

Лабораторная работа № 16

Базовая защита от атак типа «brute force»

Демидова Екатерина Алексеевна

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Защита с помощью Fail2ban	6
3.2	Проверка работы Fail2ban	13
3.3	Внесение изменений в настройки внутреннего окружения вирту- альных машины	17
4	Контрольные вопросы	19
5	Выводы	22

Список иллюстраций

3.1	Запуск просмотра журнала событий fail2ban	7
3.2	Добавление времени блокировки и включение защиты SSH customisation.local	8
3.3	Просмотр журнала событий fail2ban	9
3.4	Включение защиты HTTP в файле customisation.local	10
3.5	Просмотр журнала событий fail2ban	11
3.6	Включение защиты почты в файле customisation.local	12
3.7	Просмотр журнала событий fail2ban	13
3.8	Просмотр статуса fail2ban, защиты SSH и установка количества ошибок для SSH	14
3.9	Попытки соединения по SSH с сервером с неправильным паролем	14
3.10	Проверка блокировки клиента на сервере	14
3.11	Снятие блокировки с клиента	15
3.12	Добавление в конфигурационный файл игнорирования адреса кли- ента	15
3.13	Просмотр журнала событий fail2ban	16
3.14	Просмотр статуса защиты SSH после подключение к серверу с кли- ента по SSH с неправильным паролем	17
3.15	Скрипта файла /vagrant/provision/server/protect.sh	18

1 Цель работы

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

2 Задание

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.

3 Выполнение лабораторной работы

3.1 Защита с помощью Fail2ban

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом:

```
cd /var/tmp/eademidova/vagrant
```

Затем запустим виртуальную машину server:

```
make server-up
```

На сервере установите fail2ban:

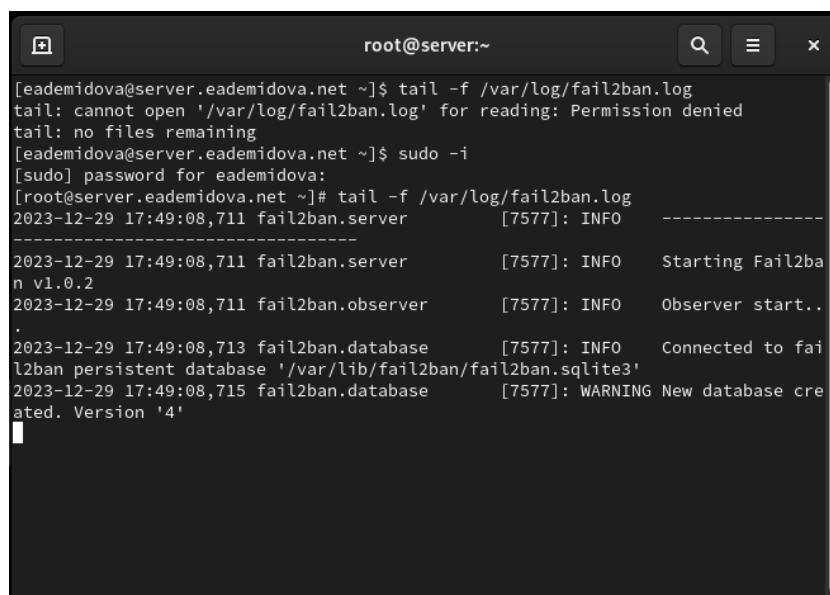
```
dnf -y install fail2ban
```

Запустим сервер fail2ban:

```
systemctl start fail2ban
```

```
systemctl enable fail2ban
```

В дополнительном терминале запустим просмотр журнала событий fail2ban(рис. 3.1):



