

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 16

«Базовая защита от атак типа «brute force»»

Дисциплина: Администрирование сетевых подсистем

Студент: Карташова А.С.

Группа: НФИбд-03-18

МОСКВА

2020 г.

Оглавление

Цель работы	2
Задачи.....	2
Ход работы	2
Защита с помощью Fail2ban	2
Проверка работы Fail2ban	6
Внесение изменений в настройки внутреннего окружения виртуальных машин.....	9
Заключение.....	10
Контрольные вопросы.....	11

Цель работы

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

Задачи

1. Установить и настроить Fail2ban для отслеживания работы установленных на сервере служб
2. Проверить работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH
3. Написать скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban

Ход работы

Защита с помощью Fail2ban

На сервере установим fail2ban:

Команда: `dnf -y install fail2ban`

Запустим сервер fail2ban:

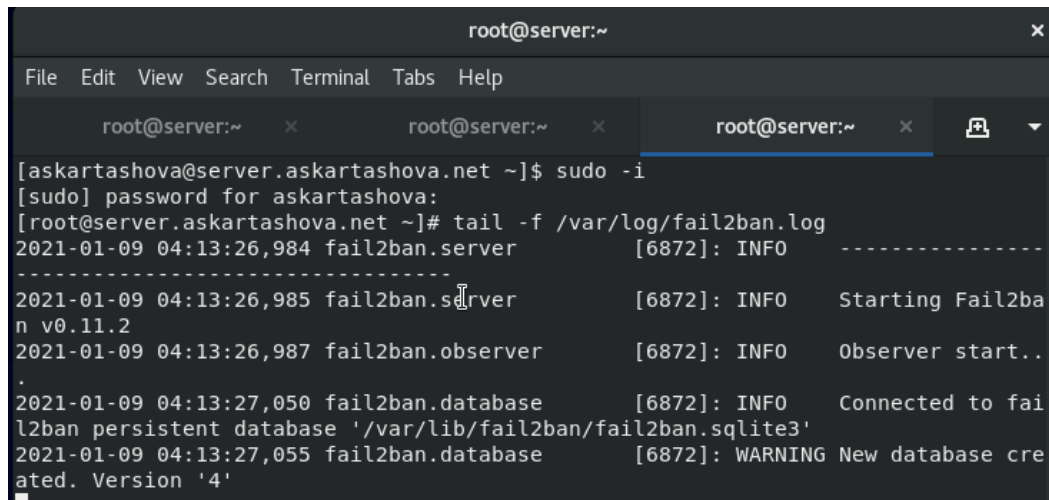
Команда: `systemctl start fail2ban`

`systemctl enable fail2ban`

```
bash: !251501: command not found...  
[root@server.askartashova.net ~]# systemctl start fail2ban  
[root@server.askartashova.net ~]# systemctl enable fail2ban
```

В дополнительном терминале запустим просмотр журнала событий fail2ban:

Команда: `tail -f /var/log/fail2ban.log`



```
root@server:~  
File Edit View Search Terminal Tabs Help  
root@server:~ x root@server:~ x root@server:~ x  
[askartashova@server.askartashova.net ~]$ sudo -i  
[sudo] password for askartashova:  
[root@server.askartashova.net ~]# tail -f /var/log/fail2ban.log  
2021-01-09 04:13:26,984 fail2ban.server [6872]: INFO -----  
-----  
2021-01-09 04:13:26,985 fail2ban.server [6872]: INFO Starting Fail2ban v0.11.2  
2021-01-09 04:13:26,987 fail2ban.observer [6872]: INFO Observer started.  
.  
2021-01-09 04:13:27,050 fail2ban.database [6872]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'  
2021-01-09 04:13:27,055 fail2ban.database [6872]: WARNING New database created. Version '4'
```

Создадим файл с локальной конфигурацией fail2ban:

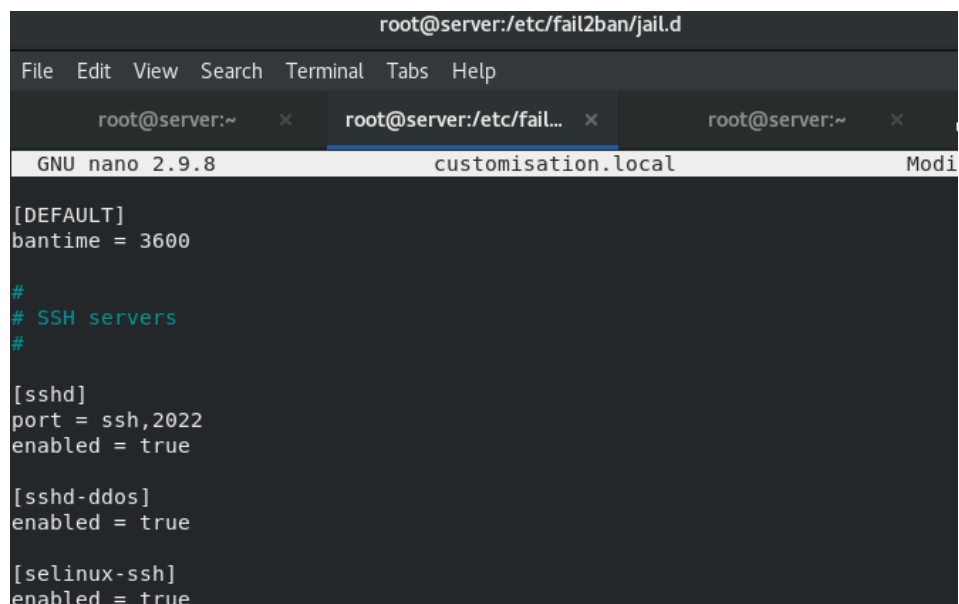
Команда: `touch /etc/fail2ban/jail.d/customisation.local`

