Laboratório - Explorar Técnicas de Engenharia

# Objetivos

Parte 1: Explorar Técnicas de Engenharia Social

Parte 2: Crie um pôster de conscientização de segurança digital

# Apresentação

A segurança digital é essencial porque envolve a proteção do acesso não autorizado a dados confidenciais, informações pessoalmente identificáveis (PII), informações de saúde protegidas (PHI), informações pessoais, propriedade intelectual (IP) e sistemas confidenciais. Engenharia social – manipulação do indivíduo para executar ações ou divulgar informações confidenciais Neste laboratório, você vai explorar técnicas de engenharia social, às vezes chamadas de hacking humano, que é uma categoria ampla para diferentes tipos de ataques.

# Recursos necessários

PC ou dispositivo móvel com acesso à internet

# Histórico/Cenário

Uma pesquisa recente revela que os tipos mais comuns de ataques cibernéticos estão se tornando mais sofisticados e os alvos de ataque estão crescendo. O objetivo de um ataque é roubar informações, desativar sistemas ou serviços essenciais, interromper sistemas, atividades e operações. Alguns ataques são projetados para destruir informações ou sistemas de informação, controlar mal-intencionado um ambiente de computação ou sua infraestrutura ou destruir a integridade de dados e / ou sistemas de informação. Uma das maneiras mais eficazes de um invasor obter acesso à rede de uma empresa é enganar-se com simplicidade. No mundo da segurança digital, isso é chamado de engenharia social.

****Ataques de engenharia social****

Ataques de engenharia social são muito eficazes porque as pessoas querem confiar em outras pessoas e ataques de engenharia social não são o tipo de ataque contra o qual um usuário comum se protege; os usuários se preocupam com botnets, roubo de identidade ou ransomware. Essas são grandes ameaças externas, então não pensam em questionar o que parece ser uma mensagem legítima.

****Iscas****

A isca depende da curiosidade ou da ganância da vítima. O que distingue a isca de outros tipos de engenharia social é a promessa de um item ou bem que os hackers usam para atrair as vítimas. A Baiters pode oferecer downloads gratuitos de músicas ou filmes se os usuários entregarem suas credenciais de login em um determinado site. Os ataques de isca não se restringem a esquemas on-line. Os invasores podem explorar a curiosidade humana com mídia física, como unidades USB.

****Navegação bisbilhoteira****

A tiracolo está literalmente olhando por cima do ombro de alguém para obter informações. A navegação na mão é uma maneira eficaz de obter informações em locais com muita gente, porque é relativamente fácil ficar ao lado de alguém e observar como eles preenchem um formulário ou inserem um número PIN em um caixa eletrônico. A tirolesa também pode ser feita a longa distância com a ajuda de telefones celulares modernos, binóculos ou outros dispositivos para melhorar a visão. Para evitar que surjam, os especialistas recomendam que você proteja a papelada ou o teclado usando o corpo ou a mão. Há até escudos de tela que tornam a navegação no ombro muito mais difícil.

****Pretexting****

Pretexto é usar engano para criar um cenário para convencer as vítimas a divulgar informações que não devem divulgar. O pretexto é frequentemente usado em empresas que retêm dados do cliente, como dados financeiros, números de cartão de crédito, números de contas de serviços públicos e outras informações confidenciais. Os pretextores geralmente solicitam informações de indivíduos em uma empresa ao se passar por um supervisor, funcionário do helpdesk ou cliente, geralmente por telefone, e-mail ou texto.

****Ataques de phishing, spear phishing e baleia****

Nos ataques de phishing, os invasores tentam obter informações ou dados pessoais, como nome de usuário, senha e detalhes do cartão de crédito, disfarçando-se como entidades confiáveis. O phishing é realizado principalmente por e-mail e telefonemas. O spear phishing é a versão mais direcionada do phishing, na qual um invasor escolhe indivíduos ou empresas específicas e depois personaliza o ataque de phishing para as vítimas, a fim de torná-lo menos visível. A caça à baleia ocorre quando o alvo específico é um funcionário de destaque, como um CEO ou CFO.

****Scareware e ransomware****

Os ataques de ransomware envolvem a injeção de malware que criptografa os dados essenciais da vítima.Os criminosos digitais solicitam o pagamento de um resgate para descriptografar os dados. No entanto, mesmo que um resgate seja pago, não há garantia de que os criminosos digitais descriptografem as informações. O ransomware é um dos tipos de ataque cibernético que mais cresce e afetou milhares de organizações financeiras, agências governamentais, instalações de serviços de saúde e até mesmo escolas e nossos sistemas de ensino.