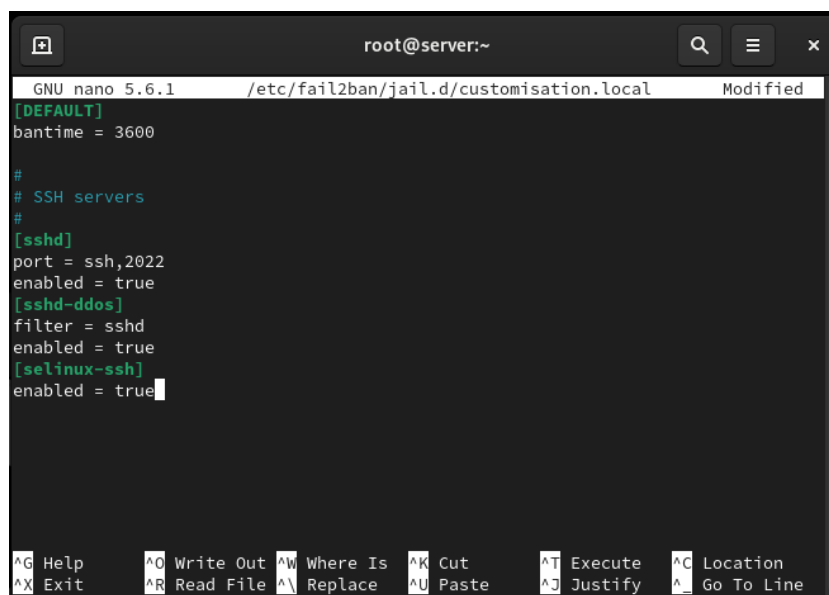
```
root@server:~  
[eademidova@server.eademidova.net ~]$ tail -f /var/log/fail2ban.log  
tail: cannot open '/var/log/fail2ban.log' for reading: Permission denied  
tail: no files remaining  
[eademidova@server.eademidova.net ~]$ sudo -i  
[sudo] password for eademidova:  
[root@server.eademidova.net ~]# tail -f /var/log/fail2ban.log  
2023-12-29 17:49:08,711 fail2ban.server [7577]: INFO -----  
2023-12-29 17:49:08,711 fail2ban.server [7577]: INFO Starting Fail2ban v1.0.2  
2023-12-29 17:49:08,711 fail2ban.observer [7577]: INFO Observer start..  
2023-12-29 17:49:08,713 fail2ban.database [7577]: INFO Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'  
2023-12-29 17:49:08,715 fail2ban.database [7577]: WARNING New database created. Version '4'
```

Рис. 3.1: Запуск просмотра журнала событий fail2ban

Создадим файл с локальной конфигурацией fail2ban:

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

И в этом файле `etc/fail2ban/jail.d/customisation.local` зададим время блокирования на 1 час (время задаётся в секундах) и включим защиту SSH(рис. 3.2):



```
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified
[DEFAULT]
bantime = 3600

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

Рис. 3.2: Добавление времени блокировки и включение защиты SSH customisation.local

Перезапустим сервер fail2ban:

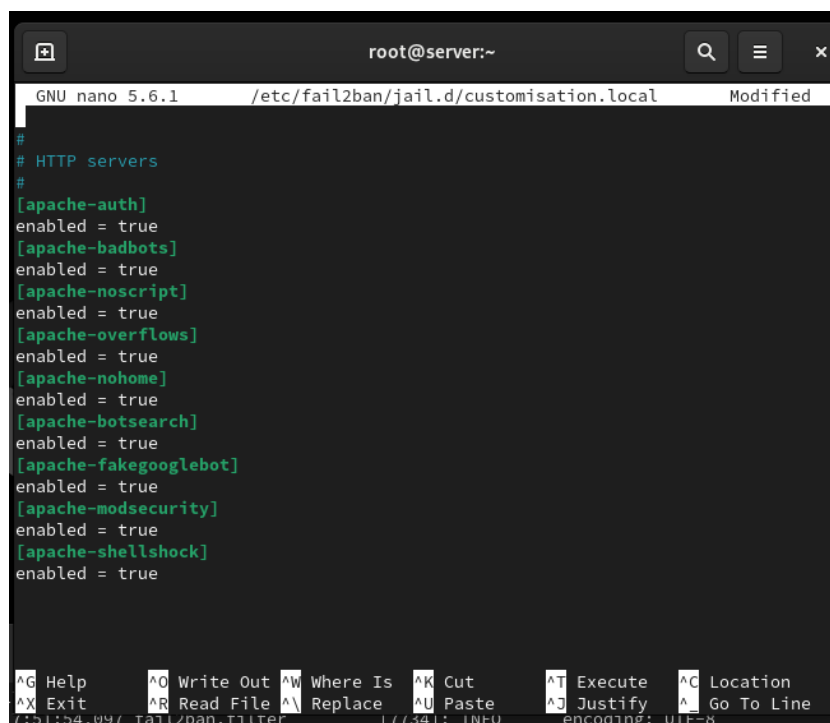
```
systemctl restart fail2ban
```

И посмотрим журнал событий(3.3):


