ManageEngine
ADSelfService Plus

Thwarting hackers with better Active Directory password policies

Thwarting hackers with better Active Directory password policies

Hacking passwords is the easiest way to gain access to a user account in Active Directory. Hackers have been able to easily compromise the passwords of Microsoft Active Directory users for years. This is no surprise, considering the password policy and password controls in Active Directory have not been changed since 2000. Security was much different seventeen years ago, and it's time to consider improving your Active Directory password policy controls and environment to thwart hackers.

Password hacking strategies

In general, password hacking technologies have not changed much over the past 15 years. This is due to the fact that the controls over passwords have not changed. Microsoft has not provided any additional password controls in Active Directory since its inception in 2000. Therefore, current hacker strategies and technologies still work on a Windows Server 2012 R2 Active Directory user, just as they did on a Windows 2000 Mixed Mode Active Directory domain.

Most password cracking tools use the same logic as the foundation for obtaining the password. First, the attacker must obtain the password hash. The password hash is a mathematical algorithm that converts the password to a alphanumeric string, which is not reversible back to the password. This hash is generated by the operating system, in this case Active Directory. The hash is stored in the Active Directory database and is also stored in the security database on the client computer when the user logs in. The hash is needed to authenticate the user as they gain access to resources throughout the network. The attacker can obtain the hash from the Active Directory database, the local client computer, or from authentication packets.

Second, a set of characters is chosen from which a hash is calculated. This set of characters can be chosen from a dictionary, or chosen by specifying parameters such as characters, minimum password length, and maximum password length. Finally, the hash obtained by the first step is compared to the hash generated by the second step. If the hashes match, the password is known as the set of characters that generated the matching hash.

Dictionary attacks

A dictionary attack takes a set list of words from a dictionary file as the foundation for the hack. In most cases, there are many dictionaries used in an attack against password hashes. These dictionaries might be normal language dictionaries or hacker dictionaries. Hacker dictionaries usually take normal language dictionaries and addl words that use character replacements. See Figure 1 for examples.

Language dictionary word	Hacker dictionary words		
password	Pa$$word	P@55w0rd	p@$$w0rD
admin	@dmin	@Dm1n	Adm!N
american	Am3R!c@n	amEr1c@N	@m3r1c@n

Figure 1. Examples of words that might be in hacker dictionaries.

Since the parameters of these words follows those of words that already exist, dictionary attacks are faster than other types of attacks.

Brute force attacks

A brute force attack uses a logical sequence of characters to develop hashes which are then compared to the password hash(es) that are obtained. Instead of using a list of words, like a dictionary attack, brute force attacks use every possible combination of characters, with specified lengths of characters. The possible characters used in a brute force attack include lowercase alpha, uppercase alpha, numeric, and special (a, A, 1, $). For password length, anywhere from a single character on up is used (Cain & Abel, the popular password recovery tool, for example, has a maximum password length of 32 characters). For example, if only lower case alphas are used in a brute force attack, and the minimum password length is two and the maximum is three, Figure 2 would be examples of passwords that would in turn develop hashes for comparison.

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

Figure 2. A sample of passwords that are used in brute force attacks.

Just like any password attack, the resulting hashes from the character combinations will be compared to the hashes that are acquired. If there is a match, the password is known.

Rainbow table attacks

Rainbow table attacks are the next generation of brute force attacks. Brute force attacks require the attacker to define a character space (a, A, 1, and/or $) along with password lengths. Each time a brute force attack is attempted, the same character combinations and resulting hashes are produced. Instead of taking the time to produce the same hashes each time, a rainbow table caches the hashes. Now, instead of taking the time to develop the hash, a simple comparison can be done with the hash table to the captured hashes. This can take much less time, some estimate about one tenth the time of brute force attacks.

Pattern attacks

Pattern attacks exploit characteristics that are commonly found in the typical user's password. For instance, that users like to use consecutive passwords when they change their password. This makes it easier for them to remember. Consecutive passwords would be Password1, Password2, Password3, etc.

Another pattern is that users will typically start their password with an uppercase alpha character. This again makes it easier for them to remember, as we start sentences with an uppercase letter. Finally, another pattern is that when users are forced to use three of the four types of characters (a, A, 1, $), they will usually use all but the special characters.

Knowing these patterns lets the attacker develop attacks that will take advantage of the patterns, in turn reducing the time needed to hack the password.

For more detailed information on the capabilities of hacking password hashes using patterns, please refer to this whitepaper from NTT-Group.

Password policies

The password policy for an operating system contains controls a user must adhere to when creating their password. For example, the password will be required to have a minimum number and maximum number of characters. The makeup of the password policy should help defend against the known password attacks and vulnerabilities for the password and its hash. This is unfortunately not the case in most situations.

