1.Vetores de ameaça

Os ***ativos*** são tudo de valor para uma organização, como dados e outras propriedades intelectuais, servidores, computadores, smartphones e muito mais. O caminho ou ferramenta usado por um agente de ameaça mal-intencionado pode ser chamado de ***vetor de ataque***.

Uma *ameaça* é um perigo em potencial para um ativo, como dados ou a própria rede. É o potencial de alguém ou alguma coisa explorar uma vulnerabilidade e causar uma violação de segurança. As ameaças podem ser naturais, humanas ou causadas por erros não intencionais. A pessoa ou coisa que representa uma ameaça é chamada de ***agente de ameaça***.

Uma *vulnerabilidade* é uma fraqueza em um sistema ou em seu design que pode ser explorado por uma ameaça. As vulnerabilidades podem resultar de falhas de segurança, configurações inadequadas, falhas de projeto em aplicativos, falta de atualizações de software e correções, uso indevido de softwares ou protocolos de comunicação, arquitetura de rede mal projetada, segurança física inadequada e outros fatores.

Já uma ***superfície de ataque*** é a soma total das vulnerabilidades em um determinado sistema que são acessíveis a um invasor. **A superfície de ataque descreve diferentes pontos em que um invasor pode entrar em um sistema e onde ele pode obter dados do sistema**. Para avaliar a superfície de ataque, é necessário considerar o tipo de agente da ameaça. A superfície de ataque pode ser considerada para uma rede como um todo, mas também é analisada para aplicações de software individuais. Minimizar a superfície de ataque significa restringir o acesso para que apenas alguns endpoints, protocolos/portas e serviços/métodos conhecidos sejam permitidos.

***Exploit* é o mecanismo que é usado para alavancar uma vulnerabilidade a fim de comprometer um ativo**. As explorações podem ser remotas, funciona através da rede sem qualquer acesso prévio ao sistema de destino, ou locais, onde o ator de ameaça tem algum tipo de acesso administrativo ou de usuário ao sistema final.

Um *vetor de ataque* é um caminho pelo qual um atacante pode obter acesso a um servidor, equipamento ou rede. Estes vetores de ataques podem se originar de dentro ou de fora de uma organização. Ameaças internas têm o potencial de causar maior dano que as ameaças externas, pois os usuários internos têm acesso direto ao edifício e a seus dispositivos de infraestrutura. Os invasores internos também têm conhecimento da rede corporativa, de seus recursos e de seus dados confidenciais. As ameaças externas de amadores ou invasores habilidosos podem explorar vulnerabilidades em dispositivos conectados em uma rede ou podem usar engenharia

social para obter acesso. Ataques externos tem como foco explorar fraquezas e vulnerabilidades para obter acesso a recursos externos.

2.Vetores de ataque baseado em software

2.1 Malware

O termo abrange várias formas de software malicioso, incluindo vírus, worms, cavalos de Troia, spyware e ransomware. Esses programas são projetados para infectar sistemas e causar danos, roubar informações ou criar uma porta dos fundos para os invasores.

2.2 SQL injection

Isso inclui ataques como injeção de SQL e injeção de código, onde os invasores inserem código malicioso em aplicativos da web para explorar vulnerabilidades e obter acesso não autorizado a bancos de dados ou sistemas.

2.3 Ataques ransomware

Os ataques de ransomware envolvem a criptografia de arquivos ou sistemas, com os invasores exigindo um resgate em troca da chave de descriptografia.

2.4 0Days

Os invasores procuram e exploram vulnerabilidades em software, sistemas operacionais e aplicativos para ganhar acesso não autorizado. Isso inclui exploits de dia zero, que atacam vulnerabilidades desconhecidas.

2.5 Ataques a dispositivos IoT

Os dispositivos da Internet das Coisas frequentemente têm poucas medidas de segurança, tornando-os alvos para invasores que podem explorar vulnerabilidades nesses dispositivos para acessar redes maiores.

2.6 Evasão de firewall

Esses ataques visam enganar os firewalls de segurança para permitir o acesso não autorizado a sistemas ou redes.

3.Vetores de ataques sociais e psicológicos

3.1 Phishing

O phishing envolve a criação de mensagens de e-mail, sites da web ou mensagens de texto falsas que parecem legítimas para enganar os destinatários a fornecer informações confidenciais, como senhas, números de cartão de crédito ou informações bancárias.

3.2 Engenharia social

É uma técnica que envolve a manipulação psicológica de indivíduos para obter informações confidenciais ou acesso a sistemas. Pode incluir táticas como manipulação, persuasão ou pretextos enganosos.

3.3 Ataques de engenharia reversa

Isso envolve a desmontagem e análise de código de software ou dispositivos para descobrir segredos, como algoritmos de criptografia ou protocolos de segurança.

3.4 Ataques MitM

Envolve um invasor que se posiciona entre a comunicação entre duas partes, interceptando ou alterando os dados durante a transmissão.

3.5 Spoofing

Isso inclui o spoofing de IP, onde os invasores mascaram seu endereço IP real para parecer que estão em outro lugar na rede.

4.Vetores de ataque de redes e tráfego

4.1 Ataques DoS

Envolvem uma inundação de tráfego de rede direcionada a um servidor ou serviço, sobrecarregando-o e tornando-o inacessível para os usuários legítimos.

4.2 Ataques a redes wireless

Incluem a interceptação de comunicações em redes Wi-Fi, a quebra de senhas de rede e a criação de pontos de acesso falsos.

4.3 Flooding

Envolvem o envio de tráfego excessivo para um alvo, sobrecarregando os recursos e tornando-os inacessíveis.

5.Vetores de ataque de autenticação e senhas

5.1 Ataques de força bruta

Nesse tipo de ataque, os invasores tentam adivinhar senhas ou chaves de criptografia ao testar várias combinações rapidamente até encontrar a correta.

5.2 Ataques de dicionário

Nesse tipo de ataque, os invasores usam uma lista de palavras-chave comuns e combinações previsíveis como base para a tentativa de adivinhar a senha. Eles testam cada palavra ou combinação em uma tentativa de encontrar uma correspondência válida.

5.3 Rainbow tables

São tabelas de pré-cálculo que contêm hashes (representações criptografadas) de senhas comuns e suas correspondentes senhas em texto simples. Os invasores podem usar essas tabelas para procurar hashes de senhas roubadas e, assim, obter as senhas correspondentes.

5.4 Ataques de risco de senhas online e offline

Os ataques de risco em senhas podem ser conduzidos tanto online quanto offline. No ataque online, os invasores tentam adivinhar senhas diretamente em sistemas de autenticação, como sites. No ataque offline, eles tentam quebrar hashes de senhas roubadas de bancos de dados sem precisar interagir diretamente com o sistema em questão.