Отчёт по лабораторной работе №16

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Содержание

# 1. Цель работы

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

# 2. Выполнение лабораторной работы

## 2.1 Защита с помощью Fail2ban

### 2.1.1 Установка Fail2ban

На сервере выполнена установка пакета fail2ban с использованием менеджера пакетов dnf. В процессе установки также автоматически установлены зависимости: fail2ban-firewalld, fail2ban-selinux, fail2ban-sendmail, fail2ban-server. Установка выполнена из репозитория epel ([рис. 1](#fig-1)).

|  |
| --- |
| Рисунок 1: Установка пакета fail2ban и зависимостей через dnf |

### 2.1.2 Запуск и добавление службы в автозагрузку

После установки выполнен запуск службы fail2ban командой systemctl start fail2ban, затем служба добавлена в автозагрузку командой systemctl enable fail2ban. Создана символическая ссылка в каталоге multi-user.target.wants, что подтверждает корректную регистрацию службы в системе ([рис. 2](#fig-2)).

|  |
| --- |
| Рисунок 2: Запуск службы fail2ban и включение автозагрузки |

### 2.1.3 Контроль журнала событий Fail2ban

В дополнительном терминале выполнен мониторинг журнала /var/log/fail2ban.log с помощью команды tail -f. В журнале зафиксирован запуск сервера Fail2ban версии 1.1.0, инициализация observer и создание новой базы данных fail2ban.sqlite3 ([рис. 3](#fig-3)).

|  |
| --- |
| Рисунок 3: Просмотр журнала fail2ban.log в реальном времени |

### 2.1.4 Создание файла локальной конфигурации

Создан файл локальной конфигурации /etc/fail2ban/jail.d/customisation.local с использованием команды touch, после чего выполнено его редактирование в текстовом редакторе nano ([рис. 6](#fig-5)).

|  |
| --- |
| Рисунок 4: Создание и перезапуск службы после настройки |

### 2.1.5 Настройка параметров блокирования и защиты SSH

В файле /etc/fail2ban/jail.d/customisation.local заданы параметры:

* В секции [DEFAULT] установлено время блокировки bantime = 3600 секунд (1 час).
* Включена защита SSH в секциях [sshd], [sshd-ddos], [selinux-ssh].
* Для sshd указан порт ssh,2022.
* Для всех перечисленных служб установлен параметр enabled = true ([рис. 5](#fig-4)).

|  |
| --- |
| Рисунок 5: Конфигурация customisation.local с параметрами bantime и SSH |

### 2.1.6 Перезапуск службы Fail2ban

После внесения изменений выполнен перезапуск службы командой systemctl restart fail2ban, что обеспечивает применение новой конфигурации ([рис. 6](#fig-5)).

|  |
| --- |
| Рисунок 6: Создание и перезапуск службы после настройки |

### 2.1.7 Просмотр журнала событий Fail2ban

После перезапуска службы выполнен мониторинг журнала /var/log/fail2ban.log. В журнале зафиксирована инициализация backend pyinotify, параметры maxLines, maxRetry, findtime, banTime = 3600, а также запуск jail-модулей sshd, selinux-ssh, sshd-ddos ([рис. 7](#fig-6)).

|  |
| --- |
| Рисунок 7: Журнал запуска jail-модулей SSH в fail2ban |

### 2.1.8 Включение защиты HTTP

В файле /etc/fail2ban/jail.d/customisation.local активированы jail-модули для HTTP-сервера Apache: apache-auth, apache-badbots, apache-noscript, apache-overflows, apache-nohome, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-shellshock. Для каждого модуля установлен параметр enabled = true ([рис. 8](#fig-7)).

|  |
| --- |
| Рисунок 8: Конфигурация HTTP jail-модулей в customisation.local |

### 2.1.9 Перезапуск Fail2ban после настройки HTTP

После внесения изменений выполнен перезапуск службы systemctl restart fail2ban, что обеспечило загрузку новых jail-настроек ([рис. 10](#fig-8)).