The reason most password policy solutions and implementations have insufficient controls to protect against known password attacks is usually due to end user limitations. A long, strong, complex password is not what most users are willing and able to deal with on a daily basis. As a compromise, corporations allow users to input short, weak, and somewhat complex passwords. These passwords are often easy to hack.

Ideally, the password policy should have controls that combat the known password attacks, while still giving the user the flexibility to have a password they can remember. Below we look at the Microsoft password policy solutions and then an add on from ManageEngine.

Microsoft password policy

Microsoft provides two ways to implement the password policy to Active Directory domain users. One is through Group Policy and the other is through fine-grained password policies (FGPPs). Regardless of the implementation technology you use, the same controls are available. The controls for the Microsoft password policy solutions include the following:

- Enforce password history
- Maximum password age
- Minimum password age

- Minimum password length
- Password must meet complexity requirements
- Store passwords using reversible encryption

These controls have been in place since the onset of Windows Active Directory back in 2000. These settings have proven to be inferior in an attempt to secure passwords against hacking technologies. The default of a seven character minimum length password is weak and does not provide the level of control needed to combat password-cracking technologies. The setting for complexity requirements is also limited in breadth and effectiveness. The complexity requirements by Microsoft are defined as the following:

- The password must not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- The password must be at least six characters in length
- The password must contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example !, $, #, %)

Defending against dictionary, brute force, rainbow table, and pattern attacks is not addressed by Microsoft in their password policy controls.

Password policy implemented via Group Policy

At the foundation of Active Directory is a password policy that controls all domain user account passwords. This password policy, by default, is configured in the Default Domain Policy Group Policy Object (GPO). This GPO is linked to the Active Directory domain node. There are a few details that need to be explained regarding the password policy for domain users that is implemented using Group Policy:

1. The password policy does not need to be configured in the Default Domain Policy
2. The password policy must be configured in a GPO that is linked to the domain
3. The password policy controls will be implemented from the GPO(s) linked at the domain with the highest precedence for each control
4. GPOs containing password policy control settings linked to organizational units (OUs) do not affect domain users

The result of these details regarding the GPO-based password policy is that there can only be a single password policy for all domain users. There is no way to use Group Policy to have multiple password policies in a single Active Directory domain.

Password policy implemented via FGPP

Starting with Windows Server 2008, Microsoft added another password policy technology called fine-grained password policies (FGPPs). Instead of using Group Policy to implement the password policy, Microsoft instead decided to use an Active Directory object approach. The controls for the password policy are nearly the same, but FGPPs do provide these additional aspects:

- Precedence of each FGPP in relation to one another (so that only one FGPP can apply to each user)
- Application of each FGPP to one or more security groups

The outcome of this approach to password policies is that there can be more than one password policy in the same Active Directory domain. Any user having membership in a group which is associated with an FGPP will receive the highest precedence FGPP applying to each user. If a user is not a member of a group that is associated with a FGPP, the user will receive the password policy which is implemented through Group Policy.

Password policy implemented via ADSelfService Plus

Since the Microsoft password policy solutions fail to secure passwords, there needs to be a solution that works with Active Directory and the Group Policy/FGPP based password policies that does protect your Active Directory passwords. ADSelfService Plus is designed to protect against the most recent passwords attacks and is implemented using your current Active Directory OU design.

ADSelfService Plus provides enhancements to the Microsoft password policy solutions, allowing for different password policy enhancements in a single Active Directory domain. The password policy enhancements seamlessly work with the Windows password policy settings to enhance the portions of the password essential for your needs. The following are features of ADSelfService Plus with regard to Active Directory user passwords:

- Different password policy enhancements in a single domain
- Provides implementation over group membership or user locations in OU
- Dictionaries can be imported to negate the use of these words as passwords
- Password pattern controls (incremental, omitting of special characters, palindromes, etc.)
- The password policy is enforced through ADSelfService Plus's web portal and mobile application
- The password policy is enforced through the Ctrl+Alt+Del Change Password screen

- The password policy is enforced when the administrator resets the end user password from within Active Directory users and computers

ADSelfService Plus provides an easy to configure and manage environment for your Active Directory password policies, as shown in Figure 3. The ADSelfService Plus password policy architecture is an enhancement to the existing Microsoft Group Policy and/or FGPP password policy. If a user does not have a ADSelfService Plus password policy associated with them (via group membership or OU), only the password policy, either FGPP or Group Policy-based, will apply to the user. This provides a simple and effective way to implement additional controls over your passwords, without needing to re-architect your current Active Directory environment.

