TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 6. System Hacking

Módulo 7. Malware Threats

Módulo 8. Sniffing

Módulo 9. Social Engineering

Módulo 10. Denial-of-Service (DoS)

Conceitos de Engenharia Social:

A engenharia social refere-se ao método de influenciar e persuadir as pessoas a revelar informações sensíveis, a fim de executarem alguma ação maliciosa. Com a ajuda de truques de engenharia social, os atacantes podem obter informações confidenciais, detalhes de autorização, e detalhes de acesso de pessoas.

Os atacantes podem facilmente quebrar a segurança de uma organização usando truques de engenharia social. Todas as medidas de segurança adotadas pela organização são em vão quando os funcionários caem na "engenharia social". Alguns exemplos de engenharia social incluem, responder às perguntas de estranhos sem querer, responder a e-mail de spam e se gabar na frente dos colegas de trabalho.

CEHv12 (ANSI)

09.Social Engineering

Comportamentos vulneráveis

I. **Human nature of trust** is the basis of any social engineering attack

II. **Ignorance about social engineering** and its effects among the workforce makes the organization an easy target

III. **Fear** of severe losses in case of non-compliance to the social engineer's request

IV. Social engineers lure the targets to divulge information by **promising something for nothing** (**greediness**)

V. Targets are asked for help and they comply out of a sense of **moral obligation**

Impactos

- Economic Losses
- Loss of Privacy
- Damage of Goodwill
- Temporary or Permanent Closure
- Lawsuits and Arbitrations
- Dangers of Terrorism

Fases do ataque

Pesquisar sobre a empresa alvo

O atacante, antes de realmente atacar qualquer rede, reúne informações a fim de encontrar possíveis formas de se introduzir na rede de destino. O atacante inicialmente procede à investigação sobre a empresa alvo para encontrar informações básicas, como tipo de negócio, localização da organização, número de empregados, etc. Durante esta fase, o atacante pode conduzir dumpter diving, navegar através do site da empresa, encontrar detalhes de empregados e etc.

Selecionar uma vítima

Depois de realizar uma investigação aprofundada sobre a empresa alvo, o atacante escolhe uma vítima para obter a informação sensível. Funcionários descontentes da empresa são uma benção para o atacante. O atacante tenta encontrar esses funcionários e atraí-los para revelar a informação da companhia. Como eles estão insatisfeitos com a empresa, eles podem estar dispostos a vazar ou divulgar dados confidenciais da empresa para o atacante.

Desenvolver um relacionamento

Uma vez que esses trabalhadores são identificados, os atacantes tentam desenvolver relações com eles para que eles possam extrair informações confidenciais a partir deles. Em seguida, eles usam essa informação para obter mais informações ou para lançar ataques.

Explorar a relação

Uma vez que o atacante constrói uma relação com os funcionários da empresa, o atacante tenta explorar a relação do funcionário com companhia e tenta extrair informações sensíveis, tais como informações de conta, informações financeiras, as atuais tecnologias utilizadas, os planos futuros, etc.

Alvos comuns dos atacantes

Recepcionistas e pessoal de Help Desk

Os engenheiros sociais geralmente tem como alvo o service desk ou help desk da organização alvo e tentam enganá-los a fim de revelar informações confidenciais sobre a empresa.

Suporte técnico

Executivos de suporte técnico podem ser um dos alvos dos engenheiros sociais como eles podem chamar os executivos de suporte técnico e tentar obter informações confidenciais, fingindo ser um administrador de gerenciamento de nível superior, cliente, fornecedor, etc.

Usuários e clientes

Um atacante pode chamar os usuários e clientes, fingindo ser uma pessoa do suporte técnico e pode tentar extrair informações sensíveis.

Administradores de sistema

Os engenheiros sociais sabem que o administrador do sistema é a pessoa que mantém a segurança da organização. O administrador do sistema é responsável por manter os sistemas da empresa, e pode saber informações como contas e senhas de administrador. Se o atacante é capaz de engana-lo, em seguida, o atacante pode obter informações úteis. Portanto, os administradores de sistema podem também ser alvo de atacantes.

Os vendedores da organização alvo

As vezes um engenheiro social pode também ter como alvo os vendedores da empresa para tentar obter informações confidencias sobre a organização.

Técnicas

Human-based

Fingindo ser um usuário final legítimo: Um intruso poderia utilizar a técnica de representar um empregado, e em seguida, recorrer a métodos incomuns para ter acesso aos dados privilegiados. Ele pode dar uma identidade falsa e pedir informações confidenciais. Outro exemplo disso é que um "amigo" de um funcionário pode tentar recuperar as informações que um empregado acamado supostamente precisa.

