

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: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

МОСКВА

2022 г.

Цель работы:

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

Выполнение работы:

1. Защита с помощью Fail2ban

1. На сервере установите fail2ban:

```
dnf -y install fail2ban
```

```
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# dnf -y install fail2ban
Last metadata expiration check: 2:57:06 ago on Fri 30 Dec 2022 05:38:09 PM MSK.
Dependencies resolved.
=====
Package                                Architecture      Version           Repository        Size
=====
Installing:
fail2ban                               noarch            1.0.1-2.el9      epel              8.5 k
Installing dependencies:
fail2ban-firewalld                     noarch            1.0.1-2.el9      epel              8.7 k
fail2ban-sendmail                       noarch            1.0.1-2.el9      epel              11 k
fail2ban-server                         noarch            1.0.1-2.el9      epel             442 k
=====
Transaction Summary
=====
Install 4 Packages

Total download size: 471 k
Installed size: 1.4 M
Downloading Packages:
(1/4): fail2ban-firewalld-1.0.1-2.el9.noarch.rpm    16 kB/s | 8.7 kB    00:00
(2/4): fail2ban-sendmail-1.0.1-2.el9.noarch.rpm     19 kB/s | 11 kB     00:00
(3/4): fail2ban-1.0.1-2.el9.noarch.rpm             14 kB/s | 8.5 kB    00:00
(4/4): fail2ban-server-1.0.1-2.el9.noarch.rpm       3.6 MB/s | 442 kB   00:00
-----
Total                                           197 kB/s | 471 kB   00:02
Running transaction check
Transaction check succeeded.
```

2. Запустите сервер fail2ban:

```
systemctl start fail2ban
```

```
systemctl enable fail2ban
```

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

3. В дополнительном терминале запустите просмотр журнала событий fail2ban:

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

```
root@server:~ x root@server:~ x
[kreachna@server.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@server.kreachna.net ~]# tail -f /var/log/fail2ban.log
2022-12-30 20:35:40,297 fail2ban.server [7003]: INFO -----
-----
2022-12-30 20:35:40,298 fail2ban.server [7003]: INFO Starting Fail2ban v1.0.1
2022-12-30 20:35:40,299 fail2ban.observer [7003]: INFO Observer start...
2022-12-30 20:35:40,302 fail2ban.database [7003]: INFO Connected to fail2ban persistent databa
se '/var/lib/fail2ban/fail2ban.sqlite3'
2022-12-30 20:35:40,304 fail2ban.database [7003]: WARNING New database created. Version '4'
```

4. Создайте файл с локальной конфигурацией fail2ban:

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

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

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

```
[root@server.kreachna.net ~]# vim /etc/fail2ban/jail.d/customisation.local
[root@server.kreachna.net ~]# cat /etc/fail2ban/jail.d/customisation.local
[DEFAULT]
bantime = 3600

#
# SSH servers
#

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
enabled = true

[selinux-ssh]
enabled = true
```

6. Перезапустите fail2ban

systemctl restart fail2ban

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

7. Посмотрите журнал событий:

tail -f /var/log/fail2ban.log

```
-----
2022-12-30 20:39:10,332 fail2ban.server [7105]: INFO Starting Fail2ban v1.0.1
2022-12-30 20:39:10,332 fail2ban.observer [7105]: INFO Observer start...
2022-12-30 20:39:10,337 fail2ban.database [7105]: INFO Connected to fail2ban persistent database
'/var/lib/fail2ban/fail2ban.sqlite3'
2022-12-30 20:39:10,338 fail2ban.jail [7105]: INFO Creating new jail 'sshd'
2022-12-30 20:39:10,366 fail2ban.jail [7105]: INFO Jail 'sshd' uses systemd {}
2022-12-30 20:39:10,367 fail2ban.jail [7105]: INFO Initiated 'systemd' backend
2022-12-30 20:39:10,369 fail2ban.filter [7105]: INFO maxLines: 1
2022-12-30 20:39:10,403 fail2ban.filtersystemd [7105]: INFO [sshd] Added journal match for: '_SYSTEMD
UNIT=sshd.service + COMM=sshd'
2022-12-30 20:39:10,403 fail2ban.filter [7105]: INFO maxRetry: 5
2022-12-30 20:39:10,403 fail2ban.filter [7105]: INFO findtime: 600
2022-12-30 20:39:10,403 fail2ban.actions [7105]: INFO banTime: 3600
2022-12-30 20:39:10,403 fail2ban.filter [7105]: INFO encoding: UTF-8
2022-12-30 20:39:10,404 fail2ban.jail [7105]: INFO Creating new jail 'selinux-ssh'
2022-12-30 20:39:10,405 fail2ban.jail [7105]: INFO Jail 'selinux-ssh' uses poller {}
2022-12-30 20:39:10,405 fail2ban.jail [7105]: INFO Initiated 'polling' backend
2022-12-30 20:39:10,407 fail2ban.datedetector [7105]: INFO date pattern '': `Epoch`
2022-12-30 20:39:10,407 fail2ban.filter [7105]: INFO maxRetry: 5
2022-12-30 20:39:10,408 fail2ban.filter [7105]: INFO findtime: 600
2022-12-30 20:39:10,408 fail2ban.actions [7105]: INFO banTime: 3600
2022-12-30 20:39:10,408 fail2ban.filter [7105]: INFO encoding: UTF-8
2022-12-30 20:39:10,409 fail2ban.filter [7105]: INFO Added logfile: '/var/log/audit/audit.log'
(pos = 0, hash = 4f489a3f6c1e9ec450cab47395f1f1e4e56dalf4)
2022-12-30 20:39:10,410 fail2ban.transmitter [7105]: ERROR Jail 'sshd-ddos' skipped, because of wrong
configuration: Unable to read the filter 'sshd-ddos'
2022-12-30 20:39:10,414 fail2ban.filtersystemd [7105]: INFO [sshd] Jail is in operation now (process
new journal entries)
2022-12-30 20:39:10,415 fail2ban.jail [7105]: INFO Jail 'sshd' started
2022-12-30 20:39:10,422 fail2ban.jail [7105]: INFO Jail 'selinux-ssh' started
2022-12-30 20:39:10,442 fail2ban.filter [7105]: WARNING [selinux-ssh] Ignoring all log entries ol
der than 600s; these are probably messages generated while fail2ban was not running.
2022-12-30 20:39:10,443 fail2ban.filter [7105]: WARNING [selinux-ssh] Please check a jail for a t
iming issue. Line with odd timestamp: type=SERVICE_STOP msg=audit(1672421130.092:1026): pid=1 uid=0 auid=
4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=geoclue comm="systemd" exe="/usr/lib
/systemd/systemd" hostname=? addr=? terminal=? res=success'UID="root" AUID="unset"
```

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
```

9. Перезапустите fail2ban

systemctl restart fail2ban

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

10. Посмотрите журнал событий:

tail -f /var/log/fail2ban.log

```
2022-12-30 20:43:11,947 fail2ban.filter [7146]: INFO Added logfile: '/var/log/httpd/error_log'
(pos = 0, hash = 1f9d79026ed3b665ea3798333a46f1318a62e4a8)
2022-12-30 20:43:11,952 fail2ban.filter [7146]: INFO Added logfile: '/var/log/httpd/www.kreach
na.net-error_log' (pos = 0, hash = 1c32277df9116767612313097997f9fe621f77ef)
2022-12-30 20:43:11,953 fail2ban.jail [7146]: INFO Creating new jail 'apache-shellshock'
2022-12-30 20:43:11,956 fail2ban.jail [7146]: INFO Jail 'apache-shellshock' uses poller {}
2022-12-30 20:43:11,956 fail2ban.jail [7146]: INFO Initiated 'polling' backend
2022-12-30 20:43:11,969 fail2ban.filter [7146]: INFO maxRetry: 1
2022-12-30 20:43:11,973 fail2ban.filter [7146]: INFO findtime: 600
2022-12-30 20:43:11,975 fail2ban.actions [7146]: INFO banTime: 3600
2022-12-30 20:43:11,980 fail2ban.filter [7146]: INFO encoding: UTF-8
2022-12-30 20:43:11,983 fail2ban.filter [7146]: INFO Added logfile: '/var/log/httpd/server.kre
achna.net-error_log' (pos = 0, hash = )
2022-12-30 20:43:11,989 fail2ban.filter [7146]: INFO Added logfile: '/var/log/httpd/ssl_error_
log' (pos = 0, hash = )
2022-12-30 20:43:11,999 fail2ban.filter [7146]: INFO Added logfile: '/var/log/httpd/error_log'
(pos = 0, hash = 1f9d79026ed3b665ea3798333a46f1318a62e4a8)
2022-12-30 20:43:12,002 fail2ban.filter [7146]: INFO Added logfile: '/var/log/httpd/www.kreach
na.net-error_log' (pos = 0, hash = 1c32277df9116767612313097997f9fe621f77ef)
2022-12-30 20:43:12,005 fail2ban.transmitter [7146]: ERROR Jail 'sshd-ddos' skipped, because of wron
g configuration: Unable to read the filter 'sshd-ddos'
2022-12-30 20:43:12,007 fail2ban.filtersystemd [7146]: INFO [sshd] Jail is in operation now (process
new journal entries)
2022-12-30 20:43:12,018 fail2ban.jail [7146]: INFO Jail 'sshd' started
2022-12-30 20:43:12,041 fail2ban.jail [7146]: INFO Jail 'selinux-ssh' started
2022-12-30 20:43:12,075 fail2ban.jail [7146]: INFO Jail 'apache-auth' started
2022-12-30 20:43:12,120 fail2ban.jail [7146]: INFO Jail 'apache-badbots' started
2022-12-30 20:43:12,231 fail2ban.jail [7146]: INFO Jail 'apache-noscript' started
2022-12-30 20:43:12,308 fail2ban.jail [7146]: INFO Jail 'apache-overflows' started
2022-12-30 20:43:12,329 fail2ban.jail [7146]: INFO Jail 'apache-nohome' started
2022-12-30 20:43:12,343 fail2ban.jail [7146]: INFO Jail 'apache-botsearch' started
2022-12-30 20:43:12,347 fail2ban.jail [7146]: INFO Jail 'apache-fakegooglebot' started
2022-12-30 20:43:12,353 fail2ban.jail [7146]: INFO Jail 'apache-modsecurity' started
2022-12-30 20:43:12,365 fail2ban.jail [7146]: INFO Jail 'apache-shellshock' started
```

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
```

