Лабораторная работа №16

Базовая защита от атак типа «brute force»

Спелов А. Н.

17 декабря 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Спелов Андрей Николаевич
- НПИбд-02-23 Студ. билет: 1132231839
- Российский университет дружбы народов
- 1132231839@pfur.ru

Вводная часть

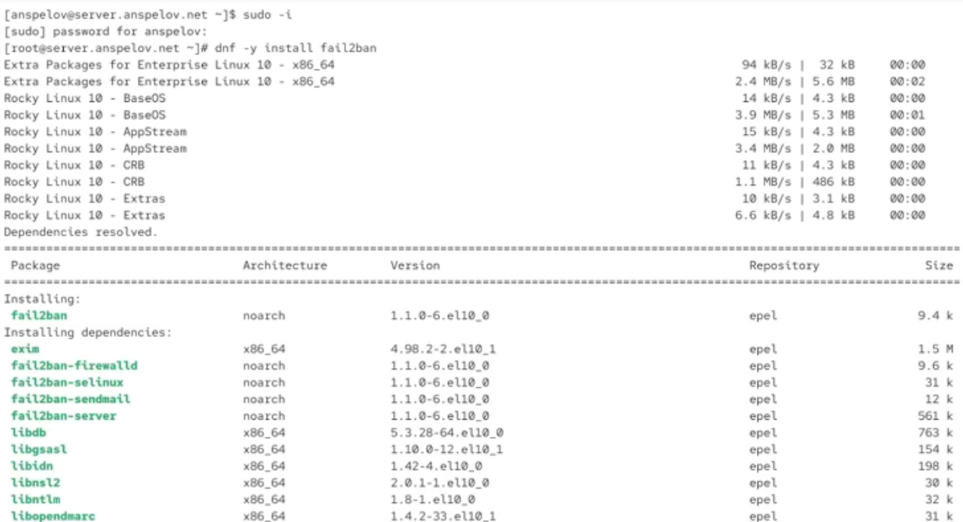
Цель работы

- Целью данной работы является приобретение навыков настройки сервера NFS для удалённого доступа к ресурсам.

Основная часть

Защита с помощью Fail2ban

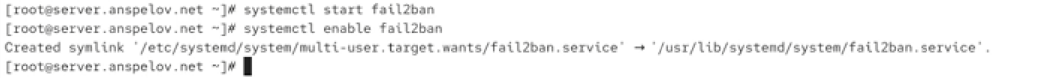
- Установка на сервере fail2ban.



```
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]# dnf -y install fail2ban
Extra Packages for Enterprise Linux 10 - x86_64                                                           94 kB/s |  32 kB     00:00
Extra Packages for Enterprise Linux 10 - x86_64                                                          2.4 MB/s | 5.6 MB     00:02
Rocky Linux 10 - BaseOS                                                                                   14 kB/s | 4.3 kB     00:00
Rocky Linux 10 - BaseOS                                                                                  3.9 MB/s | 5.3 MB     00:01
Rocky Linux 10 - AppStream                                                                                15 kB/s | 4.3 kB     00:00
Rocky Linux 10 - AppStream                                                                               3.4 MB/s | 2.0 MB     00:00
Rocky Linux 10 - CRB                                                                                      11 kB/s | 4.3 kB     00:00
Rocky Linux 10 - CRB                                                                                     1.1 MB/s | 486 kB     00:00
Rocky Linux 10 - Extras                                                                                   10 kB/s | 3.1 kB     00:00
Rocky Linux 10 - Extras                                                                                  6.6 kB/s | 4.8 kB     00:00
Dependencies resolved.
========================================================================================================================================
 Package                          Architecture        Version                                     Repository                Size
========================================================================================================================================
Installing:
 fail2ban                         noarch              1.1.0-6.el10_0                              epel                     9.4 k
Installing dependencies:
 exim                             x86_64              4.98.2-2.el10_1                             epel                     1.5 M
 fail2ban-firewalld               noarch              1.1.0-6.el10_0                              epel                     9.6 k
 fail2ban-selinux                 noarch              1.1.0-6.el10_0                              epel                      31 k
 fail2ban-sendmail                noarch              1.1.0-6.el10_0                              epel                      12 k
 fail2ban-server                  noarch              1.1.0-6.el10_0                              epel                     561 k
 libdb                            x86_64              5.3.28-64.el10_0                            epel                     763 k
 libgsasl                         x86_64              1.10.0-12.el10_1                            epel                     154 k
 libidn                           x86_64              1.42-4.el10_0                               epel                     198 k
 libnsl2                          x86_64              2.0.1-1.el10_0                              epel                      30 k
 libntlm                          x86_64              1.8-1.el10_0                                epel                      32 k
 libopendmarc                     x86_64              1.4.2-33.el10_1                             epel                      31 k
```

Защита с помощью Fail2ban

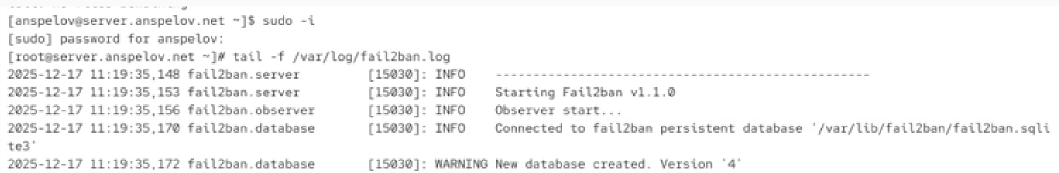
- Запуск сервера fail2ban.



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

Защита с помощью Fail2ban

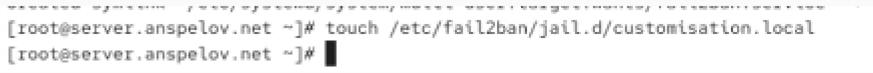
- Запуск просмотра в дополнительном терминале журнала событий fail2ban.



```
[anspelov@server.anspelov.net ~]$ sudo -i
[sudo] password for anspelov:
[root@server.anspelov.net ~]# tail -f /var/log/fail2ban.log
2025-12-17 11:19:35,148 fail2ban.server         [15030]: INFO    --------------------------------------------------
2025-12-17 11:19:35,153 fail2ban.server         [15030]: INFO    Starting Fail2ban v1.1.0
2025-12-17 11:19:35,156 fail2ban.observer       [15030]: INFO    Observer start...
2025-12-17 11:19:35,170 fail2ban.database       [15030]: INFO    Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sqli
te3'
2025-12-17 11:19:35,172 fail2ban.database       [15030]: WARNING New database created. Version '4'
```

Защита с помощью Fail2ban

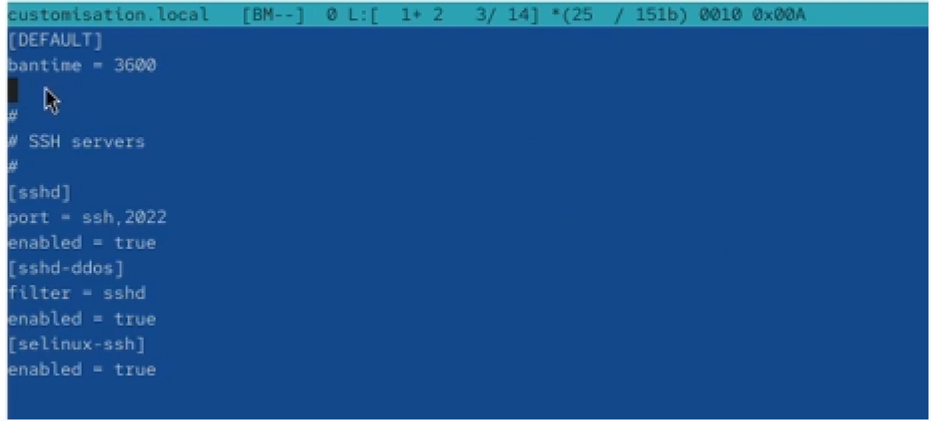
- Создание файла с локальной конфигурацией fail2ban.



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

Защита с помощью Fail2ban

- Настройка в файле /etc/fail2ban/jail.d/customisation.local времени блокирования на 1 час и включение защиты SSH.

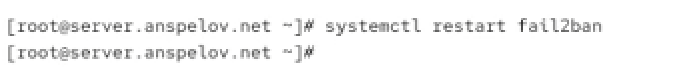


```
customisation.local   [BM--]  0 L:[  1+ 2   3/ 14] *(25  / 151b) 0010 0x00A
[DEFAULT]
bantime = 3600

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

Защита с помощью Fail2ban

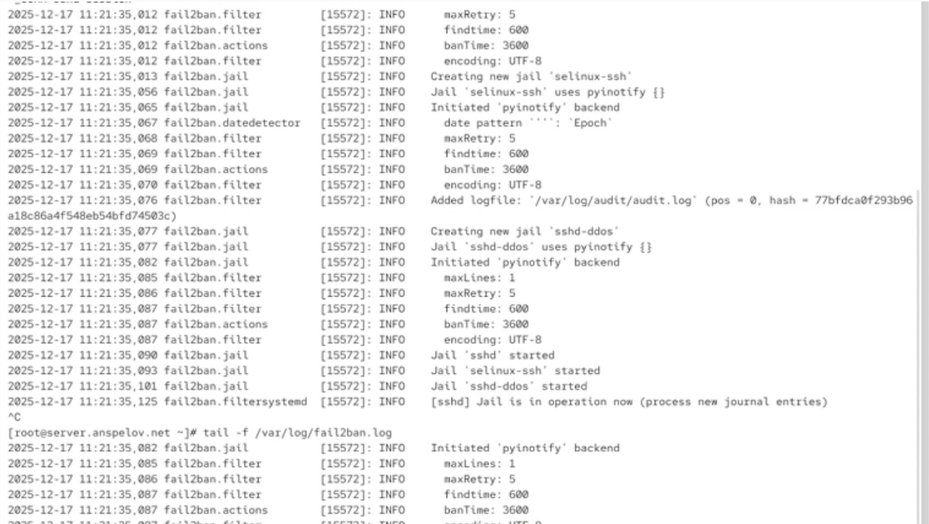
- Перезапуск fail2ban.



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

Защита с помощью Fail2ban

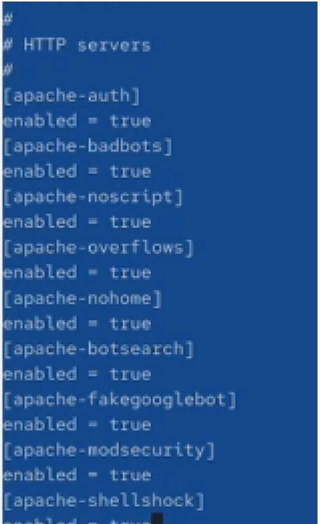
- Просмотр журнала событий.



```
2025-12-17 11:21:35,012 fail2ban.filter         [15572]: INFO      maxRetry: 5
2025-12-17 11:21:35,012 fail2ban.filter         [15572]: INFO      findtime: 600
2025-12-17 11:21:35,012 fail2ban.actions        [15572]: INFO      banTime: 3600
2025-12-17 11:21:35,012 fail2ban.filter         [15572]: INFO      encoding: UTF-8
2025-12-17 11:21:35,013 fail2ban.jail           [15572]: INFO    Creating new jail 'selinux-ssh'
2025-12-17 11:21:35,056 fail2ban.jail           [15572]: INFO    Jail 'selinux-ssh' uses pyinotify {}
2025-12-17 11:21:35,065 fail2ban.jail           [15572]: INFO    Initiated 'pyinotify' backend
2025-12-17 11:21:35,067 fail2ban.datedetector   [15572]: INFO      date pattern `''`: `Epoch`
2025-12-17 11:21:35,068 fail2ban.filter         [15572]: INFO      maxRetry: 5
2025-12-17 11:21:35,069 fail2ban.filter         [15572]: INFO      findtime: 600
2025-12-17 11:21:35,069 fail2ban.actions        [15572]: INFO      banTime: 3600
2025-12-17 11:21:35,070 fail2ban.filter         [15572]: INFO      encoding: UTF-8
2025-12-17 11:21:35,076 fail2ban.filter         [15572]: INFO    Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 77bfdca0f293b96
a18c86a4f548eb54bfd74503c)
2025-12-17 11:21:35,077 fail2ban.jail           [15572]: INFO    Creating new jail 'sshd-ddos'
2025-12-17 11:21:35,077 fail2ban.jail           [15572]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-17 11:21:35,082 fail2ban.jail           [15572]: INFO    Initiated 'pyinotify' backend
2025-12-17 11:21:35,085 fail2ban.filter         [15572]: INFO      maxLines: 1
2025-12-17 11:21:35,086 fail2ban.filter         [15572]: INFO      maxRetry: 5
2025-12-17 11:21:35,087 fail2ban.filter         [15572]: INFO      findtime: 600
2025-12-17 11:21:35,087 fail2ban.actions        [15572]: INFO      banTime: 3600
2025-12-17 11:21:35,087 fail2ban.filter         [15572]: INFO      encoding: UTF-8
2025-12-17 11:21:35,090 fail2ban.jail           [15572]: INFO    Jail 'sshd' started
2025-12-17 11:21:35,093 fail2ban.jail           [15572]: INFO    Jail 'selinux-ssh' started
2025-12-17 11:21:35,101 fail2ban.jail           [15572]: INFO    Jail 'sshd-ddos' started
2025-12-17 11:21:35,125 fail2ban.filtersystemd  [15572]: INFO    [sshd] Jail is in operation now (process new journal entries)
^C
[root@server.anspelov.net ~]# tail -f /var/log/fail2ban.log
2025-12-17 11:21:35,082 fail2ban.jail           [15572]: INFO    Initiated 'pyinotify' backend
2025-12-17 11:21:35,085 fail2ban.filter         [15572]: INFO      maxLines: 1
2025-12-17 11:21:35,086 fail2ban.filter         [15572]: INFO      maxRetry: 5
2025-12-17 11:21:35,087 fail2ban.filter         [15572]: INFO      findtime: 600
2025-12-17 11:21:35,087 fail2ban.actions        [15572]: INFO      banTime: 3600
2025-12-17 11:21:35,087 fail2ban.filter         [15572]: INFO      encoding: UTF-8
```

Защита с помощью Fail2ban

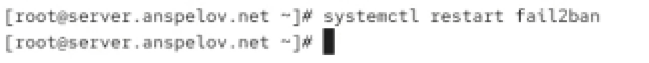
- Включение защиты HTTP в файле /etc/fail2ban/jail.d/customisation.local.



```
#
# 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
```

Защита с помощью Fail2ban

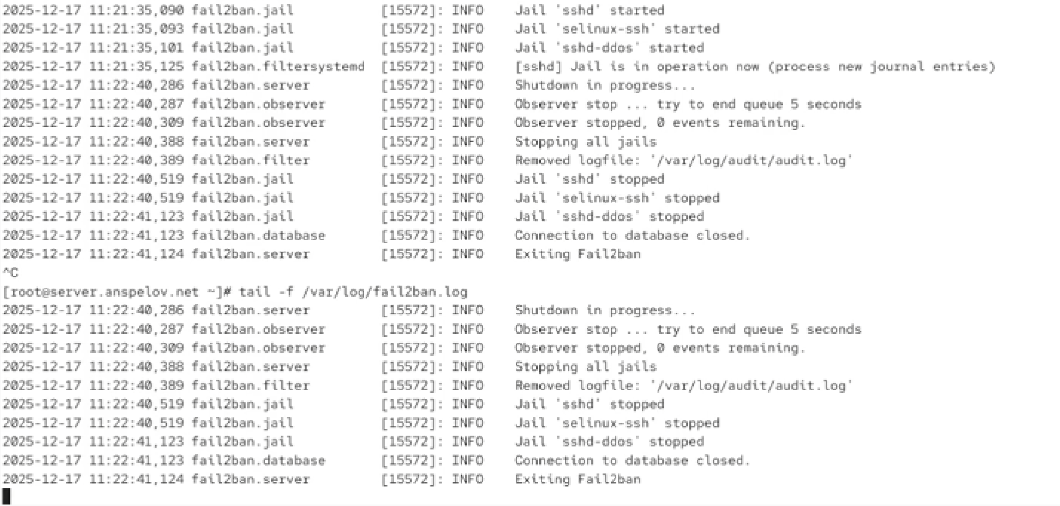
- Перезапуск fail2ban.



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

Защита с помощью Fail2ban

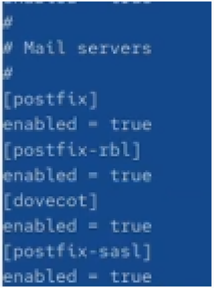
- Просмотр журнала событий.



```
2025-12-17 11:21:35,090 fail2ban.jail           [15572]: INFO    Jail 'sshd' started
2025-12-17 11:21:35,093 fail2ban.jail           [15572]: INFO    Jail 'selinux-ssh' started
2025-12-17 11:21:35,101 fail2ban.jail           [15572]: INFO    Jail 'sshd-ddos' started
2025-12-17 11:21:35,125 fail2ban.filtersystemd  [15572]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-12-17 11:22:40,286 fail2ban.server         [15572]: INFO    Shutdown in progress...
2025-12-17 11:22:40,287 fail2ban.observer       [15572]: INFO    Observer stop ... try to end queue 5 seconds
2025-12-17 11:22:40,309 fail2ban.observer       [15572]: INFO    Observer stopped, 0 events remaining.
2025-12-17 11:22:40,388 fail2ban.server         [15572]: INFO    Stopping all jails
2025-12-17 11:22:40,389 fail2ban.filter         [15572]: INFO    Removed logfile: '/var/log/audit/audit.log'
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'sshd' stopped
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'selinux-ssh' stopped
2025-12-17 11:22:41,123 fail2ban.jail           [15572]: INFO    Jail 'sshd-ddos' stopped
2025-12-17 11:22:41,123 fail2ban.database       [15572]: INFO    Connection to database closed.
2025-12-17 11:22:41,124 fail2ban.server         [15572]: INFO    Exiting Fail2ban
^C
[root@server.anspelov.net ~]# tail -f /var/log/fail2ban.log
2025-12-17 11:22:40,286 fail2ban.server         [15572]: INFO    Shutdown in progress...
2025-12-17 11:22:40,287 fail2ban.observer       [15572]: INFO    Observer stop ... try to end queue 5 seconds
2025-12-17 11:22:40,309 fail2ban.observer       [15572]: INFO    Observer stopped, 0 events remaining.
2025-12-17 11:22:40,388 fail2ban.server         [15572]: INFO    Stopping all jails
2025-12-17 11:22:40,389 fail2ban.filter         [15572]: INFO    Removed logfile: '/var/log/audit/audit.log'
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'sshd' stopped
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'selinux-ssh' stopped
2025-12-17 11:22:41,123 fail2ban.jail           [15572]: INFO    Jail 'sshd-ddos' stopped
2025-12-17 11:22:41,123 fail2ban.database       [15572]: INFO    Connection to database closed.
2025-12-17 11:22:41,124 fail2ban.server         [15572]: INFO    Exiting Fail2ban
```

Защита с помощью Fail2ban

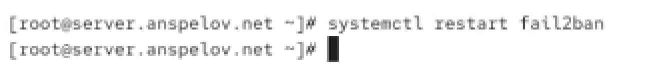
- Включение защиты почты в файле /etc/fail2ban/jail.d/customisation.local.



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

Защита с помощью Fail2ban

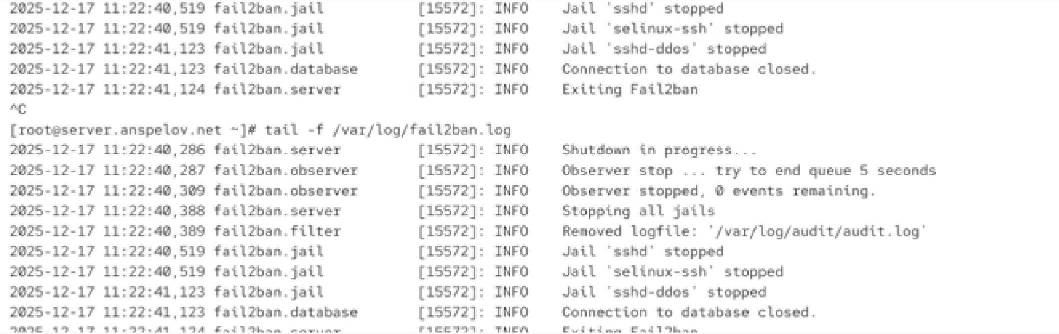
- Повторный перезапуск fail2ban.



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

Защита с помощью Fail2ban

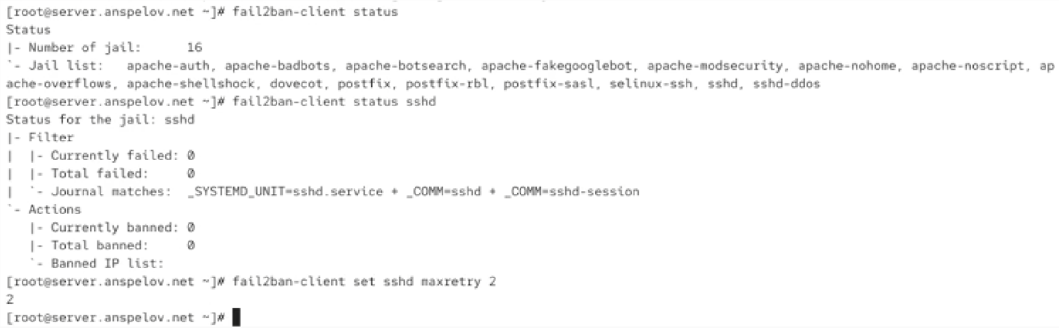
- Просмотр журнала событий.



```
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'sshd' stopped
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'selinux-ssh' stopped
2025-12-17 11:22:41,123 fail2ban.jail           [15572]: INFO    Jail 'sshd-ddos' stopped
2025-12-17 11:22:41,123 fail2ban.database       [15572]: INFO    Connection to database closed.
2025-12-17 11:22:41,124 fail2ban.server         [15572]: INFO    Exiting Fail2ban
^C
[root@server.anspelov.net ~]# tail -f /var/log/fail2ban.log
2025-12-17 11:22:40,286 fail2ban.server         [15572]: INFO    Shutdown in progress...
2025-12-17 11:22:40,287 fail2ban.observer       [15572]: INFO    Observer stop ... try to end queue 5 seconds
2025-12-17 11:22:40,309 fail2ban.observer       [15572]: INFO    Observer stopped, 0 events remaining.
2025-12-17 11:22:40,388 fail2ban.server         [15572]: INFO    Stopping all jails
2025-12-17 11:22:40,389 fail2ban.filter         [15572]: INFO    Removed logfile: '/var/log/audit/audit.log'
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'sshd' stopped
2025-12-17 11:22:40,519 fail2ban.jail           [15572]: INFO    Jail 'selinux-ssh' stopped
2025-12-17 11:22:41,123 fail2ban.jail           [15572]: INFO    Jail 'sshd-ddos' stopped
2025-12-17 11:22:41,123 fail2ban.database       [15572]: INFO    Connection to database closed.
2025-12-17 11:22:41,124 fail2ban.server         [15572]: INFO    Exiting Fail2ban
```

Проверка работы Fail2ban

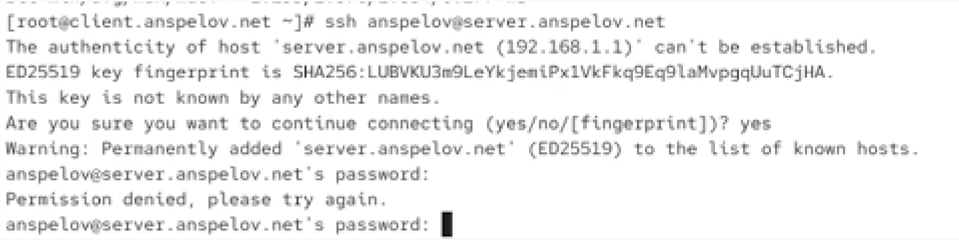
- Просмотр на сервере статуса fail2ban, статуса защиты SSH в fail2ban и установка максимального количества ошибок для SSH (=2).



```
[root@server.anspelov.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, ap
ache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.anspelov.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 + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.anspelov.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.anspelov.net ~]# █
```

Проверка работы Fail2ban

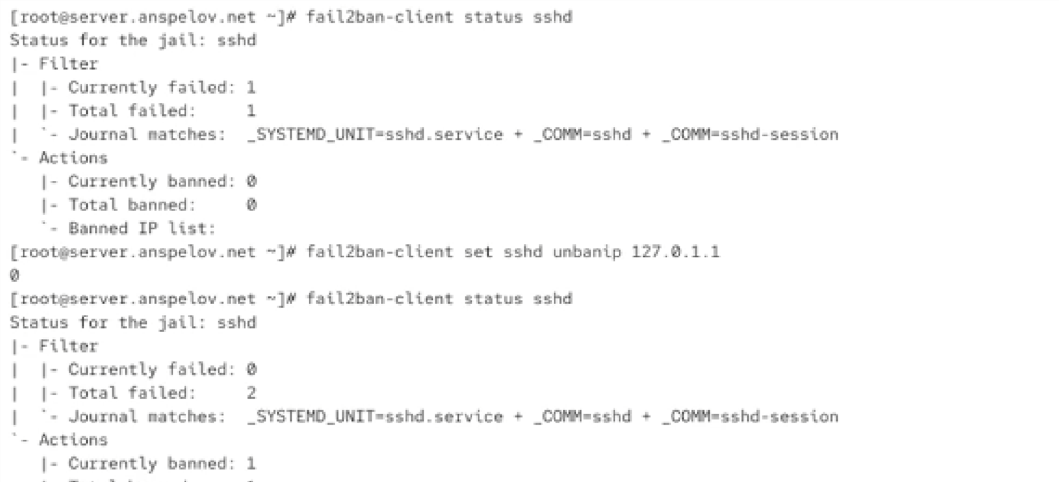
- Попытка зайти с клиента по SSH на сервер с неправильным паролем.



```
[root@client.anspelov.net ~]# ssh anspelov@server.anspelov.net
The authenticity of host 'server.anspelov.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:LUBVKU3m9LeYkjemiPx1VkFkq9Eq9laMvpgqUuTCjHA.
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.anspelov.net' (ED25519) to the list of known hosts.
anspelov@server.anspelov.net's password:
Permission denied, please try again.
anspelov@server.anspelov.net's password: 
```

Проверка работы Fail2ban

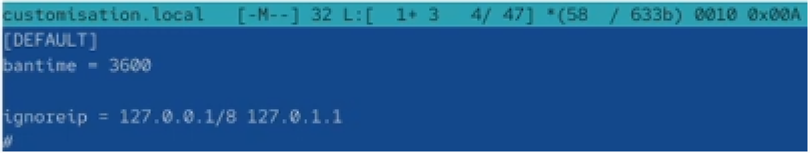
- Просмотр на сервере статуса защиты SSH, разблокировка IP-адреса клиента и повторная проверка.



```
[root@server.anspelov.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 + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[root@server.anspelov.net ~]# fail2ban-client set sshd unbanip 127.0.1.1
0
[root@server.anspelov.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 + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
```

Проверка работы Fail2ban

- Добавление в раздел по умолчанию игнорирование адреса клиента в конфигурационном файле /etc/fail2ban/jail.d/customisation.local.

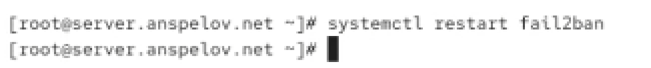


```
customisation.local   [-M--] 32 L:[  1+ 3   4/ 47] *(58  / 633b) 0010 0x00A
[DEFAULT]
bantime = 3600

ignoreip = 127.0.0.1/8 127.0.1.1
#
```

Проверка работы Fail2ban

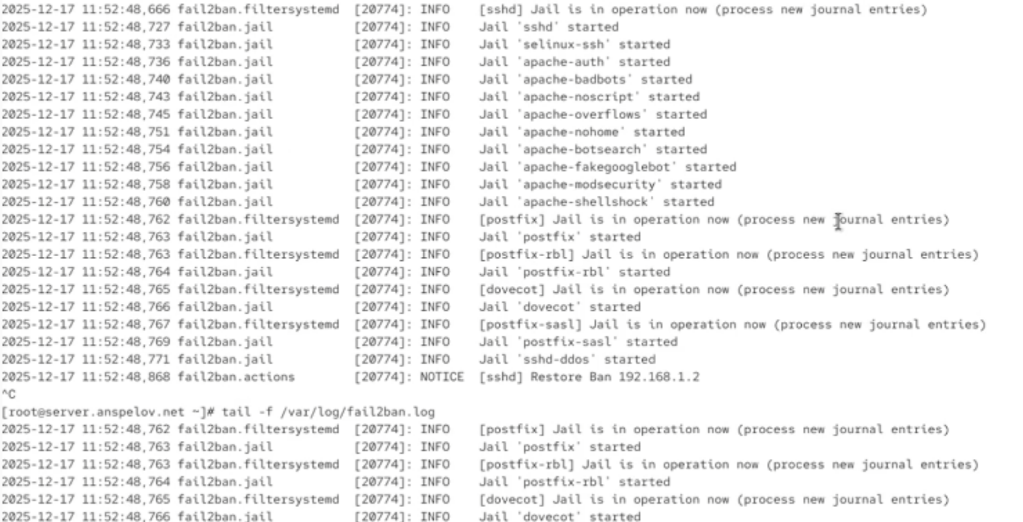
- Перезапуск fail2ban.



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

Проверка работы Fail2ban

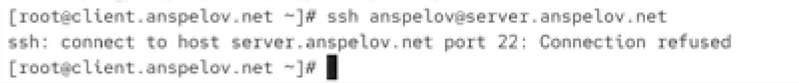
- Просмотр журнала событий.



```
2025-12-17 11:52:48,666 fail2ban.filtersystemd  [20774]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,727 fail2ban.jail           [20774]: INFO    Jail 'sshd' started
2025-12-17 11:52:48,733 fail2ban.jail           [20774]: INFO    Jail 'selinux-ssh' started
2025-12-17 11:52:48,736 fail2ban.jail           [20774]: INFO    Jail 'apache-auth' started
2025-12-17 11:52:48,740 fail2ban.jail           [20774]: INFO    Jail 'apache-badbots' started
2025-12-17 11:52:48,743 fail2ban.jail           [20774]: INFO    Jail 'apache-noscript' started
2025-12-17 11:52:48,745 fail2ban.jail           [20774]: INFO    Jail 'apache-overflows' started
2025-12-17 11:52:48,751 fail2ban.jail           [20774]: INFO    Jail 'apache-nohome' started
2025-12-17 11:52:48,754 fail2ban.jail           [20774]: INFO    Jail 'apache-botsearch' started
2025-12-17 11:52:48,756 fail2ban.jail           [20774]: INFO    Jail 'apache-fakegooglebot' started
2025-12-17 11:52:48,758 fail2ban.jail           [20774]: INFO    Jail 'apache-modsecurity' started
2025-12-17 11:52:48,760 fail2ban.jail           [20774]: INFO    Jail 'apache-shellshock' started
2025-12-17 11:52:48,762 fail2ban.filtersystemd  [20774]: INFO    [postfix] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,763 fail2ban.jail           [20774]: INFO    Jail 'postfix' started
2025-12-17 11:52:48,763 fail2ban.filtersystemd  [20774]: INFO    [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,764 fail2ban.jail           [20774]: INFO    Jail 'postfix-rbl' started
2025-12-17 11:52:48,765 fail2ban.filtersystemd  [20774]: INFO    [dovecot] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,766 fail2ban.jail           [20774]: INFO    Jail 'dovecot' started
2025-12-17 11:52:48,767 fail2ban.filtersystemd  [20774]: INFO    [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,769 fail2ban.jail           [20774]: INFO    Jail 'postfix-sasl' started
2025-12-17 11:52:48,771 fail2ban.jail           [20774]: INFO    Jail 'sshd-ddos' started
2025-12-17 11:52:48,868 fail2ban.actions        [20774]: NOTICE  [sshd] Restore Ban 192.168.1.2
^C
[root@server.anspelov.net ~]# tail -f /var/log/fail2ban.log
2025-12-17 11:52:48,762 fail2ban.filtersystemd  [20774]: INFO    [postfix] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,763 fail2ban.jail           [20774]: INFO    Jail 'postfix' started
2025-12-17 11:52:48,763 fail2ban.filtersystemd  [20774]: INFO    [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,764 fail2ban.jail           [20774]: INFO    Jail 'postfix-rbl' started
2025-12-17 11:52:48,765 fail2ban.filtersystemd  [20774]: INFO    [dovecot] Jail is in operation now (process new journal entries)
2025-12-17 11:52:48,766 fail2ban.jail           [20774]: INFO    Jail 'dovecot' started
```

Проверка работы Fail2ban

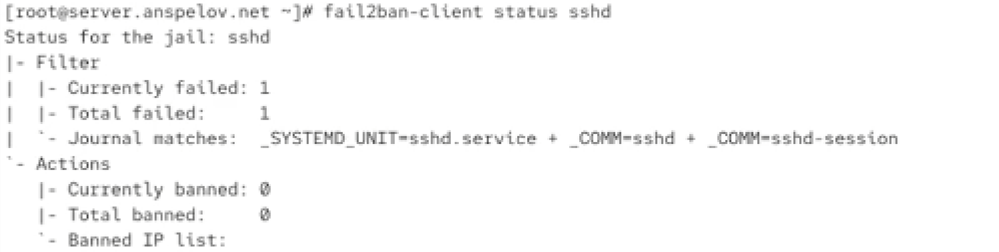
- Попытка войти с клиента на сервер с неправильным паролем.



```
[root@client.anspelov.net ~]# ssh anspelov@server.anspelov.net
ssh: connect to host server.anspelov.net port 22: Connection refused
[root@client.anspelov.net ~]# 
```

Проверка работы Fail2ban

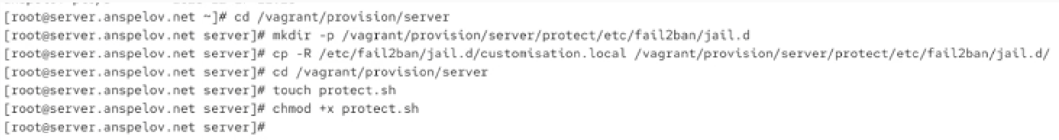
- Просмотр статуса защиты SSH.



```
[root@server.anspelov.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 + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

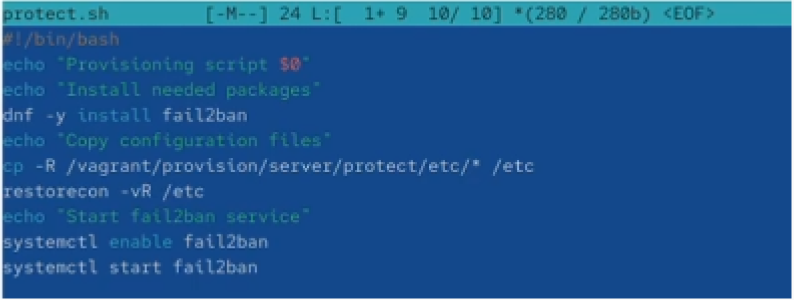
- Переход на виртуальной машине server в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога protect, в который помещаем в соответствующие подкаталоги конфигурационные файлы. Создание в каталоге /vagrant/provision/server исполняемого файла protect.sh.



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

Внесение изменений в настройки внутреннего окружения виртуальных машин

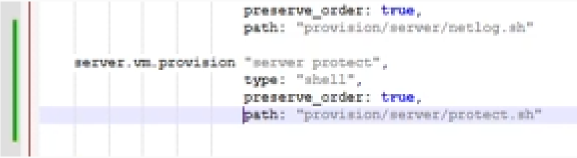
- Открытие файла на редактирование и добавление в него скрипта.



```
protect.sh          [-M--] 24 L:[  1+ 9  10/ 10] *(280 / 280b) <EOF>
#!/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
```

Внесение изменений в настройки внутреннего окружения виртуальных машин

- Добавление конфигураций в конфигурационном файле Vagrantfile для сервера.



```
                                  preserve_order: true,
                                  path: "provision/server/netlog.sh"

    server.vm.provision "server protect",
                                  type: "shell",
                                  preserve_order: true,
                                  path: "provision/server/protect.sh"
```

Вывод

Вывод

- В ходе выполнения лабораторной работы были получены навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».