Fingindo ser um importante utilizador: A representação é levada para um nível mais alto, assumindo a identidade de um funcionário importante, a fim de adicionar um elemento de intimidação. O fator reciprocidade desempenha um papel neste cenário, onde os funcionários de nível inferior podem sair de seus caminhos para ajudar um funcionário de nível superior, de modo que seu favor recebe a atenção positiva necessária para ajudá-los no ambiente corporativo.

Filmes

- Preda-me se for capaz
- Uma saída de mestre
- Os Vigaristas
- Quebrando a Banca
- VIPS
- Invasores
- Takedown

Livros

- A Arte de Enganar
- A Arte de Invadir

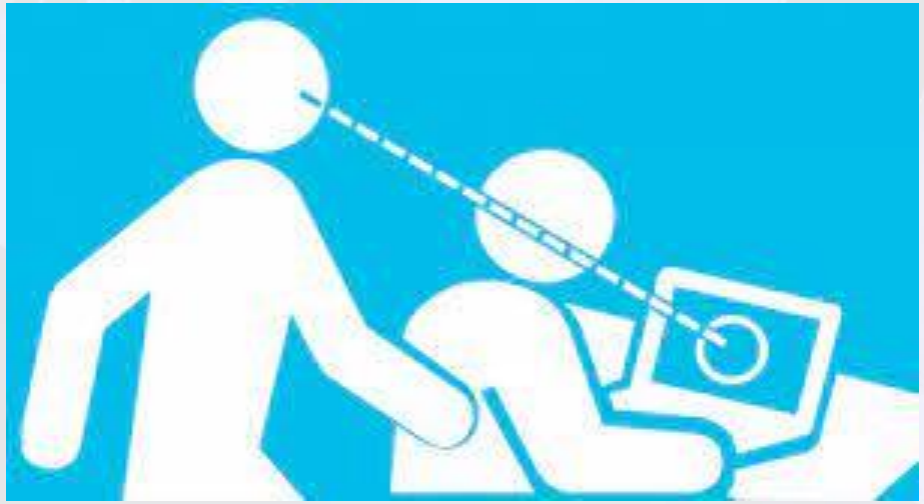
Técnicas

Eavesdropping/Espionagem

Eavesdropping refere-se ao processo de escuta não autorizada para a comunicação entre pessoas ou a leitura não autorizada de mensagens. Inclui a intercepção de qualquer forma de comunicação, incluindo áudio, vídeo ou por escrito. Ele também pode ser feito utilizando canais de comunicação como linhas telefonicas, e-mail, mensagens instantâneas, etc.

Shoulder surfing

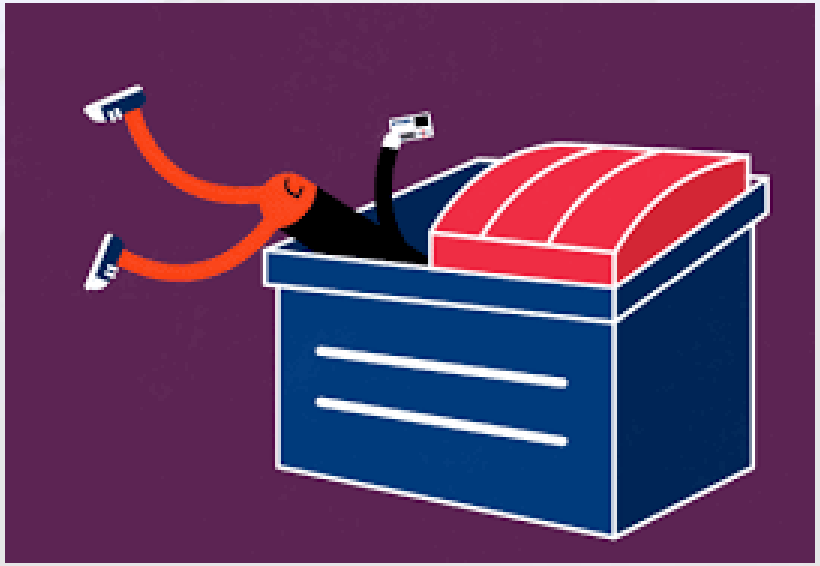
Shoulder surfing é o processo de observação por cima do ombro de alguém, enquanto a pessoa está digitando senhas, informações pessoais, números PIN, números de conta e outras informações. Ladrões olham por cima do ombro, ou mesmo assistem a uma distância usando binóculos, a fim de obter essas informações.



