Introdução a Engenharia Social

Engenharia social

- O termo “engenharia social” (em inglês “social engineering”) designa a arte de manipular pessoas a fim de contornar dispositivos de segurança. Trata-se assim de uma técnica que consiste em obter informações por parte dos utilizadores por telefone, por correio eletrônico, por correio tradicional ou contato direto.

Engenharia social

A engenharia social é baseada na utilização da força de persuasão e na exploração da ingenuidade dos utilizadores, fazendo-se passar para uma pessoa da casa, um técnico, um administrador, etc.

Geralmente, os métodos de engenharia social desenrolam-se de acordo com o esquema seguinte:

Engenharia social

Uma fase de abordagem que permite pôr o utilizador à vontade, fazendo-se passar por uma pessoa da sua hierarquia, da empresa, do seu meio ou por um cliente, um fornecedor, etc.

Um alerta, a fim de o desestabilizar e assegurar-se da rapidez da sua reação. Pode tratar-se, por exemplo, de um pretexto de segurança ou de uma situação de emergência;

Uma diversão, quer dizer, uma frase ou uma situação que permite tranquilizar o utilizador e evitar que se focalize no alerta. Pode tratar-se, por exemplo, de um agradecimento que anuncia que tudo voltou à normalidade, no caso de um correio eletrônico ou de um site web, de um redirecionamento para o site web da empresa.

Engenharia social

- A engenharia social pode assumir várias formas:
  - Por telefone,
  - Por correio eletrônico (phishing),
  - Por correio escrito,
  - Pretexting (criação de cenários ou histórias falsas),
  - Por serviço de mensagens instantâneas,
  - Mídias sociais,
  - Força tarefa (intimidação ou pressão da vítima),
  - Ataques de "amizade" ou "relacionamento“,
  - Pessoalmente,
  - Etc.

Engenharia social

- Para se proteger da engenharia social, devemos utilizar o bom senso e evitar compartilhar informações que possam prejudicar a segurança da empresa. Independentemente do tipo de informação solicitada, devemos seguir as seguintes diretrizes:

  - Confirmar a identidade do solicitante, obtendo informações precisas (nome completo, empresa, número de telefone).
  - Verificar as informações fornecidas, se necessário.
  - Perguntar a si mesmo sobre a importância das informações solicitadas.

Engenharia social - Formas de ataque

- Existem várias formas de ataque, todas elas explorando a vulnerabilidade e ingenuidade das pessoas. É imprescindível mencionar Kevin Mitnick (Goodell, 1996) ao discutir ataques de engenharia social, já que, até sua captura, ele era reconhecido como o maior hacker de todos os tempos. Atualmente, há muitos outros como ele, empregando táticas essencialmente semelhantes.

- Antes de explorar as diversas formas de ataque, é importante destacar quem são os intrusos/atacantes. É um equívoco acreditar que todos os ataques são orquestrados exclusivamente por hackers.

Intrusos	**Objetivos**
Estudantes	Bisbilhotar mensagens de correio eletrônico de outras pessoas por diversão;
Hackers/Crackers	Testar sistemas de segurança, ou roubar informações;
Representantes Comerciais	Descobrir planilhas de preços e cadastro de clientes;
Executivos	Descobrir plano estratégico dos concorrentes;
Ex-funcionários	Sabotagem por vingança;
Contadores	Desfalques financeiros;
Corretores de valores	Distorcer informações para lucrar com o valor das ações;
Vigaristas	Roubar informações, como senhas e números de cartões de crédito;
Espiões	Descobrir planos militares;
Terroristas	Espalhar pânico pela rede e roubo de informações estratégicas.

Engenharia social - Formas de ataque

- Os ataques de Engenharia Social podem ter dois aspectos diferentes:
  - Físico, como local de trabalho, por telefone, no lixo ou mesmo on-line.
  - Psicológico, que se refere à maneira como o ataque é executado, tal como persuasão.

Local de Trabalho

- Nomes, lista de ramais, endereços eletrônicos, organogramas e outros dados da empresa, comumente ficam expostos em lugares onde transitam pessoas estranhas.

- Um hacker pode simplesmente entrar na empresa como se fosse um técnico em manutenção ou consultor que tem livre acesso às dependências da empresa e, enquanto caminha pelos corredores, pode ir captando todas estas informações que porventura estejam expostas.