12. Перезапустите fail2ban:

```
systemctl restart fail2ban
```

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

13. Посмотрите журнал событий:

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

```
2022-12-30 20:45:13,535 fail2ban.jail [7200]: INFO Jail 'apache-auth' started
2022-12-30 20:45:13,552 fail2ban.jail [7200]: INFO Jail 'apache-badbots' started
2022-12-30 20:45:13,572 fail2ban.jail [7200]: INFO Jail 'apache-noscript' started
2022-12-30 20:45:13,579 fail2ban.jail [7200]: INFO Jail 'apache-overflows' started
2022-12-30 20:45:13,583 fail2ban.jail [7200]: INFO Jail 'apache-nohome' started
2022-12-30 20:45:13,585 fail2ban.jail [7200]: INFO Jail 'apache-botsearch' started
2022-12-30 20:45:13,602 fail2ban.jail [7200]: INFO Jail 'apache-fakegooglebot' started
2022-12-30 20:45:13,604 fail2ban.jail [7200]: INFO Jail 'apache-modsecurity' started
2022-12-30 20:45:13,614 fail2ban.jail [7200]: INFO Jail 'apache-shellshock' started
2022-12-30 20:45:13,616 fail2ban.jail [7200]: INFO Jail 'postfix' started
2022-12-30 20:45:13,636 fail2ban.filterssystemd [7200]: INFO [postfix] Jail is in operation now (process new j
ournal entries)
2022-12-30 20:45:13,639 fail2ban.filterssystemd [7200]: INFO [postfix-rbl] Jail is in operation now (process n
ew journal entries)
2022-12-30 20:45:13,649 fail2ban.jail [7200]: INFO Jail 'postfix-rbl' started
2022-12-30 20:45:13,652 fail2ban.jail [7200]: INFO Jail 'dovecot' started
2022-12-30 20:45:13,654 fail2ban.filterssystemd [7200]: INFO [dovecot] Jail is in operation now (process new j
ournal entries)
2022-12-30 20:45:13,672 fail2ban.filterssystemd [7200]: INFO [postfix-sasl] Jail is in operation now (process
new journal entries)
2022-12-30 20:45:13,687 fail2ban.jail [7200]: INFO Jail 'postfix-sasl' started
```

2. Проверка работы Fail2ban

1. На сервере посмотрите статус fail2ban:

```
fail2ban-client status
```

```
[root@server.kreachna.net ~]# fail2ban-client status
Status
|- Number of jail:      15
|- Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsec
urity, apache-nohome, apache-noscript, apache-overflows, apache-shellshock, dovecot, postfix, post
fix-rbl, postfix-sasl, selinux-ssh, sshd
```

2. Посмотрите статус защиты SSH в fail2ban:

```
fail2ban-client status sshd
```

```
[root@server.kreachna.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:
```

