O que é Engenharia Social?

Engenharia social é um termo que é amplamente utilizado, mas mal compreendido. É geralmente definido como qualquer tipo de ataque que não é de natureza técnica e que envolve algum tipo de interação humana com o objetivo de tentar enganar ou coagir uma vítima a revelar informações ou violar as práticas normais de segurança.

Os engenheiros sociais estão interessados ??em obter informações que podem usar para realizar ações como roubo de identidade ou roubo de senhas, ou para encontrar informações para uso posterior. Scams pode tentar fazer uma vítima acreditar que o atacante é do suporte técnico ou alguém com autoridade. Um atacante pode vestir alguma maneira com a intenção de enganar a vítima a pensar que a pessoa tem autoridade. O objetivo final de cada abordagem é a vítima baixar a guarda ou a atacar para obter informações suficientes para coordenar melhor e planejar um ataque posterior.

A categoria de ataque baseia-se nas fraquezas ou forças do ser humano em vez da aplicação de tecnologia. Os seres humanos foram mostrados para ser muito facilmente manipulados em fornecer informações ou outros detalhes que podem ser úteis para um atacante.

Se isso ajuda, você pode pensar nos engenheiros sociais no mesmo contexto que artistas. Normalmente, os indivíduos que se envolvem neste tipo de atividade são muito bons em reconhecer sinais indicadores ou comportamentos que podem ser úteis na extração de informações, como as seguintes:

- **Obrigação Moral** – Um atacante pode se alimentar do desejo da vítima de prestar assistência porque se sente compelido a fazê-lo por um senso de dever.
- **Confiança –** Os seres humanos têm uma tendência inerente

a confiar nos outros. Os engenheiros sociais exploram a tendência de um ser humano confiar usando buzzwords ou outros meios. No caso de buzzwords, por exemplo, o uso de termos familiares pode levar a vítima a acreditar que um atacante tem conhecimentos privilegiados de um projeto ou lugar.

- **Ameaças –** Um engenheiro social pode ameaçar uma vítima se não cumprir um pedido.
- **Algo para Nada –** O atacante pode prometer a uma vítima que, por pouco ou nenhum trabalho, eles vão colher recompensas tremendas.
- **Ignorância –** A realidade é que muitas pessoas não percebem os perigos associados com engenharia social e não reconhecem como uma ameaça.

Por que a engenharia social funciona?

A engenharia social é eficaz por uma série de razões, cada uma das quais pode ser corrigida ou explorada dependendo se você é o defensor ou o atacante. Vamos dar uma olhada em cada um:

- **Falta de um reparo tecnológico –** A tecnologia pode fazer corrigir problemas de segurança, mas, ao mesmo tempo, pode ser uma fonte de fraqueza. Uma coisa que a tecnologia tem pouco ou nenhum impacto sobre é diminuir a eficácia da engenharia social. Isso ocorre principalmente porque a tecnologia pode ser contornada ou incorretamente configurada pelos seres humanos.
- **Políticas de segurança insuficientes –** As políticas que indicam como as informações, os recursos e outros itens relacionados devem ser tratados são muitas vezes incompletas ou insuficientes na melhor das hipóteses.
- **Detecção difícil –** A engenharia social por sua própria natureza pode ser difícil de detectar. Pense nisso: Um ataque contra a tecnologia pode deixar trilhas em um

arquivo de log ou em um sistema de detecção de intrusão (IDS), mas a engenharia social provavelmente não.

- **Falta de treinamento –** A falta de treinamento ou treinamento insuficiente sobre engenharia social e como reconhecê-lo pode ser uma grande fonte de problemas.

O EC-Council gosta de dizer: “Não há patch para a estupidez humana”. Esta declaração soa meio espirituoso, mas faz você entender que, embora você possa corrigir com patch a tecnologia, você não pode corrigir um ser humano para resolver seus problemas.O treinamento é uma forma de corrigir maus comportamentos e conscientização dos problemas e questões antes do tempo.

Um dos exemplos em que a Engenharia Social pode ser usada é coms cavalos de Tróia, que exploram as técnicas de engenharia social para atrair uma vítima a abrir um arquivo executável ou anexo infectado por malware. Um cavalo de Tróia é um pedaço de malware que se baseia principalmente no elemento de engenharia social como um mecanismo para iniciar uma infecção. Usando o aspecto de engenharia social, os escritores de vírus podem fazer uma vítima inocente executar um malware com a promessa de dar-lhes algo que eles esperam ou querem.

