

Лабораторная работа №16 (Базовая защита от атак типа «brute force»)

Шубина София Антоновна

11 ноября 2025

Российский университет дружбы народов

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

1. Установите и настройте сервер Samba.
2. Настройте на клиенте доступ к разделяемым ресурсам.
3. Напишите скрипты для Vagrant, фиксирующие действия по установке и настройке сервера Samba для доступа к разделяемым ресурсам во внутреннем окружении виртуальных машин server и client.
Соответствующим образом необходимо внести изменения в Vagrantfile.

Выполнение лабораторной работы

Защита с помощью Fail2ban

На сервере установим fail2ban:

```
[root@server.sashubina.net ~]# dnf -y install fail2ban
Last metadata expiration check: 3:02:58 ago on Mon 10 Nov 2025 03:26:23 PM UTC.
Dependencies resolved.
=====
Package                Architecture    Version          Repository        Size
=====
Installing:
fail2ban                noarch          1.1.0-6.el10_0  epel              9.4 k
Installing dependencies:
fail2ban-firewalld      noarch          1.1.0-6.el10_0  epel              9.6 k
fail2ban-selinux        noarch          1.1.0-6.el10_0  epel              31 k
fail2ban-sendmail       noarch          1.1.0-6.el10_0  epel              12 k
fail2ban-server         noarch          1.1.0-6.el10_0  epel              561 k
=====
Transaction Summary
=====
Install 5 Packages

Total download size: 623 k
Installed size: 1.8 M
Downloading Packages:
(1/5): fail2ban-1.1.0-6.el10_0.noarch.rpm                224 kB/s | 9.4 kB    00:00
(2/5): fail2ban-firewalld-1.1.0-6.el10_0.noarch.rpm      200 kB/s | 9.6 kB    00:00
(3/5): fail2ban-selinux-1.1.0-6.el10_0.noarch.rpm        496 kB/s | 31 kB     00:00
(4/5): fail2ban-sendmail-1.1.0-6.el10_0.noarch.rpm       324 kB/s | 12 kB     00:00
(5/5): fail2ban-server-1.1.0-6.el10_0.noarch.rpm         4.7 MB/s | 561 kB    00:00
-----
Total                                                    666 kB/s | 623 kB    00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : 1/1
  Running scriptlet: fail2ban-selinux-1.1.0-6.el10_0.noarch 1/5
  Installing     : fail2ban-selinux-1.1.0-6.el10_0.noarch 1/5
```

Рис. 1: загрузка

Запустим сервер fail2ban:

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

Рис. 2: запуск

В дополнительном терминале запустим просмотр журнала событий fail2ban:

```
[sashubina@server.sashubina.net ~]$ sudo -i
[sudo] password for sashubina:
[root@server.sashubina.net ~]# tail -f /var/log/fail2ban.log
2025-11-10 18:30:02,590 fail2ban.server [6821]: INFO -----
2025-11-10 18:30:02,591 fail2ban.server [6821]: INFO Starting Fail2ban v1.1.0
2025-11-10 18:30:02,591 fail2ban.observer [6821]: INFO Observer start...
2025-11-10 18:30:02,598 fail2ban.database [6821]: INFO Connected to fail2ban persistent database '/var/lib/fail
2ban/fail2ban.sqlite3'
2025-11-10 18:30:02,600 fail2ban.database [6821]: WARNING New database created. Version '4'
```

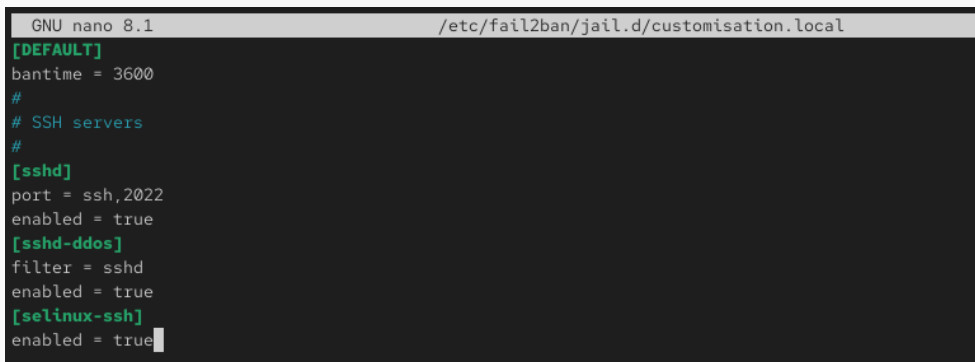
Рис. 3: Запуск просмотра журнала событий fail2ban

