Презентация лабораторной работы №16

Бакулин Никита 1032201747

Цель работы

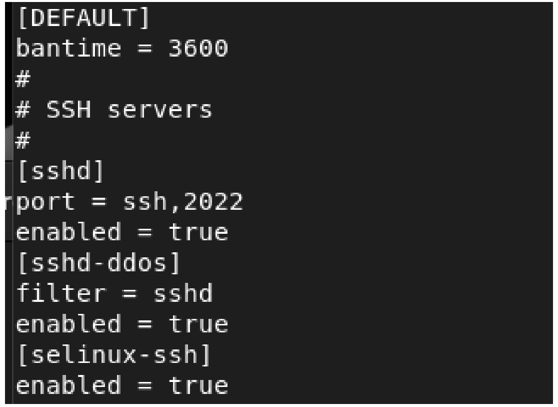
- Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

Задачи

- Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб.
- Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH.
- Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban

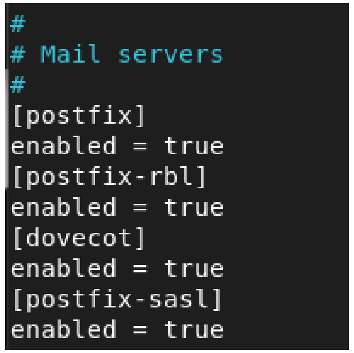
Результаты выполнения

- Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб.



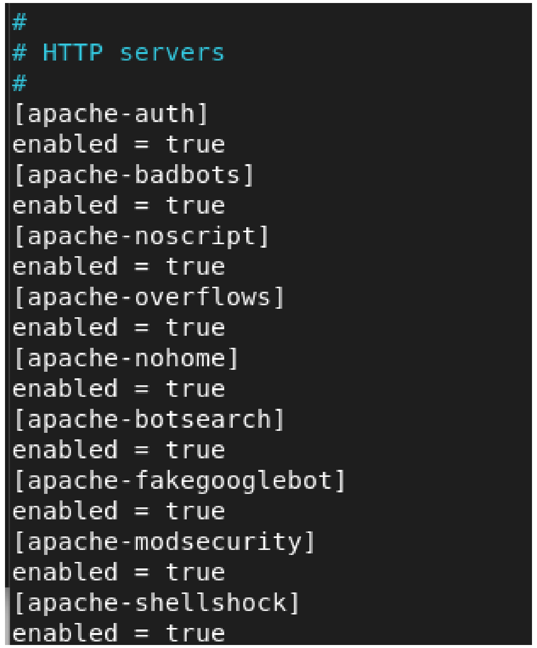
```
[DEFAULT]
bantime = 3600
#
# SSH servers
#
[sshd]
port = ssh,2022
enabled = true
[sshd-ddos]
filter = sshd
enabled = true
[selinux-ssh]
enabled = true
```

