Задание 3.

10 октября 2024 года в 17:25 SIEM система компании «Must Do It» обнаружила **угрозу межсайтового скриптинга** на одном из компьютеров пользователей. Известно, что злоумышленник пользовался в это время браузером **Mozilla Firefox**. После чего в здании было вырублено электричество, и нарушитель успел скрыться. Из-за перебоев с электричеством записи с камер и часть журнала безопасности были повреждены. Вам необходимо восстановить резервную копию базы данных на своем компьютере при помощи инструмента DBeaver с подключенной СУБД PostgreSQL. При помощи SQL-запросов определите **имя и ip-адрес преступника**, используя всю доступную вам информацию в базе данных. И помните, время не на вашей стороне. Советуем начать с таблицы **security_journal,** схемы БД и сайта баз данных угроз ФСТЭК - https://bdu.fstec.ru/threat, для определения названия угрозы.

*Резервная копия базы данных **TaskSQL.backup** расположена в том же репозитории, где файл с этим заданием. В качестве ответа на задание необходимо создать файл с расширением «.txt» или «.sql». В файле необходимо указать имя и ip_адрес преступника, а также SQL-запросы, которые подтверждают причастность данного сотрудника к произошедшему инциденту, т.е. с помощью которых вы нашли злоумышленника. Оценивается правильность ваше ответа, а также количество и структура SQL-запросов с помощью которых вы выполнили задание.*

В базе данных расположены следующие таблицы:

1. *security_journal – таблица с произошедшими угрозами ИБ в компании*
2. *vlan – таблица с номерами виртуальных сетей компании*
3. *pc – таблица с информацией об устройствах в сети организации*
4. *employees – таблица с данными о сотрудниках организации*
5. *statuses – таблица с данными о рабочем статусе сотрудника*
6. *employee_report – таблица с отчетами сотрудников и их алиби в день происшествия*
7. *applications – таблица с сессиями браузеров и временем их запуска на устройствах*