**Успешным считается выполнение не менее 75% заданий**

1. Разобрать (распарсить) события с помощью регулярных выражений с целью подготовки представления признаков событий под формат нормализованного события SIEM.

Задание выполнять с помощью [regex101.com](https://regex101.com/) для указанных примеров событий (события однострочные).

Должно быть не менее 3 токенов (групп) и точка в конце события должна отсекаться (при наличии). При выполнении разбора событий (парсинга) использовать синтаксис регулярных выражений (общепринятые символы/метасимволы, классы).

Возможно применение базовых и расширенных POSIX.

Для **первого и второго события** разбор данных начинать с начала.

Для **третьего и четвертого события** разбор данных начинать с конца.

Дать описание разбираемых событий. Указать ссылки с [regex101.com](https://regex101.com/) по результатам выполнения задания.

* Jun 6 17:51:24 ksmg.loc KSMG: Delete all messages in MTA queues: success, queues: [def].

|  |  |
| --- | --- |
| Regex-выражение | ^(\w{3}\s+\d\s[\d:]\*)\s(\S+)\s(\w+)\:\s([\w+\s]\*)\:\s(\w\*),\s(\S\*\s\S\*)[^\/] |
| Regex Link | https://regex101.com/r/U4YAE0/1 |
| Описание события | Удаление очереди писем в MTA Kaspersky Secure Male Gateway  Разобрал событие на группы: Date\_time, Log\_file, Type, Message, Status, Result |

* <181>Oct 15 2018 07:49:40 HuaweiS6700 %%01SHELL/2/CHANGE\_PASSWORD\_FAIL(s)[680]:Failed to change the password. (Ip=10.10.185.132, VpnName=, UserName=efros\_w, Times=5, FailedReason=many\_incorrect\_logon\_attempts)

|  |  |
| --- | --- |
| Regex-выражение | (\<\d{1,5}\>)(\w{3}\s\d+\s\d{1,4}\s[\d:]\*)\s(\S\*)\s(\S\*):([\w\s]\*.)\s\((\w\*\=[\d.]\*)\,\s(\w\*\=\S\*)\,\s(\w\*\=\w\*)\,\s(\w\*\=\d)\,\s(\w\*\=\w\*)\) |
| Regex Link | https://regex101.com/r/WHlZuP/1 |
| Описание события | Ошибка смены пароля, пароль введен 5 раз неверно  Разобрал событие на группы: Num, Date\_time, Device, Reguests, Message, IP, VpnName, UserName, Times, Reason |

* <27>Dec 29 14:50:29 hmc-p730 HMC: HSCE2001 User name hscroot: Logical Partition test with ID 14\*8231-E2C\*06C5DER failed to be created in managed system Server-8231-E2C-SN06C5DER

|  |  |
| --- | --- |
| Regex-выражение | (\<\d{1,5}\>)(\w{3}\s{2}\d{2}\s[\d:]\*)\s(.\*?)\:\s(\S\*)\s([\w\s]\*)\:\s([\S\*\s]\*(ID\s\S\*)\s[a-z]\*.\*)\s(\S\*)$ |
| Regex Link | https://regex101.com/r/GM1YiT/1 |
| Описание события | Пользователь hscroot, ошибка создания логического раздела (test) на сервере  Разобрал на группы: Num, Date\_time, Device, ParentPartition, User, Message, ID\_Partition, ServerName |

* 2017/12/26 13:03:12 MSK,0,0,,Authentication Service,Success Access,27,Initial authentication successful,otadmin@otds.admin,,Authentication success: otadmin@otds.admin from host 10.56.70.77 with address 10.56.70.77 for resource \_\_OTDS\_AS\_\_