Рис. 1



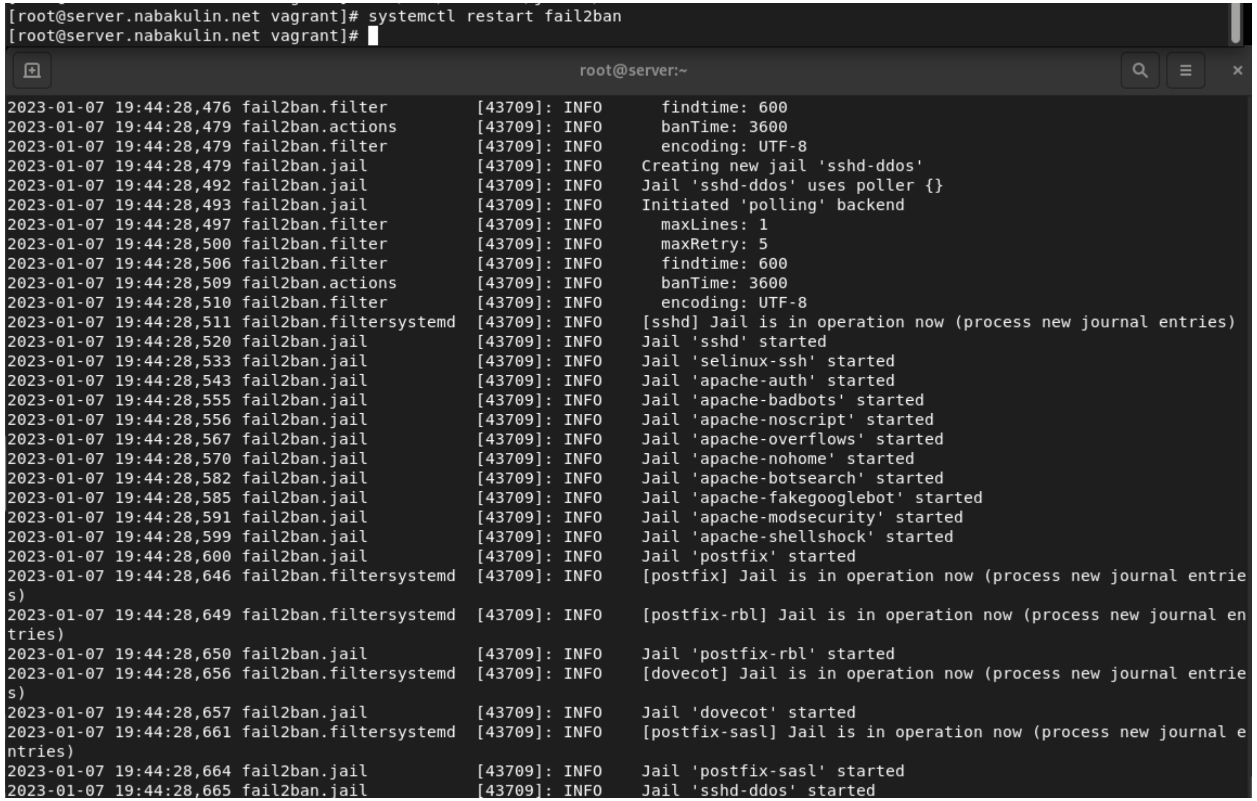
```
#
# Mail servers
#
[postfix]
enabled = true
[postfix-rbl]
enabled = true
[dovecot]
enabled = true
[postfix-sasl]
enabled = true
```

