

اسکن پورت های باز در ویندوز

زمانی که خطایابی برنامه های سمت کلاینت یا سرور موضوع اصلی باشد، گاهی لازم است تا از بسته بودن پورتی که آن برنامه از آن استفاده می کند اطمینان حاصل نماییم.

در این مقاله باهم نگاهی سریع به اینکه چگونه بتوانیم پورت های باز را به کمک اعدادی که در ابزارهای ساده ویندوز موجود است، ببینیم. ممکن است از اینکه چقدر این راهکار آسان می تواند در شناسایی پورت های باز کمک تان کند، شگفت زده شوید. با این کار می توانید ریشه تمامی مشکل ها را بیابید.

NetStat.exe

اولین ابزار مورد توجه ابزاری است که تمامی ادمین های شبکه و پشتیبانان فنی اسم آن را شنیده اند، NetStat.exe در فولدر Win32 موجود در windows قرار دارد و به شما این امکان را می دهد تا ببینید کدام پورت ها باز هستند و کدام پورت ها در هاست مورد نظر در حال استفاده اند. این ابزار را با اسکنر پورت شبکه که در هاست به دنبال پورت باز می گردد، اشتباه نگیرید.

برای دیدن پورت های باز در هاست محلی تان، در محیط Command، عبارت زیر را بنویسید:

```
netstat -an | find /i "listening"
```

نتیجه در ۴ ستون مجزا بیان می شود، Protocol type، Local IP address and associated port، foreign IP address، number و در ستون آخر، حالت را مشاهده می کنیم. ستون مورد نظر این بحث، ستون شماره دو است.

```

C:\Windows\system32\cmd.exe
C:\>netstat -an |find /i "listening"
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2869 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING
TCP 0.0.0.0:17500 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5354 0.0.0.0:0 LISTENING
TCP 127.0.0.1:27015 0.0.0.0:0 LISTENING
TCP 192.168.0.7:139 0.0.0.0:0 LISTENING
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:2869 [::]:0 LISTENING
TCP [::]:5357 [::]:0 LISTENING
TCP [::]:49152 [::]:0 LISTENING
TCP [::]:49153 [::]:0 LISTENING
TCP [::]:49154 [::]:0 LISTENING
TCP [::]:49155 [::]:0 LISTENING
TCP [::]:49157 [::]:0 LISTENING
C:\>
  
```

اگر در دستور نوشته شده در محیط Command، پارامتر O را نیز اضافه کنیم، ستون پنجمی نمایش داده می شود که نشان دهنده process ID برنامه ها می است که با پورت باز در حال کار کردن هستند. دستور کامل برای نمایش ستون پنجم به شرح زیر است:

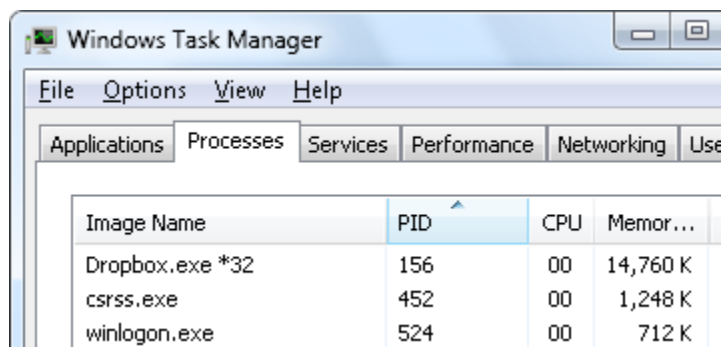
netstat -ano |find /i "listening"

```

C:\Windows\system32\cmd.exe
C:\>netstat -ano |find /i "listening"
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 744
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:2869 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:17500 0.0.0.0:0 LISTENING 156
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING 440
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING 928
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING 996
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING 544
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING 500
TCP 127.0.0.1:5354 0.0.0.0:0 LISTENING 1676
TCP 127.0.0.1:27015 0.0.0.0:0 LISTENING 1624
TCP 192.168.0.7:139 0.0.0.0:0 LISTENING 4
TCP [::]:135 [::]:0 LISTENING 744
TCP [::]:445 [::]:0 LISTENING 4
TCP [::]:2869 [::]:0 LISTENING 4
TCP [::]:5357 [::]:0 LISTENING 4
TCP [::]:49152 [::]:0 LISTENING 440
TCP [::]:49153 [::]:0 LISTENING 928
TCP [::]:49154 [::]:0 LISTENING 996
TCP [::]:49155 [::]:0 LISTENING 544
TCP [::]:49157 [::]:0 LISTENING 500
C:\>
  
