Лабораторная работа №16

Администрирование сетевых подсистем

Мишина А. А.

5 декабря 2024

Цели и задачи

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

Защита с помощью Fail2ban

Выполнение лабораторной работы

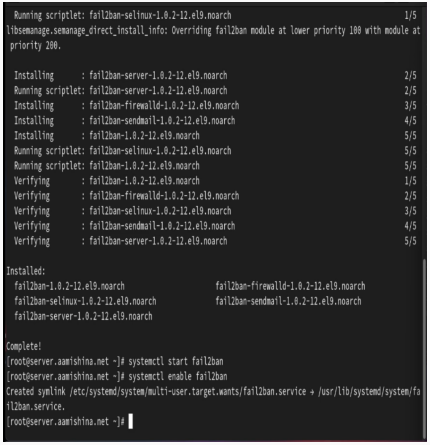


Рис. 1: Установка и запуск `fail2ban`

Выполнение лабораторной работы

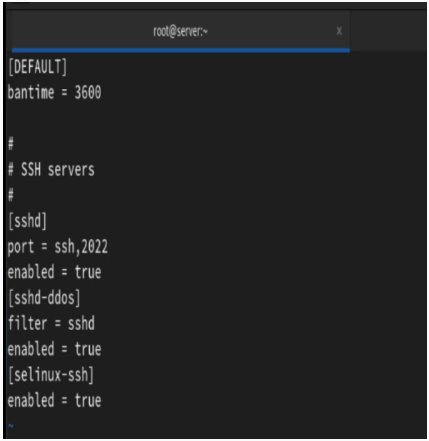


Рис. 2: Редактирование файла с локальной конфигурацией: задание времени блокировки, защита SSH

Выполнение лабораторной работы

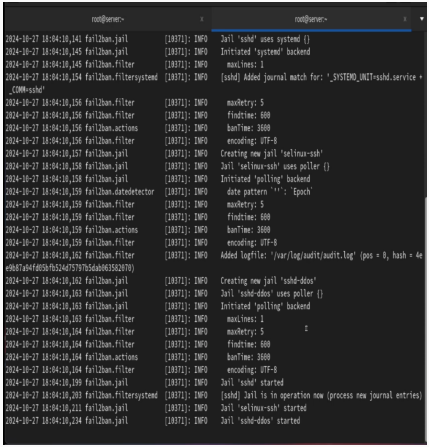


Рис. 3: Просмотр журнала событий `fail2ban`

Выполнение лабораторной работы

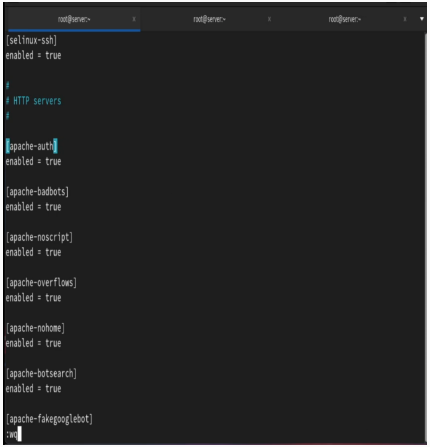


Рис. 4: Редактирование файла с локальной конфигурацией: защита HTTP

Выполнение лабораторной работы

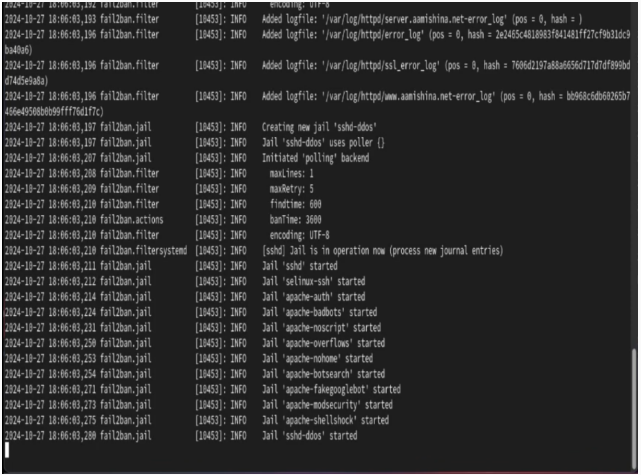


Рис. 5: Просмотр журнала событий `fail2ban`

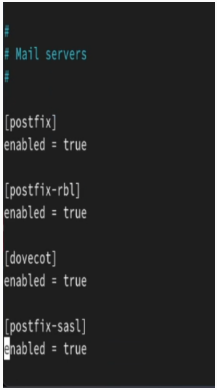


Рис. 6: Редактирование файла с локальной конфигурацией: защита почты

Выполнение лабораторной работы

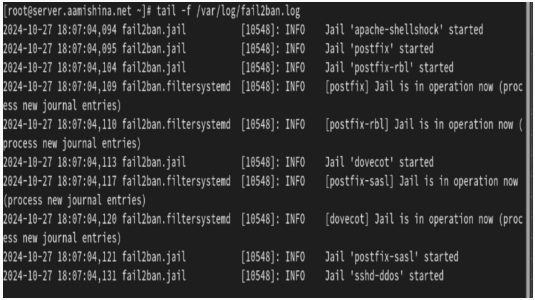


Рис. 7: Просмотр журнала событий `fail2ban`

Проверка работы Fail2ban

Выполнение лабораторной работы

```
[root@server.aamishina.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, postf
ix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.aamishina.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.aamishina.net ~]# fail2ban-client set sshd maxretry 2
2
[root@server.aamishina.net ~]#
```

