

Лабораторная работа №16

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

2026-02-13

Содержание I

1 1. Цель работы

2 2. Выполнение лабораторной работы

3 3. Выводы

Раздел 1

1. Цель работы

1.1 Цель работы

- Получение навыков работы с Fail2ban
- Настройка базовой защиты от атак типа brute force

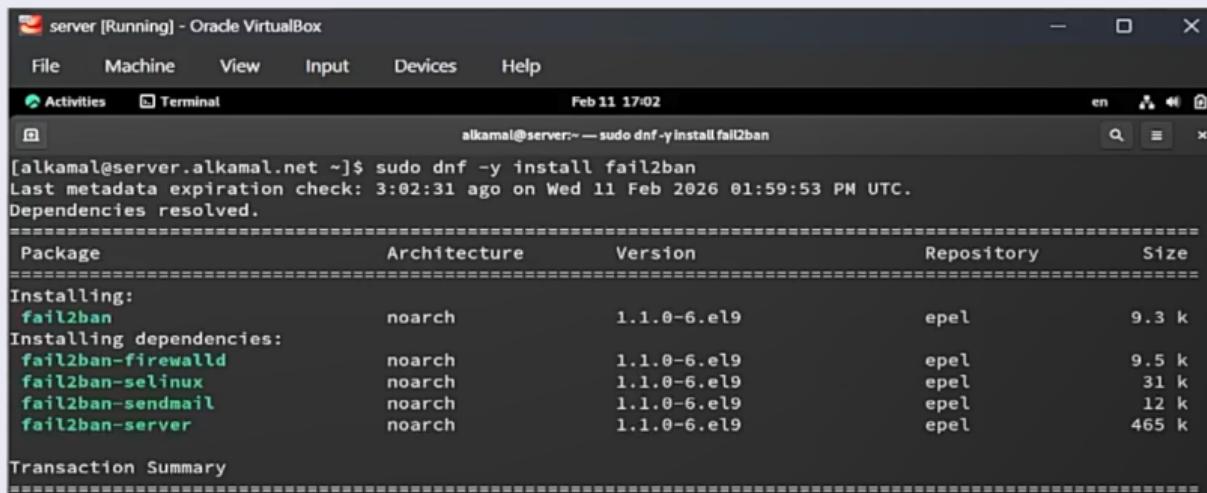
Раздел 2

2. Выполнение лабораторной работы

2.1 Защита с помощью Fail2ban

2.1.1 Установка Fail2ban

- Установлен пакет fail2ban через dnf
- Установлены зависимости: fail2ban-firewalld, fail2ban-selinux, fail2ban-sendmail, fail2ban-server
- Использован репозиторий epel



```
[alkamal@server.alkamal.net ~]$ sudo dnf -y install fail2ban
Last metadata expiration check: 3:02:31 ago on Wed 11 Feb 2026 01:59:53 PM UTC.
Dependencies resolved.
=====
 Package           Architecture   Version      Repository  Size
 =====
 Installing:
  fail2ban          noarch       1.1.0-6.el9    epel        9.3 k
 Installing dependencies:
  fail2ban-firewalld  noarch       1.1.0-6.el9    epel        9.5 k
  fail2ban-selinux   noarch       1.1.0-6.el9    epel        31 k
  fail2ban-sendmail  noarch       1.1.0-6.el9    epel        12 k
  fail2ban-server    noarch       1.1.0-6.el9    epel       465 k
 Transaction Summary
 =====
```

2.1.2 Запуск и добавление службы в автозагрузку

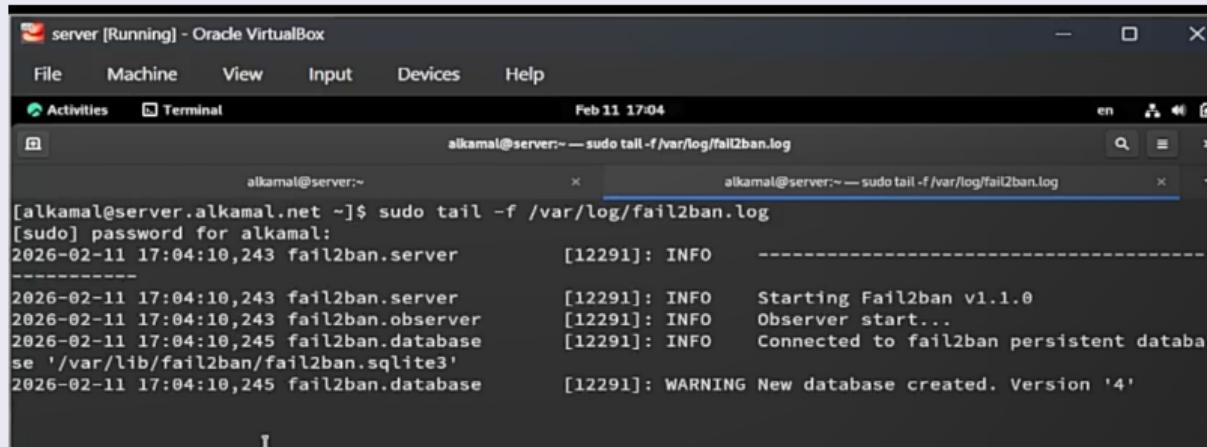
- Выполнен `sudo systemctl start fail2ban`
- Выполнен `sudo systemctl enable fail2ban`
- Создана ссылка в `multi-user.target.wants`

```
[alkamal@server.alkamal.net ~]$ sudo systemctl start fail2ban
[alkamal@server.alkamal.net ~]$ sudo systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.
[alkamal@server.alkamal.net ~]$ █
```

Рисунок 2: Запуск службы fail2ban и включение автозагрузки

2.1.3 Контроль журнала событий Fail2ban

- Выполнен `tail -f /var/log/fail2ban.log`
- Зафиксирован запуск Fail2ban 1.1.0
- Инициализирован observer
- Создана база `fail2ban.sqlite3`



```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 17:04
alkamal@server:~ — sudo tail -f /var/log/fail2ban.log
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:04:10,243 fail2ban.server      [12291]: INFO  -----
2026-02-11 17:04:10,243 fail2ban.observer    [12291]: INFO  Starting Fail2ban v1.1.0
2026-02-11 17:04:10,243 fail2ban.database    [12291]: INFO  Observer start...
2026-02-11 17:04:10,245 fail2ban.database    [12291]: INFO  Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2026-02-11 17:04:10,245 fail2ban.database    [12291]: WARNING New database created. Version '4'
```

