**ЛАБОРАТОРНАЯ РАБОТА №1. LIME И VOLATILITY. ФОРЕНЗИКА.**

Касаткин Александр Денисович

11-902

**Содержание**

1. **Создание виртуальной машины**
2. **Смена паролей в Metasploitable**
3. **Обновление источников пакета**
4. **Установка LiMe**
5. **Установка вспомогательных библиотек**
6. **Скачивание, настройка и установка фреймворка Volatility**
7. **Форензика**
8. **Оформление результатов работы**

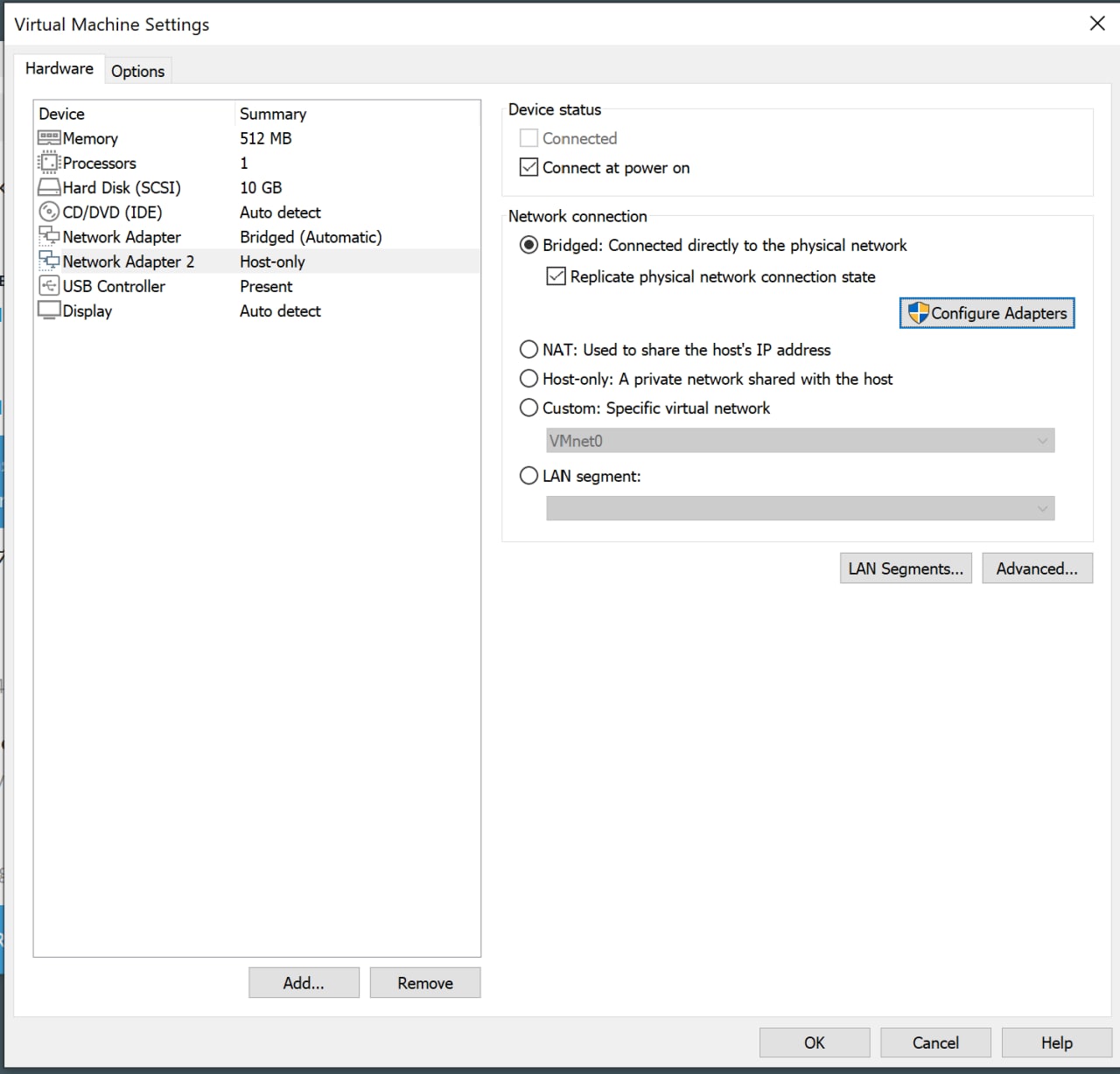
Создание виртуальной машины

## Цель упражнения

Научится создавать виртуальную машину

## Выполнение задания

1. Скачиваем VMware
2. Скачиваем Metasploitable
