ShieldsUP!!

Port Authority Edition – Internet Vulnerability Profiling

by Steve Gibson, Gibson Research Corporation.

Determine the status of your system's first 1056 ports

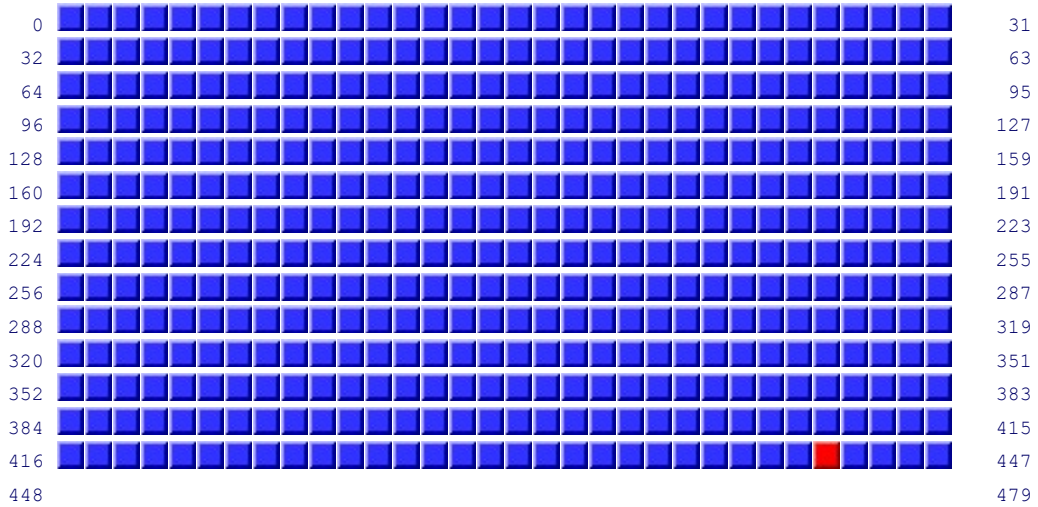
This Internet service ports "grid scan" determines the status — Open, Closed, or Stealth — of your system's first 1056 TCP ports.

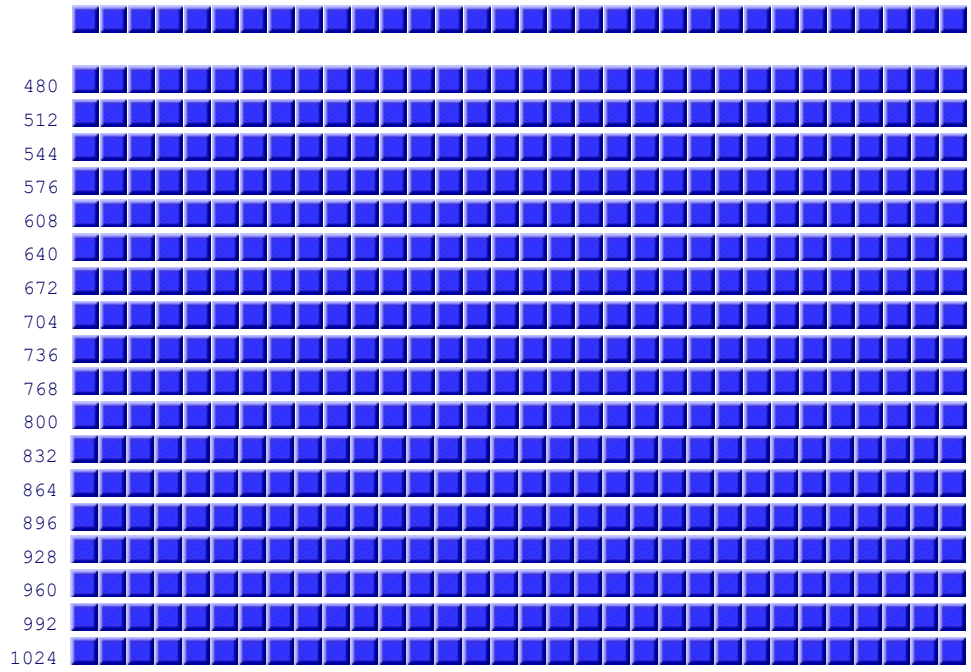
- 32 ports, represented by each horizontal row, are probed as a group. The results are posted as the next set of ports are probed.
- During off-peak hours the entire scan requires just over one minute.
- For guaranteed accuracy, the scanning time will increase during peak usage when many people are sharing our scanning bandwidth.
- A scan of a stealthed system is up to four times slower since many more probes must be sent to guarantee against Internet packet loss.
- The test may be abandoned at any time if you do not wish to wait for the scan to finish.
- You may hover your mouse cursor over any grid cell to determine which port it represents, or click on the cell to jump to the corresponding Port Authority database page to learn about the port's specific role, history, and security consequences. (Depress SHIFT when clicking to open new window and allow unfinished test to continue.)

Your computer at IP:

84.17.61.212

Is being carefully examined:





The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

Open Closed Stealth

Text Summary

Total elapsed testing time: 21.117 seconds

TruStealth Analysis

Solicited TCP Packets: **RECEIVED (FAILED)** — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active user community.

