Сабирзянова А.М.

11-901

LIME и VOLATILITY. ФОРЕНЗИКА

Содержание:

1. [**Создание виртуальной машины Metasploitable**](#_c93awmmpz97f) **1**

[**2. Смена паролей в Metaspoitable**](#_ta6tmtp881ik) **2**

[**3. Обновление источников пакетов**](#_e6mnoer6xmz3) **4**

[**4. Установка LIME**](#_5fcjzzonzu36) **6**

[**5. Установка вспомогательных библиотек**](#_rjg6wa4l1j0u) **7**

[**6. Скачивание Volatility**](#_m8k7i5lsumc6) **8**

[**7. Форензика**](#_svcpnu4nuqte) **10**

[**8. Результаты работы**](#_nde483ef9j9o) **11**

## Создание виртуальной машины Metasploitable

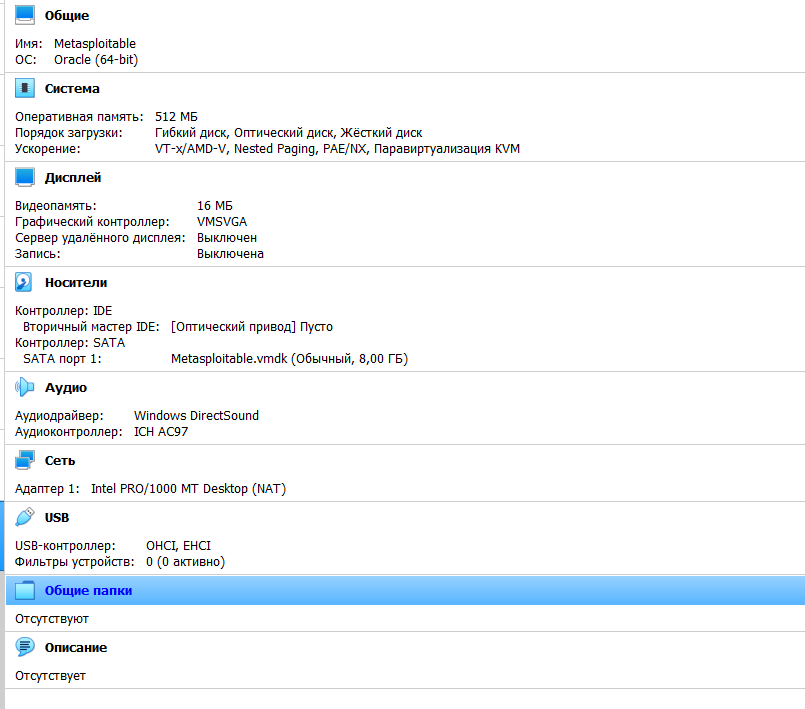
Цель: Создать машину для последующей работы

Начальная ситуация: имеем скачанное ПО

Алгоритм:

1. Заходим в VirtualBox
2. Создаем машину

Результат: машина создана

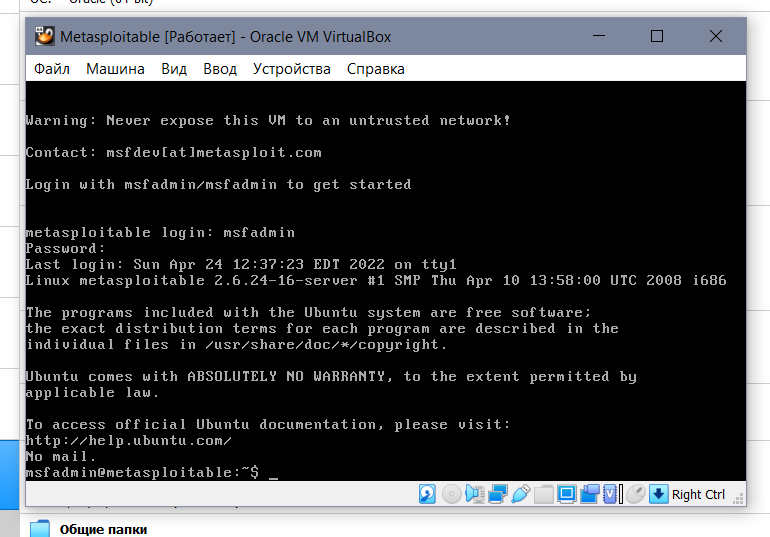
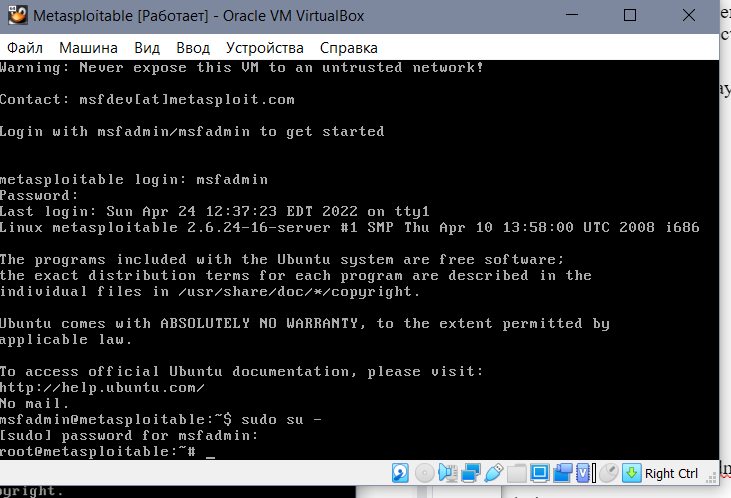


## 2. Смена паролей в Metaspoitable

Цель: Научиться менять пароли

Начальная ситуация: пользователь с паролем msfadmin и логином msfadmin

Алгоритм:

1. Вход в учетную запись с данными msfadmin, msfadmin
2. Получаем привилегии для суперпользователя sudo su - и вводим пароль 
3. Вводим команду passwd, задаем и подтверждаем новый пароль

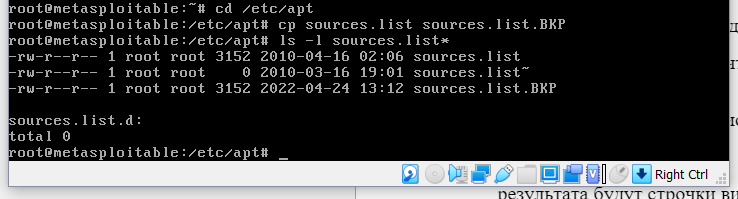
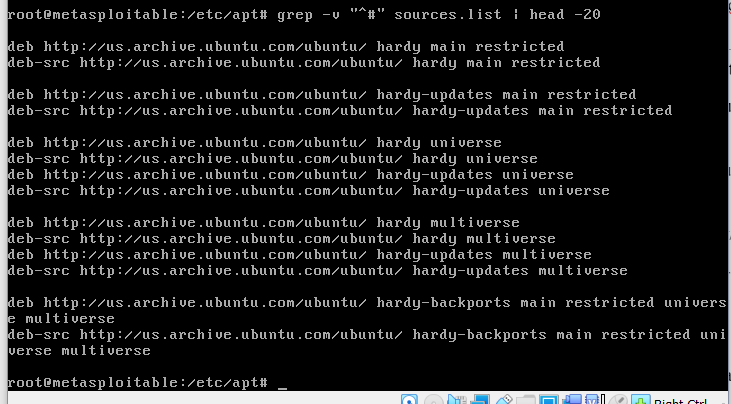
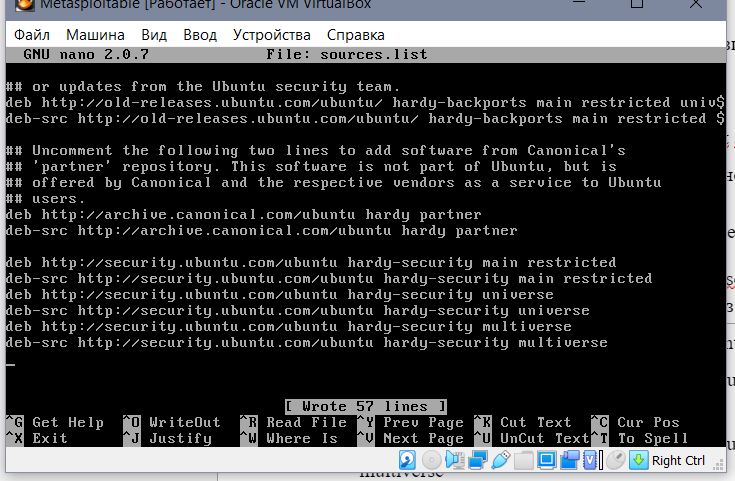
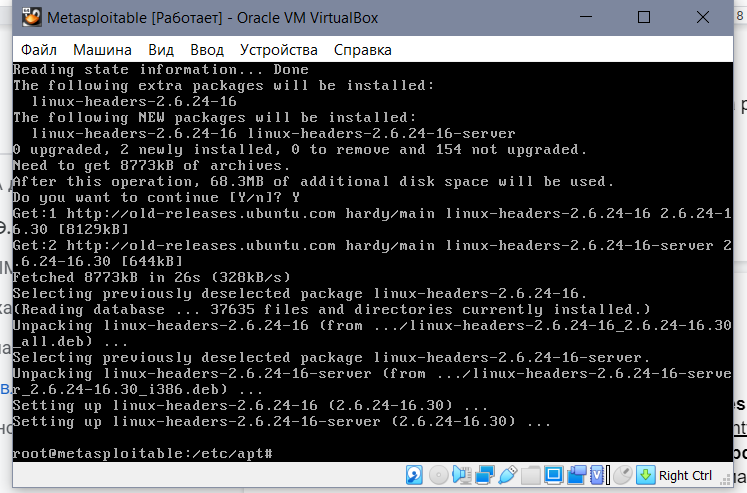
Результат: новый пароль задан успешно, проверка осуществлялась с помощью выхода из системы и повторного входа

