Отчёт по лабораторной работе 16

Базовая защита от атак типа «brute force»

Метвалли Ахмед Фарг Набеех

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

2 Выполнение

2.1 Установка и запуск Fail2ban

1. На сервер был установлен пакет Fail2ban с помощью пакетного менеджера. После установки система добавила необходимые модули, включая серверную часть и средства интеграции с firewalld.

2. При первой попытке запуска была допущена ошибка в имени сервиса, после чего выполнен корректный запуск Fail2ban и добавление его в автозагрузку. Система подтвердила создание символьной ссылки для автоматического запуска.

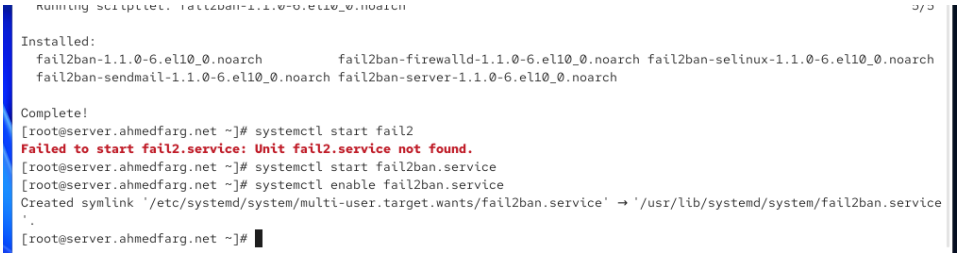

Рис. 2.1: Установка и запуск сервиса fail2ban

2.2 Просмотр журнала Fail2ban

3. Был выполнен просмотр журнала `/var/log/fail2ban.log`.
   При запуске без прав root появилась ошибка доступа, после чего журнал был успешно открыт с использованием привилегий.

В журнале зафиксировано:

– запуск Fail2ban-сервера;

– запуск наблюдателя;

– подключение к базе данных;

– создание новой базы.

```
[ahmedfarg@server.ahmedfarg.net ~]$
[ahmedfarg@server.ahmedfarg.net ~]$ tail -f /var/log/fail2ban.log
tail: cannot open '/var/log/fail2ban.log' for reading: Permission denied
tail: no files remaining
[ahmedfarg@server.ahmedfarg.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for ahmedfarg:
2025-11-08 10:32:57,391 fail2ban.server         [14445]: INFO    --------------------------------------------------
2025-11-08 10:32:57,391 fail2ban.server         [14445]: INFO    Starting Fail2ban v1.1.0
2025-11-08 10:32:57,391 fail2ban.observer       [14445]: INFO    Observer start...
2025-11-08 10:32:57,395 fail2ban.database       [14445]: INFO    Connected to fail2ban persistent database '/var/lib/fail2
ban/fail2ban.sqlite3'
2025-11-08 10:32:57,396 fail2ban.database       [14445]: WARNING New database created. Version '4'
```

Рис. 2.2: Просмотр журнала /var/log/fail2ban.log

2.3 Создание локального файла конфигурации

4. Создан файл локальных настроек `/etc/fail2ban/jail.d/customisation.local`.

5. В файл добавлены базовые параметры и включена защита SSH с использованием стандартного порта и альтернативного порта 2022.

