1. Создание виртуальной машины

Цель: Создание виртуальной машины

Начальная ситуация: скачанный образ

Алгоритм:   
Скачать и открыть VM

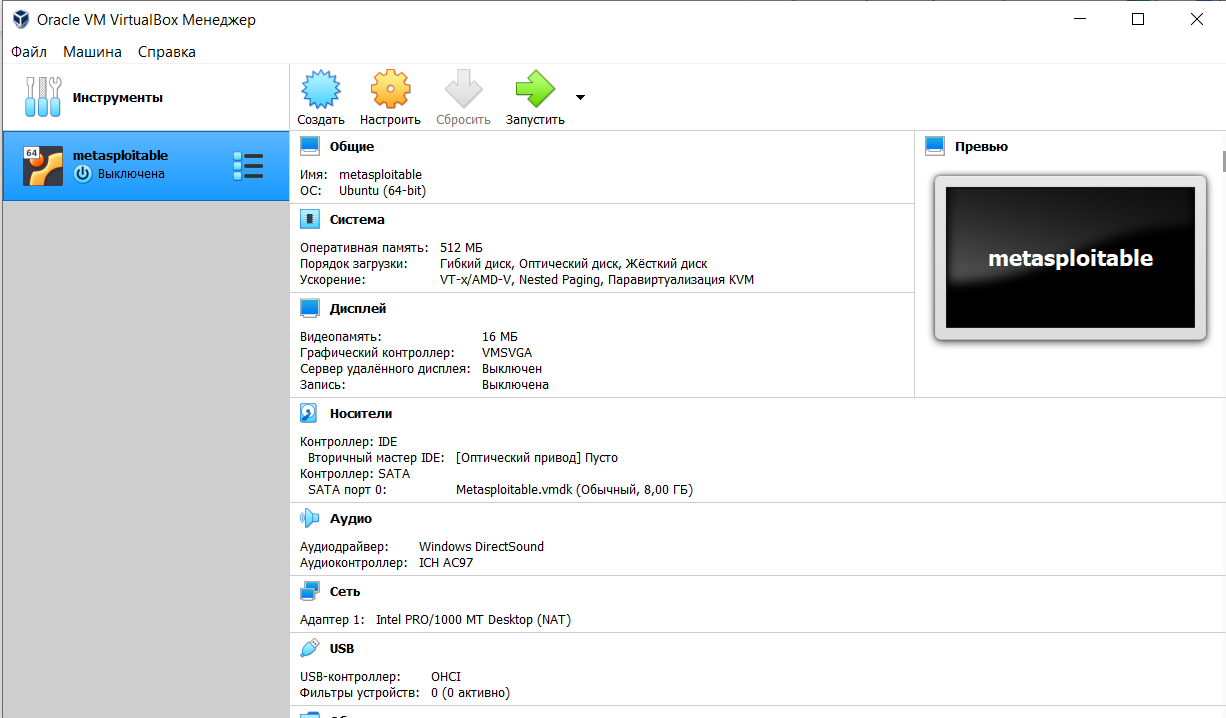
Создать машину

Архитектура: х64  
Количество процессоров: 1

ОЗУ: 512гб

Жесткий диск: 10гб

Тип сетевого подключения: сетевой мост



Итог: машина создана

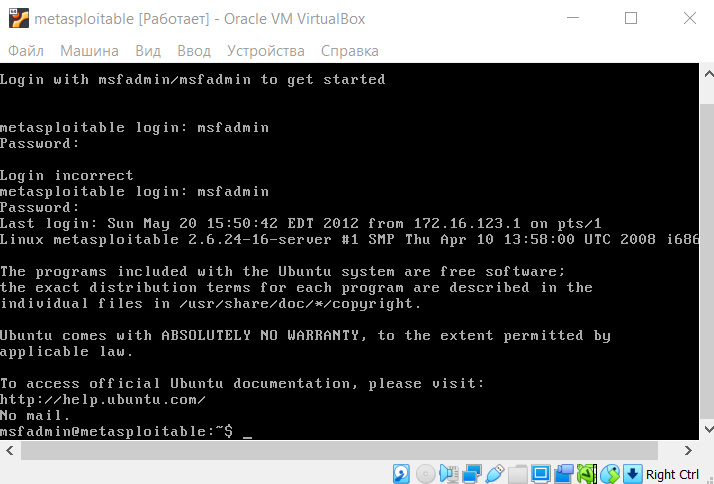
1. Смена паролей

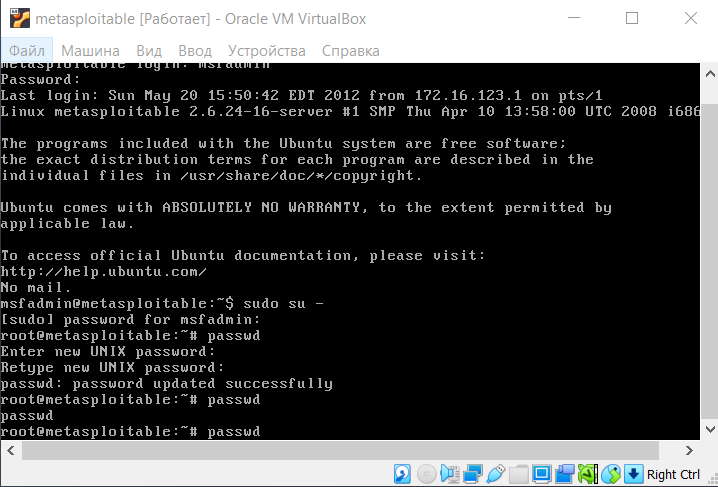