3. Установите максимальное количество ошибок для SSH, равное 2:

fail2ban-client set sshd maxretry 2

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

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

```
[kreachna@client.kreachna.net ~]$ sudo -i
[sudo] password for kreachna:
[root@client.kreachna.net ~]# ssh kreachna@server.kreachna.net
The authenticity of host 'server.kreachna.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:/2uvDHfM1QlaLTeqPJTnsRSayzizIaAix/x7vXlm2m4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server.kreachna.net' (ED25519) to the list of known hosts.
kreachna@server.kreachna.net's password:
Permission denied, please try again.
kreachna@server.kreachna.net's password:
Permission denied, please try again.
kreachna@server.kreachna.net's password:
kreachna@server.kreachna.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
```

5. На сервере посмотрите статус защиты SSH:

fail2ban-client status sshd

```
[root@server.kreachna.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
```

Убедитесь, что произошла блокировка адреса клиента.

2022-12-30 20:45:13,649 fail2ban.jail	[7200]: INFO	Jail 'postfix-rbl' started
2022-12-30 20:45:13,652 fail2ban.jail	[7200]: INFO	Jail 'dovecot' started
2022-12-30 20:45:13,654 fail2ban.filtersystemd	[7200]: INFO	[dovecot] Jail is in operation now (process new journal entries)
2022-12-30 20:45:13,672 fail2ban.filtersystemd	[7200]: INFO	[postfix-sasl] Jail is in operation now (process new journal entries)
2022-12-30 20:45:13,687 fail2ban.jail	[7200]: INFO	Jail 'postfix-sasl' started
2022-12-30 20:47:15,105 fail2ban.filter	[7200]: INFO	maxRetry: 2
2022-12-30 20:50:01,039 fail2ban.filter	[7200]: INFO	[sshd] Found 192.168.1.30 - 2022-12-30 20:49:58
2022-12-30 20:50:01,040 fail2ban.filter	[7200]: INFO	[sshd] Found 192.168.1.30 - 2022-12-30 20:49:59
2022-12-30 20:50:01,287 fail2ban.actions	[7200]: NOTICE	[sshd] Ban 192.168.1.30

6. Разблокируйте IP-адрес клиента:

```
fail2ban-client set sshd unbanip 192.168.1.30
```

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

7. Вновь посмотрите статус защиты SSH:

```
fail2ban-client status sshd
```

```
[root@server.kreachna.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:
```

Убедитесь, что блокировка клиента снята.

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
```

9. Перезапустите fail2ban.

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

10. Посмотрите журнал событий:

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

