Laboratório - Como explorar o mundo dos profissionais de segurança digital

Objetivos

Pesquise as funcionalidades de segurança usadas por empresas como a Google e a Cisco para proteger os dados.

Parte 1: Como proteger os dados

Parte 2: Como melhorar a segurança da conta da Google

Histórico/Cenário

Este capítulo apresenta o aluno ao mundo virtual. Esse mundo virtual é cheio de reinos de dados que operam quantidades inimagináveis de informações pessoais e organizacionais. Como um profissional de segurança digital, é importante entender os tipos de defesas da segurança digital que uma empresa deve implementar para preservar os dados que armazenam, gerenciam e protegem. Nesse laboratório, você explorará uma das maiores empresas de gerenciamento de dados do mundo, a Google. Você assistirá a dois vídeos e depois responderá uma série de perguntas. Cada vídeo apresenta um aspecto diferente da defesa da segurança usada na Google. Ao concluir, você terá um melhor entendimento das medidas e serviços de segurança que as empresas como a Google utilizam para proteger as informações e sistemas de informação.

Vídeos:

Como a Google protege os dados

Chave de segurança

Recursos necessários

- Computador ou dispositivo móvel com acesso à Internet

Parte 1: Como proteger os dados

Como um dos maiores repositórios de dados pessoais do mundo, a Google armazena enormes quantidades de dados. A Google é responsável por aproximadamente 50% de toda a atividade de busca na Internet. Para complicar ainda mais a situação, a Google detém e opera o YouTube, o sistema operacional Android e muitas outras fontes importantes de coleta de dados. Nesta atividade, você assistirá a um vídeo rápido e tentará identificar várias das medidas que os profissionais de segurança digital da Google utilizam para proteger os dados.

Passo 1: Abra o navegador e assista ao seguinte vídeo:

Como a Google protege os dados

a. Como a Google assegura que os servidores instalados nos data centers não são infectados por malware pelos fabricantes dos equipamentos?

b. Como a Google protege contra o acesso físico aos servidores localizados nos data centers da Google?

c. Como a Google protege os dados dos clientes em um sistema de servidor?

Passo 2: Identifique as vulnerabilidades dos dados.

a. Como é possível observar pelo vídeo, os dados nos data centers da Google são protegidos adequadamente, contudo, ao usar a Google, nem todos os dados estão localizados nos data centers da Google. Onde mais você pode encontrar seus dados ao usar o mecanismo de busca da Google?

b. É possível tomar providências para proteger os dados ao usar o mecanismo de busca da Google? Quais são as providências que você pode tomar para proteger seus dados?

Parte 2: Como melhorar a segurança da conta da Google

A maior ameaça do uso de serviços da Web, como a Google, é proteger as informações da conta pessoal (nome de usuário e senha). Para piorar a situação, essas contas normalmente são compartilhadas e usadas para autenticar você em outros serviços da Web, como o Facebook, Amazon ou LinkedIn. Existem diversas opções para melhorar o manuseio das credenciais de login da Google. Essas medidas incluem a criação de uma verificação de dois passos ou um código de acesso com um nome de usuário e senha. A Google também estimula o uso de chaves de segurança. Nesta atividade, você assistirá a um vídeo rápido e tentará identificar as medidas que podem ser utilizadas para proteger as credenciais, ao usar as contas da Web.

Passo 1: Abra o navegador e assista ao seguinte vídeo:

O segredo para trabalhar com mais inteligência, rapidez e segurança

a. O que é verificação de dois passos? Como essa verificação pode proteger a conta da Google?

b. O que é uma chave de segurança e qual é sua função? É possível usar a chave de segurança em vários sistemas?

c. Clique aqui para ver as perguntas comuns sobre a chave de segurança. Se você configurar sua conta para usar uma chave de segurança, ainda é possível entrar na conta sem ter uma chave física?

Passo 2: Proteja o acesso à conta de Gmail.

a. O uso de uma conta de Gmail se tornou extremamente popular. Atualmente a Google possui mais de 1 bilhão de contas de Gmail ativas. Uma das funcionalidades práticas das contas de Gmail é a capacidade de conceder acesso a outros usuários. Essa funcionalidade de acesso de compartilhamento cria uma conta de e-mail compartilhada. Hackers podem usar essa funcionalidade para acessar sua conta de Gmail. Para verificar sua conta, entre na conta de Gmail e clique no ícone de engrenagem no canto

superior direito (configurações). Ao abrir a tela de configurações, uma barra de menu será exibida na tela Settings (Configurações). (General (Geral) – Labels (Rótulos) – Inbox (Caixa de Entrada) – Accounts and Import (Contas e Importação) – Filters and Blocked Addresses (Filtros e Endereços Bloqueados)…)

b. Clique no item de menu **Accounts and Import (Contas e Importação)**. Marque a opção **Grant access to your account (Conceder acesso à conta)**. Exclua os usuários compartilhados não autorizados da conta.

Passo 3: Verifique a atividade de sua conta de Gmail.

a. Os usuários de Gmail também podem verificar a atividade da conta, para se certificar de que outros usuários não acessaram sua conta pessoal de Gmail. Essa funcionalidade pode identificar quem acessou a conta e de que localidade. Use a opção **Last account activity (Última atividade da conta)** para determinar se mais alguém acessou sua conta. Para acessar a **Last account activity (Última atividade da conta)** siga esses passos:

   1) Entre na conta de Gmail.

   2) Selecione a opção **Last account activity (Última atividade da conta):** encontrada na parte inferior da página. Essa opção exibirá a última vez que um usuário não autorizado acessou a conta e de onde.

   3) Há um hyperlink de detalhes logo abaixo dessa mensagem. Clique no hyperlink de detalhes.

b. Visualize a atividade da conta. Se encontrar um usuário não autorizado, você pode desconectá-lo clicando no botão na parte superior esquerda **Sign out all other web sessions (Finalizar todas as outras sessões da Web)**. Agora mude a senha para impedir que o usuário não autorizado acesse a conta.

