1.Application attacks

Ataques de injeção são uma forma comum de exploração de vulnerabilidades em aplicações, permitindo que invasores insiram código malicioso em dados enviados para um servidor ou dispositivo cliente. Normalmente, esses ataques são bloqueados por verificações adequadas na aplicação, mas falhas nesse controle possibilitam que o código malicioso seja executado. Um exemplo bastante conhecido é a **injeção de SQL**, mas ataques semelhantes podem ser realizados em HTML, XML, LDAP e outros formatos de dados.

Outro ataque relacionado é o **buffer overflow**, que ocorre quando um programa recebe mais dados do que a memória reservada para determinada variável pode armazenar. Esse excesso de informações transborda para áreas adjacentes da memória, podendo corromper dados ou permitir que um invasor execute código malicioso. Descobrir uma vulnerabilidade desse tipo exige grande conhecimento técnico, pois o comportamento da memória varia conforme a aplicação. Em muitos casos, o ataque apenas faz com que o programa falhe e encerre, mas se explorado corretamente, pode conceder ao atacante controle sobre o sistema.

O **ataque de repetição (replay attack)** envolve capturar informações de autenticação de um usuário legítimo e reutilizá-las para obter acesso não autorizado. Para isso, o invasor pode interceptar dados na rede usando técnicas como **ARP poisoning** ou instalar malware no computador da vítima para roubar credenciais. Com um nome de usuário e hash de senha ou um ID de sessão válido, o ataque pode ser realizado repetindo esses dados para o servidor. Em alguns casos, essa técnica é combinada com **ataques Man-in-the-Middle**, nos quais o invasor intercepta comunicações entre o usuário e o servidor.

A **elevação de privilégios** é um dos objetivos principais dos invasores, permitindo que obtenham acessos administrativos dentro de um sistema. Quando um usuário comum se autentica em uma aplicação, ele recebe permissões limitadas. No entanto, se houver falhas de segurança ou bugs na aplicação, um atacante pode explorá-los para obter permissões mais altas. Esse processo pode ocorrer de duas formas: **elevação vertical**, em que o invasor passa de usuário comum para administrador, e **elevação horizontal**, que permite assumir a identidade de outro usuário sem necessariamente ganhar permissões adicionais. Para mitigar esse risco, é essencial manter sistemas atualizados, utilizar ferramentas de segurança como antivírus e configurar políticas de controle de acesso adequadas.

Um exemplo real de vulnerabilidade desse tipo é a **CVE-2023-29336**, um problema identificado no driver **win32k** do Windows, que afetava versões como Windows Server 2008, 2012, 2016 e Windows 10. Explorando essa falha, um invasor poderia obter permissões **System**, que representam o mais alto nível de privilégio dentro do sistema operacional Windows.

Outro ataque frequente é a **falsificação de solicitação entre sites (CSRF – Cross-Site Request Forgery)**, também conhecida como **"Sea Surf"**. **Esse ataque ocorre quando um site legítimo confia nas requisições feitas pelo navegador de um usuário autenticado**. O invasor explora essa confiança induzindo a vítima a clicar em um link malicioso ou carregar uma página que faz solicitações automáticas em nome do usuário, sem seu conhecimento. Se bem-sucedido, o ataque pode ser usado para alterar configurações de conta, transferir dinheiro ou realizar outras ações sem que a vítima perceba. Para evitar esse tipo de exploração, muitas aplicações utilizam **tokens criptográficos** para validar cada requisição, garantindo que apenas comandos legítimos sejam processados.

Outro método de exploração é a **travessia de diretórios (directory traversal)**, **que explora falhas na configuração do servidor web para acessar arquivos e pastas que normalmente estariam protegidos**. Servidores corretamente configurados restringem o acesso dos usuários a um diretório específico, impedindo que naveguem por outras partes do sistema. No entanto, se houver uma falha na configuração ou vulnerabilidade no software do servidor, um invasor pode utilizar comandos como "../" para mover-se entre diretórios e acessar arquivos críticos do sistema.

Um indício comum de tentativa desse ataque pode ser encontrado nos logs do servidor, onde solicitações suspeitas incluem "../../windows/system.ini", demonstrando que alguém tentou acessar arquivos do sistema operacional diretamente pelo navegador. Esse tipo de exploração pode permitir que um invasor leia, altere ou até exclua arquivos críticos, comprometendo a segurança do servidor.

Diante dessas ameaças, é fundamental que aplicações e servidores sejam desenvolvidos e configurados seguindo boas práticas de segurança. Medidas como validação rigorosa de entradas, aplicação de patches de segurança, uso de criptografia forte e monitoramento contínuo da rede ajudam a reduzir os riscos e proteger sistemas contra ataques maliciosos.