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

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

а) задайте время блокирования на 1 час (время задаётся в секундах):

б) включим защиту SSH:



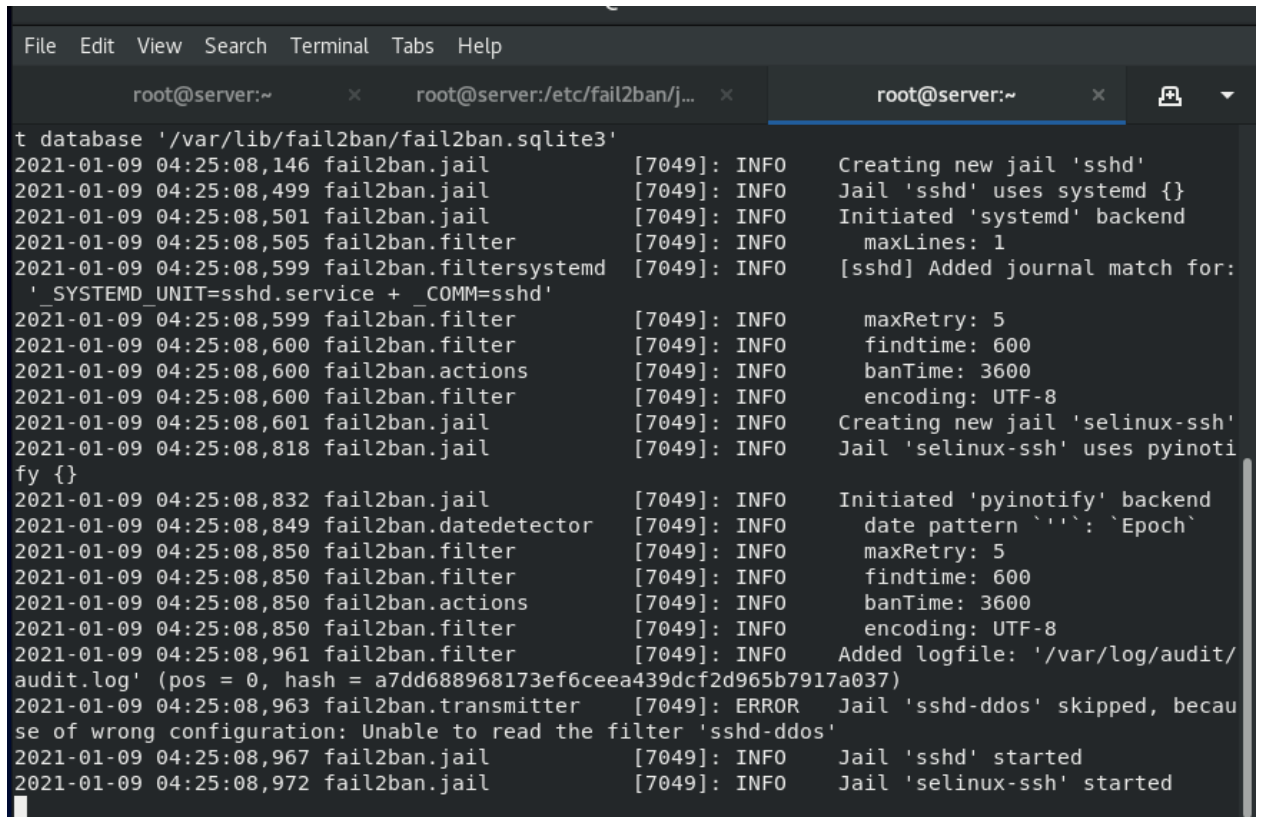
```
root@server:/etc/fail2ban/jail.d  
File Edit View Search Terminal Tabs Help  
root@server:~ x root@server:/etc/fail... x root@server:~ x  
GNU nano 2.9.8 customisation.local Modi  
[DEFAULT]  
bantime = 3600  
#  
# SSH servers  
#  
[sshd]  
port = ssh,2022  
enabled = true  
  
[sshd-ddos]  
enabled = true  
  
[selinux-ssh]  
enabled = true
```

Перезапустим fail2ban

Команда: systemctl restart fail2ban

Посмотрим журнал событий:

Команда: tail -f /var/log/fail2ban.log



```
File Edit View Search Terminal Tabs Help
root@server:~ x root@server:/etc/fail2ban/j... x root@server:~ x
t database '/var/lib/fail2ban/fail2ban.sqlite3'
2021-01-09 04:25:08,146 fail2ban.jail [7049]: INFO Creating new jail 'sshd'
2021-01-09 04:25:08,499 fail2ban.jail [7049]: INFO Jail 'sshd' uses systemd {}
2021-01-09 04:25:08,501 fail2ban.jail [7049]: INFO Initiated 'systemd' backend
2021-01-09 04:25:08,505 fail2ban.filter [7049]: INFO maxLines: 1
2021-01-09 04:25:08,599 fail2ban.filtersystemd [7049]: INFO [sshd] Added journal match for:
'_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2021-01-09 04:25:08,599 fail2ban.filter [7049]: INFO maxRetry: 5
2021-01-09 04:25:08,600 fail2ban.filter [7049]: INFO findtime: 600
2021-01-09 04:25:08,600 fail2ban.actions [7049]: INFO banTime: 3600
2021-01-09 04:25:08,600 fail2ban.filter [7049]: INFO encoding: UTF-8
2021-01-09 04:25:08,601 fail2ban.jail [7049]: INFO Creating new jail 'selinux-ssh'
2021-01-09 04:25:08,818 fail2ban.jail [7049]: INFO Jail 'selinux-ssh' uses pyinoti
fy {}
2021-01-09 04:25:08,832 fail2ban.jail [7049]: INFO Initiated 'pyinotify' backend
2021-01-09 04:25:08,849 fail2ban.datedetector [7049]: INFO date pattern `''`: `Epoch`
2021-01-09 04:25:08,850 fail2ban.filter [7049]: INFO maxRetry: 5
2021-01-09 04:25:08,850 fail2ban.filter [7049]: INFO findtime: 600
2021-01-09 04:25:08,850 fail2ban.actions [7049]: INFO banTime: 3600
2021-01-09 04:25:08,850 fail2ban.filter [7049]: INFO encoding: UTF-8
2021-01-09 04:25:08,961 fail2ban.filter [7049]: INFO Added logfile: '/var/log/audit/
audit.log' (pos = 0, hash = a7dd688968173ef6ceea439dcf2d965b7917a037)
2021-01-09 04:25:08,963 fail2ban.transmitter [7049]: ERROR Jail 'sshd-ddos' skipped, becau
se of wrong configuration: Unable to read the filter 'sshd-ddos'
2021-01-09 04:25:08,967 fail2ban.jail [7049]: INFO Jail 'sshd' started
2021-01-09 04:25:08,972 fail2ban.jail [7049]: INFO Jail 'selinux-ssh' started
```

Мы видим, что запустились службы sshd и selinux-ssh

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

```
mc [root@server.askartashova.net]:/etc/fail2ban/filter.d
File Edit View Search Terminal Tabs Help
root@server:~ x mc [root@server.askartashova.ne... x root@serv
GNU nano 2.9.8 /etc/fail2ban/jail.d/customisation.local

# 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
```

Перезапустим fail2ban

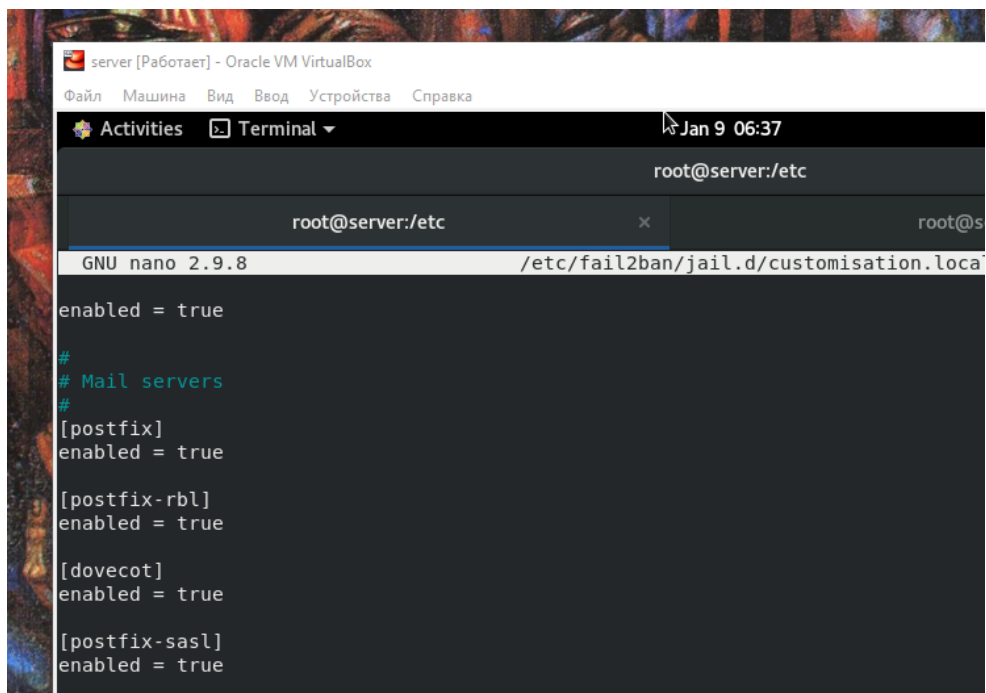
Команда: systemctl restart fail2ban

Посмотрим журнал событий:

```
2021-01-09 05:42:39,169 fail2ban.jail [5828]: INFO Jail 'sshd' uses systemd {}
2021-01-09 05:42:39,190 fail2ban.jail [5828]: INFO Initiated 'systemd' backend
2021-01-09 05:42:39,192 fail2ban.filter [5828]: INFO maxlines: 1
2021-01-09 05:42:39,286 fail2ban.filtersystemd [5828]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + COMM=sshd'
2021-01-09 05:42:39,286 fail2ban.filter [5828]: INFO maxRetry: 5
2021-01-09 05:42:39,286 fail2ban.filter [5828]: INFO findtime: 600
2021-01-09 05:42:39,286 fail2ban.actions [5828]: INFO banTime: 3600
2021-01-09 05:42:39,287 fail2ban.filter [5828]: INFO encoding: UTF-8
2021-01-09 05:42:39,287 fail2ban.jail [5828]: INFO Creating new jail 'selinux-ssh'
2021-01-09 05:42:39,360 fail2ban.jail [5828]: INFO Jail 'selinux-ssh' uses pyinotify {}
2021-01-09 05:42:39,369 fail2ban.jail [5828]: INFO Initiated 'pyinotify' backend
2021-01-09 05:42:39,373 fail2ban.datedetector [5828]: INFO date pattern '': 'Epoch'
2021-01-09 05:42:39,374 fail2ban.filter [5828]: INFO maxRetry: 5
2021-01-09 05:42:39,374 fail2ban.filter [5828]: INFO findtime: 600
2021-01-09 05:42:39,374 fail2ban.actions [5828]: INFO banTime: 3600
2021-01-09 05:42:39,374 fail2ban.filter [5828]: INFO encoding: UTF-8
2021-01-09 05:42:39,399 fail2ban.filter [5828]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 2253998, hash = a7dd688968173ef6ceea439dcf2d965b7917a037)
2021-01-09 05:42:39,400 fail2ban.transmitter [5828]: ERROR Jail 'sshd-ddos' skipped, because of wrong configuration: Unable to read the filter 'sshd-ddos'
2021-01-09 05:42:39,413 fail2ban.jail [5828]: INFO Jail 'sshd' started
2021-01-09 05:42:39,415 fail2ban.jail [5828]: INFO Jail 'selinux-ssh' started
2021-01-09 05:45:54,980 fail2ban.server [5828]: INFO Shutdown in progress...
2021-01-09 05:45:54,981 fail2ban.observer [5828]: INFO Observer stop ... try to end queue 5 seconds
2021-01-09 05:45:55,001 fail2ban.observer [5828]: INFO Observer stopped, 0 events remaining.
2021-01-09 05:45:55,042 fail2ban.server [5828]: INFO Stopping all jails
2021-01-09 05:45:55,043 fail2ban.filter [5828]: INFO Removed logfile: '/var/log/audit/audit.log'
2021-01-09 05:45:55,778 fail2ban.jail [5828]: INFO Jail 'sshd' stopped
2021-01-09 05:45:55,779 fail2ban.jail [5828]: INFO Jail 'selinux-ssh' stopped
2021-01-09 05:45:55,779 fail2ban.database [5828]: INFO Connection to database closed.
2021-01-09 05:45:55,779 fail2ban.server [5828]: INFO Exiting Fail2ban
```

