Защита лабораторной работы № 16

Базовая защита от атак типа «brute force»

Администрирование сетевых подсистем

Работу Выполнил:
Саинт-Амур Измаэль
Группа: НПИбд-02-20

Цель работы

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

Защита с помощью Fail2ban

```
[root@server.saismael.net ~]# dnf -y install fail2ban
Last metadata expiration check: 1:00:33 ago on Sat 31 Dec 2022 08:48:58 AM UTC.
Dependencies resolved.
================================================================================
 Package                 Architecture  Version              Repository   Size
================================================================================
Installing:
 fail2ban                noarch        1.0.1-2.el9          epel        8.5 k
Installing dependencies:
 fail2ban-firewalld      noarch        1.0.1-2.el9          epel        8.7 k
 fail2ban-sendmail       noarch        1.0.1-2.el9          epel         11 k
 fail2ban-server         noarch        1.0.1-2.el9          epel        442 k

Transaction Summary
================================================================================
Install  4 Packages

Total download size: 471 k
Installed size: 1.4 M
Downloading Packages:
(1/4): fail2ban-firewalld-1.0.1-2.el9.noarch.rp  28 kB/s | 8.7 kB     00:00
(2/4): fail2ban-1.0.1-2.el9.noarch.rpm           25 kB/s | 8.5 kB     00:00
(3/4): fail2ban-sendmail-1.0.1-2.el9.noarch.rpm  30 kB/s |  11 kB     00:00
```

```
[root@server.saismael.net ~]# systemctl start fail2bam
Failed to start fail2bam.service: Unit fail2bam.service not found.
[root@server.saismael.net ~]# systemctl start fail2ban
[root@server.saismael.net ~]# systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /
usr/lib/systemd/system/fail2ban.service.
[root@server.saismael.net ~]# tail -f /var/log/fail2ban.log
2022-12-31 09:50:42,618 fail2ban.server         [4853]: INFO    ----------------
--------------------------------
2022-12-31 09:50:42,618 fail2ban.server         [4853]: INFO    Starting Fail2ba
n v1.0.1
2022-12-31 09:50:42,620 fail2ban.observer       [4853]: INFO    Observer start..
.
2022-12-31 09:50:42,628 fail2ban.database       [4853]: INFO    Connected to fai
l2ban persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2022-12-31 09:50:42,635 fail2ban.database       [4853]: WARNING New database cre
ated. Version '4'
```

root@server:~

```
[DEFAULT]
bantime = 3600

#
# SSH servers
#

[sshd]
port = ssh, 2022
enabled = true

[sshd-ddos]
enabled = true

[selinux-ssh]
enabled = true
```

