Introduction

Fail2ban is an intrusion prevention software framework which protects computer servers from brute-force attacks.[1] Written in the Python programming language, it is able to run on POSIX systems that have an interface to a packet-control system or firewall installed locally, for example, iptables or TCP Wrapper.

Fail2ban operates by monitoring log files (e.g. /var/log/auth.log, /var/log/apache/access.log, etc.) for selected entries and running scripts based on them. Most commonly this is used to block selected IP addresses that may belong to hosts that are trying to breach the system's security. It can ban any host IP that makes too many login attempts or performs any other unwanted action within a time frame defined by the administrator. Fail2ban is typically set up to unban a blocked host within a certain period, so as to not “lock out” any genuine connections that may have been temporarily misconfigured. However, an unban time of several minutes is usually enough to stop a network connection being flooded by malicious connections, as well as reducing the likelihood of a successful dictionary attack.

Fail2ban can perform multiple actions whenever an abusive IP is detected:[2] update Netfilter/iptables or PF firewall rules, TCP Wrapper's hosts.deny table, to reject an abuser's IP address; email notifications; or any user-defined action that can be carried out by a Python script.

The standard configuration ships with filters for Apache, Lighttpd, sshd, vsftpd, qmail, Postfix and Courier Mail Server.[3] Filters are defined by Python regexes, which may be conveniently customized by an administrator familiar with regular expressions. A combination of a filter and an action is known as a “jail” and is what causes a malicious host to be blocked from accessing specified network services. As well as the examples that are distributed with the software, a “jail” may be created for any network-facing process that creates a log file of access.

Content

Resources

- http://www.fail2ban.org/wiki/index.php/Main_Page