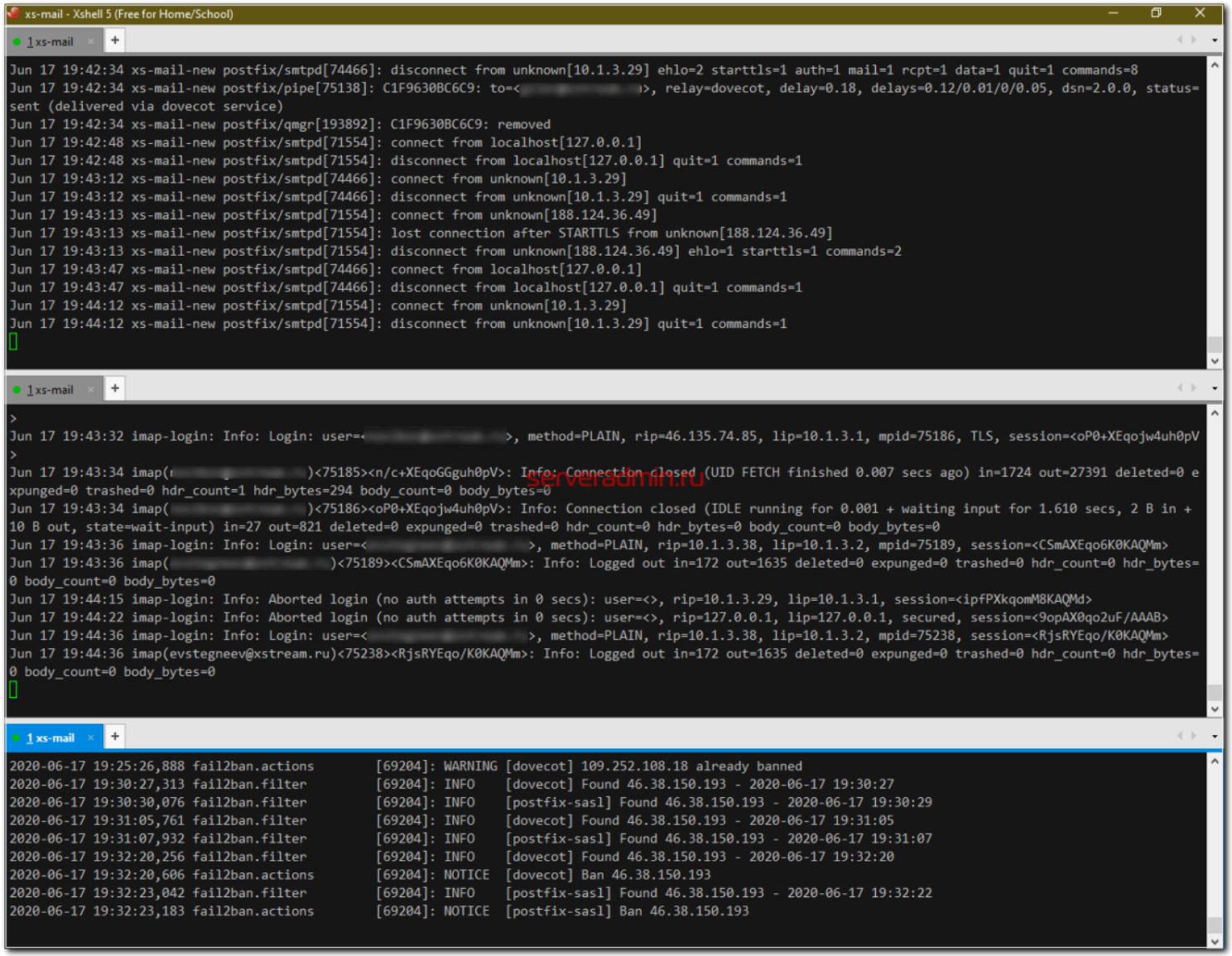

xs-mail - Xshell 5 (Free for Home/School)
1 xs-mail
Jun 17 19:42:34 xs-mail-new postfix/smtpd[74466]: disconnect from unknown[10.1.3.29] ehlo=2 starttls=1 auth=1 mail=1 rcpt=1 data=1 quit=1 commands=8
Jun 17 19:42:34 xs-mail-new postfix/pipe[75138]: C1F9630BC6C9: to=<[redacted]>, relay=dovecot, delay=0.18, delays=0.12/0.01/0/0.05, dsn=2.0.0, status=sent (delivered via dovecot service)
Jun 17 19:42:34 xs-mail-new postfix/qmgr[193892]: C1F9630BC6C9: removed
Jun 17 19:42:48 xs-mail-new postfix/smtpd[71554]: connect from localhost[127.0.0.1]
Jun 17 19:42:48 xs-mail-new postfix/smtpd[71554]: disconnect from localhost[127.0.0.1] quit=1 commands=1
Jun 17 19:43:12 xs-mail-new postfix/smtpd[74466]: connect from unknown[10.1.3.29]
Jun 17 19:43:12 xs-mail-new postfix/smtpd[74466]: disconnect from unknown[10.1.3.29] quit=1 commands=1
Jun 17 19:43:13 xs-mail-new postfix/smtpd[71554]: connect from unknown[188.124.36.49]
Jun 17 19:43:13 xs-mail-new postfix/smtpd[71554]: lost connection after STARTTLS from unknown[188.124.36.49]
Jun 17 19:43:13 xs-mail-new postfix/smtpd[71554]: disconnect from unknown[188.124.36.49] ehlo=1 starttls=1 commands=2
Jun 17 19:43:47 xs-mail-new postfix/smtpd[74466]: connect from localhost[127.0.0.1]
Jun 17 19:43:47 xs-mail-new postfix/smtpd[74466]: disconnect from localhost[127.0.0.1] quit=1 commands=1
Jun 17 19:44:12 xs-mail-new postfix/smtpd[71554]: connect from unknown[10.1.3.29]
Jun 17 19:44:12 xs-mail-new postfix/smtpd[71554]: disconnect from unknown[10.1.3.29] quit=1 commands=1
1 xs-mail
Jun 17 19:43:32 imap-login: Info: Login: user=<[redacted]>, method=PLAIN, rip=46.135.74.85, lip=10.1.3.1, mpid=75186, TLS, session=<oP0+XEqojw4uh0pV
Jun 17 19:43:34 imap([redacted])<75185><n/c+XEqoGGguh0pV>: Info: Connection closed (UID FETCH finished 0.007 secs ago) in=1724 out=27391 deleted=0 expunged=0 trashed=0 hdr_count=1 hdr_bytes=294 body_count=0 body_bytes=0
Jun 17 19:43:34 imap([redacted])<75186><oP0+XEqojw4uh0pV>: Info: Connection closed (IDLE running for 0.001 + waiting input for 1.610 secs, 2 B in + 10 B out, state=wait-input) in=27 out=821 deleted=0 expunged=0 trashed=0 hdr_count=0 hdr_bytes=0 body_count=0 body_bytes=0
Jun 17 19:43:36 imap-login: Info: Login: user=<[redacted]>, method=PLAIN, rip=10.1.3.38, lip=10.1.3.2, mpid=75189, session=<CSmAXEqo6K0KAQMm>
Jun 17 19:43:36 imap([redacted])<75189><CSmAXEqo6K0KAQMm>: Info: Logged out in=172 out=1635 deleted=0 expunged=0 trashed=0 hdr_count=0 hdr_bytes=0 body_count=0 body_bytes=0
Jun 17 19:44:15 imap-login: Info: Aborted login (no auth attempts in 0 secs): user=<>, rip=10.1.3.29, lip=10.1.3.1, session=<ipfPXkqomM8KAQMd>
Jun 17 19:44:22 imap-login: Info: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0.1, lip=127.0.0.1, secured, session=<9opAX0qo2uF/AAAB>