```
root@server:~  
[root@server.eademidova.net ~]# tail -f /var/log/fail2ban.log  
2023-12-29 17:49:08,711 fail2ban.server [7577]: INFO -----  
2023-12-29 17:49:08,711 fail2ban.server [7577]: INFO Starting Fail2ban v1.0.2  
2023-12-29 17:49:08,711 fail2ban.observer [7577]: INFO Observer start...  
2023-12-29 17:49:08,713 fail2ban.database [7577]: INFO Connected to fail2ban persistent database '/var/lib  
fail2ban/fail2ban.sqlite3'  
2023-12-29 17:49:08,715 fail2ban.database [7577]: WARNING New database created. Version '4'  
2023-12-29 17:51:53,882 fail2ban.server [7577]: INFO Shutdown in progress...  
2023-12-29 17:51:53,883 fail2ban.observer [7577]: INFO Observer stop ... try to end queue 5 seconds  
2023-12-29 17:51:53,893 fail2ban.observer [7577]: INFO Observer stopped, 0 events remaining.  
2023-12-29 17:51:53,944 fail2ban.server [7577]: INFO Stopping all jails  
2023-12-29 17:51:53,945 fail2ban.database [7577]: INFO Connection to database closed.  
2023-12-29 17:51:53,945 fail2ban.server [7577]: INFO Exiting Fail2ban  
2023-12-29 17:51:54,061 fail2ban.server [7734]: INFO -----  
2023-12-29 17:51:54,061 fail2ban.server [7734]: INFO Starting Fail2ban v1.0.2  
2023-12-29 17:51:54,062 fail2ban.observer [7734]: INFO Observer start...  
2023-12-29 17:51:54,063 fail2ban.database [7734]: INFO Connected to fail2ban persistent database '/var/lib  
fail2ban/fail2ban.sqlite3'  
2023-12-29 17:51:54,064 fail2ban.jail [7734]: INFO Creating new jail 'sshd'  
2023-12-29 17:51:54,077 fail2ban.jail [7734]: INFO Jail 'sshd' uses systemd {}  
2023-12-29 17:51:54,077 fail2ban.jail [7734]: INFO Initiated 'systemd' backend  
2023-12-29 17:51:54,078 fail2ban.filter [7734]: INFO maxLines: 1  
2023-12-29 17:51:54,089 fail2ban.filtersystemd [7734]: INFO [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd'  
2023-12-29 17:51:54,097 fail2ban.filter [7734]: INFO maxRetry: 5  
2023-12-29 17:51:54,097 fail2ban.filter [7734]: INFO findtime: 600  
2023-12-29 17:51:54,097 fail2ban.actions [7734]: INFO banTime: 3600  
2023-12-29 17:51:54,097 fail2ban.filter [7734]: INFO encoding: UTF-8  
2023-12-29 17:51:54,097 fail2ban.jail [7734]: INFO Creating new jail 'selinux-ssh'  
2023-12-29 17:51:54,100 fail2ban.jail [7734]: INFO Jail 'selinux-ssh' uses poller {}  
2023-12-29 17:51:54,101 fail2ban.jail [7734]: INFO Initiated 'polling' backend  
2023-12-29 17:51:54,102 fail2ban.datedetector [7734]: INFO date pattern '': 'Epoch'  
2023-12-29 17:51:54,102 fail2ban.filter [7734]: INFO maxRetry: 5  
2023-12-29 17:51:54,102 fail2ban.filter [7734]: INFO findtime: 600  
2023-12-29 17:51:54,102 fail2ban.actions [7734]: INFO banTime: 3600  
2023-12-29 17:51:54,102 fail2ban.filter [7734]: INFO encoding: UTF-8  
2023-12-29 17:51:54,103 fail2ban.filter [7734]: INFO Added logfile: '/var/log/audit/audit.log' (pos = 0,  
sh = 05970ce754972f6219fd38cd637d7a297084cfd)  
2023-12-29 17:51:54,103 fail2ban.jail [7734]: INFO Creating new jail 'sshd-ddos'  
2023-12-29 17:51:54,104 fail2ban.jail [7734]: INFO Jail 'sshd-ddos' uses poller {}  
2023-12-29 17:51:54,104 fail2ban.jail [7734]: INFO Initiated 'polling' backend  
2023-12-29 17:51:54,104 fail2ban.filter [7734]: INFO maxLines: 1  
2023-12-29 17:51:54,105 fail2ban.filter [7734]: INFO maxRetry: 5  
2023-12-29 17:51:54,105 fail2ban.filter [7734]: INFO findtime: 600  
2023-12-29 17:51:54,105 fail2ban.actions [7734]: INFO banTime: 3600  
2023-12-29 17:51:54,105 fail2ban.filter [7734]: INFO encoding: UTF-8  
2023-12-29 17:51:54,112 fail2ban.filtersystemd [7734]: INFO [sshd] Jail is in operation now (process new journa  
ntries)  
2023-12-29 17:51:54,113 fail2ban.jail [7734]: INFO Jail 'sshd' started  
2023-12-29 17:51:54,114 fail2ban.jail [7734]: INFO Jail 'selinux-ssh' started  
2023-12-29 17:51:54,114 fail2ban.jail [7734]: INFO Jail 'sshd-ddos' started
```

Рис. 3.3: Просмотр журнала событий fail2ban

В файле /etc/fail2ban/jail.d/customisation.local включим защиту HTTP(3.4):