3. Запускаем VMware, выбираем существующую виртуальную машину
4. Настраиваем виртуальную машину в соответствии с примечанием в задании
5. Запускаем виртуальную машину



## Результат

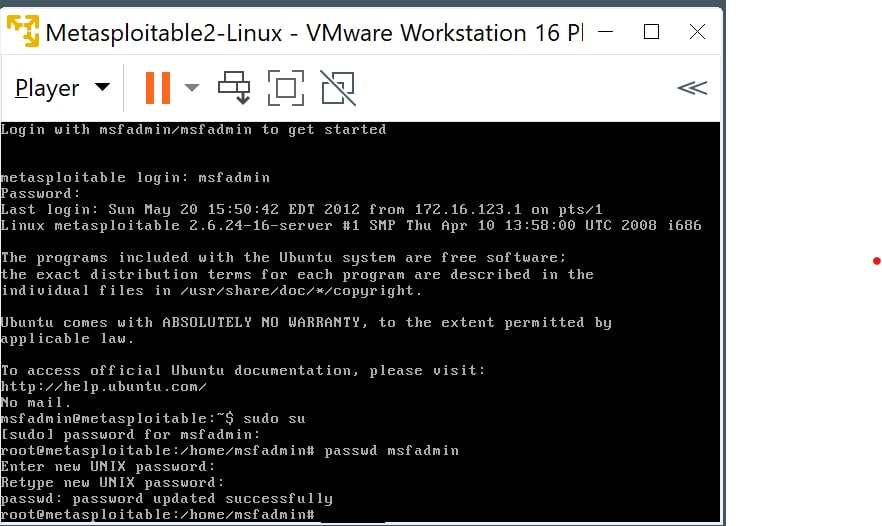
Научились открывать (создавать) виртуальную маг=шину в VMWare

Смена паролей в Metasploitable

## Цель упражнения

Научится менять пароль в Metasploitable

## Выполнение задания



## Результат

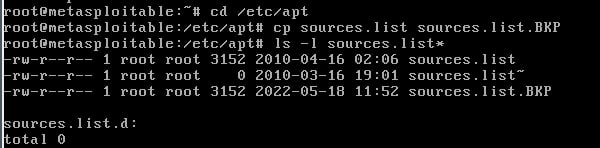
Научились менять пароль

Обновление источников пакета

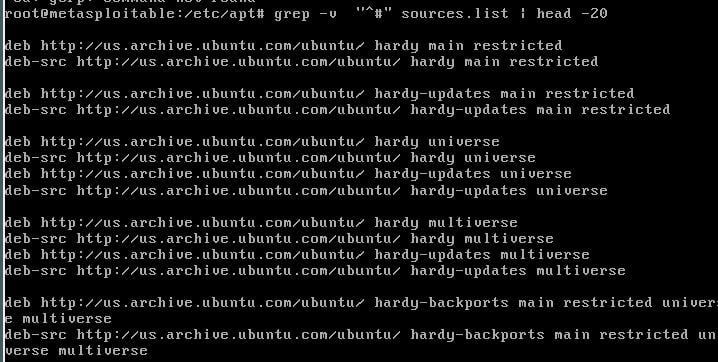
## Цель упражнения

Научиться обновлять пакетный менеджер (apt)

