



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:

173.218.9.135

Is being profiled. Please stand by. . .



Total elapsed testing time: 5.075 seconds

FAILED

**TruStealth
Analysis**

FAILED

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 Echo: PASSED — Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server.

Port	Service	Status	Security Implications
<u>0</u>	<nil>	Closed	Your computer has responded that this port exists but is currently closed to connections.
<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!

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

[Click here to check your router now...](#)

GRC's Instant UPnP Exposure Test

[HOME](#)

ShieldsUP!! Services

[HELP](#)

[File Sharing](#)

[Common Ports](#)

[All Service Ports](#)

[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 173.218.9.135 will be tested.



Gibson Research Corporation is owned and operated by Steve Gibson. The contents of this page are Copyright (c) 2020 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