1.Ataques contra senhas

A segurança das credenciais de usuários é fundamental para a proteção de sistemas, e uma das maiores vulnerabilidades ocorre quando senhas são armazenadas **em texto claro** (plain text). Se um atacante conseguir acesso ao banco de dados ou arquivos que contêm essas informações, poderá obter todas as credenciais instantaneamente, comprometendo a segurança de toda a organização. Para evitar esse risco, senhas devem ser armazenadas utilizando **funções de hash**.

O hashing transforma uma entrada de tamanho variável em uma saída de tamanho fixo, conhecida como **impressão digital** (fingerprint). Diferentes entradas geram hashes distintos, e a principal vantagem desse método é a **irreversibilidade**, ou seja, não é possível calcular a senha original a partir do hash. Isso significa que, mesmo que um banco de dados seja comprometido, os atacantes não terão acesso direto às senhas dos usuários.

No entanto, ataques contra hashes ainda são possíveis. Muitos invasores utilizam **tabelas de correspondência pré-computadas**, conhecidas como **Rainbow Tables**, que contêm milhões de hashes gerados a partir de senhas comuns. Para mitigar esse risco, as senhas podem ser protegidas com **salt**, um valor aleatório adicionado antes de gerar o hash, tornando ataques desse tipo ineficazes.

Outra técnica amplamente utilizada por atacantes é o **ataque de pulverização (password spraying)**. **Em vez de tentar várias senhas para um único usuário, o invasor testa um número pequeno de senhas comuns em um grande conjunto de contas**. Isso evita bloqueios por tentativas excessivas e pode conceder acesso a contas protegidas por senhas fracas. Muitas pessoas ainda utilizam senhas previsíveis, como "123456", "password" ou "qwerty", facilitando esse tipo de ataque.

Se a pulverização não for eficaz, o atacante pode recorrer a um **ataque de força bruta, que testa todas as combinações possíveis de caracteres até encontrar a senha correta**. Esse processo pode ser extremamente demorado, mas a velocidade do ataque depende da força do algoritmo de hash utilizado e do comprimento da senha. Senhas curtas e sem complexidade podem ser quebradas rapidamente, enquanto senhas longas e aleatórias oferecem maior proteção.

Os ataques de força bruta são ainda mais perigosos quando os atacantes conseguem obter um arquivo de senhas hash e realizam o ataque **offline**, sem o risco de bloqueios automáticos do sistema. Uma vez em posse do arquivo, eles podem utilizar máquinas poderosas para testar milhões de combinações por segundo, sem restrições de tempo ou tentativas.

Para proteger sistemas contra essas ameaças, são recomendadas várias práticas de segurança, incluindo:

- **Exigir senhas fortes**, com combinações de letras maiúsculas e minúsculas, números e caracteres especiais.
- **Implementar políticas de bloqueio de conta**, para impedir ataques de força bruta.
- **Utilizar hashes seguros**, como bcrypt, PBKDF2 ou Argon2, que dificultam ataques de força bruta ao aumentar o tempo necessário para calcular cada hash.
- **Adicionar salt às senhas**, para evitar ataques baseados em Rainbow Tables.
- **Monitorar tentativas de login suspeitas**, identificando padrões de ataques antes que causem danos.

A segurança das credenciais depende da implementação correta dessas medidas, garantindo que senhas não possam ser facilmente exploradas por atacantes.