1.Introdução de ataques contra senhas

1.1 Ataques de senha

Quando um usuário escolhe uma senha, a senha é convertida em um hash usando uma função criptográfica, como MD5 ou SHA. Isso significa que, em teoria, ninguém, exceto o usuário (nem mesmo o administrador do sistema), conhece a senha, porque o texto simples não deve ser recuperável a partir do hash.

1.2 Ataque de texto simples/não criptografado

Um ataque de texto simples/não criptografado (plaintext/unencrypted attack) explora o armazenamento de senhas ou um protocolo de autenticação de rede que não usa criptografia. Esse tipo de ataque ocorre quando as senhas são transmitidas ou armazenadas em formato legível, sem qualquer forma de criptografia. Os atacantes podem interceptar ou acessar diretamente essas senhas.

Os exemplos incluem PAP, autenticação HTTP/FTP básica e Telnet. Esses protocolos não devem ser usados. As senhas nunca devem ser salvas em um arquivo não gerenciado. Um tipo comum de violação de credenciais são as senhas incorporadas no código do aplicativo que foram posteriormente carregadas em um repositório público.

2.Ataques online

Um ataque de senha online ocorre quando o agente da ameaça interage diretamente com o serviço de autenticação – um formulário de login na web ou gateway VPN, por exemplo. O invasor envia senhas usando um banco de dados de senhas conhecidas (e variações) ou uma lista de senhas que foram quebradas offline. Os ataques online envolvem tentativas automáticas e contínuas de login em uma conta, geralmente usando força bruta ou dicionário. Atacantes exploram a capacidade de realizar tentativas repetidas para encontrar a combinação correta de nome de usuário e senha. Uma forma de evitar esse tipo de ataque é implementando bloqueios automáticos após várias tentativas mal sucedidas, utilizar autenticação de dois fatores (2FA) e encorajar o uso de senhas fortes.

3.Pulverização de senhas

A pulverização de senhas é um ataque on-line horizontal de força bruta. Isso significa que o invasor escolhe uma ou mais senhas comuns (por exemplo, “senha” ou “123456”) e as testa em conjunto com vários nomes de usuário. Neste tipo de ataque, o invasor tenta poucas combinações de senhas em várias contas, evitando detecção automática. Ao limitar o número de tentativas por conta, os atacantes evitam bloqueios automáticos, tornando mais difícil a detecção de atividades suspeitas. Para tentar evitar este tipo de ataque monitore padrões de login, implemente bloqueios baseados em comportamento e utilize ferramentas de detecção de pulverização de senhas.

4.Ataques offline

Ataques offline envolvem a obtenção de informações de autenticação armazenadas localmente, como hashes de senhas, permitindo tentativas de quebra sem interação com o sistema alvo. Um invasor pode obter acesso a bancos de dados de senhas comprometidos e usar técnicas offline, como ataques de força bruta ou dicionário. Uma maneira de evitar esses ataques é armazenando senhas de maneira segura, utilizando técnicas de hash fortes e mantendo sistemas e bancos de dados protegidos contra acessos não autorizados.

Um ataque offline significa que o invasor conseguiu obter um banco de dados de hashes de senha. Uma vez obtido o banco de dados de senhas, o cracker não interage com o sistema de autenticação. O único indicador desse tipo de ataque (além do erro de conta no caso de um ataque bem-sucedido) é um log de auditoria do sistema de arquivos que registra a conta maliciosa que acessa um desses arquivos.

Os atores da ameaça também podem ler credenciais da memória do host; nesse caso, o único indicador confiável pode ser a presença de ferramentas de ataque em um host. Se o invasor não conseguir obter um banco de dados de senhas, um sniffer de pacotes poderá ser usado para obter a resposta do cliente a um desafio do servidor em um protocolo como NTLM ou CHAP/MS-CHAP. Embora esses protocolos evitem enviar o hash da senha diretamente, o ID da resposta derivou dela de alguma forma. Os crackers de senhas podem explorar os pontos fracos de um protocolo para calcular o hash e combiná-lo com uma palavra do dicionário ou forçá-lo com força bruta.

5.Ataques de força bruta

Alguns ataques de senha exploram credenciais fracas escolhidas pelos usuários. Outros podem explorar vulnerabilidades no mecanismo de armazenamento. Um ataque de força bruta tenta todas as combinações possíveis no espaço de saída para corresponder a um hash capturado e adivinhar o texto simples que o gerou. O espaço de saída é determinado pelo número de bits usados pelo algoritmo.

Quanto maior o espaço de saída e quanto mais caracteres forem usados na senha de texto simples, mais difícil será calcular e testar cada hash possível para encontrar uma correspondência. Os ataques de força bruta são fortemente limitados pelo tempo e pelos recursos computacionais e, portanto, são mais eficazes na quebra de senhas curtas. No entanto, ataques de força bruta distribuídos em vários componentes de hardware, como um cluster de placas gráficas de última geração, podem ter sucesso na quebra de senhas mais longas.

6.Ataques de dicionário

Ataques de força bruta tentam todas as combinações possíveis de senhas, enquanto ataques de dicionário usam uma lista de palavras comuns. Um ataque de dicionário pode ser usado onde há uma boa chance de adivinhar o valor provável do texto simples, como uma senha não complexa. O software gera valores de hash a partir de um dicionário de textos simples para tentar combinar um com um hash capturado.

Atacantes exploram a previsibilidade de senhas comuns ou sequências alfanuméricas, tentando exaustivamente todas as combinações. Uma forma de evitar é reforçando políticas de senhas, promovendo o uso de senhas complexas e implementando bloqueios automáticos após tentativas mal sucedidas.

7.Ataque híbrido

O ataque híbrido de senha usa uma combinação de ataques de dicionário e de força bruta. É direcionado principalmente contra senhas ingênuas com complexidade inadequada, como "james1". O algoritmo de quebra de senha testa palavras e nomes de dicionário em combinação com uma máscara que limita o número de variações a serem testadas, como a adição de prefixos e/ou sufixos numéricos.

Outros tipos de algoritmos podem ser aplicados, com base no que os hackers sabem sobre como os usuários se comportam quando são forçados a selecionar senhas complexas que eles realmente não querem que sejam difíceis de lembrar. Outros exemplos podem incluir a substituição de “s” por “S” ou “o” por “0”. Ataques híbridos otimizam a eficácia do ataque. Os atacantes buscam equilibrar a eficiência de um ataque de força bruta com a previsibilidade de padrões de senha comuns.

Para inibir essas ações incentive a criação de senhas únicas e complexas, além de utilizar bloqueios automáticos e monitoramento proativo contra padrões de ataque híbridos.