

NAME

stegbreak – launches brute-force dictionary attacks on JPG image

SYNOPSIS

stegdetect [**-q***v*] [**-r** *rules*] [**-f** *wordlist*] [**-t** *tests*] [**-c**] [*file ...*]

DESCRIPTION

The **stegbreak** states a brute-force dictionary attack against the specified JPG images.

The options are as follows:

- q** Only reports images for which the dictionary attack succeeded.
- v** Displays the version number of the software.
- r** *rules* Contains rules with transformations that will be applied to the words in the wordlist. The rules follow the same syntax as in Solar Designers password cracking program John the Ripper. The default is `rules.ini`.
- f** *wordlist* Specifies the file that contains the words for the dictionary attack. The default is `/usr/share/dict/words`.
- t** *tests* Sets the tests that are being run on the image. The following characters are understood:
 - o** The dictionary attack follows the embedding used by outguess.
 - p** The dictionary attack follows the embedding used by jphide.
 - j** The dictionary attack follows the embedding used by jsteg-shell.
 The default value is *p*.
- c** Specifies that the JPG images should be converted to a small sized object that contains all the information necessary for the dictionary attack. This can be used to reduce the size of the data set in distributed computing applications.

The **stegbreak** prints the filename, the embedding system and the password when the attack succeeded for an image. For jsteg-shell and outguess, it also prints analysis results from the built in `file` utility.

Pressing Ctrl-C causes a status line to be displayed, pressing Ctrl-C a second time within one second aborts the program.

EXAMPLES

stegbreak -t p auto.jpg

Launches a brute-force dictionary attack against `auto.jpg` assuming that information has been embedded with jphide.

FILES

`/usr/share/dict/words` default wordfile for the dictionary attack.
`/usr/local/share/stegbreak/rules.ini` rules on how to manipulate words for the dictionary attack, from John the Ripper.

SEE ALSO

`stegdetect(1)`

ACKNOWLEDGEMENTS

This program contains source code from Solar Designer's John the Ripper. It has been placed under a BSD-license with his permission.

This product includes software developed by Ian F. Darwin and others. The **stegbreak** utility uses Darwin's file magic to verify results from OutGuess key guessing.

Korejwa provided information on the data format used by JSteg Shell.

AUTHORS

The **stegbreak** utility has been developed by Niels Provos.