Outro exemplo de como funciona a engenharia social é o caso do scareware. Este tipo de malware é projetado para assustar uma vítima em agir quando não é necessário. O melhor exemplo é o caso de falsos produtos antivírus que solicitam aos usuários mensagens muito realistas, mas falsas, que eles devem baixar um “antivírus” para desinfetar seu sistema.

Em ambos os casos, treinamento simples e conscientização podem facilmente parar um ataque antes que ocorra um incidente de segurança. Você deve conhecer os sinais de engenharia social e incluir uma dose de senso comum antes de implementar engenharia social em seus testes. Alguns sinais comuns que podem indicar um ataque de engenharia social incluem, mas não estão limitados a:

- Uso da autoridade por um atacante, como fazer referências explícitas a quem eles são ou quem eles conhecem ou até mesmo fazer ameaças com base em seu poder ou autoridade reivindicada.
- Incapacidade de fornecer informações de contato válidas que permitiriam que o atacante fosse chamado ou contatado conforme necessário.
- Fazer pedidos informais ou off-the-book projetado para incentivar a vítima a dar informações que não podem de outra forma.
- Excesso de nomes de quem conhece dentro da organização.
- Uso excessivo de elogios ou elogios projetados para adular uma vítima
- Desconforto quando questionado

O Poder da Engenharia Social

Por que a engenharia social é uma ferramenta tão poderosa, e por que ela continuará sendo assim? Para responder a isso, você deve primeiro entender por que ele funciona e o que isso significa para você como um pentester. Indo além do ser humano em vez da tecnologia, funciona por uma série de razões:

- **Confiança** – Os seres humanos são um monte de confiança. É construído dentro da espécie. Quando você vê alguém vestido de uma certa maneira (como usar um uniforme) ou ouvi-los dizer as palavras certas, você confia neles mais do que você normalmente faria. Por exemplo, se você ver alguém vestido em um conjunto de esfregões e carregando um estetoscópio, você tende a confiar neles. Esta tendência para confiar é uma fraqueza que pode ser explorada.
- **Hábito Humano e Natureza –** Os seres humanos tendem a seguir certos hábitos e ações padrão sem pensar. As pessoas seguem o mesmo caminho para trabalhar, dizem as mesmas coisas, e tomam as mesmas ações sem pensar. Em muitos casos, as pessoas têm que conscientemente tentar

agir de forma diferente da norma, a fim de quebrar seus hábitos aprendidos. Um bom engenheiro social pode observar esses hábitos e usá-los para rastrear pessoas ou seguir as ações de grupos e ganhar entrada em edifícios ou acesso a informações.

Fases de engenharia social

A engenharia social, como os outros ataques que exploramos neste livro, consiste em múltiplas fases, cada uma projetada para mover o atacante um passo mais perto do objetivo final. Vejamos cada uma dessas fases e como a informação obtida de uma leva ao seguinte:

1. Use footprinting e colete detalhes sobre um alvo através de pesquisa e observação. Fontes de informação podem incluir dumpster diving, phishing, sites, funcionários, passeios da empresa, ou outras interações.
2. Selecione um indivíduo ou grupo específico que possa ter o acesso ou informações que você precisa para se aproximar do alvo desejado. Procure por fontes como pessoas que estão frustradas, excessivamente confiantes ou arrogantes e dispostas a fornecer informações prontamente. Na verdade, a presença deste tipo de pessoa pode assumir a forma de uma ameaça interna.
3. Forjar um relacionamento com a vítima pretendida através de conversas, discussões, e-mails ou outros meios.
4. Explorar a relação com a vítima, e extrair as informações desejadas. Você também pode olhar essas quatro fases como três componentes distintos do processo de engenharia social:
   Pesquisa (etapa 1)
   Desenvolvimento (etapas 2 e 3)
   Exploração (passo 4)

O EC-Council recomenda assistir filmes como *Prenda-me se For Capaz*, *Um Golpe à Italiana* e *Os Vigaristas* como ótimas

maneiras de observar diferentes tipos de Engenharia social em ação. Prenda-me se For Capaz é uma dramatização das façanhas de um engenheiro social da vida real. Se você assistir a esses filmes, preste muita atenção às diferentes técnicas de engenharia social podem ser empregadas, como eles funcionam e por que eles são eficazes.

Qual é o impacto da engenharia social?