|  |
| --- |
| Рисунок 9: Журнал запуска HTTP jail-модулей |

### 2.1.10 Контроль журнала после включения HTTP-защиты

В журнале /var/log/fail2ban.log зафиксирован запуск jail-модулей apache-auth, apache-badbots, apache-noscript, apache-overflows, apache-nohome, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-shellshock, а также повторная активация sshd-ddos ([рис. 10](#fig-8)).

|  |
| --- |
| Рисунок 10: Подтверждение запуска HTTP jail-модулей в журнале |

### 2.1.11 Включение защиты почтовых сервисов

В файле /etc/fail2ban/jail.d/customisation.local активированы jail-модули для почтовых сервисов: postfix, postfix-rbl, dovecot, postfix-sasl. Для каждого модуля установлен параметр enabled = true ([рис. 11](#fig-9)).

|  |
| --- |
| Рисунок 11: Конфигурация jail-модулей для почтовых сервисов |

### 2.1.12 Перезапуск Fail2ban после настройки почтовых служб

После добавления конфигурации выполнен перезапуск службы fail2ban для применения изменений ([рис. 13](#fig-10)).

|  |
| --- |
| Рисунок 12: Журнал запуска jail-модулей почтовых сервисов |

### 2.1.13 Контроль журнала после включения почтовой защиты

В журнале событий зафиксирован запуск jail-модулей postfix, postfix-rbl, dovecot, postfix-sasl. Для каждого модуля отображается сообщение Jail is in operation now, что подтверждает успешную активацию защиты почтовых сервисов ([рис. 13](#fig-10)).

|  |
| --- |
| Рисунок 13: Подтверждение работы jail-модулей почтовых сервисов |

## 2.2 Проверка работы Fail2ban

### 2.2.1 Просмотр общего статуса Fail2ban

На сервере выполнена команда fail2ban-client status. В выводе отображено общее количество jail-модулей (16) и их список, включая apache-\*, dovecot, postfix, sshd, sshd-ddos, selinux-ssh и другие. Это подтверждает активную работу всех ранее настроенных модулей ([рис. 16](#fig-11)).

|  |
| --- |
| Рисунок 14: Общий статус fail2ban-client |

### 2.2.2 Просмотр статуса защиты SSH

Выполнена команда fail2ban-client status sshd. В разделе Filter указаны значения Currently failed: 0, Total failed: 0. В разделе Actions значения Currently banned: 0, Total banned: 0, список заблокированных IP-адресов отсутствует. Это подтверждает отсутствие попыток неуспешной аутентификации на момент проверки ([рис. 16](#fig-11)).

|  |
| --- |
| Рисунок 15: Статус jail-модуля sshd до проверки |

### 2.2.3 Установка максимального количества ошибок

Выполнена команда fail2ban-client set sshd maxretry 2, устанавливающая параметр maxretry = 2 для jail-модуля sshd. После двух неудачных попыток входа IP-адрес клиента должен быть заблокирован ([рис. 16](#fig-11)).

|  |
| --- |
| Рисунок 16: Установка параметра maxretry для sshd |

### 2.2.4 Попытка входа по SSH с неправильным паролем

С клиента выполнена попытка подключения к серверу по SSH с использованием неверного пароля. После нескольких попыток аутентификации сервер возвращает сообщение Permission denied, что фиксируется Fail2ban как ошибки входа ([рис. 17](#fig-12)).

|  |
| --- |
| Рисунок 17: Попытки входа по SSH с неверным паролем |

### 2.2.5 Проверка блокировки IP-адреса

На сервере повторно выполнена команда fail2ban-client status sshd. В разделе Actions указано Currently banned: 1, Total banned: 1, а в списке Banned IP list отображён адрес клиента 192.168.1.30. Это подтверждает успешную блокировку IP-адреса после превышения установленного порога ошибок ([рис. 18](#fig-13)).

