Laboratório – Criar e armazenar senhas fortes (arquivo modificado)

Nome: IGOR EIKI FERREIRA KUBOTA RA: 19.02466-5

Nome: BRUNO BORGIANI TACLA RA: 19.01821-5

Nome: LUCAS REIS AZEVEDO RA: 19.02659-5

Objetivos

**Saiba o que compõe uma senha forte.**

Parte 1: Conheça o que compõe uma senha forte.

Parte 2: Saiba como armazenar suas senhas com segurança.

1. Histórico/Cenário

Senhas são muito utilizadas para dar acesso aos recursos. Os invasores usarão muitas técnicas para descobrir as senhas dos usuários e obter acesso não autorizado a um recurso ou aos dados.

Para melhor proteger-se, é importante entender o que torna uma senha forte e como armazená-lo de forma segura.

1. Recursos necessários

* Computador ou dispositivo móvel com acesso à Internet

1. Como criar uma senha forte

Há quatro requisitos principais para criar uma senha forte, listados em ordem de importância:

* + - 1. O usuário consegue lembrar a senha com facilidade.
      2. Não é fácil para ninguém adivinhar uma senha.
      3. Não é fácil para um programa adivinhar ou descobrir uma senha.
      4. Deve ser complexo, contendo números, símbolos e uma combinação de letras maiúsculas e minúsculas.

Levando em consideração a lista acima, a primeira exigência é provavelmente a mais importante, porque você precisa ser capaz de se lembrar de sua senha. Por exemplo, a senha **#4ssFrX^-aartPOknx25\_70!xAdk<d!** é considerada uma senha forte porque satisfaz as três últimas exigências, mas é muito difícil de lembrar.

Muitas empresas exigem senhas que contenham uma combinação de números, símbolos e letras maiúsculas e minúsculas. Não há problemas com senhas que estejam de acordo com essas condições, desde que sejam fáceis para o usuário lembrar. Veja abaixo uma amostra de condições de senha criadas para uma empresa típica:

* A senha deve ter pelo menos 8 caracteres
* A senha deve ter letras maiúsculas e minúsculas
* A senha não pode ter números
* A senha deve ter um caractere não-alfanumérico

Analise as características de uma senha forte e as condições de criação de senha comum demonstrada acima. Na sua opinião, quais as melhores formas de se gerar senhas fortes e seguras? Explique.

***Uma senha forte e segura deve ter diversos caracteres, podendo diferenciá-los em números, caracteres especiais, letras maiúsculas e minúsculas, além de não conter informações pessoais ou sequencias conhecidas. Dessa maneira, a dificuldade de quebrar a senha aumenta exponencialmente.***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Uma boa maneira de criar senhas fortes é escolher quatro ou mais palavras aleatórias e reuni-las. A senha **televisaosapobotasigreja** é mais forte que **J0n@than#81**. Observe que, embora a segunda senha esteja em conformidade com as condições descritas acima, programas de cracker de senha são muito eficientes ao adivinhar esse tipo de senha. Embora muitas condições de criação de senha não aceitem a primeira senha, **televisaosapobotasigreja**, é muito mais forte do que a segunda. É mais fácil para o usuário lembrar (especialmente se estiver associado a uma imagem), é muito longa e seu fator aleatório torna difícil por crackers adivinharem a senha.

Usando uma ferramenta de criação de senha online, crie senhas com base no conjunto comum de políticas de senha da empresa descrito acima.

* + 1. Abra um navegador da Web e acesse <https://howsecureismypassword.net/>
    2. Digite algumas senhas que utiliza normalmente. Você as considera seguras? Justifique.

***Não, as senhas que são normalmente utilizadas não são seguras porque são reutilizadas e normalmente são palavras de alguma importância para nós.***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Abra um navegador da Web e acesse <http://passwordsgenerator.net>
    2. Selecione as opções de acordo com as condições de criação de senha estabelecidas
    3. Gere a senha.

A senha gerada é fácil de lembrar?

***A senha gerada não é fácil de lembrar, embora o site sugira uma opção de leitura da senha para ajudar no processo de memoriza-la.***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Usando uma ferramenta de criação de senha on-line, crie senhas usando palavras aleatórias. Observe que as palavras não são vistas como palavras dicionarizadas, visto que estão aglutinadas.

* + 1. Abra um navegador da Web e acesse <http://preshing.com/20110811/xkcd-password-generator/>
    2. Gere uma senha usando palavras aleatórias clicando em **Generate Another!** (Gerar Outra!) na parte superior da página da Web.
    3. A senha gerada é fácil de lembrar?

***A senha é relativamente fácil de lembrar, por ser formada por palavras comuns ao nosso vocabulário.***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Armazenamento seguro de senhas

Se o usuário optar por usar um gerenciador de senhas, a primeira característica de uma senha forte pode ser descartada porque o usuário tem acesso ao gerenciador de senha a qualquer momento. Observe que alguns usuários só confiam em suas memórias para guardar suas senhas. Gerenciadores de senha, locais ou remotos, precisam ter um armazenamento de senhas e podem ser comprometidos.

O armazenamento de senha do gerenciador de senha deve ser fortemente criptografado e o acesso a ele deve ser rigidamente controlado. Com aplicativos e interfaces da Web para celulares, os gerenciadores de senha em nuvem dão acesso integral e ininterrupto a seus usuários.

Gerenciadores de senhas:

<https://www.lastpass.com>

<https://www.dashlane.com>

* + 1. Quando você adiciona senhas nos gerenciadores de senhas, onde as senhas são armazenadas?

***As senhas armazenadas pelos gerenciadores (como o Dashlane) armazenam as senhas no próprio dispositivo do usuário, em uma espécie de cofre que necessita de uma chave-mestra para abrir.***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Embora possa parecer uma boa ideia ter todas as senhas armazenadas no mesmo lugar, há inconvenientes. Você consegue pensar em algum?

***Se alguém tem acesso à sua chave-mestra, esse individuo tem acesso à todas suas senhas. Além de que a utilização de diversos aparelhos pode complicar o acesso por vários motivos. Sites e redes sociais podem não ter suporte ao gerenciador de senhas etc.***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Então, o que é uma senha forte?

Usando as características de senha forte apresentadas no início deste laboratório, escolha uma senha que seja fácil de lembrar, mas difícil de ser descoberta. Senhas complexas são ótimas, desde que isso não afete as exigências mais importantes, como a capacidade de lembrar facilmente dela.

Se você usar um gerenciador de senhas, não precisará se preocupar em lembrar das senhas.

Veja abaixo um resumo rápido:

Escolha uma senha da qual você possa se lembrar.

Escolha uma senha que outra pessoa não conseguirá associar a você.

Escolha senhas diferentes e nunca use a mesma senha para diferentes serviços.

Senhas complexas são ótimas, desde que elas não sejam mais difíceis de lembrar.