NAME

fail2ban - a set of server and client programs to limit brute force authentication attempts.

DESCRIPTION

Fail2Ban consists of a client, server and configuration files to limit brute force authentication attempts.

The server program **fail2ban-server** is responsible for monitoring log files and issuing ban/unban commands. It gets configured through a simple protocol by **fail2ban-client**, which can also read configuration files and issue corresponding configuration commands to the server.

For details on the configuration of fail2ban see the fail2ban-jail.conf(5) manual page. A jail (as specified in jail.conf) couples filters and actions definitions for any given list of files to get monitored.

For details on the command-line options of fail2ban-server see the fail2ban-server(1) manual page.

For details on the command-line options and commands for configuring the server via fail2ban-client see the fail2ban-client(1) manual page.

For testing regular expressions specified in a filter using the fail2ban-regex program may be of use and its manual page is fail2ban-regex(1).

LIMITATION

Fail2Ban is able to reduce the rate of incorrect authentications attempts however it cannot eliminate the risk that weak authentication presents. Configure services to use only two factor or public/private authentication mechanisms if you really want to protect services.

A local user is able to inject messages into syslog and using a Fail2Ban jail that reads from syslog, they can effectively trigger a DoS attack against any IP. Know this risk and configure Fail2Ban/grant shell access accordingly.

FILES

*/etc/fail2ban/**

AUTHOR

Manual page written by Daniel Black and Yaroslav Halchenko

REPORTING BUGS

Report bugs to https://github.com/fail2ban/fail2ban/issues

COPYRIGHT

SEE ALSO

fail2ban-server(1) fail2ban-client(1) fail2ban-regex(1) fail2ban-jail.conf(5)