bilgiler, bir saldırganın hedef siteye özel parola tahmini listeleri oluşturmasına olanak tanır. CeWL, özellikle sosyal mühendislik ve parola analiz süreçlerinde değerli bir bilgi toplama aracıdır.

**Sonuç**

CeWL, kaba kuvvet saldırılarına zeka ve strateji katan, küçük ama son derece etkili bir araçtır. Milyonlarca deneme yanılma yapmak yerine, hedefi analiz ederek ve sosyal mühendislik prensiplerini kullanarak başarı olasılığını katbekat artırır. Bir sızma testinde, hedefin dijital ayak izlerinden faydalanarak onlara özel bir anahtar yaratmak, çoğu zaman en kilitli kapıları bile açabilir.

Her zaman hatırlanması gerektiği gibi, CeWL ve benzeri araçlar büyük bir güç ve sorumluluk gerektirir. Bu aracı **kesinlikle ve yalnızca yasal olarak test etme izniniz olan sistemlerde** kullanarak, bilginizi ve yeteneklerinizi siber güvenliği artırma yönünde, etik sınırlar içinde kullanmalısınız.