Técnicas para quebrar uma senha

Na fase de enumeração de um pentest, foram coletadas diversas informações sobre o alvo, incluindo usuários. Estes usuários são importantes nesta fase porque eles te dão uma visão em que se deve focar durante o ataque a um sistema. Use a quebra de senhas para obter credenciais de uma conta com a intenção de usar esta conta para ganhar acesso autorizado ao sistema com um usuário legítimo.

De forma resumida, a quebra de senha é o processo de recuperar senhas transmitidas ou armazenadas como dados. Desta forma, um invasor pode recuperar e usar uma senha extraviada ou esquecida. Administradores de sistemas pode usar este processo para auditar e testar por brechas em um sistema para avaliar a força delas e os invasores poderão fazer este processo para tentar causar prejuízos.

Tipicamente, o processo de invasão inicia-se com as senhas, pois elas podem ser quebradas ou auditadas usando técnicas manuais ou automatizadas com a intenção de revelar as credenciais.

Antes de continuar falando sobre a quebra de senha, temos que entender o que é uma senha. A senha foi feita para ser algo que um indivíduo possa lembrar facilmente mas ao mesmo tempo não ser fácil de ser adivinhada ou quebrada. É onde o problema reside, pois o ser humano tende a escolher senhas fáceis de lembrar, o que as tornam fáceis de adivinhar.

Veja alguns exemplos de senhas que são fáceis de serem quebradas:

- Somente com números;
- Somente com letras;
- Totalmente com letras maiúsculas ou minúsculas;

- Nomes próprios;
- Palavras de dicionário;
- Senhas curtas (menor que oito caracteres);

De forma geral, se você seguir as regras para se criar senhas fortes, você já terá uma linha de defesa contra ataques que iremos ver a seguir. Muitas empresas adotam estas regras no formulário de senhas como um requisito de complexidade da senha.

Empresas possuem uma política de senhas ou um documento que guia como criar uma senha segura, que dizem para evitar características semelhantes a estas:

- Com letras, caracteres especiais e números: sdjr#36
- Somente números: 984583725
- Somente caracteres especiais: @%*@$&@#(&
- Somente números e letras: quret15
- Somente com letras: PHITLY
- Somente letras e caracteres especiais: r@x#t@g
- Somente caracteres especiais e números 2794!*5

O usuário que escolhe uma senha que seja semelhante aos padrões mostrados acima, estão mais vulneráveis às técnicas de recuperação de senhas que veremos a diante.

Técnicas de quebra de senhas

Ataque de dicionário

É uma forma de pegar uma lista de palavras conhecidas e possíveis senhas em um software que irá testar cada uma delas para tentar recuperar a senha. Sistemas que usam *passphrases* normalmente não são vulneráveis a este tipo de ataque.

Ataque de força bruta

Neste ataque, tenta-se várias combinações de caracteres até achar a senha correta.

Ataque híbrido

Esta forma de ataque usa dicionário com alguns passos adicionais como parte do processo. Na maioria dos casos, significa dizer que as senhas tentadas durante o ataque de dicionário são modificadas com a adição ou substituição de caracteres especiais e números, como *P@ssw0rd* ao invés de *Password*.

Ataque das sílabas

É uma combinação de força bruta e o ataque de dicionários, mas é útil quando a senha usada não é baseada em uma palavra ou senha.

Ataque baseada nas regras

Pode ser considerado um ataque avançado. Assume-se que o usuário criou uma senha usando informações que o invasor conheça, como tendência de palavras ou dígitos que o usuário usa.

Ataques passivos online

Ataques desta categoria são realizadas somente aguardando e ouvindo, neste caso, através da tecnologia, usando ferramentas de sniffing como o Wireshark, ataques man-in-the-middle ou replays attacks.

Ataques ativos online

Este tipo é mais agressivo que o passivo, pois o processo requer um engajamento maior com o alvo. Nos casos de senhas fracas ou pobres, ataques ativos são efetivos. Formas deste ataque incluem adivinhação de senha, trojan/spyware/key loggers, injeção de hash e phishing.

Ataques offline

Este tipo de ataque foi feito para atacar não a fraqueza da senha, mas da forma que ela foi armazenada. Como as senhas são armazenadas em algum formato, o atacante procura obte-las onde elas estão armazenadas, explorando a segurança fraca ou uma brecha do sistemas. Se as credenciais forem armazenadas no formato de texto puro ou de forma não criptografada, o invasor irá obter as credenciais. Formas deste ataque incluem hashes precomputados, ataques distribuídos na rede e ataques rainbow.

Ataques não tecnológicos

Este ataque sai do mundo da tecnologia para o mundo real. Uma característica deste ataque é que não precisa de nenhum conhecimento técnico. Formas de ataques incluem o shoulder surfing (olhar por cima dos ombros), engenharia social e dumpster diving (vasculhar os lixos).

Sugestões de livros: