

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 16

дисциплина: Администрирование сетевых подсистем

Студент: Бакулин Никита 1032201747

Группа: НПИбд-01-20

МОСКВА

2022 г.

Постановка задачи

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб.
2. Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH.
3. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban.

Выполнение работы

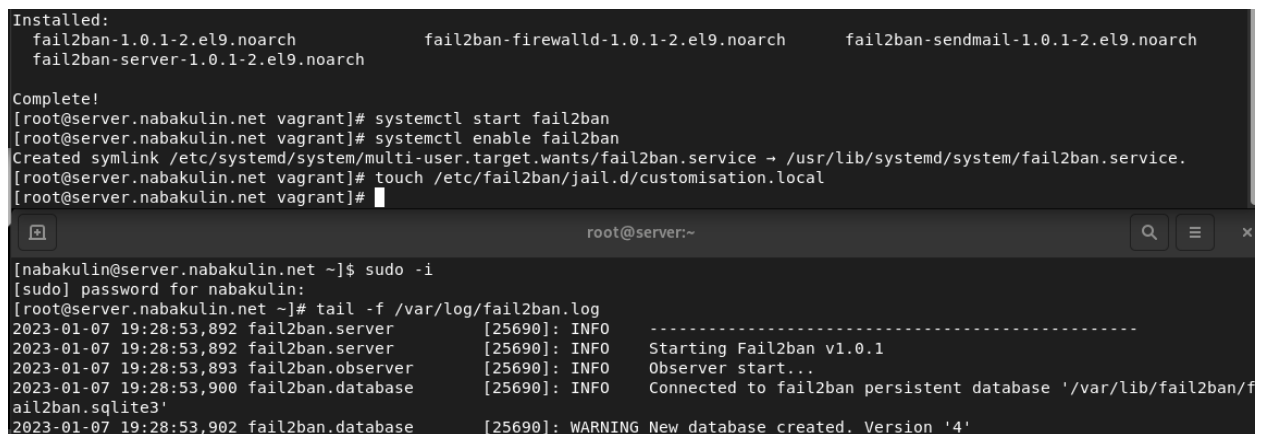
1.

1.1. На сервере установите fail2ban

1.2. Запустите сервер fail2ban

1.3. В дополнительном терминале запустите просмотр журнала событий fail2ban

1.4. Создайте файл с локальной конфигурацией fail2ban



```
Installed:
  fail2ban-1.0.1-2.el9.noarch      fail2ban-firewalld-1.0.1-2.el9.noarch      fail2ban-sendmail-1.0.1-2.el9.noarch
  fail2ban-server-1.0.1-2.el9.noarch

Complete!
[root@server.nabakulin.net vagrant]# systemctl start fail2ban
[root@server.nabakulin.net vagrant]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/system/fail2ban.service.
[root@server.nabakulin.net vagrant]# touch /etc/fail2ban/jail.d/customisation.local
[root@server.nabakulin.net vagrant]#

[nabakulin@server.nabakulin.net ~]$ sudo -i
[sudo] password for nabakulin:
[root@server.nabakulin.net ~]# tail -f /var/log/fail2ban.log
2023-01-07 19:28:53,892 fail2ban.server [25690]: INFO -----
2023-01-07 19:28:53,892 fail2ban.server [25690]: INFO Starting Fail2ban v1.0.1
2023-01-07 19:28:53,893 fail2ban.observer [25690]: INFO Observer start...
2023-01-07 19:28:53,900 fail2ban.database [25690]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/f
ail2ban.sqlite3'
2023-01-07 19:28:53,902 fail2ban.database [25690]: WARNING New database created. Version '4'
```

Рисунок 1

- 1.5. В файле /etc/fail2ban/jail.d/customisation.local задайте время блокирования на 1 час, включите защиту SSH

```

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

