ManageEngine
ADSelfService Plus

Frustrando os hackers com melhores políticas de senha do Active Directory

Frustrando os hackers com melhores políticas de senha do Active Directory

A invasão de senhas é a maneira mais fácil de obter acesso a uma conta de usuário no Active Directory. Há anos, os hackers conseguem comprometer facilmente as senhas dos usuários do Microsoft Active Directory. Isso não é nenhuma surpresa, considerando que a política de senhas e seu controle no Active Directory não foram alterados desde 2000. A segurança era muito diferente há vinte anos, e é hora de considerar a possibilidade de melhorar os controles e o ambiente da política de senhas do Active Directory para impedir os hackers.

Estratégias de invasão de senhas

Em geral, as tecnologias de invasão de senhas não mudaram muito nos últimos 15 anos. Isso se deve ao fato de que os controles sobre as senhas não mudaram. A Microsoft não forneceu nenhum controle de senha adicional no Active Directory desde a sua criação em 2000. Portanto, as estratégias e tecnologias atuais dos hackers ainda funcionam em um usuário do Active Directory do Windows Server 2012 R2, da mesma forma que em um domínio do Active Directory do Windows 2000 Mixed Mode.

A maioria das ferramentas de quebra de senha usa a mesma lógica como base para a obter. Primeiro, o invasor deve obter o hash da senha. O hash da senha é um algoritmo matemático que converte a senha em uma cadeia alfanumérica, que não é reversível de volta à senha. Esse hash é gerado pelo sistema operacional, nesse caso, o Active Directory. O hash é armazenado no banco de dados do Active Directory e também é armazenado no banco de dados de segurança do computador cliente quando o usuário faz login. Ele é necessário para autenticar o usuário à medida que ele obtém acesso a recursos em toda a rede. O invasor pode obter o hash do banco de dados do Active Directory, do computador cliente local ou de pacotes de autenticação.

Em segundo lugar, um conjunto de caracteres é escolhido a partir do qual um hash é calculado. Esse conjunto pode ser escolhido em um dicionário ou por meio da especificação de parâmetros como caracteres, tamanho mínimo e máximo da senha. Por fim, o hash obtido pela primeira etapa é comparado com o hash gerado pela segunda etapa. Se os hashes forem iguais, a senha será conhecida como o conjunto de caracteres que gerou o hash correspondente.

Ataques de dicionário

Um ataque de dicionário usa uma lista definida de palavras de um arquivo de dicionário como base para a invasão. Na maioria dos casos, há muitos dicionários usados em um ataque contra hashes de senha. Esses dicionários podem ser dicionários de idiomas normais ou de hackers. Os dicionários de hackers geralmente pegam os de idiomas normais e adicionam palavras que usam substituições de caracteres. Veja exemplos na Figura 1.

Palavra do dicionário de idiomas	Palavras do dicionário Hacker		
password	Pa$$word	P@55w0rd	p@$$w0rD
admin	@dmin	@Dm1n	Adm!N
american	Am3R!c@n	amEr1c@N	@m3r1c@n

Figura 1. Exemplos de palavras que podem estar em dicionários de hackers.

Como os parâmetros dessas palavras seguem os das que já existem, os ataques de dicionário são mais rápidos do que outros tipos de ataques.

Ataques de força bruta

Um ataque de força bruta usa uma sequência lógica de caracteres para desenvolver hashes que, em seguida, são comparados com o(s) hash(s) da senha obtido(s). Em vez de usar uma lista de palavras, como em um ataque de dicionário, os ataques de força bruta usam todas as combinações possíveis de caracteres, com comprimentos de caracteres especificado, que incluem alfa minúsculo, alfa maiúsculo, numérico e especial (a, A, 1, $). Para o comprimento da senha, é usado um único caractere ou mais (Cain & Abel, a popular ferramenta de recuperação de senhas, por exemplo, tem um comprimento máximo de senha de 32 caracteres). Por exemplo, se apenas letras minúsculas forem usadas em um ataque de força bruta, e o comprimento mínimo da senha for dois e o máximo for três, a Figura 2 seria exemplos de senhas que, por sua vez, desenvolveriam hashes para comparação.

aa	ba
ab	bb
ac	bc
…	…
ax	bx
ay	by
az	bz
…	…
aaa	baa
aab	bab

Figura 2. Uma amostra de senhas que são usadas em ataques de força bruta.

Assim como em qualquer ataque de senha, os hashes resultantes das combinações de caracteres serão comparados com os adquiridos. Se houver uma correspondência, a senha será conhecida.