```

2022-12-30 20:54:46,601 fail2ban.jail [7333]: INFO Jail 'dovecot' uses systemd {}
2022-12-30 20:54:46,601 fail2ban.jail [7333]: INFO Initiated 'systemd' backend
2022-12-30 20:54:46,657 fail2ban.datedetector [7333]: INFO date pattern `{}: ^{LN-BEG}TAI64N`
2022-12-30 20:54:46,658 fail2ban.filtersystemd [7333]: INFO [dovecot] Added journal match for: '_SYSTEMD_UNIT=dovecot.service'
2022-12-30 20:54:46,658 fail2ban.filter [7333]: INFO maxRetry: 5
2022-12-30 20:54:46,659 fail2ban.filter [7333]: INFO findtime: 600
2022-12-30 20:54:46,659 fail2ban.actions [7333]: INFO banTime: 3600
2022-12-30 20:54:46,663 fail2ban.filter [7333]: INFO encoding: UTF-8
2022-12-30 20:54:46,665 fail2ban.jail [7333]: INFO Creating new jail 'postfix-sasl'
2022-12-30 20:54:46,665 fail2ban.jail [7333]: INFO Jail 'postfix-sasl' uses systemd {}
2022-12-30 20:54:46,666 fail2ban.jail [7333]: INFO Initiated 'systemd' backend
2022-12-30 20:54:46,671 fail2ban.filtersystemd [7333]: INFO [postfix-sasl] Added journal match for: '_SYSTEMD_UNIT=postfix.service'
2022-12-30 20:54:46,688 fail2ban.filter [7333]: INFO maxRetry: 5
2022-12-30 20:54:46,695 fail2ban.filter [7333]: INFO findtime: 600
2022-12-30 20:54:46,695 fail2ban.actions [7333]: INFO banTime: 3600
2022-12-30 20:54:46,697 fail2ban.filter [7333]: INFO encoding: UTF-8
2022-12-30 20:54:46,702 fail2ban.transmitter [7333]: ERROR Jail 'sshd-ddos' skipped, because of wrong configuration: Unable to read the filter 'sshd-ddos'
2022-12-30 20:54:46,704 fail2ban.filtersystemd [7333]: INFO [sshd] Jail is in operation now (process new journal entries)
2022-12-30 20:54:46,705 fail2ban.jail [7333]: INFO Jail 'sshd' started
2022-12-30 20:54:46,725 fail2ban.jail [7333]: INFO Jail 'selinux-ssh' started
2022-12-30 20:54:46,734 fail2ban.jail [7333]: INFO Jail 'apache-auth' started
2022-12-30 20:54:46,760 fail2ban.jail [7333]: INFO Jail 'apache-badbots' started
2022-12-30 20:54:46,777 fail2ban.jail [7333]: INFO Jail 'apache-noscript' started
2022-12-30 20:54:46,779 fail2ban.jail [7333]: INFO Jail 'apache-overflows' started
2022-12-30 20:54:46,781 fail2ban.jail [7333]: INFO Jail 'apache-nohome' started
2022-12-30 20:54:46,795 fail2ban.jail [7333]: INFO Jail 'apache-botsearch' started
2022-12-30 20:54:46,804 fail2ban.jail [7333]: INFO Jail 'apache-fakegooglebot' started
2022-12-30 20:54:46,810 fail2ban.jail [7333]: INFO Jail 'apache-modsecurity' started
2022-12-30 20:54:46,829 fail2ban.jail [7333]: INFO Jail 'apache-shellshock' started
2022-12-30 20:54:46,833 fail2ban.filtersystemd [7333]: INFO [postfix] Jail is in operation now (process new journal entries)
2022-12-30 20:54:46,846 fail2ban.jail [7333]: INFO Jail 'postfix' started
2022-12-30 20:54:46,859 fail2ban.filtersystemd [7333]: INFO [postfix-rbl] Jail is in operation now (process new journal entries)
2022-12-30 20:54:46,861 fail2ban.jail [7333]: INFO Jail 'postfix-rbl' started
2022-12-30 20:54:46,869 fail2ban.filtersystemd [7333]: INFO [dovecot] Jail is in operation now (process new journal entries)
2022-12-30 20:54:46,873 fail2ban.jail [7333]: INFO Jail 'dovecot' started
2022-12-30 20:54:46,880 fail2ban.filtersystemd [7333]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2022-12-30 20:54:46,897 fail2ban.jail [7333]: INFO Jail 'postfix-sasl' started

```

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

```

[root@client.kreachna.net ~]# ssh kreachna@server.kreachna.net
kreachna@server.kreachna.net's password:
Permission denied, please try again.
kreachna@server.kreachna.net's password:
Permission denied, please try again.
kreachna@server.kreachna.net's password:
kreachna@server.kreachna.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.kreachna.net ~]# ssh -p2022 kreachna@server.kreachna.net
kreachna@server.kreachna.net's password:
Permission denied, please try again.
kreachna@server.kreachna.net's password:
Permission denied, please try again.
kreachna@server.kreachna.net's password:
kreachna@server.kreachna.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.kreachna.net ~]#

```



```
[root@server.kreachna.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:
```

3. Внесение изменений в настройки внутреннего окружения виртуальных машин

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.kreachna.net ~]# cd /vagrant/provision/server
[root@server.kreachna.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
[root@server.kreachna.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/etc/fail2ban/jail.d/
```

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

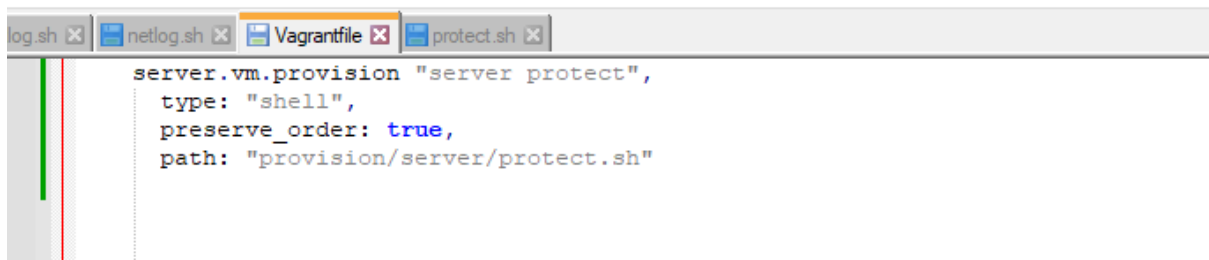
```
cd /vagrant/provision/server
touch protect.sh
chmod +x protect.sh
```