Команда: tail -f /var/log/fail2ban.log

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



```
server [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Activities  Terminal
Jan 9 06:37
root@server:/etc
GNU nano 2.9.8 /etc/fail2ban/jail.d/customisation.local

enabled = true

#
# Mail servers
#
[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

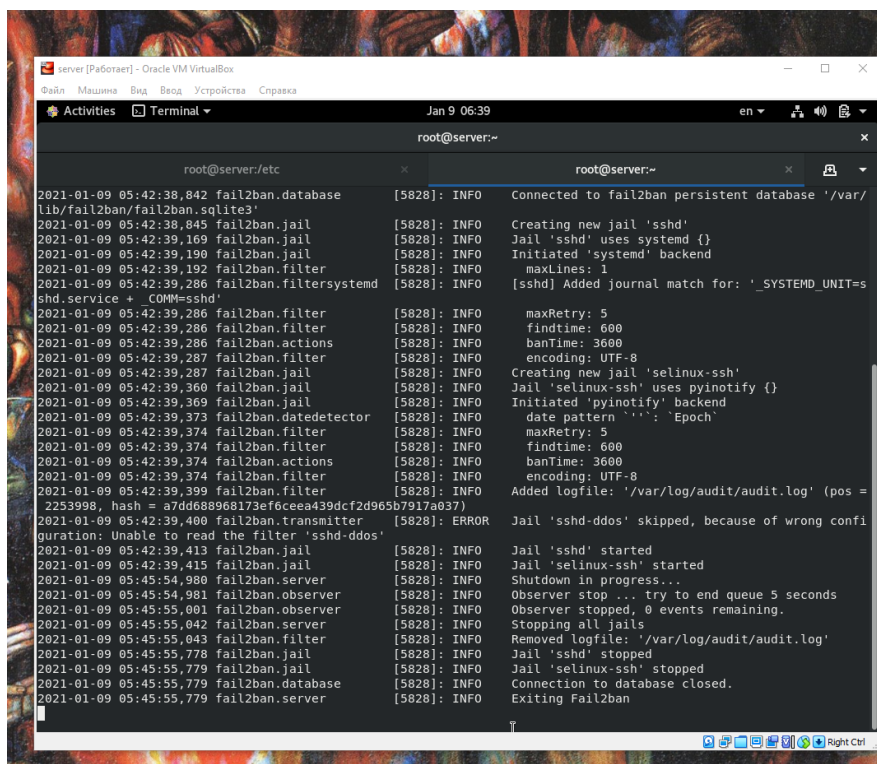
[postfix-sasl]
enabled = true
```

Перезапустим fail2ban:

Команда: systemctl restart fail2ban

Посмотрим журнал событий:

Команда: tail -f /var/log/fail2ban.log



```
server [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Jan 9 06:39
root@server:~
root@server:/etc
root@server:~
2021-01-09 05:42:38,842 fail2ban.database [5828]: INFO Connected to fail2ban persistent database '/var/
lib/fail2ban/fail2ban.sqlite3'
2021-01-09 05:42:38,845 fail2ban.jail [5828]: INFO Creating new jail 'sshd'
2021-01-09 05:42:39,169 fail2ban.jail [5828]: INFO Jail 'sshd' uses systemd {}
2021-01-09 05:42:39,190 fail2ban.jail [5828]: INFO Initiated 'systemd' backend
2021-01-09 05:42:39,192 fail2ban.filter [5828]: INFO maxLines: 1
2021-01-09 05:42:39,286 fail2ban.filtersystemd [5828]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=s
shd.service + _COMM=sshd'
2021-01-09 05:42:39,286 fail2ban.filter [5828]: INFO maxRetry: 5
2021-01-09 05:42:39,286 fail2ban.filter [5828]: INFO findtime: 600
2021-01-09 05:42:39,286 fail2ban.actions [5828]: INFO banTime: 3600
2021-01-09 05:42:39,287 fail2ban.filter [5828]: INFO encoding: UTF-8
2021-01-09 05:42:39,287 fail2ban.jail [5828]: INFO Creating new jail 'selinux-ssh'
2021-01-09 05:42:39,360 fail2ban.jail [5828]: INFO Jail 'selinux-ssh' uses pyinotify {}
2021-01-09 05:42:39,369 fail2ban.jail [5828]: INFO Initiated 'pyinotify' backend
2021-01-09 05:42:39,373 fail2ban.datedetector [5828]: INFO date pattern '': 'Epoch'
2021-01-09 05:42:39,374 fail2ban.filter [5828]: INFO maxRetry: 5
2021-01-09 05:42:39,374 fail2ban.filter [5828]: INFO findtime: 600
2021-01-09 05:42:39,374 fail2ban.actions [5828]: INFO banTime: 3600
2021-01-09 05:42:39,374 fail2ban.filter [5828]: INFO encoding: UTF-8
2021-01-09 05:42:39,399 fail2ban.filter [5828]: INFO Added logfile: '/var/log/audit/audit.log' (pos =
2253998, hash = a7dd688968173ef6ceea439dcf2d965b7917a037)
2021-01-09 05:42:39,400 fail2ban.transmitter [5828]: ERROR Jail 'sshd-ddos' skipped, because of wrong confi
guration: Unable to read the filter 'sshd-ddos'
2021-01-09 05:42:39,413 fail2ban.jail [5828]: INFO Jail 'sshd' started
2021-01-09 05:42:39,415 fail2ban.jail [5828]: INFO Jail 'selinux-ssh' started
2021-01-09 05:45:54,980 fail2ban.server [5828]: INFO Shutdown in progress...
2021-01-09 05:45:54,981 fail2ban.observer [5828]: INFO Observer stop ... try to end queue 5 seconds
2021-01-09 05:45:55,001 fail2ban.observer [5828]: INFO Observer stopped, 0 events remaining.
2021-01-09 05:45:55,042 fail2ban.server [5828]: INFO Stopping all jails
2021-01-09 05:45:55,043 fail2ban.filter [5828]: INFO Removed logfile: '/var/log/audit/audit.log'
2021-01-09 05:45:55,778 fail2ban.jail [5828]: INFO Jail 'sshd' stopped
2021-01-09 05:45:55,779 fail2ban.jail [5828]: INFO Jail 'selinux-ssh' stopped
2021-01-09 05:45:55,779 fail2ban.database [5828]: INFO Connection to database closed.
2021-01-09 05:45:55,779 fail2ban.server [5828]: INFO Exiting Fail2ban
```

