FPort v2.0

Posted At : November 19, 2004 4:19 PM | Posted By : Steven Erat
Related Categories: ColdFusion, Macromedia

Got caught with your ports open?

When netstat's not good enough, try FPort instead. FPort from **Foundstone** is a Windows utility that does netstat one better; it identifies the process id and process name for each port that is open or connected to on the system. With the -a switch it can sort by process name for easier readability. Check it out.

First here's nestat output on my system:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:>netstat -a

Active Connections

Proto Local Address Foreign Address State
TCP SERAT03:ftp SERAT03:0 LISTENING
TCP SERAT03:http SERAT03:0 LISTENING
TCP SERAT03:81 SERAT03:0 LISTENING
TCP SERAT03:epmap SERAT03:0 LISTENING
TCP SERAT03:microsoft-ds SERAT03:0 LISTENING
TCP SERAT03:1025 SERAT03:0 LISTENING
TCP SERAT03:1041 SERAT03:0 LISTENING
TCP SERAT03:1162 SERAT03:0 LISTENING
TCP SERAT03:2030 SERAT03:0 LISTENING
TCP SERAT03:2234 SERAT03:0 LISTENING
TCP SERAT03:2478 SERAT03:0 LISTENING
TCP SERAT03:2522 SERAT03:0 LISTENING
TCP SERAT03:2561 SERAT03:0 LISTENING
TCP SERAT03:2693 SERAT03:0 LISTENING
TCP SERAT03:2827 SERAT03:0 LISTENING
TCP SERAT03:2829 SERAT03:0 LISTENING
TCP SERAT03:2901 SERAT03:0 LISTENING
TCP SERAT03:3389 SERAT03:0 LISTENING
TCP SERAT03:3884 SERAT03:0 LISTENING
TCP SERAT03:4261 SERAT03:0 LISTENING
TCP SERAT03:4565 SERAT03:0 LISTENING
TCP SERAT03:5000 SERAT03:0 LISTENING
TCP SERAT03:5800 SERAT03:0 LISTENING
TCP SERAT03:5900 SERAT03:0 LISTENING
TCP SERAT03:8103 SERAT03:0 LISTENING
TCP SERAT03:19997 SERAT03:0 LISTENING
TCP SERAT03:19998 SERAT03:0 LISTENING
TCP SERAT03:51010 SERAT03:0 LISTENING
TCP SERAT03:netbios-ssn SERAT03:0 LISTENING
TCP SERAT03:netbios-ssn 10.4.32.70:1028 ESTABLISHED
TCP SERAT03:1162 fileserver.macromedia.com:microsoft-ds ESTABLISHED
TCP SERAT03:1829 SERAT03:0 LISTENING
TCP SERAT03:2234 oam-d12c.blue.aol.com:5190 ESTABLISHED
TCP SERAT03:2369 SERAT03:0 LISTENING
TCP SERAT03:2382 SERAT03:0 LISTENING
```

```
TCP SERAT03:2561 smartftp.com:http CLOSE_WAIT
TCP SERAT03:2693 mailserver.macromedia.com:5031 ESTABLISHED
TCP SERAT03:2806 SERAT03:0 LISTENING
TCP SERAT03:2822 10.4.32.70:netbios-ssn TIME_WAIT
TCP SERAT03:2823 10.1.240.14:631 TIME_WAIT
TCP SERAT03:2827 10.4.112.10:imap ESTABLISHED
TCP SERAT03:2829 10.172.16.42:http ESTABLISHED
TCP SERAT03:2835 10.1.122.64:netbios-ssn TIME_WAIT
TCP SERAT03:3154 SERAT03:0 LISTENING
TCP SERAT03:3277 SERAT03:0 LISTENING
TCP SERAT03:3277 ps-snap.allaire.com:netbios-ssn ESTABLISHED
TCP SERAT03:3283 SERAT03:0 LISTENING
TCP SERAT03:3283 ps-snap.allaire.com:netbios-ssn ESTABLISHED
TCP SERAT03:3607 SERAT03:0 LISTENING
TCP SERAT03:3884 64.12.31.124:5190 ESTABLISHED
TCP SERAT03:4565 mailserver.macromedia.com:5030 ESTABLISHED
TCP SERAT03:7692 SERAT03:0 LISTENING
TCP SERAT03:http localhost:2828 TIME_WAIT
TCP SERAT03:http localhost:2830 TIME_WAIT
TCP SERAT03:2477 SERAT03:0 LISTENING
TCP SERAT03:2477 localhost:2478 ESTABLISHED
TCP SERAT03:2478 localhost:2477 ESTABLISHED
TCP SERAT03:5180 SERAT03:0 LISTENING
UDP SERAT03:microsoft-ds *:*
UDP SERAT03:isakmp *:*
UDP SERAT03:1028 *:*
UDP SERAT03:1049 *:*
UDP SERAT03:1053 *:*
UDP SERAT03:1696 *:*
UDP SERAT03:2364 *:*
UDP SERAT03:2365 *:*
UDP SERAT03:2967 *:*
UDP SERAT03:3456 *:*
UDP SERAT03:4567 *:*
UDP SERAT03:38037 *:*
UDP SERAT03:ntp *:*
UDP SERAT03:netbios-ns *:*
UDP SERAT03:netbios-dgm *:*
UDP SERAT03:1900 *:*
UDP SERAT03:10102 *:*
UDP SERAT03:36190 *:*
UDP SERAT03:ntp *:*
UDP SERAT03:1051 *:*
UDP SERAT03:1057 *:*
UDP SERAT03:1900 *:*
UDP SERAT03:2440 *:*
```

Now compare that to the FPort output:

```
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid Process Port Proto Path
924 -> 5000 TCP
280 OUTLOOK -> 2693 TCP C:Program FilesMicrosoft OfficeOFFICE11OUTLOOK.EXE
280 OUTLOOK -> 2837 TCP C:Program FilesMicrosoft OfficeOFFICE11OUTLOOK.EXE
280 OUTLOOK -> 4565 TCP C:Program FilesMicrosoft OfficeOFFICE11OUTLOOK.EXE
```

```
2240 SmartFTP -> 2561 TCP C:Program FilesSmartFTPSmartFTP.exe
4 System -> 1162 TCP
4 System -> 139 TCP
4 System -> 1829 TCP
4 System -> 2369 TCP
4 System -> 2382 TCP
4 System -> 2806 TCP
0 System -> 2822 TCP
0 System -> 2835 TCP
4 System -> 3154 TCP
4 System -> 3277 TCP
4 System -> 3283 TCP
4 System -> 3607 TCP
4 System -> 445 TCP
0 System -> 80 TCP
1948 WinVNC -> 5800 TCP C:Program FilesRealVNCWinVNCWinVNC.exe
1948 WinVNC -> 5900 TCP C:Program FilesRealVNCWinVNCWinVNC.exe
1820 aim -> 2234 TCP C:PROGRA~1AIMaim.exe
1820 aim -> 3884 TCP C:PROGRA~1AIMaim.exe
1820 aim -> 5180 TCP C:PROGRA~1AIMaim.exe
2528 firefox -> 2477 TCP C:Program FilesMozilla Firefoxfirefox.exe
2528 firefox -> 2478 TCP C:Program FilesMozilla Firefoxfirefox.exe
2528 firefox -> 2829 TCP C:Program FilesMozilla Firefoxfirefox.exe
1288 inetinfo -> 1041 TCP C:WINDOWSSystem32inetsrvinetinfo.exe
1288 inetinfo -> 21 TCP C:WINDOWSSystem32inetsrvinetinfo.exe
1288 inetinfo -> 81 TCP C:WINDOWSSystem32inetsrvinetinfo.exe
4072 jrun -> 2522 TCP C:CFusionMX untimeinjrun.exe
4072 jrun -> 2901 TCP C:CFusionMX untimeinjrun.exe
4072 jrun -> 4261 TCP C:CFusionMX untimeinjrun.exe
4072 jrun -> 51010 TCP C:CFusionMX untimeinjrun.exe
4072 jrun -> 80 TCP C:CFusionMX untimeinjrun.exe
4072 jrun -> 8103 TCP C:CFusionMX untimeinjrun.exe
820 msmsgs -> 7692 TCP C:Program FilesMessengermsmsgs.exe
1416 omtsreco -> 2030 TCP C:ora9inomtsreco.exe
744 svchost -> 1025 TCP C:WINDOWSSystem32svchost.exe
692 svchost -> 135 TCP C:WINDOWSsystem32svchost.exe
744 svchost -> 3389 TCP C:WINDOWSSystem32svchost.exe
1196 swagent -> 19997 TCP C:CFusionMXdbslserver52inswagent.exe
3760 swsoc -> 19998 TCP C:CFusionMXdbslserver52inswsoc.exe

924 -> 1900 UDP
280 OUTLOOK -> 1057 UDP C:Program FilesMicrosoft OfficeOFFICE11OUTLOOK.EXE
280 OUTLOOK -> 137 UDP C:Program FilesMicrosoft OfficeOFFICE11OUTLOOK.EXE
280 OUTLOOK -> 1900 UDP C:Program FilesMicrosoft OfficeOFFICE11OUTLOOK.EXE
2240 SmartFTP -> 123 UDP C:Program FilesSmartFTPSmartFTP.exe
4 System -> 1053 UDP
4 System -> 2365 UDP
1948 WinVNC -> 2440 UDP C:Program FilesRealVNCWinVNCWinVNC.exe
1820 aim -> 123 UDP C:PROGRA~1AIMaim.exe
1820 aim -> 3456 UDP C:PROGRA~1AIMaim.exe
2528 firefox -> 138 UDP C:Program FilesMozilla Firefoxfirefox.exe
2528 firefox -> 4567 UDP C:Program FilesMozilla Firefoxfirefox.exe
1288 inetinfo -> 1028 UDP C:WINDOWSSystem32inetsrvinetinfo.exe
1288 inetinfo -> 2364 UDP C:WINDOWSSystem32inetsrvinetinfo.exe
1288 inetinfo -> 445 UDP C:WINDOWSSystem32inetsrvinetinfo.exe
4072 jrun -> 10102 UDP C:CFusionMX untimeinjrun.exe
4072 jrun -> 1051 UDP C:CFusionMX untimeinjrun.exe
4072 jrun -> 38037 UDP C:CFusionMX untimeinjrun.exe
4072 jrun -> 500 UDP C:CFusionMX untimeinjrun.exe
1416 omtsreco -> 2967 UDP C:ora9inomtsreco.exe
```

```
692 svchost -> 1049 UDP C:WINDOWSsystem32svchost.exe
744 svchost -> 1696 UDP C:WINDOWSSystem32svchost.exe
744 svchost -> 36190 UDP C:WINDOWSSystem32svchost.exe
```