```

Рисунок 2

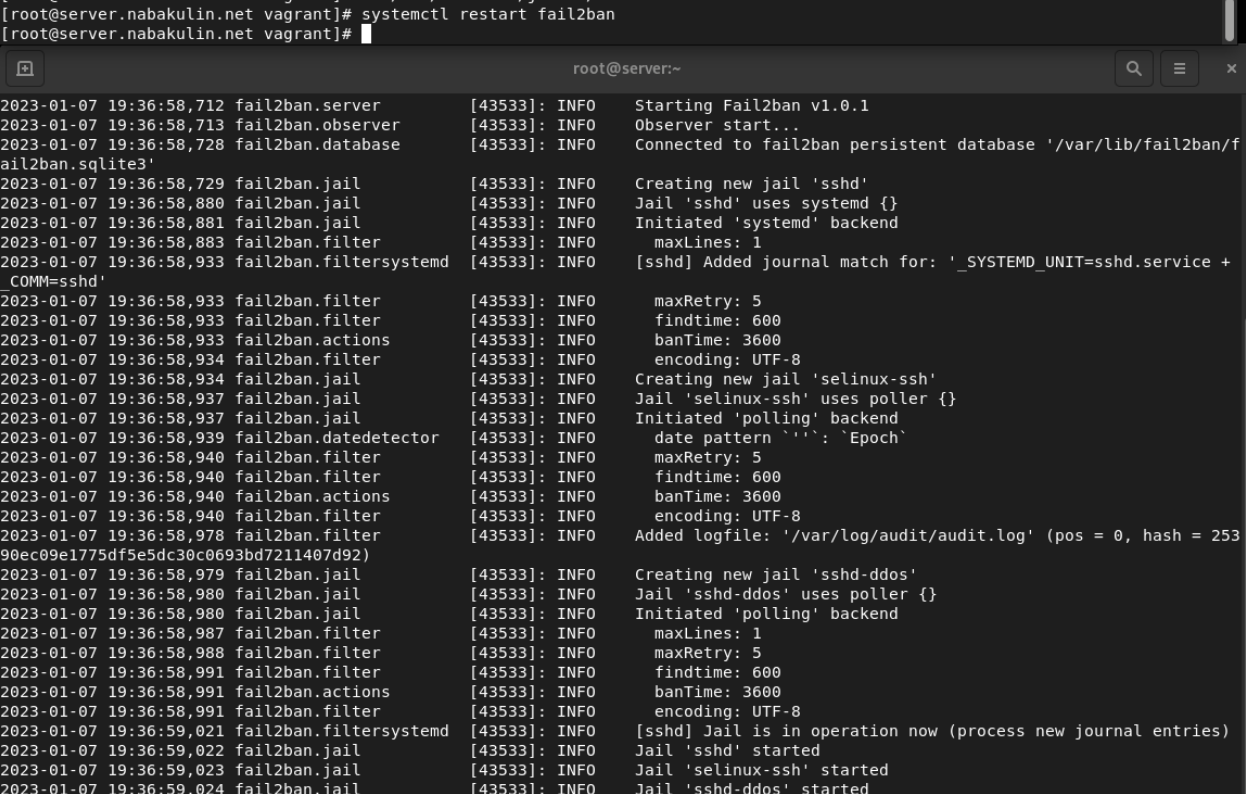
1.6. Перезапустите fail2ban

1.7. Посмотрите журнал событий

```

[root@server.nabakulin.net vagrant]# systemctl restart fail2ban
[root@server.nabakulin.net vagrant]#

```



```

2023-01-07 19:36:58,712 fail2ban.server [43533]: INFO Starting Fail2ban v1.0.1
2023-01-07 19:36:58,713 fail2ban.observer [43533]: INFO Observer start...
2023-01-07 19:36:58,728 fail2ban.database [43533]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/f
ail2ban.sqlite3'
2023-01-07 19:36:58,729 fail2ban.jail [43533]: INFO Creating new jail 'sshd'
2023-01-07 19:36:58,880 fail2ban.jail [43533]: INFO Jail 'sshd' uses systemd {}
2023-01-07 19:36:58,881 fail2ban.jail [43533]: INFO Initiated 'systemd' backend
2023-01-07 19:36:58,883 fail2ban.filter [43533]: INFO maxLines: 1
2023-01-07 19:36:58,933 fail2ban.filtersystemd [43533]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service +
COMM=sshd'
2023-01-07 19:36:58,933 fail2ban.filter [43533]: INFO maxRetry: 5
2023-01-07 19:36:58,933 fail2ban.filter [43533]: INFO findtime: 600
2023-01-07 19:36:58,933 fail2ban.actions [43533]: INFO bantime: 3600
2023-01-07 19:36:58,934 fail2ban.filter [43533]: INFO encoding: UTF-8
2023-01-07 19:36:58,934 fail2ban.jail [43533]: INFO Creating new jail 'selinux-ssh'
2023-01-07 19:36:58,937 fail2ban.jail [43533]: INFO Jail 'selinux-ssh' uses poller {}
2023-01-07 19:36:58,937 fail2ban.jail [43533]: INFO Initiated 'polling' backend
2023-01-07 19:36:58,939 fail2ban.datedetector [43533]: INFO date pattern '': 'Epoch'
2023-01-07 19:36:58,940 fail2ban.filter [43533]: INFO maxRetry: 5
2023-01-07 19:36:58,940 fail2ban.filter [43533]: INFO findtime: 600
2023-01-07 19:36:58,940 fail2ban.actions [43533]: INFO bantime: 3600
2023-01-07 19:36:58,940 fail2ban.filter [43533]: INFO encoding: UTF-8
2023-01-07 19:36:58,978 fail2ban.filter [43533]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 253
90ec09e1775df5e5dc30c0693bd7211407d92)
2023-01-07 19:36:58,979 fail2ban.jail [43533]: INFO Creating new jail 'sshd-ddos'
2023-01-07 19:36:58,980 fail2ban.jail [43533]: INFO Jail 'sshd-ddos' uses poller {}
2023-01-07 19:36:58,980 fail2ban.jail [43533]: INFO Initiated 'polling' backend
2023-01-07 19:36:58,987 fail2ban.filter [43533]: INFO maxLines: 1
2023-01-07 19:36:58,988 fail2ban.filter [43533]: INFO maxRetry: 5
2023-01-07 19:36:58,991 fail2ban.filter [43533]: INFO findtime: 600
2023-01-07 19:36:58,991 fail2ban.actions [43533]: INFO bantime: 3600
2023-01-07 19:36:58,991 fail2ban.filter [43533]: INFO encoding: UTF-8
2023-01-07 19:36:59,021 fail2ban.filtersystemd [43533]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-01-07 19:36:59,022 fail2ban.jail [43533]: INFO Jail 'sshd' started
2023-01-07 19:36:59,023 fail2ban.jail [43533]: INFO Jail 'selinux-ssh' started
2023-01-07 19:36:59,024 fail2ban.jail [43533]: INFO Jail 'sshd-ddos' started

```

Рисунок 3

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

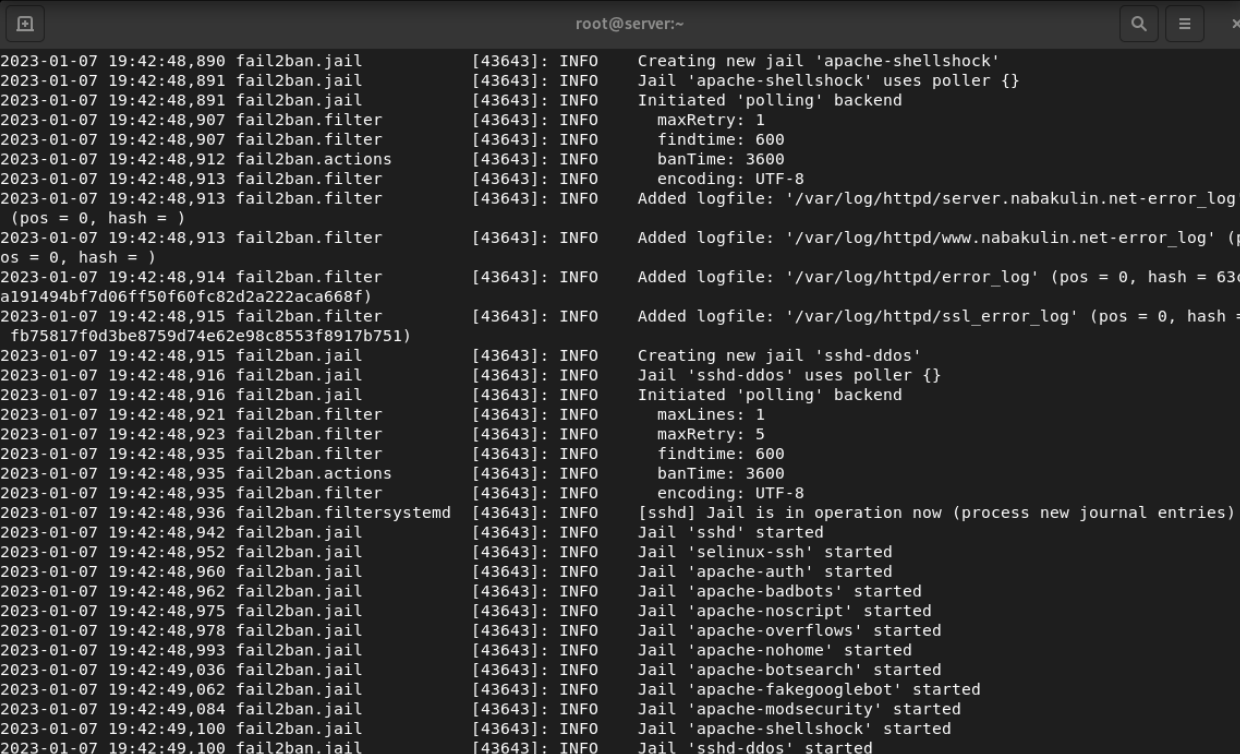
```
#
# HTTP servers
#
[apache-auth]
enabled = true
[apache-badbots]
enabled = true
[apache-noscript]
enabled = true
[apache-overflows]
enabled = true
[apache-nohome]
enabled = true
[apache-botsearch]
enabled = true
[apache-fakegooglebot]
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true
```