Проверка работы Fail2ban

На сервере посмотрим статус fail2ban:

Команда: fail2ban-client status

```
[root@server.askartashova.net etc]# fail2ban-client status
Status
|- Number of jail:      6
`- Jail list:  dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd
[root@server.askartashova.net etc]#
```

Посмотрим статус защиты SSH в fail2ban:

Команда: fail2ban-client status sshd

```
[root@server.askartashova.net etc]# fail2ban-client status
Status
|- Number of jail:      6
`- Jail list:  dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd
[root@server.askartashova.net etc]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:    0
|  `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:    0
   `-- Banned IP list:
```

Установим максимальное количество ошибок для SSH, равное 2:

Команда: fail2ban-client set sshd maxretry 2

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

С клиента попытаемся зайти по SSH на сервер с неправильным паролем.

```
connection to server.askartashova.net closed.
[root@client.askartashova.net ~]# ssh askartashova@server.askartashova.net
askartashova@server.askartashova.net's password:
Permission denied, please try again.
askartashova@server.askartashova.net's password: █
```

На сервере посмотрим статус защиты SSH:

Команда: fail2ban-client status sshd

```
[root@server.askartashova.net etc]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 1
|   |- Total failed:    1
|   \- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
|   |- Currently banned: 0
|   |- Total banned:    0
|   \- Banned IP list:
[root@server.askartashova.net etc]#
```

Убедимся, что произошла блокировка адреса клиента.

Разблокируем IP-адрес клиента:

Команда: `fail2ban-client set sshd unbanip 192.168.1.30`

Вновь посмотрим статус защиты SSH:

Команда: `fail2ban-client status sshd`

Убедимся, что блокировка клиента снята

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

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

Перезапустим fail2ban.

```
[root@server.askartashova.net fz]# nano /etc/fail2ban/jail.d/customisation.local
[root@server.askartashova.net fz]# systemctl restart fail2ban
```

Посмотрим журнал событий:

Команда: tail -f /var/log/fail2ban.log

```
Activities Terminal Jan 9 09:53 en
root@server:~
root@server:/var/named/master/fz
2021-01-09 09:53:01,343 fail2ban.filter [9189]: INFO Removed logfile: '/var/log/audit/audit.log'
2021-01-09 09:53:01,360 fail2ban.jail [9189]: INFO Jail 'sshd' stopped
2021-01-09 09:53:01,360 fail2ban.jail [9189]: INFO Jail 'selinux-ssh' stopped
2021-01-09 09:53:01,360 fail2ban.database [9189]: INFO Connection to database closed.
2021-01-09 09:53:01,360 fail2ban.server [9189]: INFO Exiting Fail2ban
2021-01-09 09:53:01,715 fail2ban.server [9216]: INFO -----
2021-01-09 09:53:01,716 fail2ban.server [9216]: INFO Starting Fail2ban v0.11.2
2021-01-09 09:53:01,717 fail2ban.observer [9216]: INFO Observer start...
2021-01-09 09:53:01,721 fail2ban.database [9216]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2021-01-09 09:53:01,722 fail2ban.jail [9216]: INFO Creating new jail 'sshd'
2021-01-09 09:53:01,750 fail2ban.jail [9216]: INFO Jail 'sshd' uses systemd {}
2021-01-09 09:53:01,750 fail2ban.jail [9216]: INFO Initiated 'systemd' backend
2021-01-09 09:53:01,753 fail2ban.filter [9216]: INFO maxLines: 1
2021-01-09 09:53:01,818 fail2ban.filtersystemd [9216]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2021-01-09 09:53:01,818 fail2ban.filter [9216]: INFO maxRetry: 5
2021-01-09 09:53:01,819 fail2ban.filter [9216]: INFO findtime: 600
2021-01-09 09:53:01,819 fail2ban.actions [9216]: INFO banTime: 3600
2021-01-09 09:53:01,819 fail2ban.filter [9216]: INFO encoding: UTF-8
2021-01-09 09:53:01,820 fail2ban.jail [9216]: INFO Creating new jail 'selinux-ssh'
2021-01-09 09:53:01,849 fail2ban.jail [9216]: INFO Jail 'selinux-ssh' uses pyinotify {}
2021-01-09 09:53:01,860 fail2ban.jail [9216]: INFO Initiated 'pyinotify' backend
2021-01-09 09:53:01,865 fail2ban.datedetector [9216]: INFO date pattern '': 'Epoch'
2021-01-09 09:53:01,865 fail2ban.filter [9216]: INFO maxRetry: 5
2021-01-09 09:53:01,866 fail2ban.filter [9216]: INFO findtime: 600
2021-01-09 09:53:01,866 fail2ban.actions [9216]: INFO banTime: 3600
2021-01-09 09:53:01,866 fail2ban.filter [9216]: INFO encoding: UTF-8
2021-01-09 09:53:01,867 fail2ban.filter [9216]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 2572576, hash = a7dd688968173ef6ceea439dcf2d965b7917a037)
2021-01-09 09:53:01,868 fail2ban.transmitter [9216]: ERROR Jail 'sshd-ddos' skipped, because of wrong configuration: Unable to read the filter 'sshd-ddos'
2021-01-09 09:53:01,887 fail2ban.jail [9216]: INFO Jail 'sshd' started
2021-01-09 09:53:01,901 fail2ban.jail [9216]: INFO Jail 'selinux-ssh' started
```

