# СЗИ-9-1

## Жители в опасности

### Условие задачи

На деревню жителей была совершена атака: служба приёма соискателей захвачена и разорена. Наблюдатель сумел записать происходящее и передал файл журналов. Необходимо проанализировать CSV‑логи Elastic‑агента и ответить на ряд вопросов. Для каждого вопроса допускается не более трёх попыток, ответы отправляются без форматирования vsosh{}.

### Что требуется найти

1. Название вредоносного документа, который загрузил пользователь (с расширением).
2. Адрес и порт, на которые был установлен обратный шелл (формат ip:port).
3. Исполняемый файл, с помощью которого злоумышленник повысил привилегии (полный путь).
4. Команда, которой злоумышленник нашёл этот файл.
5. Команда, с помощью которой злоумышленник получил хэши пользователей.

### Используемые инструменты

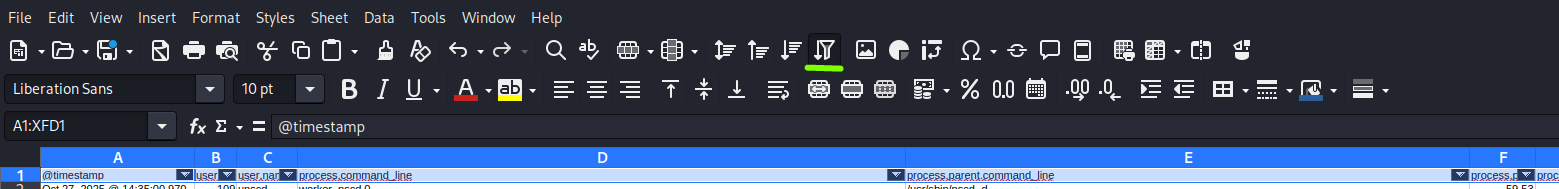
LibreOffice Calc, текстовые редакторы

### Анализ и решение

Логи отражают этапы атаки: сначала пользователь загружает вредоносный документ, затем злоумышленник устанавливает обратное соединение, повышает привилегии, ищет файлы SUID и читает /etc/shadow.

**Вредоносный документ**

1. Открываем логи и создаем сортировку для столбцов



1. Проверяем столбец с ip адресами, находим странные подключения, похожие на реверс-шелл

Изображение выглядит как текст, снимок экрана, число, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

1. Сверяем process id процессов – родительского и дочернего и видим, что открытие файла с резюме resume\_somina\_olga.odt привело к реверс-шеллу.

**Адрес обратного шелла.** В логах сетевых подключений присутствует исходящее соединение на 92.255.109.123:9001. Такой тип соединения называют реверс-шеллом: атакуемый устанавливает связь с сервером атакующего. Ответ: 92.255.109.123:9001

**Далее все этапы можно найти, применяя фильтры по parent process id/пользователю**

**Файл для повышения привилегий.** Анализ команд показывает запуск бинарника /tmp/security-check с повышенными правами. Этот исполняемый файл использовался для получения root. Ответ: /tmp/security-check

**Команда поиска.** Перед запуском этого бинарника злоумышленник выполнил поиск всех файлов с установленным битом SUID: find / -perm -4000 2>/dev/null. Эта команда перебирает всю файловую систему, игнорируя сообщения об ошибках. Ответ: find / -perm -4000 2>/dev/null (вариант без перенаправления ошибок также принимается).

**Получение хэшей пользователей.** После повышения привилегий злоумышленник просматривает содержимое файла /etc/shadow, который содержит хеши паролей. Команда cat /etc/shadow позволяет вывести его содержимое. Ответ: cat /etc/shadow

### Итог

| Вопрос | Ответ |
| --- | --- |
| 1 | resume\_somina\_olga.odt |
| 2 | 92.255.109.123:9001 |
| 3 | /tmp/security-check |
| 4 | find / -perm -4000 2>/dev/null |
| 5 | cat /etc/shadow |