```

از Task Manager برای پیدا کردن این برنامه ها که با پورت باز در حال کار کردن هستند، استفاده نمایید.

اطلاعاتی **Process ID – PID** – در پیدا کردن برنامه هایی که با پورت باز کار می کنند، مفید واقع می شود. برای مثال، در شکل بالا PID ۱۵۶ مربوط به پورت ۱۷۵۰۰ است. به کمک **CTRL + SHIFT+ ESC – Task Manager** می توانیم بفهمیم که ۱۵۶ متعلق به برنامه **DropBox.exe** است.



Tasklist.exe نیز از طریق محیط **command** به شما این امکان را می دهد تا بفهمید چه برنامه ای با پورت باز کار می کند. در واقع **Tasklist.exe** همان اطلاعاتی را در محیط **Command** به شما نشان می دهد که **Windows Task Manager** در محیط گرافیکی در اختیاران قرار می دهد.

در خروجی این دستور نیز، ستون مورد توجه، ستون دوم است که **PID** هر برنامه ای که در حال اجرا است را نشان می دهد. در هر دو روش ذکر شده می توانید اطلاعات دیگری نیز کسب کنید، مثلا بفهمید چه کاربری در حال استفاده از برنامه مورد نظر است.

برای دست یابی به لیست کامل پارامترها و اطلاعات ثانویه، کفایت این دستورات را در محیط **Command** بنویسید،

“netstat /?”

“tasklist /?”

TCPView.exe

مانند **netstat.exe**، **TCPView.exe** نیز همان اطلاعات را در اختیاران قرار می دهد اما با جزئیاتی بیشتر و در قالب واسطی گرافیکی.

TCPView.exe را می توانید از **Microsoft SysInternals website** دانلود کنید و به عنوان برنامه ای که نیاز به نصب ندارد اجراش کنید. با استفاده از **TCPView** نه تنها می توانید پورت های باز را شناسایی کرده، بلکه می توانید

مانند یک فرآیند مهیج، اطلاعات ارتباطات محلی یا راه دور را ببینید، مثل بسته های ارسالی و دریافتی یا پروتکل در حال استفاده.

PortQry.exe

ابزار جذاب دیگری که باید با آن آشنا باشید، PortQry.exe است. این ابزار را می توانید از Microsoft Download Center دانلود نمایید و مانند یک برنامه مستقل در محیط Command Line قابل استفاده است. PortQry.exe به شما این امکان را می دهد که پورت های باز محلی و راه دور را ببینید. به محض آنکه این ابزار را دانلود کرده و از حالت zip خارج کنید، محیط Command باز می شود. PortQry.exe را بنویسید و کنارش از پارامترها و سوئیچ های مورد نظر استفاده کنید.

برای مثال، با نوشتن **“portqry.exe –local”** پورت TCP/UDP مورد استفاده در هاست محلی را در اختیارتان قرار می دهد. اطلاعات نمایش داده شده در این روش، مانند روش netstat.exe است.

برای مشاهده پورت های باز TCP/UDP هاست راه دور عبارت زیر را بنویسید:

“portqry.exe –n [hostname/IP]”