Вновь попытаюсь войти с клиента на сервер с неправильным паролем и посмотрит статус защиты SSH.

```
askartashova@server.askartashova.net's password:
Connection closed by 192.168.1.1 port 22
[root@client.askartashova.net ~]#
```

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

Внесение изменений в настройки внутреннего окружения виртуальных машин

На виртуальной машине server перейдем в каталог для внесения изменений в

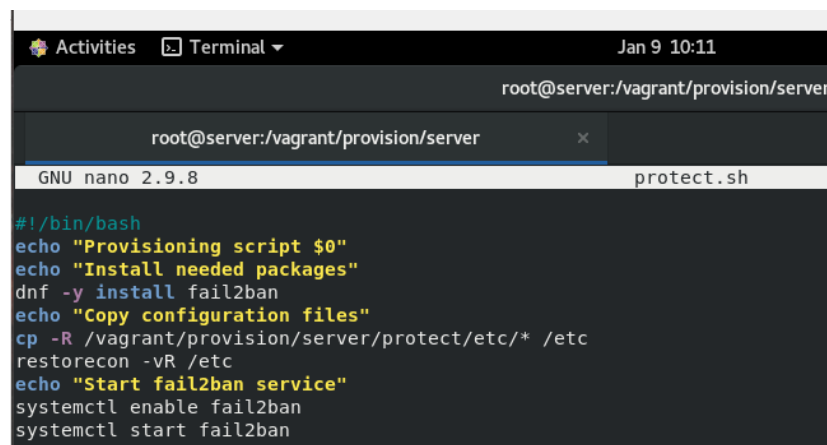
настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог protect, в который поместим в соответствующие подкаталоги конфигурационные файлы.

```
- Banned IP list:
[root@server.askartashova.net fz]# cd /vagrant/provision/server
[root@server.askartashova.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.askartashova.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/s
protect/etc/fail2ban/jail.d/
```

В каталоге /vagrant/provision/server создайте исполняемый файл protect.sh:

Открыв его на редактирование, пропишем в нём скрипт, повторяющий наши действия.

```
[root@server.askartashova.net server]# cd /vagrant/provision/server
[root@server.askartashova.net server]# touch protect.sh
[root@server.askartashova.net server]# chmod +x protect.sh
[root@server.askartashova.net server]# nano protect.sh
[root@server.askartashova.net server]#
```



```
Activities Terminal Jan 9 10:11
root@server:/vagrant/provision/server
root@server:/vagrant/provision/server
GNU nano 2.9.8 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
```

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в соответствующем разделе конфигураций для сервера

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

Заключение

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

Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban отслеживает сетевую активность на портах узла путём сканирования текстовых лог-файлов. При выявлении программой неадекватной активности какого-то узла, его IP-адрес помещается в чёрный список, а все пакеты с этого адреса блокируются. Блокировка настраивается путём внесения изменений в правила межсетевого экрана.

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

Основной файл конфигурации конкретных служб в Fail2ban — `/etc/fail2ban/jail.conf`, для нас приоритетнее собственные настройки, размещенные в файле `customisation.local`

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Настройки оповещения о срабатывании блокировки Fail2ban находятся в разделе `[DEFAULT]`. Если на машине был настроен почтовый сервер, он отправит письма на внешний адрес. Иначе все письма будут доставлены к локальной учетной записи Linux.

Для настройки используются два параметра:

- **destemail** - этот параметр задает адрес электронной почты, на который вы хотите получать сообщения. Значение по умолчанию `root@localhost`;
- **mta** - определяет почтовый агент, который будет использоваться для доставки почты. Если же письма нужно доставлять на локальную машину поменяйте значение на `mail`.

