Лабораторная работа №16

Базовая защита от атак типа «brute force»

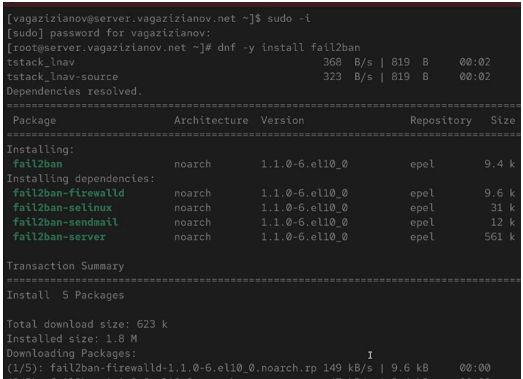
Газизянов Владислав Альбертович

2025-12-19

Содержание I

1. Цели и задачи

Цель: Получить навыки работы с **Fail2ban** для защиты от атак «brute force».
Задачи: - Установить и настроить Fail2ban для мониторинга служб - Проверить работу через тестирование SSH-аутентификации - Автоматизировать настройку через скрипт Vagrant



2. Установка и базовая настройка

Начальная конфигурация: - Установка пакета fail2ban через dnf - Запуск службы и добавление в автозагрузку - Мониторинг журнала событий в реальном времени

```
[vagazizianov@server.vagazizianov.net ~]$ sudo -i
[sudo] password for vagazizianov:
[root@server.vagazizianov.net ~]# tail -f /var/log/fail2ban.log
2025-12-19 11:50:46,695 fail2ban.server         [16558]: INFO    ------------------
--------------------------------
2025-12-19 11:50:46,728 fail2ban.server         [16558]: INFO    Starting Fail2ban
v1.1.0
2025-12-19 11:50:46,747 fail2ban.observer       [16558]: INFO    Observer start...
2025-12-19 11:50:46,823 fail2ban.database       [16558]: INFO    Connected to fail2
ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-12-19 11:50:46,842 fail2ban.database       [16558]: WARNING New database creat
ed. Version '4'
```

Рисунок 2: Запуск мониторинга журнала Fail2ban

3. Создание локальной конфигурации

Настройка параметров защиты: - Создание файла customisation.local - Установка времени блокировки на 1 час - Определение глобальных параметров DEFAULT

Рисунок 3: Создание файла локальной конфигурации Fail2ban

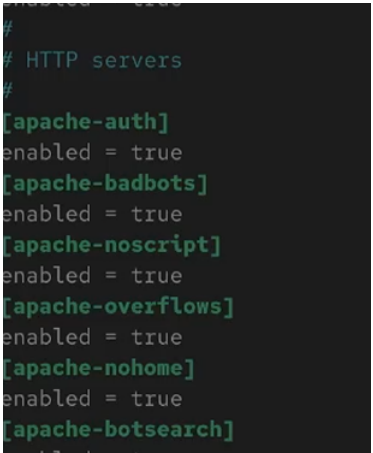
4. Настройка защиты SSH

Защита доступа по SSH: - Включение защиты для портов 22 и 2022 - Активация фильтров sshd и sshd-ddos - Настройка правил для обнаружения атак

Рисунок 4: Настройка защиты SSH в конфигурационном файле

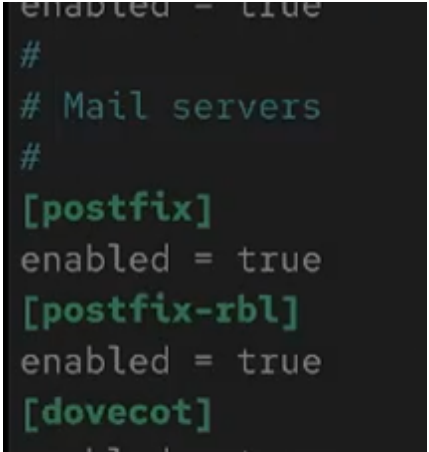
5. Настройка защиты веб-сервера

Защита Apache: - Включение защиты от атак на аутентификацию - Активация фильтров для блокировки ботов - Защита от переполнений и скриптовых атак



6. Настройка защиты почтовых служб

Защита почтовой системы: - Активация защиты Postfix и Dovecot - Настройка фильтров для почтовой аутентификации - Защита от спама и RBL-атак



7. Перезапуск и проверка службы

Применение изменений: - Перезапуск службы Fail2ban - Проверка журнала событий - Подтверждение корректной работы конфигураций

Рисунок 7: Перезапуск службы Fail2ban и проверка журнала

8. Проверка статуса защиты

Мониторинг работы системы: - Проверка общего статуса Fail2ban - Просмотр статуса защиты SSH - Убеждение в активности всех настроенных фильтров

```
[root@server.vagazizianov.net ~]# systemctl restart fail2ban
[root@server.vagazizianov.net ~]# fail2ban-client status
Status
|- Number of jail:      7
`- Jail list:   dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, ssh
d-ddos
[root@server.vagazizianov.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-sessio
n
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.vagazizianov.net ~]# fail2ban-client set sshd maxretry 2
```