Técnicas

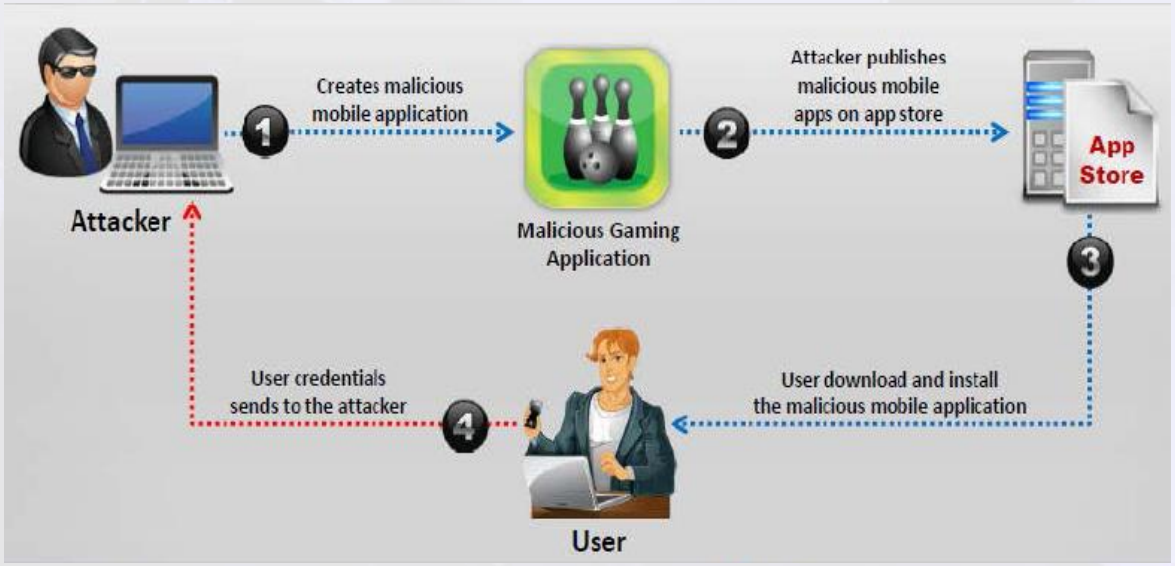
Dumpster Diving

Dumpster diving é um processo de recuperação de informações através de pesquisa no lixo para obter dados como códigos de acesso, senhas escritas em notas, listas de telefones, agendas e organograma para roubar sua identidade. Os atacantes podem usar esta informação para lançar um ataque na rede do alvo.



Mobile-based

Na engenharia social baseada em dispositivo móvel, o atacante realiza estes tipos de ataques com a ajuda de aplicações móveis. Aqui o atacante primeiro cria aplicativos maliciosos, tais como aplicativos de jogos com características atraentes e nomes eles o de aplicativos populares, e publica-os em grandes lojas de aplicativos.



Técnicas

Piggybacking

Piggybacking é um processo de ataque de dados que pode ser feito eletronicamente e fisicamente. O piggybacking físico é alcançado mediante a utilização fraudulenta de uma falsa associação para ganhar vantagem e ter acesso. Um atacante pode deslizar por trás de um empregado legítimo e obter acesso a uma área segura que normalmente seria bloqueado ou exigir algum tipo de acesso biométrico para entrada e mecanismo de controle para abrir uma fechadura de porta, etc.

Tailgating

Uma pessoa não autorizada usando um crachá falso entra em uma área segura, seguindo de perto uma pessoa autorizada através de uma porta que requer chave de acesso. Uma pessoa autorizada pode não estar ciente de ter fornecido uma pessoa o acesso não autorizado a uma área segura. A utilização não autorizada envolve conectar um usuário a um computador na mesma sessão como outro usuário, cuja sessão foi interrompida.

Técnicas

Ameaças internas

Um insider é qualquer empregado (pessoa de confiança), com acesso adicional aos ativos de uma organização. Um ataque insider envolve o uso de um acesso privilegiado violando as regras ou causando ameaça a sistemas de informação da organização em qualquer forma intencional.

Insiders podem facilmente contornar as regras de segurança e acessar informações sensíveis. É muito difícil descobrir este tipo de ataque interno. Estes ataques internos também podem causar grandes perdas para uma empresa

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.