


FEBRUARY 10, 2020

Credential Access – Password Filter DLL

 by Administrator. In Credential Access. Leave a Comment

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:

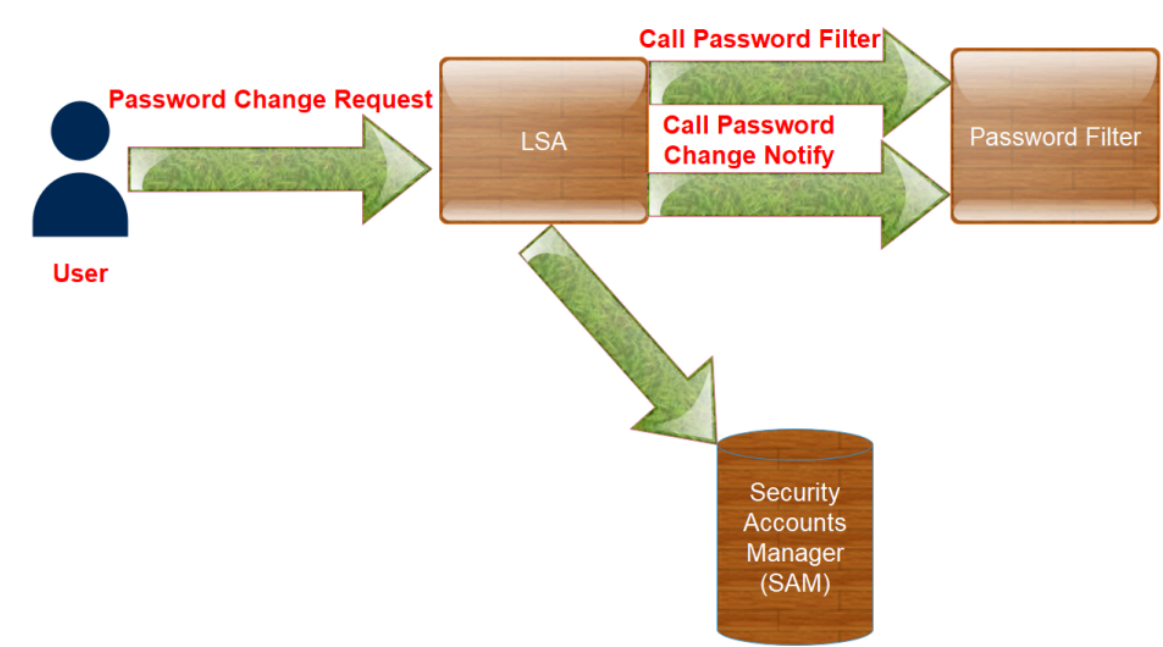
1. Password Filter DLL should be dropped into C:\Windows\System32
2. Registry key modification to register the Password Filter DLL
3. System reboot to load the password filter DLL into the LSASS process

Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to day job and by students and lecturers in academia. If you have benefit by the content all these years and you would like to support us on the maintenance costs please consider a donation.

