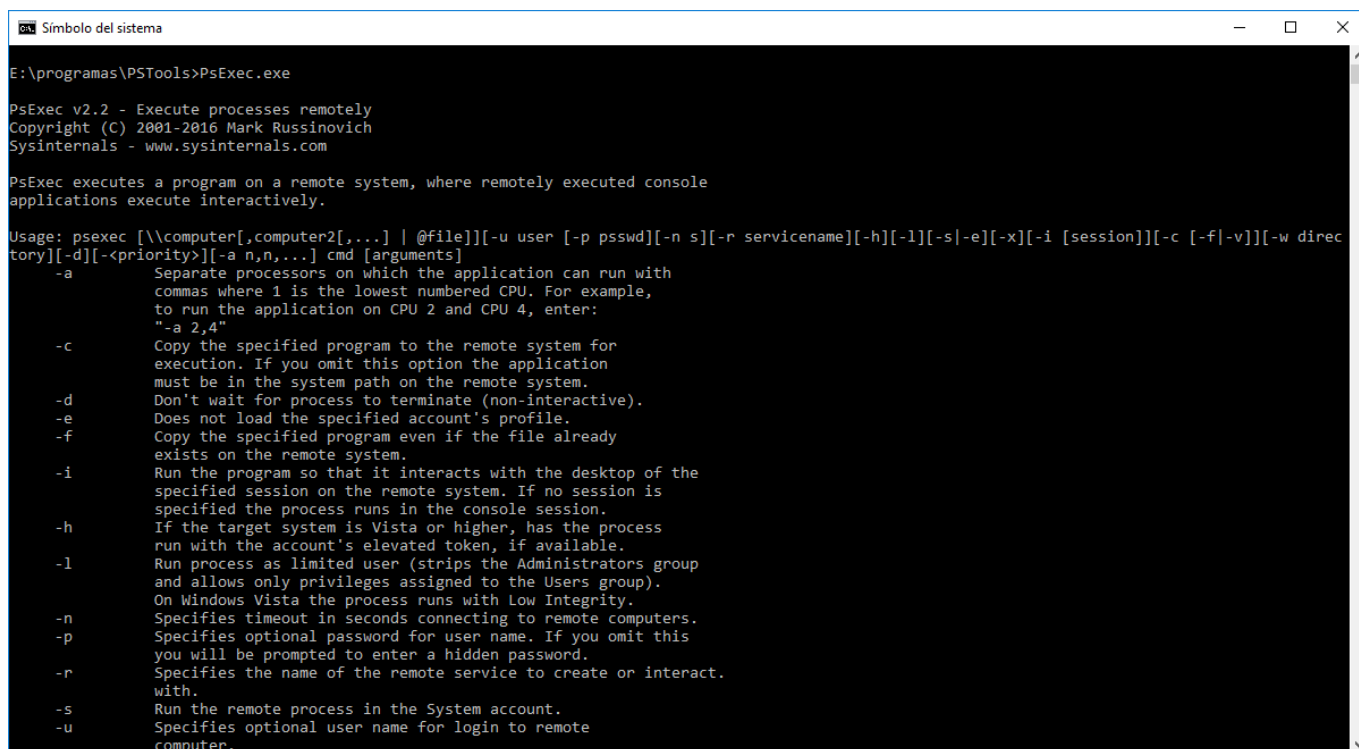


PsExec

PsExec is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named PsTools.



```
E:\programas\PsTools>PsExec.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

PsExec executes a program on a remote system, where remotely executed console
applications execute interactively.

Usage: psexec [[\computer[,computer2[,...]] @file]] [-u user [-p psswd]] [-n s] [-r servicename] [-h] [-l] [-s] [-e] [-x] [-i [session]] [-c [-f|-v]] [-w direc
tory] [-d] [-<priority>] [-a n,n,...] cmd [arguments]
-a          Separate processors on which the application can run with
            commas where 1 is the lowest numbered CPU. For example,
            to run the application on CPU 2 and CPU 4, enter:
            "-a 2,4"
-c          Copy the specified program to the remote system for
            execution. If you omit this option the application
            must be in the system path on the remote system.
-d          Don't wait for process to terminate (non-interactive).
-e          Does not load the specified account's profile.
-f          Copy the specified program even if the file already
            exists on the remote system.
-i          Run the program so that it interacts with the desktop of the
            specified session on the remote system. If no session is
            specified the process runs in the console session.
-h          If the target system is Vista or higher, has the process
            run with the account's elevated token, if available.
-l          Run process as limited user (strips the Administrators group
            and allows only privileges assigned to the Users group).
            On Windows Vista the process runs with Low Integrity.
-n          Specifies timeout in seconds connecting to remote computers.
-p          Specifies optional password for user name. If you omit this
            you will be prompted to enter a hidden password.
-r          Specifies the name of the remote service to create or interact
            with.
-s          Run the remote process in the System account.
-u          Specifies optional user name for login to remote
            computer.
```

Utilities like Telnet and remote control programs like Symantec's PC Anywhere let you execute programs on remote systems, but they can be a pain to set up and require that you install client software on the remote systems that you wish to access. PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems.

Note: some anti-virus scanners report that one or more of the tools are infected with a «remote admin» virus. None of the PsTools contain viruses, but they have been used by viruses,

which is why they trigger virus notifications.

Download

<https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>

Examples

This article I wrote [describes how PsExec works](#) and gives tips on how to use it:

The following command launches an interactive command prompt on \\marklap:

```
[crayon-6a9d8d6434f8a209954101/]
```

This command executes IpConfig on the remote system with the /all switch, and displays the resulting output locally:

```
[crayon-6a9d8d6434f93190333063/]
```

This command copies the program test.exe to the remote system and executes it interactively:

```
[crayon-6a9d8d6434f95276226832/]
```

Specify the full path to a program that is already installed on a remote system if its not on the system's path:

```
[crayon-6a9d8d6434f98198454229/]
```

Run Regedit interactively in the System account to view the contents of the SAM and SECURITY keys::

```
[crayon-6a9d8d6434f9a311206890/]
```

To run Internet Explorer as with limited-user privileges use this command:

```
[crayon-6a9d8d6434f9c407662668/]
```