HASH NEDİR? NE İŞE YARAR?

Merhaba arkadaşlar

Bugünkü yazımda size hash konusundan bahsetmek istiyorum. Hash nedir biliyor musunuz? Bu konuda fikiriniz var mı? Bu konudaki fikirlerinizi yorum olarak yazarsanız çok mutlu olurum. 🙂

> ***A cryptographic hash function (CHF) is a mathematical algorithm that maps data of an arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest")***
>
> ***https://en.wikipedia.org/wiki/Cryptographic_hash_function***

Hash Fonksiyonu Nedir?

Hash, fonksiyonu, genellikle mesaj olarak adlandırılan rastgele bir boyuttaki bir veriyi, sabit uzunlukta eşsiz bir değer oluşturan matematiksel bir algoritmadır. Kriptoloji tekniği de diyebiliriz.

Peki bu fonksiyon bizim ne işimize yarayacak!

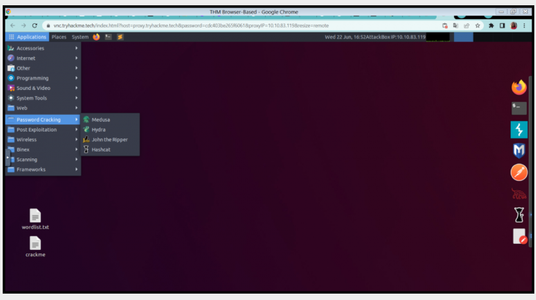
Herhangi bir siteye üye olduğumuzda bizim üye olarak girdiğimiz parolalar, şifreleme teknikleri ile ilgili veritabanlarına şifre olarak kaydedilirler(Parola ve şifreyi doğru söylediim değil mi :D). Sonuç itibari ile bizim kolay olarak aklımızda kalması için kullandığımız 123456 ya da illoveyou gibi parolalar saniyeler içinde kırılır. Yani, bizim yetkimiz dışında birileri bizim adımıza işlem yapabilir, sosyal medya hesaplarımızı ele geçirebilir, hatta banka hesaplarımızı boşaltabilir. Bu kelimeleri milyonlarca kez duymuş olabilirsiniz. Sunu belirtmeliyim ki insan kendi başına gelmediği sürece uzaktan olup biteni izlediğinde film gibi seyredebilir. Ben lafı fazla uzatmadan hash konusuna dönmek istiyorum. 🙂

Bu anlatacaklarım sadece eğitim amaçlıdır. Kötü amaçlı kullanımlardan sorumlu değilim.

Hash Kırma Araçları ?

Hash algoritmalarını kırmak için Kali Linux'ta hashcat, John gibi araçlar mevcut. Tabi ki hash algoritmasını kırmak için hangi algoritma ile şifrelendiğini bilmek ya da onu bulmak ve ya kaba kuvvet saldırısı (bruto force) ile onu çözmek gerekir. Bu konu çok derin olmakla birlikte bilinen hash algoritmaları olarak Md5 , Sha algoritmalarını örnek verebilirim. (Not: Bana xxx hash kodunu kır şeklinde mesaj atacaksanız lütfen mesaj atmayın. Ben sadece hashcat aracı hakkında bilgi vereceğim.)

> ***Hashcat aracını kullanmak için***
> ***https://hashcat.net sitesini ziyaret ederek detaylı bilgiye sahibi olabilirsiniz.***
>
> ***Windows veya Linux versiyonunu kullanabilirsiniz.***
>
> ***Ben Linux versiyonunu kullanacağım.***

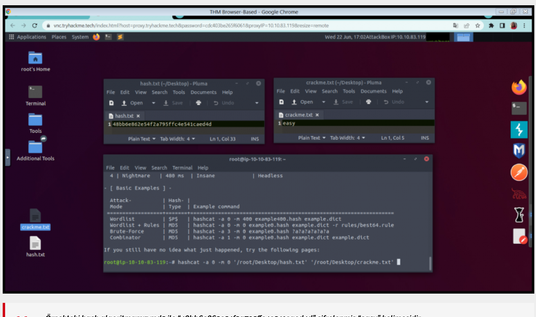


Kali Linux işletim sisteminde hashcat aracını kullanmak için

- 1.Yol - Kali başlat menüsünden Password Attacks/hashcat yolunu izleriz.
- 2. Yol - Terminal ekranından sudo apt-get install hashcat kodunu çalıştırırız.

Hashcat aracını çalıştırdım ve hash kodunu ve istenilen gizli parolayı ayrı dosyalara ekledim. Şimdi onu bulmaya çalışacağım. Umarım çok zor bir parola seçmemişimdir. 🙂

> ***hashcat –help kodunu çalıştırarak hashcat ile ilgili gerekli tüm parametreleri görebiliriz.***



> ***Örnektehi hash algoritmamız md5 ile "48bb6e862e54f2a795ffc4e541caed4d" şifrelenmiş "easy" helimesidir.***
>
> ***Terminal ekranına aşağıdahi hodu yazarız.***
>
> ***hashcat -a 0 -m 0 /home/hali/Desktop/hash.txt /home/hali/Desktop/crackme.txt***
>
> ***Buradahi parametlerin açıklamalarını –help homutu ile öğrenebilirsiniz. En sondahi "0" parametresi md5 olduğu için eklenmiştir. Bunu nasıl anladığımı sorarsanız ben tryhachme.com sitesindehi ipucundan faydalandım ancak***
>
> ***https://hashcat.net/wiki/doku.php?id=example_hashes***
>
> ***adresinden algoritmaları inceleyebilirsiniz.***
>
> ***Buraya kadar okuduğunuz için teşekkür ederim. Yorumlarınızı, eklemem ya da düzeltmem gereken noktalar var ise lütfen belirtin.***
>
> ***Saygılar ve sevgiler*** 🙂

YENİ YAZILAR

GENEL SİBERGÜVENLİK
Hash Nedir? Ne İşe Yarar? Nasıl Kullanılır?
HAZ 22, 2022 HALTUNER

GENEL SİBERGÜVENLİK
TRYHACKME SİTESİNDE OPENVPN
HAZ 19, 2022 HALTUNER

GENEL SİBERGÜVENLİK
SOC -Siber Güvenlik Analisti Kimdir? Ne iş Yapar?
ŞUB 11, 2022 HALTUNER

GENEL SİBERGÜVENLİK YAZILIM
Siber Güvenlik Tehdit Aktörleri ve Tehlikeler
OCA 27, 2022 HALTUNER

ARA

Search