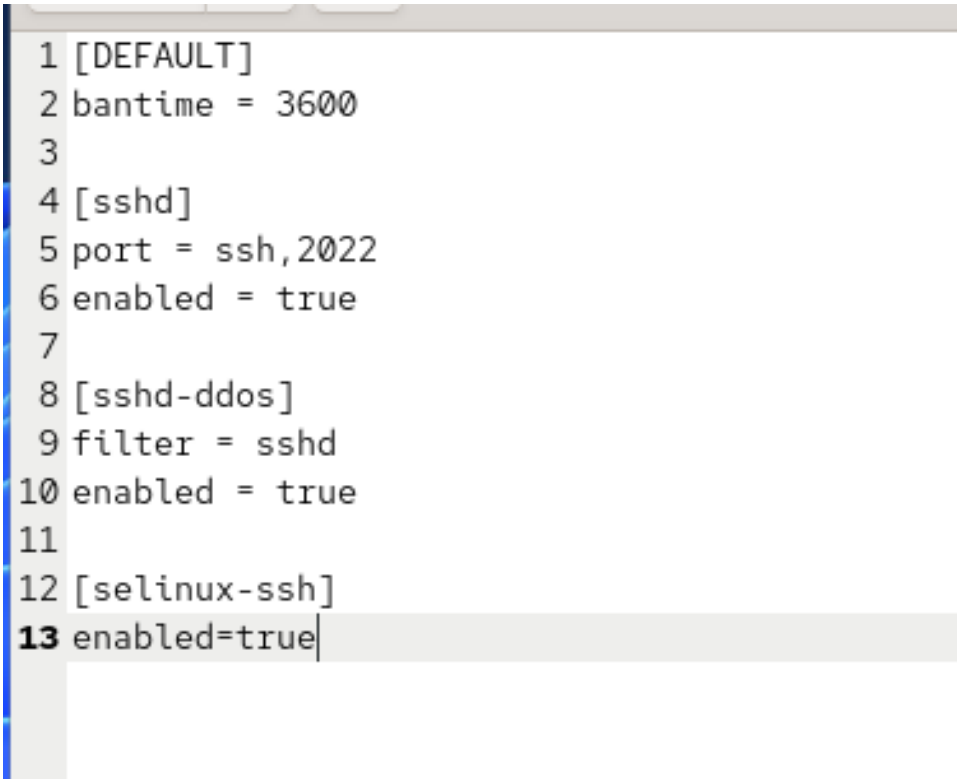

Рис. 2.3: Базовая локальная конфигурация Fail2ban (SSH-защита)

2.4 Перезапуск Fail2ban и проверка журналов (SSH)

6. Сервис Fail2ban был перезапущен для применения новой конфигурации.

7. В журнале зафиксировано создание и запуск тюрем для SSH, включая защиту от DDoS и интеграцию с SELinux.
   Все компоненты успешно инициализированы и запущены.

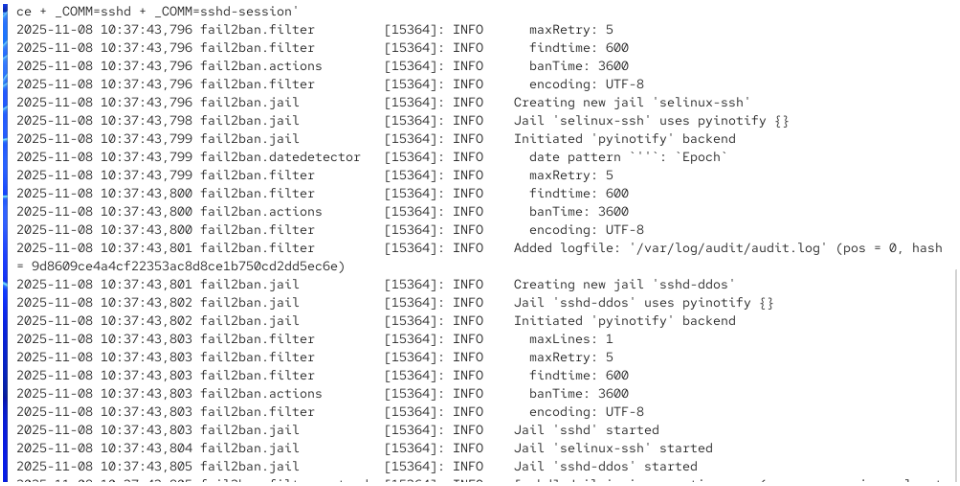

Рис. 2.4: Создание и запуск SSH-тюрем Fail2ban

2.5 Включение защиты HTTP-сервисов

8. В локальной конфигурации были включены тюрьмы для защиты HTTP-сервисов Apache.

