CST0203 - Ameaças, vulnerabilidades e ataques a Segurança Cibernética: Parte 3 - Tipos de Ataques

Data do Post	@July 1, 2022 9:00 AM
Status	Done
Palavras-chave	Ameaças vulnerabilidades e ataques a Segurança Cibernética
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☑

Post- Linkedin

Nos últimos 2 ou 3 anos vivenciamos inúmeras ataques cibernéticos em empresas nacionais e, até mesmo internacionais. Essa situação gerou uma situação alarmante nas pessoas, pois muitas se sentiram inseguras por não saberem as principais características desses ataques e, até mesmo, por não saberem diferenciar os tipos de ataques. Nessa ordem de ideias, esse artigo apresenta mais um conteúdo informativo que visa elucidar os leitores sobre os tipos de ataques e algumas características básicas dos mesmos. Leia o artigo na íntegra para saber isso e muito mais.

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech
Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/
#cybersecurity #technology #linux #programming #hacking #vulnerabilities #maliciouscode #malwares #protection

Introdução

Um ataque cibernético é uma situação que coloca em risco eminente os três pilares da segurança cibernética — disponibilidade, integridade e confiabilidade. Como é de conhecimento geral, todos estamos expostos a um ataque, pois todos os dias encontramos e são descobertas novas vulnerabilidades nos softwares e dispositivos que usamos diariamente o que pode gerar uma ameaça que abre um caminho para um possível ataque.

Existem inúmeros tipos de ataques de manifestam e têm comportamentos diferentes. Conhecer o básico possível sobre esses ataques é uma maneira básica e primordial para saber como nos proteger.

Tipos de ataques cibernéticos

Denial-of-Service (DoS)

Os ataques de negação de serviço são um tipo de ataque de rede que resulta nalgum tipo de interrupção dos serviços de rede e negar acesso a utilizadores autorizados, tornando a rede indisponível para tais utilizadores, dispositivos ou aplicações.

Existem dois tipos principais de ataque DoS:

- **Enorme Quantidade de Tráfego** — Uma enorme quantidade de dados é enviada a uma velocidade que a rede, um dispositivo anfitrião ou aplicação não consegue processar causando lentidão na transmissão, ou na resposta, ou o bloqueio de um dispositivo, ou serviço.

- **Pacotes com Formatação Maliciosa** — Um pacote com formatação maliciosa é enviado a um dispositivo anfitrião ou a uma aplicação e o recetor não consegue processá-lo, e o dispositivo recetor funciona de forma muito lenta ou é bloqueado.

Os ataques DoS são considerados um risco grave, na medida em que podem interromper facilmente a comunicação e provocar perdas significativas de tempo e dinheiro. Estes ataques são relativamente fáceis de realizar, mesmo por um atacante com poucas aptidões.

Distributed DoS Attack (DDoS)

Um ataque DoS Distribuído é semelhante a um ataque DoS, mas tem origem em múltiplas fontes coordenadas. Um ataque DDoS pode ocorrer quando um atacante cria uma rede de dispositivos anfitriões infetados, denominada botnet, composta por dispositivos infetados e controlados pelo atacante que são designados por zombies. Eles analisam constantemente e infetam mais hosts, criando mais zombies. Quando estiver pronto, o pirata informático dá ordem aos sistemas de controlo para que façam com que a botnet de zombies realize um ataque DDoS.

Sniffing

Sniffing é similar a escutar ou espiar alguém às escondidas. Ocorre quando os atacantes examinam todo o tráfego de rede enquanto este passa através das suas interfaces de rede. Os criminosos realizam sniffing de rede com uma ferramenta de software, um dispositivo de hardware ou uma combinação de ambos. O sniffing visualiza todo o tráfego de rede ou pode atingir um protocolo específico, serviço, ou até mesmo sequência de caracteres, como um login ou palavra-passe. Alguns sniffers de rede observam todo o tráfego e também podem modificar parte ou todo o tráfego.

Spoofing

Spoofing, ou falsificação, é um ataque de imitação, que se aproveita de uma relação confiável entre dois sistemas. Se dois sistemas aceitarem a autenticação realizada um pelo outro, um usuário logado a um sistema poderá não ter que passar por um novo processo de autenticação para aceder ao outro sistema. Um atacante tirar vantagem deste arranjo através do envio de um pacote para um sistema como se parecesse ter vindo de um sistema confiável. Como o relacionamento confiável está em vigor, o sistema destino pode executar a tarefa solicitada sem autenticação.

Tipos de ataques de spoofing.

- **MAC address spoofing:** é a falsificação de endereços MAC e ocorre quando um computador aceita pacotes de dados com base no endereço MAC de outro computador.
- **IP spoofing: falsificação IP** consiste no envio de pacotes IP de um endereço de origem falsificado para se disfarçar.

O Address Resolution Protocol (ARP) é um protocolo que resolve endereços IP para os correspondentes endereços MAC para transmitir dados. ARP spoofing baseia-se no envio de mensagens ARP falsificadas numa rede LAN para associar o MAC address do criminoso com o endereço IP de um membro autorizado da rede.