Рисунок 3: Просмотр журнала fail2ban.log в реальном времени

2.1.4 Создание файла локальной конфигурации

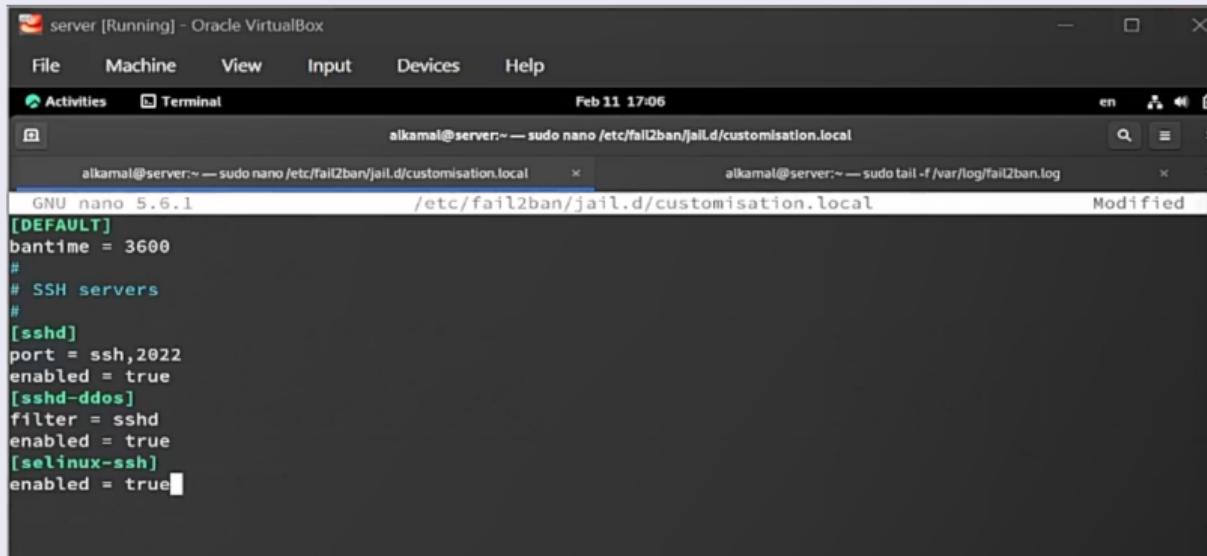
- Создан файл /etc/fail2ban/jail.d/customisation.local
- Выполнено редактирование в nano

```
[alkamal@server.alkamal.net ~]$ sudo touch /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo nano /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo systemctl restart fail2ban
[alkamal@server.alkamal.net ~]$
```

Рисунок 4: Создание и перезапуск службы после настройки

2.1.5 Настройка параметров блокирования и защиты SSH

- В [DEFAULT] установлен `bantime = 3600`
- Активированы [sshd], [sshd-ddos], [selinux-ssh]
- Указан порт ssh, 2022
- Для всех секций `enabled = true`



The screenshot shows a terminal window titled "Activities" with two tabs open: "Terminal" and "fail2ban". The "Terminal" tab shows the command "sudo nano /etc/fail2ban/jail.d/customisation.local". The content of the file is displayed in the terminal window:

```
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```

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

2.1.6 Перезапуск службы Fail2ban

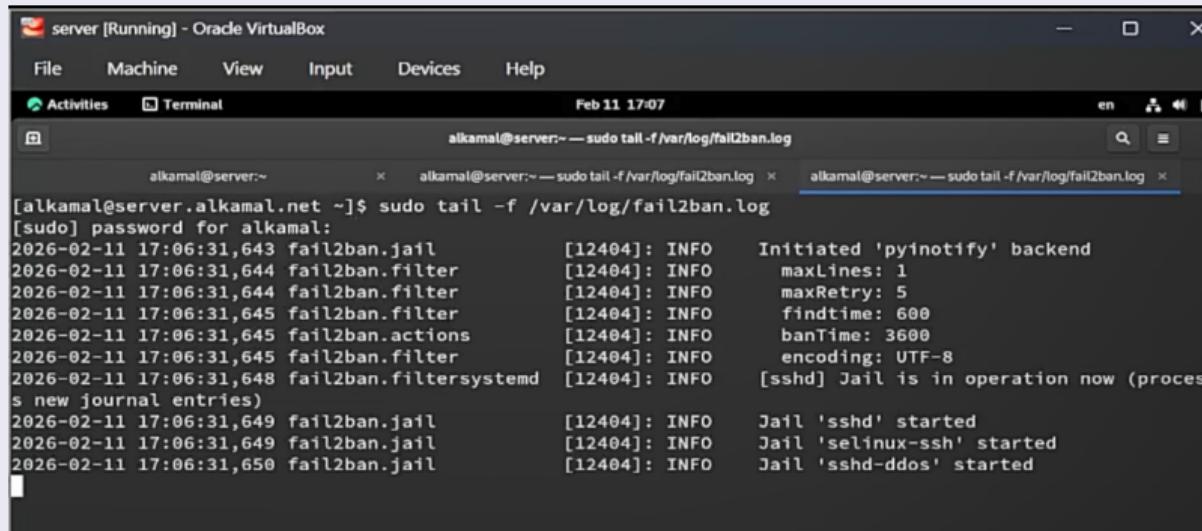
- Выполнен `systemctl restart fail2ban`
- Применена новая конфигурация

```
[alkamal@server.alkamal.net ~]$ sudo touch /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo nano /etc/fail2ban/jail.d/customisation.local
[alkamal@server.alkamal.net ~]$ sudo systemctl restart fail2ban
[alkamal@server.alkamal.net ~]$
```

Рисунок 6: Создание и перезапуск службы после настройки

2.1.7 Просмотр журнала после настройки SSH

- Инициализирован backend pyinotify
- Установлены параметры maxRetry, findtime, banTime = 3600
- Запущены jail-модули sshd, selinux-ssh, sshd-ddos

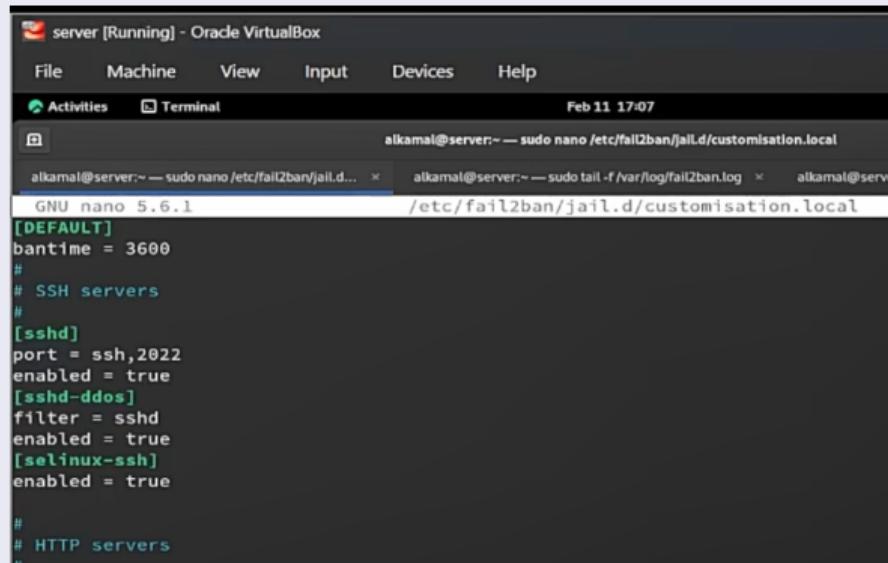