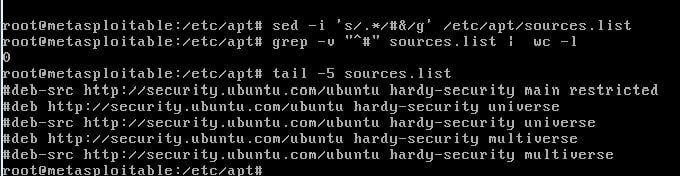
## Выполнение задания

План:   
**1.Создание backup-файла репозиториев**

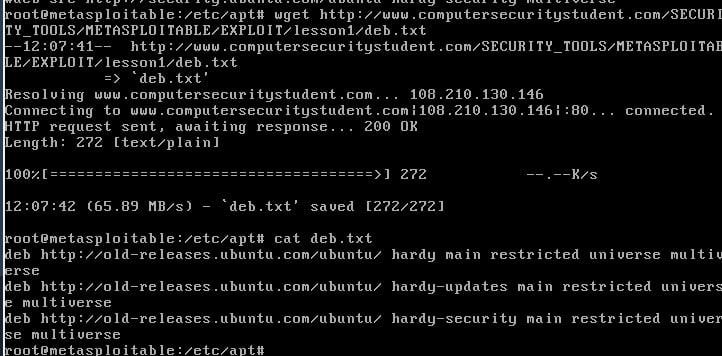
### **2.Просмотр списка репозиториев**

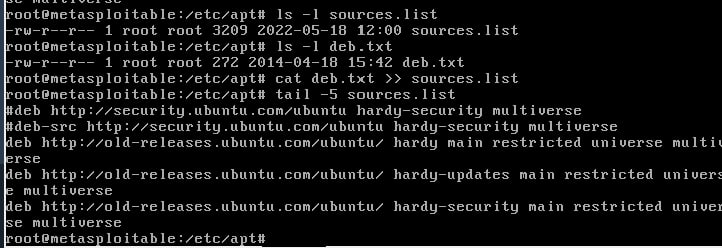


### **3.Отключение репозиториев**

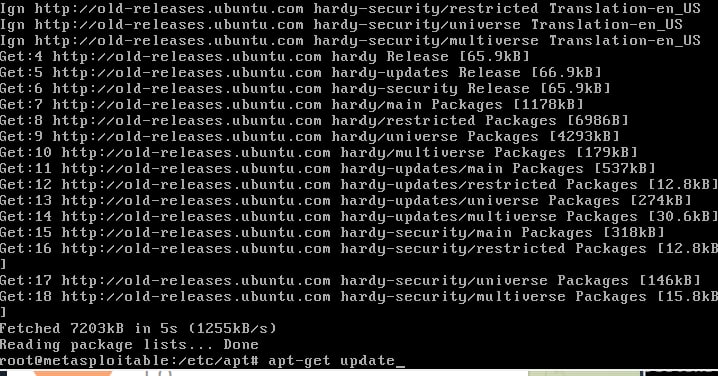


### **4.Добавление репозиториев из файла deb.txt в список репозиториев**

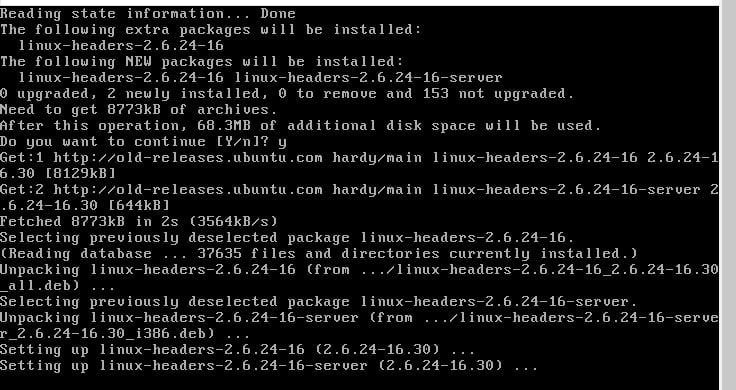