Цель: поменять пароль

Исходная ситуация: пользователь (msfadmin, msfadmin)

Алгоритм:

Запускаем машину, используем msfadmin для логина и пароля



Получаем права супер пользователя и меняем пароль

Итог: пароль изменен

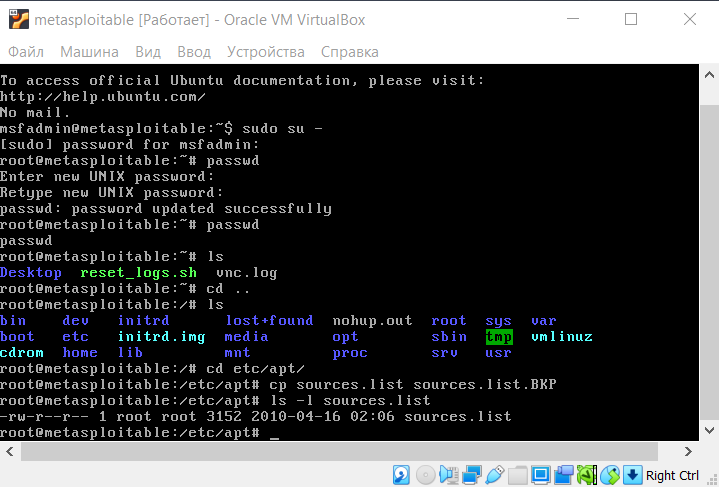
1. Создание backup-файла репозиториев

Цель: Обновление репозиториев

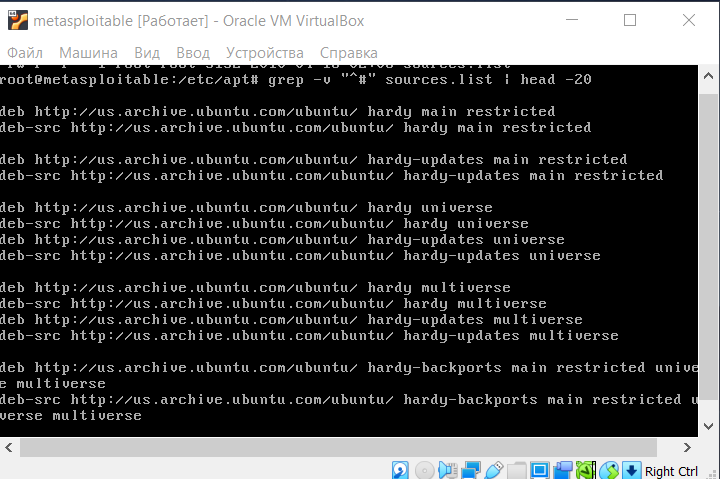
Начальная ситуация: исходные репозитории

