Инструкция для запуска скрипта пересылки сообщений между сервером Syslog-ng и Fortinet Single Sign On

Оглавление

1. Предварительная настройка системы

1.1. Проверьте, что у вас установлен Python третьей версии:

```
python3 –V
```

1.2. Установите утилиту pip для python3:

```
apt install python3-pip
```

1.2.1. Если возникает ошибка ‘Unable to locate package python-pip’, в файл sources.list добавьте в конце каждой строчки тег universe:

```
deb http://archive.ubuntu.com/ubuntu bionic-security main universe
deb http://archive.ubuntu.com/ubuntu bionic-updates main universe
deb http://archive.ubuntu.com/ubuntu bionic main universe
```

1.2.2. Обновите пакеты:

```
apt update
```

1.2.3. Установите pip:

```
apt install python3-pip
```

1.3. Установите пакеты для работы с библиотекой ldap:

```
apt install build-essential python3-dev libldap2-dev libsasl2-dev slapd ldap-utils valgrind
```

2. Установка модулей python и подготовка скрипта

2.1. Установите модули python3

```
pip install python-ldap pyrad configparser
```

2.2. Склонируйте с помощью git или скачайте скрипт:

https://github.com/PakshNina/syslog-ng-radius

2.3. Перейдите в скачанную папку.

Откройте файл конфигурации скрипта initial.conf:

```
nano initial.conf
```

2.3.1. Данные поля оставьте без изменений

```
[ALIES]
User-Name=User-Name
Calling-Station-ID=Framed-IP-Address
[ADDITIONAL FIELDS]
Acct-Status-Type=Start
```

2.3.2. В данном разделе задайте IP адрес, секретный ключ и полный путь к словарям Radius:

```
[RADIUS]
IP = 10.31.46.196
SECRET = q1q1q1Q!Q!Q!
DICT_PATH = /home/python-radius/dicts/dictionary
```

2.3.3. В данном разделе задайте путь к логу, в который скрипт python записывает результаты операций

```
[RESULT_LOG]
LOG_PATH = /var/log/syslog-python.log
```

2.3.4. Данный раздел не изменяйте

```
[TARGET_ATTR]
ATTR = User-Name
```

2.3.5. В данном раздела задайте настройки ldap сервера: IP-адрес, логин, пароль администратора. LDAP_ATTR оставьте без изменений.

Измените имя подразделения LDAP_OU (Organizational Unit) и доменное имя LDAP_DOMAIN:

```
[LDAP]
LDAP_URL = ldap://10.31.46.139:389
LDAP_USERNAME = administrator@fortidomain.local
LDAP_PSWD = q1q1q1Q!Q!Q!
LDAP_ATTR = userPrincipalName
LDAP_OU = HQ
LDAP_DOMAIN = fortidomain.local
```

3. Запуск скрипта через syslog-ng

3.1. Задайте настройки syslog-ng, например, по пути:

```
nano /etc/syslog-ng/conf.d/ise.conf
```

Полный конфиг:

```
source s_net { udp(ip(0.0.0.0) port(514)); };
filter f_ise_host     {    (
                           host("10.31.34.101") or
                           host("127.0.0.1")
                           );
                     };
filter f_ise_auth { message("Authentication succeeded"); };
destination d_NS_ISE { file("/var/log/test.log"); };
destination d_python { program("python3 -u /home/python-
radius/syslog_sysrador_program.py"
        flags(no_multi_line)
        flush_timeout(1000)
); };
log {   source(s_net);
        filter(f_ise_host);
        filter(f_ise_auth);
        destination(d_NS_ISE);
        destination(d_python);
};
```

Вместо `/var/log/test.log` – укажите путь к логу, куда syslog-ng отправляет события.
Вместо `/home/python-radius/syslog_sysrador_program.py` – полный путь к файлу python syslog_sysrador_program.py.

3.2. Откройте редактор файла syslog_sysrador_program.py:

```
nano syslog_sysrador_program.py
```

На строчке `sysrad = SysRador('/home/python-radius/initial.conf')` вместо '/home/python-radius/initial.conf' укажите полный путь к файлу initial.conf :

```
from fortigator.sysrador import SysRador
import sys
if __name__ =='__main__':
    sysrad = SysRador('/home/python-radius/initial.conf')
    try:
        line = sys.stdin.readline()
```

```
        sysrad.send(line)
    except Exception as err:
        raise Exception('Problem occured: {0}'.format(err))
```

3.3. Сгенерируйте вручную события логирования через терминал.

3.3.1. Для пользователей без доменного имени:

```
logger -n 127.0.0.1 Passed-Authentication: Authentication succeeded, User-Name=surfservice, Calling-Station-ID=10.0.0.1
```

3.3.2. Для пользователей со стандартным UDN:

```
logger -n 127.0.0.1 Passed-Authentication: Authentication succeeded, User-Name=cpservice@fortidomain.local, Calling-Station-ID=10.0.0.2
```

3.3.3. Для пользователей с e-mail вместо логина:

```
logger -n 127.0.0.1 Passed-Authentication: Authentication succeeded, User-Name=figoluis@fortidomain.local, Calling-Station-ID=10.0.0.3
```

3.3.4. Для пользователей с альтернативной записью домена

```
logger -n 127.0.0.1 Passed-Authentication: Authentication succeeded, User-Name=fortidomain.local\\r.carlos, Calling-Station-ID=10.0.0.4
```

3.4. Проверьте результат

4. Запуск скрипта через консоль

4.1. Очистка лога:

```
rm /var/log/test.log
```

4.2. Закомментируйте в конфигурации syslog-ng строчку логирования в скрипт python:

```
# destination(d_python);
```

4.3. Перейдите в каталог со скриптами (syslog-ng-radius) и запустите генератор заходов пользователей, где после –n идет количество генерируемых пользователей:

```
python3 user_creator_multiproc.py -n 400
```

4.4. Запустите скрипт из каталога со скриптами:

```
python3 terminal_sysrador_program.py
```

4.5. Проверьте результат