Exécution de code à distance

1. Service Control Manager (SCM)

ex. : `sc REMOTECOMPUTERNAME create myservicename binPath= executableToRun start= auto`

Writing to the svcctl named pipe (a.k.a. srvsvc) on remote computer over SMB. (TCP port 139 or 445 owned by kernel, forwarded to srvsvc pipe). srvsvc pipe hosted by Server service in `svchost.exe` running as `SYSTEM`.

2. Task scheduler

Ex. : `AT \\REMOTECOMPUTERNAME 12:34 "command to run"`

Writing to atsvc named pipe on remote computer over SMB. (TCP port 139 or 445 owned by kernel, forwarded to atsvc pipe). atsvc pipe hosted by Task Scheduler (Schedule) service in `svchost.exe` running as `SYSTEM`.

3. WMI

Ex. : `WMIC /node:REMOTECOMPUTERNAME PROCESS call create "command to run"`

Connecting to remote procedure call interface (RpcSs service in `svchost.exe` directly listening on `TCP port 135`)

4. Remote Registry

Ex. : `REG ADD \\REMOTECOMPUTERNAME\HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v myentry /t REG_SZ /d "command to run"`

Writing to the winreg named pipe on remote computer over SMB. (TCP port 139 or 445 owned by kernel, forwarded to winreg pipe). The winreg pipe is hosted by Remote Registry service in `svchost.exe`

Exécution de code à distance

5. Remote File Access

Ex. :`xcopy executabletorun.exe "\\REMOTECOMPUTERNAME\C$ \ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\e.exe"`

Writing to remote administrative shares using SMB. (`TCP port 139 or 445` owned by kernel)

6. Remote Desktop

Ex. : `rdesktop 1.2.3.4`

Hosted by the TermService service (“Remote Desktop Services”) in `svchost.exe` by a server socket listening on `TCP port 3389`.

7. Windows Remote Management

Ex. : `winrs -r:REMOTECOMPUTERNAME` command to run

Hosted by Windows Remote Management service (`svchost.exe`), listens on `TCP/80 or TCP/5985` and can share port with `IIS`