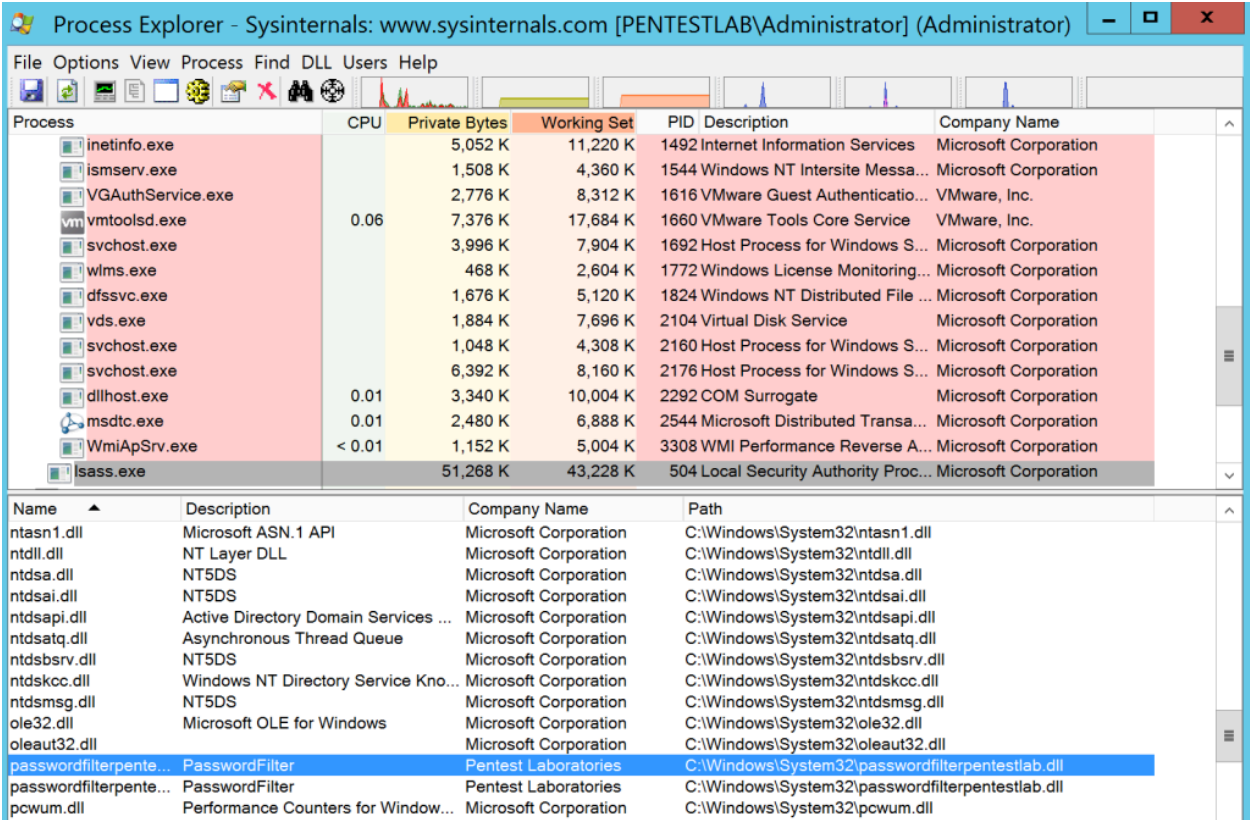
One-Time	Monthly	Yearly
Make a one-time donation		
Choose an amount		
£5.00		£15.00
£100.00		
Or enter a custom amount		

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



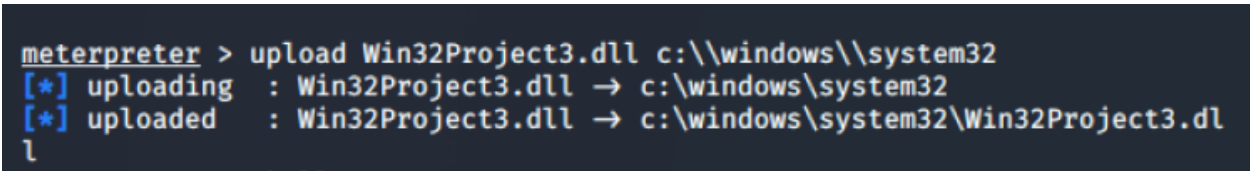
Password Change Request – Flow

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.



Password Filter DLL

£ 30.00

Your contribution is appreciated.

DONATE

FOLLOW PENTEST LAB

Enter your email address to followthis blog and receive notifications of newarticles by email.

