Лабораториа работа 16

Базовая защита от атак типа «brute force»

ПОДГОТОВИЛА: КИМ РЕАЧНА
ГРУППА: НПИБД-02-20

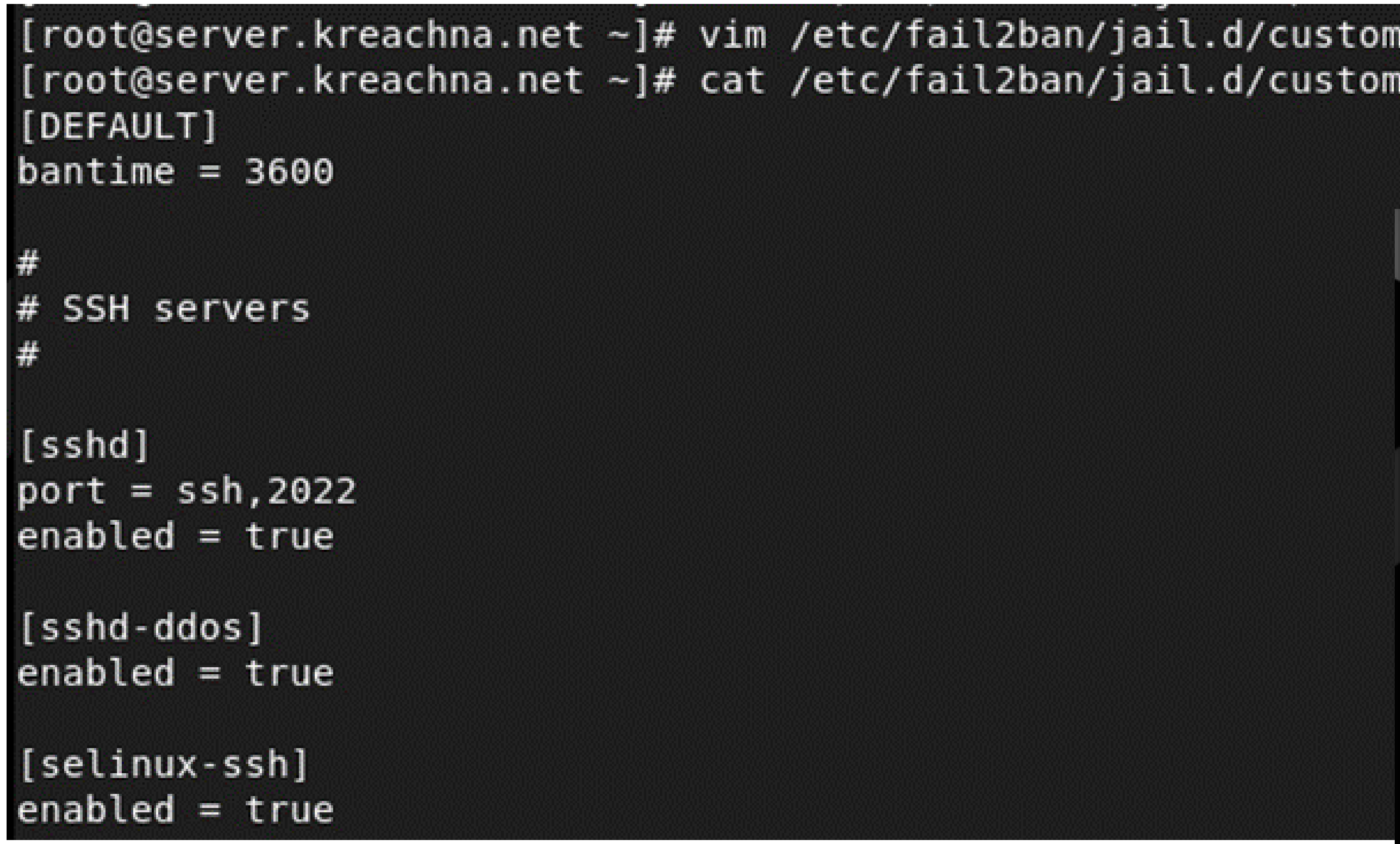
Цель работы:

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

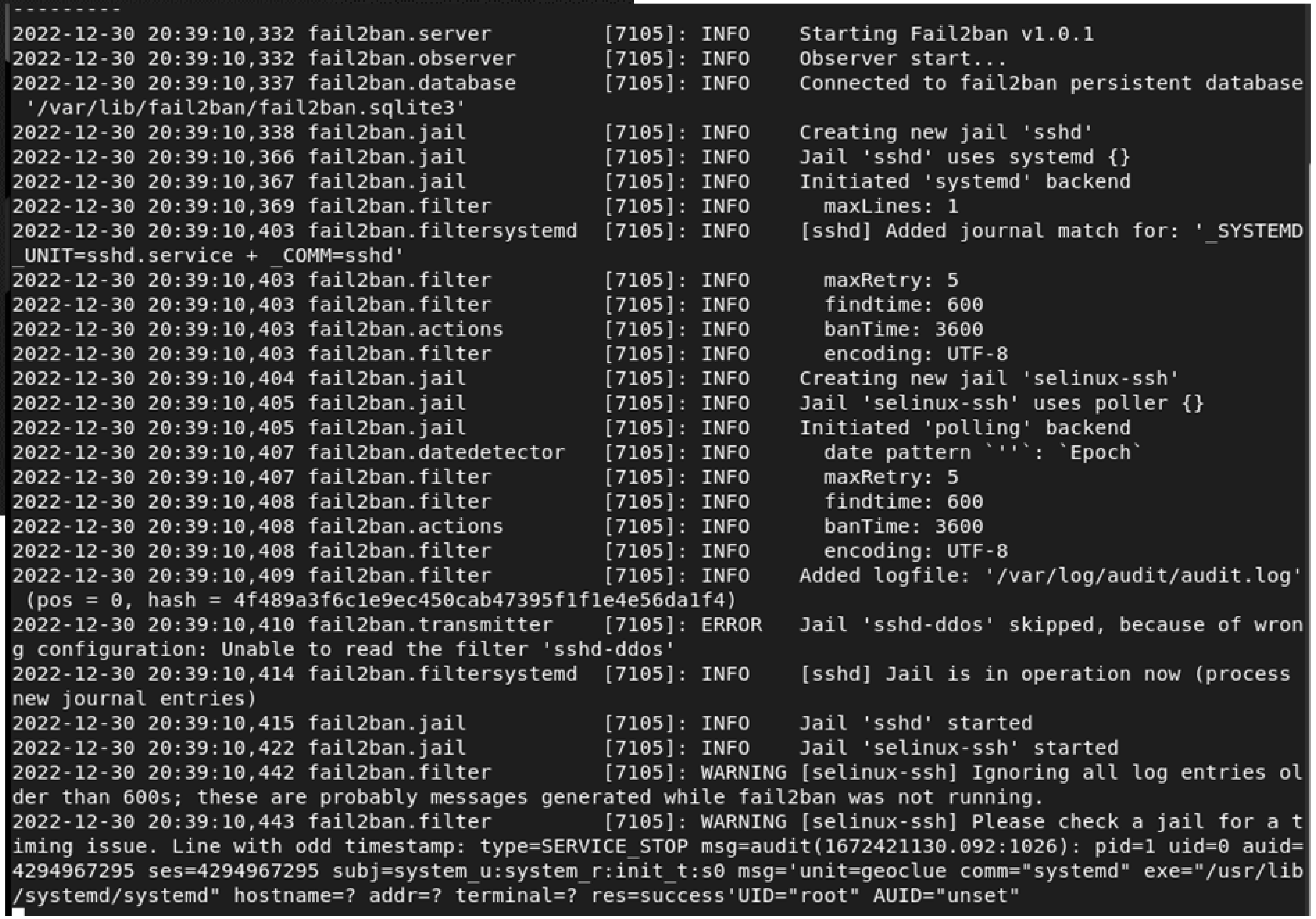
Задание:

- Защита с помощью Fail2ban
- Проверка работы Fail2ban
- Внесение изменений в настройки внутреннего окружения виртуальных машин

Защита с помощью Fail2ban

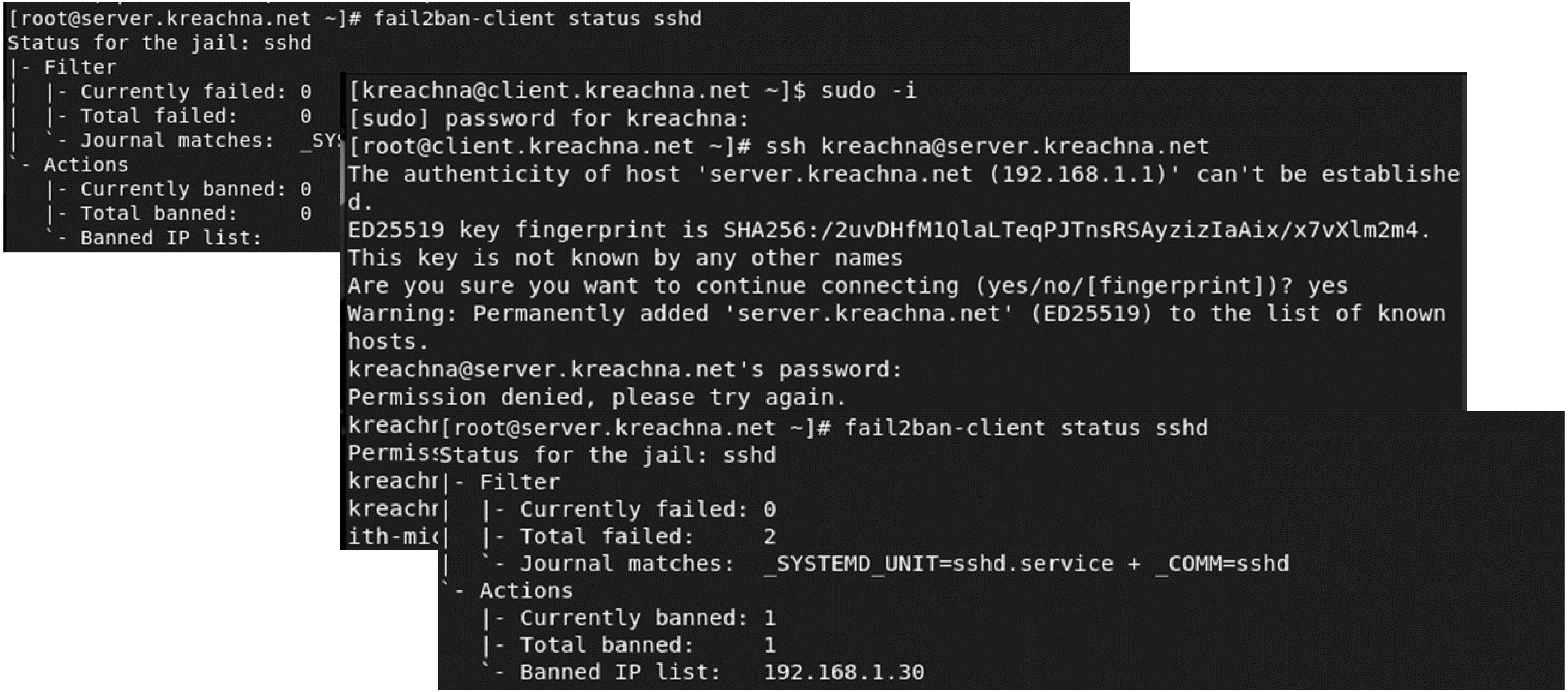


```
[root@server.kreachna.net ~]# vim /etc/fail2ban/jail.d/customisation.local
[root@server.kreachna.net ~]# cat /etc/fail2ban/jail.d/customisation.local
[DEFAULT]
bantime = 3600

#
# SSH servers
#

[sshd]
port = ssh,2022
enabled = true

[sshd-ddos]
enabled = true

[selinux-ssh]
enabled = true
```



```
---------
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 = 4f489a3f6c1e9ec450cab47395f1f1e4e56da1f4)
2022-12-30 20:39:10,410 fail2ban.transmitter    [7105]: ERROR   Jail 'sshd-ddos' skipped, because of wron
g 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"
```