```
[alkamal@server:~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
[2026-02-11 17:06:31,643 fail2ban.jail          [12404]: INFO    Initiated 'pyinotify' backend
[2026-02-11 17:06:31,644 fail2ban.filter       [12404]: INFO    maxLines: 1
[2026-02-11 17:06:31,644 fail2ban.filter       [12404]: INFO    maxRetry: 5
[2026-02-11 17:06:31,645 fail2ban.filter       [12404]: INFO    findtime: 600
[2026-02-11 17:06:31,645 fail2ban.actions     [12404]: INFO    banTime: 3600
[2026-02-11 17:06:31,645 fail2ban.filter       [12404]: INFO    encoding: UTF-8
[2026-02-11 17:06:31,648 fail2ban.filtersystemd [12404]: INFO    [sshd] Jail is in operation now (processes new journal entries)
[2026-02-11 17:06:31,649 fail2ban.jail          [12404]: INFO    Jail 'sshd' started
[2026-02-11 17:06:31,649 fail2ban.jail          [12404]: INFO    Jail 'selinux-ssh' started
[2026-02-11 17:06:31,650 fail2ban.jail          [12404]: INFO    Jail 'sshd-ddos' started
```

Рисунок 7: Журнал запуска jail-модулей SSH в fail2ban

2.1.8 Включение защиты HTTP

- Активированы jail-модули: apache-auth, apache-badbots, apache-noscript, apache-overflows, apache-nohome, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-shellshock
- Для всех enabled = true

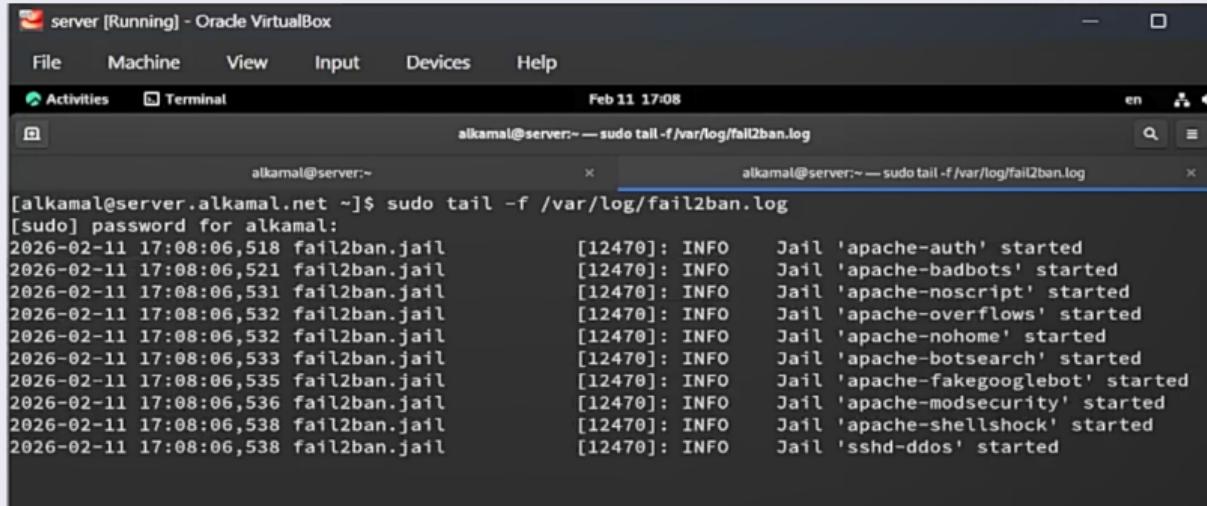


```
GNU nano 5.6.1
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true

#
# HTTP servers
```

2.1.9 Перезапуск после настройки HTTP

- Выполнен `systemctl restart fail2ban`
- Загружены HTTP jail-модули



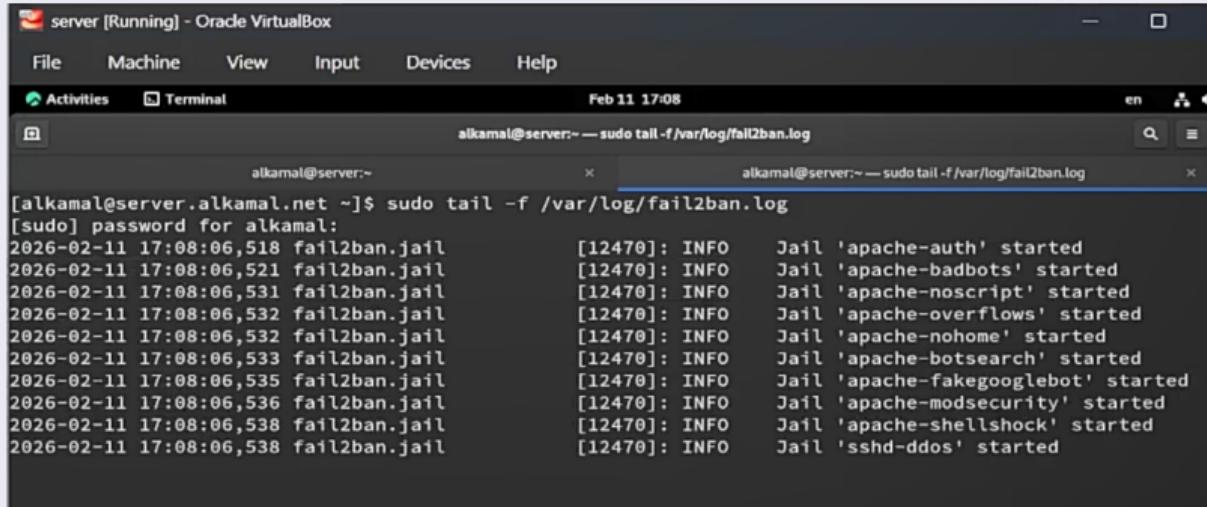
The screenshot shows a terminal window titled "Activities" with two tabs open. The left tab shows the command `[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log`. The right tab shows the output of this command, which lists various jail modules being started at 2026-02-11 17:08:06.518. The output is as follows:

```
[2026-02-11 17:08:06,518 fail2ban.jail      [12470]: INFO    Jail 'apache-auth' started
[2026-02-11 17:08:06,521 fail2ban.jail      [12470]: INFO    Jail 'apache-badbots' started
[2026-02-11 17:08:06,531 fail2ban.jail      [12470]: INFO    Jail 'apache-noscript' started
[2026-02-11 17:08:06,532 fail2ban.jail      [12470]: INFO    Jail 'apache-overflows' started
[2026-02-11 17:08:06,532 fail2ban.jail      [12470]: INFO    Jail 'apache-nohome' started
[2026-02-11 17:08:06,533 fail2ban.jail      [12470]: INFO    Jail 'apache-botsearch' started
[2026-02-11 17:08:06,535 fail2ban.jail      [12470]: INFO    Jail 'apache-fakegooglebot' started
[2026-02-11 17:08:06,536 fail2ban.jail      [12470]: INFO    Jail 'apache-modsecurity' started
[2026-02-11 17:08:06,538 fail2ban.jail      [12470]: INFO    Jail 'apache-shellshock' started
[2026-02-11 17:08:06,538 fail2ban.jail      [12470]: INFO    Jail 'sshd-ddos' started
```

Рисунок 9: Журнал запуска HTTP jail-модулей

2.1.10 Контроль журнала HTTP-защиты

- В журнале зафиксирован запуск всех apache-* jail
- Подтверждена активация sshd-ddos



```
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:08:06,518 fail2ban.jail      [12470]: INFO    Jail 'apache-auth' started
2026-02-11 17:08:06,521 fail2ban.jail      [12470]: INFO    Jail 'apache-badbots' started
2026-02-11 17:08:06,531 fail2ban.jail      [12470]: INFO    Jail 'apache-noscript' started
2026-02-11 17:08:06,532 fail2ban.jail      [12470]: INFO    Jail 'apache-overflows' started
2026-02-11 17:08:06,532 fail2ban.jail      [12470]: INFO    Jail 'apache-nohome' started
2026-02-11 17:08:06,533 fail2ban.jail      [12470]: INFO    Jail 'apache-botsearch' started
2026-02-11 17:08:06,535 fail2ban.jail      [12470]: INFO    Jail 'apache-fakegooglebot' started
2026-02-11 17:08:06,536 fail2ban.jail      [12470]: INFO    Jail 'apache-modsecurity' started
2026-02-11 17:08:06,538 fail2ban.jail      [12470]: INFO    Jail 'apache-shellshock' started
2026-02-11 17:08:06,538 fail2ban.jail      [12470]: INFO    Jail 'sshd-ddos' started
```

Рисунок 10: Подтверждение запуска HTTP jail-модулей в журнале

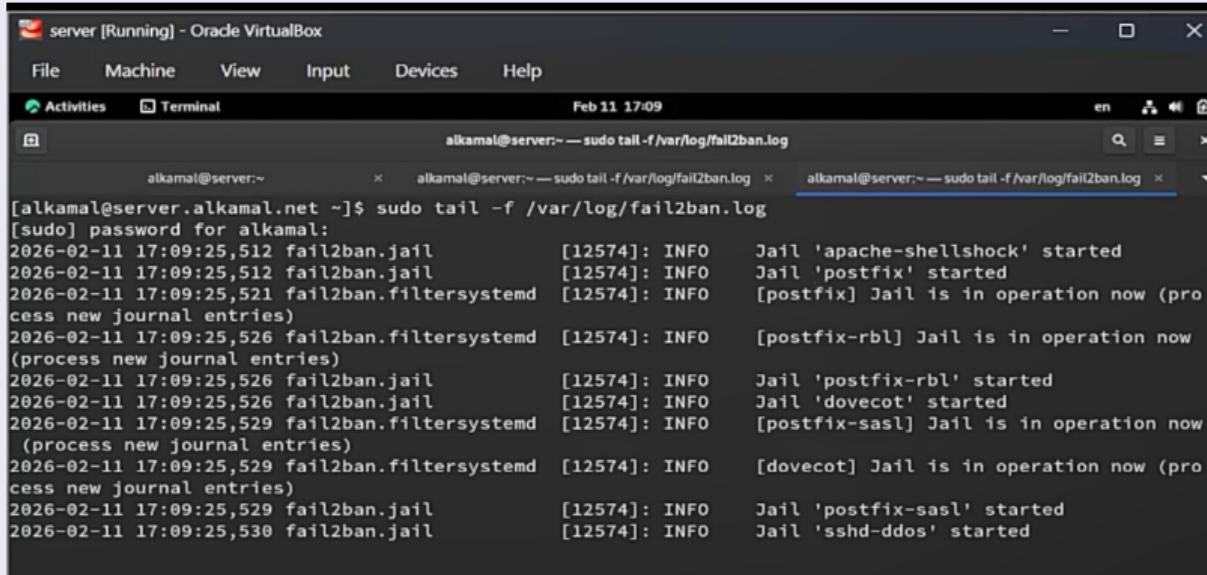
2.1.11 Включение защиты почтовых сервисов

- Активированы jail-модули: postfix, postfix-rbl, dovecot, postfix-sasl
- Установлено enabled = true

