1.Introdução a ataques

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.

Ataques cibernéticos como o Stuxnet provaram que um ataque cibernético pode destruir ou interromper infraestruturas essenciais. Em um nível pessoal, é preciso proteger suas identidades, seus dados e seus dispositivos computacionais. No nível corporativo, é

responsabilidade dos funcionários proteger a reputação, os dados e os clientes da organização. No nível do estado, a segurança nacional e a segurança e o bem estar dos cidadãos estão em jogo. As iniciativas para proteger o estilo de vida das pessoas entram em conflito com o seu direito à privacidade.

1.1 Vetores de ataques baseado em software

- **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.
- **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.
- **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.
- **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.
- **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.
- **Evasão de firewall:** Esses ataques visam enganar os firewalls de segurança para permitir o acesso não autorizado a sistemas ou redes.

1.2 Vetores de ataques sociais e psicológicos

- **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.
- **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.
- **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.
- **Ataques MitM:** Envolve um invasor que se posiciona entre a comunicação entre duas partes, interceptando ou alterando os dados durante a transmissão.
- **Spoofing:** Isso inclui o spoofing de IP, onde os invasores mascaram seu endereço IP real para parecer que estão em outro lugar na rede.

1.3 Vetores de ataque de redes e tráfego

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

1.4 Vetores de ataques de autenticação e senhas

- **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.
- **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.
- **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.
- **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.

1.5 Ataques de escuta (eavesdropping)

Um ataque de espionagem que ocorre quando um agente de ameaça captura e escuta o tráfego da rede. Esse ataque também é chamado de sniffing ou snooping.

1.6 Ataques de modificação de dados

Ataques de modificação de dados ocorrem quando um agente de ameaça captura o tráfego da empresa e altera os dados nos pacotes sem o conhecimento do remetente ou receptor.

1.7 Ataques de falsificação de endereços IP

Um ataque de falsificação de endereço IP ocorre quando um ator de ameaça constrói um pacote IP que parece se originar de um endereço válido dentro da Internet corporativa.

1.8 Ataques baseados em senha

Ataques baseados em senha ocorrem quando um ator de ameaça obtém as credenciais de uma conta de usuário válida e em seguida, os atores de ameaças usam essa conta para obter listas de outros usuários e informações de rede.

1.9 Ataques DoS

Este ataque impede o uso normal de um computador ou rede por usuários válidos. Após obter acesso a uma rede, um ataque DoS pode travar aplicativos ou serviços de rede. Um ataque de DoS pode inundar um computador ou toda a rede com tráfego até que um desligamento ocorra devido a sobrecarga.

1.10 Ataques MitM

Um ataque MitM ocorre quando os agentes da ameaça se posicionam entre a origem e o destino. Agora eles podem monitorar, capturar e controlar ativamente a comunicação de forma transparente.

1.11 Ataque MitMO

Man-in-the-Mobile é uma variação onde se assume o controle de um dispositivo móvel. O dispositivo infectado envia as informações confidenciais do usuário para os invasores. Um ataque de repetição ocorre quando um invasor captura uma parte de uma comunicação entre dois hosts e retransmite a mensagem capturada mais tarde. Os ataques de repetição driblam os mecanismos de autenticação.

1.12 Ataques de chave comprometida

Um ataque de chave comprometida ocorre quando um ator de ameaça obtém uma chave secreta. Isso é referido como uma chave comprometida e pode ser usada para obter acesso a uma comunicação segura sem que o remetente ou destinatário esteja ciente do ataque.

1.13 Ataque sniffer

Um sniffer é um aplicativo ou dispositivo que pode ler, monitorar e capturar trocas de dados de rede e ler pacotes de rede. Se os pacotes não estiverem criptografados, um sniffer fornece uma visão completa dos dados dentro do pacote.

1.14 Ataques de reconhecimento

Este tipo de ataque realiza a coleta de informações e é análogo a um ladrão que inspeciona um bairro indo de porta em porta fingindo vender alguma coisa. Os atores de ameaças usam ataques de sistemas, serviços ou vulnerabilidades. Os ataques de reconhecimento precedem ataques de acesso ou ataques DoS. Os seguintes passos são tomados para realizar este tipo de ataque: Executar uma consulta de informações de um alvo, iniciar uma varredura de ping da rede de destino, iniciar uma verificação de porta nos endereços IP ativos, executar o scanner de vulnerabilidades e por fim executar ferramentas de exploração.

1.15 Ataques de acesso

Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços FTP e serviços Web com o objetivo de obter acesso a contas, bancos de dados e outras informações confidenciais. Os atores usam ataques de acesso a dispositivos de rede e computadores para recuperar dados, escalar seus privilégios ou obter acesso. Alguns tipos de ataques são: Ataques de senha, spoofing, exploração de confiança, redirecionamento de porta, MitM e buffer overflow.

1.16 Ataques de Engenharia Social

Este tipo de ataque é de tentar manipular indivíduos para realizar ações ou divulgar informações confidenciais. Algumas técnicas de engenharia social são realizadas pessoalmente, enquanto outras podem usar o telefone ou a Internet. Engenheiros sociais frequentemente dependem da boa vontade das pessoas para ajudá-los, explorando a fraqueza delas. O agente de ameaças pode recorrer à vaidade do funcionário, valer-se de autoridade usando técnicas que citam nomes ou apelar para a ganância do funcionário. Ataques comuns de engenharia social são: Pretexting, phishing, spear phishing, spam, tailgating, busca de informações na lixeira, iscas, algo por algo e outros.

1.17 Ataques de Spoofing

É um ataque de representação e tira o proveito de uma relação de confiança entre dois sistemas. Se ambos aceitarem a autenticação de cada um deles, um indivíduo conectado a um sistema pode não passar novamente pelo processo de autenticação novamente para acessar outros sistemas. Um invasor pode se aproveitar desse arranjo, enviando um pacote para um sistema que parece ter vindo de um sistema confiável. Existem vários tipos de ataques de spoofing como os de endereço MAC, endereço IP, spoofing ARP e spoofing DNS.

Se os atores da ameaça comprometer muitos hosts, eles podem iniciar um ataque DDoS, ataques semelhantes, porém com aumento na magnitude pois se origina de diversas fontes de forma coordenada. Alguns dos termos utilizados neste tipo de ataque são os zumbis, grupo de hosts comprometidos (agentes) por um worm; bots, malware projetado para infectar um host e se comunicar com um sistema; handler, se referindo ao servidor primário de comando e controle, responsável pelos zumbis ou a própria botnet; botnet, referindo-se a todos os hosts infectados pelo worm controlador.

1.18 Ataques de buffer overflow

O objetivo de um ataque de buffer overflow é encontrar uma falha relacionada à memória do sistema em um servidor e explorá-la sobrecarregando-a com valores inesperados, geralmente causando um DoS.

1.19 Ataque de keyboard logging

É um programa de software que grava ou registra os toques de teclas do usuário do sistema. Os criminosos podem implementar registros de toque de tela no software instalado em um sistema de computador ou por meio de um hardware fisicamente conectado a um computador. O criminoso configura o software registrador de tecla para enviar um e-mail com o arquivo de log. Os toques de tecla capturados no arquivo de log podem revelar nomes de usuários, sites visitados e outras informações confidenciais. Muitos aplicativos anti-spyware são capazes de detectar e remover registradores de teclado não autorizados.

1.20 Ataque de Evil Twin

Este usa um access point do criminoso aprimorado com antenas de maior potência e maior ganho, para parecer uma melhor opção de conexão para os usuários. Depois que os usuários se conectam aos access point do invasor, os criminosos podem analisar o tráfego e executar ataques MitM.

1.21 Ataque Cross-site Scripting (XSS)

É uma vulnerabilidade encontrada nos aplicativos da Web. XSS permite que os criminosos injetem scripts contendo código malicioso em páginas Web. O script entre o site tem três participantes: o criminoso, a vítima e o site. O criminosos virtual não mira diretamente na vítima. O criminoso explora a vulnerabilidade dentro de um site ou aplicativo da Web. Os criminosos injetam scripts no cliente em páginas Web visualizadas pelos usuários. O script mal-intencionado inadvertidamente passa para o navegador do usuário. Se obtiver o cookie de sessão da vítima, os criminosos poderão se passar pelo usuário.

1.22 Injeção de XMI

Ao usar um banco de dados XMI, uma injeção de XMI é um ataque que pode corromper os dados. Depois que o usuário dá a entrada, o sistema acessa os dados necessários através de uma consulta. O problema ocorre quando o sistema não examina corretamente a solicitação de entrada fornecida pelo usuário. Os criminosos podem manipular a consulta, programando para atender às necessidades dos criminosos e acessar as informações no banco de dados. Todos os dados confidenciais armazenados no banco de dados são acessíveis para os criminosos e eles podem efetuar quantas alterações desejar no site.

1.23 Injeção SQL

O criminoso virtual explora uma vulnerabilidade, inserindo uma instrução SQL mal-intencionada em um campo de entrada. Mais uma vez, o sistema não filtra a entrada do usuário corretamente para os caracteres em uma instrução de SQL em sites ou qualquer banco de dados SQL. Os criminosos podem falsificar uma identidade, modificar os dados existentes, destruir os dados ou se tornar os administradores do servidor do banco de dados.

2.Indicadores de comprometimento/Indicadores de malware (IOC)

Os indicadores de malware, ou simplesmente indicadores de comprometimento (IoCs), desempenham um papel crítico na detecção, análise e prevenção de ameaças cibernéticas maliciosas, como vírus, worms, cavalos de Troia e outras formas de software mal-intencionado. Eles representam traços, pistas ou evidências deixadas pelo software malicioso em um sistema ou rede que podem ser usados para identificar a presença ou atividade desse software. Eles são como impressões digitais virtuais que permitem que os profissionais de segurança rastreiem e analisem o comportamento suspeito ou malicioso.

Os indicadores de malware não se limitam a um único formato. Eles abrangem uma variedade de pistas que podem ser usadas para identificar a presença de software malicioso. Alguns exemplos incluem notificações de antivírus, que sinalizam a detecção de código malicioso, a execução de um ambiente de sandbox, que pode revelar tentativas de evasão; o

consumo anormal de recursos do sistema e mudanças no sistema de arquivos, que podem indicar a presença de malware.

Muitos ataques podem ser evitados se compartilhando informações sobre. Cada ataque tem atributos identificáveis únicos, indicadores de compromisso são a evidência de que um ataque ocorreu. IOCs podem ser recursos que identificam arquivos de malware, endereços IP de servidores que são usados em ataques, nomes de arquivos e alterações características feitas no software final do sistema.

3.Indicadores de ataque (IOA)

Estes se concentram mais na motivação por trás de um ataque e nos potenciais meios pelos quais os atores da ameaça têm, ou irão, comprometer vulnerabilidades para obter acesso a ativos. IOAs buscam saber das estratégias usadas e ao invés de informar a resposta a uma única ameaça, eles podem ajudar a gerar uma abordagem de segurança proativa. É importante entender que os atores de ameaças usam uma variedade de ferramentas de segurança para realizar esses ataques.