1.Replay attacks

Os ataques de repetição (Replay Attacks) são uma vulnerabilidade de segurança em que um invasor intercepta e reutiliza transmissões de dados legítimas para obter acesso não autorizado a um sistema. Esse tipo de ataque é especialmente perigoso quando envolve detalhes sensíveis de autenticação.

Em uma transação de rede típica, um cliente envia dados para um servidor, e o servidor responde. Se um invasor capturar essa comunicação, ele poderá reproduzir os dados interceptados para se passar pelo usuário legítimo. Diversas técnicas podem ser usadas para interceptar esses dados, como o uso de um "tap" físico na rede, envenenamento de ARP (**ARP poisoning**) ou a instalação de malware no dispositivo da vítima. Uma vez capturados, os atacantes podem reutilizar tokens de autenticação, como senhas criptografadas (hashes), para obter acesso ao sistema.

Um exemplo desse ataque é a técnica "***Pass-the-Hash***", **em que o invasor captura senhas em formato hash durante o processo de autenticação e as reutiliza para acessar um sistema sem precisar da senha original**. Para mitigar esse risco, a criptografia é essencial. Ao criptografar corretamente o tráfego de rede, evita-se que invasores extraiam dados úteis. Além disso, a adição de um ***salt*** aos hashes de autenticação garante que cada tentativa de login gere um hash único, dificultando a reutilização das credenciais capturadas.