Hash nedir?

Hash belirli bir algoritmayla şifreleme türüdür. Parolalar ve gizli veriler tek yönlü algoritma ile şifrelenerek veri tabanında tutulur. SHA-1, SHA-256, MD2, MD5 gibi türleri vardır. Saldırganlar veri tabanına erişseler bile şifrelenmiş hash değerlerini gördükleri için doğrudan şifreleri göremezler.

Hash nasıl kırılır?

Hash kırmak için kali linuxdan araçlar mevcuttur bu araçlar makine çözümlerinde de sıkça kullanılır. Bunlardan birisi john the ripperdır. Kullanımı kolay ve hash değerlerini kolaylıkla kırabilir. Bir diğer hash kırma aracı ise hashcat'tir. Hashcat ekran kartını kullandığı için daha hızlı hash kırar.

Nasıl korunulur?

Şifre kırma saldırılarından korunmak için en önemli husus zaman ve hızdır. Uzun ve kırılması zor şifreler oluşturulması gerekiyor. Modern ve popüler şifreleme yöntemlerini kullanmak şifrelerin bulunma sürecini uzatacaktır.

Nasıl çalışır?

Hash kırma aracı ile belirttiğimiz hash parametreye göre kırılır ve görüntülenir.

Sonuçları:

Hash kırma saldırısı için john the ripper kullandım. Md5 formatında şifrelerin hashini oluşturdum ardından bunları bir txt dosyasına kaydettim. John the ripper aracım ile hash türünü ve dosyayı belirttim ardından Show parametresi ile kırılan hashlerin karşılığı görüntüledim.