РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 16

дисциплина: Администрирование сетевых подсистем

Студент:

Группа:

**МОСКВА**

2022 г.

# Цель работы:

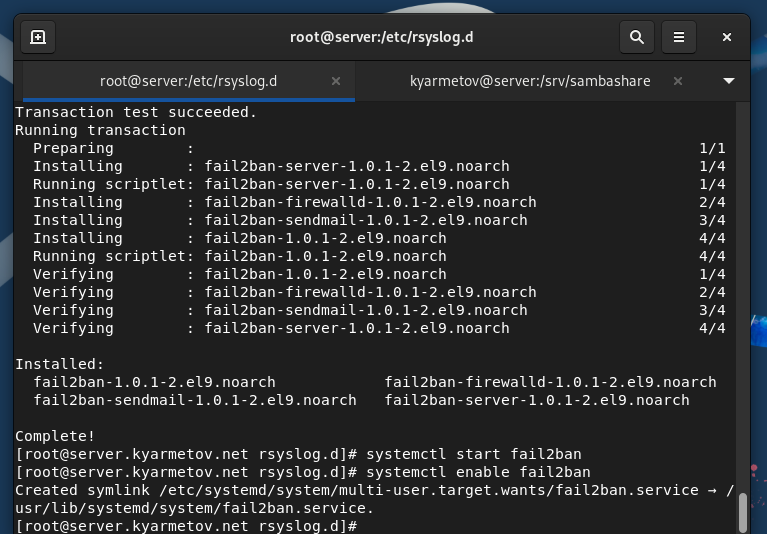
Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

# Ход работы:

**16.4.1. Защита с помощью Fail2ban**

1. На сервере установите fail2ban: dnf -y install fail2ban

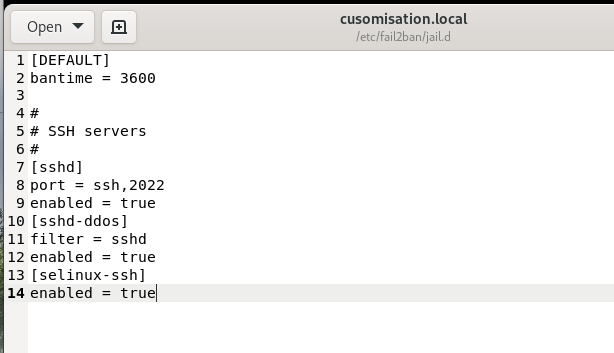
2. Запустите сервер fail2ban: systemctl start fail2ban systemctl enable fail2ban



3. В дополнительном терминале запустите просмотр журнала событий fail2ban: tail -f /var/log/fail2ban.log

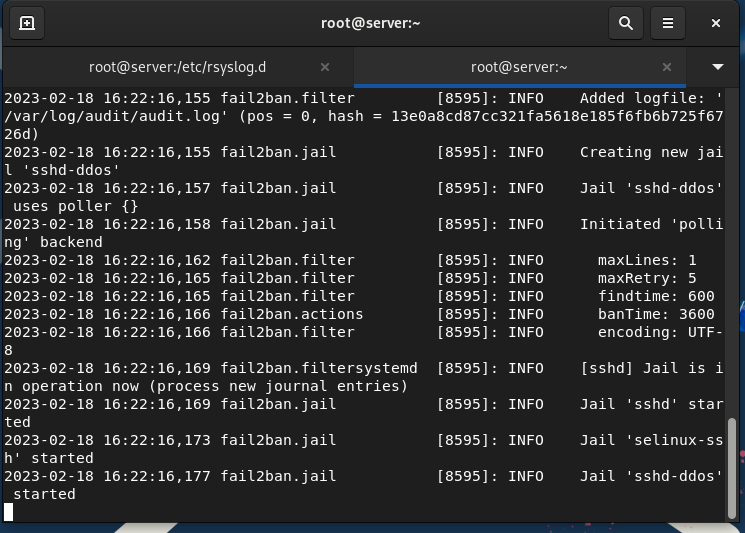
4. Создайте файл с локальной конфигурацией fail2ban: touch /etc/fail2ban/jail.d/customisation.local

5. В файле /etc/fail2ban/jail.d/customisation.local: (a) задайте время блокирования на 1 час (время задаётся в секундах): [DEFAULT] bantime = 3600 (b) включите защиту SSH: # # SSH servers # [sshd] port = ssh,2022 enabled = true [sshd-ddos] enabled = true [selinux-ssh] enabled = true