## 3. Обновление источников пакетов

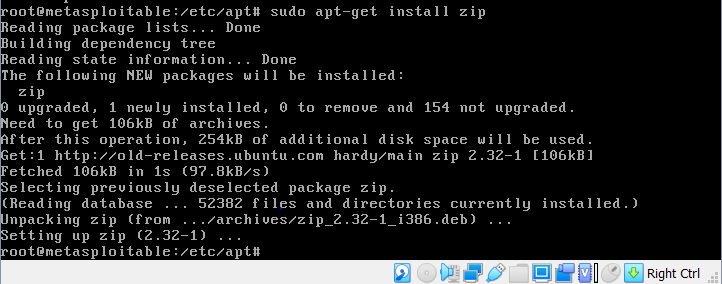
Цель: Поменять используемые репозитории

Начальная ситуация: есть исходные репозитории

Алгоритм:

1. В /etc/apt создаем файл sources.list.BKP 
2. Смотрим репозитории, которые есть на данный момент с помощью команды grep -v “^#” sources.list | head -20: (утилита работает с помощью регулярки, просматривает строки в файле sources.list, выводит все, которые не начинаются с #, просматриваем первые 20) 
3. Заходим в sources.list с админскими правами sudo nano sources.list, заменяем все us.archive на old-releases, сохраняем: 
4. Обновляем apt-get update
5. Узнаем версию ядра uname -r
6. Скачиваем заголовочные файлы ядра apt-get install linux-headers-2.6.24-16-server

