

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ

ВЫПОЛНЕННОЙ ЛАБОРАТОРНОЙ РАБОТЫ № 16

дисциплина: Администрирование сетевых подсистем

Базовая защита от атак типа «brute force»

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

МОСКВА

2023 г.

Цель работы

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

Предварительные сведения

Одно из решений по защите узла сети от несанкционированного доступа и атак типа «brute force» (в частности, подбора паролей администратора методом полного перебора) — использование 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. Файл `/etc/fail2ban/fail2ban.conf` содержит настройки запуска процесса Fail2ban. Основной файл конфигурации конкретных служб в Fail2ban — `/etc/fail2ban/jail.conf`, настройки для локального узла должны быть размещены в файле `NAMEFILE.local` в каталоге `/etc/fail2ban/jail.d`, конфигурации для работы с различными службами размещаются в отдельных подкаталогах и файлах в каталоге `/etc/fail2ban/`. Каждый конфигурационный файл Fail2ban имеет секции, каждая из которых описывает определённую службу и тип атаки.

Защита с помощью Fail2ban

```
[root@server.etanribergenov.net ~]# dnf -y install fail2ban
Last metadata expiration check: 0:07:36 ago on Fri 14 Apr 2023 07:58:03 PM UTC.
Dependencies resolved.
=====
Package                                Arch      Version              Repository           Size
=====
Installing:
fail2ban                                noarch    1.0.2-3.el9          epel                  8.3 k
Upgrading:
libselinux                             x86_64    3.4-3.el9            baseos                85 k
libselinux-utils                       x86_64    3.4-3.el9            baseos               158 k
libsemanage                             x86_64    3.4-2.el9            baseos               118 k
libsepol                                x86_64    3.4-1.1.el9          baseos               315 k
policycoreutils                       x86_64    3.4-4.el9            baseos               202 k
policycoreutils-python-utils           noarch    3.4-4.el9            appstream             69 k
python3-libselinux                     x86_64    3.4-3.el9            appstream            185 k
python3-libsemanage                    x86_64    3.4-2.el9            appstream             80 k
python3-policycoreutils                noarch    3.4-4.el9            appstream            2.0 M
selinux-policy                         noarch    34.1.43-1.el9_1.2    baseos                52 k
selinux-policy-targeted                 noarch    34.1.43-1.el9_1.2    baseos               6.4 M
Installing dependencies:
fail2ban-firewalld                     noarch    1.0.2-3.el9          epel                  8.5 k
=====
```

Рис. 1. Установка fail2ban

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

Рис. 2. Запуск сервера fail2ban

```
[etanribergenov@server.etanribergenov.net ~]$ sudo -i
[sudo] password for etanribergenov:
[root@server.etanribergenov.net ~]# tail -f /var/log/fail2ban.log
2023-04-14 20:11:39,182 fail2ban.server [46696]: INFO -----
-----
2023-04-14 20:11:39,182 fail2ban.server [46696]: INFO Starting Fail2b
an v1.0.2
2023-04-14 20:11:39,184 fail2ban.observer [46696]: INFO Observer start.
..
2023-04-14 20:11:39,209 fail2ban.database [46696]: INFO Connected to fa
il2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2023-04-14 20:11:39,215 fail2ban.database [46696]: WARNING New database cr
eated. Version '4'
2023-04-14 20:17:08,610 fail2ban.server [46696]: INFO Shutdown in pro
gress...
2023-04-14 20:17:08,611 fail2ban.observer [46696]: INFO Observer stop .
.. try to end queue 5 seconds
2023-04-14 20:17:08,632 fail2ban.observer [46696]: INFO Observer stoppe
d, 0 events remaining.
2023-04-14 20:17:08,674 fail2ban.server [46696]: INFO Stopping all ja
ils
2023-04-14 20:17:08,674 fail2ban.database [46696]: INFO Connection to d
atabase closed.
2023-04-14 20:17:08,675 fail2ban.server [46696]: INFO Exiting Fail2ba
```

Рис. 3. Просмотр журнала событий fail2ban

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

Рис. 4. Создание файла с локальной конфигурацией fail2ban

```
customis~on.local
[DEFAULT]
bantime = 3600
```

Рис. 5. Настройка времени блокирования

```
#
# SSH servers
#

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
filter = sshd
enabled = true

[selinux-ssh]
enabled = true
```