Ataque de tabela arco-íris

Os ataques de tabela arco-íris são a próxima geração de ataques de força bruta. Os ataques de força bruta exigem que o invasor defina um espaço de caracteres (a, A, 1 e/ou $) juntamente com os comprimentos das senhas. Cada vez que um deles é tentado, as mesmas combinações de caracteres e os hashes resultantes são produzidos. Em vez de gastar tempo para produzir os mesmos hashes todas as vezes, uma tabela arco-íris armazena os hashes em cache. Agora, em vez de dedicar tempo para desenvolver o hash, é possível fazer uma comparação simples com a tabela de hash com os já capturados. Isso pode levar muito menos tempo, alguns estimam cerca de um décimo do tempo dos ataques de força bruta.

Ataques padrão

Os ataques padrão exploram características que são comumente encontradas na senha de um usuário típico. Por exemplo, os usuários gostam de usar senhas consecutivas quando alteram suas senhas. Isso facilita a memorização. As senhas consecutivas seriam Senha1, Senha2, Senha3, etc.

Outro padrão é que os usuários geralmente iniciam a senha com um caractere alfa maiúsculo. Isso também facilita a memorização, pois começamos as frases com uma letra maiúscula. Por fim, outro padrão é que, quando os usuários são forçados a usar três dos quatro tipos de caracteres (a, A, 1, $), eles geralmente usam todos, exceto os caracteres especiais.

Conhecer esses padrões permite que o invasor desenvolva ataques que aproveitem os padrões, reduzindo, por sua vez, o tempo necessário para hackear a senha.

Políticas de senha

A política de senha de um sistema operacional contém controles que um usuário deve seguir ao criar sua senha. Por exemplo, será necessário que a senha tenha um número mínimo e um número máximo de caracteres. A composição da política de senha deve ajudar na defesa contra os ataques de senha conhecidos e as vulnerabilidades da senha e de seu hash. Infelizmente, esse não é o caso na maioria das situações.

O motivo pelo qual a maioria das soluções e implementações de políticas de senhas tem controles insuficientes para proteger contra ataques de senhas conhecidos geralmente se deve às limitações do usuário final. Uma senha longa, forte e complexa não é o que a maioria dos usuários deseja e pode fazer diariamente. Como solução de compromisso, as empresas permitem que os usuários digitem senhas curtas, fracas e um pouco complexas. Essas senhas geralmente são fáceis de serem hackeadas.

O ideal é que se tenha controles que combatam os ataques de senhas conhecidos e, ao mesmo tempo, ofereça ao usuário a flexibilidade de ter uma senha que ele possa lembrar. A seguir, examinaremos as soluções de política de senha da Microsoft e, em seguida, um complemento da ManageEngine.

Política de senha da Microsoft

A Microsoft oferece duas maneiras de implementar a política de senha para os usuários do domínio do Active Directory. Uma delas é por meio da Política de Grupo e a outra é por meio de políticas de senha refinadas (FGPPs). Independentemente da tecnologia de implementação utilizada, os mesmos controles estão disponíveis, que incluem o seguinte:

- Aplicação do histórico de senhas
- Idade máxima da senha
- Idade mínima da senha

- Comprimento mínimo da senha
- A senha deve atender aos requisitos de complexidade
- Armazenamento de senhas usando criptografia reversível

Esses controles estão em vigor desde o início do Windows Active Directory, em 2000. Essas configurações provaram ser inferiores em uma tentativa de proteger as senhas contra tecnologias de hacking. O padrão de uma senha com comprimento mínimo de sete caracteres é fraco e não oferece o nível de controle necessário para combater as tecnologias de quebra de senha. A configuração dos requisitos de complexidade também é limitada em termos de amplitude e eficácia. Os requisitos de complexidade da Microsoft são definidos da seguinte forma:

- A senha não deve conter o nome da conta do usuário ou partes do nome completo do usuário que excedam dois caracteres consecutivos.
- A senha deve ter pelo menos seis caracteres de comprimento
- A senha deve conter caracteres de três das quatro categorias a seguir:
    - Caracteres em caixa alta (de A a Z)
    - Caracteres em minúsculas (de a a z)
    - Dígitos de base 10 (0 a 9)
    - Caracteres não alfabéticos (por exemplo, !, $, #, %)

A defesa contra ataques de dicionário, força bruta, tabela arco-íris e padrão não é abordada pela Microsoft em seus controles de política de senha.