Проверка работы Fail2ban

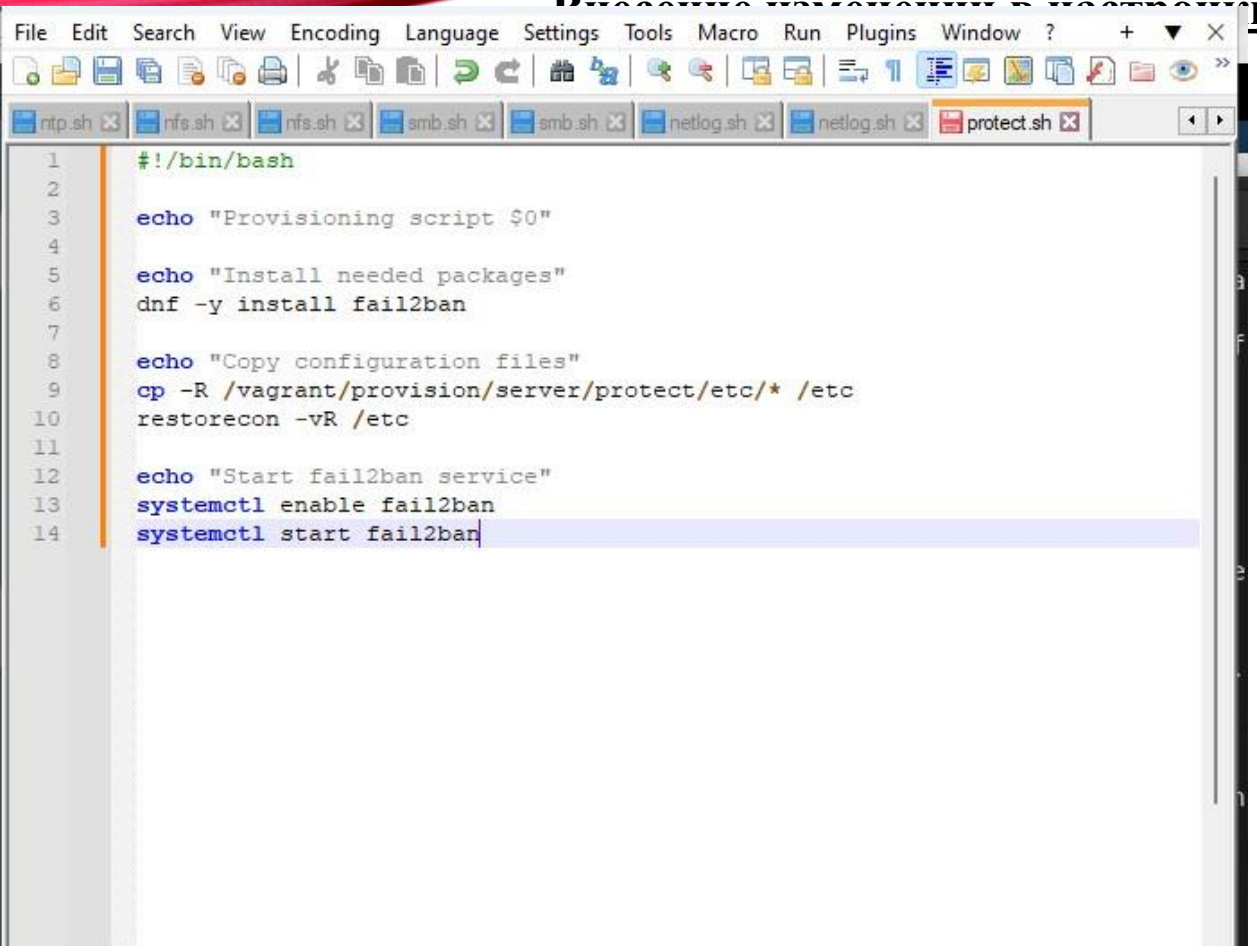
```
[root@server.saismael.net ~]# fail2ban-client status
Status
|- Number of jail:      14
`- Jail list:   apache-auth, apache-badbots, apache-botsearch, apache-fakegoo
bot, apache-modsecurity, apache-nohome, apache-noscript, apache-overflows, ap
e-shellshock, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd
[root@server.saismael.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.saismael.net ~]# fail2ban-client set sshd maxretry 2
2
```

Проверка работы Fail2ban

```
[root@server.saismael.net ~]# ssh saismael@server.saismael.net
The authenticity of host 'server.saismael.net (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:zqbOam9bCTBqb0qNzuP7z0xlgOqvGhkHxMkw2sQdblo.
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.saismael.net' (ED25519) to the list of known hosts.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
Permission denied, please try again.
saismael@server.saismael.net's password:
saismael@server.saismael.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic
,password).
```

```
[root@server.saismael.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:
```

Внесение изменений в настройки внутреннего окружения виртуальной машины




```
[root@server.saismael.net ~]#
[root@server.saismael.net ~]# cd /vagrant/provision/server
[root@server.saismael.net server]#
[root@server.saismael.net server]# mkdir -p /vagrant/provision/server/protect/et
c/fail2ban/jail.d
[root@server.saismael.net server]#
[root@server.saismael.net server]# cp -R /etc/fail2ban/jail.d/customisatin.local
 /vagrant/provision/server/protect/etc/fail2ban/jail.d/
cp: cannot stat '/etc/fail2ban/jail.d/customisatin.local': No such file or direc
tory
[root@server.saismael.net server]# cp -R /etc/fail2ban/jail.d/customisation.loca
l /vagrant/provision/server/protect/etc/fail2ban/jail.d/
[root@server.saismael.net server]#
[root@server.saismael.net server]#
[root@server.saismael.net server]# cd /vagrant/provision/server
[root@server.saismael.net server]# touch protect.sh
[root@server.saismael.net server]# chmod +x protect.sh
[root@server.saismael.net server]#
```

Вывод

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