|  |  |
| --- | --- |
| Regex-выражение | (\d{4}[\/\d{1,2}]\*\s[\d{1,2}:]\*\s[A-Z]\*[,\d]\*)([\w\s]\*)\,([\w\s]\*)\,(\d{1,3})\,([\w\s]\*\,[\w\@\.]\*\,\S)([\S\s]\*\:\s[\w\@\.]\*)\s\w\*\s([\w]\*\s[\d{1,2}\.]\*\s[\w\s]\*\s[\d{1,2}\.]\*)\s[[a-z]+\s]\*([\w\s]\*)$ |
| Regex Link | https://regex101.com/r/fW04A8/1 |
| Описание события | Успешная аутентификация на сервере OTDS пользователя otadmin@otds.admin c хоста 10.56.70.77  Разобрал на группы: Date\_time, Service, AccessStatus, ProcessPID, InitialUserAuthenticationStatus, UserAuthenticationStatus, SourceHost, Resource |

1. Написать SQL запрос, который cделает выборку всех данных, объединив 3 таблицы вместе «DAT.PUBLIC.COMMON», «DAT.PUBLIC.USER», «DAT.PUBLIC.DOC» по общим признакам (объедение сделать через JOIN). Исключить из выборки события от пользователя с UserID=14. При этом отсортировать дату позднее «11-05-2018 12:13».

Чем будет отличаться SQL-запрос, если указанные данные будут храниться в СУБД Oracle?

SELECT \* FROM 'DAT.PUBLIC.COMMON'

JOIN 'DAT.PUBLIC.USER' ON ('DAT.PUBLIC.USER'.UserID = 'DAT.PUBLIC.COMMON'.UserID)

JOIN 'DAT.PUBLIC.DOC' ON ('DAT.PUBLIC.DOC'.DataID = 'DAT.PUBLIC.COMMON'.DataID )

WHERE 'DAT.PUBLIC.COMMON'.UserID <> 14

ORDER BY datetime(Timestamp) > '11-05-2018 12:13'

Конкретно данный запрос, я думаю, не будет отличаться, если данные будут храниться в Oracle, единственное может операции управлением временными данными.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DAT.PUBLIC.COMMON |  |  |  |  |  |  |  |  |  |  |
| **Timestamp** | **EventNubmer** | **Severity** | **EventID** | **EventName** | **UserID** | **ServerID** | **ServerName** | **DeviceID** | **DeviceName** | **DataID** |
| 11-05-2018 12:13:05.135 | 1 | Critical | 45 | Печать выходной формы №23 | 12 | 10.10.10.10 | GEOSERVER.CORP.LOC | 11 | Printer-11 | 1245 |
| 12-05-2018 15:55:05.555 | 2 | Info | 45 | Печать выходной формы №23 | 13 | 10.10.10.10 | GEOSERVER.CORP.LOC | 11 | Printer-11 | 1145 |
| 13-05-2018 10:35:03.353 | 3 | High | 44 | Вывод на экран выходной формы №23 | 12 | 10.10.10.10 | GEOSERVER.CORP.LOC | 4 | Monitor-4 | 1245 |
| 14-05-2018 12:25:00.250 | 4 | Info | 44 | Вывод на экран выходной формы №23 | 13 | 10.10.10.10 | GEOSERVER.CORP.LOC | 4 | Monitor-4 | 1145 |
| 15-05-2018 18:43:05.435 | 5 | Info | 15 | Успешный вход пользователя | 14 | 10.10.10.10 | GEOSERVER.CORP.LOC |  |  |  |
| 16-05-2018 20:03:55.355 | 6 | High | 16 | Неуспешный вход пользователя | 13 | 10.10.10.10 | GEOSERVER.CORP.LOC |  |  |  |
| 18-05-2018 11:23:02.232 | 7 | High | 33 | Просмотр защищаемого ресурса | 12 | 10.10.10.10 | GEOSERVER.CORP.LOC |  |  | 1246 |