Рисунок 4

1.9. Перезапустите fail2ban

1.10. Посмотрите журнал событий

```
[root@server.nabakulin.net vagrant]# systemctl restart fail2ban
[root@server.nabakulin.net vagrant]#
```



```
2023-01-07 19:42:48,890 fail2ban.jail [43643]: INFO Creating new jail 'apache-shellshock'
2023-01-07 19:42:48,891 fail2ban.jail [43643]: INFO Jail 'apache-shellshock' uses poller {}
2023-01-07 19:42:48,891 fail2ban.jail [43643]: INFO Initiated 'polling' backend
2023-01-07 19:42:48,907 fail2ban.filter [43643]: INFO maxRetry: 1
2023-01-07 19:42:48,907 fail2ban.filter [43643]: INFO findtime: 600
2023-01-07 19:42:48,912 fail2ban.actions [43643]: INFO banTime: 3600
2023-01-07 19:42:48,913 fail2ban.filter [43643]: INFO encoding: UTF-8
2023-01-07 19:42:48,913 fail2ban.filter [43643]: INFO Added logfile: '/var/log/httpd/server.nabakulin.net-error_log'
(pos = 0, hash = )
2023-01-07 19:42:48,913 fail2ban.filter [43643]: INFO Added logfile: '/var/log/httpd/www.nabakulin.net-error_log' (p
os = 0, hash = )
2023-01-07 19:42:48,914 fail2ban.filter [43643]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 63c
a191494bf7d06ff50f60fc82d2a222aca668f)
2023-01-07 19:42:48,915 fail2ban.filter [43643]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash =
fb75817f0d3be8759d74e62e98c8553f8917b751)
2023-01-07 19:42:48,915 fail2ban.jail [43643]: INFO Creating new jail 'sshd-ddos'
2023-01-07 19:42:48,916 fail2ban.jail [43643]: INFO Jail 'sshd-ddos' uses poller {}
2023-01-07 19:42:48,916 fail2ban.jail [43643]: INFO Initiated 'polling' backend
2023-01-07 19:42:48,921 fail2ban.filter [43643]: INFO maxLines: 1
2023-01-07 19:42:48,923 fail2ban.filter [43643]: INFO maxRetry: 5
2023-01-07 19:42:48,935 fail2ban.filter [43643]: INFO findtime: 600
2023-01-07 19:42:48,935 fail2ban.actions [43643]: INFO banTime: 3600
2023-01-07 19:42:48,935 fail2ban.filter [43643]: INFO encoding: UTF-8
2023-01-07 19:42:48,936 fail2ban.filtersystemd [43643]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-01-07 19:42:48,942 fail2ban.jail [43643]: INFO Jail 'sshd' started
2023-01-07 19:42:48,952 fail2ban.jail [43643]: INFO Jail 'selinux-ssh' started
2023-01-07 19:42:48,960 fail2ban.jail [43643]: INFO Jail 'apache-auth' started
2023-01-07 19:42:48,962 fail2ban.jail [43643]: INFO Jail 'apache-badbots' started
2023-01-07 19:42:48,975 fail2ban.jail [43643]: INFO Jail 'apache-noscript' started
2023-01-07 19:42:48,978 fail2ban.jail [43643]: INFO Jail 'apache-overflows' started
2023-01-07 19:42:48,993 fail2ban.jail [43643]: INFO Jail 'apache-nohome' started
2023-01-07 19:42:49,036 fail2ban.jail [43643]: INFO Jail 'apache-botsearch' started
2023-01-07 19:42:49,062 fail2ban.jail [43643]: INFO Jail 'apache-fakegooglebot' started
2023-01-07 19:42:49,084 fail2ban.jail [43643]: INFO Jail 'apache-modsecurity' started
2023-01-07 19:42:49,100 fail2ban.jail [43643]: INFO Jail 'apache-shellshock' started
2023-01-07 19:42:49,100 fail2ban.jail [43643]: INFO Jail 'sshd-ddos' started
```

Рисунок 5

1.11. В файле /etc/fail2ban/jail.d/customisation.local включите защиту почты

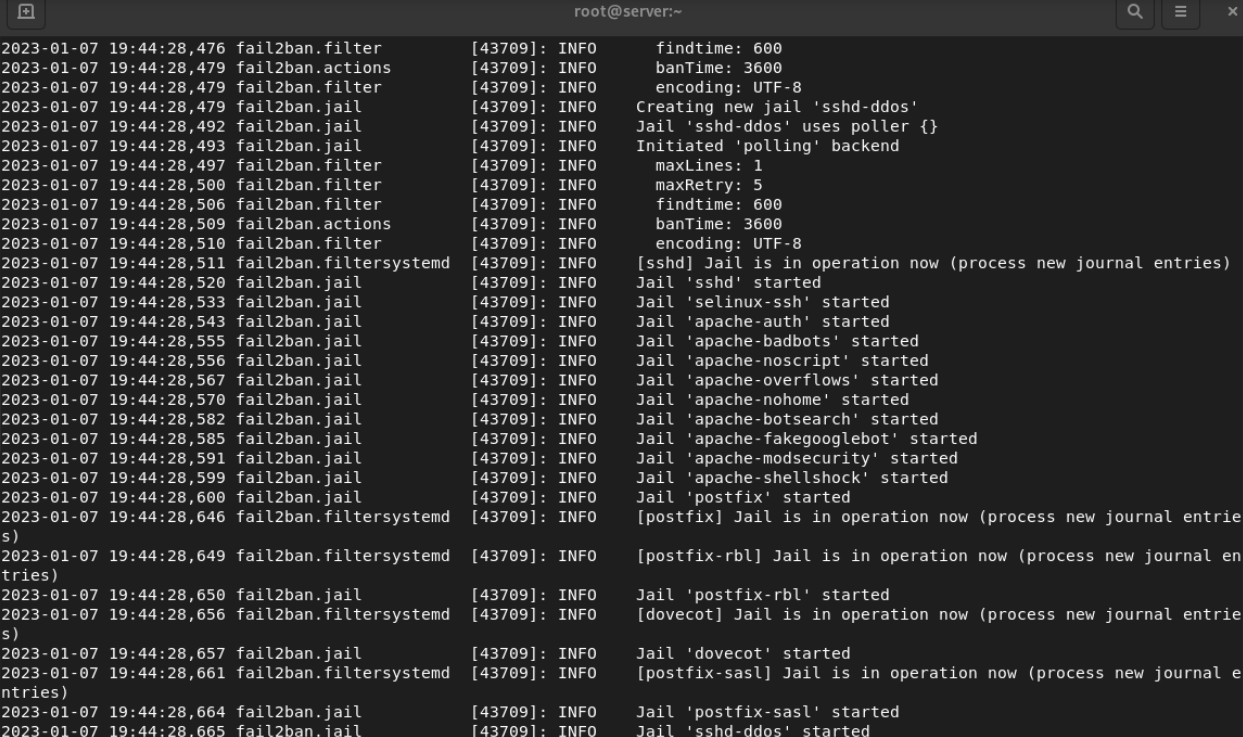
```
#
# Mail servers
#
[postfix]
enabled = true
[postfix-rbl]
enabled = true
[dovecot]
enabled = true
[postfix-sasl]
enabled = true
```

