Lab — Güçlü Parolalar Oluşturun ve Saklayın

Hedefler

Güçlü bir parolanın arkasındaki kavramları anlayın.

Bölüm 1: Güçlü bir parola oluşturmanın ardındaki kavramları keşfedin.

Bölüm 2: Parolalarınızı güvenli bir şekilde saklamanın ardındaki kavramları keşfedin.

Arka Plan / Senaryo

Parolalar kaynaklara erişimi zorlamak için yaygın olarak kullanılır. Saldırganlar, kullanıcıların parolalarını öğrenmek ve bir kaynağa veya verilere yetkisiz erişim elde etmek için birçok teknik kullanır.

Kendinizi daha iyi korumak için, güçlü bir parolanın ne olduğunu ve güvenli bir şekilde nasıl saklanacağını anlamak önemlidir.

Gerekli Kaynaklar

- İnternet erişimi olan PC

Bölüm 1: Güçlü Parola Oluşturma

Güçlü parolaların önem sırasına göre listelenen dört ana gereksinimleri vardır:

1) Kullanıcı parolayı kolayca hatırlayabilir.
2) Başka bir kişinin bir parolayı tahmin etmesi önemsiz değildir.
3) Bir programın bir parolayı tahmin etmesi veya keşfetmesi önemsiz değildir.
4) Karmaşık olmalı, sayılar, semboller ve büyük harf ve küçük harflerin bir karışımını içermelidir.

Yukarıdaki listeye dayanarak, ilk gereksinim muhtemelen en önemlisidir, çünkü şifrenizi hatırlamanız gerekir. Örneğin, şifre **#4ssFrX ^-aartPOknx25_70! xAdk<d!** güçlü bir şifre olarak kabul edilir, çünkü son üç gereksinimi karşılar, ancak hatırlamak çok zordur**.**

Birçok kuruluş, sayılar, semboller ve küçük ve büyük harflerin birleşimini içerecek parolalara ihtiyaç duyar. Bu ilkeye uygun parolalar, kullanıcının hatırlaması kolay olduğu sürece sorun değildir. Aşağıda tipik bir kuruluş için ayarlanmış örnek bir parola ilkesi verilmiştir:

- Parola en az 8 karakter uzunluğunda olmalıdır
- Parola büyük ve küçük harfler içermelidir
- Parola bir sayı içermelidir
- Parola alfasayısal olmayan bir karakter içermelidir

Güçlü bir parolanın özelliklerini ve yukarıda gösterilen ortak parola ilkesi setini analiz etmek için biraz zaman ayırın. Politika seti ilk iki maddeyi neden ihmal ediyor? Açıklayın.

_____

_____

_____

_____

_____

_____

Güçlü parolalar oluşturmanın iyi bir yolu, dört veya daha fazla rastgele kelime seçmek ve bunları bir araya getirmektir. Parola **televisionfrogbootschurch J0n@than#81** 'den daha güçlüdür. İkinci parola yukarıda açıklanan politikalara uygun olsa da, parola kırıcı programlarının bu tür parolayı tahmin etmede çok etkili olduğuna dikkat edin. Birçok parola ilkesi setleri ilk parolayı (**televisionfrogbootschurch**) kabul etmeyecek olsa da, ikinciden çok daha güçlüdür. Kullanıcının hatırlaması daha kolaydır (özellikle bir görüntü ile ilişkilidir), çok uzun ve rastgele faktörü, parola kırıcıların tahmin etmesini zorlaştırır.

Çevrimiçi bir parola oluşturma aracını kullanarak, yukarıda açıklanan ortak şirket parola ilkesi kümesine dayalı parolalar oluşturun.

a. Bir web tarayıcısı açın ve http://passwordsgenerator.net adresine gidin.

b. Parola ilke kümesine uygun seçenekleri belirleyin

c. Parola Üret

   Oluşturulan parolanın hatırlanması kolay mı?

   _____

   _____

   Çevrimiçi bir parola oluşturma aracını kullanarak rastgele kelimelere dayalı parolalar oluşturun. Sözcükler birbirine eklendiğinden sözlük sözcükleri olarak görülmediğine dikkat edin.

d. Bir web tarayıcısı açın ve http://preshing.com/20110811/xkcd-password-generator/ adresine gidin.

e. Web sayfasının başında yer alan **Başka Oluştur (Generate Another!)** tıklayarak rastgele bir kelime parolası oluşturun.

f. Oluşturulan parolanın hatırlanması kolay mı?

   _____

   _____

Bölüm 2: Parolaları Güvenli Bir şekilde Saklama

Kullanıcı parola yöneticisi kullanmayı seçerse, kullanıcı her zaman parola yöneticisine erişimi olduğundan ilk güçlü parola karakteristiği bırakılabilir. Bazı kullanıcıların parolalarını hatırlamak için yalnızca kendi belleğine güvendiğine dikkat edin. Yerel veya uzak parola yöneticilerinin bir parola deposuna sahip olması gerekir ve tehlikeye atılabilir.

Parola yöneticisi parola deposu güçlü bir şekilde şifrelenmeli ve erişim sıkıca kontrol edilmelidir. Bulut tabanlı parola yöneticileri cep telefonu uygulamaları ve web arayüzleri sayesinde kullanıcılarına her zaman kesintisiz erişim sağlar.

Popüler bir parola yöneticisi Last Pass.

Bir deneme Lastpass hesabı oluşturun:

a. Bir web tarayıcısı açın ve https://lastpass.com/ adresine gidin.
b. Deneme hesabı oluşturmak için **Start Trial** tıklayın.
c. Talimatlara göre alanları doldurun.
d. Bir ana parola belirleyin. Bu parola LastPass hesabınıza erişmenizi sağlar.
e. İşletim sisteminiz için LastPass'ın istemcisini indirin ve yükleyin.
f. İstemciyi açın ve LastPass ana parolanızla giriş yapın.
g. LastPass parola yöneticisini keşfedin.

Lastpass'e eklediğiniz parolalar nerede saklanır?

_____

Sizin haricinizde, en az bir başka varlık daha parolalarınıza erişebilir. Kim bu varlık?

_____

Tüm parolalarınız aynı yerde saklamanın, dezavantajları vardır. Aklınıza bir şey geliyor mu?

_____

_____

_____

Bölüm 3: Güçlü Parola Nedir?

Bu laboratuvarın başında verilen güçlü parola özelliklerini kullanarak hatırlanması kolay ama tahmin edilmesi zor bir parola seçin. Karmaşık parolalar, kolayca hatırlama yeteneği gibi daha önemli gereksinimleri etkilemediği sürece sorun değildir.

Bir parola yöneticisi kullanılıyorsa, kolayca hatırlanması gerekliliği rahatlatılabilir.

Aşağıda hızlı bir özet verilmiştir:

Hatırlayabileceğiniz bir parola seçin.

Başkasının sizinle ilişki kuramayacağı bir parola seçin.

Farklı parolalar seçin ve farklı hizmetler için asla aynı parolayı kullanmayın.

Karmaşık parolalar, hatırlamak zorlaşmadığı sürece uygundur.