Проверка работы Fail2ban

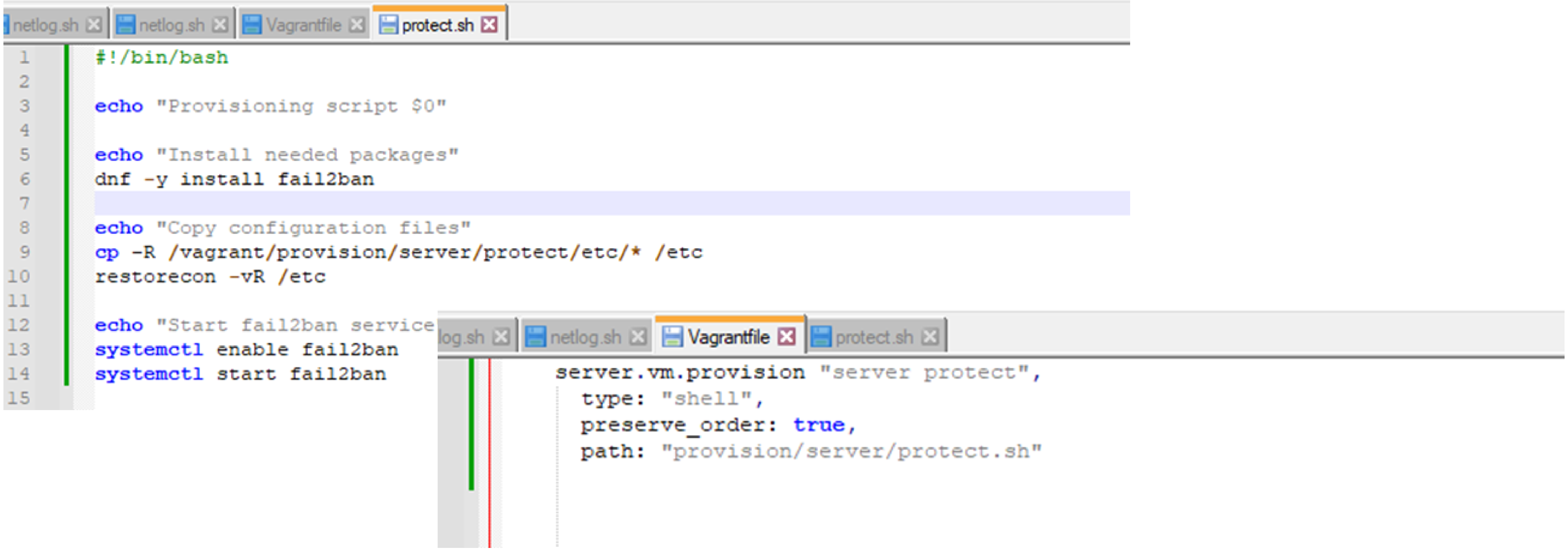


```
[root@server.kreachna.net ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SY
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

```
[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 establishe
d.
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.
kreachr
Permis
kreachr
kreachr
ith-mi
```

```
[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
```

Внесение изменений в настройки внутреннего окружения виртуальной машины



```
#!/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

```

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

Вывод

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

Спасибо за внимание!