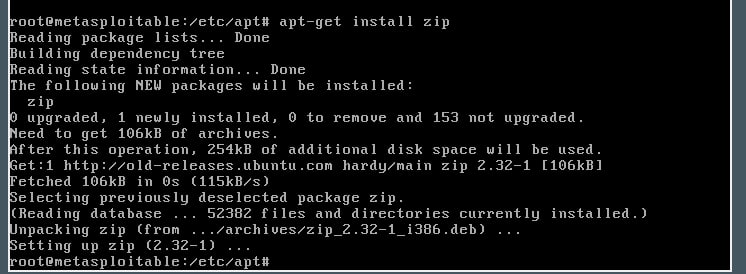
### **5.Обновить список репозиториев для менеджера пакетов apt**



### **6.Установка заголовочных файлов ядра**



### **7.Установка утилиты Zip**

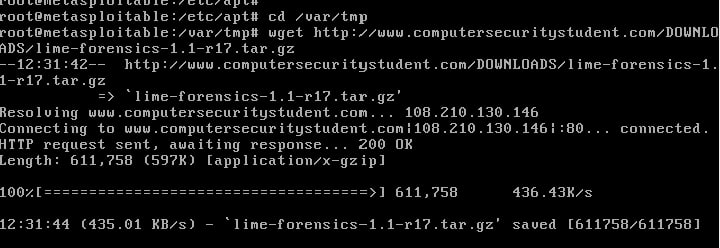


## Результат

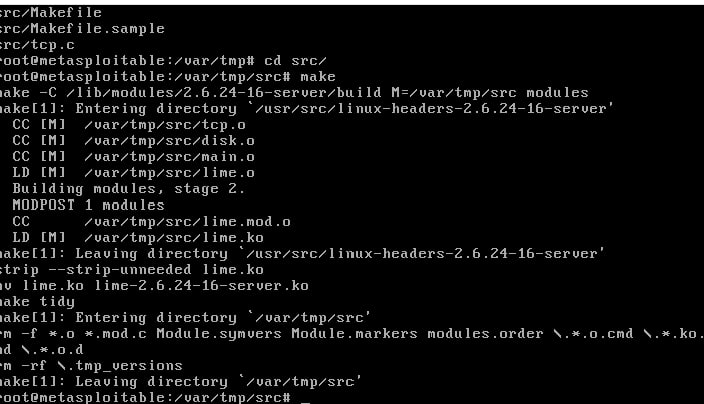
Научились обновлять пакетный менеджер (apt)