Рисунок 6

1.12. Перезапустите fail2ban

1.13. Посмотрите журнал событий

```
[root@server.nabakulin.net vagrant]# systemctl restart fail2ban
[root@server.nabakulin.net vagrant]#
```



```
2023-01-07 19:44:28,476 fail2ban.filter [43709]: INFO findtime: 600
2023-01-07 19:44:28,479 fail2ban.actions [43709]: INFO banTime: 3600
2023-01-07 19:44:28,479 fail2ban.filter [43709]: INFO encoding: UTF-8
2023-01-07 19:44:28,479 fail2ban.jail [43709]: INFO Creating new jail 'sshd-ddos'
2023-01-07 19:44:28,492 fail2ban.jail [43709]: INFO Jail 'sshd-ddos' uses poller {}
2023-01-07 19:44:28,493 fail2ban.jail [43709]: INFO Initiated 'polling' backend
2023-01-07 19:44:28,497 fail2ban.filter [43709]: INFO maxLines: 1
2023-01-07 19:44:28,500 fail2ban.filter [43709]: INFO maxRetry: 5
2023-01-07 19:44:28,506 fail2ban.filter [43709]: INFO findtime: 600
2023-01-07 19:44:28,509 fail2ban.actions [43709]: INFO banTime: 3600
2023-01-07 19:44:28,510 fail2ban.filter [43709]: INFO encoding: UTF-8
2023-01-07 19:44:28,511 fail2ban.filtersystemd [43709]: INFO [sshd] Jail is in operation now (process new journal entries)
2023-01-07 19:44:28,520 fail2ban.jail [43709]: INFO Jail 'sshd' started
2023-01-07 19:44:28,533 fail2ban.jail [43709]: INFO Jail 'selinux-ssh' started
2023-01-07 19:44:28,543 fail2ban.jail [43709]: INFO Jail 'apache-auth' started
2023-01-07 19:44:28,555 fail2ban.jail [43709]: INFO Jail 'apache-badbots' started
2023-01-07 19:44:28,556 fail2ban.jail [43709]: INFO Jail 'apache-noscript' started
2023-01-07 19:44:28,567 fail2ban.jail [43709]: INFO Jail 'apache-overflows' started
2023-01-07 19:44:28,570 fail2ban.jail [43709]: INFO Jail 'apache-nohome' started
2023-01-07 19:44:28,582 fail2ban.jail [43709]: INFO Jail 'apache-botsearch' started
2023-01-07 19:44:28,585 fail2ban.jail [43709]: INFO Jail 'apache-fakegooglebot' started
2023-01-07 19:44:28,591 fail2ban.jail [43709]: INFO Jail 'apache-modsecurity' started
2023-01-07 19:44:28,599 fail2ban.jail [43709]: INFO Jail 'apache-shellshock' started
2023-01-07 19:44:28,600 fail2ban.jail [43709]: INFO Jail 'postfix' started
2023-01-07 19:44:28,646 fail2ban.filtersystemd [43709]: INFO [postfix] Jail is in operation now (process new journal entries)
2023-01-07 19:44:28,649 fail2ban.filtersystemd [43709]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2023-01-07 19:44:28,650 fail2ban.jail [43709]: INFO Jail 'postfix-rbl' started
2023-01-07 19:44:28,656 fail2ban.filtersystemd [43709]: INFO [dovecot] Jail is in operation now (process new journal entries)
2023-01-07 19:44:28,657 fail2ban.jail [43709]: INFO Jail 'dovecot' started
2023-01-07 19:44:28,661 fail2ban.filtersystemd [43709]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2023-01-07 19:44:28,664 fail2ban.jail [43709]: INFO Jail 'postfix-sasl' started
2023-01-07 19:44:28,665 fail2ban.jail [43709]: INFO Jail 'sshd-ddos' started
```