```
root@server:~
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified
#
# 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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
(151154,047 Tail2ban.Filter | / / 34 | INFO encoding: UTF-8
```

Рис. 3.4: Включение защиты HTTP в файле customisation.local

Перезапустим сервер fail2ban:

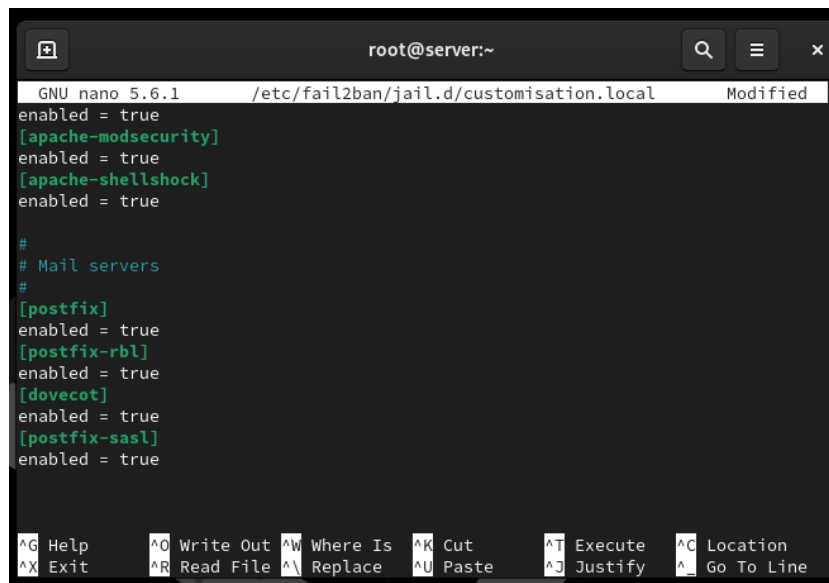
```
systemctl restart fail2ban
```

И посмотрим журнал событий(3.5):

```
root@server:~  
2023-12-29 17:53:40,577 fail2ban.jail [7775]: INFO Jail 'apache-modsecurity' uses poller {}  
2023-12-29 17:53:40,577 fail2ban.jail [7775]: INFO Initiated 'polling' backend  
2023-12-29 17:53:40,578 fail2ban.filter [7775]: INFO maxRetry: 2  
2023-12-29 17:53:40,578 fail2ban.filter [7775]: INFO findTime: 600  
2023-12-29 17:53:40,579 fail2ban.actions [7775]: INFO banTime: 3600  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO encoding: UTF-8  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/server.eadimidova.ne  
rror_log' (pos = 0, hash = )  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0,  
sh = 0dd417186aac038b0221688ec9cca9f0ee4a3757)  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos  
, hash = 3837407b2265d724d1c6cfb9943fdce67f980517)  
2023-12-29 17:53:40,579 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/www.eadimidova.net-e  
r_log' (pos = 0, hash = 4451f17b3b874cbb36bae5e8792cd99583b50772)  
2023-12-29 17:53:40,579 fail2ban.jail [7775]: INFO Creating new jail 'apache-shellshock'  
2023-12-29 17:53:40,580 fail2ban.jail [7775]: INFO Jail 'apache-shellshock' uses poller {}  
2023-12-29 17:53:40,580 fail2ban.jail [7775]: INFO Initiated 'polling' backend  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO maxRetry: 1  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO findTime: 600  
2023-12-29 17:53:40,581 fail2ban.actions [7775]: INFO banTime: 3600  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO encoding: UTF-8  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/server.eadimidova.ne  
rror_log' (pos = 0, hash = )  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0,  
sh = 0dd417186aac038b0221688ec9cca9f0ee4a3757)  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos  
, hash = 3837407b2265d724d1c6cfb9943fdce67f980517)  
2023-12-29 17:53:40,581 fail2ban.filter [7775]: INFO Added logfile: '/var/log/httpd/www.eadimidova.net-e  
r_log' (pos = 0, hash = 4451f17b3b874cbb36bae5e8792cd99583b50772)  
2023-12-29 17:53:40,582 fail2ban.jail [7775]: INFO Creating new jail 'sshd-ddos'  
2023-12-29 17:53:40,582 fail2ban.jail [7775]: INFO Jail 'sshd-ddos' uses poller {}  
2023-12-29 17:53:40,582 fail2ban.jail [7775]: INFO Initiated 'polling' backend  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO maxLines: 1  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO maxRetry: 5  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO findTime: 600  
2023-12-29 17:53:40,583 fail2ban.actions [7775]: INFO banTime: 3600  
2023-12-29 17:53:40,583 fail2ban.filter [7775]: INFO encoding: UTF-8  
2023-12-29 17:53:40,584 fail2ban.filtersystemd [7775]: INFO [sshd] Jail is in operation now (process new journa  
l entries)  
2023-12-29 17:53:40,584 fail2ban.jail [7775]: INFO Jail 'sshd' started  
2023-12-29 17:53:40,585 fail2ban.jail [7775]: INFO Jail 'selinux-ssh' started  
2023-12-29 17:53:40,587 fail2ban.jail [7775]: INFO Jail 'apache-auth' started  
2023-12-29 17:53:40,588 fail2ban.jail [7775]: INFO Jail 'apache-badbots' started  
2023-12-29 17:53:40,589 fail2ban.jail [7775]: INFO Jail 'apache-noscript' started  
2023-12-29 17:53:40,592 fail2ban.jail [7775]: INFO Jail 'apache-overflows' started  
2023-12-29 17:53:40,603 fail2ban.jail [7775]: INFO Jail 'apache-nohome' started  
2023-12-29 17:53:40,604 fail2ban.jail [7775]: INFO Jail 'apache-botsearch' started  
2023-12-29 17:53:40,605 fail2ban.jail [7775]: INFO Jail 'apache-fakegooglebot' started  
2023-12-29 17:53:40,606 fail2ban.jail [7775]: INFO Jail 'apache-modsecurity' started  
2023-12-29 17:53:40,607 fail2ban.jail [7775]: INFO Jail 'apache-shellshock' started  
2023-12-29 17:53:40,607 fail2ban.jail [7775]: INFO Jail 'sshd-ddos' started
```

Рис. 3.5: Просмотр журнала событий fail2ban

В файле /etc/fail2ban/jail.d/customisation.local включим защиту почты(3.6):