Unsolicited Packets: **PASSED** — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

Ping Reply: **RECEIVED (FAILED)** — Your system REPLIED to our Ping (ICMP Echo) requests, making it visible on the Internet. Most personal firewalls can be configured to block, drop, and ignore such ping requests in order to

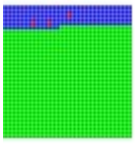
better hide systems from hackers. This is highly recommended since "Ping" is among the oldest and most common methods used to locate systems prior to further exploitation.

Why the first 1056 Ports?

Internet ports are numbered from 1 through 65535, but the first 1023 ports are special. By tradition, and some enforcement, ports 1 through 1023 are generally reserved for the acceptance of incoming connections by services running on the receiving system. Internet services "listen" on various standard low-numbered ports so that clients wishing to have access to those services know where they may be found. Web servers traditionally listen on port 80, eMail servers listen on ports 25 and 110, FTP servers listen on port 21 and Telnet servers listen on port 23. And the list goes on. Here's the official Internet Assigned Numbers Authority (IANA) port assignment list.

Although it is possible to have higher-numbered ports listening for incoming connections, our scan of the entire "service port range" will detect all standard services running and listening on the standard service ports.

Due to the insecure behavior of Microsoft's Windows operating systems, we have added an additional 33 ports to these first 1023 ports, bringing the total to 1056. Windows has a tendency to establish globally available listening services on the first few ports in the "client port" range which begins just past 1023. If you are not running a personal firewall, or you are allowing ShieldsUP! probes into your network, you may discover one or more additional open ports at, or just above, 1024.



Strange Results?

Personal firewalls are beginning to exhibit "adaptive behavior". The grid shown to the left starts off showing ports mostly closed with a few open (mostly blue with a few red cells). Then at some point it suddenly switches into "stealth mode". This can occur when a firewall "adapts" to the scanning IP and raises its defenses against just the attacker. This complicates the job of accurately checking a system's security.

Two things you can do: If you are not certain whether your firewall is adaptive, you can re-run any test here to compare the results. Differing behavior often indicates that your firewall has "learned" that it is being probed from our IP and is treating it differently. For the most accurate scan results, disable any adaptive behavior during the testing.

You can use these tests to learn exactly how your firewall deals with probes to specific ports, and to port ranges.

Beyond providing a comprehensive test of your system's first 1056 ports, this service ports scan can be used for additional research:

Service Ports Scan Application Guide

(Cool things you can do with our Service Ports Probe)

Detecting Ports Blocked by Your ISP

Internet service providers often block specific traffic entering their network before it reaches their customers, or after leaving their customers before it exits their network. This is sometimes done to block the exploitation of common security vulnerabilities, and sometimes to prevent their customers from offering proscribed Internet services.

As a customer, it can be useful and interesting to know which service ports, if any, an ISP has chosen to preemptively block in order to restrict their customers' global Internet traffic.

ISP port blocking can be easily tested, often quite rapidly, by arranging to allow the ShieldsUP! probe to have access to an unprotected computer. Since all non-stealth machines will respond to every open request — either affirmatively or negatively — ports appearing as STEALTH will be those blocked by your ISP, corporate firewall, or other external agency.

- If your system is unprotected, without any personal firewall or NAT router, any ports showing as stealth  are being blocked somewhere between your computer and the public Internet. This is probably being done by your ISP. Internet traffic directed to your computer at the stealth ports will be dropped before reaching your machine.

- If your system has a personal firewall that can be instructed to "trust" a specific remote IP, you can temporarily instruct it to trust the ShieldsUP! probe IP of [4.79.142.206]. If, after doing so, most of the service ports change to either open  or closed  , you have succeeded and any which remain stealth are being blocked by your ISP.

- If your system is operating behind a residential "NAT" router, the router will be acting as a natural and excellent hardware firewall. But that's not what you want for the moment. You can temporarily remove your NAT router and connect an unprotected computer directly to your cable modem or DSL line. Or, if you are comfortable reconfiguring your NAT router, you may be able to point the router's "DMZ" at one of your computers which has been instructed to "trust" our probe IP of **[4.79.142.206]**. If, after doing so, most of the service ports change to either open  or closed  , you have succeeded and any remaining stealth are being blocked by your ISP.

- Finally, if your Internet security system, NAT router, personal firewall, or whatever, can produce detailed logs of incoming Internet packets, you could leave your existing security in place, clear your log, run the service ports scan, then carefully inspect your log for any consistently missing port probes. We send out four sets of probing packets because individual packets are sometimes dropped along the way. Therefore, it won't be unusual to see occasional missing packets from your logs. What you're looking for is a complete lack of packets bound for a specific port. A careful and detailed examination of your log will reveal any missing ports which are being blocked before they reach your logging tool. (Note that this technique is not quite as foolproof as the other approaches since ISPs could be blocking outbound packets from their customers, which the other approaches would detect but log-watching would not.)

After completing the experiments above, remember to return your system to its previous tight security and verify that everything is safe again by re-running any of our tests.