Установка LiME

1. **Скачивание архива с исходными текстами Lime**

****

1. **Распаковка и сборка Lime**

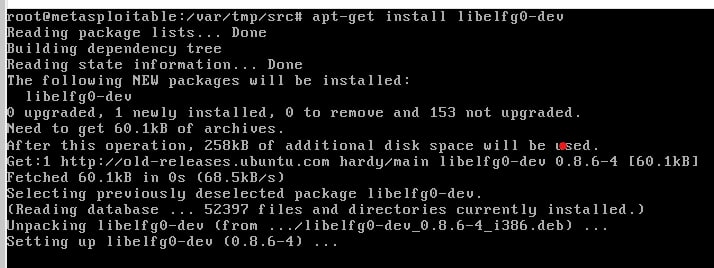


## Результат

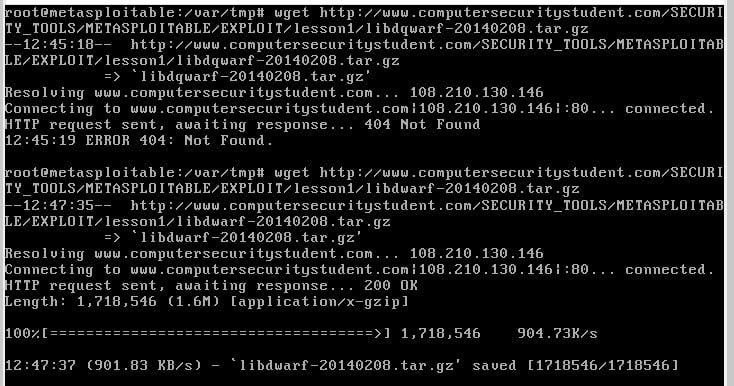
Установил LiMe

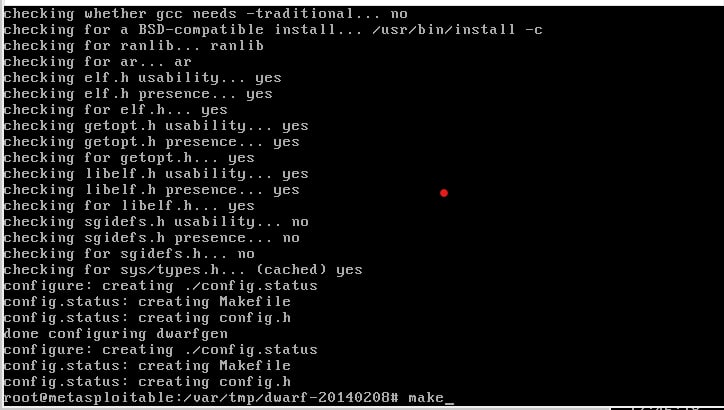
Установка вспомогательных библиотек

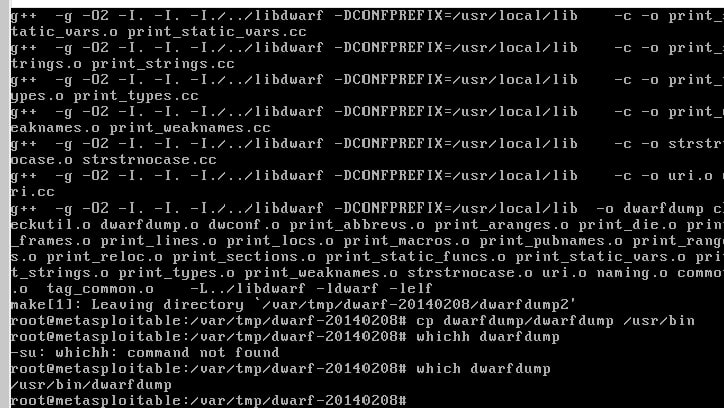
1. **Установка заголовочных файлов библиотеки libelf**

****

1. **Скачивание, настройка и установка библиотеки libdwarf**



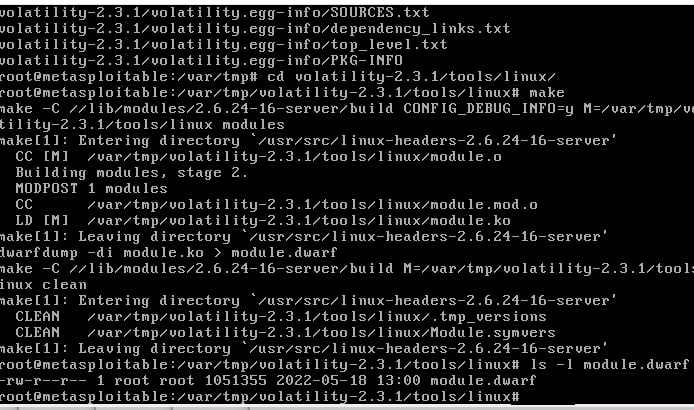
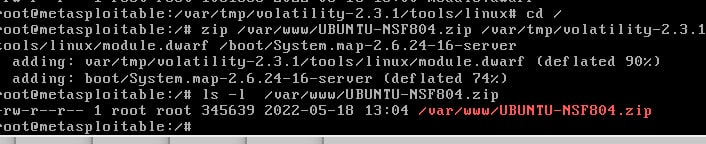