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

Открыв его на редактирование, пропишите в нём следующий скрипт:

```
netlog.sh x netlog.sh x Vagrantfile x protect.sh x
1  #!/bin/bash
2
3  echo "Provisioning script $0"
4
5  echo "Install needed packages"
6  dnf -y install fail2ban
7
8  echo "Copy configuration files"
9  cp -R /vagrant/provision/server/protect/etc/* /etc
10 restorecon -vR /etc
11
12 echo "Start fail2ban service"
13 systemctl enable fail2ban
14 systemctl start fail2ban
15
```

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"
```

Ответы на контрольные вопросы

1. Поясните принцип работы Fail2ban.

Fail2ban считывает логи (например, /var/log/apache2/error.log) и блокирует IP-адреса, активность которых является подозрительной (например, большое количество попыток войти с неправильно введенным паролем, выполнение опасных или бессмысленных действий и т.д.). В случае обнаружения подобных действий программа обновляет правила брандмауэра для блокировки такого IP адреса на определенный промежуток времени.

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

После установки в каталоге /etc/fail2ban будет такая структура конфигурационных файлов

- /etc/fail2ban/jail.conf
- /etc/fail2ban/jail.d/*.conf
- /etc/fail2ban/jail.local
- /etc/fail2ban/jail.d/*.local

Конфигурационные файлы считываются сверху вниз. Последний считанный файл имеет высший приоритет. В данном случае при существовании файлов с расширением local будут более приоритетны.

3. Как настроить оповещение администратора при срабатывании Fail2ban?

Если вы хотите настроить оповещение о срабатывании блокировки Fail2ban по электронной почте, это тоже настраивается в разделе [DEFAULT]. Только необходимо чтобы на вашей машине был настроен почтовый сервер и он мог отправлять письма на внешний адрес. Иначе все письма будут доставлены к локальной учетной записи Linux.

- 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 у вас настроен Sendmail, оставьте значение по умолчанию. 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.

В данном файле, если мы откроем часть «HTTP servers», мы встретим описание нескольких правил. Они имеют следующий синтаксис: `[название правила]`, `port` — порт целевого сервиса, `logpath` — расположение лог-файла, в котором фильтр будет искать подозрительную активность на основе описанных критериев, `bantime` — время бана в секундах, по истечении которого IP-адрес удаляется из списка заблокированных, `maxretry` — количество подозрительных совпадений, после которых применяется правило. Здесь присутствуют несколько секций, например, `[apache-auth]` - определяет неудачные попытки ввода пароля, `[apache-badbots]` - определяет ботов, которые ищут email адреса, `[apache-noscript]` - блокирует доступ к определенным скриптам, `[apache-overflows]` - предотвращает попытки переполнения Apache, `[apache-nohome]` - блокирует неудачные попытки поиска домашней директории. Но они не активированы, чтобы это исправить, нужно в каждую секцию добавить параметр `enabled = true`.

```
jail.conf [----] 0 L:[297+ 0 297/981] *(11124/25607b) 0010 0x00A
#
# 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

[apache-nohome]
port      = http,https
logpath   = %(apache_error_log)s
maxretry  = 2

[apache-botsearch]
port      = http,https
logpath   = %(apache_error_log)s
```

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

В данном файле, если мы откроем часть «MAIL servers», мы встретим описание нескольких правил. Они имеют следующий синтаксис: [название правила], port — порт целевого сервиса, logpath — расположение лог-файла, в котором фильтр будет искать подозрительную активность на основе описанных критериев, maxretry — количество подозрительных совпадений, после которых применяется правило.

```
#
# Mail servers
#

# 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
```

6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса?

Где можно посмотреть описание действий для последующего использования в настройках Fail2ban?

Действие определяется в переменной action в зависимости от предпочтений администратора. Все правила реагирования на действия злоумышленника описаны в файле /etc/fail2ban/action.d. Соответственно, в качестве значения параметра action не может быть указана информация, которой нет в файле /etc/fail2ban/action.d

7. Как получить список действующих правил Fail2ban?

fail2ban-client status

8. Как получить статистику заблокированных Fail2ban адресов?

fail2ban-client status <имя клетки>

9. Как разблокировать IP-адрес?

fail2ban-client set <имя клетки> unbanip <ip-адрес>

Вывод:

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