```
#  
# Mail servers  
  
[postfix]  
enabled = true  
[postfix-rbl]  
enabled = true  
[dovecot]  
enabled = true  
[postfix-sasl]  
enabled = true
```

2.1.12 Перезапуск после настройки почтовых служб

- Выполнен перезапуск fail2ban
- Загружены почтовые jail-модули

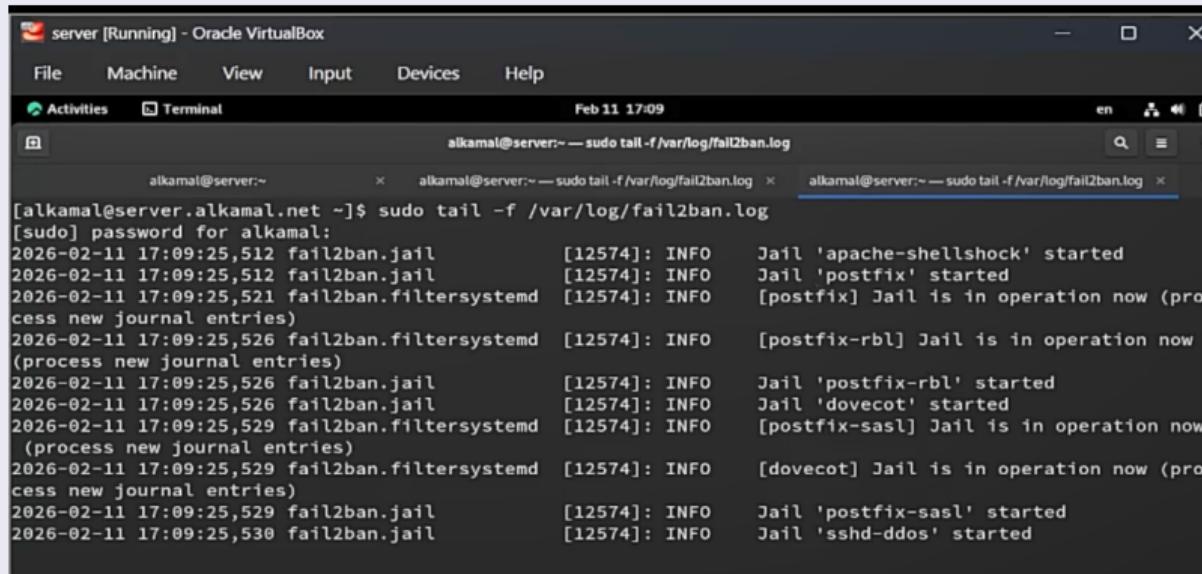


```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 17:09
alkamal@server:~ — sudo tail -f /var/log/fail2ban.log
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:09:25,512 fail2ban.jail [12574]: INFO Jail 'apache-shellshock' started
2026-02-11 17:09:25,512 fail2ban.jail [12574]: INFO Jail 'postfix' started
2026-02-11 17:09:25,521 fail2ban.filtersystemd [12574]: INFO [postfix] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,526 fail2ban.filtersystemd [12574]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,526 fail2ban.jail [12574]: INFO Jail 'postfix-rbl' started
2026-02-11 17:09:25,526 fail2ban.jail [12574]: INFO Jail 'dovecot' started
2026-02-11 17:09:25,529 fail2ban.filtersystemd [12574]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,529 fail2ban.filtersystemd [12574]: INFO [dovecot] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,529 fail2ban.jail [12574]: INFO Jail 'postfix-sasl' started
2026-02-11 17:09:25,530 fail2ban.jail [12574]: INFO Jail 'sshd-ddos' started
```

Рисунок 12: Журнал запуска jail-модулей почтовых сервисов

2.1.13 Контроль журнала почтовой защиты

- Зафиксировано Jail is in operation now
- Подтверждена активация postfix, dovecot, postfix-sasl



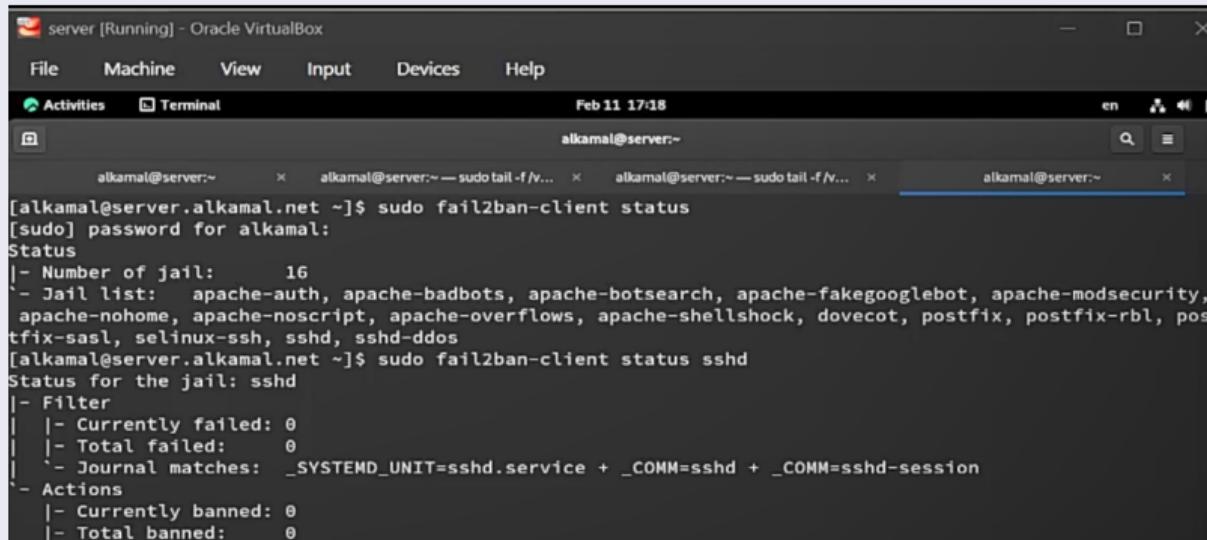
```
server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Feb 11 17:09
alkamal@server:~ — sudo tail -f /var/log/fail2ban.log
alkamal@server:~ — sudo tail -f /var/log/fail2ban.log × alkamal@server:~ — sudo tail -f /var/log/fail2ban.log ×
[alkamal@server.alkamal.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for alkamal:
2026-02-11 17:09:25,512 fail2ban.jail [12574]: INFO Jail 'apache-shellshock' started
2026-02-11 17:09:25,512 fail2ban.jail [12574]: INFO Jail 'postfix' started
2026-02-11 17:09:25,521 fail2ban.filtersystemd [12574]: INFO [postfix] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,526 fail2ban.filtersystemd [12574]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,526 fail2ban.jail [12574]: INFO Jail 'postfix-rbl' started
2026-02-11 17:09:25,526 fail2ban.jail [12574]: INFO Jail 'dovecot' started
2026-02-11 17:09:25,529 fail2ban.filtersystemd [12574]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,529 fail2ban.filtersystemd [12574]: INFO [dovecot] Jail is in operation now (process new journal entries)
2026-02-11 17:09:25,529 fail2ban.jail [12574]: INFO Jail 'postfix-sasl' started
2026-02-11 17:09:25,530 fail2ban.jail [12574]: INFO Jail 'sshd-ddos' started
```

Рисунок 13: Подтверждение работы jail-модулей почтовых сервисов

2.2 Проверка работы Fail2ban

2.2.1 Просмотр общего статуса

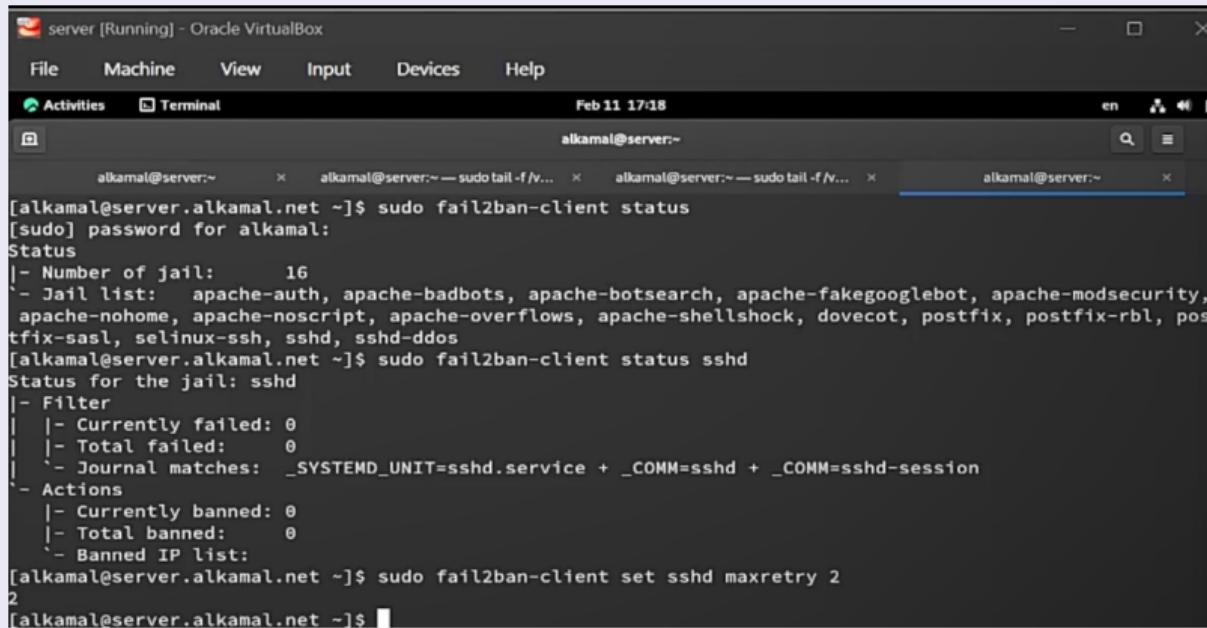
- Выполнен fail2ban-client status
- Активировано 16 jail-модулей
- Отображены apache-*, sshd, dovecot, postfix