1. Устанавливаем утилиты zip apt-get install zip



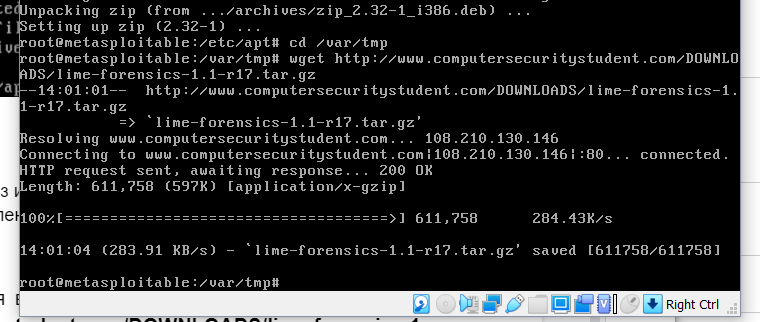
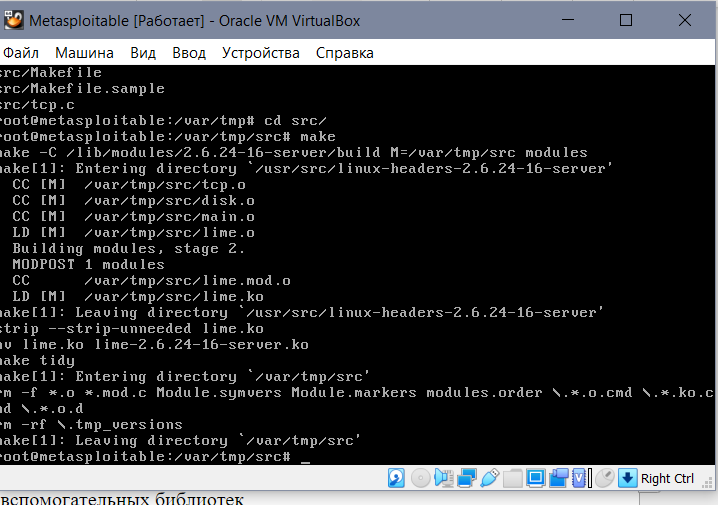
Результат: нужные утилиты установлены с нужных нам репозиториев

## 4. Установка LIME

Цель: установить LIME из исходных кодов

Начальное состояние: LIME не установлен

Алгоритм:

1. Входим в каталог cd /vat/tmp, скачиваем исходные коды wget <http://www.computersecuritystudent.com/DOWNLOADS/lime-forensics-1.1-r17.tar.gz> 
2. Распаковали архив tar zxvf lime\*.tar.gz, переходим в диалог исходных текстов, выполняем сборку 

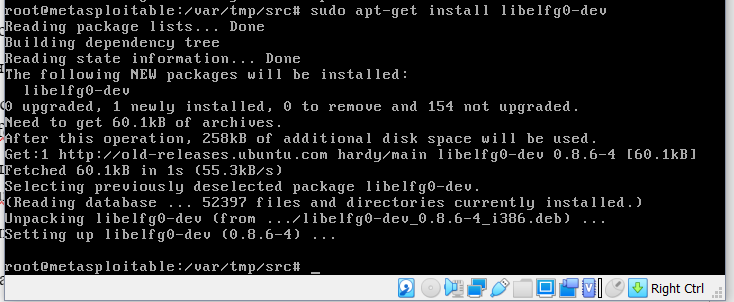
Результат: LIME установлен, но были проблемы с исходными кодами с сайта предложенного в описании лабы, пришлось использовать другой.

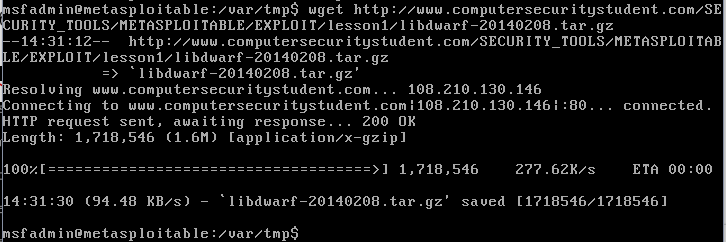
## 5. Установка вспомогательных библиотек

Цель: установить библиотеки

Ожидаемый результат: библиотеки установлены

Алгоритм:

1. Установим заголовочные файлы библиотеки libelf sudo apt-get install libelfg0-dev
2. Выходим из src cd .. и скачиваем библиотеку libdwarf wget http://www.computersecuritystudent.com/SECURITY\_TOOLS/METASPLOITABLE/EXPLOIT/lesson1/libdwarf-20140208.tar.gz



1. Распаковываем скачанный архив командой tar zxfv libdwarf-20140208.tar.gz
2. Переходим в распакованную папку cd libdwarf-20140208.tar.gz
3. Подготовим исходные тексты к сборке, вводим ./configure
4. Выполняем сборку командой make
5. Перемещаем dwarfdump в каталог исполняемых файлов командой cp dwarfdump/dwarfdump /usr/bin
6. Проверяем верно ли он перенесен