Создадим файл с локальной конфигурацией fail2ban:

```
[root@server.sashubina.net ~]# touch /etc/fail2ban/jail.d/customisation.local  
[root@server.sashubina.net ~]#
```

Рис. 4: создание файла

И в этом файле `etc/fail2ban/jail.d/customisation.local` зададим время блокирования на 1 час (время задаётся в секундах) и включим защиту SSH:



```
GNU nano 8.1 /etc/fail2ban/jail.d/customisation.local
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```

Рис. 5: Добавление времени блокировки и включение защиты SSH
`customisation.local`

Перезапустим сервер fail2ban:

```
[root@server.sashubina.net ~]# systemctl restart fail2ban  
[root@server.sashubina.net ~]#
```

Рис. 6: запуск сервера

И посмотрим журнал событий:

```
[root@server.nashidm.net ~]# tail -f /var/log/fail2ban.log
2025-11-10 18:30:02.590 fail2ban.server [6021]: INFO .....
2025-11-10 18:30:02.591 fail2ban.server [6021]: INFO Starting Fail2ban v1.3.0
2025-11-10 18:30:02.591 fail2ban.observer [6021]: INFO Observer starts...
2025-11-10 18:30:02.598 fail2ban.database [6021]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-11-10 18:30:02.600 fail2ban.database [6021]: WARNING New database created. Version '4'
2025-11-10 18:32:16.222 fail2ban.server [6021]: INFO Shutdown in progress...
2025-11-10 18:32:16.262 fail2ban.observer [6021]: INFO Observer stop... try to end queue 5 seconds
2025-11-10 18:32:16.344 fail2ban.observer [6021]: INFO Observer stopped, 8 events remaining.
2025-11-10 18:32:16.387 fail2ban.server [6021]: INFO Stopping all jails
2025-11-10 18:32:16.391 fail2ban.database [6021]: INFO Connection to database closed.
2025-11-10 18:32:16.392 fail2ban.server [6021]: INFO Exiting Fail2ban
2025-11-10 18:32:16.561 fail2ban.server [7143]: INFO .....
2025-11-10 18:32:16.561 fail2ban.server [7143]: INFO Starting Fail2ban v1.3.0
2025-11-10 18:32:16.562 fail2ban.observer [7143]: INFO Observer starts...
2025-11-10 18:32:16.578 fail2ban.database [7143]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-11-10 18:32:16.571 fail2ban.jail [7143]: INFO Creating new jail 'sshd'
2025-11-10 18:32:16.584 fail2ban.jail [7143]: INFO Jail 'sshd' uses systemd {}
2025-11-10 18:32:16.596 fail2ban.jail [7143]: INFO Initiated 'systemd' backend
2025-11-10 18:32:16.589 fail2ban.filter [7143]: INFO maxlines: 1
2025-11-10 18:32:16.599 fail2ban.filter [7143]: INFO [sshd] Added journal match for: '.SYSTEMD_UNIT=sshd.service + .COMM=sshd + .COMM=sshd-session'
2025-11-10 18:32:16.599 fail2ban.filter [7143]: INFO maxRetry: 5
2025-11-10 18:32:16.599 fail2ban.filter [7143]: INFO findtime: 600
2025-11-10 18:32:16.600 fail2ban.action [7143]: INFO banTime: 3600
2025-11-10 18:32:16.600 fail2ban.filter [7143]: INFO encoding: UTF-8
2025-11-10 18:32:16.600 fail2ban.jail [7143]: INFO Creating new jail 'uclinux-ssh'
2025-11-10 18:32:16.612 fail2ban.jail [7143]: INFO Jail 'uclinux-ssh' uses pyinotify {}
2025-11-10 18:32:16.614 fail2ban.jail [7143]: INFO Initiated 'pyinotify' backend
2025-11-10 18:32:16.616 fail2ban.datadector [7143]: INFO date pattern: '%Y-%m-%d %H:%M:%S'
2025-11-10 18:32:16.616 fail2ban.filter [7143]: INFO maxRetry: 5
2025-11-10 18:32:16.616 fail2ban.filter [7143]: INFO findtime: 600
2025-11-10 18:32:16.616 fail2ban.action [7143]: INFO banTime: 3600
2025-11-10 18:32:16.616 fail2ban.filter [7143]: INFO encoding: UTF-8
2025-11-10 18:32:16.618 fail2ban.filter [7143]: INFO Added logfiles: '/var/log/auth/auth.log' (pos = 0, hash = d95fc44779943838f7a5807bb4c1c9d8d1dc74)
2025-11-10 18:32:16.618 fail2ban.jail [7143]: INFO Creating new jail 'sshd-ddos'
2025-11-10 18:32:16.618 fail2ban.jail [7143]: INFO Jail 'sshd-ddos' uses pyinotify {}
2025-11-10 18:32:16.620 fail2ban.jail [7143]: INFO Initiated 'pyinotify' backend
2025-11-10 18:32:16.621 fail2ban.filter [7143]: INFO maxlines: 1
2025-11-10 18:32:16.622 fail2ban.filter [7143]: INFO maxRetry: 5
2025-11-10 18:32:16.622 fail2ban.filter [7143]: INFO findtime: 600
2025-11-10 18:32:16.622 fail2ban.action [7143]: INFO banTime: 3600
2025-11-10 18:32:16.622 fail2ban.filter [7143]: INFO encoding: UTF-8
2025-11-10 18:32:16.623 fail2ban.jail [7143]: INFO Jail 'sshd' started
2025-11-10 18:32:16.624 fail2ban.jail [7143]: INFO Jail 'uclinux-ssh' started
2025-11-10 18:32:16.625 fail2ban.jail [7143]: INFO Jail 'sshd-ddos' started
2025-11-10 18:32:16.627 fail2ban.filter [7143]: INFO [sshd] Jail is in operation now (process new journal entries)
```

Рис. 7: Просмотр журнала событий fail2ban

В файле `/etc/fail2ban/jail.d/customisation.local` включим защиту HTTP:



```
GNU nano 8.1 /etc/fail2ban/jail.d/customisation.local M
# HTTP servers
#
[apache-auth]
enabled = true
[apache-badbots]
enabled = true
[apache-noscript]
enabled = true
[apache-overflows]
enabled = true
[apache-nohome]
enabled = true
[apache-botsearch]
enabled = true
[apache-fakegooglebot]
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true
```

Рис. 8: Включение защиты HTTP в файле `customisation.local`

Перезапустим сервер fail2ban:

```
[root@server.sashubina.net ~]# systemctl restart fail2ban
```

Рис. 9: запуск сервера

И посмотрим журнал событий:

```
[root@server.sashubina.net ~]# tail -f /var/log/fail2ban.log
2025-11-10 18:35:18,637 fail2ban.jail [7277]: INFO Jail 'apache-auth' started
2025-11-10 18:35:18,638 fail2ban.jail [7277]: INFO Jail 'apache-badbots' started
2025-11-10 18:35:18,639 fail2ban.jail [7277]: INFO Jail 'apache-noscript' started
2025-11-10 18:35:18,639 fail2ban.jail [7277]: INFO Jail 'apache-overflows' started
2025-11-10 18:35:18,640 fail2ban.jail [7277]: INFO Jail 'apache-nohome' started
2025-11-10 18:35:18,642 fail2ban.jail [7277]: INFO Jail 'apache-botsearch' started
2025-11-10 18:35:18,644 fail2ban.jail [7277]: INFO Jail 'apache-fakegooglebot' started
2025-11-10 18:35:18,644 fail2ban.jail [7277]: INFO Jail 'apache-modsecurity' started
2025-11-10 18:35:18,645 fail2ban.jail [7277]: INFO Jail 'apache-shellshock' started
2025-11-10 18:35:18,646 fail2ban.jail [7277]: INFO Jail 'sshd-ddos' started
```

Рис. 10: Просмотр журнала событий fail2ban

В файле `/etc/fail2ban/jail.d/customisation.local` включим защиту почты:

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

Рис. 11: Включение защиты почты в файле `customisation.local`

посмотрим журнал событий:

```
[root@server.sashubina.net ~]# tail -f /var/log/fail2ban.log
2025-11-10 18:38:40,415 fail2ban.jail [7457]: INFO Jail 'apache-shellshock' started
2025-11-10 18:38:40,416 fail2ban.jail [7457]: INFO Jail 'postfix' started
2025-11-10 18:38:40,417 fail2ban.jail [7457]: INFO Jail 'postfix-rbl' started
2025-11-10 18:38:40,417 fail2ban.jail [7457]: INFO Jail 'dovecot' started
2025-11-10 18:38:40,419 fail2ban.filtersystemd [7457]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2025-11-10 18:38:40,419 fail2ban.jail [7457]: INFO Jail 'postfix-sasl' started
2025-11-10 18:38:40,420 fail2ban.filtersystemd [7457]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2025-11-10 18:38:40,420 fail2ban.jail [7457]: INFO Jail 'sshd-ddos' started
2025-11-10 18:38:40,421 fail2ban.filtersystemd [7457]: INFO [postfix] Jail is in operation now (process new journal entries)
2025-11-10 18:38:40,422 fail2ban.filtersystemd [7457]: INFO [dovecot] Jail is in operation now (process new journal entries)
```

Рис. 12: Просмотр журнала событий fail2ban

Проверка работы Fail2ban

На сервере посмотрим статус fail2ban и статус защиты SSH в fail2ban

```
[root@server.sashubina.net ~]# fail2ban-client status
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, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.sashubina.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.sashubina.net ~]#
```

Рис. 13: Просмотр статуса fail2ban

а затем установим максимальное количество ошибок для SSH, равное 2:

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

Рис. 14: установка количества ошибок

С клиента попытайтесь зайти по SSH на сервер с неправильным паролем:

```
[sashubina@client.sashubina.net ~]$ ssh sashubina@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:LJpSqM044iVZ+0Xnopuu/dN//5izIhYfJcVSZXbg00k.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [server.sashubina.net]:2022
  ~/.ssh/known_hosts:2: server.sashubina.net
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.
sashubina@192.168.1.1's password:
Permission denied, please try again.
sashubina@192.168.1.1's password:
Permission denied, please try again.
sashubina@192.168.1.1's password:
sashubina@192.168.1.1: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[sashubina@client.sashubina.net ~]$ █
```

Рис. 15: Попытки соединения по SSH с сервером с неправильным паролем

На сервере посмотрите статус защиты SSH, убедившись, что произошла блокировка адреса клиента:

```
[root@server.sashubina.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.sashubina.net ~]#
```

Рис. 16: Проверка блокировки клиента на сервере

Разблокируем IP-адрес клиента и вновь посмотрим статус защиты SSH, убедившись, что блокировка с клиента снята:

```
[root@server.sashubina.net ~]# fail2ban-client set sshd unbanip 192.168.1.30  
1  
[root@server.sashubina.net ~]#
```

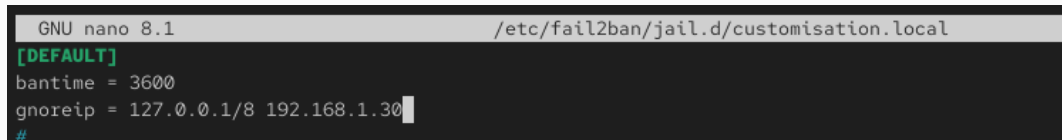
Рис. 17: Снятие блокировки с клиента

Вновь посмотрим статус защиты SSH:

```
[root@server.sashubina.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.sashubina.net ~]#
```

Рис. 18: просмотр статуса защиты

На сервере внесем изменение в конфигурационный файл `/etc/fail2ban/jail.d/customisation.local`, добавив в раздел по умолчанию игнорирование адреса клиента:



```
GNU nano 8.1 /etc/fail2ban/jail.d/customisation.local
[DEFAULT]
bantime = 3600
gignoreip = 127.0.0.1/8 192.168.1.30
#
```

Рис. 19: Добавление в конфигурационный файл игнорирования адреса клиента

Перезапустим fail2ban

```
[root@server.sashubina.net ~]# systemctl restart fail2ban  
[root@server.sashubina.net ~]#
```

Рис. 20: перезапуск fail2ban

посмотрим журнал событий