O Scareware se aproveita do medo do usuário ao convencê-lo a instalar um software antivírus falso.

Tailgating

A utilização indevida engana a vítima e ajuda o invasor a obter acesso não autorizado às instalações físicas da empresa. O invasor busca entrar em uma área restrita onde o acesso é controlado por dispositivos eletrônicos de software ou guardas humanos. A utilização não autorizada também pode envolver o invasor seguindo um funcionário de perto para passar por uma porta trancada antes que a porta seja bloqueada atrás do funcionário.

Busca de informações na lixeira

No mundo da engenharia social, o mergulho no lixo é uma técnica usada para recuperar informações descartadas jogadas no lixo para realizar um ataque a uma pessoa ou empresa. O mergulho no lixão não se limita à pesquisa no lixo em busca de tesouros óbvios, como códigos de acesso ou senhas escritos em notas, também pode envolver informações eletrônicas deixadas em desktops ou armazenadas em unidades USB.

# Parte 1: Explore as Técnicas de engenharia social

### Etapa 1: Explore a isca, a navegação no ombro e o pré-texto.

O National Support Center for Systems Security and Information Assurance (CSSIA) hospeda uma atividade interativa de **engenharia social**. O link atual para o site é <https://www.cssia.org/social_engineering/>. No entanto, se o link for alterado, tente pesquisar por "CSSIA Social Engineering Interactive".

Clique em **Avançar** na atividade interativa e use o conteúdo para responder às seguintes perguntas.

O que é isca? Você clicou na unidade USB? O que aconteceu com o sistema da vítima?

Digite suas respostas aqui.

O que é Shoulder Surfing? Qual dispositivo foi usado para realizar o shoulder surfing? Que informações foram obtidas?

Digite suas respostas aqui.

O que é pretexting? Que tipo de informação o criminoso digital solicitou? Você seria vítima?

Digite suas respostas aqui.

### Etapa 2: Explore Phishing, Spear Phishing e Whaling

O phishing foi projetado para fazer com que as vítimas cliquem em links para sites mal-intencionados, abram anexos que contêm malware ou revelam informações confidenciais. Use a atividade interativa para explorar diferentes técnicas de phishing.

Neste exemplo de phishing, qual é o estratagema que o invasor usa para enganar a vítima e acessar o site da armadilha?Para que serve o site de interceptação?

Digite suas respostas aqui.

Qual é a diferença entre phishing e spear phishing ou whaling?

Digite suas respostas aqui.

### Etapa 3: Explore o Scareware e o ransomware

Scareware é quando as vítimas são enganadas e pensam que seu sistema está infectado com malware e recebem alarmes falsos, o que os leva a instalar um software desnecessário ou é um malware em si. O ransomware é um tipo de malware que ameaça publicar os dados da vítima ou criptografa os dados da vítima, impedindo o acesso ou a capacidade de usar os dados. As vítimas são impedidas de acessar seus arquivos pessoais do sistema ou até que façam um pagamento de resgate para recuperar o acesso.

Quais dados o invasor afirma ter neste exemplo? Você cairia nesse engodo?

Digite suas respostas aqui.

O que o invasor está solicitando que a vítima faça para recuperar os dados?

Digite suas respostas aqui.

O que é tailgating (utilização não autorizada)?

Digite suas respostas aqui.

Ofereça três formas de evitar ataques de engenharia social?

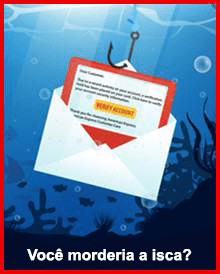
Digite suas respostas aqui.

# Parte 2: Criar um pôster de conscientização de segurança digital

Use o PowerPoint para criar um pôster que conscientize as pessoas sobre as diferentes técnicas de engenharia social usadas para obter acesso não autorizado a uma empresa ou a seus dados.

Selecione: Isca, Navegação por meio do ombro, Pretexting, Phishing, Scareware, Ransomware,Tailgating ou Dumpster Diving.

O pôster deve descrever as técnicas usadas e como os usuários podem evitar um desses ataques de engenharia social. Inclua também instruções sobre onde o pôster deve ser colocado dentro da empresa.



*Fim do documento*