Gautam, Deepak

Deepak.gautam@hpe.com

Abstract

The following automation is to reset and maintain Active Directory users expired password based on their password expiry date. Automation involves sending multiple reminders to reset password via email before their password expiry date and if required, do it automatically by sending a random password to users on the password expiry date. This will minimize the efforts involved of multiple Wintel engineers to reset password of different accounts each day.

Password Reset Automation

High Level Explanation

High Level Explanation of Password Reset Automation

**Database: -**

“Display Name”, “SamAccountName”, “mail”, “PasswordLastSet”, “Expiry\_Date”, “PwdReminder15” , “PwdReminder7”, “PwdReminder3”, “PwdReminder2”, “PwdReminder1”, “pwd\_expiry\_email”, “ExpReminder25”, “ExpReminder55”, “Disable\_date”

* Script will run daily based on a scheduled task on any of the DC or member server (with RSAT tools installed).
* Script will identify users where password is going to expire in next 15 days, expiring today, already expired but it's been less than 60 days, and already expired but it's been more than 60 days since password expiry.
* This information is matched against with current database and missing entries or changed information is updated.
* Users where password is expiring in next 15 days will be sent an email along with instructions on how to reset the password and current date is updated in PwDreminder15 field of database.
* Similarly, password expiring reminder will be sent at 7th, 3rd, 2nd and last day before the password expiry date and each corresponding field PwDreminder7, PwDreminder3, PwDreminder2, PwDreminder1 will be updated respectively.
* On the date of password expiry, an email with random password and instructions to reset password is sent to the user and current date is updated in pwd\_expiry\_email field of database.
* Users where password has expired but it's been less than 60 days, reminder will be sent at 25 and 55 and corresponding ExpReminder25 and ExpReminder55 fields are updated respectively.
* After 60 days of expired password, user account will be disabled following ITSM process and Disable\_date field is updated in database.
* Apart from csv database, there will be another pwd\_reset.log maintained for the script.

**Note-**

1. Database entries are set to overwrite as to keep the size of csv database as minimum as possible.

2. pwd\_reset.log will also keep a tab of emails sent to each user with their respective dates.

3. Script will save the O365 mailbox password in an encrypted (AES 256 Bit) file only to be decrypted at runtime and cleared from the memory afterwards.

4. No additional passwords are saved or required by the script.

**Deployment-**

1. Script must be copied to C:\windows\system32\Passwordexpiry.ps1.

2. Once we double click on it, it will setup a scheduled task to run at 8 AM every day in context of "NT Authority/SYSTEM".