|  |
| --- |
| Рисунок 18: Блокировка IP-адреса клиента в sshd |

### 2.2.6 Разблокировка IP-адреса клиента

Выполнена команда fail2ban-client set sshd unbanip 192.168.1.30, снимающая блокировку с IP-адреса клиента ([рис. 19](#fig-14)).

|  |
| --- |
| Рисунок 19: Команда разблокировки IP-адреса клиента |

### 2.2.7 Проверка снятия блокировки

Повторно выполнена команда fail2ban-client status sshd. В разделе Actions указано Currently banned: 0, список заблокированных IP-адресов пуст. Это подтверждает успешное снятие блокировки клиента ([рис. 20](#fig-15)).

|  |
| --- |
| Рисунок 20: Статус sshd после снятия блокировки |

### 2.2.8 Добавление игнорирования IP-адреса клиента

В файл /etc/fail2ban/jail.d/customisation.local в секции [DEFAULT] добавлен параметр ignoreip = 127.0.0.1/8 192.168.1.30, где 192.168.1.30 — IP-адрес клиента. Параметр ignoreip исключает указанный адрес из процедуры блокировки независимо от количества ошибок аутентификации ([рис. 21](#fig-16)).

|  |
| --- |
| Рисунок 21: Добавление параметра ignoreip в customisation.local |

### 2.2.9 Перезапуск службы Fail2ban

После изменения конфигурации выполнен перезапуск службы командой systemctl restart fail2ban для применения параметра ignoreip ([рис. 22](#fig-17)).

|  |
| --- |
| Рисунок 22: Попытка входа с клиента после изменения конфигурации |

### 2.2.10 Просмотр журнала событий

В журнале /var/log/fail2ban.log отображаются сообщения вида [sshd] Ignore 192.168.1.30 by ip и [selinux-ssh] Ignore 192.168.1.30 by ip, что подтверждает корректную обработку параметра ignoreip и исключение клиента из механизма блокировки ([рис. 23](#fig-19)).

|  |
| --- |
| Рисунок 23: Сообщения журнала о игнорировании IP-адреса |

### 2.2.11 Повторная попытка входа и проверка статуса SSH

С клиента выполнены повторные попытки входа по SSH с неправильным паролем. Несмотря на ошибки аутентификации, IP-адрес не блокируется.

При проверке статуса jail-модуля sshd (fail2ban-client status sshd) указано: Currently banned: 0, Total banned: 0, список Banned IP list пуст, что подтверждает отсутствие блокировки благодаря параметру ignoreip ([рис. 24](#fig-18)).

|  |
| --- |
| Рисунок 24: Статус sshd после включения ignoreip |

## 2.3 Внесение изменений в настройки внутреннего

### 2.3.1 Подготовка каталога и копирование конфигурации Fail2ban

На виртуальной машине server выполнен переход в каталог /vagrant/provision/server. Создан каталог protect/etc/fail2ban/jail.d, после чего файл customisation.local скопирован из системного каталога /etc/fail2ban/jail.d/ во внутреннюю структуру provision. Это обеспечивает перенос текущей конфигурации Fail2ban в среду автоматической настройки Vagrant ([рис. 25](#fig-20)).

|  |
| --- |
| Рисунок 25: Создание каталога protect и копирование customisation.local |

### 2.3.2 Создание и настройка скрипта protect.sh

В каталоге /vagrant/provision/server создан исполняемый файл protect.sh и открыт для редактирования. В скрипте реализованы следующие действия:

* установка пакета fail2ban;
* копирование конфигурационных файлов из /vagrant/provision/server/protect/etc/ в /etc;
* восстановление контекстов SELinux командой restorecon -vR /etc;
* включение и запуск службы fail2ban.