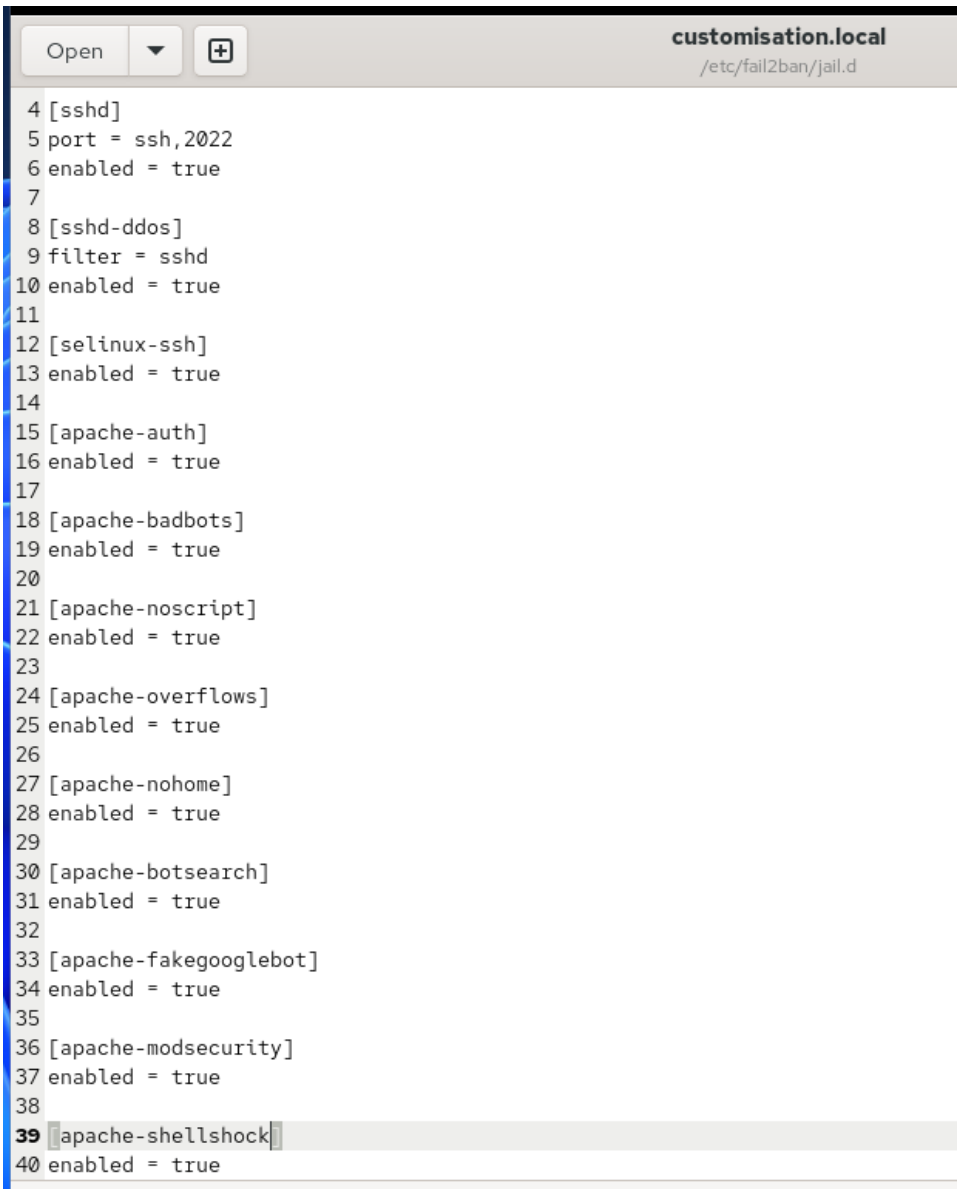

Рис. 2.5: Включение защиты HTTP-сервисов в customisation.local

9. Сервис Fail2ban перезапущен.

10. Просмотр журнала показал создание и запуск всех HTTP-тюрем.

    Fail2ban успешно подключился к логам веб-сервера и начал их мониторинг.