|  |  |  |  |
| --- | --- | --- | --- |
| DAT.PUBLIC.USER |  |  |  |
| **UserID** | **UserName** | **ClientAddress** | **ClientHostName** |
| 12 | Иванов А. А. | 192.168.45.35 | ARM-2.CORP.LOC |
| 13 | Петров А. А. | 192.168.45.36 | ARM-1.CORP.LOC |
| 14 | Сидоров А.А. | 192.168.45.37 | ARM-3.CORP.LOC |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DAT.PUBLIC.DOC |  |  |  |  |
| **DataID** | **DataName** | **DataDetail1** | **DataDetail2** | **DataConfidLevel** |
| 1245 | Doc1 | DOC1-1245 | Шифр "DOC1-1245" | Коммерческая тайна |
| 1145 | Doc14 | DOC14-1145 | Шифр "DOC1-1145" | Не коммерческая тайна |
| 1246 | Doc2 | DOC2-1246 | Шифр "DOC1-1246" | Коммерческая тайна |

1. Разработать bash-cкрипт[[1]](#footnote-1)1).

В каталоге /etc следующее содержимое:

[root@server /]# ls -l /etc/

drwxr-xr-x.  2 root root        6 Jun  6  2017 chkconfig.d

-rw-r--r--.  1 root root     1100 Jan 31  2017 chrony.conf

-rw-r-----.  1 root chrony    481 Jan 31  2017 chrony.keys

drwxr-xr-x.  2 root root       26 Jun 17 13:48 cifs-utils

drwxr-xr-x.  2 root root       54 Jun 17 13:48 cron.d

drwxr-xr-x.  2 root root       70 Jun 17 13:48 cron.daily

-rw-------.  1 root root        0 Mar 29  2017 cron.deny

drwxr-xr-x.  2 root root       41 Jun 17 13:48 cron.hourly

drwxr-xr-x.  2 root root        6 Dec 27  2013 cron.monthly

-rw-r--r--.  1 root root      451 Dec 27  2013 crontab

drwxr-xr-x.  2 root root        6 Dec 27  2013 cron.weekly

-rw-------.  1 root root        0 Jun 17 13:43 crypttab

-rw-r--r--.  1 root root     1620 May  4  2016 csh.cshrc

Необходимо написать скрипт для выполнения следующей задачи:

* в директории /etc выполнить архивацию каталогов, начинающихся с префикса cron\*;
* название архива должно совпадать с именем папки;
* сохранить архивы в папку /etc/bkp/.

После выполнения скрипта должен получится такой результат:

[root@server /]# ls -l /etc/bkp/

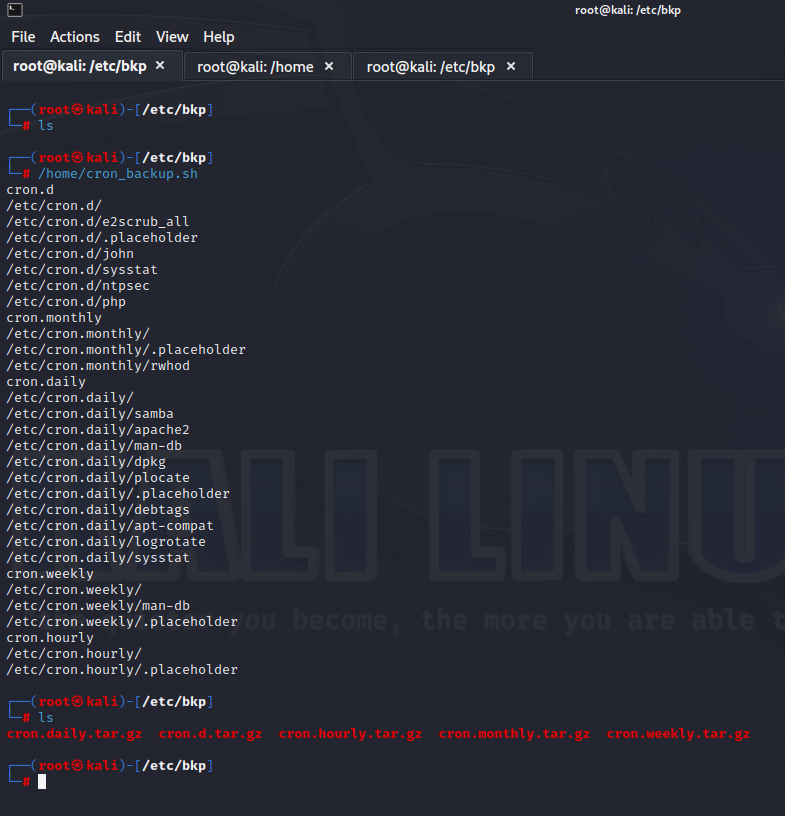
-rwxr-xr-x.  2 root root       54 Jun 17 13:48 cron.d.tar.gz