Política de senha implementada por meio da Política de Grupo

A base do Active Directory é uma política de senha que controla todas as senhas de contas de usuários do domínio. Essa política de senha, por padrão, é configurada no objeto de política de grupo de domínio padrão (GPO). Esse GPO está vinculado ao nó de domínio do Active Directory. Há alguns detalhes que precisam ser explicados sobre a política de senha para usuários do domínio que é implementada usando a Política de Grupo:

1. A política de senha não precisa ser configurada na Política de domínio padrão
2. A política de senha deve ser configurada em um GPO vinculado ao domínio.
3. Os controles da política de senha serão implementados a partir do(s) GPO(s) vinculado(s) ao domínio com a maior precedência para cada controle.
4. Os GPOs que contêm configurações de controle de política de senha vinculados a unidades organizacionais (OUs) não afetam os usuários do domínio.

O resultado desses detalhes referentes à política de senha baseada em GPO é que só pode haver uma única política de senha para todos os usuários do domínio. Não há como usar a Política de Grupo para ter várias políticas de senha em um único domínio do Active Directory.

Política de senha implementada via FGPP

A partir do Windows Server 2008, a Microsoft adicionou outra tecnologia de política de senha chamada FGPPs (fine-grained password policies). Em vez de usar a Política de Grupo para implementar a política de senha, a Microsoft decidiu usar uma abordagem de objeto do Active Directory. Os controles da política de senha são praticamente os mesmos, mas as FGPPs oferecem esses aspectos adicionais:

- Precedência de cada FGPP em relação ao outro (de modo que apenas um FGPP possa ser aplicado a cada usuário)
- Aplicação de cada FGPP a um ou mais grupos de segurança

O resultado dessa abordagem às políticas de senha é que pode haver mais de uma política de senha no mesmo domínio do Active Directory. Qualquer usuário que seja membro de um grupo associado a um FGPP receberá o de maior precedência aplicável a cada usuário. Se um usuário não for membro de um grupo associado, ele receberá a política de senha implementada por meio da Política de Grupo.

Política de senha implementada por meio do ADSelfService Plus

Como as soluções de política de senhas da Microsoft não protegem as senhas, é necessário que haja uma solução que funcione com o Active Directory e com as políticas de senhas baseadas em Group Policy/FGPP que faça isso. O ADSelfService Plus foi projetado para proteger contra os ataques de senhas mais recentes e é implementado usando o design atual da UO do Active Directory.

O ADSelfService Plus fornece aprimoramentos às soluções de política de senhas da Microsoft, permitindo diferentes aprimoramentos de política de senhas em um único domínio do Active Directory. Os aprimoramentos da política de senhas funcionam perfeitamente com as configurações da política de senhas do Windows para melhorar as partes essenciais para suas necessidades. Veja a seguir os recursos do ADSelfService Plus com relação às senhas de usuários do Active Directory:

- Diferentes aprimoramentos da política de senhas em um único domínio
- Fornece implementação sobre associação a grupos ou locais de usuários na OU
- Os dicionários podem ser importados para impedir o uso dessas palavras como senhas
- Controles de padrão de senha (incremental, omissão de caracteres especiais, palíndromos, etc.)
- A política de senhas é aplicada por meio do portal da Web e da aplicação móvel do ADSelfService Plus.
- A política de senha é aplicada por meio da tela Ctrl+Alt+Del Alterar senha

- A política de senha é aplicada quando o administrador redefine a senha do usuário final nos usuários e computadores do Active Directory

O ADSelfService Plus oferece um ambiente fácil de configurar e gerenciar para suas políticas de senha do Active Directory, conforme mostrado na Figura 3. A arquitetura da política de senha do ADSelfService Plus é um aprimoramento da política de senha existente do Microsoft Group Policy e/ou FGPP. Se um usuário não tiver uma política de senha do ADSelfService Plus associada a ele (por meio de associação a grupo ou OU), somente a política de senha, baseada em FGPP ou Política de Grupo, será aplicada ao usuário. Isso proporciona uma maneira simples e eficaz de implementar controles adicionais sobre as senhas, sem a necessidade de rearquitetar o ambiente atual do Active Directory.