## Результат

Установил все нужные вспомогательные библиотеки

Скачивание, настройка и установка фреймворка Volatility

1. **Скачивание Volatility **
2. **Создание файла с отладочной информацией модуля ядра Metasploitable – module.dwarf **
3. **Создание профиля Volatility для Metasploitable **

## Результат

Скачал и настроил фреймворк Volality

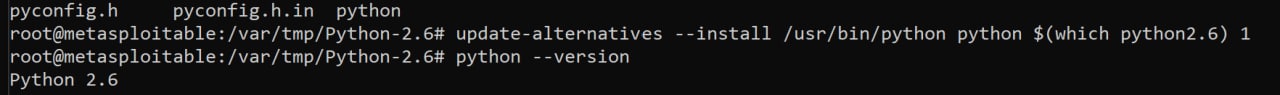
Форензика

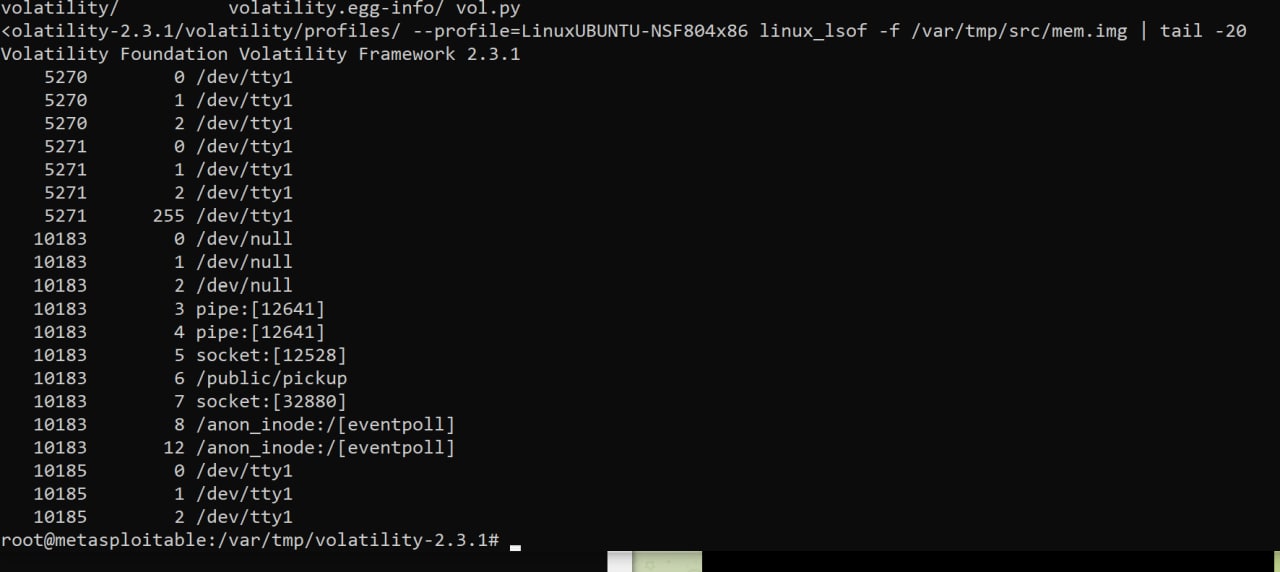
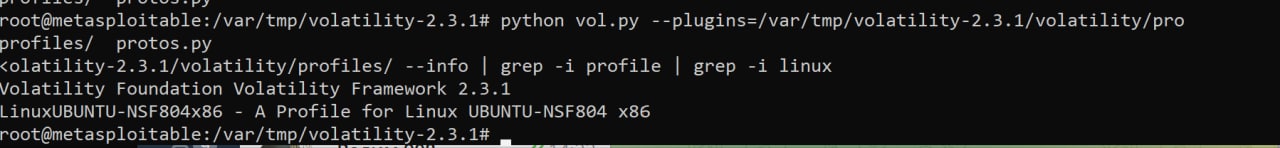
1. **Создание дампа памяти с помощью LiME**