Рис. 6. Включение защиты SSH

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

Рис. 7. Перезапуск fail2ban

```
2023-04-14 20:17:10,070 fail2ban.filter [46823]: INFO Added logfile:
'/var/log/audit/audit.log' (pos = 0, hash = 7c234ea41e96fe055c87355690edf0fe2078
a4e7)
2023-04-14 20:17:10,072 fail2ban.jail [46823]: INFO Creating new ja
il 'sshd-ddos'
2023-04-14 20:17:10,096 fail2ban.jail [46823]: INFO Jail 'sshd-ddos
' uses poller {}
2023-04-14 20:17:10,097 fail2ban.jail [46823]: INFO Initiated 'poll
ing' backend
2023-04-14 20:17:10,113 fail2ban.filter [46823]: INFO maxLines: 1
2023-04-14 20:17:10,130 fail2ban.filter [46823]: INFO maxRetry: 5
2023-04-14 20:17:10,130 fail2ban.filter [46823]: INFO findtime: 600
2023-04-14 20:17:10,131 fail2ban.actions [46823]: INFO banTime: 3600
2023-04-14 20:17:10,133 fail2ban.filter [46823]: INFO encoding: UTF
-8
2023-04-14 20:17:10,164 fail2ban.jail [46823]: INFO Jail 'sshd' sta
rted
2023-04-14 20:17:10,183 fail2ban.filtersystemd [46823]: INFO [sshd] Jail is
in operation now (process new journal entries)
2023-04-14 20:17:10,201 fail2ban.jail [46823]: INFO Jail 'selinux-s
sh' started
2023-04-14 20:17:10,209 fail2ban.jail [46823]: INFO Jail 'sshd-ddos
' started
```

Рис. 8. Просмотр журнала событий

```
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
```

Рис. 9. Включение защиты HTTP

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

Рис. 10. Перезапуск fail2ban

```
2023-04-14 20:24:30,721 fail2ban.jail [46888]: INFO Jail 'selinux-s
sh' started
2023-04-14 20:24:30,750 fail2ban.jail [46888]: INFO Jail 'apache-au
th' started
2023-04-14 20:24:30,798 fail2ban.jail [46888]: INFO Jail 'apache-ba
dbots' started
2023-04-14 20:24:30,836 fail2ban.jail [46888]: INFO Jail 'apache-no
script' started
2023-04-14 20:24:30,876 fail2ban.jail [46888]: INFO Jail 'apache-ov
erflows' started
2023-04-14 20:24:30,885 fail2ban.jail [46888]: INFO Jail 'apache-no
home' started
2023-04-14 20:24:30,905 fail2ban.jail [46888]: INFO Jail 'apache-bo
tsearch' started
2023-04-14 20:24:30,948 fail2ban.jail [46888]: INFO Jail 'apache-fa
kegooglebot' started
2023-04-14 20:24:30,980 fail2ban.jail [46888]: INFO Jail 'apache-mo
dsecurity' started
2023-04-14 20:24:30,990 fail2ban.jail [46888]: INFO Jail 'apache-sh
ellshock' started
2023-04-14 20:24:31,008 fail2ban.jail [46888]: INFO Jail 'sshd-ddos
' started
```

Рис. 11. Просмотр журнала событий

```
#
# Mail servers
#

[postfix]
enabled = true

[postfix-rbl]
enabled = true

[dovecot]
enabled = true

[postfix-sasl]
enabled = true
```

Рис. 12. Включение защиты почты

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

Рис. 13. Перезапуск fail2ban

```
2023-04-14 20:40:27,769 fail2ban.jail [47164]: INFO Jail 'apache-auth' s
tated
2023-04-14 20:40:27,779 fail2ban.jail [47164]: INFO Jail 'apache-badbots
' started
2023-04-14 20:40:27,801 fail2ban.jail [47164]: INFO Jail 'apache-noscrip
t' started
2023-04-14 20:40:27,815 fail2ban.jail [47164]: INFO Jail 'apache-overflo
ws' started
2023-04-14 20:40:27,829 fail2ban.jail [47164]: INFO Jail 'apache-nohome'
started
2023-04-14 20:40:27,836 fail2ban.jail [47164]: INFO Jail 'apache-botsear
ch' started
2023-04-14 20:40:27,865 fail2ban.jail [47164]: INFO Jail 'apache-fakegoo
glebot' started
2023-04-14 20:40:27,889 fail2ban.jail [47164]: INFO Jail 'apache-modsecu
rity' started
2023-04-14 20:40:27,930 fail2ban.jail [47164]: INFO Jail 'apache-shellsh
ock' started
2023-04-14 20:40:27,954 fail2ban.filtersystemd [47164]: INFO [postfix] Jail is in
operation now (process new journal entries)
```