Jun 17 19:44:36 imap-login: Info: Login: user=<[redacted]>, method=PLAIN, rip=10.1.3.38, lip=10.1.3.2, mpid=75238, session=<RjsRYEqo/K0KAQMm>
Jun 17 19:44:36 imap(evstegneev@xstream.ru)<75238><RjsRYEqo/K0KAQMm>: Info: Logged out in=172 out=1635 deleted=0 expunged=0 trashed=0 hdr_count=0 hdr_bytes=0 body_count=0 body_bytes=0
1 xs-mail
2020-06-17 19:25:26,888 fail2ban.actions [69204]: WARNING [dovecot] 109.252.108.18 already banned
2020-06-17 19:30:27,313 fail2ban.filter [69204]: INFO [dovecot] Found 46.38.150.193 - 2020-06-17 19:30:27
2020-06-17 19:30:30,076 fail2ban.filter [69204]: INFO [postfix-sasl] Found 46.38.150.193 - 2020-06-17 19:30:29
2020-06-17 19:31:05,761 fail2ban.filter [69204]: INFO [dovecot] Found 46.38.150.193 - 2020-06-17 19:31:05
2020-06-17 19:31:07,932 fail2ban.filter [69204]: INFO [postfix-sasl] Found 46.38.150.193 - 2020-06-17 19:31:07
2020-06-17 19:32:20,256 fail2ban.filter [69204]: INFO [dovecot] Found 46.38.150.193 - 2020-06-17 19:32:20
2020-06-17 19:32:20,606 fail2ban.actions [69204]: NOTICE [dovecot] Ban 46.38.150.193
2020-06-17 19:32:23,042 fail2ban.filter [69204]: INFO [postfix-sasl] Found 46.38.150.193 - 2020-06-17 19:32:22
2020-06-17 19:32:23,183 fail2ban.actions [69204]: NOTICE [postfix-sasl] Ban 46.38.150.193

https://serveradmin.ru/audio/fail2ban-postfix-dovecot.ogg

У меня есть много статей про настройку почтового сервера, где я постоянно пропускаю важную тему защиты почтового сервера от перебора паролей. Пришло время это исправить и рассказать, как защитить postfix и dovecot с помощью fail2ban от подбора паролей к почтовым ящикам. Метод традиционный, простой и надежный — будем банить по ip тех, кто будет пытаться пройти авторизацию с неверными учетными данными.

Теоретический курс по основам **сетевых технологий**. Позволит системным администраторам упорядочить и восполнить пробелы в знаниях. Цена очень доступная, есть бесплатный доступ. Все подробности по . Можно пройти тест на знание сетей, бесплатно и без регистрации.

Содержание

Введение

Данная статья написана на примере настройки почтового сервера по моей статье — Настройка postfix + dovecot на CentOS 8. Но в контексте описываемого материала это не принципиально, так как fail2ban, postfix и dovecot имеют одинаковые конфиги и логи на всех дистрибутивах linux. Так что представленная в статье информация будет актуальна для любого сервера, где используется этот софт.

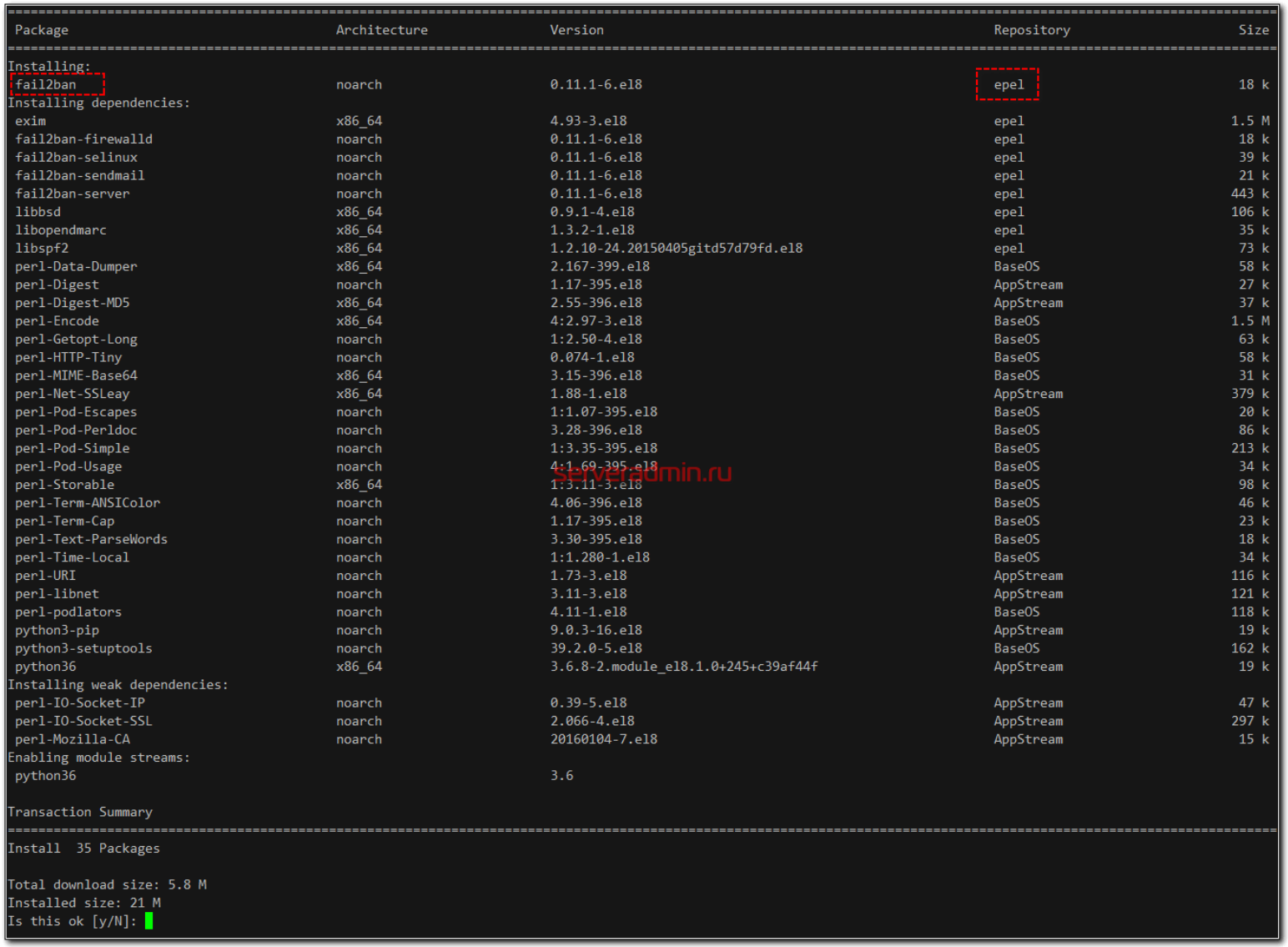
Второй важный момент. Я в своей работе везде использую нативные iptables. Для блокировки ip адресов с помощью fail2ban я буду использовать именно этот firewall. Если у вас его нет и вы хотите настроить, то добро пожаловать в мою статью по этой теме — настройка iptables. Далее я не буду останавливаться на этом.

Установка и настройка fail2ban

Установка fail2ban на любом дистрибутиве не представляет никаких сложностей, так как продукт популярный и присутствует почти во всех репозиториях. Ставим через пакетный менеджер в Centos 7,8. У вас должен быть подключен репозиторий epel.

```
# yum install fail2ban
```

```
# dnf install fail2ban
```



```
================================================================================
 Package                 Architecture    Version                        Repository      Size
================================================================================
Installing:
 fail2ban                noarch          0.11.1-6.el8                   epel            18 k
Installing dependencies:
 exim                    x86_64          4.93-3.el8                     epel           1.5 M
 fail2ban-firewalld      noarch          0.11.1-6.el8                   epel            18 k
 fail2ban-selinux        noarch          0.11.1-6.el8                   epel            39 k
 fail2ban-sendmail       noarch          0.11.1-6.el8                   epel            21 k
 fail2ban-server         noarch          0.11.1-6.el8                   epel           443 k
 libbsd                  x86_64          0.9.1-4.el8                    epel           106 k
 libopendmarc            x86_64          1.3.2-1.el8                    epel            35 k
 libspf2                 x86_64          1.2.10-24.20150405gitd57d79fd.el8 epel         73 k
 perl-Data-Dumper        x86_64          2.167-399.el8                  BaseOS          58 k
 perl-Digest             noarch          1.17-395.el8                   AppStream       27 k
 perl-Digest-MD5         x86_64          2.55-396.el8                   AppStream       37 k
 perl-Encode             x86_64          4:2.97-3.el8                   BaseOS         1.5 M
 perl-Getopt-Long        noarch          1:2.50-4.el8                   BaseOS          63 k
 perl-HTTP-Tiny          noarch          0.074-1.el8                    BaseOS          58 k
 perl-MIME-Base64        x86_64          3.15-396.el8                   BaseOS          31 k
 perl-Net-SSLeay         x86_64          1.88-1.el8                     AppStream      379 k
 perl-Pod-Escapes        noarch          1:1.07-395.el8                 BaseOS          20 k
 perl-Pod-Perldoc        noarch          3.28-396.el8                   BaseOS          86 k
 perl-Pod-Simple         noarch          1:3.35-395.el8                 BaseOS         213 k
 perl-Pod-Usage          noarch          4:1.69-395.el8                 BaseOS          34 k
 perl-Storable           x86_64          1:3.11-3.el8                   BaseOS          98 k
 perl-Term-ANSIColor     noarch          4.06-396.el8                   BaseOS          46 k
 perl-Term-Cap           noarch          1.17-395.el8                   BaseOS          23 k
 perl-Text-ParseWords    noarch          3.30-395.el8                   BaseOS          18 k
 perl-Time-Local         noarch          1:1.280-1.el8                  BaseOS          34 k
 perl-URI                noarch          1.73-3.el8                     AppStream      116 k
 perl-libnet             noarch          3.11-3.el8                     AppStream      121 k
 perl-podlators          noarch          4.11-1.el8                     BaseOS         118 k
 python3-pip             noarch          9.0.3-16.el8                   AppStream       19 k
 python3-setuptools      noarch          39.2.0-5.el8                   BaseOS         162 k
 python36                x86_64          3.6.8-2.module_el8.1.0+245+c39af44f AppStream  19 k
Installing weak dependencies:
 perl-IO-Socket-IP       noarch          0.39-5.el8                     AppStream       47 k
 perl-IO-Socket-SSL      noarch          2.066-4.el8                    AppStream      297 k
 perl-Mozilla-CA         noarch          20160104-7.el8                 AppStream       15 k
Enabling module streams:
 python36                                3.6

Transaction Summary
================================================================================
Install  35 Packages

Total download size: 5.8 M
Installed size: 21 M
Is this ok [y/N]:
```

serveradmin.ru

В Ubuntu / Debian fail2ban ставится из базовых репозиториев.

```
# apt install fail2ban
```

В Centos по умолчанию используется firewalld для управления правилами фаервола. Чтобы изменить это и перейти на iptables, достаточно удалить файл *00-firewalld.conf.*

```
# rm /etc/fail2ban/jail.d/00-firewalld.conf
```

Дальше нас будет интересовать конфигурационный файл *jail.conf*. По умолчанию в нем очень много параметров и комментариев. Мне не удобно работать с таким огромным файлом. Большая часть информации оттуда мне не нужна. Я привел его к такому виду.

```
[INCLUDES]
before = paths-fedora.conf

[DEFAULT]
ignoreip = 127.0.0.1/8  10.1.3.29/32
bantime  = 30m
findtime  = 30m
maxretry = 5
backend = auto
usedns = warn
logencoding = auto
enabled = false
mode = normal
```

Я выделил ip адрес zabbix сервера, на котором настроен мониторинг работы почтового сервера и мониторинг tls сертификатов. Если его не добавить в исключения, то он будет забанен, так как регулярно подключается к почтовому серверу, но не проходит авторизацию. Ему это не нужно для работы.

Когда будете редактировать, не забудьте на всякий случай сохранить оригинал конфига. Базовая настройка fail2ban закончена. Все остальное я оставил дефолтное. Переходим к настройке правил блокировки.

Защита postfix с помощью fail2ban

Изначально fail2ban идет с комплектом готовых настроек и фильтров для защиты большинства популярных сервисов. К ним относится и postfix. Но когда я посмотрел в готовый набор с regexp для postfix, я слегка растерялся :) Он просто огромен. И самое главное, что в таком виде он не заработал на моем лог файле.

```
postfix.conf_orig   [----]  0 L:[  1+ 0   1/ 81] *(0   /3100b) 0035 0x023                                                [*][X]
# Fail2Ban filter for selected Postfix SMTP rejections
#
#

[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# common.local
before = common.conf

[Definition]

_daemon = postfix(-\w+)?/\w+(?:/smtp[ds])?
_port = (?::\d+)?

prefregex = ^%(__prefix_line)s<mdpr-<mode>> <F-CONTENT>.+</F-CONTENT>$

mdpr-normal = (?:\w+: reject:|(?:improper command pipelining|too many errors) after \S+)
mdre-normal=^RCPT from [^[]*\[<HOST>\]%(_port)s: 55[04] 5\.7\.1\s
            ^RCPT from [^[]*\[<HOST>\]%(_port)s: 45[04] 4\.7\.\d+ (?:Service unavailable\b|Client host rejected: cannot find your (reverse )?hostname\b)
            ^RCPT from [^[]*\[<HOST>\]%(_port)s: 450 4\.7\.\d+ (<[^>]*>)?: Helo command rejected: Host not found\b
            ^EHLO from [^[]*\[<HOST>\]%(_port)s: 504 5\.5\.\d+ (<[^>]*>)?: Helo command rejected: need fully-qualified hostname\b
            ^(RCPT|VRFY) from [^[]*\[<HOST>\]%(_port)s: 550 5\.1\.1\s
            ^RCPT from [^[]*\[<HOST>\]%(_port)s: 450 4\.1\.\d+ (<[^>]*>)?: Sender address rejected: Domain not found\b
            ^from [^[]*\[<HOST>\]%(_port)s:?

mdpr-auth = warning:
mdre-auth = ^[^[]*\[<HOST>\]%(_port)s: SASL ((?i)LOGIN|PLAIN|(?:CRAM|DIGEST)-MD5) authentication failed:(?! Connection lost to authentication server| Invalid authenti
mdre-auth2= ^[^[]*\[<HOST>\]%(_port)s: SASL ((?i)LOGIN|PLAIN|(?:CRAM|DIGEST)-MD5) authentication failed:(?! Connection lost to authentication server)
# todo: check/remove "Invalid authentication mechanism" from ignore list, if gh-1243 will get finished (see gh-1297).

# Mode "rbl" currently included in mode "normal", but if needed for jail "postfix-rbl" only:
mdpr-rbl = %(mdpr-normal)s
mdre-rbl  = ^RCPT from [^[]*\[<HOST>\]%(_port)s: [45]54 [45]\.7\.1 Service unavailable; Client host \[\S+\] blocked\b

# Mode "rbl" currently included in mode "normal" (within 1st rule)
mdpr-more = %(mdpr-normal)s
mdre-more = %(mdre-normal)s
```

serveradmin.ru

Мне стало лень ковыряться в этих правилах. Для защиты postfix от перебора паролей почтовых ящиков, достаточно банить ip адреса из следующих строк лога.

```
Jun 17 03:14:07 mail postfix/smtpd[175371]: warning: unknown[46.38.145.252]: SASL LOGIN authentication failed:
UGFzc3dvcmQ6
```

Для этого достаточно относительно простого regexp.

```
^%(__prefix_line)swarning: [-._\w]+\[<HOST>\]: SASL (?:LOGIN|PLAIN|(?:CRAM|DIGEST)-MD5) authentication failed(: [ A-Za-
z0-9+/]*={0,2})?\s*$
```

Его придумал не я. Честно подсмотрел на просторах интернета. Примеров масса и у нас, и в англоязычном гугле. Далее создаем конфигурационный файл с фильтром из этого regexp — */etc/fail2ban/filter.d/**postfix-sasl.conf***.

```
[INCLUDES]
before = common.conf
[Definition]
_daemon = postfix/smtpd
failregex = ^%(__prefix_line)swarning: [-._\w]+\[\]: SASL (?:LOGIN|PLAIN|(?:CRAM|DIGEST)-MD5) authentication failed(: [
A-Za-z0-9+/]*={0,2})?\s*$
ignoreregex =
```

Можно сразу же проверить работу этого фильтра с помощью **fail2ban-regex**. Эта утилита никого не банит, а просто выводит информацию о работе фильтра.

```
# fail2ban-regex /var/log/maillog /etc/fail2ban/filter.d/postfix-sasl.conf
```

Команда успешно отработала и вывела результат.

```
Running tests
=============

Use   failregex filter file : postfix-sasl, basedir: /etc/fail2ban
Use      datepattern : Default Detectors
Use         log file : /var/log/maillog
Use         encoding : UTF-8


Results
=======

Failregex: 24327 total
|-  #) [# of hits] regular expression
|   1) [24327] ^(?:\[\])?\s*(?:<[^.]+\.[^.]+>\s+)?(?:\S+\s+)?(?:kernel:\s?\[ *\d+\.\d+\]:?\s+)?(?:@vserver_\S+\s+)?(?:(?:(?:\[\d+\])?:\s+[\[\(]?\S*(?:\(\S+\))?[\]\)]?
:?|[\[\(]?\S*(?:\(\S+\))?[\]\)]?:?(?:\[\d+\])?:?)\s+)?(?:\[ID \d+ \S+\]\s+)?warning: [-._\w]+\[<HOST>\]: SASL (?:LOGIN|PLAIN|(?:CRAM|DIGEST)-MD5) authentication faile
d(: [ A-Za-z0-9+/]*={0,2})?\s*$
`-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [102762] {^LN-BEG}(?:DAY )?MON Day %k:Minute:Second(?:\.Microseconds)?(?: ExYear)?
`-

Lines: 102762 lines, 0 ignored, 24327 matched, 78435 missed
[processed in 14.01 sec]

Missed line(s): too many to print.  Use --print-all-missed to print all 78435 lines
```

serveradmin.ru

24327 раз данный фильтр распознал строки, попадающие под работу фильтра. Изначально я напрягся, когда прикинул, что именно такое количество ip адресов поедет в бан с помощью iptables. Это еще не критично большое количество, но все равно достаточно много. По одному добавлять такое количество адресов не стоит. Нужно использовать списки, например, ipset.

На деле зря испугался. Никаких проблем не будет и дальше я покажу почему. Правило обработки лога мы проверили и убедились, что оно работает. Дальше добавляем в *jail.conf* новую секцию.