Рис. 2



```
#
# 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
```

Рис. 3



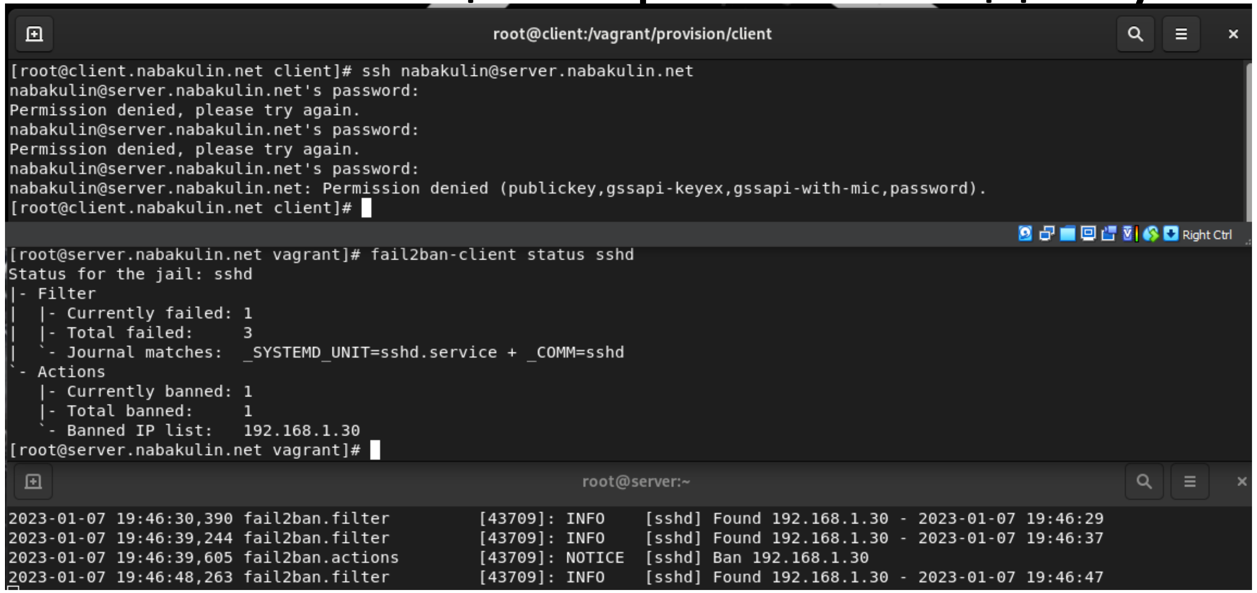
```
[root@server.nabakulin.net vagrant]# systemctl restart fail2ban
[root@server.nabakulin.net vagrant]# █
```

```
2023-01-07 19:44:28,476 fail2ban.filter         [43709]: INFO      findtime: 600
2023-01-07 19:44:28,479 fail2ban.actions        [43709]: INFO      banTime: 3600
2023-01-07 19:44:28,479 fail2ban.filter         [43709]: INFO      encoding: UTF-8
2023-01-07 19:44:28,479 fail2ban.jail           [43709]: INFO    Creating new jail 'sshd-ddos'
2023-01-07 19:44:28,492 fail2ban.jail           [43709]: INFO    Jail 'sshd-ddos' uses poller {}
2023-01-07 19:44:28,493 fail2ban.jail           [43709]: INFO    Initiated 'polling' backend
2023-01-07 19:44:28,497 fail2ban.filter         [43709]: INFO      maxLines: 1
2023-01-07 19:44:28,500 fail2ban.filter         [43709]: INFO      maxRetry: 5
2023-01-07 19:44:28,506 fail2ban.filter         [43709]: INFO      findtime: 600
2023-01-07 19:44:28,509 fail2ban.actions        [43709]: INFO      banTime: 3600
2023-01-07 19:44:28,510 fail2ban.filter         [43709]: INFO      encoding: UTF-8
2023-01-07 19:44:28,511 fail2ban.filtersystemd  [43709]: INFO    [sshd] Jail is in operation now (process new journal entries)
2023-01-07 19:44:28,520 fail2ban.jail           [43709]: INFO    Jail 'sshd' started
2023-01-07 19:44:28,533 fail2ban.jail           [43709]: INFO    Jail 'selinux-ssh' started
2023-01-07 19:44:28,543 fail2ban.jail           [43709]: INFO    Jail 'apache-auth' started
2023-01-07 19:44:28,555 fail2ban.jail           [43709]: INFO    Jail 'apache-badbots' started
2023-01-07 19:44:28,556 fail2ban.jail           [43709]: INFO    Jail 'apache-noscript' started
2023-01-07 19:44:28,567 fail2ban.jail           [43709]: INFO    Jail 'apache-overflows' started
2023-01-07 19:44:28,570 fail2ban.jail           [43709]: INFO    Jail 'apache-nohome' started
2023-01-07 19:44:28,582 fail2ban.jail           [43709]: INFO    Jail 'apache-botsearch' started
2023-01-07 19:44:28,585 fail2ban.jail           [43709]: INFO    Jail 'apache-fakegooglebot' started
2023-01-07 19:44:28,591 fail2ban.jail           [43709]: INFO    Jail 'apache-modsecurity' started
2023-01-07 19:44:28,599 fail2ban.jail           [43709]: INFO    Jail 'apache-shellshock' started
2023-01-07 19:44:28,600 fail2ban.jail           [43709]: INFO    Jail 'postfix' started
2023-01-07 19:44:28,646 fail2ban.filtersystemd  [43709]: INFO    [postfix] Jail is in operation now (process new journal entrie
s)
2023-01-07 19:44:28,649 fail2ban.filtersystemd  [43709]: INFO    [postfix-rbl] Jail is in operation now (process new journal en
tries)
2023-01-07 19:44:28,650 fail2ban.jail           [43709]: INFO    Jail 'postfix-rbl' started
2023-01-07 19:44:28,656 fail2ban.filtersystemd  [43709]: INFO    [dovecot] Jail is in operation now (process new journal entrie
s)
2023-01-07 19:44:28,657 fail2ban.jail           [43709]: INFO    Jail 'dovecot' started
2023-01-07 19:44:28,661 fail2ban.filtersystemd  [43709]: INFO    [postfix-sasl] Jail is in operation now (process new journal e
ntries)
2023-01-07 19:44:28,664 fail2ban.jail           [43709]: INFO    Jail 'postfix-sasl' started
2023-01-07 19:44:28,665 fail2ban.jail           [43709]: INFO    Jail 'sshd-ddos' started
```