Рис. 14. Просмотр журнала событий

Проверка работы Fail2ban

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

Рис. 15. Просмотр статуса fail2ban

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

Рис. 16. Просмотр статуса защиты SSH в fail2ban

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

Рис. 17. Установка количества прав на ошибку при подключении (вводе пароля)


```
[etanribergenov@client.etanribergenov.net ~]$ ssh etanribergenov@server.etanribergenov.net
The authenticity of host 'server.etanribergenov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqb0am9bCTBqb0qNzuP7z0xlg0qvGhkHxMkw2sQdblo.
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.etanribergenov.net' (ED25519) to the list of known hosts.
etanribergenov@server.etanribergenov.net's password:
Permission denied, please try again.
etanribergenov@server.etanribergenov.net's password:
Permission denied, please try again.
etanribergenov@server.etanribergenov.net's password:
etanribergenov@server.etanribergenov.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[etanribergenov@client.etanribergenov.net ~]$
```

Рис. 18. Попытка подключения к серверу по SSH с неправильным паролем

```
[root@server.etanribergenov.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 1
|   |- Total failed: 3
|   `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
    |- Currently banned: 1
    |- Total banned: 1
    `-- Banned IP list: 192.168.1.125
[root@server.etanribergenov.net ~]#
```

Рис. 19. Просмотр статуса защиты SSH

```
[root@server.etanribergenov.net ~]# fail2ban-client set sshd unbanip 192.168.1.125
1
[root@server.etanribergenov.net ~]#
```

Рис. 20. Разблокировка IP-адреса клиента

```

[root@server.etanribergenov.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|   |- Currently failed: 0
|   |- Total failed:     4
|   \- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
\-- Actions
    |- Currently banned: 0
    |- Total banned:     1
    \- Banned IP list:
[root@server.etanribergenov.net ~]#

```

Рис. 21. Просмотр статуса защиты SSH

```

customisation.local [----] 9 L:[ ]
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 192.168.1.125

```

Рис. 22. Добавление в раздел по умолчанию игнорирование адреса клиента

```

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

```

Рис. 23. Перезапуск fail2ban

```

2023-04-14 20:42:07,749 fail2ban.filter [47164]: INFO [sshd] Ignore 192.16
8.1.125 by ip
2023-04-14 20:42:15,453 fail2ban.filter [47164]: INFO [sshd] Ignore 192.16
8.1.125 by ip
2023-04-14 20:42:19,883 fail2ban.filter [47164]: INFO [sshd] Ignore 192.16
8.1.125 by ip

