

# Testing TLS/SSL encryption

Article Number: 649 | Rating: Unrated | Last Updated: Thu, Jan 16, 2020 4:58 PM

## testssl.sh

is a [free](#) command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as recent cryptographic flaws and more.

Name	Last Modified	Size	Type
<a href="#">2.6/</a>	2018-Nov-15 22:02:23	--	Directory
<a href="#">2.8/</a>	2018-Nov-15 22:46:12	--	Directory
<a href="#">2.9.5/</a>	2018-Nov-15 22:24:07	--	Directory
<a href="#">bleichenbacher/</a>	2018-Feb-23 18:00:33	--	Directory
<a href="#">openssl-1.0.2i-chacha.pm</a>	2016-Sep-26 23:15:22	--	Directory
<a href="#">.ipv6.contributed/</a>			
<a href="#">utils/</a>	2018-Nov-15 22:47:49	--	Directory
<a href="#">CREDITS.md</a>	2018-Oct-09 12:36:15	2.65KB	MD File
<a href="#">Dockerfile</a>	2018-Oct-09 12:36:15	412.00B	Unknown File
<a href="#">LICENSE.txt</a>	2014-May-03 11:04:22	17.59KB	TXT Type Document
<a href="#">OPENSSL-LICENSE.txt</a>	2017-May-09 13:14:16	6.13KB	TXT Type Document
<a href="#">etc+doc.tar.gz</a>	2018-Nov-15 22:32:16	889.75KB	GZ Compressed Archive
<a href="#">openssl-1.0.2k-chacha.p</a>	2017-May-12 18:11:02	9.51MB	GZ Compressed Archive
<a href="#">m.ipv6.Linux+FreeBSD.201705.tar.gz</a>			
<a href="#">openssl-1.0.2k-dev-chach</a>	2017-Jul-19 09:28:30	9.51MB	GZ Compressed Archive
<a href="#">a.pm.ipv6.Linux+FreeBS</a>			
<a href="#">D.tar.gz</a>			
<a href="#">openssl-</a>	2018-Nov-08 20:40:06	59.51KB	HTML File
<a href="#">iana.mapping.html</a>			
<a href="#">openssl-</a>	2016-Apr-15 12:36:23	4.24MB	X86_64 File

[ms14-066.Linux.x86\\_64](#)

[testssl.1.html](#)

2018-Dec-17 21:11:03

55.38KB

HTML File

[testssl.sh](#)

2018-Dec-06 11:25:32

879.78KB

SH File

[testssl\\_german\\_owasp\\_dan](#)

2018-Nov-18 13:53:38

1.11MB

PDF Type Document

[y.pdf](#)

## Key features

- Clear output: you can tell easily whether anything is good or bad
- Ease of installation: It works for Linux, Mac OSX, FreeBSD and WSL/MSYS2/Cygwin out of the box: no need to install or configure something, no gems, CPAN, pip or the like.
- Flexibility: You can test any SSL/TLS enabled and STARTTLS service, not only web servers at port 443
- Toolbox: Several command line options help you to run YOUR test and configure YOUR output
- Reliability: features are tested thoroughly
- Verbosity: If a particular check cannot be performed because of a missing capability on your client side, you'll get a warning
- Privacy: It's only you who sees the result, not a third party
- Freedom: It's 100% open source. You can look at the code, see what's going on and you can change it. Heck, even the development is open (github)
- Documentation: [Yes!](#)

Posted - Thu, Jan 16, 2020 4:58 PM. This article has been viewed 13450 times.

Online URL: <http://kb.ictbanking.net/article.php?id=649>