O Domain Name System (DNS) associa nomes de domínio a endereços IP. A falsificação por DNS server spoofing modifica o servidor DNS para redirecionar um nome de domínio específico para um endereço IP diferente controlado pelo criminoso.

Man-in-the-middle (MitM)

Consiste na interceptação das comunicações entre computadores para roubar as informações que atravessam a rede. O criminoso pode também optar por manipular mensagens e retransmitir informações falsas entre dispositivos, uma vez que os dispositivos não sabem que ocorreu uma modificação às mensagens. Um ataque MitM permite que o atacante assuma o controlo de um dispositivo sem conhecimento do utilizador.

Ataques de Dia Zero

Um ataque Zero-Day, ou de Dia Zero, às vezes referido como uma ameaça de dia zero, é um ataque de computador que tenta explorar vulnerabilidades de software que são desconhecidas ou não divulgadas pelo fornecedor. O termo hora zero descreve o momento em que alguém descobre a exploração das vulnerabilidades. Durante o tempo que o fornecedor de software leva para desenvolver e disponibilizar um patch, a rede está vulnerável a essas explorações. Defender esses ataques rápidos exigem que os profissionais de segurança de rede adotem uma visão mais sofisticada da arquitetura de rede. Não é mais possível conter intrusões em alguns pontos da rede.

Keyboard Logging

Keyboard Logging, ou registo de teclado, é um programa de software que regista as teclas digitadas pelo utilizador do sistema. Os criminosos podem implementar registadores de teclas (keystroke loggers) através do software instalado num computador ou através de hardware fisicamente ligado a um computador. O criminoso configura o software do registo de teclas para enviar por e-mail o ficheiro de log. As teclas digitadas e registadas no ficheiro log podem revelar nomes de utilizador, palavras-passe de acesso, websites visitados e outra informação confidencial.

Os registadores de teclas podem ser software comercial legítimo. Frequentemente, os pais de crianças compram software key logger para rastrear os websites e o comportamento das crianças usando a Internet. Muitas aplicações anti-spyware são capazes de detectar e remover registadores de teclas não autorizados. Embora o software keylogging seja legal, os criminosos usam o software para fins ilegais.

Defesa contra ataques

Uma organização pode tomar uma série de medidas para se defender contra vários ataques. Configurar firewalls para descartar todos os pacotes vindos de fora da rede que tenham endereços indicando que tiveram origem de dentro da rede. Esta situação normalmente não ocorre, e indica que um atacante virtual tentou um ataque de falsificação.

Para evitar ataques DoS e DDoS, é necessário que os softwares e dispositivos estejam sempre atualizados. Também é importante distribuir a carga de trabalho entre sistemas de servidor e bloqueie na fronteira pacotes Internet Control Message Protocol (ICMP) do exterior. O ICMP é usado por dispositivos de rede para enviar mensagens de erro. Por exemplo, o comando ping usa pacotes ICMP para verificar se um dispositivo pode comunicar com outro na rede.

Os sistemas podem impedir que sejam vítimas de um ataque de retransmissão cifrando o tráfego, fornecendo autenticação criptográfica e incluindo uma etiqueta temporal da data/hora com cada parte da mensagem.

A principal forma de proteger o ambiente virtual de um negócio é adotando bons recursos de cibersegurança e oferecendo educação e treinamento aos colaboradores.

Para ter um sistema mais seguro e proteger os dados, vale observar as seguintes dicas:

- desconfie e oriente seus funcionários (no caso das empresas) a sempre desconfiarem de e-mails com ofertas incríveis e muito chamativas, eles podem conter malwares
- instale um bom antivírus, que ofereça proteção completa para seu sistema, de acordo com a necessidade do seu negócio
- mantenha sistemas operacionais e softwares sempre atualizados, pois versões desatualizadas são mais vulneráveis a ciberataques
- garanta que o seu firewall esteja sempre ativo
- crie uma política de definição de senhas fortes e que sejam mudadas de tempos em tempos
- faça backup periódico de todos os arquivos, eles serão muito úteis no caso de um ataque bem sucedido
- para quem trabalha em home office ou em trabalho remoto, use uma conexão VPN para garantir a segurança e o controle dos dados

Conclusão

Cada um de nós de estar atento à segurança cibernética para evitar prejuízos e interrupções dos sistemas. Criminosos virtuais estão o tempo todo procurando oportunidades e estão sempre atualizando as suas práticas ilícitas o que requer mais cuidados através da buscar meios de prevenir e proteger os seus dados que podem ser medidas preventivas que envolvam pessoas, tecnologias e a correta gestão das ações para criar uma cultura de segurança da informação e evitar ataques cibernéticos.

Siga-me e veja outros posts no meu Instagram @idaleciosilvatech
Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
Link do perfil no IG: https://www.instagram.com/idaleciosilvatech/
#cybersecurity #technology #linux #programming #hacking #vulnerabilities #maliciouscode #malwares #protection