```
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local Modified
enabled = true
[apache-modsecurity]
enabled = true
[apache-shellshock]
enabled = true

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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

Рис. 3.6: Включение защиты почты в файле customisation.local

Перезапустим сервер fail2ban:

```
systemctl restart fail2ban
```

И посмотрим журнал событий(3.7):

```
root@server:~  
2023-12-29 17:55:04,289 fail2ban.jail [7834]: INFO Initiated 'systemd' backend  
2023-12-29 17:55:04,294 fail2ban.datedetector [7834]: INFO date pattern '': {'^LN-BEG}TAI64N'  
2023-12-29 17:55:04,294 fail2ban.filterssystemd [7834]: INFO [dovecot] Added journal match for: '_SYSTEMD_UNIT=d  
ot.service'  
2023-12-29 17:55:04,294 fail2ban.filter [7834]: INFO maxRetry: 5  
2023-12-29 17:55:04,294 fail2ban.filter [7834]: INFO findtime: 600  
2023-12-29 17:55:04,294 fail2ban.actions [7834]: INFO banTime: 3600  
2023-12-29 17:55:04,294 fail2ban.filter [7834]: INFO encoding: UTF-8  
2023-12-29 17:55:04,295 fail2ban.jail [7834]: INFO Creating new jail 'postfix-sasl'  
2023-12-29 17:55:04,295 fail2ban.jail [7834]: INFO Jail 'postfix-sasl' uses systemd {}  
2023-12-29 17:55:04,295 fail2ban.jail [7834]: INFO Initiated 'systemd' backend  
2023-12-29 17:55:04,296 fail2ban.filterssystemd [7834]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_U  
postfix.service'  
2023-12-29 17:55:04,296 fail2ban.filter [7834]: INFO maxRetry: 5  
2023-12-29 17:55:04,296 fail2ban.filter [7834]: INFO findtime: 600  
2023-12-29 17:55:04,297 fail2ban.actions [7834]: INFO banTime: 3600  
2023-12-29 17:55:04,297 fail2ban.filter [7834]: INFO encoding: UTF-8  
2023-12-29 17:55:04,297 fail2ban.jail [7834]: INFO Creating new jail 'sshd-ddos'  
2023-12-29 17:55:04,297 fail2ban.jail [7834]: INFO Jail 'sshd-ddos' uses poller {}  
2023-12-29 17:55:04,298 fail2ban.jail [7834]: INFO Initiated 'polling' backend  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO maxlines: 1  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO maxRetry: 5  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO findtime: 600  
2023-12-29 17:55:04,300 fail2ban.actions [7834]: INFO banTime: 3600  
2023-12-29 17:55:04,300 fail2ban.filter [7834]: INFO encoding: UTF-8  
2023-12-29 17:55:04,301 fail2ban.filterssystemd [7834]: INFO [sshd] Jail is in operation now (process new journa  
l entries)  
2023-12-29 17:55:04,302 fail2ban.jail [7834]: INFO Jail 'sshd' started  
2023-12-29 17:55:04,303 fail2ban.jail [7834]: INFO Jail 'selinux-ssh' started  
2023-12-29 17:55:04,303 fail2ban.jail [7834]: INFO Jail 'apache-auth' started  
2023-12-29 17:55:04,304 fail2ban.jail [7834]: INFO Jail 'apache-badbots' started  
2023-12-29 17:55:04,304 fail2ban.jail [7834]: INFO Jail 'apache-noscript' started  
2023-12-29 17:55:04,305 fail2ban.jail [7834]: INFO Jail 'apache-overflows' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'apache-nohome' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'apache-botsearch' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'apache-fakegooglebot' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'apache-modsecurity' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'apache-shellshock' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'postfix' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'postfix-rbl' started  
2023-12-29 17:55:04,306 fail2ban.filterssystemd [7834]: INFO [postfix] Jail is in operation now (process new jou  
l entries)  
2023-12-29 17:55:04,306 fail2ban.filterssystemd [7834]: INFO [postfix-rbl] Jail is in operation now (process new  
journal entries)  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'dovecot' started  
2023-12-29 17:55:04,306 fail2ban.filterssystemd [7834]: INFO [dovecot] Jail is in operation now (process new jou  
l entries)  
2023-12-29 17:55:04,306 fail2ban.filterssystemd [7834]: INFO [postfix-sasl] Jail is in operation now (process ne  
w journal entries)  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'postfix-sasl' started  
2023-12-29 17:55:04,306 fail2ban.jail [7834]: INFO Jail 'sshd-ddos' started
```

