**Kırık Şifrelerin Peşindeki Çevrimiçi Dedektif: findmyhash Nedir ve Nasıl Kullanılır?**

Bir sızma testi sırasında bir veritabanı sızıntısı bulduğunuzu hayal edin. Elinizde kullanıcı adları ve yanlarında d8578edf8458ce06fbc5bb76a58c5ca4 gibi anlamsız görünen karakter dizileri var. Bunlar, kullanıcı şifrelerinin "hash"lenmiş halleridir. Bir sonraki adımınız, bu hash'leri kırarak orijinal şifreleri elde etmektir. Ancak bu işlem, güçlü bilgisayarlar ve saatler süren denemeler gerektirebilir. Peki ya internetin kolektif gücünü kullanarak bu hash'leri saniyeler içinde kırmanın bir yolu olsaydı? İşte bu noktada sahneye **findmyhash** çıkıyor.

Bu yazıda, findmyhash'in ne olduğunu, neden bir siber güvenlik uzmanının zamanından tasarruf sağlayan en iyi dostlarından biri olduğunu, nasıl kurulduğunu ve bu akıllı aracı kullanarak hash'lenmiş şifrelerin sırlarını nasıl çözeceğinizi adım adım, pratik örneklerle anlatacağız.

**1. findmyhash Aracı Nedir?**

**findmyhash**, verilen bir şifre hash'ini kırmak için çok sayıda ücretsiz çevrimiçi hash kırma hizmetini aynı anda sorgulayan, Python ile yazılmış bir komut satırı aracıdır. Temelde bir "meta-araç" veya "toplayıcı"dır. Yani, şifreyi kırmak için kendi başına bir işlem yapmaz; bunun yerine sizin için internetteki onlarca farklı servise gider, hash'inizi gönderir ve hangisinin doğru şifreyi bulduğunu size raporlar.

CrackStation, MD5Online, GromWeb gibi siteler, milyarlarca hash'i ve karşılık gelen orijinal metinleri (şifreleri) içeren devasa veritabanlarına sahiptir. findmyhash, bu sitelere tek tek girip hash'inizi manuel olarak yapıştırma zahmetinden sizi kurtarır ve tüm bu süreci tek bir komutla otomatikleştirir.

**2. Neden Kullanılır?**

findmyhash, özellikle "hızlı kazanımlar" (quick wins) elde etmek için kullanılır ve birçok avantaj sunar:

* **Muazzam Zaman Tasarrufu:** Onlarca farklı web sitesini manuel olarak ziyaret etmek yerine, tek bir komutla hepsini aynı anda sorgulayarak dakikalar içinde sonuç almanızı sağlar.
* **Maliyet ve Kaynak Verimliliği:** Güçlü bir GPU'ya sahip bir "cracking rig" (şifre kırma sistemi) kurmak ve çalıştırmak pahalıdır. findmyhash, yaygın veya zayıf şifrelerin hash'lerini, hiçbir donanım maliyeti olmadan kırmak için internetin mevcut gücünden faydalanır.
* **Yüksek Başarı Oranı (Yaygın Şifreler İçin):** Eğer bir şifre 123456, password veya qwerty gibi yaygın bir şifre ise, çevrimiçi servislerin veritabanlarında bulunma olasılığı çok yüksektir.
* **Hash Tanımlama:** Bazen elinizdeki hash'in hangi algoritmaya (MD5, SHA1, NTLM vb.) ait olduğunu bilemeyebilirsiniz. findmyhash, hash'in yapısını analiz ederek olası algoritma türlerini size söyleyebilir.
* **Sessiz Bir İlk Adım:** Eğer bir hash findmyhash ile kırılamıyorsa, muhtemelen daha karmaşık ve daha az yaygın bir şifredir. Bu durumda, zamanınızı Hashcat veya John the Ripper gibi daha güçlü çevrimdışı araçlara ayırmanız gerektiğini anlarsınız.

**3. Nasıl Kurulum Yapılır?**

findmyhash, genellikle standart paket yöneticilerinde bulunmaz, bu yüzden en yaygın kurulum yöntemi doğrudan GitHub deposundan klonlamaktır.

**Yöntem 1: Git ile Klonlayarak Kurulum (Önerilen)**

# Projeyi GitHub'dan klonlayın

git clone https://github.com/frdm/findmyhash.git

# Proje dizinine gidin

cd findmyhash

Bu kadar! Araç bir Python betiği olduğu için, genellikle ek bir kuruluma ihtiyaç duymaz. Doğrudan python findmyhash.py komutuyla çalıştırılabilir.

**Yöntem 2: Kali Linux**

Eğer Kali Linux gibi bir siber güvenlik dağıtımı kullanıyorsanız, findmyhash genellikle sisteme önceden yüklenmiş olarak veya apt ile kurulabilir bir paket olarak gelebilir.

sudo apt update && sudo apt install findmyhash

Eğer paket bulunamazsa, Yöntem 1'i kullanmak en garantisidir.

