Integrantes Do Grupo

Otavio Paiva/ RA: 824147017
Gabriel Prieto/ RA: 824142064
Eduardo Baptistella/ RA: 824147595

1. Vulnerabilidades(s):
Defina as vulnerabilidades: Uma vulnerabilidade é um defeito ou vulnerabilidade em um sistema, rede ou aplicativo que pode ser aproveitada por um invasor (cracker) para adquirir acesso não permitido ou provocar danos.
Exemplos frequentes de fragilidades:
Defeitos em software: Erros de programação em sistemas, aplicativos ou servidores que podem ser explorados.
Senhas vulneráveis: Aplicação de senhas fáceis de descobrir ou ações como força bruta.
Ausência de criptografia: Informações sensíveis sem a devida proteção.
Ausência de atualização de software: Sistemas sem as atualizações de segurança necessárias.
Phishing: Prática que explora vulnerabilidades humanas, induzindo os usuários a fornecerem informações confidenciais.

2. Tipos e Técnicas de Ataque Utilizados:
Formas e Métodos de Ataque Empregados:
Emergência Social:
O criminoso engana indivíduos para que forneçam informações confidenciais, tais como senhas ou informações pessoais.
Fraude:
Disparo de mensagens ou links fraudulentos para adquirir dados sensíveis, como senhas ou números de cartões de crédito.
Análise de falhas de software (Exploit):
A utilização de defeitos em sistemas ou programas para a execução de códigos maliciosos, como o excesso de buffer, pode possibilitar a execução de ações não autorizadas.
Ataques de negação de serviço distribuída (DDoS):
Um ataque onde o invasor busca sobrecarregar um sistema ou servidor com um volume excessivo de tráfego, tornando-o inoperante.
Mali Malware:

A utilização de vírus, worms, ransomware ou trojans com o intuito de acessar sistemas ou impedir a utilização de dados.
SQL Injection:Inserção de comandos maliciosos em consultas SQL, permitindo que um atacante acesse ou altere dados de um banco de dados.
Ransomware:
Ataque onde o atacante criptografa os arquivos de um sistema e exige um resgate para a chave de descriptografia.

3. Motivação do Cracker:
Razão do Hacker:
Finanças:
Vários ataques são impulsionados por lucros monetários, como o roubo de informações bancárias, extorsão por meio de ransomware ou fraudes com cartões de crédito.
Conceitual:
Certos hackers agem motivados por questões políticas ou ideológicas, como o ativismo digital ou o hacktivismo, com o objetivo de promover uma causa ou manifestar-se contra algo específico.
Vigilância:
Empresas ou governos podem ser vítimas de ataques que visam roubar informações confidenciais, tais como segredos de negócios ou informações delicadas de segurança nacional.
Desafio ou gratificação:
Alguns atacantes, particularmente os novatos ou denominados "hackers éticos", podem executar ataques para testar suas competências ou obter destaque em comunidades de segurança.
Retribuição:
Ataques motivados por desentendimentos ou rivalidades podem ser executados com o intuito de prejudicar alguém ou uma entidade.