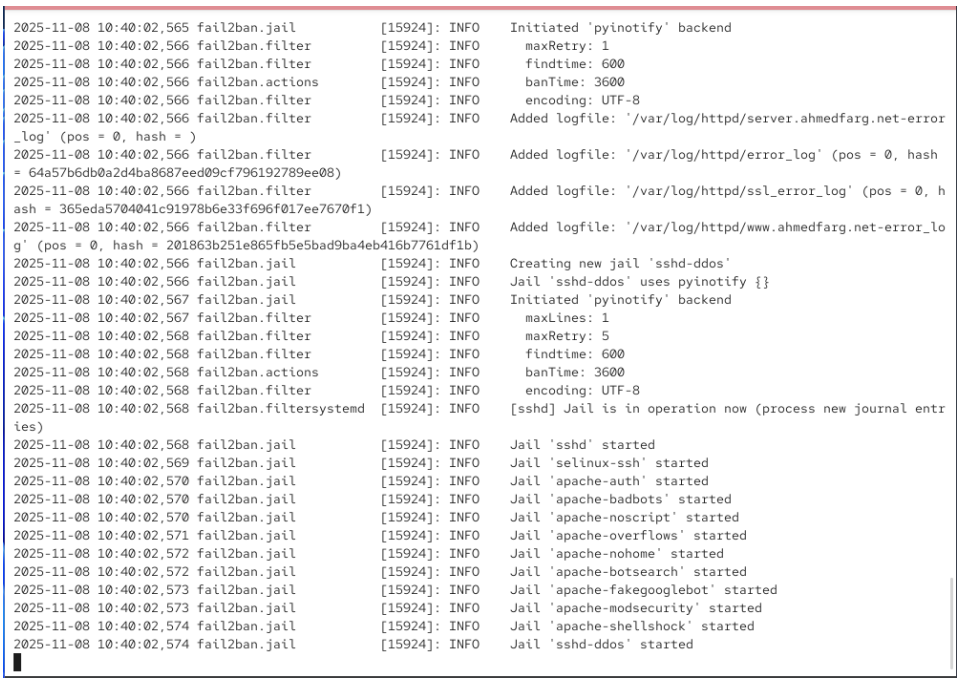

Рис. 2.6: Запуск HTTP-тюрем Fail2ban

2.6 Включение защиты почтовых сервисов

11. В локальной конфигурации были активированы тюрьмы для защиты почтовых сервисов Postfix и Dovecot.