-rwxr-xr-x.  2 root root       70 Jun 17 13:48 cron.daily.tar.gz

-rwxr-xr-x.  2 root root       41 Jun 17 13:48 cron.hourly.tar.gz

-rwxr-xr-x.  2 root root        6 Dec 27  2013 cron.monthly.tar.gz

-rwxr-xr-x.  2 root root        6 Dec 27  2013 cron.weekly.tar.gz

 #!/bin/bash

find /etc -maxdepth 1 -name 'cron.\*' | sed 's|.\*/||' |

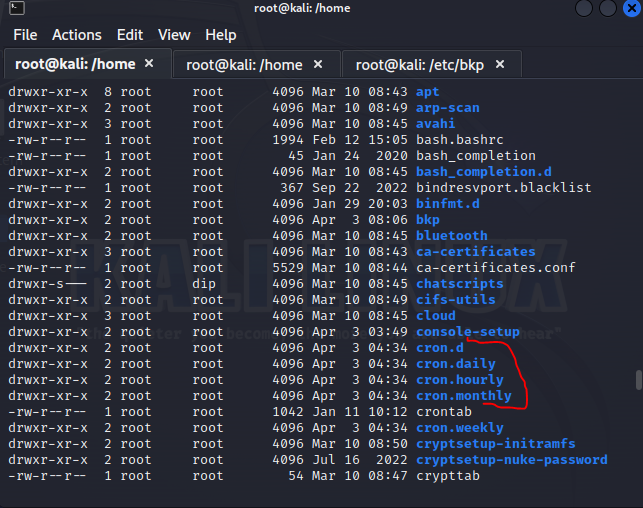
while read -r line

do

echo $line

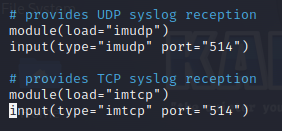
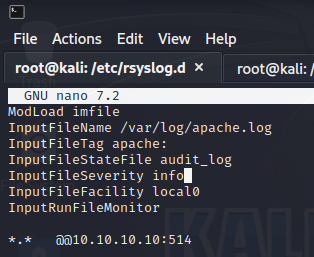
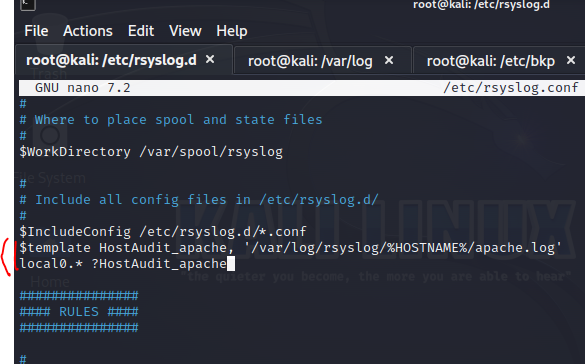
tar -cvf /etc/bkp/$line.tar.gz -P /etc/$line

