

Computer Ports: What You Should Know to Defend Yourself

By Aaron Turpen

Computer Ports: What You Should Know to Defend Yourself

Aaron Turpen
aaron@aaronzwebworkz.com

Aaronz WebWorkz <http://www.AaronzWebWorkz.com>

The number one way a computer is exposed for nefarious uses online is by exploiting open ports on that system.

Ports are names or “handles” given to various network connections your computer uses to communicate with other computers. For example, your connection to the Internet is through a port protocol called TCP/IP (Transmission Control Protocol/Internet Protocol) using well-known ports such as HTTP or “port 80.” While it sounds complicated, the way all this works is actually fairly simple.

A program (called a “daemon” in Unix or a “service” in Windows) “listens” or watches a specific port. So, for instance, a web server daemon will watch port 80 for queries from outside the server. When a query comes in, the daemon immediately responds by accepting the query and sending the requested information.

On a home computer, many of these ports are open by default, many for good reason, but many more for no good reason. Trojan horse programs (software that pretends to be one thing, but is actually another), AdWare (software that runs using online advertising), SpyWare (software that “spies” on your activity in order to target advertising to you, or for other reasons), and other questionable or downright devious programs will listen at unusual ports to send or receive information. Information that you may not want transmitted.

There are several ways to check these ports and ensure that they are OK. The best and easiest is to use a software firewall such as ZoneAlarm (<http://www.qksrv.net/click-983614-9925654>) to monitor your incoming and outgoing data and alert you to anything suspicious. I highly recommend this route for most users.

If you are a little more technical and/or more adventurous, you can open a command window (MS-DOS window in Windows) and type the command “netstat -an” at the prompt (no quotes) and see a list of currently open ports and the IP addresses associated with them.

Often overlooked, open ports are the easiest and most common way for a hacker, virus, or worm to take advantage of your computer or data. Learning about the open ports on your machine and how to guard them is important.

=====

Aaron has a new eMasters ebook to be released at the end of October titled “Hackers, Fraud, and

Trust Online: The Netpreneur's Quick & Easy Guide to Cyber-Crime Prevention.” If you would like to advertise in this much-anticipated ebook, follow this link:

<http://hop.clickbank.net/?aaronicus/admasters1>

[Get-Articles.com : 1000's of reprintable business and internet marketing-related articles.](#)

[Submit your article for reprint.](#)