Engenharia Social por Telefone

- Esta modalidade de ataque vai desde roubar informações de funcionários ingênuos até a clonagem ou grampo telefônico. Um hacker chega na empresa passando-se por um técnico que fará manutenção da central telefônica e, em seguida, desvia uma linha de onde pode efetuar ligações para qualquer parte do mundo, ou então pode grampear os telefones de algum executivo.

- Outro alvo importante, também são os call centers. Os atendentes têm por obrigação atender a todos da melhor maneira possível, solucionando todas as dúvidas possíveis. Então entra em cena o talento do hacker que poderá, com isso, conseguir dicas de utilização dos sistemas e até senhas de acesso

Lixo

- O lixo das empresas pode ser uma fonte muito rica de informações para um hacker. Vasculhar o lixo, é um método muito usado pelos invasores, porque é comum encontrarmos itens como cadernetas com telefones, organograma da empresa, manuais de sistemas utilizados, memorandos, relatórios com informações estratégicas, apólices de seguro e até anotações com login e senha de usuários.

- As listas telefônicas podem fornecer os nomes e números das pessoas-alvo, o organograma mostra quem são as pessoas que estão no comando, as apólices mostram o quanto a empresa é segura ou insegura, os manuais dos sistemas ensinam como acessar as informações e assim todo e qualquer lixo poderá ser de grande valia para uma pessoa mal intencionada.

Desafio das Senhas

- As senhas são os principais pontos fracos das empresas. É comum as pessoas dividirem senhas com outras ou escolherem senhas fracas, sem a menor preocupação. Muitos usam como senha, palavras que existem em todos os dicionários, seus apelidos, ou até mesmo o próprio nome que, com um software gerenciador de senhas, é possível decifrá-las em segundos.

- Segundo Kevin Mitnick (2001), elas chegam a representar 70% do total de senhas utilizadas nas empresas.

Engenharia Social On-line

- Talvez a maneira mais fácil de se conseguir um acesso é através da internet.
- A displicência dos usuários que criam senhas fáceis de serem descobertas, que ficam longos períodos sem alterá-las, e ainda utilizam a mesma senha para acesso a várias contas, torna o ataque mais simples.
- Basta enviar um cadastro oferecendo um brinde ou a participação em um sorteio que solicite o nome e senha do usuário e pronto. O hacker terá a sua disposição tudo o que é necessário para um ataque, sem grande esforço.

Engenharia Social On-line

- As salas de bate-papo também são um canal explorado para o roubo de informações. Homens e mulheres se dizem jovens, atraentes e de bom papo. Na verdade podem ser farsantes que manipulam os sentimentos das pessoas em busca de informações.

- Outro meio de se obter informação on-line, é se passar pelo administrador da rede, que, através de um e-mail, solicita aos operadores nome e senha. Porém, este tipo de ataque já não é mais tão eficaz, porque os operadores que trabalham nessas áreas geralmente são pessoas mais experientes e não caem nesse tipo de truque tão facilmente.

Engenharia Social On-line

- Os e-mails (ataque de phishing e suas variantes, spear phishing, whaling, pharming, vishing, smishing e outros) também podem ser usados como meio para conseguir acesso a um sistema.

- Por exemplo, um e-mail enviado para alguém pode conter um vírus de computador ou cavalos de Tróia, que, quando instalados no computador da vítima, podem destruir todas as informações, ou simplesmente ficar ocultos e transmitindo ao invasor todo tipo de informação como, senhas, números de cartão de crédito, ou mesmo abrir o firewall da empresa, deixando-a vulnerável a qualquer tipo de ataque.

Tipos de ataque de Phishing

- **Phishing por E-mail**: Os atacantes enviam e-mails fraudulentos que parecem ser de fontes confiáveis, como bancos, empresas ou serviços online, solicitando informações pessoais, como senhas, números de cartão de crédito ou informações de login.

- **Spear Phishing:** Esse tipo de phishing é direcionado a um indivíduo ou organização específica. Os atacantes personalizam os e-mails com informações relevantes para a vítima, tornando-os mais convincentes.

