

# Port Scanning; the Good, Bad, & Ugly

By,

**Brian Wilson**

CCNA, CSE, CCAI, MCP, Network+

[Slimjim100@gmail.com](mailto:Slimjim100@gmail.com)

[www.middlegeorgia.org](http://www.middlegeorgia.org)

[www.middlegeorgia.info](http://www.middlegeorgia.info)

[www.slimjim100.com](http://www.slimjim100.com)

What is port scanning you might ask? Well port scanning can be describe many ways but basically is the act of sending packets to a destination of group of hosts to try to get a response. Why do I need to port scan and do others port scan me? You might want to port scan your broadband connection to see what your network has open to the internet and others may port scan you to find a way into your network. Port scanning can be done for good reasons and malicious purposes. Other real good reasons for port scanning is to see what ports your software might be using this can help you trouble shoot network issues. There are too many reasons to list here on the pros of ports scans and port scan software but you must first understand what a port is and how it affects you computer and network.

What is a port and how dose it work?

Ports are similar to addresses for example if you send a package to a friend you will have to put many entries on the shipping label for it to get to him. You would need a name, street number, city, State, zip code, and sometimes a country. Without this information your package would not get the recipient. Ports work in a similar way. Ports are part of the address for internet traffic. Ports also have to have other data to be used like an IP address, Protocol, and transport media.

Who controls port numbers?

Ports numbers are standardized though the "Internet Assigned Numbers Authority" or IANA. The port numbers are divided into three ranges: The Well Known Ports, Registered Ports, and the Dynamic and/or Private Ports.

The Well Known Ports are those from 0 through 1023. DCCP Well Known ports SHOULD NOT be used without IANA registration. The registration procedure is defined in [RFC4340], Section 19.9.

The Registered Ports are those from 1024 through 49151 DCCP Registered ports SHOULD NOT be used without IANA registration. The registration procedure is defined in [RFC4340], Section 19.9.

The Dynamic and/or Private Ports are those from 49152 through 65535.

Port Scanning Software.

Let's now take a look at software that is used for port scanning. A lot of the software out there for port scanning also has other futures for vulnerability scanning. One of the most well known port scanning tools is NMAP.

Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. Nmap is free and open source (description from NMAP's website).

Angry IP scanner is a very fast IP scanner and port scanner. It can scan IP addresses in any range as well as any their ports. Its binary file size is very small compared to other IP or port scanners. Angry IP scanner simply pings each IP address to check if it's alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with the available plugin's (description from [angryziber.com](http://angryziber.com)).

SuperScan 4 is a Powerful TCP port scanner, pinger, and resolver. Here are some of the features; Superior scanning speed, Support for unlimited IP ranges, Improved host detection using multiple ICMP methods, TCP SYN scanning, UDP scanning (two methods), IP address import supporting ranges and CIDR formats, Simple HTML report generation, Source port scanning, Fast hostname resolving, Extensive banner grabbing, Massive built-in port list description database, IP and port scan order randomization, A selection of useful tools (ping, trace route, Whois etc). SuperScan is from [foundstone.com](http://foundstone.com) and this description was gathered from there website.

#### Online Scanners

There are also websites that offer free port scans to help you secure your network. Here is a list of a few scanning sites.

Sygate Online Scan ([scan.sygate.com](http://scan.sygate.com)) extended security check (Stealth Scan, Trojan Scan).

Planet Security Firewall-Check ([planet-security.net](http://planet-security.net)) Fast, extended check, checks currently high-endangered ports.

Crucialtests ([crucialtests.com](http://crucialtests.com)) concise, incl. advisor.

ShieldsUP ([grc.com](http://grc.com)) Quick Scanner, clearly laid out.

#### How to block all the scanning

Now that you have seen what ports scanning is and the uses for it you might want to know how to protect you network from scans. The best thing to do is have a firewall and use up-to-date Anti-virus & Anti-Spyware programs. You will not be able to stop the scans on your network but with a good firewall the person scanning you will not see any traffic back and hopefully assume your connection is not on or no assemble. To find more information on port scanning and the tools used try to Google it.