```
[alkamal@server:~]$ sudo fail2ban-client status
[sudo] password for alkamal:
Status
|- Number of jail:      16
`- Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity,
    apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, pos
    tfix-sasl, selinux-ssh, sshd, sshd-ddos
[alkamal@server.alkamal.net ~]$ sudo 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
```

2.2.2 Просмотр статуса SSH

- Выполнен fail2ban-client status sshd
- Currently banned: 0
- Total banned: 0



```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client status
[sudo] password for alkamal:
Status
|- Number of jail:      16
`- Jail list: apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity,
  apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, pos
  tfix-sasl, selinux-ssh, sshd, sshd-ddos
[alkamal@server.alkamal.net ~]$ sudo 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:
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client set sshd maxretry 2
2
[alkamal@server.alkamal.net ~]$
```

2.2.3 Установка maxretry

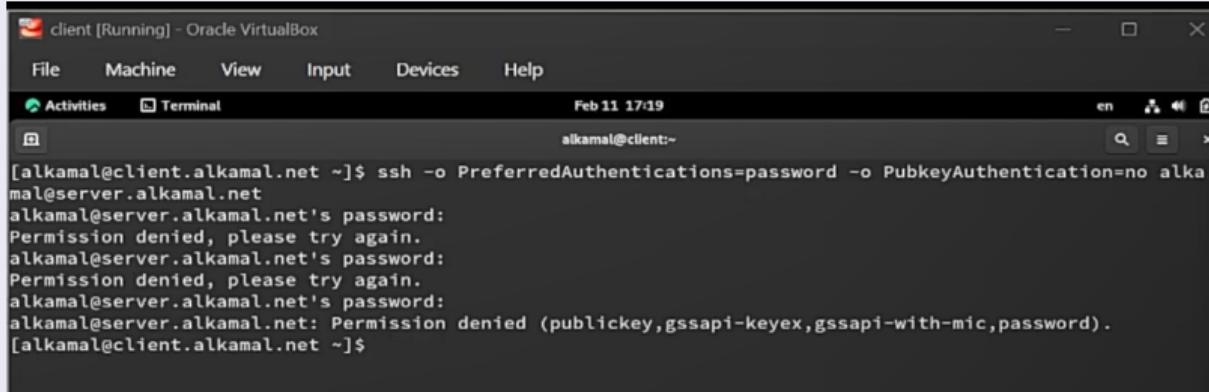
- Выполнено fail2ban-client set sshd maxretry 2
- После 2 ошибок IP должен блокироваться

```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client status
[sudo] password for alkamal:
Status
|- Number of jail:      16
`- Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity,
    apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, pos
    tfix-sasl, selinux-ssh, sshd, sshd-ddos
[alkamal@server.alkamal.net ~]$ sudo 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:
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client set sshd maxretry 2
2
[alkamal@server.alkamal.net ~]$
```

Рисунок 16: Установка параметра maxretry для sshd

2.2.4 Попытка входа с неверным паролем

- С клиента выполнены неудачные попытки SSH-входа
- Зафиксированы ошибки Permission denied



The screenshot shows a terminal window titled "client [Running] - Oracle VirtualBox". The terminal is running on a system with the user "alkamal" and the host "client.alkamal.net". The user has entered the command:

```
[alkamal@client.alkamal.net ~]$ ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no alkamal@server.alkamal.net
```

and is prompted for a password. The terminal displays the following output:

```
alkamal@server.alkamal.net's password:  
Permission denied, please try again.  
alkamal@server.alkamal.net's password:  
Permission denied, please try again.  
alkamal@server.alkamal.net's password:  
alkamal@server.alkamal.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).  
[alkamal@client.alkamal.net ~]$
```

Рисунок 17: Попытки входа по SSH с неверным паролем

2.2.5 Проверка блокировки IP

- Выполнен fail2ban-client status sshd
- Currently banned: 1
- IP 192.168.1.30 в списке блокировки

```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client status sshd
[sudo] password for alkamal:
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
[alkamal@server.alkamal.net ~]$ █
```

Рисунок 18: Блокировка IP-адреса клиента в sshd

2.2.6 Разблокировка IP

- Выполнено fail2ban-client set sshd unbanip 192.168.1.30

```
[alkamal@server.alkamal.net ~]$ sudo fail2ban-client set sshd unbanip 192.168.1.30
1
[alkamal@server.alkamal.net ~]$
```

Рисунок 19: Команда разблокировки IP-адреса клиента

2.2.7 Проверка снятия блокировки

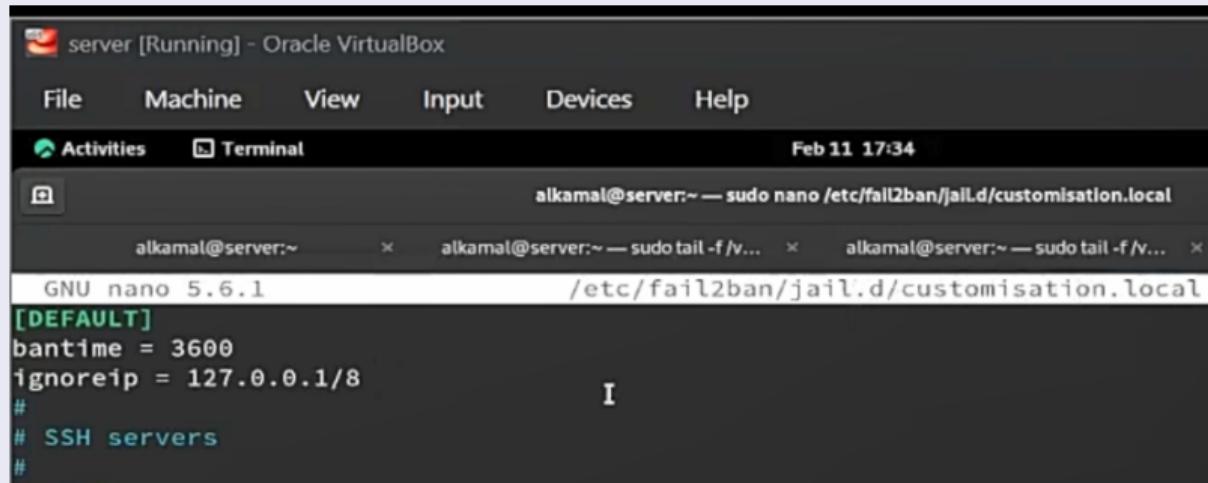
- Повторный `status sshd`
- Currently banned: 0
- Список пуст

```
[alkamal@server.alkamal.net ~]$ sudo 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:
[alkamal@server.alkamal.net ~]$
```

Рисунок 20: Статус sshd после снятия блокировки

2.2.8 Добавление ignoreip

- В [DEFAULT] добавлен ignoreip = 127.0.0.1/8 192.168.1.30
- IP клиента исключён из блокировки



The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The window has tabs for "Activities" and "Terminal". The terminal shows the command "sudo nano /etc/fail2ban/jail.d/customisation.local". The file content is as follows:

```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8
#
# SSH servers
#
```

Рисунок 21: Добавление параметра ignoreip в customisation.local

2.2.9 Перезапуск службы

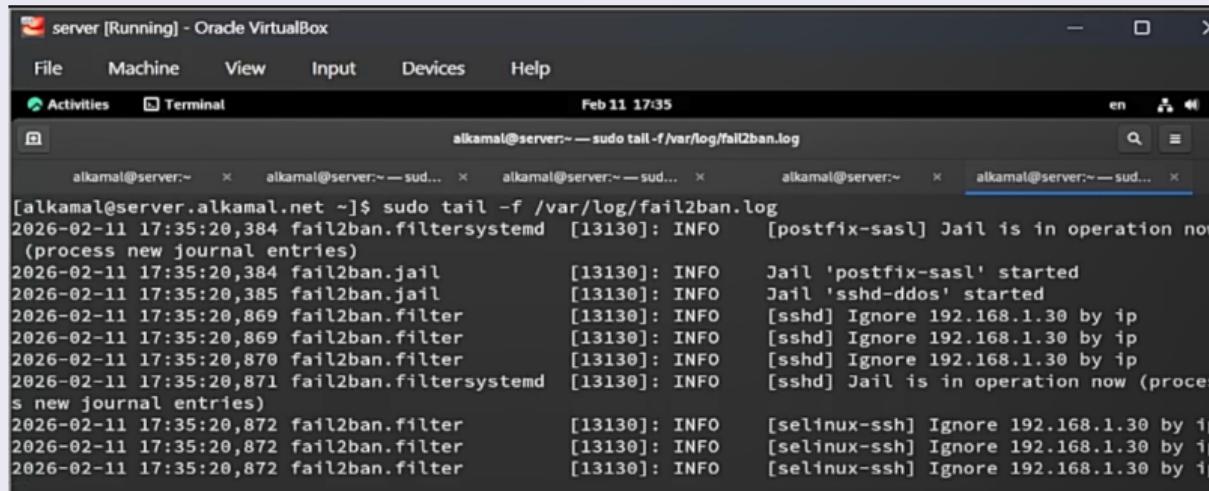
- Выполнен `systemctl restart fail2ban`
- Применена новая конфигурация

```
[alkamal@client.alkamal.net ~]$ ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no alkamal@server.alkamal.net
alkamal@server.alkamal.net's password:
Permission denied, please try again.
alkamal@server.alkamal.net's password:
Permission denied, please try again.
alkamal@server.alkamal.net's password:
alkamal@server.alkamal.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[alkamal@client.alkamal.net ~]$
```

Рисунок 22: Попытка входа с клиента после изменения конфигурации

2.2.10 Просмотр журнала ignoreip

- В журнале отображено Ignore 192.168.1.30 by ip
- IP корректно исключён



The screenshot shows a terminal window titled "Activities" in a "server [Running] - Oracle VM VirtualBox" interface. The terminal window has tabs for "Activities" and "Terminal". The terminal content is a log from the "/var/log/fail2ban.log" file, dated February 11 at 17:35. The log entries show the fail2ban system processing journal entries and ignoring the IP address 192.168.1.30 for various services like postfix-sasl, sshd, and selinux-ssh.