Рис. 4

Результаты выполнения

- Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH.

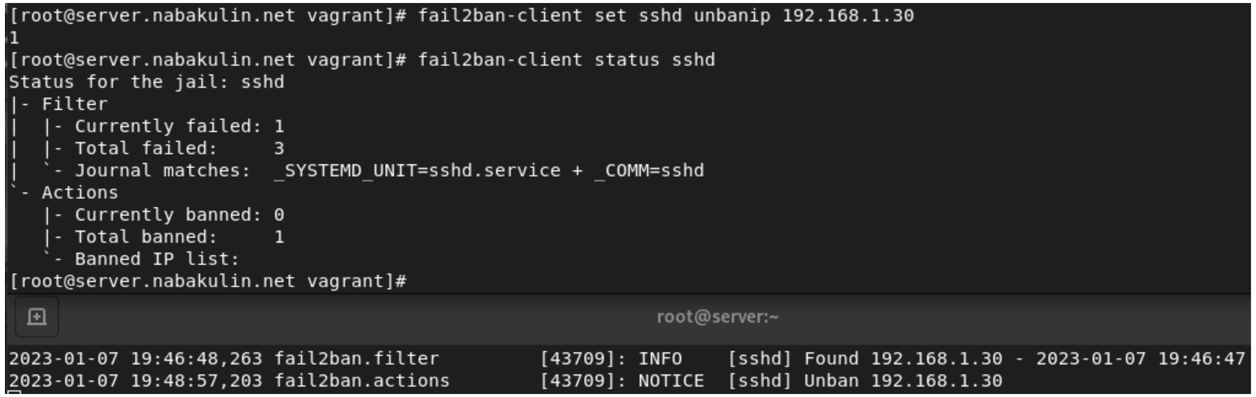


```
[root@client.nabakulin.net client]# ssh nabakulin@server.nabakulin.net
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password:
nabakulin@server.nabakulin.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@client.nabakulin.net client]#
```

```
[root@server.nabakulin.net vagrant]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.30
[root@server.nabakulin.net vagrant]#
```

```
2023-01-07 19:46:30,390 fail2ban.filter         [43709]: INFO    [sshd] Found 192.168.1.30 - 2023-01-07 19:46:29
2023-01-07 19:46:39,244 fail2ban.filter         [43709]: INFO    [sshd] Found 192.168.1.30 - 2023-01-07 19:46:37
2023-01-07 19:46:39,605 fail2ban.actions        [43709]: NOTICE  [sshd] Ban 192.168.1.30
2023-01-07 19:46:48,263 fail2ban.filter         [43709]: INFO    [sshd] Found 192.168.1.30 - 2023-01-07 19:46:47
```

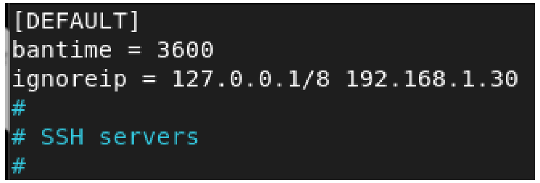
Рис. 5



```
[root@server.nabakulin.net vagrant]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.nabakulin.net vagrant]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     3
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     1
   `- Banned IP list:
[root@server.nabakulin.net vagrant]#
```