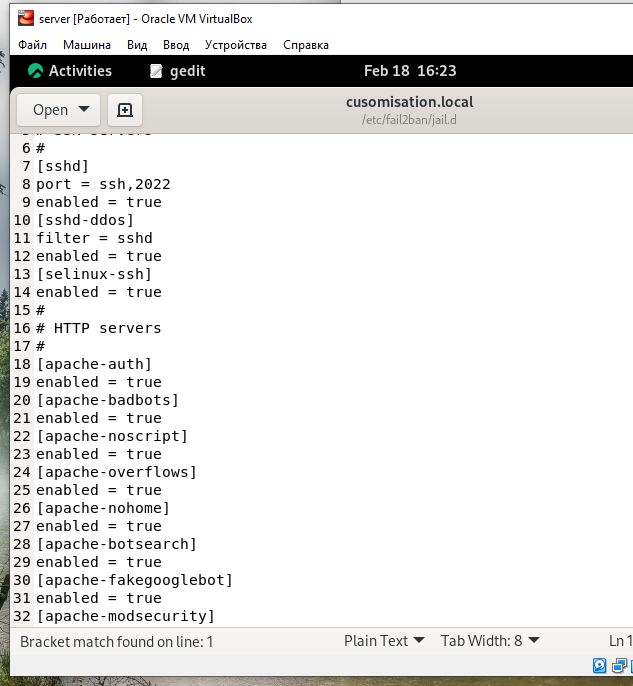


6. Перезапустите fail2ban systemctl restart fail2ban

7. Посмотрите журнал событий: tail -f /var/log/fail2ban.log

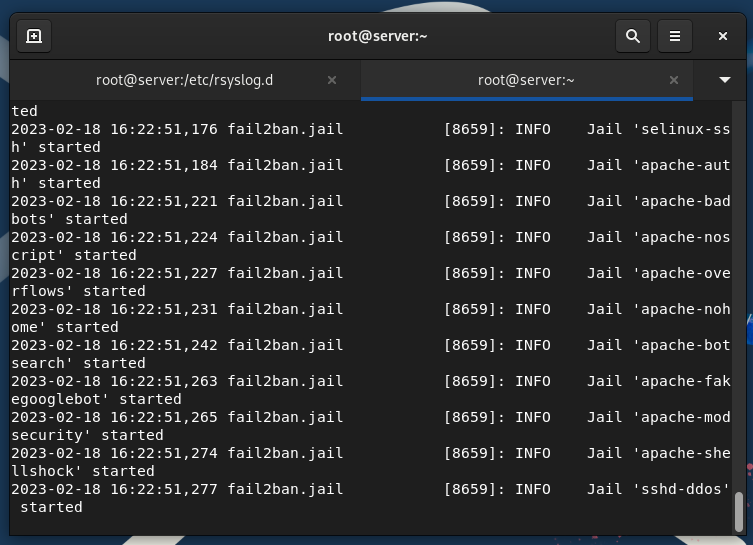


8. В файле /etc/fail2ban/jail.d/customisation.local включите защиту HTTP: # # HTTP servers # [apache-auth] enabled = true [apache-badbots] enabled = true [apache-noscript] enabled = true [apache-overflows] enabled = true [apache-nohome] enabled = true [apache-botsearch] enabled = true [apache-fakegooglebot] enabled = true [apache-modsecurity] enabled = true [apache-shellshock] enabled = true