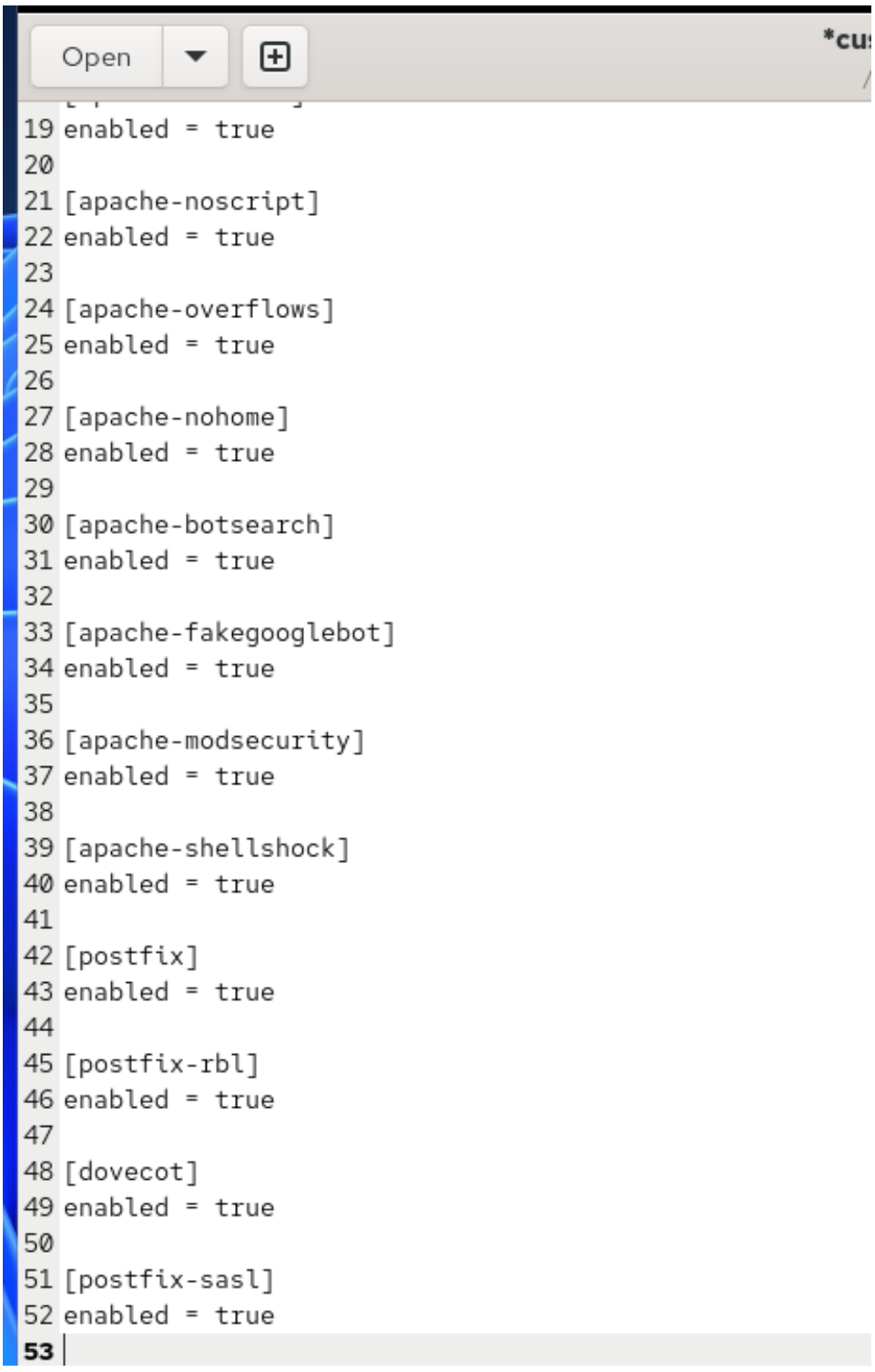

Рис. 2.7: Добавление тюрем защиты почты

12. Сервис Fail2ban вновь перезапущен.

13. В журнале зафиксировано создание и запуск всех почтовых тюрем.

    Тюрьмы перешли в рабочий режим и начали обработку новых записей журналов.

```
2025-11-08 10:41:47,746 fail2ban.filter         [16208]: INFO      findtime: 600
2025-11-08 10:41:47,746 fail2ban.actions        [16208]: INFO      banTime: 3600
2025-11-08 10:41:47,746 fail2ban.filter         [16208]: INFO      encoding: UTF-8
2025-11-08 10:41:47,746 fail2ban.filtersystemd  [16208]: INFO    [sshd] Jail is in operation now (process new journal entr
ies)
2025-11-08 10:41:47,747 fail2ban.jail           [16208]: INFO    Jail 'sshd' started
2025-11-08 10:41:47,748 fail2ban.jail           [16208]: INFO    Jail 'selinux-ssh' started
2025-11-08 10:41:47,750 fail2ban.jail           [16208]: INFO    Jail 'apache-auth' started
2025-11-08 10:41:47,751 fail2ban.jail           [16208]: INFO    Jail 'apache-badbots' started
2025-11-08 10:41:47,752 fail2ban.jail           [16208]: INFO    Jail 'apache-noscript' started
2025-11-08 10:41:47,752 fail2ban.jail           [16208]: INFO    Jail 'apache-overflows' started
2025-11-08 10:41:47,753 fail2ban.jail           [16208]: INFO    Jail 'apache-nohome' started
2025-11-08 10:41:47,753 fail2ban.jail           [16208]: INFO    Jail 'apache-botsearch' started
2025-11-08 10:41:47,753 fail2ban.jail           [16208]: INFO    Jail 'apache-fakegooglebot' started
2025-11-08 10:41:47,753 fail2ban.jail           [16208]: INFO    Jail 'apache-modsecurity' started
2025-11-08 10:41:47,754 fail2ban.jail           [16208]: INFO    Jail 'apache-shellshock' started
2025-11-08 10:41:47,754 fail2ban.jail           [16208]: INFO    Jail 'postfix' started
2025-11-08 10:41:47,754 fail2ban.jail           [16208]: INFO    Jail 'postfix-rbl' started
2025-11-08 10:41:47,755 fail2ban.jail           [16208]: INFO    Jail 'dovecot' started
2025-11-08 10:41:47,756 fail2ban.filtersystemd  [16208]: INFO    [dovecot] Jail is in operation now (process new journal e
ntries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd  [16208]: INFO    [postfix-sasl] Jail is in operation now (process new jour
nal entries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd  [16208]: INFO    [postfix-rbl] Jail is in operation now (process new journ
al entries)
2025-11-08 10:41:47,756 fail2ban.filtersystemd  [16208]: INFO    [postfix] Jail is in operation now (process new journal e
ntries)
2025-11-08 10:41:47,756 fail2ban.jail           [16208]: INFO    Jail 'postfix-sasl' started
2025-11-08 10:41:47,757 fail2ban.jail           [16208]: INFO    Jail 'sshd-ddos' started
```

Рис. 2.8: Запуск тюрем Fail2ban для почтовых сервисов

2.7 Просмотр статуса Fail2ban

1. На сервере был выполнен просмотр общего статуса Fail2ban.