****

****

1. **Просмотр активности в памяти в момент снятия дампа с помощью Volatility Теперь чтобы скачать файлы надо полностью перенастраивать apt, поэтому проще перекинуть файлы по ssh. Узнаю адрес и можно подключиться. После чего распакую файлы и поменяю python and python-crypto на vm**

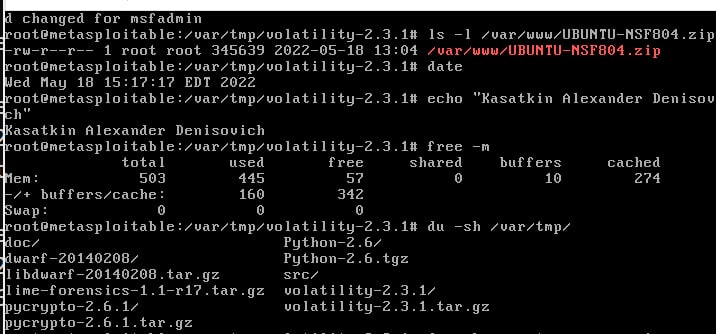
****

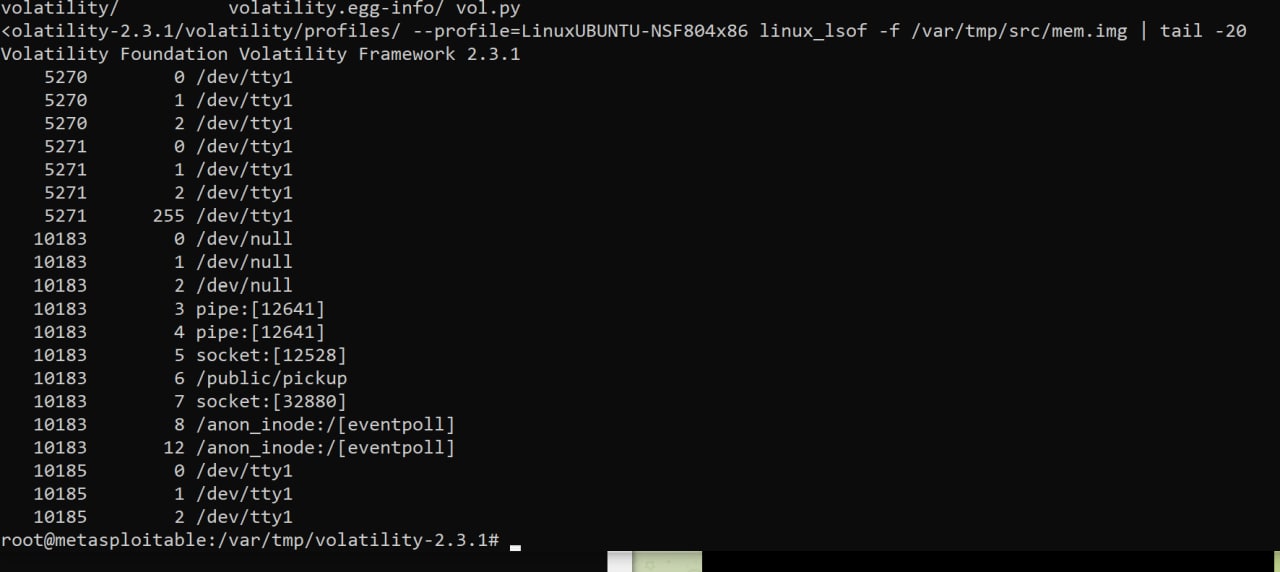
****

Результат

Научились передавать файлы по на vm и анализировать дампы памяти

**Оформление результатов работы**

****

****