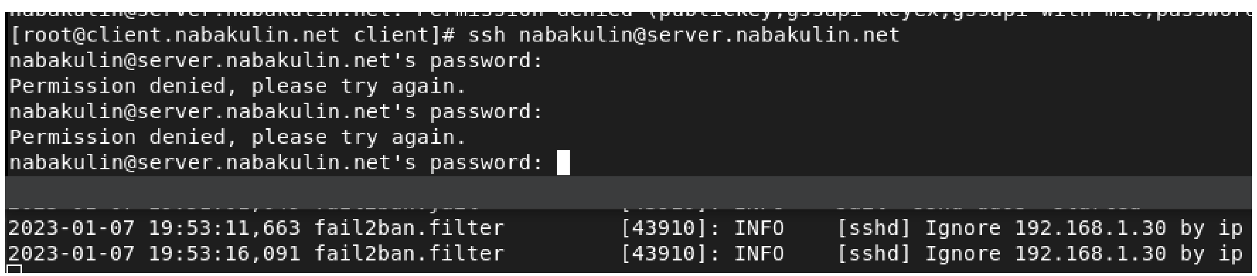
```
2023-01-07 19:46:48,263 fail2ban.filter         [43709]: INFO    [sshd] Found 192.168.1.30 - 2023-01-07 19:46:47
2023-01-07 19:48:57,203 fail2ban.actions        [43709]: NOTICE  [sshd] Unban 192.168.1.30
```

Рис. 6



```
[DEFAULT]
bantime = 3600
ignoreip = 127.0.0.1/8 192.168.1.30
#
# SSH servers
#
```

Рис. 7



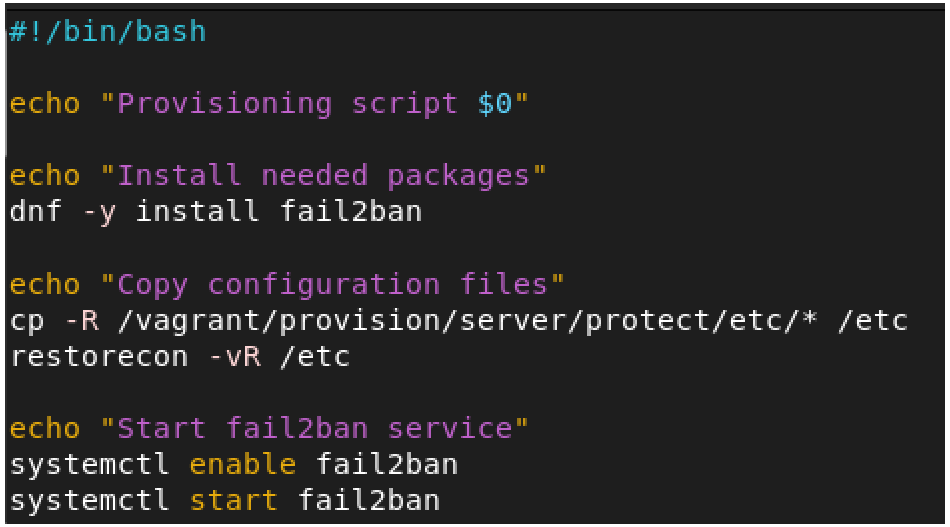
```
nabakulin@server.nabakulin.net: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,passwor
[root@client.nabakulin.net client]# ssh nabakulin@server.nabakulin.net
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password:
Permission denied, please try again.
nabakulin@server.nabakulin.net's password:
```

```
2023-01-07 19:53:11,663 fail2ban.filter         [43910]: INFO    [sshd] Ignore 192.168.1.30 by ip
2023-01-07 19:53:16,091 fail2ban.filter         [43910]: INFO    [sshd] Ignore 192.168.1.30 by ip
```

Рис. 8

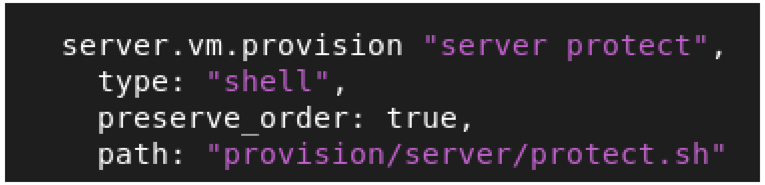
Результаты выполнения

- Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban



```
#!/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. 11



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

Рис. 12