Скрипт предназначен для автоматической настройки защиты при развертывании виртуальной машины ([рис. 26](#fig-21)).

|  |
| --- |
| Рисунок 26: Содержимое скрипта protect.sh |

### 2.3.3 Добавление provision-конфигурации в Vagrantfile

В файле Vagrantfile в разделе конфигурации виртуальной машины server добавлен блок:

server.vm.provision "server protect",  
 type: "shell",  
 preserve\_order: true,  
 path: "provision/server/protect.sh"

Данная конфигурация обеспечивает выполнение скрипта protect.sh при запуске или пересоздании виртуальной машины server, тем самым автоматизируя применение настроек Fail2ban ([рис. 27](#fig-22)).

|  |
| --- |
| Рисунок 27: Добавление блока provision в Vagrantfile |

# 3. Выводы

В ходе работы выполнена установка и базовая настройка системы предотвращения вторжений Fail2ban на сервере. Реализована защита сервисов SSH, HTTP (Apache) и почтовых служб (Postfix, Dovecot) с заданием времени блокировки и порога ошибок аутентификации.

Экспериментально подтверждена корректность механизма блокировки IP-адреса клиента при превышении значения maxretry, а также возможность снятия блокировки вручную. Дополнительно проверена работа параметра ignoreip, обеспечивающего исключение заданного адреса из процесса блокировки.

Настройки Fail2ban вынесены в систему автоматического развёртывания Vagrant посредством создания скрипта protect.sh и добавления соответствующего блока provision в Vagrantfile. Это обеспечивает воспроизводимость конфигурации и автоматическую активацию механизмов защиты при запуске виртуальной машины.

# 4. Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban - это программное обеспечение, которое предотвращает атаки на сервер, анализируя лог-файлы и блокируя IP-адреса, с которых идут подозрительные или злонамеренные действия. Он работает следующим образом:

* Мониторит указанные лог-файлы на наличие заданных событий (например, неудачных попыток входа).
* Когда число попыток превышает определенный порог, Fail2ban временно блокирует IP-адрес, добавляя правила в файрвол.
* Заблокированный IP-адрес может быть разблокирован автоматически после определенного периода времени

1. Настройки какого файла более приоритетны: jail.conf или jail.local?

Настройки файла jail.local более приоритетны, чем настройки файла jail.conf.

1. Как настроить оповещение администратора при срабатывании Fail2ban?

Чтобы настроить оповещение администратора при срабатывании Fail2ban, необходимо настроить отправку уведомлений по электронной почте или другим способом. Это можно сделать, изменяя настройки в файле jail.local, добавляя адрес электронной почты администратора и настройки SMTPсервера.

1. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе.

Примеры настроек по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе:

* [apache] - секция, относящаяся к веб-серверу Apache.
* enabled = true - включение проверки лог-файлов Apache.
* port = http,https - указание портов для мониторинга.
* filter = apache-auth - указание фильтра для обработки лог-файлов.
* logpath = /var/log/apache\*/\*error.log - путь к лог-файлам Apache.
* maxretry = 5 - максимальное количество попыток до блокировки адреса.
* bantime = 600 - продолжительность блокировки в секундах.

1. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе.

Примеры настроек по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе:

* [postfix] - секция, относящаяся к почтовому серверу Postfix.
* enabled = true - включение проверки лог-файлов Postfix.
* port = smtp,ssmtp - указание портов для мониторинга.
* filter = postfix - указание фильтра для обработки лог-файлов.
* logpath = /var/log/mail.log - путь к лог-файлам Postfix.
* maxretry = 3 - максимальное количество попыток до блокировки адреса.
* bantime = 3600 - продолжительность блокировки в секундах

1. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в настройках Fail2ban?

Fail2ban может выполнять различные действия при обнаружении атакующего IP-адреса, такие как блокировка адреса через файрвол, добавление правил в IP-таблицы, отправка уведомлений администратору и другие. Описание доступных действий можно найти в документации или руководстве Fail2ban.

1. Как получить список действующих правил Fail2ban?

Можно использовать команду: fail2ban-client status.

1. Как получить статистику заблокированных Fail2ban адресов?

Можно использовать команду fail2ban-client status <jail-name>, где <jail-name> - имя конкретного jail, например, “ssh” или “apache”.

1. Как разблокировать IP-адрес?

fail2ban-client set sshd unbanip <ip-адрес клиента>