done

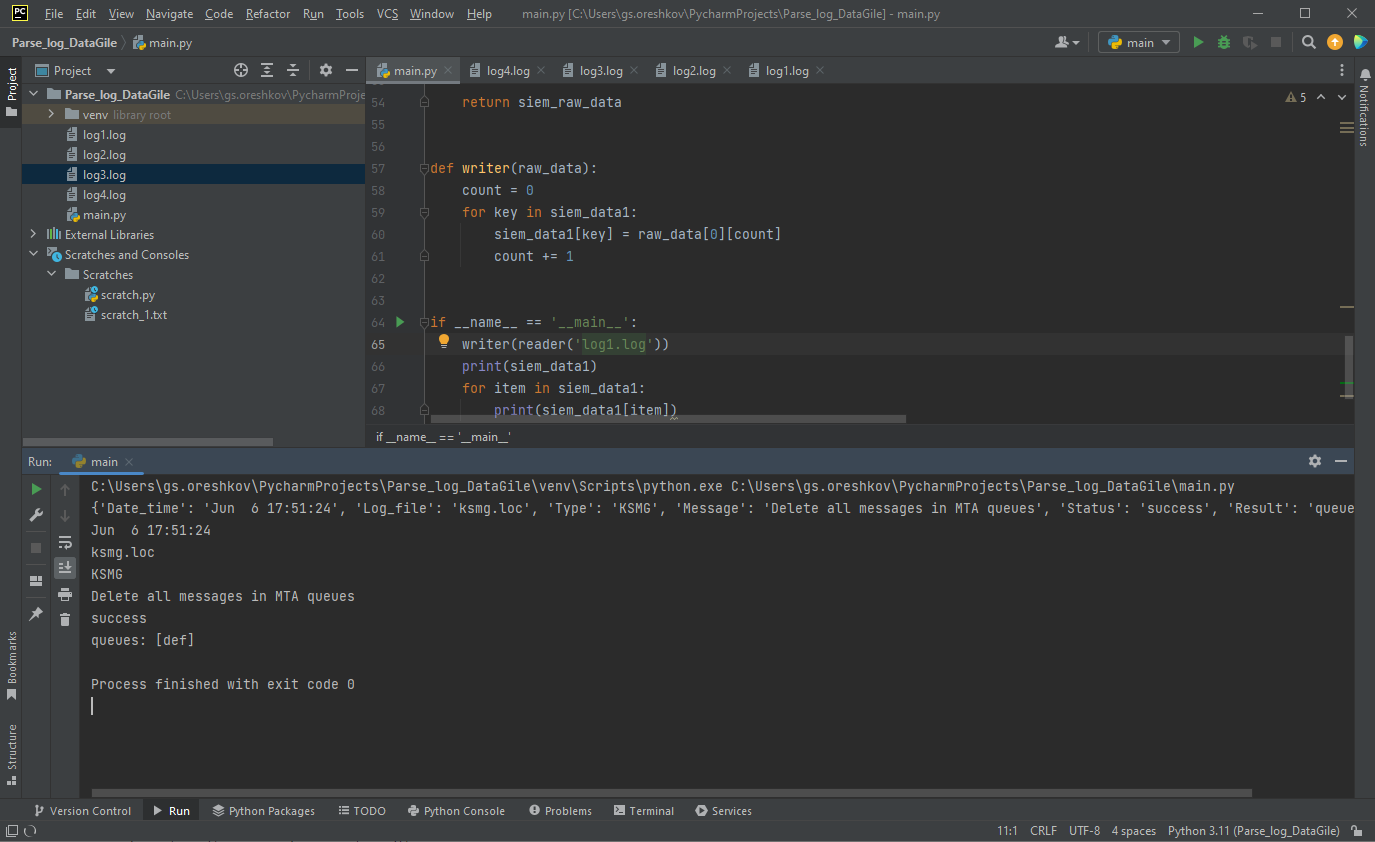


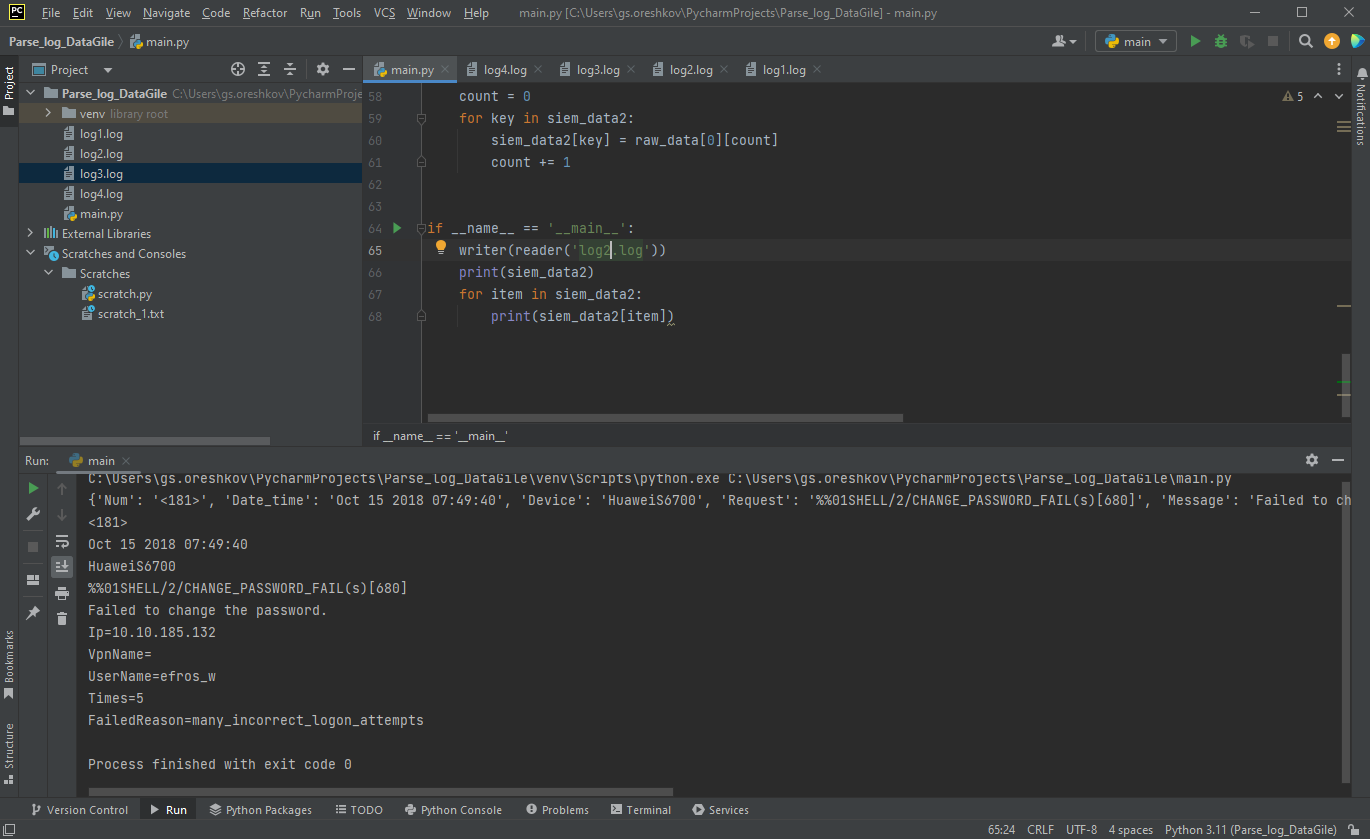
1. Привести перечень настроек для выполнения следующей задачи в Linux-подобной ОС (например, CentOS) - в ОС ведется запись событий ПО Apache в файл /var/log/apache.log. Используя демон rsyslog, настроить онлайн мониторинг файла и отправку событий по протоколу syslog на сервер 10.10.10.10:

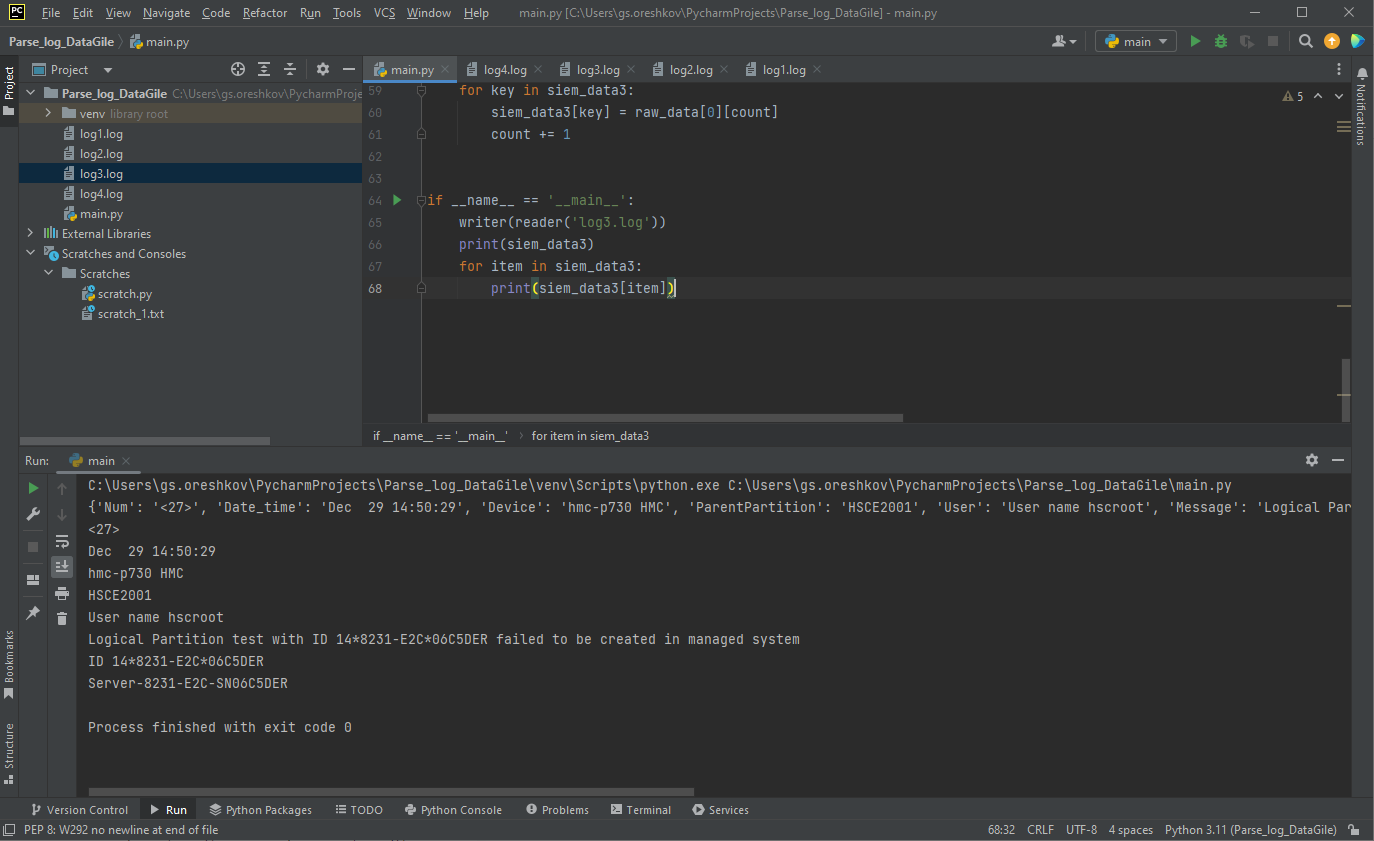
* Описать настройки rsyslog. Для всех событий добавлять метку «apache». События передавать на уровень local0.