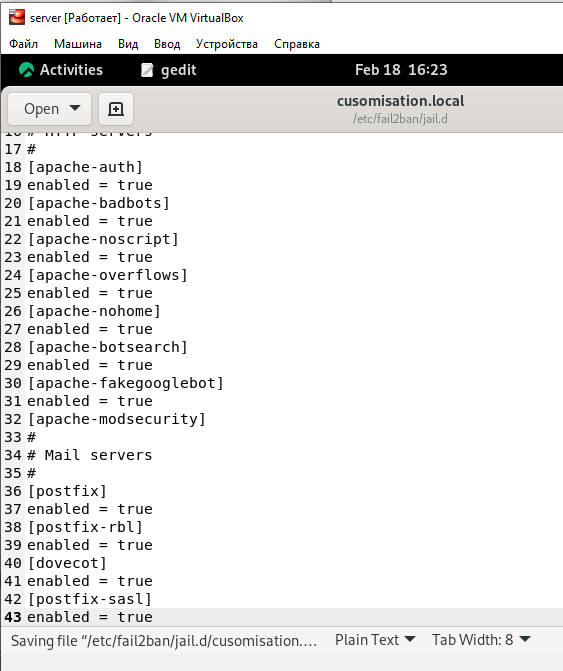


9. Перезапустите fail2ban systemctl restart fail2ban

10. Посмотрите журнал событий: tail -f /var/log/fail2ban.log

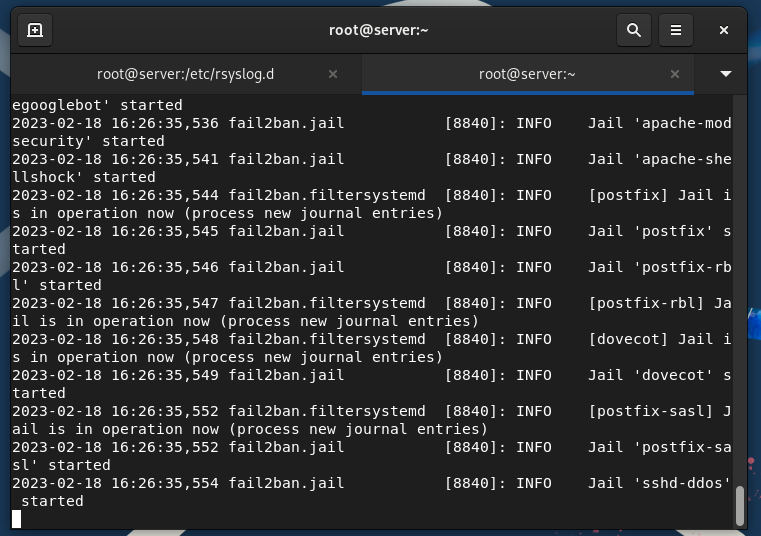


11. В файле /etc/fail2ban/jail.d/customisation.local включите защиту почты: # # Mail servers # [postfix] enabled = true [postfix-rbl] enabled = true [dovecot] enabled = true [postfix-sasl] enabled = true



12. Перезапустите fail2ban: systemctl restart fail2ban

13. Посмотрите журнал событий: tail -f /var/log/fail2ban.log

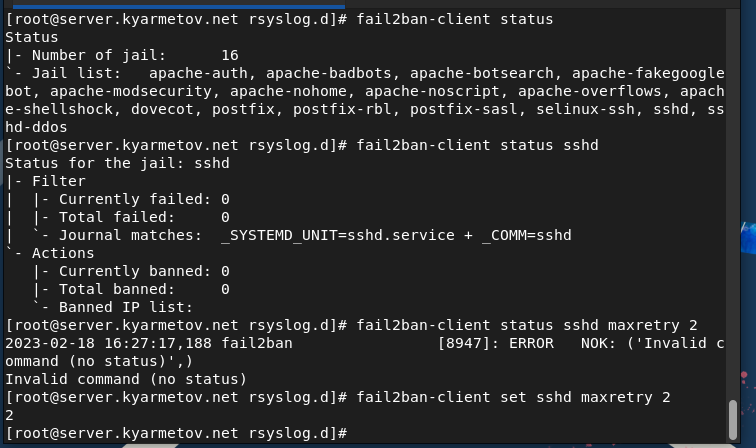


**16.4.2. Проверка работы Fail2ban**

1. На сервере посмотрите статус fail2ban: fail2ban-client status

2. Посмотрите статус защиты SSH в fail2ban: fail2ban-client status sshd

3. Установите максимальное количество ошибок для SSH, равное 2: fail2ban-client set sshd maxretry 2

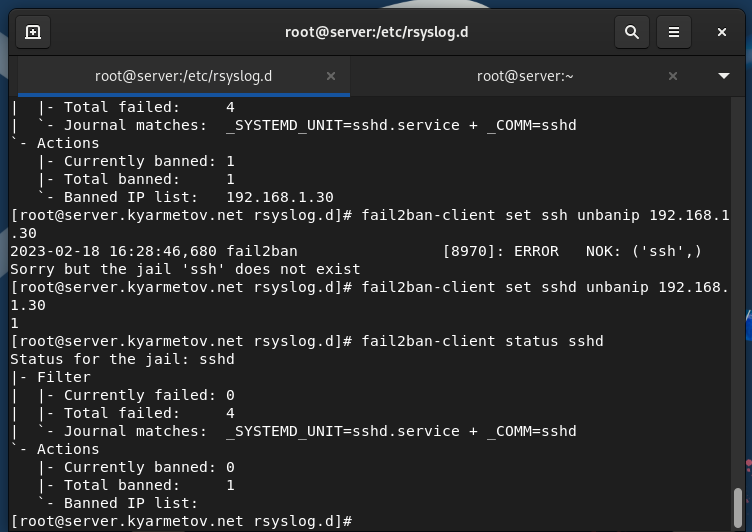


4. С клиента попытайтесь зайти по SSH на сервер с неправильным паролем.