Email Address

FOLLOW

Join 2,312 other subscribers

Supported by



VISIT MALDEV ACADEMY

SEARCH TOPIC

Enter keyword here

Q

RECENT POSTS

Web Browser Stored Credentials

Persistence – DLL Proxy Loading

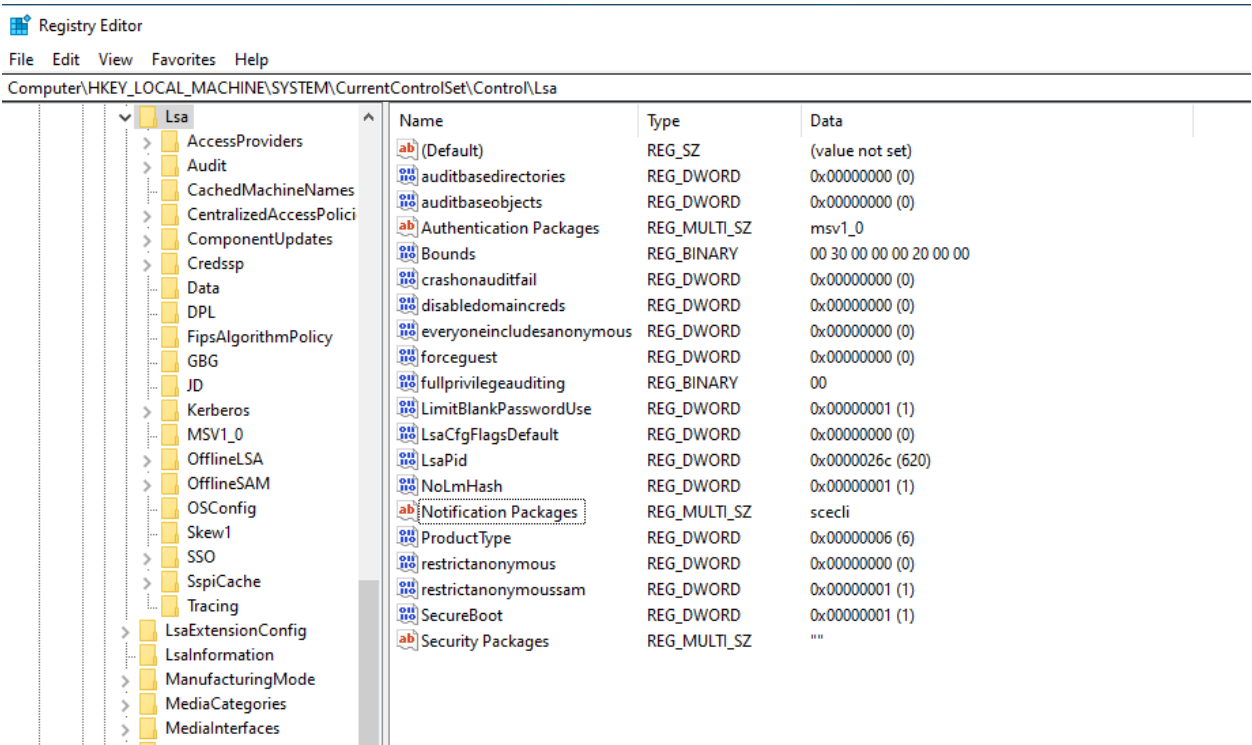
Persistence – Explorer

Persistence – Visual Studio Code Extensions

AS-REP Roasting

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 "Notific
2 | REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notific

Credential Access – Notification Packages Registry Key Modification

CATEGORIES

Coding (10)

Exploitation Techniques (19)

External Submissions (3)

General Lab Notes (22)

Information Gathering (12)

Infrastructure (2)

Maintaining Access (4)

Mobile Pentesting (7)

Network Mapping (1)

Post Exploitation (13)

Red Team (132)

Credential Access (5)

Defense Evasion (22)

Domain Escalation (6)

Domain Persistence (4)

Initial Access (1)

Lateral Movement (3)

Man-in-the-middle (1)

Persistence (39)

Privilege Escalation (17)

Reviews (1)

Social Engineering (11)

Tools (7)

VoIP (4)

Web Application (14)

Wireless (2)

February 2020

M T W T F S S						
					1	2

Comment Reblog Subscribe

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

3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	

« Jan Mar »

PEN TEST LAB STATS

7,615,555 hits

FACEBOOK PAGE



• • •

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.