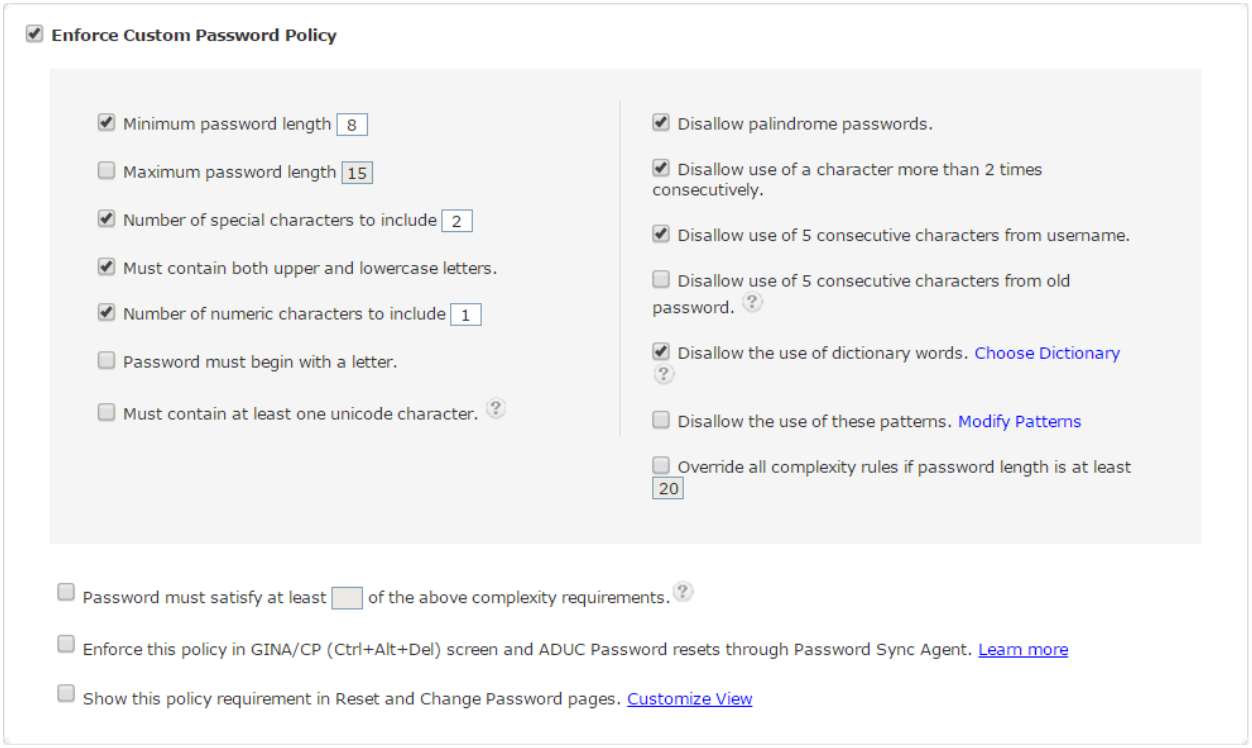

Figure 3. ADSelfService Plus password policy enhancement controls.

With the ability to import one or more dictionaries into your password policy controls, you are able to defend against dictionary attacks. The password pattern controls in ADSelfService Plus provide security for your users, preventing them from using common password pattern mistakes. These controls provide additional security to enhance your Active Directory users' passwords against common password attacks.

Summary

We are under attack! However, Microsoft has not provided any additional password policy controls to help protect your Active Directory users' passwords. Without some additional help and technologies in place, there won't be enough to protect your passwords. Group Policy and FGPP-implemented password policies do not provide the needed password controls. Only FGPP provides more than one password

policy for a single domain, but the controls are distributed via group membership, not even the OU location. These are significant limitations, and prevent you from protecting your passwords.

ADSelfService Plus provides a sophisticated solution that gives your Active Directory domain users' passwords the protection needed. The ability to have multiple password policies in a single domain distributed through user group membership or OU is essential for most Active Directory installations. The ability to have controls to protect against dictionary and password pattern attacks is also required to help reduce attacks against these password weaknesses. ADSelfService Plus is an easy to implement, easy to configure, easy to manage, and secure solution to any Active Directory domain.

If you need assistance, please contact
support@adselfserviceplus.com

Dial Toll Free:
+1-408-916-9890 (Direct)

Visit www.adselfserviceplus.com

ManageEngine
ADSelfService Plus *Starts @ $595*

ManageEngine ADSelfService Plus is a secure, web-based, end-user password reset management program. This software helps domain users to perform self service password reset , self service account unlock and employee self update of personal details(e.g telephone numbers,etc) in Microsoft Windows Active Directory. Administrators find it easy to automate password resets, account unlocks while managing optimizing the expenses associated with helpdesk calls.

$ Get Quote Download