Рис. 3.7: Просмотр журнала событий fail2ban

3.2 Проверка работы Fail2ban

На сервере посмотрим статус fail2ban и статус защиты SSH в fail2ban, а затем установим максимальное количество ошибок для SSH, равное 2(3.8):

```

[root@server.eademidova.net ~]# systemctl restart fail2ban
[root@server.eademidova.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.eademidova.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
|- Actions
| |- Currently banned: 0
| |- Total banned:    0
| |- Banned IP list:
[root@server.eademidova.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.eademidova.net ~]#

```

Рис. 3.8: Просмотр статуса fail2ban, защиты SSH и установка количества ошибок для SSH

С клиента попытайтесь зайти по SSH на сервер с неправильным паролем(3.9):

```

[eademidova@client.eademidova.net ~]$ ssh eademidova@server.eademidova.net
eademidova@server.eademidova.net's password:
Permission denied, please try again.
eademidova@server.eademidova.net's password:
Permission denied, please try again.
eademidova@server.eademidova.net's password: 

```

Рис. 3.9: Попытки соединения по SSH с сервером с неправильным паролем

На сервере посмотрите статус защиты SSH, убедившись, что произошла блокировка адреса клиента(3.10):

```

[root@server.eademidova.net ~]# 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.eademidova.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:    2
| |- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
|- Actions
| |- Currently banned: 1
| |- Total banned:    1
| |- Banned IP list:  192.168.1.30
[root@server.eademidova.net ~]#

```

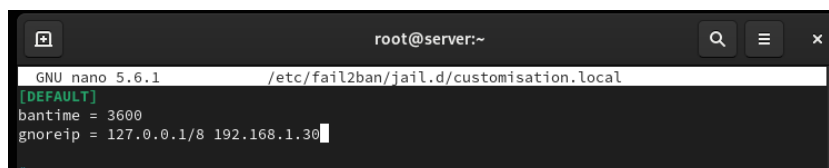
Рис. 3.10: Проверка блокировки клиента на сервере

Разблокируем IP-адрес клиента и вновь посмотрим статус защиты SSH, убедившись, что блокировка с клиента снята(рис. 3.11):

```
- Banned IP list: 192.168.1.30
[root@server.eademidova.net ~]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.eademidova.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 2
| |- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
- Actions
| |- Currently banned: 0
| |- Total banned: 1
| - Banned IP list:
[root@server.eademidova.net ~]#
```

Рис. 3.11: Снятие блокировки с клиента

На сервере внесем изменение в конфигурационный файл `/etc/fail2ban/jail.d/customisation.local`, добавив в раздел по умолчанию игнорирование адреса клиента(рис. 3.12):



```
GNU nano 5.6.1 /etc/fail2ban/jail.d/customisation.local
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.30
#
```

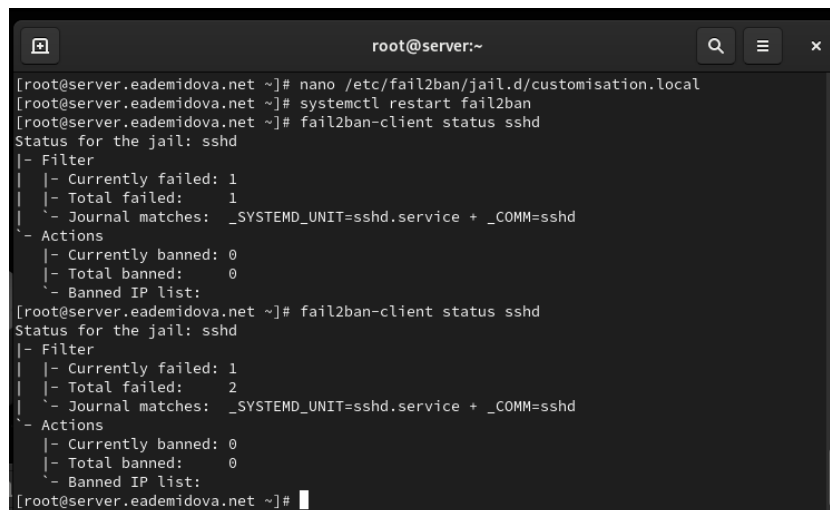
Рис. 3.12: Добавление в конфигурационный файл игнорирования адреса клиента