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

Clear-Text Password Logged

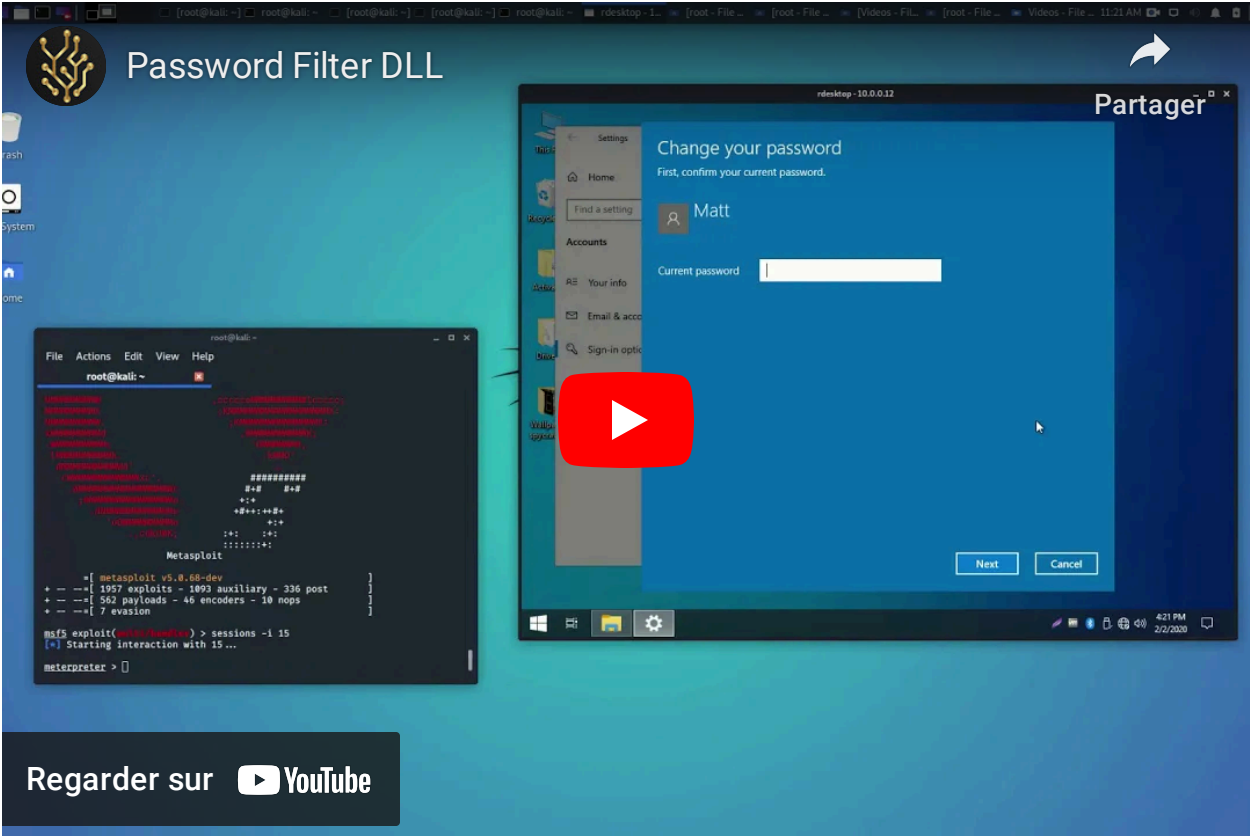
Clear-Text Password Logged

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

```
1 $passwordFilterName = (Copy-Item "Win32Project3.dll" -Destination .)
2 $lsaKey = Get-Item "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\NotificationPackagesValues"
3 $notificationPackagesValues = $lsaKey.GetValue("Notification PackagesValues")
4 $notificationPackagesValues += $passwordFilterName
5 Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\NotificationPackagesValues" $notificationPackagesValues
6 Restart-Computer -Confirm
```

PowerShell Filter DLL – PowerShell

YouTube



References

- <https://attack.mitre.org/techniques/T1174/>
- <https://docs.microsoft.com/en-us/windows/win32/secmgmt/installing-and-registering-a-password-filter-dll>
- <https://docs.microsoft.com/en-us/windows/win32/secmgmt/password-filters>
- <https://github.com/3gstudent/PasswordFilter>
- <https://malicious.link/post/2013/2013-09-11-stealing-passwords-every-time-they-change/>
- <https://github.com/GoSecure/DLLPasswordFilterImplant>
- <https://clymb3r.wordpress.com/2013/09/15/intercepting-password-changes-with-function-hooking/>

6 Votes

Rate this:

Share this:

Loading...

Related

- Stored Credentials

April 19, 2017

In "Privilege Escalation"
- Dumping Clear-Text Credentials

April 4, 2018

In "Post Exploitation"
- Attacking the FTP Service

March 1, 2012

In "Exploitation Techniques"

CREDENTIALS

DLL

LSASS

PASSWORD

PASSWORD FILTER

Leave a comment

Comment

Reblog

Subscribe



PREVIOUS

Persistence – WaitFor



NEXT

Persistence – RID Hijacking

