==== fail2ban untuk memonitor aktivitas mencurigakan dan memblokir IP yang mencoba mengakses file sensitif seperti .env. ====

1. *sudo apt-get install fail2ban*
2. **Konfigurasi jail untuk nginx**:
   sudo nano /etc/fail2ban/jail.local
   Tambahkan konfigurasi berikut:
   [nginx-env]
   enabled = true
   port = http,https
   filter = nginx-env
   logpath = /var/log/nginx/access.log
   maxretry = 1
   bantime = 86400 # Ban for one day

```
[nginx-env]
enabled  = true
port     = http,https
filter   = nginx-env
logpath  = /var/log/nginx/access.log
maxretry = 1
bantime  = 86400  # Ban for one day
```

3. **Buat filter untuk nginx**:
   sudo nano /etc/fail2ban/filter.d/nginx-env.conf
   Tambahkan filter regex berikut:
   [Definition]
   failregex = <HOST> -.*GET.* /.env

```
[Definition]
failregex = <HOST> -.*GET.* /.env
```

4. *sudo systemctl restart fail2ban*
5. Gunakan perintah berikut untuk memeriksa status fail2ban dan memastikan bahwa jail yang Anda konfigurasi berjalan:
   sudo fail2ban-client status "nama-file"

```bash
$ sudo fail2ban-client status nginx-env
Status for the jail: nginx-env
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     5
|  `- File list:        /var/log/nginx/access.log
`- Actions
   |- Currently banned: 2
   |- Total banned:     2
   `- Banned IP list:   128.1.227.230 72.14.201.147
```

6. **Periksa IP yang Terblokir**
   sudo iptables -L -n
7. **Lepaskan blokir IP**:
   sudo fail2ban-client set nginx-file-manager unbanip 114.10.98.205
8. **Melihat daftar total dibanned ketik perintah**
   *sudo zgrep 'Ban' /var/log/fail2ban.log**

```
eoffice-oki@eoffice-oki:/var/log/nginx$ sudo zgrep 'Ban' /var/log/fail2ban.log*
2024-07-27 04:21:40,825 fail2ban.actions        [666145]: NOTICE  [nginx-file-manager] Ban 114.10.98.205
2024-07-27 04:33:09,663 fail2ban.actions        [666145]: NOTICE  [nginx-file-manager] Ban 114.10.98.205
2024-07-27 04:33:34,910 fail2ban.actions        [666145]: NOTICE  [nginx-file-manager] Ban 114.10.98.205
2024-07-27 04:41:49,515 fail2ban.actions        [666145]: NOTICE  [nginx-file-manager] Ban 128.1.227.232
2024-07-27 05:57:35,042 fail2ban.actions        [666145]: NOTICE  [nginx-file-manager] Ban 114.10.99.30
2024-07-27 06:24:11,781 fail2ban.actions        [787122]: NOTICE  [nginx-filemanager] Ban 128.1.227.232
2024-07-27 06:29:10,966 fail2ban.actions        [790786]: NOTICE  [nginx-filemanager] Restore Ban 128.1.227.232
2024-07-27 06:29:45,630 fail2ban.actions        [791369]: NOTICE  [nginx-filemanager] Restore Ban 128.1.227.232
2024-07-27 06:32:10,403 fail2ban.actions        [792999]: NOTICE  [nginx-filemanager] Restore Ban 128.1.227.232
2024-07-27 06:32:30,604 fail2ban.actions        [793354]: NOTICE  [nginx-filemanager] Restore Ban 128.1.227.232
```

9. **Hapus File Database (Opsional)**
   sudo systemctl stop fail2ban
   sudo rm /var/lib/fail2ban/fail2ban.sqlite3
   sudo systemctl start fail2ban
10. **Restart Jail untuk Menghapus Semua Blokir:**
    sudo fail2ban-client restart nginx-env
11. **Jika Ingin menghapus daftar IP**
    *Sudo rm -rf /var/log/fail2ban.log**