Лабораторная работа № 16. Базовая защита от атак типа «brute force»

16.1. Цель работы

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

16.2. Предварительные сведения

Одно из решений по защите узла сети от несанкционированного доступа и атак типа «brute force» (в частности, подбора паролей администратора методом полного перебора) — использование Fail2ban [1]. Данное программное средство отслеживает сетевую активность на портах узла путём сканирования текстовых лог-файлов. При выявлении программой неадекватной активности какого-то узла его IP-адрес помещается в чёрный список, а все пакеты с этого адреса блокируются. Блокировка настраивается путём внесения изменений в правила межсетевого экрана.

Файл `/etc/fail2ban/fail2ban.conf` содержит настройки запуска процесса Fail2ban. Основной файл конфигурации конкретных служб в Fail2ban — `/etc/fail2ban/jail.conf`, настройки для локального узла должны быть размещены в файле `NAMEFILE.local` в каталоге `/etc/fail2ban/jail.d`, конфигурации для работы с различными службами размещаются в отдельных подкаталогах и файлах в каталоге `/etc/fail2ban/`.

Каждый конфигурационный файл Fail2ban имеет секции, каждая из которых описывает определённую службу и тип атаки.

Базовые правила `fail2ban` в конфигурационном файле:

- `ignoreip` — не блокировать IP-адреса из этого списка; несколько IP-адресов разделяются пробелами;
- `bantime` — время блокировки в секундах (по умолчанию — 600, т.е. 10 минут); для постоянного блокирования используется любое отрицательное число;
- `findtime` — длительность интервала времени в секундах, в течение которого `fail2ban` отслеживает подозрительную активность (по умолчанию — 10 минут);
- `maxretry` — количество подозрительных совпадений, после которых IP-адрес блокируется (по умолчанию — 3 попытки).

16.3. Задание

1. Установите и настройте Fail2ban для отслеживания работы установленных на сервере служб (см. раздел 16.4.1).
2. Проверьте работу Fail2ban посредством попыток несанкционированного доступа с клиента на сервер через SSH (см. раздел 16.4.2).
3. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке Fail2ban (см. раздел 16.4.3).

16.4. Последовательность выполнения 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]
   filter = sshd
   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 <ip-адрес клиента>
   ```
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 <ip-адрес клиента>
   ```
   (вместо <ip-адрес клиента> 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:
```
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/
```
2. В каталоге /vagrant/provision/server создайте исполняемый файл protect.sh:
```
cd /vagrant/provision/server
touch protect.sh
chmod +x protect.sh
```
Открыв его на редактирование, пропишите в нём следующий скрипт:
```
#!/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
```
3. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в соответствующем разделе конфигураций для сервера:
```
server.vm.provision "server protect",
   type: "shell",
   preserve_order: true,
   path: "provision/server/protect.sh"
```

16.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение работы;
   - подробное описание настроек служб в соответствии с заданием;
   - полные тексты конфигурационных файлов настраиваемых в работе служб;
   - результаты проверки корректности настроек служб в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

16.6. Контрольные вопросы

1. Поясните принцип работы Fail2ban.
2. Настройки какого файла более приоритетны: `jail.conf` или `jail.local`?
3. Как настроить оповещение администратора при срабатывании Fail2ban?
4. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к веб-службе.
5. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к почтовой службе.
6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где можно посмотреть описание действий для последующего использования в настройках Fail2ban?
7. Как получить список действующих правил Fail2ban?
8. Как получить статистику заблокированных Fail2ban адресов?
9. Как разблокировать IP-адрес?

Список литературы

1. Сайт Fail2ban. — URL: `https://www.fail2ban.org` (visited on 09/13/2021).