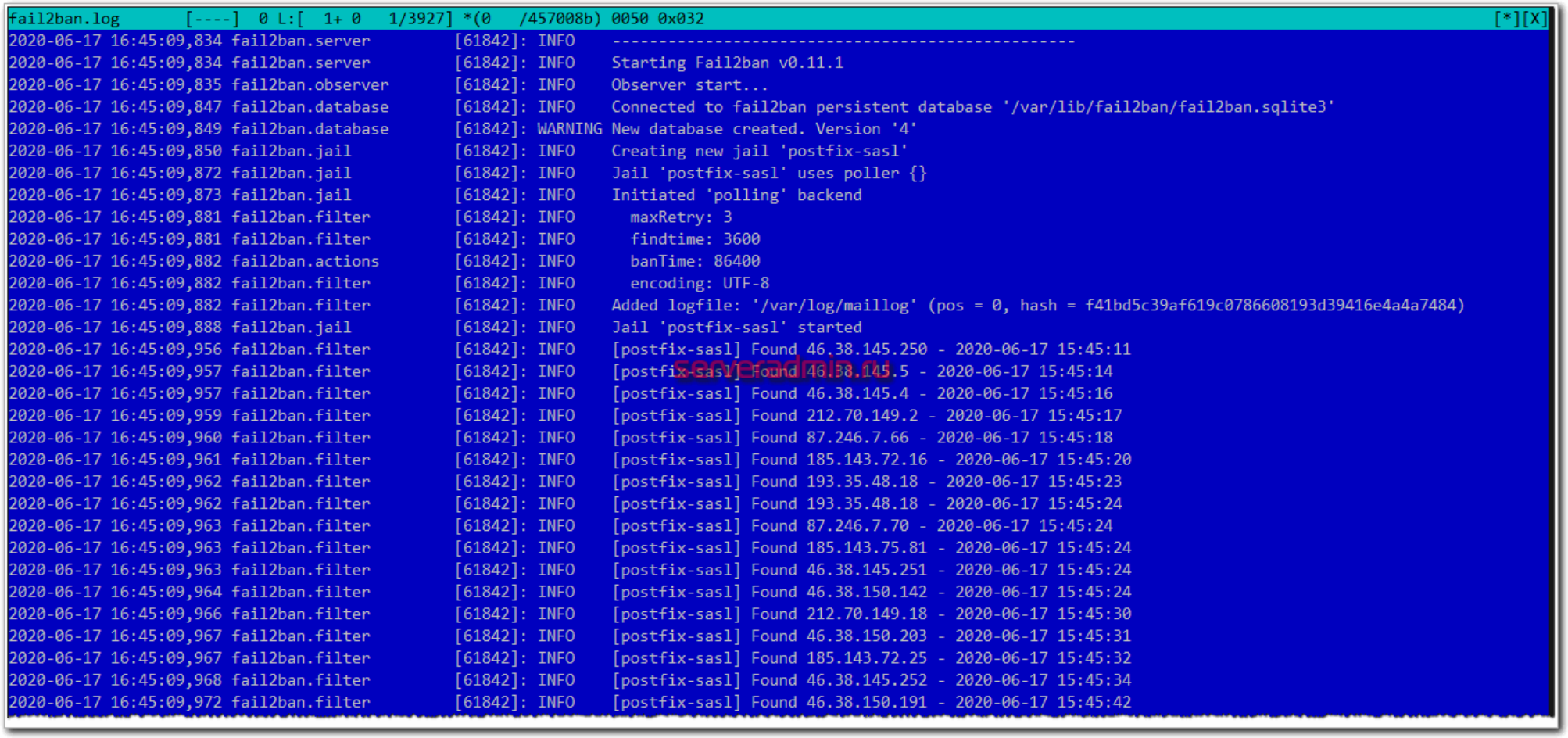
```
[postfix-sasl]
enabled = true
filter  = postfix-sasl
port    = smtp,465,submission,imap,imaps,pop3,pop3s
action  = iptables[name=Postfix-sals, port=smtp, protocol=tcp]
logpath = /var/log/maillog
bantime = 60m
maxretry = 3
findtime = 60m
```

Пояснять тут особо нечего и так все понятно. Настройка блокировки будет проверять лог файл и записи в нем за последние 60 минут. Если будут 3 совпадения с regexp из фильтра postfix-sasl, ip адрес будет забанен на 60 минут. Таким образом, список забаненных ip адресов будет не очень большой, так как большая часть адресов будет повторяться.

Запускаем fail2ban и добавляем в автозагрузку.

```
# systemctl enable — now fail2ban
```

Проверяем лог файл */var/log/fail2ban*.



Смотрим правила iptables.

```
# iptables -L -v -n
```

```
Chain f2b-Postfix-sals (1 references)
 pkts bytes target     prot opt in     out     source               destination
    8   480 REJECT     all  --  *      *       46.38.145.247        0.0.0.0/0            reject-with icmp-port-unreachable
   28  1600 REJECT     all  --  *      *       46.38.145.4          0.0.0.0/0            reject-with icmp-port-unreachable
   18  1080 REJECT     all  --  *      *       46.38.145.251        0.0.0.0/0            reject-with icmp-port-unreachable
   26  1496 REJECT     all  --  *      *       185.143.72.16        0.0.0.0/0            reject-with icmp-port-unreachable
   22  1320 REJECT     all  --  *      *       46.38.145.253        0.0.0.0/0            reject-with icmp-port-unreachable
   32  1856 REJECT     all  --  *      *       46.38.145.254        0.0.0.0/0            reject-with icmp-port-unreachable
   29  1660 REJECT     all  --  *      *       46.38.145.248        0.0.0.0/0            reject-with icmp-port-unreachable
   19  1140 REJECT     all  --  *      *       46.38.145.5          0.0.0.0/0            reject-with icmp-port-unreachable
   19  1140 REJECT     all  --  *      *       46.38.145.249        0.0.0.0/0            reject-with icmp-port-unreachable
   27  1620 REJECT     all  --  *      *       46.38.145.250        0.0.0.0/0            reject-with icmp-port-unreachable
   31  1812 REJECT     all  --  *      *       46.38.150.188        0.0.0.0/0            reject-with icmp-port-unreachable
   30  1720 REJECT     all  --  *      *       46.38.145.6          0.0.0.0/0            reject-with icmp-port-unreachable
   30  1720 REJECT     all  --  *      *       46.38.145.252        0.0.0.0/0            reject-with icmp-port-unreachable
   41  2388 REJECT     all  --  *      *       185.143.72.23        0.0.0.0/0            reject-with icmp-port-unreachable
   42  2448 REJECT     all  --  *      *       185.143.72.25        0.0.0.0/0            reject-with icmp-port-unreachable
   44  2690 REJECT     all  --  *      *       193.35.48.18         0.0.0.0/0            reject-with icmp-port-unreachable
   44  2568 REJECT     all  --  *      *       185.143.72.27        0.0.0.0/0            reject-with icmp-port-unreachable
   49  2860 REJECT     all  --  *      *       46.38.150.190        0.0.0.0/0            reject-with icmp-port-unreachable
```

serveradmin.ru

У вас должна появиться отдельная цепочка правил **f2b-Postfix-sals** с заблокированными ip адресами, которые добавил fail2ban. С защитой postfix с помощью fail2ban все. Переходим к Dovecot.

Защита dovecot с помощью fail2ban

Для защиты от перебора логинов в dovecot мы будем действовать аналогично. Единственное отличие, я буду использовать дефолтный фильтр для dovecot, который шел из коробки. Я его попробовал и он сразу заработал. Вот его содержимое.

```
# cat /etc/fail2ban/filter.d/dovecot.conf
```

```
[INCLUDES]

before = common.conf

[Definition]

_auth_worker = (?:dovecot: )?auth(?:-worker)?
_daemon = (?:dovecot(?:-auth)?|auth)

prefregex = ^%(__prefix_line)s(?:%(_auth_worker)s(?:\([^\)]+\))?: )?(?:%(__pam_auth)s(?:\(dovecot:auth\))?:
|(?:pop3|imap)-login: )?(?:Info: )?.+$

failregex = ^authentication failure; logname=\S* uid=\S* euid=\S* tty=dovecot ruser=\S* rhost=(?:\s+user=\S*)?\s*$
            ^(?:Aborted login|Disconnected)(?::(?: [^ \(]+)+)? \((?:auth failed, \d+ attempts(?: in \d+ secs)?|tried to
use (?:disabled|disallowed) \S+ auth|proxy dest auth failed)\):(?: user=<[^>]*>,)?(?: method=\S+,)? rip=(?:[^>]*(?:,
session=<\S+>)?)\s*$
            ^pam\(\S+,(?:,\S*)?\): pam_authenticate\(\) failed: (?:User not known to the underlying authentication
module: \d+ Time\(s\)|Authentication failure \(password mismatch\?\)|Permission denied)\s*$
            ^[a-z\-]{3,15}\(\S*,(?:,\S*)?\): (?:unknown user|invalid credentials|Password mismatch)\s*$
            <mdre->

mdre-aggressive = ^(?:Aborted login|Disconnected)(?::(?: [^ \(]+)+)? \((?:no auth attempts|disconnected before auth was
ready,|client didn't finish \S+ auth,)(?: (?:in|waited) \d+ secs)?\):(?: user=<[^>]*>,)?(?: method=\S+,)?
rip=(?:[^>]*(?:, session=<\S+>)?)\s*$

mdre-normal =

mode = normal
```

```
ignoreregex =

journalmatch = _SYSTEMD_UNIT=dovecot.service

datepattern = {^LN-BEG}TAI64N
              {^LN-BEG}
```

Полный лог dovecot у меня располагается в файле */var/log/dovecot/info.log*. В параметрах dovecot у меня добавлено:

```
auth_verbose = yes
```

С этим параметром у вас дополнительно в логе будут следующие строки:

```
Jun 17 04:14:11 auth-worker(175697): Info: sql(mcm@mail.ru,87.246.7.66): unknown user
```

По дефолту их нет, а они помогут в нашей задаче по защите от перебора паролей учетных записей dovecot. Проверим работу фильтра.

```
# fail2ban-regex /var/log/dovecot/info.log /etc/fail2ban/filter.d/dovecot.conf
```

```
Running tests
=============

Use   failregex filter file : dovecot, basedir: /etc/fail2ban
Use      datepattern : Default Detectors
Use         log file : /var/log/dovecot/info.log
Use         encoding : UTF-8


Results
=======

Failregex: 26849 total
|-  #) [# of hits] regular expression
|   2) [1178] ^(?:Aborted login|Disconnected)(?::(?: [^ \(]+)+)? \((?:auth failed, \d+ attempts(?: in \d+ secs)?|tried to use (?:disabled|disallowed) \S+ auth|proxy d
est auth failed)\):(?: user=<<F-USER>[^>]*</F-USER>>,)?(?: method=\S+,)? rip=<HOST>(?:[^>]*(?:, session=<\S+>)?)\s*$
|   4) [25671] ^[a-z\-]{3,15}\(\S*,<HOST>(?:,\S*)?\): (?:unknown user|invalid credentials|Password mismatch)\s*$
`-

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [35670] {^LN-BEG}(?:DAY )?MON Day %k:Minute:Second(?:\.Microseconds)?(?: ExYear)?
`-

Lines: 35670 lines, 0 ignored, 26849 matched, 8821 missed
[processed in 5.77 sec]
```

serveradmin.ru

Сработок очень много. Судя по всему, фильтр работает. Добавляем в конфиг *jail.conf*.