Также для локальной почты нужно заменить строчку **action_mw** на **action_mwl**:

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

```
jail.conf [----] 31 L:[304+10 314/965] *(11345/24996b) 0105 0
# HTTP servers
#

[apache-auth]

port      = http,https
logpath   = %(apache_error_log)s

[apache-badbots]
# Ban hosts which agent identifies spammer robots crawling the web
# for email addresses. The mail outputs are buffered.
port      = http,https
logpath   = %(apache_access_log)s
bantime   = 48h
maxretry  = 1

[apache-noscript]

port      = http,https
logpath   = %(apache_error_log)s

[apache-overflows]

port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 2
```

```
jail.conf [----] 21 L:[334+10 344/965] *(11811/24996b) 06
[apache-nohome]

port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 2

[apache-botsearch]

port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 2

[apache-fakegooglebot]

port      = http,https
logpath   = %(apache_access_log)s
maxretry  = 1
ignorecommand = %(ignorecommands_dir)s/apache-fakegooglebot <ip>

[apache-modsecurity]

port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 2

[apache-shellshock]

port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 1
```

apache-auth, apache-overflows, apache-auth, apache-nohome, apache-botsearch, apache-auth, apache-auth, apache-auth – сервисы(jails) веб-сервера apache

`maxretry`-количество срабатываний правил, после которого надо применять фильтр (бан)

`bantime` - Указывается в секундах. Определяет на какой период времени будет блокироваться доступ, в случае срабатывания правила

Параметр `filter` определяет является ли строка в логах индикатором об ошибочной авторизации или нет.

`logpath` – логи которые необходимо анализировать на предмет атаки

`port`- номера портов, которые необходимо блокировать

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

```
# ASSP SMTP Proxy Jail
[assp]

port      = smtp,465,submission
logpath   = /root/path/to/assp/logs/maillog.txt

[courier-smtp]

port      = smtp,465,submission
logpath   = %(syslog_mail)s
backend   = %(syslog_backend)s

[postfix]
# To use another modes set filter parameter "mode" in jail.local:
mode      = more
port      = smtp,465,submission
logpath   = %(postfix_log)s
backend   = %(postfix_backend)s

[postfix-rbl]

filter     = postfix[mode=rbl]
port      = smtp,465,submission
logpath    = %(postfix_log)s
backend    = %(postfix_backend)s
maxretry   = 1
```

```
jail.conf [---] 0 L:[596+ 8 604/965] *(16861/249968) 0010 0x00A

[sendmail-auth]
port      = submission,465,smtp
logpath   = %(syslog_mail)s
backend   = %(syslog_backend)s

[sendmail-reject]
# To use more aggressive modes set filter parameter "mode" in jail.local:
# normal (default), extra or aggressive
# See "tests/files/logs/sendmail-reject" or "filter.d/sendmail-reject.conf" for
#mode      = normal
port       = smtp,465,submission
logpath    = %(syslog_mail)s
backend    = %(syslog_backend)s

[qmail-rbl]
filter     = qmail
port       = smtp,465,submission
logpath    = /service/qmail/log/main/current

# dovecot defaults to logging to the mail syslog facility
# but can be set by syslog_facility in the dovecot configuration.
[dovecot]
port       = pop3,pop3s,imap,imaps,submission,465,sieve
logpath    = %(dovecot_log)s
backend    = %(dovecot_backend)s
```

```
[sieve]
port       = smtp,465,submission
logpath    = %(dovecot_log)s
backend    = %(dovecot_backend)s

[solid-pop3d]
port       = pop3,pop3s
logpath    = %(solidpop3d_log)s

[exim]
# see filter.d/exim.conf for further modes supported from filter:
#mode = normal
port       = smtp,465,submission
logpath    = %(exim_main_log)s

[exim-spam]
port       = smtp,465,submission
logpath    = %(exim_main_log)s

[kerio]
port       = imap,smtp,imaps,465
logpath    = /opt/kerio/mailserver/store/logs/security.log
```

logpath – логи, которые необходимо анализировать на предмет атаки

port- номера портов, которые необходимо блокировать

assp – служба системы защиты от спама, распространяемая бесплатно.

exim (experimental internet mailer) — агент пересылки сообщений

postfix — агент передачи почты

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

Когда fail2ban мониторит логи сервиса, он смотрит на настроенный для этого сервиса фильтр. Фильтр предназначен для определения сбоев аутентификации этого конкретного сервиса на основе сложных регулярных выражений. Когда строка в файле лога сервиса совпадает с параметром failregex в соответствующем фильтре, fail2ban выполняет заданное фильтром действие. Действие определяется в переменной action.

Действие по умолчанию — блокировка потенциально вредоносного хоста/IP-адреса путем изменения правил брандмауэра iptables. Мы можем расширить это действие — настроить электронные уведомления администратора с данными о злоумышленнике или строками лога, которые вызвали указанное действие. Доступные действия можно посмотреть в файле /etc/fail2ban/action.d.

7. Как получить список действующих правил Fail2ban?

Команда: *fail2ban-client status*

8. Как получить статистику заблокированных Fail2ban адресов?

Команда: *fail2ban-client -v status sshd*

9. Как разблокировать IP-адрес?

Команда: *fail2ban-client set sshd unbanip <ip-адрес клиента>*