Результат: библиотеки установлены и находятся в usr/bin

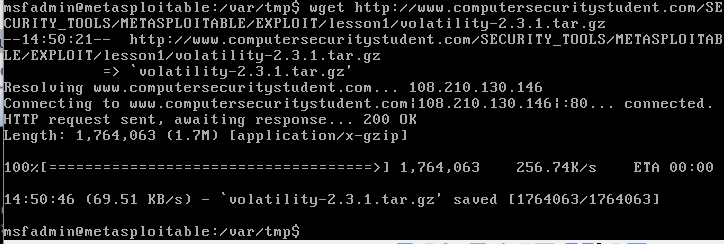
## 6. Скачивание Volatility

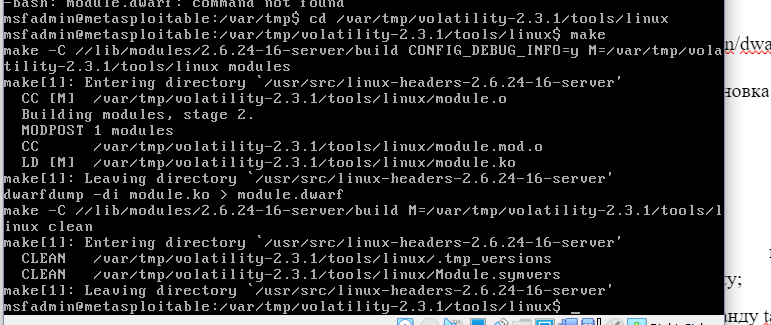
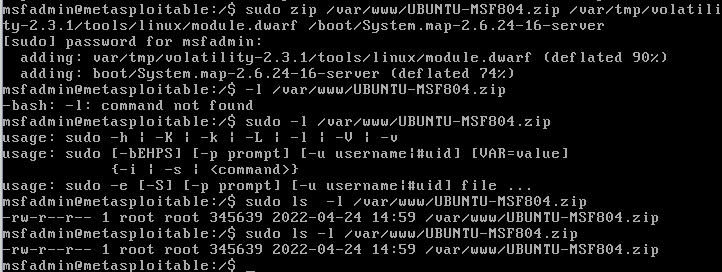
Цель: скачать Volatility

Начальная ситуация: Volatility не установлен

Алгоритм:

1. Выходим в cd var/tmp cd ..
2. Устанавливаем volatility wget http://www.computersecuritystudent.com/SECURITY\_TOOLS/METASPLOITABLE/EXPLOIT/lesson1/volatility-2.3.1.tar.gz



1. Войти в файл, собрать командой make 
2. Создать профиль командами из описания лабы, успешно: 

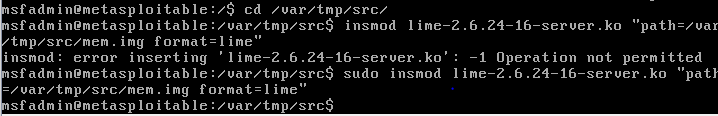
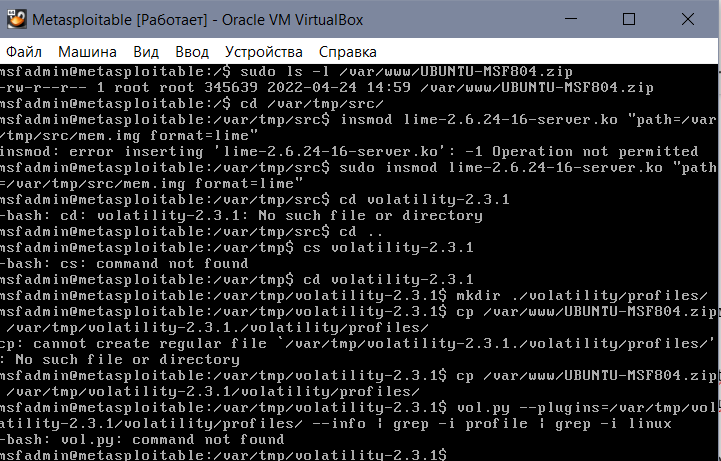
Результат: Volatility установлен и создан профиль

## 7. Форензика

Цель: создать дамп оперативки и проанализировать

Начальная ситуация: не скачана оперативная память

Алгоритм:

1. Создаем дамп памяти: 
2. Перемещаем архив и проверяем правильность переноса 

Результат: Память дампнута, но проанализировать не получилось из-за неработающего питона

## 8. Результаты работы