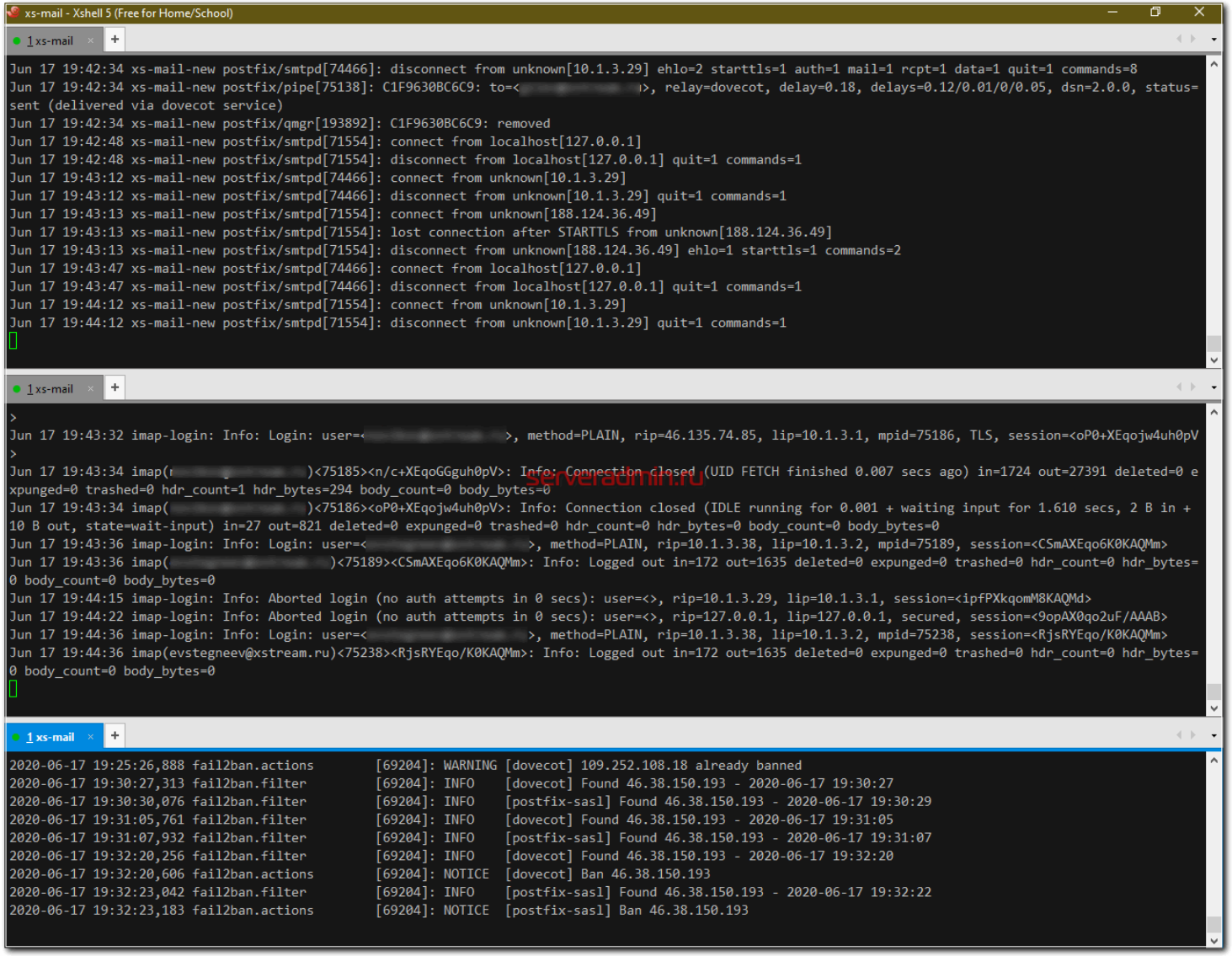
```
[dovecot]
enabled = true
filter  = dovecot
port    = imap,imaps,pop3,pop3s
action  = iptables[name=Dovecot, port=imap, protocol=tcp]
```

```
logpath = /var/log/dovecot/info.log
bantime = 60m
maxretry = 3
findtime = 60m
```

Здесь ничего нового. Все то же самое, что мы сделали выше. Перезапускайте fail2ban и проверяйте его работу. В логе должна появиться информация по работе данного jail'а. А в правилах iptables новая цепочка Dovecot.

Отладка работы fail2ban

После добавления правил блокировки ip адресов с помощью fail2ban, я некоторое время наблюдаю за сервером, чтобы проверить правильность работы. Для этого делаю вот такое окно в отдельном мониторе и наблюдаю некоторое время.


xs-mail - Xshell 5 (Free for Home/School)
1 xs-mail
Jun 17 19:42:34 xs-mail-new postfix/smtpd[74466]: disconnect from unknown[10.1.3.29] ehlo=2 starttls=1 auth=1 mail=1 rcpt=1 data=1 quit=1 commands=8
Jun 17 19:42:34 xs-mail-new postfix/pipe[75138]: C1F9630BC6C9: to=<[redacted]>, relay=dovecot, delay=0.18, delays=0.12/0.01/0/0.05, dsn=2.0.0, status=sent (delivered via dovecot service)
Jun 17 19:42:34 xs-mail-new postfix/qmgr[193892]: C1F9630BC6C9: removed
Jun 17 19:42:48 xs-mail-new postfix/smtpd[71554]: connect from localhost[127.0.0.1]
Jun 17 19:42:48 xs-mail-new postfix/smtpd[71554]: disconnect from localhost[127.0.0.1] quit=1 commands=1
Jun 17 19:43:12 xs-mail-new postfix/smtpd[74466]: connect from unknown[10.1.3.29]
Jun 17 19:43:12 xs-mail-new postfix/smtpd[74466]: disconnect from unknown[10.1.3.29] quit=1 commands=1
Jun 17 19:43:13 xs-mail-new postfix/smtpd[71554]: connect from unknown[188.124.36.49]
Jun 17 19:43:13 xs-mail-new postfix/smtpd[71554]: lost connection after STARTTLS from unknown[188.124.36.49]
Jun 17 19:43:13 xs-mail-new postfix/smtpd[71554]: disconnect from unknown[188.124.36.49] ehlo=1 starttls=1 commands=2
Jun 17 19:43:47 xs-mail-new postfix/smtpd[74466]: connect from localhost[127.0.0.1]
Jun 17 19:43:47 xs-mail-new postfix/smtpd[74466]: disconnect from localhost[127.0.0.1] quit=1 commands=1
Jun 17 19:44:12 xs-mail-new postfix/smtpd[71554]: connect from unknown[10.1.3.29]
Jun 17 19:44:12 xs-mail-new postfix/smtpd[71554]: disconnect from unknown[10.1.3.29] quit=1 commands=1
1 xs-mail
>
Jun 17 19:43:32 imap-login: Info: Login: user=<[redacted]>, method=PLAIN, rip=46.135.74.85, lip=10.1.3.1, mpid=75186, TLS, session=<oP0+XEqojw4uh0pV
>
Jun 17 19:43:34 imap([redacted])<75185><n/c+XEqoGGguh0pV>: Info: Connection closed (UID FETCH finished 0.007 secs ago) in=1724 out=27391 deleted=0 expunged=0 trashed=0 hdr_count=1 hdr_bytes=294 body_count=0 body_bytes=0
Jun 17 19:43:34 imap([redacted])<75186><oP0+XEqojw4uh0pV>: Info: Connection closed (IDLE running for 0.001 + waiting input for 1.610 secs, 2 B in + 10 B out, state=wait-input) in=27 out=821 deleted=0 expunged=0 trashed=0 hdr_count=0 hdr_bytes=0 body_count=0 body_bytes=0
Jun 17 19:43:36 imap-login: Info: Login: user=<[redacted]>, method=PLAIN, rip=10.1.3.38, lip=10.1.3.2, mpid=75189, session=<CSmAXEqo6K0KAQMm>
Jun 17 19:43:36 imap([redacted])<75189><CSmAXEqo6K0KAQMm>: Info: Logged out in=172 out=1635 deleted=0 expunged=0 trashed=0 hdr_count=0 hdr_bytes=0 body_count=0 body_bytes=0
Jun 17 19:44:15 imap-login: Info: Aborted login (no auth attempts in 0 secs): user=<>, rip=10.1.3.29, lip=10.1.3.1, session=<ipfPXkqomM8KAQMd>
Jun 17 19:44:22 imap-login: Info: Aborted login (no auth attempts in 0 secs): user=<>, rip=127.0.0.1, lip=127.0.0.1, secured, session=<9opAX0qo2uF/AAAB>
Jun 17 19:44:36 imap-login: Info: Login: user=<[redacted]>, method=PLAIN, rip=10.1.3.38, lip=10.1.3.2, mpid=75238, session=<RjsRYEqo/K0KAQMm>
Jun 17 19:44:36 imap(evstegneev@xstream.ru)<75238><RjsRYEqo/K0KAQMm>: Info: Logged out in=172 out=1635 deleted=0 expunged=0 trashed=0 hdr_count=0 hdr_bytes=0 body_count=0 body_bytes=0
1 xs-mail
2020-06-17 19:25:26,888 fail2ban.actions [69204]: WARNING [dovecot] 109.252.108.18 already banned
2020-06-17 19:30:27,313 fail2ban.filter [69204]: INFO [dovecot] Found 46.38.150.193 - 2020-06-17 19:30:27
2020-06-17 19:30:30,076 fail2ban.filter [69204]: INFO [postfix-sasl] Found 46.38.150.193 - 2020-06-17 19:30:29
2020-06-17 19:31:05,761 fail2ban.filter [69204]: INFO [dovecot] Found 46.38.150.193 - 2020-06-17 19:31:05
2020-06-17 19:31:07,932 fail2ban.filter [69204]: INFO [postfix-sasl] Found 46.38.150.193 - 2020-06-17 19:31:07
2020-06-17 19:32:20,256 fail2ban.filter [69204]: INFO [dovecot] Found 46.38.150.193 - 2020-06-17 19:32:20
2020-06-17 19:32:20,606 fail2ban.actions [69204]: NOTICE [dovecot] Ban 46.38.150.193
2020-06-17 19:32:23,042 fail2ban.filter [69204]: INFO [postfix-sasl] Found 46.38.150.193 - 2020-06-17 19:32:22
2020-06-17 19:32:23,183 fail2ban.actions [69204]: NOTICE [postfix-sasl] Ban 46.38.150.193