```
alkamal@server:~ — sudo tail -f /var/log/fail2ban.log
[2026-02-11 17:35:20,384] fail2ban.filtersystemd [13130]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
[2026-02-11 17:35:20,384] fail2ban.jail [13130]: INFO Jail 'postfix-sasl' started
[2026-02-11 17:35:20,385] fail2ban.jail [13130]: INFO Jail 'sshd-ddos' started
[2026-02-11 17:35:20,869] fail2ban.filter [13130]: INFO [sshd] Ignore 192.168.1.30 by ip
[2026-02-11 17:35:20,869] fail2ban.filter [13130]: INFO [sshd] Ignore 192.168.1.30 by ip
[2026-02-11 17:35:20,870] fail2ban.filter [13130]: INFO [sshd] Ignore 192.168.1.30 by ip
[2026-02-11 17:35:20,871] fail2ban.filtersystemd [13130]: INFO [sshd] Jail is in operation now (process new journal entries)
[2026-02-11 17:35:20,872] fail2ban.filter [13130]: INFO [selinux-ssh] Ignore 192.168.1.30 by ip
[2026-02-11 17:35:20,872] fail2ban.filter [13130]: INFO [selinux-ssh] Ignore 192.168.1.30 by ip
[2026-02-11 17:35:20,872] fail2ban.filter [13130]: INFO [selinux-ssh] Ignore 192.168.1.30 by ip
```

Рисунок 23: Сообщения журнала о игнорировании IP-адреса

2.2.11 Повторная проверка SSH

- Повторные ошибки входа не приводят к блокировке
- Currently banned: 0
- Список IP пуст

```
[alkamal@server.alkamal.net ~]$ sudo 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:
[alkamal@server.alkamal.net ~]$
```

Рисунок 24: Статус sshd после включения ignoreip

2.3 Внесение изменений в настройки внутреннего

2.3.1 Подготовка конфигурации

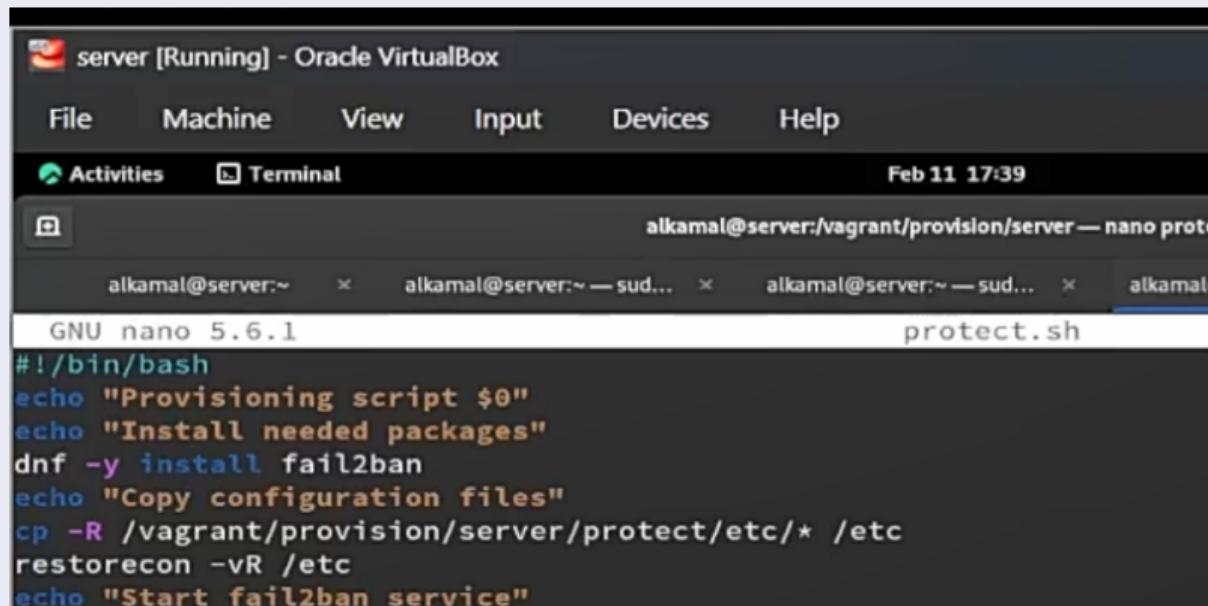
- Создан каталог `protect/etc/fail2ban/jail.d`
- Скопирован `customisation.local`

```
[alkamal@server.alkamal.net ~]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[alkamal@server.alkamal.net server]$ sudo cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/etc/fail2ban/jail.d/
[alkamal@server.alkamal.net server]$ cd /vagrant/provision/server
[alkamal@server.alkamal.net server]$ touch protect.sh
[alkamal@server.alkamal.net server]$ chmod +x protect.sh
[alkamal@server.alkamal.net server]$ nano protect.sh
```

Рисунок 25: Создание каталога `protect` и копирование `customisation.local`

2.3.2 Создание скрипта protect.sh

- Установка fail2ban
- Копирование конфигурации в /etc
- Выполнен restorecon -vR /etc
- Включена и запущена служба



The screenshot shows a Linux desktop environment within Oracle VirtualBox. The title bar says "server [Running] - Oracle VirtualBox". The menu bar includes File, Machine, View, Input, Devices, and Help. Below the menu is a dock with Activities and Terminal. The terminal window title is "Terminal" and the date is "Feb 11 17:39". The user is at the prompt "alkamal@server:~/vagrant/provision/server — nano protect.sh". The terminal content is a bash script:

```
GNU nano 5.6.1
#!/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"
```

2.3.3 Добавление provisioning в Vagrantfile

- Добавлен блок `server.vm.provision`
- Указан путь `provision/server/protect.sh`
- Использован `preserve_order: true`

```
C: > work > alkamal > vagrant > Vagrantfile
      .
      .
78   server.vm.provision "server protect",
79     type: "shell",
80     preserve_order: true,
81     path: "provision/server/protect.sh"
```

Рисунок 27: Добавление блока provision в Vagrantfile

Раздел 3

3. Выводы

3.1 Выводы

- Установлен и настроен Fail2ban
- Реализована защита SSH, HTTP и почтовых сервисов
- Проверена блокировка IP при превышении maxretry
- Выполнена ручная разблокировка
- Настроен параметр ignoreip
- Подтверждена корректная работа jail-модулей
- Настройка автоматизирована через provisioning
- Обеспечена воспроизводимая базовая защита от brute force