????????? fail2ban (?????? ?? ?????????)

Fail2ban служба в Linux которая по log–файлам приложений может обнаружить злоумышленника и заблокировать его IP адрес. Программа умеет бороться с различными атаками на все популярные *NIX–сервисы, такие как Apache, Nginx, Guacamole, sshd, Exim, Postfix и другие. В данной статье мы будем защищать службу SSH.

Установка:

```
apt-get -y install fail2ban
```

Включаем автозапуск и запускаем:

```
systemctl enable fail2ban
systemctl status fail2ban
systemctl start fail2ban
```

Правим конфиг файл:

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
vi /etc/fail2ban/jail.local
```

Содержимое файла jail.local:

```
[DEFAULT]
bantime  = 1d
findtime  = 4h
maxretry = 2

[sshd]
enabled = true
mode = aggressive
port = 2222
# incremental banning:
bantime.increment = true
# default factor (causes increment - 1h -> 1d 2d 4d 8d 16d 32d ...):
bantime.factor = 24
```

```
# max banning time = 6 week:
bantime.maxtime = 6w
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

В конфиге выше fail2ban смотрит порт 2222 службы ssh, будет блокировка на 1 день источника подключения в случае 2 неверных попыток ввода в течение 4 часов, блокировка инкрементальная, в случае если этот же источник повторит неверные действия - блок на 2 дня и так до максимального срока блокировки до 6 недель.

Перезапуск службы для применения новой конфигурации:

```
systemctl restart fail2ban
```

Проверка журнала fail2ban:

```
less /var/log/fail2ban.log
```

Подсчет количества блокирововк по журналу:

```
cat /var/log/fail2ban.log | grep "\[sshd\] Ban" | wc -l
```

Просмотр заблокированных IP-адресов:

```
fail2ban-client status | grep "Jail list" | sed -E 's/^[^:]+:[ \t]+//' | sed 's/,//g'
```

Разблокировка адреса:

```
fail2ban-client set YOURJAILNAMEHERE unbanip IPADDRESSHERE
```

Revision #3
Created 2024-04-01 12:19:43 UTC by Boris Rzr
Updated 2024-04-01 13:08:04 UTC by Boris Rzr