   Отобразилось количество активных тюрем (16) и их список.

2. Далее был просмотрен статус тюрьмы SSH (`sshd`).

   На этом этапе ошибок входа и заблокированных адресов не было.

```
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# fail2ban-client status
Status
|- Number of jail:      16
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, ap
ache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-d
dos
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.ahmedfarg.net ~]# fail2ban-client set sshd maxretry 2
2
```

Рис. 2.9: Статус SSH-тюрьмы

2.8 Установка лимита ошибок и проверка блокировки

3. Максимальное количество ошибок входа для SSH было уменьшено до двух.

4. С клиента выполнены входы по SSH с неверным паролем.

5. После этого вновь просмотрен статус SSH-защиты.
   Fail2ban зафиксировал ошибки входа и заблокировал IP клиента.
   Забаненный адрес появился в списке.

6. Затем IP-адрес клиента был разблокирован.

7. Повторный просмотр статуса показал отсутствие блокировки.

```
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.30
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.ahmedfarg.net ~]#
```

Рис. 2.10: Разблокировка IP-адреса

2.9 Игнорирование IP-адреса клиента

8. В конфигурационный файл было добавлено исключение IP клиента, поместив его в список игнорируемых адресов (`ignoreip`).
   Это предотвращает дальнейший бан данного источника.

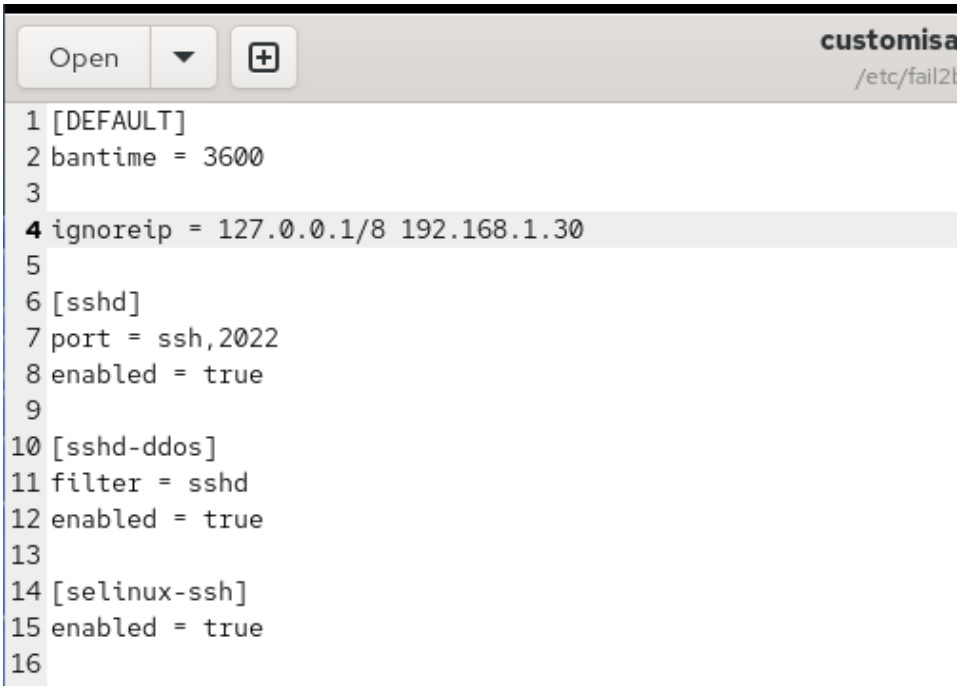

Рис. 2.11: Добавление ignoreip в конфигурацию

9. Сервис Fail2ban перезапущен.

10. В журнале событий появились сообщения о запуске тюрем и игнорировании указанного IP-адреса.