A engenharia social pode ter muitos resultados potenciais em uma organização, alguns óbvios e outros menos. É importante que você entenda cada um destes, porque eles podem ter efeitos de longo alcance:

- **Perda econômica –** Este é bastante óbvio. Um engenheiro social pode fazer com que uma empresa ou organização perca dinheiro por engano, perda de produtividade ou roubo de identidade.
- **Terrorismo –** Talvez uma das formas mais visíveis de engenharia social seja o terrorismo. Neste caso, um alvo é coagido em ação através da ameaça de violência física.
- **Perda de Privacidade –** Um atacante usando estas técnicas pode facilmente roubar informações para executar roubo de identidade em qualquer número de vítimas.
- **Ações judiciais e arbitragens –** Dependendo do compromisso, a conclusão bem-sucedida de um ataque pode resultar em ações judiciais ou outras ações contra a vítima ou a organização da vítima.
- **Encerramento Temporário ou Permanente** – Dependendo de quão ruim é a violação, o resultado pode ser catastrófico, com um fechamento de negócios inteiro por causa de perdas financeiras e processos judiciais.
- **Perda da boa vontade –** Embora todas as perdas não podem ser monetárias, eles ainda podem ser devastadores, como a perda de boa vontade de clientes ou clientes.

Se você tiver uma boa memória, você pode se lembrar de alguns dos problemas desta lista de discussões anteriores. Os ataques de engenharia social podem ser tão perigosos quanto – ou mais do que – ataques técnicos. É para o seu benefício para lembrar isso quando você está fazendo seus testes e planejamento, porque muitas vezes o elemento social é negligenciado em favor de se concentrar em tecnologia. Embora seja possível fazer coisas como cracking senhas por um ataque técnico, às vezes você pode obter o que você quer apenas perguntando da forma correto.

Alvos Comuns da Engenharia Social

Um atacante vai procurar por alvos de oportunidade ou vítimas potenciais que têm mais a oferecer. Alguns objetivos comuns incluem recepcionistas, pessoal de help desk, usuários, executivos, administradores de sistemas, fornecedores externos e até mesmo pessoal de manutenção. Vamos olhar para cada um e ver por que isso é.

- **Recepcionistas** – uma das primeiras pessoas que os visitantes vêem em muitas empresas – representam alvos principais. Eles vêem muitas pessoas entrar e sair de um escritório, e eles ouvem um monte de coisas. Além disso, recepcionistas são destinados a ser útil e, portanto, não são focados na segurança. Estabelecer um relacionamento com esses indivíduos pode facilmente produzir informações que são úteis por conta própria ou para ataques futuros.
- **Pessoal de help desk** – Outro alvo tentador e valioso devido à informação que eles podem ter sobre a infra-estrutura, entre outras coisas. O arquivamento de pedidos falsos de suporte ou a pergunta a essas pessoas podem gerar informações valiosas.
- **Os administradores de sistema** também podem ser alvos valiosos de oportunidade, novamente por causa das informações que possuem. O administrador típico pode ser

útil por ter muito alto nível de conhecimento da infra-estrutura e aplicações, bem como planos de desenvolvimento futuro. Além disso, alguns administradores de sistemas possuem conhecimento de longo alcance sobre a rede e infra-estrutura de toda a empresa. Dadas as formas corretas de abordagem e algum esforço, essas metas podem, por vezes, gerar enormes quantidades de informação. Técnicas que eu usei no passado incluem perguntas sobre sua experiência, carreira e tal, e usando isso para aprender mais sobre o que eles fazem atualmente.

- **Os executivos** são outro alvo principal para os atacantes, porque os indivíduos nesses tipos de cargos não estão focados na segurança. Na verdade, muitas das pessoas nessas posições focam em processos de negócios, vendas, finanças e outras áreas.
- **Os usuários** são provavelmente uma das maiores fontes de vazamentos, porque eles são os que manipulam, processam e gerenciam informações dia a dia. Junte isso com o fato de que muitos desses indivíduos podem estar menos preparados para lidar com essas informações de forma segura.

Uma das aplicações que eu acho mais problemática é o uso de contas backdoor. Essas contas são colocadas lá para permitir que um administrador de forma rápida e fácil de login e/ou executar determinadas tarefas sem ter que passar por métodos mais seguros ou permitidos. Essas contas, normalmente, não são monitoradas – ou até mesmo esquecidas quando o proprietário original saiu da organização. Neste último caso, as contas permanecem e não são garantidas; Ninguém sabia que eles existiam, exceto seu criador original, que há muito tempo se mudou. Sabendo que alguns administradores têm essa tendência, um bom engenheiro social pode procurar pistas sobre a existência dessas contas.

Então, por que os administradores de sistemas e similares

colocam backdoors que podem contornar a segurança em um sistema? Bem, em alguns casos, elas foram colocadas lá para fornecer um meio alternativo para entrar no sistema no caso de suas contas primárias não estejam disponíveis. Em outras palavras, elas são colocadas lá no caso de perderem o acesso ou suas contas primárias serem bloqueadas.

Sugestões de livros: