**FAIL2BAN**

Fail2Ban is a tool that can be used to monitor log files and automatically ban IP addresses that have too many failed login attempts. Here's how to use Fail2Ban to lock user accounts after failed attempts in Ubuntu and CentOS:

Install Fail2Ban: First, you need to install Fail2Ban on your system. You can do this by running the following command:

For Ubuntu**: sudo apt-get install fail2ban**

For CentOS: sudo yum install epel-release && sudo yum install fail2ban

Configure Fail2Ban: Once Fail2Ban is installed, you need to configure it to monitor the appropriate log files and to take action when too many failed login attempts occur. The configuration file for Fail2Ban is located at /etc/fail2ban/jail.conf. Open this file with your preferred text editor and add the following lines at the end of the file:

makefile

Copy code

[sshd]

enabled = true

port = ssh

filter = sshd

logpath = /var/log/auth.log

maxretry = 3

bantime = 600

This configuration will monitor the SSH log files (/var/log/auth.log) and will ban IP addresses that have 3 or more failed login attempts for a period of 10 minutes (600 seconds).

Restart Fail2Ban: Once you have made changes to the Fail2Ban configuration file, you need to restart Fail2Ban to apply the changes. You can do this by running the following command:

Copy code

sudo systemctl restart fail2ban

Test Fail2Ban: To test that Fail2Ban is working correctly, you can try logging in to your system with an incorrect password several times. After the third failed attempt, your IP address should be banned for 10 minutes.

That's it! Fail2Ban will now monitor your log files and ban IP addresses that have too many failed login attempts, helping to keep your system secure.

Regenerate response