# СЗИ-11-1

## Жители в опасности

### Условие задачи

В этом варианте был атакован сервис хранения рецептов зелий. Предоставлены журналы Elastic‑агента, содержащие события атаки на несколько хостов. Нужно ответить на семь вопросов. Для каждого вопроса допускается не более трёх попыток, ответы отправляются без форматирования vsosh{}.

### Что требуется найти

1. Путь до вредоносного файла, загруженного на хост.
2. Имя файла лога, содержащего учетные данные.
3. Протокол, использованный злоумышленником для подключения к хосту 2.
4. Название скрипта разведки, применённого на хосте 2.
5. Папка, использованная для повышения привилегий на хосте 2.
6. Учётная запись, с которой злоумышленник подключился к базе данных.
7. База данных и таблица, откуда выгружались данные пользователей (формат db\_name:table\_name).

### Используемые инструменты

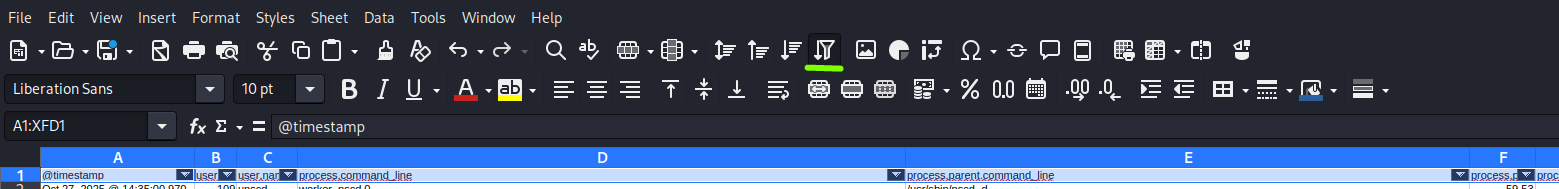
LibreOffice Calc, текстовые редакторы

### Анализ и решение

Логи отражают этапы атаки: сначала пользователь загружает вредоносный файл с и устанавливает обратное соединение, затем повышает привилегии за счет доступных логов и пароля в них, далее обнаруживает возможность подключиться ко второму хосту. Выполняет подключение по VNC и запускает разведку linpeas. Повышает привилегии за счет прав на mount и получает УЗ от базы данных сервера. Подключается к базе и эксфильтрует важные данные.

**Вредоносный файл**

1. Открываем логи и создаем сортировку для столбцов



1. Видим, что злоумышленник обнаружил OS command injection и загрузил реверс-шелл на хост - файл WSO\_4\_0\_5.php

Изображение выглядит как текст, снимок экрана, число, программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

1. Понимая, что сервис на php, можно с легко определить, что скорее всего сайт расположен в /var/www. Суди по логам, файл был загружен в папку uploads, значит ответ - /var/www/uploads/WSO\_4\_0\_5.php

**Лог с учетными данными.** Злоумышленник запускает linpeas для разведки повышения прав и судя по всему, обнаруживает доступ к файл auth.log, который обычно не доступен www-data и может содержать учетные данные входящих пользователей. Ответ: auth.log

Изображение выглядит как текст, снимок экрана, число, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Протокол подключения к хосту 2.** Смотри логи второго хоста, видим подозрительную активность пользователя Minecraft-user – запуск linpeas, просмотр bash\_history, whoami.

Изображение выглядит как текст, линия, число, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

Пытаемся найти по parent process id, откуда появился процесс /usr/bin/xtgern. Находим запись с родительским процессом – tighvncserver. Становится понятно, что протокол подключения злоумышленника - VNC. Ответ: vnc



**Скрипт разведки.** На втором хосте запускался LinEnum.sh — классический Bash‑скрипт для сбора информации о системе. Ответ: LinEnum.sh

Изображение выглядит как текст, Шрифт, число, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Папка для повышения привилегий.** В логах видно, что после перечисления LinEnum, злоумышленник пробует выполнить команду mount. Вероятно на нее были повешены sudo права и злоумышленник успешно их эксплуатирует, присоединяя корень диска в созданную папку. Ответ: /tmp/root или /dev/vda2, принимались оба.

Изображение выглядит как текст, снимок экрана, линия, Шрифт

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Учётная запись базы данных.** Для подключения к базе данных злоумышленник использовал пользователя web\_user. Ответ: web\_user

**Источник данных пользователей.** Данные выгружались из базы данных minecraft из таблицы public.users

Ответ: minecraft:public.users или minecraft:users, принимались оба.

### Итог

| Вопрос | Ответ |
| --- | --- |
| 1 | /var/www/uploads/WSO\_4\_0\_5.php |
| 2 | auth.log |
| 3 | vnc |
| 4 | LinEnum.sh |
| 5 | /tmp/root |
| 6 | web\_user |
| 7 | minecraft:public.users |