ATIVIDADE 4

ATENÇÃO:

1) **Esta Atividade deverá ser feita em GRUPO DE PELO MENOS 04 ALUNOS E DE NO MÁXIMO 08 ALUNOS embora a entrega deverá ser feita INDIVIDUALMENTE no Classroom.**
2) **Atividades feitas individualmente ou entregues com atraso NÃO SERÃO CONSIDERADAS.**.

Grupo

Maria Clara Borges Rodrigues Santos RA:82410853

Giovanna Araujo Thomazzini Codo RA:824134072

Julia Zezilia Rodrigues RA:824213803

1) Leia TODA a **Cartilha Engenharia Social Guia para proteção de conhecimentos sensíves** (1-13) disponível em:

   https://www.gov.br/abin/pt-br/acesso-a-informacao/acoes-e-programas/PNPC/boaspraticas/cartilha-engenharia-social-guia-para-protecao-de-conhecimentos-sensiveis

   Escreva pelo menos 8 parágrafos comentando detalhadamente os principais conceitos abordados.

2) Crie um Jamboard colocando o que cada membro do seu Grupo achou de mais importante na leitura do PDF do **Material 1**. Compartilhe o link do Jamboard criado aqui. (A resposta desta questão é apenas o link do Jamboard com os tópicos/conceitos que cada membro do Grupo escolheu ao ler o Capítulo citado).

3) Pesquise os materiais abaixo e preencha a Tabela abaixo:

   VÍDEOS DISPONÍVEIS NO YOUTUBE:

VÍDEO 1- https://www.youtube.com/watch?v=omBdQFxGJs4

VÍDEO 2- https://www.youtube.com/watch?v=QLHd44L8A_E

VÍDEO 3- https://www.youtube.com/watch?v=EqkOpSCa97k

LIVRO LINK ABAIXO

MATERIAL	RESUMO DO SEU CONTEÚDO
VÍDEO 1	
VÍDEO 2	
VÍDEO 3	

RESPOSTA DO ALUNO

PERGUNTA 01:

Engenharia social, é uma técnica de manipulação que visa enganar pessoas para que divulguem informações confidenciais ou realizem ações que possam ser prejudiciais a elas ou a suas organizações. Diferente de ataques físicos ou coação direta, a engenharia social se baseia na exploração da confiança e das vulnerabilidades psicológicas das pessoas. Um exemplo típico é quando alguém é induzido a fornecer sua senha de acesso, acreditando que está lidando com um representante legítimo de uma organização, sem perceber que está sendo enganado.

Assim, o engenheiro social, ou seja, a pessoa que pratica essa técnica, pode ser qualquer indivíduo com interesse em acessar informações confidenciais. Isso inclui desde agentes de inteligência de Estados nacionais até hackers amadores. A sofisticação do ataque até pode variar, mas o princípio fundamental é o mesmo: manipular as pessoas para que elas tomem decisões que favoreçam o atacante. Por exemplo, um hacker com poucos recursos pode enviar um e-mail com um link malicioso para enganar a vítima, enquanto um agente de inteligência pode usar informações detalhadas sobre a vítima para realizar uma abordagem mais convincente.

Esses ataques podem ocorrer através de diversos canais de comunicação, como interações pessoais, chamadas telefônicas, e-mails ou redes sociais. A eficácia da engenharia social está ligada à maneira como ela explora os processos

automáticos de pensamento das pessoas. Psicologicamente, os humanos tendem a operar em um "Sistema Rápido", que é mais intuitivo e automático, em oposição ao "Sistema Lento", que é mais deliberado e analítico. Quando uma situação parece familiar ou comum, as pessoas tendem a responder automaticamente, sem refletir profundamente sobre o que estão fazendo, o que facilita a ação do engenheiro social.

Desse modo, um dos principais pontos explorados pelos engenheiros sociais é a pressão, seja de tempo ou de autoridade. Quando as pessoas sentem que precisam agir rapidamente ou que estão lidando com alguém em uma posição de poder, elas são menos propensas a questionar as solicitações que recebem. Além disso, os engenheiros sociais frequentemente exploram a empatia e a disposição das pessoas em ajudar, criando cenários onde a vítima sente que deve cooperar, seja para evitar prejudicar alguém ou para evitar se sentir culpada.

Ademais, a cartilha também explora a técnica da "entrevista", uma forma específica de engenharia social onde o atacante conduz uma conversa de maneira a extrair informações sem que a vítima perceba. Essa técnica não necessariamente envolve mentiras diretas. Em vez disso, o engenheiro social manipula o fluxo da conversa, levando a vítima a fornecer informações de forma voluntária. Por exemplo, em um congresso profissional, o engenheiro social pode começar uma conversa casual e, gradualmente, guiar o diálogo para tópicos de interesse, obtendo as informações desejadas sem levantar suspeitas.

Além disso, a diferenciação entre Phishing e Spearphishing é outro ponto importante abordado no texto. O Phishing é uma técnica de engenharia social em massa, onde o atacante lança uma "rede" ampla, esperando que algumas vítimas possam “fisgar” a isca. Um exemplo clássico é o e-mail do "príncipe nigeriano" pedindo ajuda para transferir uma herança. Já o Spearphishing é uma abordagem mais direcionada e personalizada, onde o atacante coleta informações específicas sobre a vítima para criar uma isca altamente convincente. Essa forma de ataque é muito mais eficaz, com taxas de sucesso significativamente maiores.