- **Whaling:** Similar ao spear phishing, mas os alvos são indivíduos de alto escalão, como executivos ou CEOs. Os atacantes buscam obter informações confidenciais ou acesso a contas sensíveis.

- **Pharming:** Os invasores redirecionam o tráfego da web das vítimas para sites fraudulentos, muitas vezes usando ataques de DNS (sistema de nomes de domínio) falsificados, a fim de roubar informações.

- **Vishing (Phishing por Telefone):** Os atacantes usam chamadas telefônicas para se fazer passar por entidades confiáveis, como bancos ou empresas, solicitando informações pessoais ou financeiras por telefone.

- **Smishing (Phishing por SMS):** Atacantes enviam mensagens de texto falsas para dispositivos móveis, frequentemente solicitando ação imediata, como clicar em links ou fornecer informações pessoais.

- **Clone Phishing:** Os atacantes criam cópias falsas de e-mails legítimos já enviados e enviam novamente essas mensagens com links ou anexos maliciosos.

- **Evil Twin Wi-Fi:** Os invasores criam pontos de acesso Wi-Fi falsos que parecem legítimos, levando as vítimas a se conectar a redes não seguras, onde suas informações podem ser roubadas.

- **Cross-Site Scripting (XSS):** Atacantes inserem código malicioso em sites legítimos que, quando visitados por vítimas desavisadas, podem roubar informações de login ou instalar malware.

- **Watering Hole:** Os atacantes identificam sites frequentemente visitados por suas vítimas-alvo e comprometem esses sites com malware, de forma que, quando as vítimas os acessam, seus sistemas são infectados.

- **Rogue Software:** Os atacantes enganam as vítimas para instalar software malicioso, disfarçado como atualizações legítimas ou programas úteis.

- **Pishing por Redes Sociais:** Os invasores criam perfis falsos em redes sociais para se aproximar de suas vítimas, ganhar confiança e obter informações pessoais.

- **Engenharia Social Offline**: Isso envolve a manipulação de pessoas pessoalmente, seja para obter informações ou acesso físico a instalações seguras.

Footprint

- Nem sempre o invasor consegue coletar as informações desejadas através de um telefonema ou uma conversa amigável, seja porque as pessoas não detêm o conhecimento necessário ou por não conseguir alcançar pessoas ingênuas. Então o invasor utiliza uma técnica conhecida como footprint.

- "Footprint" (ou "pegada" em português) no contexto da segurança da informação refere-se ao rastro ou conjunto de informações deixado por uma organização, sistema, usuário ou dispositivo digital na internet ou em qualquer ambiente online. Essas informações podem incluir dados sobre a presença online, histórico de atividades, informações pessoais ou técnicas, e outros detalhes que podem ser usados para identificar ou rastrear entidades online.

Tipos de “pegadas digitais”

- **Pegada de navegação:** Diz respeito às informações deixadas durante a navegação na web, incluindo histórico de sites visitados, cookies e outros dados de rastreamento.

- **Pegada de rede social:** Relaciona-se às informações compartilhadas em redes sociais, como postagens, curtidas, comentários e conexões com outros usuários.

- **Pegada de e-mail:** Refere-se às informações encontradas em e-mails enviados e recebidos, como endereços de e-mail, correspondências e anexos.

- **Pegada de mídia social**: Envolve informações relacionadas à presença de uma pessoa em plataformas de mídia social, incluindo fotos, vídeos e informações de perfil.

- **Pegada digital pessoal:** Consiste em informações pessoais disponíveis online, como números de telefone, endereços, histórico educacional e profissional.

- **Pegada de dados técnicos:** Inclui informações técnicas sobre dispositivos, sistemas operacionais, endereços IP e configurações.

Footprint

- Footprint é um perfil completo da postura de segurança de uma organização (ou de uma pessoa) que se pretende invadir. Usando uma combinação de ferramentas e técnicas, atacantes podem empregar um fator desconhecido e convertê-lo em um conjunto específico de nomes de domínio, blocos de redes e endereços IP individuais de sistemas conectados diretamente na Internet. Embora haja diversas técnicas diferentes de footprint, seu objetivo primário é descobrir informações relacionadas a tecnologias de internet, acesso remoto e extranet.