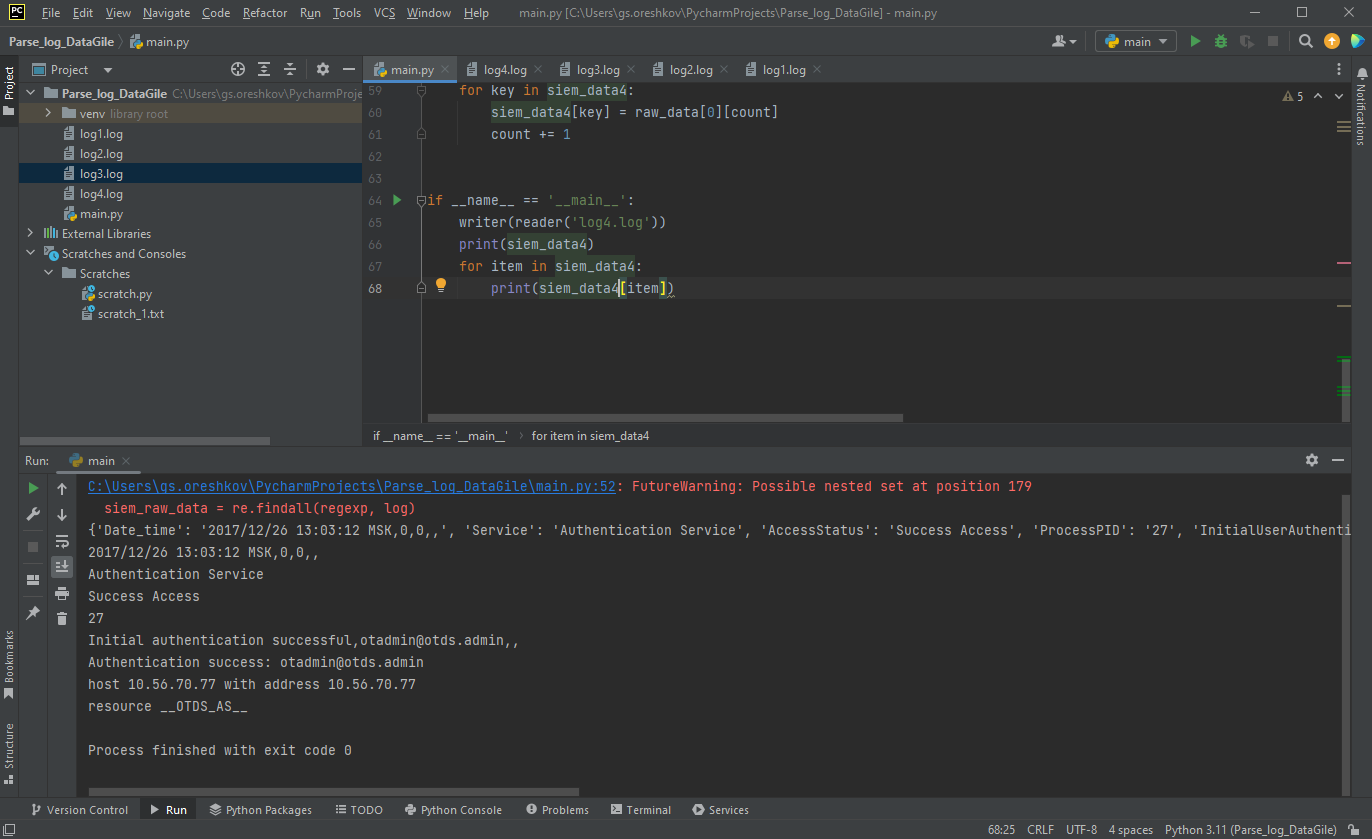
1. Синхронизирую время командой \cp /usr/share/zoneinfo/Europe/Moscow /etc/localtime
2. Открыл порты 514 tcp/udp командами: ufw allow 514/tcp && ufw allow 514/udp
3. Раскоментировал эти строки в файле rsyslog.conf для прослушивания tcp/udp на порте 514 
4. На клиенте создам в /etc/rsyslog.d конфиг rsys\_audit\_apache.conf в котором укажу метку apache, категории событий info, уровень серьезности local0, передам все логи \*.\* на сервер 10.10.10.10:514
5. На сервере настрою фильтрацию сообщений, в rsyslog.conf создам шаблон HostAudit\_apache, который принимает логи категории local0
6. Перезапущу rsyslog на сервере и клиенте после настроек командой: service rsyslog restart

Работа программы









1. 1) В случае сложностей можно использовать альтернативный язык программирования, к примеру Python [↑](#footnote-ref-1)