Nesse mesmo viés, o artigo também oferece orientações práticas sobre como se proteger contra ataques de engenharia social. A primeira linha de defesa é a desconfiança: questionar solicitações inesperadas e sempre verificar a autenticidade de quem está pedindo informações. Outra recomendação é evitar abrir anexos ou clicar em links de e-mails não verificados, pois esses são os principais vetores de ataques. A limitação das informações pessoais e profissionais disponíveis online também é crucial, pois quanto menos o atacante souber, mais difícil será para ele planejar um ataque eficaz.

Por tanto, é válido ressaltar a importância de alertar as autoridades de segurança da organização caso haja suspeita de uma tentativa de engenharia social. Uma única falha pode comprometer a segurança de toda uma instituição, por isso é fundamental que todos os membros da organização estejam cientes dos riscos e adotem uma postura proativa para se protegerem. Em suma, a

conscientização e a precaução são as principais armas contra a engenharia social, que continua a ser uma ameaça significativa no ambiente digital e no mundo real.

PERGUNTA 02:

https://jamboard.google.com/d/104hlcc4c9f9zk2xUzCVtJByPEQWsb5clOxQWUhsYgic/edit?usp=sharing

PERGUNTA 03:

MATERIAL	RESUMO DO SEU CONTEÚDO
VÍDEO 1	O algoritmo de Diffie-Hellman é um dos pilares da criptografia moderna. Ele foi criado em 1976 por Whitfield Diffie e Martin Hellman, e é usado para estabelecer uma chave secreta compartilhada entre duas partes que desejam se comunicar de forma segura, sem que um terceiro intervenha e intercepte a informação. Princípios Fundamentais, permite a criação de uma chave secreta compartilhada usando aritmética modular e logaritmos discretos, que são operações difíceis de inversor matematicamente. A essência do método é a dificuldade de resolver o problema do logaritmo discreto, o que garante a segurança do algoritmo. Fluxo do Protocolo O Diffie-Hellman funciona da seguinte maneira: 1 Escolha de intervalos públicos: - Um número primo grande \(p \). - Um número gerador \(g \), menor que \(p \). O gerador \(g \) tem propriedades matemáticas que ajudam na segurança do algoritmo. 2 Escolha de chaves privadas:** - Alice escolhe um número secreto \(a \). - Bob escolhe um número secreto \(b \). 3; Cálculo das chaves públicas: - Alice calcula \(A = g^a \mod p \) e envia \(A \) para Bob. - Bob calcula \(B = g^b \mod p \) e envia \(B \) para Alice. 4; Cálculo da chave secreta

	compartilhada: Alice calcula a chave secreta \(S_A = B^a \mod p \) usando a chave pública de Bob e seu segredo privado; Bob calcula a chave secreta \(S_B = A^b \mod p \) usando a chave pública de Alice e seu segredo privado.
VÍDEO 2	O Protocolo Needham-Schroeder é um protocolo de autenticação criado em 1978 por Roger Needham e Michael Schroeder. Ele permite que duas partes sejam autenticadas e estabeleçam uma comunicação segura, usando criptografia de chave pública ou chave simétrica, dependendo da versão do protocolo. Duas Versões Principais 1. Versão com chave simétrica (Needham-Schroeder Symmetric Key Protocol): - Usada para autenticação com um servidor de confiança. - Envolve uma troca de mensagens criptografadas usando chaves simétricas pré-compartilhadas e um servidor de autenticação central que distribui como chaves 2.
VÍDEO 3	A configuração do Squid (um servidor proxy HTTP) com autenticação transparente e Kerberos é uma solução comum para implementar autenticação automática em redes corporativas, sem a necessidade dos usuários inserirem manualmente suas credenciais. Aqui está um resumo dessa configuração e seus componentes: 1 Squid Proxy O Squid é um proxy usado para controlar e melhorar o tráfego da rede, oferecendo cache de conteúdo e controle de acesso a sites . Ele pode ser configurado para exigir autenticação dos usuários antes de permitir o acesso à internet. 2 Autenticação Transparente refere-se ao processo de autenticar usuários sem exigir que eles forneçam manualmente suas credenciais. No caso de integração com Kerberos, a autenticação é feita automaticamente usando o ticket Kerberos fornecido pelo sistema operacional quando o usuário faz login no domínio do Active

	Directory (AD). 3 Kerberos é um protocolo de autenticação de rede que usa criptografia de chave simétrica e tickets para permitir que os usuários provem sua identidade em um ambiente de rede seguro. Em ambientes Windows, ele é frequentemente usado em conjunto com o Active Directory para autenticar usuários de forma automática e transparente. Como Funciona a Integração Squid + Kerberos + Autenticação Transparente 1; Usuário faz login no domínio: Quando um usuário faz login no ambiente Windows, ele obtém um ticket de autenticação Kerberos do KDC (Key Distribution Center), que é o servidor de autenticação no Active Directory 2.