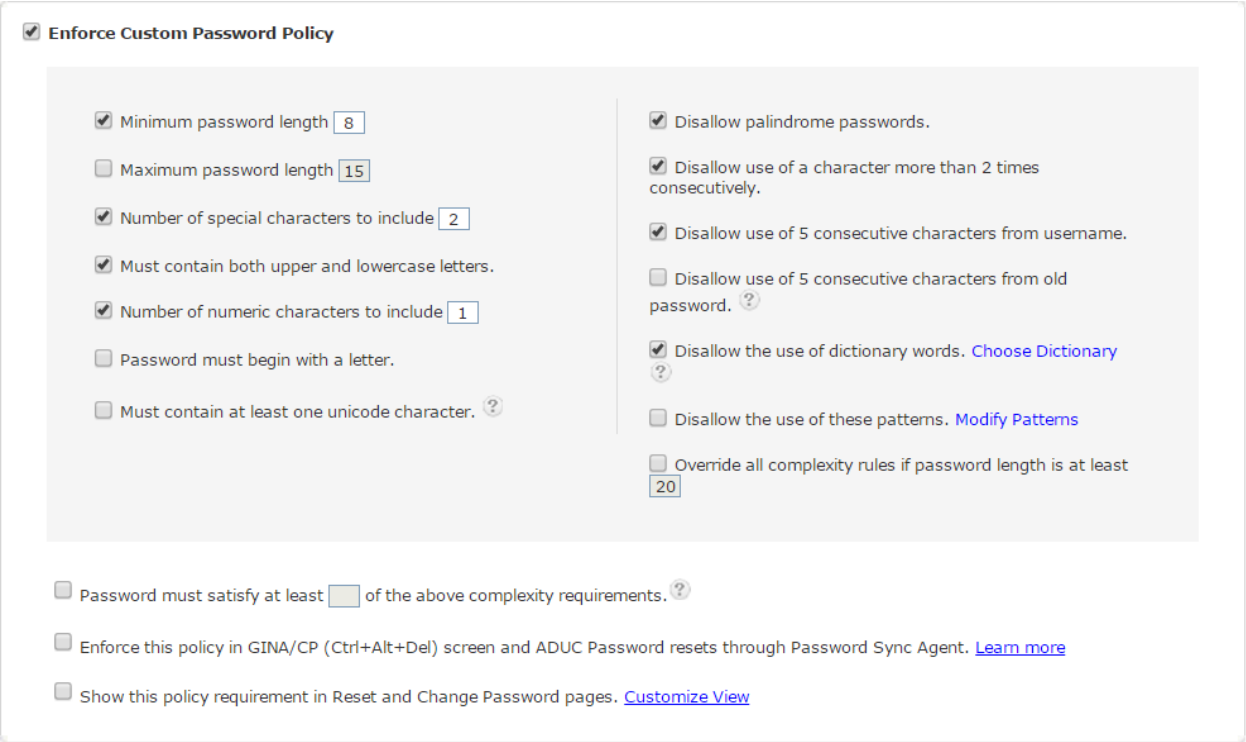

Figura 3. Controles de aprimoramento da política de senhas do ADSelfService Plus.

Com a capacidade de importar um ou mais dicionários para os controles da política de senhas, você pode se defender contra ataques de dicionário. Os controles de padrão de senha no ADSelfService Plus oferecem segurança aos seus usuários, impedindo-os de usar erros comuns de padrão de senha. Esses controles oferecem segurança adicional para aprimorar as senhas dos usuários do Active Directory contra ataques de senhas comuns.

Resumo

Estamos sendo atacados! No entanto, a Microsoft não forneceu nenhum controle adicional de política de senha para ajudar a proteger os usuários do Active Directory. Sem alguma ajuda e tecnologias adicionais, não haverá o suficiente para proteger suas senhas. A Política de Grupo e as políticas de senha implementadas pelo FGPP não fornecem os controles de senha necessários. Somente o FGPP fornece mais de uma política de senha para um único domínio, mas os controles são distribuídos por meio da associação ao grupo, nem mesmo pelo local da OU. Essas limitações são significativas e impedem que você proteja suas senhas.

O ADSelfService Plus oferece uma solução sofisticada que proporciona às senhas dos usuários do domínio do Active Directory a proteção necessária. A capacidade de ter várias políticas de senha em um único domínio distribuído por meio de associação a grupos de usuários ou OU é essencial para a maioria das instalações do Active Directory. A capacidade de ter controles para proteger contra ataques de dicionário e de padrão de senha também é necessária para ajudar a reduzir os ataques contra esses pontos fracos das senhas. O ADSelfService Plus é uma solução fácil de implementar, fácil de configurar, fácil de gerenciar e segura para qualquer domínio do Active Directory.

Se precisar de assistência, por favor, entre em contato
support@adselfserviceplus.com

Ligação gratuita
+1-408-916-9890 (Direct)

Visite www.adselfserviceplus.com

ManageEngine
ADSelfService Plus

100% FREE FOR 50 USERS

O ADSelfService Plus é um programa de gerenciamento de redefinição de senha seguro, baseado na Web, para usuários finais. Esse software ajuda os usuários do domínio a realizar a redefinição de senha de autoatendimento, o desbloqueio de conta de autoatendimento e a autoatualização de detalhes pessoais (por exemplo, números de telefone ,etc.) no Microsoft Windows Active Directory. Os administradores acham fácil automatizar a redefinição de senhas e o desbloqueio de contas e, ao mesmo tempo, gerenciar e otimizar as despesas associadas às chamadas de helpdesk.

$ Obter orçamento Download