Lab - Engenharia social

# Objetivos

Pesquise e identifique ataques de engenharia social

# Histórico/Cenário

A engenharia social é um ataque com o objetivo de fazer a vítima inserir informações pessoais ou confidenciais. Esse tipo de ataque pode ser executado por um invasor utilizando um keylogger, e-mail de phishing ou um método pessoal. Este laboratório requer a pesquisa de engenharia social e a identificação de formas de reconhecê-la e preveni-la.

# Recursos necessários

* PC ou dispositivo móvel com acesso à internet

# Instruções

Usando um navegador da web, encontre o artigo “Métodos para entender e reduzir ataques de engenharia social” no site do SANS Institute. Um motor de busca deve encontrar facilmente o artigo.

O SANS Institute é uma organização cooperativa de pesquisa e educação que oferece treinamento em segurança da informação e certificação de segurança. O SANS Reading Room possui muitos artigos relevantes para a prática da análise de segurança cibernética. Você pode ingressar na comunidade SANS criando uma conta de usuário gratuita para acessar os artigos mais recentes ou pode acessar os artigos mais antigos sem uma conta de usuário.

Leia o artigo ou escolha outro artigo sobre engenharia social, leia-o e responda às seguintes perguntas:

#### Perguntas:

* + - 1. Quais são os três métodos usados em engenharia social para obter acesso às informações?

Digite suas respostas aqui.

* + - 1. Quais são os três exemplos de ataques de engenharia social dos dois primeiros métodos na etapa 2a?

Digite suas respostas aqui.

* + - 1. Por que as redes sociais são uma ameaça à engenharia social?

Digite suas respostas aqui.

* + - 1. Como uma organização pode se defender de ataques de engenharia social?

Digite suas respostas aqui.

* + - 1. O que é o SANS Institute, autor deste artigo?

Digite suas respostas aqui.

Fim do documento