Рисунок 8: Проверка статуса Fail2ban и защиты SSH

9. Настройка параметров защиты SSH

Тонкая настройка: - Установка максимального количества попыток (maxretry = 2) - Настройка чувствительности системы защиты - Подготовка к тестированию блокировки

```
[root@server.vagazizianov.net ~]# fail2ban-client set sshd maxretry 2
2
```

Рисунок 9: Настройка параметра maxretry для SSH

10. Тестирование блокировки IP

Проверка работы защиты: - Попытки входа с неверным паролем с клиента - Автоматическая блокировка IP-адреса после 2 попыток - Подтверждение блокировки через статус службы

```
[root@client.vagazizianov.net ~]# ssh vagazizianov@192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:n1ZtBicbxSvGM1uEnnI23Z3BWSXW+txOsSpVlgKVsvU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.1' (ED25519) to the list of known hosts.
vagazizianov@192.168.1.1's password:
Permission denied, please try again.
vagazizianov@192.168.1.1's password:
Permission denied, please try again.
vagazizianov@192.168.1.1's password:
vagazizianov@192.168.1.1: Permission denied (publickey,gssapi-keyex,gssapi-with-mic
,password).
```

Рисунок 10: Тестирование блокировки IP-адреса при неудачных попытках SSH

11. Управление блокировками

Ручное управление: - Разблокировка IP-адреса клиента - Проверка снятия блокировки - Мониторинг изменений в статусе защиты

```
[root@server.vagazizianov.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
0
```

Рисунок 11: Ручная разблокировка IP-адреса клиента

12. Настройка белого списка

Исключение доверенных адресов: - Добавление IP-адреса клиента в ignoreip - Перезапуск службы для применения изменений - Проверка отсутствия блокировки для доверенного адреса

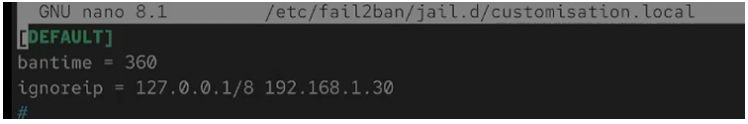


Рисунок 12: Добавление IP-адреса в белый список и проверка

13. Автоматизация развертывания

Подготовка к автоматизации: - Создание структуры каталогов для конфигураций - Копирование файлов настроек в проект Vagrant - Организация файлов для скрипта установки

```
[root@server.vagazizianov.net ~]# cd /vagrant/provision/server
[root@server.vagazizianov.net server]# mkdir -p /vagrant/provision/server/protect/e
tc/fail2ban/jail.d
[root@server.vagazizianov.net server]# cp -R /etc/fail2ban/jail.d/customisation.loc
al /vagrant/provision/server/protect/etc/fail2ban/jail.d/
[root@server.vagazizianov.net server]# cd /vagrant/provision/server
[root@server.vagazizianov.net server]# touch protect.sh
[root@server.vagazizianov.net server]# chmod +x protect.sh
[root@server.vagazizianov.net server]# nano protect.sh
```

Рисунок 13: Подготовка конфигурационных файлов для проекта Vagrant

14. Создание скрипта автоматизации

Разработка provisioning-скрипта: - Создание исполняемого bash-скрипта protect.sh - Включение установки пакетов и копирования конфигураций - Настройка прав доступа и автоматический запуск службы

```
 GNU nano 8.1                                protect.sh
#!/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
```

Рисунок 14: Создание скрипта автоматической настройки protect.sh

15. Интеграция с Vagrant

Настройка автоматического развертывания: - Добавление вызова скрипта в Vagrantfile - Настройка порядка выполнения provisioning-шагов - Обеспечение автоматической защиты при создании виртуальной машины

```
server.vm.provision "server netlog",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/server/netlog.sh"

server.vm.provision "server protect",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/server/protect.sh"

server.vm.provision "server firewall",
                    type: "shell",
                    preserve_order: true,
                    path: "provision/server/firewall.sh"
```

16. Контрольные вопросы

Ключевые вопросы: - **Принцип работы Fail2ban:** Анализ логов ⟶ обнаружение атак ⟶ блокировка через firewall - **Приоритет конфигураций:** jail.local > jail.conf - **Оповещения:** Настройка через параметр action в конфигурации - **Действия при блокировке:** Блокировка IP, отправка уведомлений, выполнение команд - **Управление:** Статус через `fail2ban-client status`, разблокировка через `unbanip`

17. Выводы

Результаты работы: - Успешно установлен и настроен Fail2ban для защиты сервера - Проверена работа системы через тестирование блокировки SSH-доступа - Настроена защита для SSH, HTTP и почтовых служб - Реализована автоматизация установки и настройки через скрипт Vagrant - Приобретены практические навыки защиты от атак типа «brute force»