Рис. 8: Просмотр статуса службы, статус защиты SSH, установка макс. кол-ва ошибок для SSH

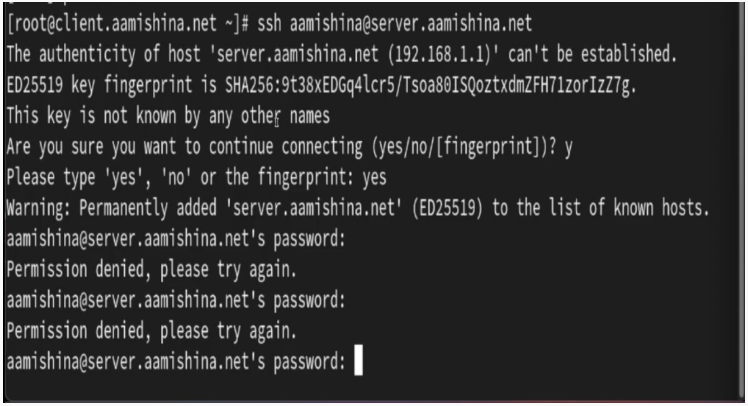


Рис. 9: Подключение к серверу по SSH с вводом неправильного пароля

Выполнение лабораторной работы

```
[root@server.aamishina.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:   192.168.1.57
[root@server.aamishina.net ~]# fail2ban-client set sshd unbanip 192.168.1.57
1
[root@server.aamishina.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: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.aamishina.net ~]#
```

Рис. 10: Просмотр статуса защиты SSH после неудачного входа, разблокировка IP-адреса клиента

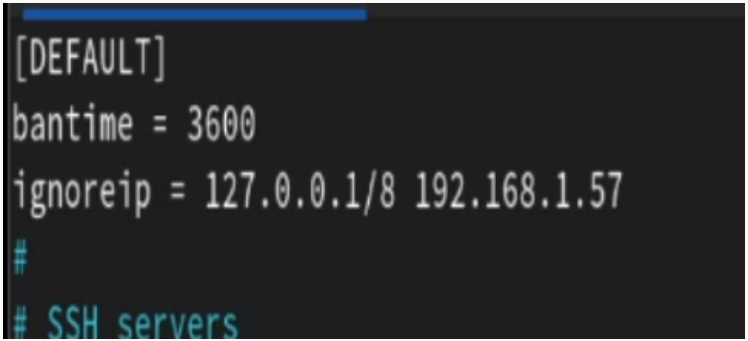


Рис. 11: Редактирование файла с локальной конфигурацией: игнорирование адреса клиента

Выполнение лабораторной работы

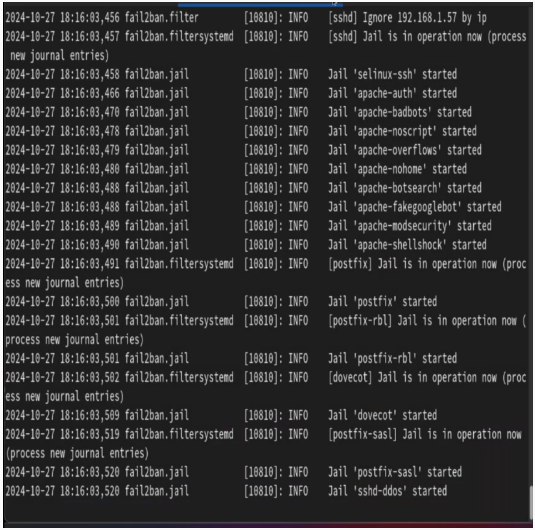
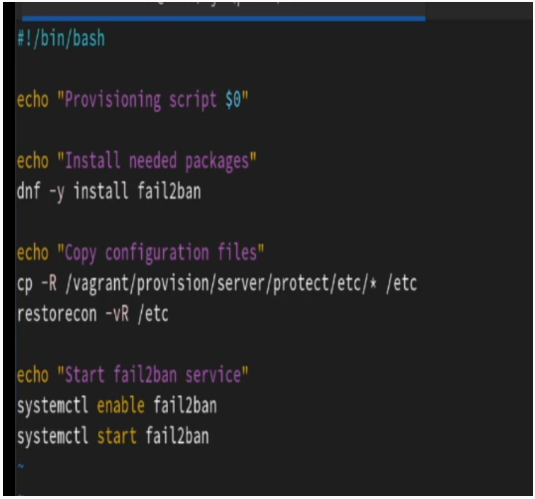


Рис. 12: Просмотр журнала событий ‘fail2ban’

Рис. 13: Просмотр статуса защиты SSH после неудачного входа

Внесение изменений в настройки внутреннего окружения виртуальной машины

```
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d
cp -R /etc/fail2ban/jail.d/customisation.local
    /vagrant/provision/server/protect/etc/fail2ban/jail.d/
```



```
#!/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. 14: Редактирование protect.sh на сервере

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

Выводы

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