```
[root@server.sashubina.net ~]# tail -f /var/log/fail2ban.log
2025-11-10 18:57:03,429 fail2ban.jail [8262]: INFO Jail 'apache-shellshock' started
2025-11-10 18:57:03,429 fail2ban.filtersystemd [8262]: INFO [postfix] Jail is in operation now (process new journal entries)
2025-11-10 18:57:03,429 fail2ban.jail [8262]: INFO Jail 'postfix' started
2025-11-10 18:57:03,430 fail2ban.filtersystemd [8262]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2025-11-10 18:57:03,430 fail2ban.jail [8262]: INFO Jail 'postfix-rbl' started
2025-11-10 18:57:03,430 fail2ban.filtersystemd [8262]: INFO [dovecot] Jail is in operation now (process new journal entries)
2025-11-10 18:57:03,430 fail2ban.jail [8262]: INFO Jail 'dovecot' started
2025-11-10 18:57:03,431 fail2ban.filtersystemd [8262]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2025-11-10 18:57:03,431 fail2ban.jail [8262]: INFO Jail 'postfix-sasl' started
2025-11-10 18:57:03,431 fail2ban.jail [8262]: INFO Jail 'sshd-ddos' started
```

Рис. 21: Просмотр журнала событий fail2ban

Вновь попытаемся войти с клиента на сервер с неправильным паролем

```

[sashubina@client.sashubina.net ~]$ ssh sashubina@192.168.1.1
sashubina@192.168.1.1's password:
Permission denied, please try again.
sashubina@192.168.1.1's password:
Permission denied, please try again.
sashubina@192.168.1.1's password:
sashubina@192.168.1.1: Permission denied (publickey,gssapi-keyex,gssapi-
with-mic,password).
[sashubina@client.sashubina.net ~]$

```

Рис. 22: попытка входа под неправильным паролем

и посмотрим статус защиты SSH:

```
[root@server.sashubina.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:    0
   `-- Banned IP list:
[root@server.sashubina.net ~]#
```

Рис. 23: Просмотр статуса защиты SSH после подключения к серверу с клиента по SSH с неправильным паролем

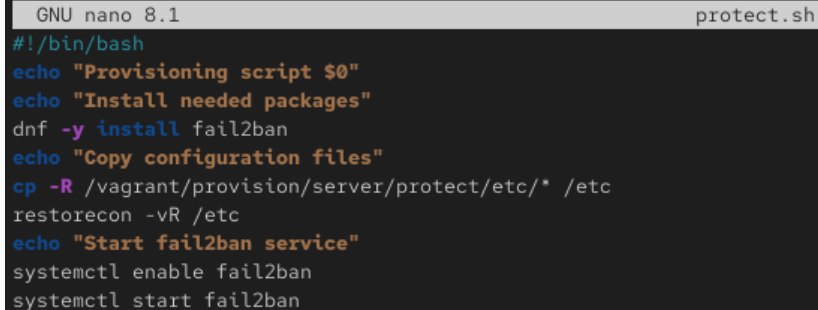
Внесение изменений в настройки внутреннего окружения виртуальных машины

На виртуальной машине `server` перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`, создадим в нём каталог `protect`, в который поместим в соответствующие подкаталоги конфигурационные файлы, а также создадим исполняемый файл `protect.sh`:

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

Рис. 24: создание файла

В каталоге `/vagrant/provision/server` создадим исполняемый файл `smb.sh` и внесем скрипт:



```
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
```

Рис. 25: Скрипта файла `/vagrant/provision/server/protect.sh`

Затем для отработки созданных скриптов в конфигурационном файле Vagrantfile необходимо добавить в соответствующих разделах конфигураций для сервера:

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

Рис. 26: Vagrantfile

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 фаервол. - Заблокированный IP-адрес может быть разблокирован автоматически после определенного периода времени.

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

Настройки файла `jail.local` более приоритетны, чем настройки файла `jail.conf`. Если в файле `jail.local` определены одни и те же параметры, они будут использованы вместо параметров из `jail.conf`.

3. 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 SMTP-сервера.

4. 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.

5. 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.

6. 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.

7. Как получить список действующих правил Fail2ban?

Для получения списка действующих правил Fail2ban можно использовать команду: `fail2ban-client status`.

8. Как получить статистику заблокированных Fail2ban адресов?

Для получения статистики заблокированных адресов Fail2ban можно использовать команду: `fail2ban-client status <jail-name>`, где `<jail-name>` - имя конкретного jail, например, “ssh” или “apache”.

9. Как разблокировать IP-адрес?

Разблокировать адрес можно с помощью следующей команды

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

В результате выполнения данной работы были приобретены практические навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».