

# ShieldsUP!!<sup>tm</sup>

Port Authority Edition – Internet Vulnerability Profiling  
by Steve Gibson, Gibson Research Corporation.

## Checking the Most Common and Troublesome Internet Ports

This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on **YOUR** computer. Since this is being done from **our** server, successful connections demonstrate which of your ports are "open" or visible and soliciting connections from passing Internet port scanners.

Your computer at IP:



Is being profiled. Please stand by. . .



Total elapsed testing time: 5.009 seconds

**PASSED**

**TruStealth  
Analysis**

**PASSED**

Your system has achieved a **perfect** "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

Port	Service	Status	Security Implications
<u>0</u>	<nil>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>21</u>	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>22</u>	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>23</u>	Telnet	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>25</u>	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>79</u>	Finger	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>80</u>	HTTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>110</u>	POP3	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>113</u>	IDENT	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>119</u>	NNTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>135</u>	RPC	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>139</u>	Net BIOS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>143</u>	IMAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>389</u>	LDAP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>443</u>	HTTPS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>445</u>	MSFT DS	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>1002</u>	ms-ils	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<u>1024</u>	DCOM	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

<a href="#">1025</a>	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<a href="#">1026</a>	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<a href="#">1027</a>	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<a href="#">1028</a>	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<a href="#">1029</a>	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<a href="#">1030</a>	Host	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<a href="#">1720</a>	H.323	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
<a href="#">5000</a>	UPnP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

### Text Summary

You may click on the Text Summary button to receive a condensed textual report of the Common Ports Probe findings displayed above.

You may also click on any port number link above to jump to detailed information about that port contained in our Port Authority database.

For help and information about the meaning and importance of "Open", "Closed" and "Stealth" port statuses, please see our [Internet Port Status Definitions](#) page.

You may press your browser's BACK button to return to the previous page, Re-run the Common Ports Probe test by "refreshing" this page, or select from among the other services available:

**ShieldsUP!! Services**

HOME 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 XXXXXXXXXX will be tested.



Gibson Research Corporation is owned and operated by Steve Gibson. The contents of this page are Copyright (c) 2010 Gibson Research Corporation. SpinRite, ShieldsUP, NanoProbe, and any other indicated trademarks are registered trademarks of Gibson Research Corporation, Laguna Hills, CA, USA. GRC's web and customer [privacy policy](#).

Jump  
To Top