Engenharia Social - Formas de prevenção

Área de Risco	**Tática do *Hacker***	**Estratégia de Combate**
Suporte de informática	Representação e persuasão;	Desenvolver na empresa uma política de mudança freqüente de senhas e treinar os demais funcionários para nunca passarem senhas ou outras informações confidenciais por telefone;
Entrada de edifícios	Acesso físico não autorizado;	Treinar os funcionários da segurança para não permitirem o acesso de pessoas sem o devido crachá de identificação e mesmo assim fazer uma verificação visual;
Escritórios	Caminhar pelo ambiente;	Não digitar senhas na presença de pessoas estranhas, a menos que você consiga fazê-las rapidamente;
Suporte telefônico	Usar de disfarces na hora de solicitar ajuda aos atendentes, geralmente se passando por outra pessoa;	Os atendentes devem solicitar sempre um código de acesso, para só então prestarem o suporte solicitado;

Escritórios	Caminhar pelos corredores à procura de salas desprotegidas;	Todos os visitantes devem ser acompanhados por um funcionário da empresa;
Sala de correspondência	Inserção de mensagens falsas;	Fechar e monitorar a sala de correspondência;
Sala dos servidores	Instalam programas analisadores de protocolo para conseguirem informações confidenciais, além da remoção de equipamentos;	Manter sala dos servidores sempre trancada, e o inventário de equipamentos atualizado;
Central telefônica	Roubar acesso a linhas telefônicas;	Controlar chamadas para o exterior e para longas distâncias, e recusar pedidos de transferências suspeitas;
Depósito de lixo	Vasculhar o lixo;	Guardar o lixo da empresa em lugar seguro, triturar todo tipo de documento, e destruir todo o tipo de mídia magnética fora de uso;
Internet e *intranet*	Criar e/ou inserir programas na *Internet* ou *intranet* para capturar senhas;	Criar senhas fortes e fazer uso consciente da mesma, alterando-a periodicamente. Os modens nunca devem ter acesso a *intranet* da empresa;
Escritório	Roubar documentos importantes;	Manter os documentos confidenciais fora do alcance de pessoas não autorizadas, de preferência em envelopes fechados.

Vídeos

- **Trechos do filme Takedown (Sobre Kevin Mitnick)**
  - https://www.youtube.com/watch?v=r5w2Vnz4HCM
- **Cine Cyber - Caçada Virtual: Operação Takedown (2000)**
  - https://www.youtube.com/watch?v=CNGqeTiuHjs
- **Engenharia Social - A arte de MANIPULAR pessoas**
  - **https://www.youtube.com/watch?v=dU-vRwBLeQ4**
- **Engenharia social – animação**
  - https://www.youtube.com/watch?v=mebxuiYb77k&t=19s

STUXNET

STUXNET

- O Stuxnet é um dos malware mais notórios e sofisticados já desenvolvidos. Ele foi descoberto em junho de 2010 e é notável por seu alvo específico e complexidade técnica. O Stuxnet foi projetado para atacar sistemas de controle industrial, especificamente os sistemas SCADA (Supervisory Control and Data Acquisition) que controlam instalações industriais, como usinas de energia e usinas nucleares.

- Embora seja notório por sua complexidade técnica e por ser um malware direcionado a sistemas de controle industrial, também envolveu elementos de engenharia social indiretamente.

STUXNET e a Engenharia Social

- **Entrega Inicial:** Engenharia social pode ter sido usada na fase de entrega inicial do Stuxnet para persuadir as vítimas a abrir ou conectar dispositivos maliciosos.
- **Falsificação de Certificados Digitais:** Os atacantes usaram assinaturas de certificado digital roubadas, o que pode ter envolvido engenharia social para obtê-las.
- **Manipulação de Operadores:** O Stuxnet explorou fraquezas humanas nos operadores de sistemas SCADA para ocultar suas atividades.
- **Propaganda e Conscientização:** O caso Stuxnet serviu como uma forma de engenharia social em nível global, destacando a importância da conscientização sobre ameaças cibernéticas e segurança em infraestruturas críticas.

Vídeo

- **STUXNET: O vírus que quase começou a 3ª Guerra Mundial**
  - https://www.youtube.com/watch?v=TY47UOIyGDs