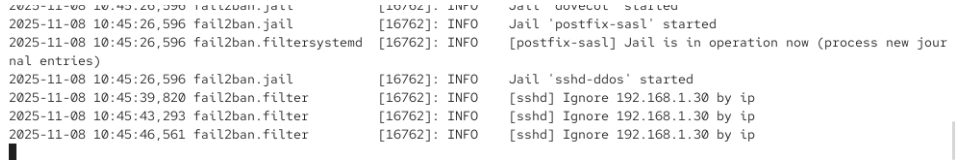

Рис. 2.12: Журнал Fail2ban после применения ignoreip

11. Повторная попытка входа с клиента с неверным паролем не вызвала блокировки — статус тюрьмы подтверждает отсутствие забаненных адресов.

```
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.ahmedfarg.net ~]#
```

Рис. 2.13: Отсутствие блокировок после ignoreip

2.10 Создание provisioning-скрипта

1. На виртуальной машине **server** создан каталог для размещения конфигурации Fail2ban внутри структуры Vagrant:

   – выполнён переход в каталог `/vagrant/provision/server/`;

   – создан подкаталог `protect/etc/fail2ban/jail.d`;

   – файл локальной конфигурации был скопирован туда.

```
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# cd /vagrant/provision/server/
[root@server.ahmedfarg.net server]# mkdir -p /vagrant/provision/server/protect/fail2ban/jail.d
[root@server.ahmedfarg.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/fail2
ban/jail.d
[root@server.ahmedfarg.net server]# touch protect.sh
[root@server.ahmedfarg.net server]#
```

Рис. 2.14: Создание каталога и копирование конфигурации

2. В каталоге `/vagrant/provision/server/` создан исполняемый файл `protect.sh`, содержащий автоматизацию установки Fail2ban, копирования конфигураций и запуска сервиса.

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install fail2ban
echo "Copy configuration files"
cp -R /vagrant/provision/server/protect/etc/* /etc
restorecon -vR /etc
echo "Start fail2ban service"
systemctl enable fail2ban
systemctl start fail2ban

```

Рис. 2.15: Содержимое protect.sh

3 Заключение

Fail2ban был успешно установлен, настроен и протестирован для защиты SSH-, HTTP- и почтовых сервисов.
Проведена проверка блокировки и разблокировки IP-адресов, добавление исключений и автоматизация конфигурации средствами Vagrant.

4 Контрольные вопросы

1. **Поясните принцип работы Fail2ban.**
   Fail2ban анализирует журналы сервисов, выявляет повторяющиеся ошибки аутентификации или подозрительные действия и временно блокирует IP-адрес источника через firewall.

2. **Настройки какого файла более приоритетны: `jail.conf` или `jail.local`?**
   Файл `jail.local` имеет более высокий приоритет и его настройки переопределяют параметры из `jail.conf`.

3. **Как настроить оповещение администратора при срабатывании Fail2ban?**
   Для этого в тюрьме необходимо выбрать действие (action), предусматривающее отправку email, например `action_mw` или `action_mwl`, и указать почтовый адрес администратора.

4. **Поясните построчно настройки по умолчанию в конфигурационном файле, относящиеся к веб-службе.**
   – указание имени тюрьмы для веб-сервера;
   – включение или выключение фильтра;
   – выбор фильтра, анализирующего журнал веб-сервера;
   – определение путей к логам веб-службы;
   – параметр `maxretry` — число ошибок до блокировки;
   – `findtime` — период, за который считаются ошибки;
   – `bantime` — длительность блокировки.

5. **Поясните построчно настройки по умолчанию для почтовой службы.**
   – включение тюрем для Postfix и Dovecot;
   – выбор фильтров, анализирующих журналы почтовых сервисов;
   – указание файлов логов Postfix и Dovecot;
   – параметры попыток входа (`maxretry`), времени учёта (`findtime`) и длительности блокировки (`bantime`).

6. **Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где посмотреть список действий?**
   Fail2ban может: блокировать IP через firewall, отправлять уведомления, выполнять сценарии, изменять маршруты, вносить записи в списки блокировки.
   Описание действий приводится в каталоге `/etc/fail2ban/action.d/`.

7. **Как получить список действующих правил Fail2ban?**
   Это выполняется через `fail2ban-client status`, где отображаются активные тюрьмы и их параметры.

8. **Как получить статистику заблокированных Fail2ban адресов?**
   Для конкретной тюрьмы используется `fail2ban-client status <jail>`, где указан список заблокированных IP.

9. **Как разблокировать IP-адрес?**
   Через команду `fail2ban-client set <jail> unbanip <ip>`, удаляющую адрес из списка заблокированных.