Здесь открыт лог postfix, dovecot и fail2ban. Если вижу, что правила отрабатываются корректно, завершаю настройку. На этом этапе могут быть заблокированы валидные ip адреса пользователей, у которых одна из учеток указана с неверным паролем. В итоге он банится по ip и у него вообще перестает работать вся почта. Если это локальные пользователи, то можно всю их подсеть добавить в доверенные, но я бы не рекомендовал так делать. В этом случае вы не узнаете, что кто-то вас перебирает из локальной сети. А это случается не редко.

Удалить ip адрес из заблокированных fail2ban

Вам может понадобиться вручную удалить какой-то ip адрес из списка заблокированных fail2ban. Часто в блок попадают ip адреса при настройке учетной записи у пользователя. Пароль может быть перепутан или копироваться с лишними символами. Всякое бывает.

Можно напрямую удалить правило через iptables. Но это будет не очень правильно. Лучше воспользоваться готовым инструментом от fail2ban для удаления ip адресов из блокировки.

Смотрим список активных jail'ов.

```
# fail2ban-client status
Status
|- Number of jail:      2
`- Jail list:   dovecot, postfix-sasl
```

Смотрим список заблокированный ip адресов в jail.

```
# fail2ban-client status postfix-sasl
Status for the jail: postfix-sasl
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     169
|  `- File list:        /var/log/maillog
`- Actions
   |- Currently banned: 27
```

```
   |- Total banned:     86
   `- Banned IP list:   46.38.150.193 87.246.7.66 212.70.149.2 141.98.80.150 46.38.150.203 185.143.75.153 212.70.149.18
46.38.150.191 87.246.7.70 185.143.75.81 185.143.72.34 46.38.150.142 46.38.150.190 185.143.72.27 185.143.72.25
185.143.72.23 46.38.145.6 46.38.145.252 46.38.150.188 46.38.145.249 46.38.145.5 46.38.145.250 46.38.145.248 46.38.145.254
46.38.145.253 185.143.72.16 46.38.145.251
```

Теперь разбаним один из адресов в fail2ban:

```
# fail2ban-client set postfix-sasl unbanip 46.38.150.193
1
```

Если получите одну из этих ошибок:

```
2020-06-17 20:15:14,809 fail2ban [77578]: ERROR NOK: ('Invalid command (no get action or not yet implemented)',)
2020-06-17 20:13:02,078 fail2ban [77464]: ERROR NOK: ("Invalid command '46.38.150.193' (no set action or not yet
implemented)",)
2020-06-17 20:11:48,132 fail2ban [77382]: ERROR   NOK: ('list index out of range',)
```

Значит у вас более старая версия fail2ban. Тогда нужно использовать другую команду для разбана ip адреса:

```
# fail2ban-client get postfix-sasl actionunban 46.38.150.193
```

Для проверки можете посмотреть на цепочки правил iptables, чтобы убедиться, в том, что адреса реально удалены из блокировки.

Заключение

> Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

На практике правила в fail2ban для dovecot особо не нужны. Пробивкой учетных записей занимаются боты, которые сразу пробивают smtp и imap порты. Все эти боты первым делом попадают в блокировку postfix и до правил dovecot просто не доходят. Но для полноты картины можно оставить и их, хотя бы для того, чтобы выявлять сотрудников с настроенными неактивными учетками.

С помощью fail2ban можно так же банить различные почтовые серверы, которые не проходят встроенные проверки postfix на спам. Но я обычно этого не делаю, так как бывают ложные срабатывания. Потом приходится лишнее время тратить на разбор полетов, так как он усложняется. Так стоит делать, если левые коннекты реально замедляют работу почтового сервера. Обычно это не добавляет каких-то серьезных проблем, в отличие от перебора паролей.

Онлайн курс по Linux

Если у вас есть желание научиться строить и поддерживать высокодоступные и надежные системы, рекомендую познакомиться с **онлайн-курсом «Администратор Linux»** в OTUS. Курс не для новичков, для поступления нужны базовые знания по сетям и установке Linux на виртуалку. Обучение длится 5 месяцев, после чего успешные выпускники курса смогут пройти собеседования у партнеров. Что даст вам этот курс:

- Знание архитектуры Linux.
- Освоение современных методов и инструментов анализа и обработки данных.
- Умение подбирать конфигурацию под необходимые задачи, управлять процессами и обеспечивать безопасность системы.
- Владение основными рабочими инструментами системного администратора.
- Понимание особенностей развертывания, настройки и обслуживания сетей, построенных на базе Linux.
- Способность быстро решать возникающие проблемы и обеспечивать стабильную и бесперебойную работу системы.

Проверьте себя на вступительном тесте и смотрите подробнее программу по .

Помогла статья? Подписывайся на telegram канал автора

Анонсы всех статей, плюс много другой полезной и интересной информации, которая не попадает на сайт.