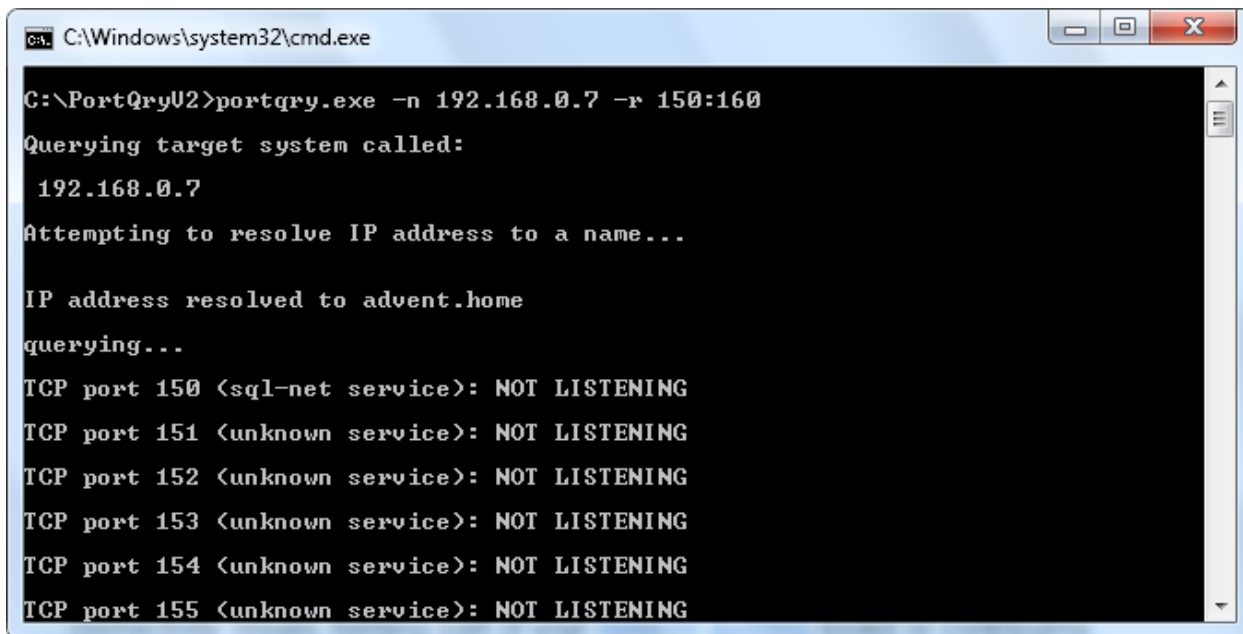
قسمت داخل کروشه را با IP هاست مورد نظر یا نام هاست جایگزین کنید. همچنین می توانید برای بررسی پورتی که مد نظرتان است عبارت **“-e [port_number]”** را بنویسید. اگر محدوده خاصی از پورت ها مدنظرتان بود این عبارت را بنویسید:

“-r [start_range:end_range]”

یا اگر گروهی از پورت ها با یک نظم مشخص مدنظرتان است دستور زیر را بنویسید:

“-o [port1, port2, port3]”

در تصویر زیر از portqry.exe استفاده شده است تا پورت های باز موجود در هاست راه دور با IP address 192.168.0.7 در بازه پورت های ۱۵۰ تا ۱۶۰ را بررسی کند.



```
C:\Windows\system32\cmd.exe
C:\PortQryU2>portqry.exe -n 192.168.0.7 -r 150:160
Querying target system called:
 192.168.0.7
Attempting to resolve IP address to a name...
IP address resolved to advent.hone
querying...
TCP port 150 (sql-net service): NOT LISTENING
TCP port 151 (unknown service): NOT LISTENING
TCP port 152 (unknown service): NOT LISTENING
TCP port 153 (unknown service): NOT LISTENING
TCP port 154 (unknown service): NOT LISTENING
TCP port 155 (unknown service): NOT LISTENING
```

برای دست یابی به لیست کامل پارامترها و اطلاعات ثانویه، کافیست “portqry.exe/?” را بنویسید.

نتیجه گیری

این مقاله راه های آسان بررسی پورت های باز را خدمتتان معرفی کرد. این تسهیلات برای خطایابی اتصالات شبکه مفید واقع می شود، همچنین می تواند قسمتی از ابزارهای ممیزی شبکه یا ابزاری برای تشخیص آسیب پذیری های شبکه باشد.

توانایی چک کردن پورت های باز یک توانایی بسیار مهم است و در خطایابی شبکه مفید واقع می شود. همچنین جنبه حیاتی در استراتژی امنیت شبکه دارد.