Перезапустим fail2ban и посмотрим журнал событий(3.13)

```
root@server:~
2023-12-29 18:08:22,009 fail2ban.jail [8234]: INFO Initiated 'systemd' backend
2023-12-29 18:08:22,019 fail2ban.datedetector [8234]: INFO date pattern '': {'^LN-BEG}TAI64N'
2023-12-29 18:08:22,020 fail2ban.filtersystemd [8234]: INFO [dovecot] Added journal match for: '_SYSTEMD_UNIT=
cot.service'
2023-12-29 18:08:22,020 fail2ban.filter [8234]: INFO maxRetry: 5
2023-12-29 18:08:22,020 fail2ban.filter [8234]: INFO findtime: 600
2023-12-29 18:08:22,020 fail2ban.actions [8234]: INFO banTime: 3600
2023-12-29 18:08:22,020 fail2ban.filter [8234]: INFO encoding: UTF-8
2023-12-29 18:08:22,021 fail2ban.jail [8234]: INFO Creating new jail 'postfix-sasl'
2023-12-29 18:08:22,021 fail2ban.jail [8234]: INFO Jail 'postfix-sasl' uses systemd {}
2023-12-29 18:08:22,021 fail2ban.jail [8234]: INFO Initiated 'systemd' backend
2023-12-29 18:08:22,023 fail2ban.filtersystemd [8234]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_
postfix.service'
2023-12-29 18:08:22,023 fail2ban.filter [8234]: INFO maxRetry: 5
2023-12-29 18:08:22,024 fail2ban.filter [8234]: INFO findtime: 600
2023-12-29 18:08:22,024 fail2ban.actions [8234]: INFO banTime: 3600
2023-12-29 18:08:22,024 fail2ban.filter [8234]: INFO encoding: UTF-8
2023-12-29 18:08:22,024 fail2ban.jail [8234]: INFO Creating new jail 'sshd-ddos'
2023-12-29 18:08:22,025 fail2ban.jail [8234]: INFO Jail 'sshd-ddos' uses poller {}
2023-12-29 18:08:22,025 fail2ban.jail [8234]: INFO Initiated 'polling' backend
2023-12-29 18:08:22,026 fail2ban.filter [8234]: INFO maxLines: 1
2023-12-29 18:08:22,030 fail2ban.filter [8234]: INFO maxRetry: 5
2023-12-29 18:08:22,031 fail2ban.filter [8234]: INFO findtime: 600
2023-12-29 18:08:22,031 fail2ban.actions [8234]: INFO banTime: 3600
2023-12-29 18:08:22,031 fail2ban.filter [8234]: INFO encoding: UTF-8
2023-12-29 18:08:22,034 fail2ban.filtersystemd [8234]: INFO [sshd] Jail is in operation now (process new jour
nals)
2023-12-29 18:08:22,035 fail2ban.jail [8234]: INFO Jail 'sshd' started
2023-12-29 18:08:22,036 fail2ban.jail [8234]: INFO Jail 'selinux-ssh' started
2023-12-29 18:08:22,037 fail2ban.jail [8234]: INFO Jail 'apache-auth' started
2023-12-29 18:08:22,037 fail2ban.jail [8234]: INFO Jail 'apache-badbots' started
2023-12-29 18:08:22,038 fail2ban.jail [8234]: INFO Jail 'apache-noscript' started
2023-12-29 18:08:22,039 fail2ban.jail [8234]: INFO Jail 'apache-overflows' started
2023-12-29 18:08:22,039 fail2ban.jail [8234]: INFO Jail 'apache-nohome' started
2023-12-29 18:08:22,040 fail2ban.jail [8234]: INFO Jail 'apache-botsearch' started
2023-12-29 18:08:22,040 fail2ban.jail [8234]: INFO Jail 'apache-fakegooglebot' started
2023-12-29 18:08:22,041 fail2ban.jail [8234]: INFO Jail 'apache-modsecurity' started
2023-12-29 18:08:22,050 fail2ban.jail [8234]: INFO Jail 'apache-shellshock' started
2023-12-29 18:08:22,050 fail2ban.filtersystemd [8234]: INFO [postfix] Jail is in operation now (process new jo
urnals)
2023-12-29 18:08:22,051 fail2ban.jail [8234]: INFO Jail 'postfix' started
2023-12-29 18:08:22,051 fail2ban.filtersystemd [8234]: INFO [postfix-rbl] Jail is in operation now (process ne
w journal entries)
2023-12-29 18:08:22,052 fail2ban.jail [8234]: INFO Jail 'postfix-rbl' started
2023-12-29 18:08:22,052 fail2ban.filtersystemd [8234]: INFO [dovecot] Jail is in operation now (process new jo
urnals)
2023-12-29 18:08:22,052 fail2ban.jail [8234]: INFO Jail 'dovecot' started
2023-12-29 18:08:22,053 fail2ban.filtersystemd [8234]: INFO [postfix-sasl] Jail is in operation now (process n
ew journal entries)
2023-12-29 18:08:22,053 fail2ban.jail [8234]: INFO Jail 'postfix-sasl' started
2023-12-29 18:08:22,053 fail2ban.jail [8234]: INFO Jail 'sshd-ddos' started
```