Рисунок 7

2.

2.1. На сервере посмотрите статус fail2ban

2.2. Посмотрите статус защиты SSH в fail2ban

2.3. Установите максимальное количество ошибок для SSH, равное 2

2.4. С клиента попытайтесь зайти по SSH на сервер с неправильным паролем

2.5. На сервере посмотрите статус защиты SSH

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

[root@server.nabakulin.net vagrant]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 1
|   |- Total failed: 3
|   `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
    |- Currently banned: 1
    |- Total banned: 1
    `-- Banned IP list: 192.168.1.30
[root@server.nabakulin.net vagrant]#

root@server:~#
2023-01-07 19:46:30,390 fail2ban.filter [43709]: INFO [sshd] Found 192.168.1.30 - 2023-01-07 19:46:29
2023-01-07 19:46:39,244 fail2ban.filter [43709]: INFO [sshd] Found 192.168.1.30 - 2023-01-07 19:46:37
2023-01-07 19:46:39,605 fail2ban.actions [43709]: NOTICE [sshd] Ban 192.168.1.30
2023-01-07 19:46:48,263 fail2ban.filter [43709]: INFO [sshd] Found 192.168.1.30 - 2023-01-07 19:46:47
```

Рисунок 8

2.6. Разблокируйте IP-адрес клиента

2.7. Вновь посмотрите статус защиты SSH

```
[root@server.nabakulin.net vagrant]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.nabakulin.net vagrant]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 1
|   |- Total failed: 3
|   `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
    |- Currently banned: 0
    |- Total banned: 1
    `-- Banned IP list:
[root@server.nabakulin.net vagrant]#

root@server:~#
2023-01-07 19:46:48,263 fail2ban.filter [43709]: INFO [sshd] Found 192.168.1.30 - 2023-01-07 19:46:47
2023-01-07 19:48:57,203 fail2ban.actions [43709]: NOTICE [sshd] Unban 192.168.1.30
```

Рисунок 9

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

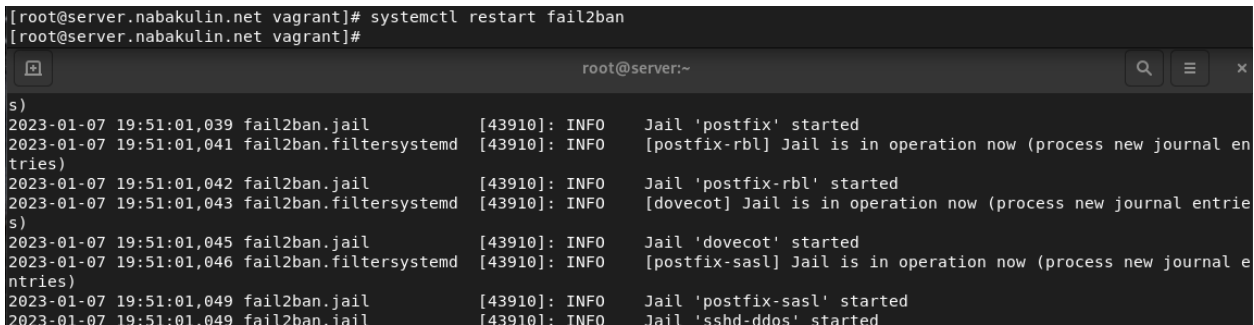
```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.30
#
# SSH servers
#
```

Рисунок 10

2.9. Перезапустите fail2ban

2.10. Посмотрите журнал событий