**4. Kullanım Parametreleri Nedir?**

findmyhash'in kullanımı oldukça basittir ve birkaç temel parametre etrafında döner:

* -h <hash>: Kırılacak tek bir hash değerini belirtir.
* -f <dosya>: İçinde her satırda bir hash bulunan bir dosyanın yolunu belirtir. Toplu kırma işlemleri için kullanılır.
* -i: Hash kırmak yerine, verilen hash'in olası algoritma türünü (MD5, SHA256 vb.) tanımlamaya çalışır.
* -g: Çevrimiçi servisler yerine, Google'ı kullanarak hash'i aramaya çalışır. Bazen hash ve kırılmış hali forumlarda veya başka sitelerde açıkça yayınlanmış olabilir.
* -v: "Verbose" (ayrıntılı) modu. Hangi servisin denendiği gibi arka plan bilgilerini gösterir.

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

Şimdi findmyhash'i pratik senaryolarda nasıl kullanacağımıza bakalım.

**Örnek 1: Tek Bir MD5 Hash'ini Kırma**

Bu, aracın en temel kullanımıdır.

python findmyhash.py -h d8578edf8458ce06fbc5bb76a58c5ca4

* **Açıklama:** Bu komut, d8578edf8458ce06fbc5bb76a58c5ca4 hash'ini alır ve desteklenen tüm çevrimiçi kırma servislerine gönderir. Bir veya daha fazla servis bu hash'in karşılığını ("password123" gibi) bulursa, sonucu ekrana basar.

**Örnek 2: Bir Dosyadaki Hash Listesini Toplu Olarak Kırma**

Gerçek bir sızma testi senaryosunda, elinizde yüzlerce hash olabilir.

# hashes.txt dosyasının içeriği:

# 5f4dcc3b5aa765d61d8327deb882cf99

# 202cb962ac59075b964b07152d234b70

# 81dc9bdb52d04dc20036dbd8313ed055

python findmyhash.py -f hashes.txt

* **Açıklama:** Bu komut, hashes.txt dosyasını okur ve içindeki her bir hash'i sırayla çevrimiçi servislere gönderir. Bulunan her hash ve karşılığı ekranda gösterilir. Bu, toplu veritabanı sızıntılarını analiz etmek için inanılmaz derecede verimlidir.

**Örnek 3: Bilinmeyen Bir Hash'in Türünü Tanımlama**

Elinizdeki hash'in hangi algoritmaya ait olduğundan emin değilseniz, bu komutu kullanabilirsiniz.

python findmyhash.py -i 2a013460594348493774cd288229b5b2496827a5

* **Açıklama:** -i parametresi, findmyhash'e kırma işlemi yapmak yerine sadece tanımlama yapmasını söyler. Verilen hash'in uzunluğuna ve karakter yapısına bakarak, "Possible hash type: SHA1" gibi bir çıktı üretecektir. Bu, daha sonra Hashcat gibi araçları doğru modda çalıştırmak için kritik bir bilgidir.

**Örnek 4: Google Gücünü Kullanarak Hash Kırma**

Bazen bir hash o kadar yaygındır ki, birileri onu çoktan kırıp bir foruma veya blog yazısına koymuştur.

python findmyhash.py -h 5f4dcc3b5aa765d61d8327deb882cf99 -g

* **Açıklama:** -g parametresi, findmyhash'in çevrimiçi servislere değil, doğrudan Google'a "5f4dcc3b5aa765d61d8327deb882cf99" şeklinde bir arama sorgusu göndermesini sağlar. Eğer Google sonuçlarında bu hash ile birlikte orijinal metin ("hello") bulunuyorsa, araç bunu size raporlar.

**Örnek 5: Komutları Zincirleyerek Otomasyon (İleri Düzey)**

Bir veritabanı dökümünden (dump.txt) sadece hash'leri çekip anında kırmaya çalışalım. Dosyanın formatı kullanici:hash şeklinde olsun.

cat dump.txt | cut -d':' -f2 | python findmyhash.py -f -

* **Açıklama (Adım Adım):**
  1. cat dump.txt: dump.txt dosyasının içeriğini okur.
  2. |: Çıktıyı bir sonraki komuta gönderir.
  3. cut -d':' -f2: Gelen her satırı : karakterine göre böler ve sadece ikinci sütunu (yani hash'leri) alır.
  4. |: Elde edilen hash listesini findmyhash'e gönderir.
  5. python findmyhash.py -f -: -f - komutu, findmyhash'e dosyadan okumak yerine standart girdiden (yani bir önceki komuttan gelen veriden) okumasını söyler. Bu, tek bir komutla tüm süreci otomatikleştiren güçlü bir tekniktir.

**Sonuç**

findmyhash, siber güvenlik uzmanının cephaneliğindeki en pratik araçlardan biridir. Kendi başına devasa bir güç olmasa da, internetin kolektif şifre kırma gücünü akıllıca kullanarak, özellikle yaygın ve zayıf şifrelere karşı inanılmaz bir hız ve verimlilik sağlar. Karmaşık ve benzersiz şifreler için her zaman Hashcat gibi çevrimdışı araçlara ihtiyaç duyulacaktır, ancak bir testin ilk saatlerinde hızlı sonuçlar almak ve "düşük asılı meyveleri" toplamak için findmyhash paha biçilmezdir.

Her zaman olduğu gibi, bu aracı **yalnızca yasal olarak test etme izniniz olan sistemlerde** ve etik kurallar çerçevesinde kullanmak, bir profesyonelin en temel sorumluluğudur.