Рис. 3.13: Просмотр журнала событий fail2ban

Вновь попытаемся войти с клиента на сервер с неправильным паролем и посмотрим статус защиты SSH(3.14):



```
root@server:~  
[root@server.eademidova.net ~]# nano /etc/fail2ban/jail.d/customisation.local  
[root@server.eademidova.net ~]# systemctl restart fail2ban  
[root@server.eademidova.net ~]# 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.eademidova.net ~]# fail2ban-client status sshd  
Status for the jail: sshd  
|- Filter  
| |- Currently failed: 1  
| |- Total failed: 2  
| '- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd  
- Actions  
| |- Currently banned: 0  
| |- Total banned: 0  
| '- Banned IP list:  
[root@server.eademidova.net ~]#
```

Рис. 3.14: Просмотр статуса защиты SSH после подключения к серверу с клиента по SSH с неправильным паролем

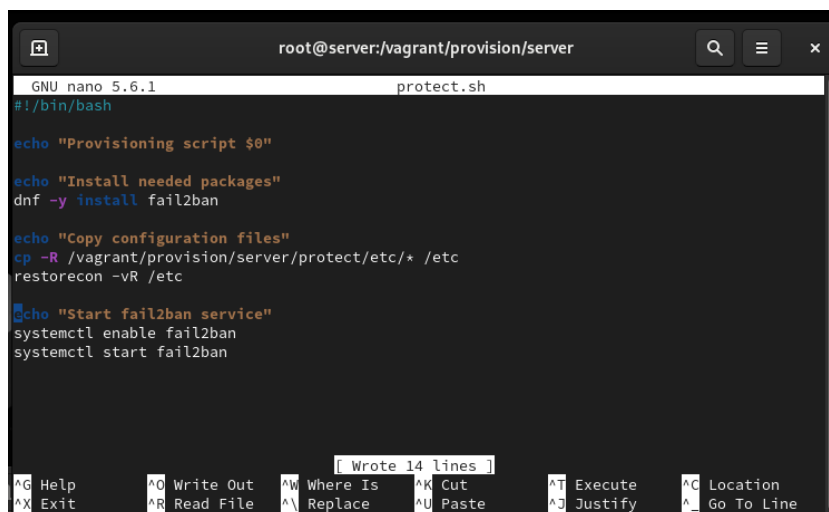
Теперь клиент не блокируется.

3.3 Внесение изменений в настройки внутреннего окружения виртуальной 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`:

```
cd /vagrant/provision/server  
mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d  
cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/  
  
touch protect.sh  
chmod +x protect.sh
```

В каталоге `/vagrant/provision/server` создадим исполняемый файл `smb.sh` и внесем скрипт(3.15):



```
root@server:/vagrant/provision/server
GNU nano 5.6.1 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. 3.15: 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"
```

4 Контрольные вопросы

1. Поясните принцип работы Fail2ban.
2. Настройки какого файла более приоритетны: jail.conf или jail.local?
3. Как настроить оповещение администратора при срабатывании Fail2ban?
4. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к веб-службе.
5. Поясните построчно настройки по умолчанию в конфигурационном файле /etc/fail2ban/jail.conf, относящиеся к почтовой службе.
6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в на-стройках Fail2ban?
7. Как получить список действующих правил Fail2ban?
8. Как получить статистику заблокированных Fail2ban адресов?
9. Как разблокировать IP-адрес?
10. 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.
11. 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`.
12. 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.
13. 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.
14. 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.

15. Fail2ban может выполнять различные действия при обнаружении атакующего IP-адреса, такие как блокировка адреса через фаервол, добавление правил в IP-таблицы, отправка уведомлений администратору и другие. Описание доступных действий можно найти в документации или руководстве Fail2ban.

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

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

18. Разблокировать адрес можно с помощью следующей команды

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

5 Выводы

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