Laboratório – Criar e armazenar palavras-passe fortes

Objetivos

Conheça os conceitos subjacentes a uma palavra-passe forte.

Parte 1: Explorar os conceitos subjacentes à criação de uma palavra-passe forte.

Parte 2: Explorar os conceitos subjacentes ao armazenamento seguro das suas palavras-passe.

Contexto/cenário

As palavras-passe são geralmente utilizadas para controlar o acesso aos recursos. Os atacantes irão utilizar diversas técnicas para descobrir as palavras-passe dos utilizadores e obter acesso não autorizado a um recurso ou a dados.

Para se proteger melhor, é importante compreender em que consiste uma palavra-passe forte e como armazená-la em segurança.

Recursos necessários

- PC ou dispositivo móvel com acesso à Internet

Parte 1: Criar uma palavra-passe forte

As palavras-passe fortes têm quatro requisitos principais, indicados por ordem de importância:

1) O utilizador consegue lembrar-se facilmente da palavra-passe.
2) Uma palavra-passe não é trivial ao ponto de ser adivinhada por outra pessoa.
3) Uma palavra-passe não é trivial ao ponto de ser adivinhada ou descoberta por um programa.
4) Tem de ser complexa, conter números, símbolos e uma mistura de letras maiúsculas e minúsculas.

Com base na lista anterior, o primeiro requisito é provavelmente o mais importante, porque é necessário que consiga lembrar-se da sua palavra-passe. Por exemplo, a palavra-passe **#4ssFrX^-aartPOknx25_70!xAdk<d!** é considerada uma palavra-passe forte porque cumpre os três últimos requisitos, mas é muito difícil de memorizar.

Muitas organizações requerem que as palavras-passe contenham uma combinação de números, símbolos e letras maiúsculas e minúsculas. As palavras-passe que estejam em conformidade com essa política são aceitáveis, desde que sejam fáceis de lembrar pelo utilizador. Segue-se um exemplo de conjunto de políticas de palavras-passe para uma organização típica:

- A palavra-passe tem de ter, pelo menos, 8 carateres
- A palavra-passe tem de conter letras maiúsculas e minúsculas
- A palavra-passe tem de conter um número
- A palavra-passe tem de conter um caráter alfanumérico

Reserve um momento para analisar as características de uma palavra-passe forte e o conjunto de políticas comuns de palavras-passe acima indicado. Por que razão o conjunto de políticas ignora os dois primeiros itens? Explique.

Uma boa forma de criar palavras-passe fortes consiste em escolher quatro ou mais palavras aleatórias e encadeá-las. A palavra passe **televisorsapobotasigreja** é mais forte do que **J0@quim#81**. Tenha em atenção que, embora a segunda palavra-passe esteja em conformidade com as políticas descritas acima, os programas de decifragem de palavras-passe são muito eficientes para adivinhar palavras-passe desse tipo. Embora muitos conjuntos de políticas de palavras-passe não aceitem a primeira, a palavra-passe **televisorsapobotasigreja**, é muito mais forte do que a segunda. É mais fácil de memorizar para o utilizador (especialmente se for associada a uma imagem), é muito longa e o fator de aleatoriedade torna-a difícil de adivinhar pelos programas de decifragem de palavras-passe.

Utilizando uma ferramenta de criação de palavras-passe online, crie palavras-passe com base no conjunto de políticas de palavras-passe da empresa comum descrito acima.

a. Abra um browser e aceda a http://passwordsgenerator.net

b. Selecione as opções que estejam em conformidade com o conjunto de políticas de palavra-passe.

c. Crie a palavra-passe.

   A palavra-passe criada é fácil de memorizar?

   Utilizando uma ferramenta de criação de palavras-passe online, crie palavras-passe com base em palavras aleatórias. Tenha em atenção que, na medida em que as palavras estão concatenadas, não são consideradas palavras de dicionário.

d. Abra um browser e aceda a http://preshing.com/20110811/xkcd-password-generator/

e. Crie uma palavra-passe com palavras aleatórias clicando em **Generate Another!** (Gerar outra) na parte superior da página Web.

f. A palavra-passe criada é fácil de memorizar?

Parte 2: Armazenamento seguro de palavras-passe

Se o utilizador optar por utilizar um gestor de palavras-passe, a primeira característica de uma palavra-passe segura pode ser ignorada porque o utilizador tem acesso permanente ao gestor de palavras-passe. Tenha em atenção que alguns utilizadores confiam exclusivamente na memória para se lembrarem das suas palavras-passe. Os gestores de palavras-passe, tanto locais como remotos, têm de ter um armazenamento de palavras-passe e este pode ficar comprometido.

O armazenamento de palavras-passe do gestor de palavras-passe tem de ter uma encriptação forte e o acesso ao mesmo tem de ser estritamente controlado. Com aplicações para telemóvel e interfaces Web, os gestores de palavras-passe baseados na cloud fornecem acesso permanente e ininterrupto aos utilizadores.

Um gestor de palavras-passe popular é o LastPass.

Crie uma conta experimental no LastPass:

a. Abra um browser e aceda a https://lastpass.com/

b. Clique em **Start Trial** (Iniciar versão experimental) e crie uma conta experimental.

c. Preencha os campos, conforme indicado.

d. Defina uma palavra-passe principal. Esta palavra-passe dá-lhe acesso à sua conta LastPass.

e. Transfira e instale o cliente do LastPass para o seu sistema operativo.

f. Abra o cliente e inicie sessão com a sua palavra-passe principal do LastPass.

g. Explore o gestor de palavras-passe LastPass.

À medida que adiciona palavras-passe ao Lastpass, onde é que são armazenadas?

Além de si, pelo menos uma outra entidade tem acesso às suas palavras-passe. Quem é essa entidade?

Embora possa ser conveniente ter todas as palavras-passe armazenadas no mesmo local, existem desvantagens. Lembra-se de alguma?

Parte 3: Então, o que é uma palavra-passe forte?

Baseando-se nas características de palavras-passe fortes indicadas no início deste laboratório, escolha uma palavra-passe que seja fácil de memorizar, mas difícil de adivinhar. A utilização de palavras-passe complexas é aceitável, desde que tal não entre em conflito com requisitos mais importantes como, por exemplo, a facilidade em recordá-las.

Se for utilizado um gestor de palavras-passe, a necessidade de ser facilmente memorizada pode ser reduzida.

Segue-se um breve resumo:

Escolha uma palavra-passe que consiga memorizar.

Escolha uma palavra-passe que ninguém consiga associar a si.

Escolha palavras-passe diferentes e nunca utilize a mesma palavra-passe para serviços diferentes.

Palavras-passe complexas são aceitáveis, desde que não se tornem mais difíceis de memorizar.