```

Рис. 24. Просмотр журнала событий

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

Рис. 25. Попытка входа с клиента на сервер с неправильным паролем

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

Рис. 26. Просмотр статуса защиты SSH

Внесение изменений в настройки внутреннего окружения виртуальной машины

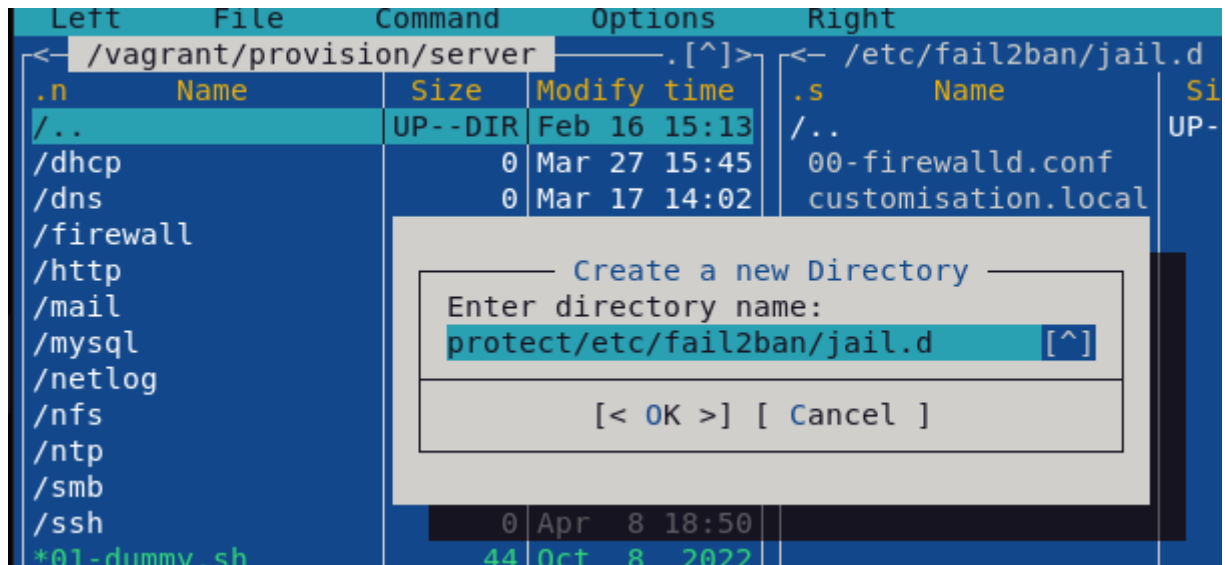


Рис. 27. Создание подкаталогов

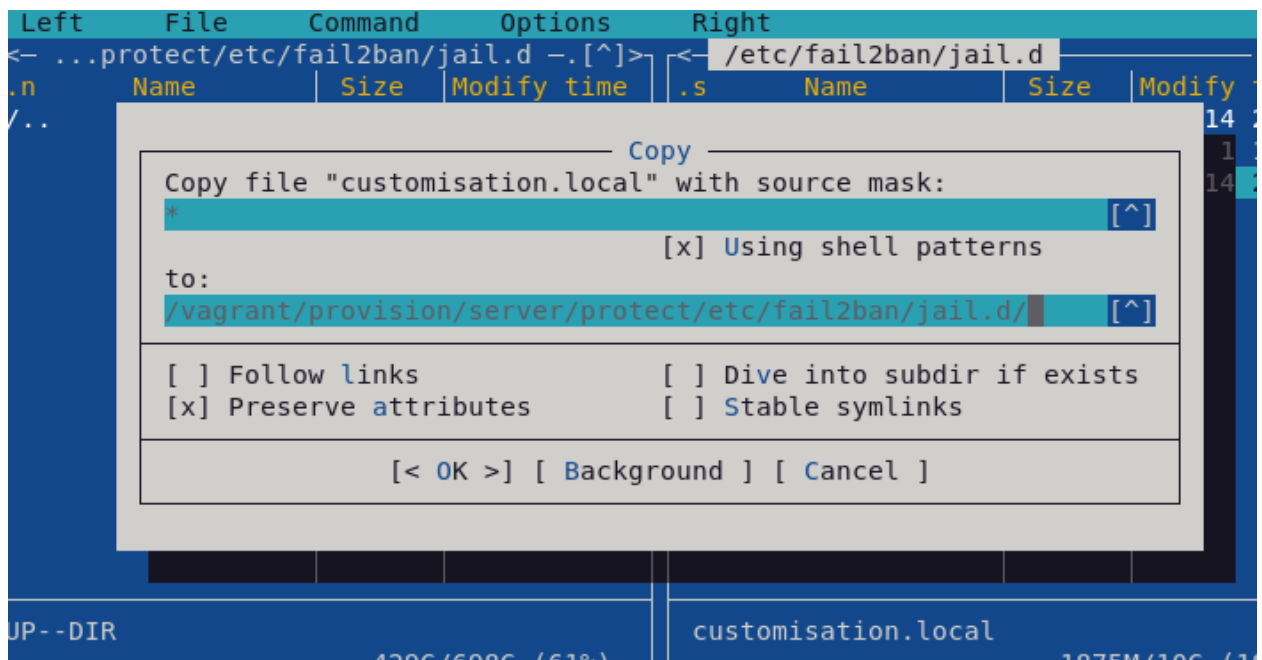


Рис. 28. Копирование конфигурационного файла fail2ban на сервере

```
[root@server.etanribergenov.net server]# touch protect.sh
[root@server.etanribergenov.net server]# chmod protect.sh
chmod: missing operand after 'protect.sh'
Try 'chmod --help' for more information.
[root@server.etanribergenov.net server]# chmod +x protect.sh
[root@server.etanribergenov.net server]#
```

Рис. 29. Создание исполняемого файла

```
protect.sh [-----] 0 L:[ 1+14 15/ 15] *(28
#!/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. 30. Скрипт в исполняемом файле

Вывод

В результате выполнения лабораторной работы я приобрёл навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».