Checking a NAT Router's WAN Security

Residential broadband "NAT" routers which allow many computers to share a single Internet connection are becoming quite popular. We love them for the security they provide to the machines placed behind them since any NAT router functions as a natural and excellent hardware firewall.

However, the Internet or "WAN" (Wide Area Network) side connection of many NAT routers and DSL gateways is not as secure as it should be. Many routers ship with web, ftp, or Telnet management ports wide open! And many are still configured with their well-known default administrative passwords. Although the router may be protecting the machines behind it, it might not be protecting itself without your deliberate closing of remote "WAN" administration ports.

ShieldsUP! automatically tests your NAT router's WAN-side security because the router's WAN IP is the single public IP that connects your internal private network to the public Internet. When a test is initiated by any system behind a NAT router, we are testing the public-side security of the router itself and not the security of the individual machines which are located behind and protected by the router.

Adaptive IDENT Stealthing Experimentation

The IDENT protocol's port 113 is quite problematical and tricky to stealth. If the user's port 113 is completely stealthed, connections to some remote Internet servers such as eMail, Internet Relay Chat (IRC), and others, may be delayed or denied altogether. For this reason, many NAT routers and personal firewalls do not attempt to stealth port 113, they settle for leaving it closed. One of the first things that caught my eye about the ZoneAlarm personal firewall was that it was clever about handling port 113: It "adaptively stealthed" the port.

To understand the following discussion, you should familiarize yourself with the details of the IDENT protocol and port 113. Please read **port 113's Port Authority database page** before proceeding.

Even after many years, the (free) ZoneAlarm personal firewall from Zone Labs is the only personal firewall to "adaptively" stealth port 113. Unlike any other firewall or NAT router (any of which could also do the same) this allows port 113 to be stealthed to any passing Internet scanners or probes, but "unstealthed" for any valid IDENT connection attempts originating from remote servers with which the user's computer is attempting to connect. (Since this could easily be done by any personal firewall or even NAT routers, I am hopeful that this feature might yet appear in other products.)

"Adaptive Stealthing" means that when a TCP SYN packet arrives to request a connection to your machine's port 113, ZoneAlarm checks, on the fly, to see whether your machine currently has any sort of "relationship" with the remote machine (such as a pending outgoing connection attempt). If so, the remote machine is considered to be "friendly" and its IDENT request packet is allowed to pass through ZoneAlarm's firewall. But if the IDENT originating machine is not known to ZoneAlarm as a "friendly" machine, the connection requesting packet is dropped and discarded, rendering port 113 stealth to all unknown port scanners. It's very slick.

IDENT, ZoneAlarm, and ShieldsUP!

Even though your computer's web browser already has a relationship with the web server at GRC, our tests originate from a different "foreign" IP address. ZoneAlarm therefore drops incoming packets to port 113 from this different probing IP address and ZoneAlarm users see that port 113 is stealthed to passing Internet scans.

To demonstrate how ZoneAlarm (and perhaps someday other firewalls or NAT routers) selectively "unstealth" port 113 — but only for known "friendly" machines — we simply initiate a connection from your web browser to the ShieldsUP! scanning IP. Even though the connection attempt will ultimately fail (since there's no web server at the probing address), ZoneAlarm will note the outgoing attempt and will unstealth port 113 for subsequent probes.

- **Step One:** Verify that our scan currently show port 113 stealthed. (You may wish to use one of the other remote port tests which will be faster than an entire 1056-port grid scan.)

- **Step Two:** Open a secondary web browser window to initiate a connection to the probing IP. (Users of Microsoft Internet Explorer can press Ctrl-N to "clone" their current browser window.)

- **Step Three:** In the secondary web browser window, click this URL or enter this address:

http://4.79.142.206

This second connection attempt will ultimately fail, but ZoneAlarm will notice the effort, which is all that's necessary.

- **Step Four:** Finally, refresh the port probe window or repeat the scan to check your system's current port status. You should find that port 113 is no longer "stealth" to the probing IP address because you are attempting to connect to it and it has been determined to be "friendly".

- **Step Five:** If you're curious, stop and close the secondary web browser window and periodically refresh your port probe window to see how long the "friendly" status persists before Zone Alarm returns the probing IP to unknown status and port 113 to full stealth.

NOTE: Clicking the "http" link above may convince a clever firewall that the remote scanning IP is "friendly" and help to demonstrate its adaptive IDENT handling. But the packets sent to us with that link will **also** trigger our "Unsolicited Packet" detection since those packets were not received in direct response to our probes.

In order to reset the memory of these deliberately unsolicited packets you must redisplay the initial ShieldsUP! "Greetings" page. (That link will take you there.)

Click here to check your router now...

GRC's Instant UPnP Exposure Test

HOME

ShieldsUP!! Services

HELP

File Sharing | Common Ports | All Service Ports | Messenger Spam | Browser Headers

You may select any service from among those listed above . . .

User Specified Custom Port Probe | Lookup Specific Port Information

Or enter a port to lookup, or the ports for a custom probe to check, then choose the service. Your computer at IP 84.17.61.212 will be tested.

Jump To Top