5. На сервере посмотрите статус защиты SSH: fail2ban-client status sshd Убедитесь, что произошла блокировка адреса клиента.

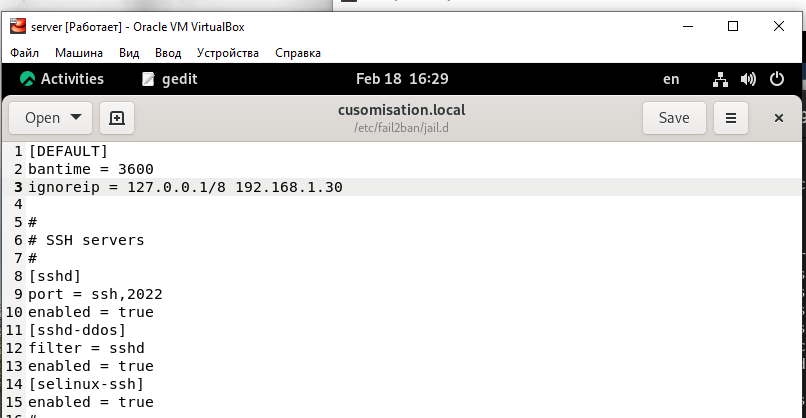
6. Разблокируйте IP-адрес клиента: fail2ban-client set sshd unbanip

7. Вновь посмотрите статус защиты SSH: fail2ban-client status sshd 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

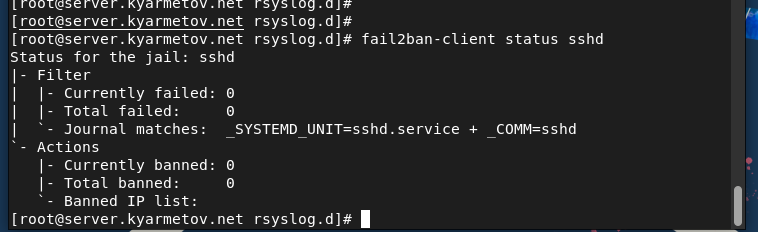
(вместо укажите конкретный адрес).

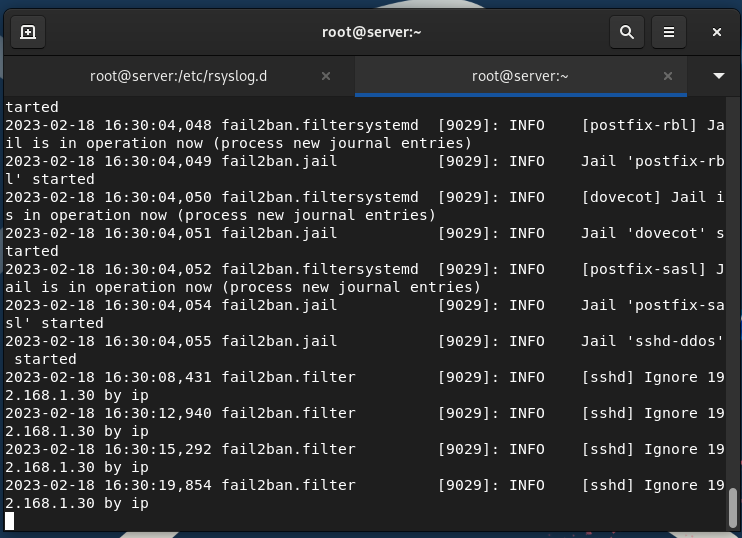


9. Перезапустите fail2ban.

10. Посмотрите журнал событий: tail -f /var/log/fail2ban.log

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



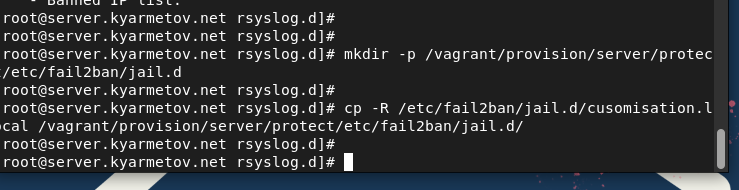


**16.4.3. Внесение изменений в настройки внутреннего окружения виртуальных машин**

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:

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

3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в соответствующем разделе конфигураций для сервера.



# Вывод:

Приобретены практические навыки работы с fail2ban