```
[root@server.nabakulin.net vagrant]# systemctl restart fail2ban
[root@server.nabakulin.net vagrant]#
```

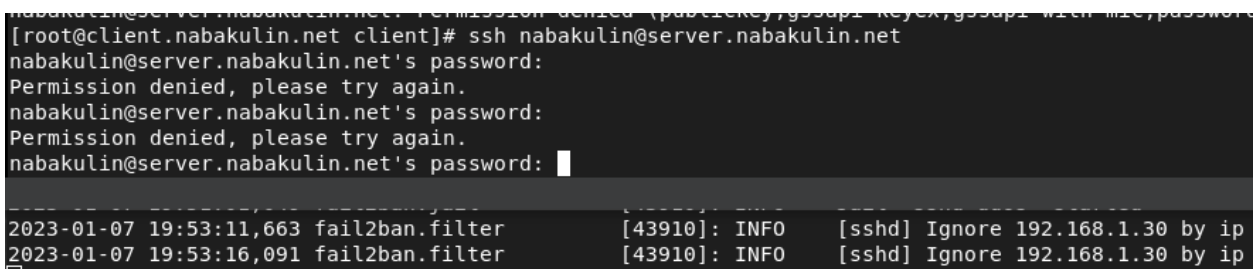


```
2023-01-07 19:51:01,039 fail2ban.jail [43910]: INFO Jail 'postfix' started
2023-01-07 19:51:01,041 fail2ban.filtersystemd [43910]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2023-01-07 19:51:01,042 fail2ban.jail [43910]: INFO Jail 'postfix-rbl' started
2023-01-07 19:51:01,043 fail2ban.filtersystemd [43910]: INFO [dovecot] Jail is in operation now (process new journal entries)
2023-01-07 19:51:01,045 fail2ban.jail [43910]: INFO Jail 'dovecot' started
2023-01-07 19:51:01,046 fail2ban.filtersystemd [43910]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2023-01-07 19:51:01,049 fail2ban.jail [43910]: INFO Jail 'postfix-sasl' started
2023-01-07 19:51:01,049 fail2ban.jail [43910]: INFO Jail 'sshd-ddos' started
```

Рисунок 11

- 2.11. Вновь попытайтесь войти с клиента на сервер с неправильным паролем и посмотрите статус защиты SSH

```
nabakulin@server.nabakulin.net: Permission denied (publickey,gssapi-keyex,gssapi-witn-ncac,passwor
[root@client.nabakulin.net client]# ssh nabakulin@server.nabakulin.net
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password: █
```



```
2023-01-07 19:53:11,663 fail2ban.filter [43910]: INFO [sshd] Ignore 192.168.1.30 by ip
2023-01-07 19:53:16,091 fail2ban.filter [43910]: INFO [sshd] Ignore 192.168.1.30 by ip
```

Рисунок 12

3.

- 3.1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог protect, в который поместите в соответствующие подкаталоги конфигурационные файлы

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

Рисунок 13

- 3.2. В каталоге /vagrant/provision/server создайте исполняемый файл 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

3.3. 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"
```

Рисунок 15

Контрольные вопросы

1. Поясните принцип работы Fail2ban.

Данное программное средство 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?

Локального

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Добавить action в конфигурацию jail

4. Как получить список действующих правил Fail2ban?

fail2ban-client status

5. Как получить статистику заблокированных Fail2ban адресов?

fail2ban-client banned

6. Как разблокировать IP-адрес?

fail2ban-client set <jail> unbanip <ip>