Алгоритм:

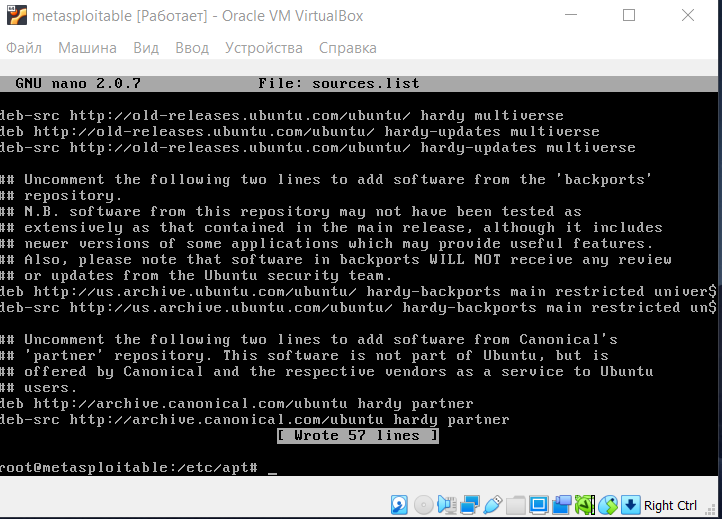
Создание sources.list



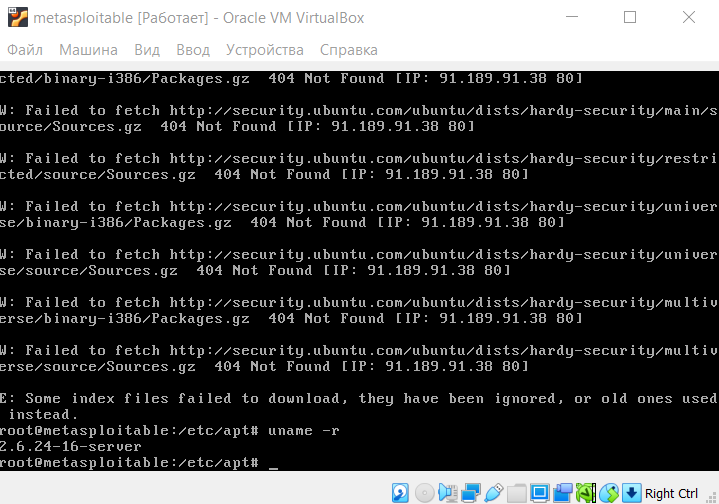
Просмотр списка репозиториев



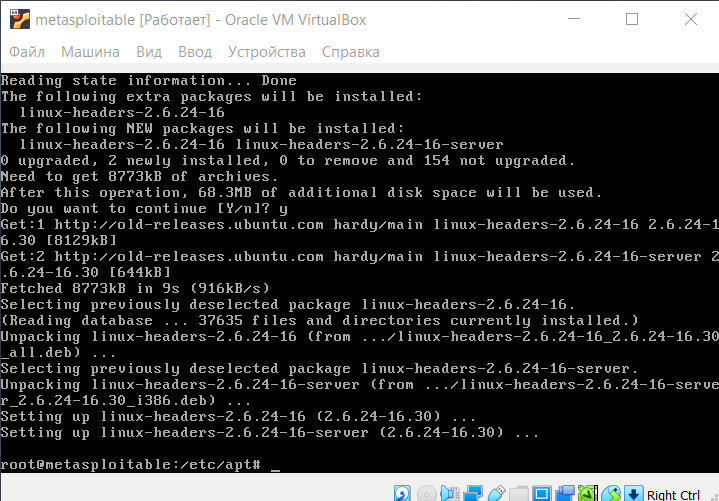
Замена репозиториев



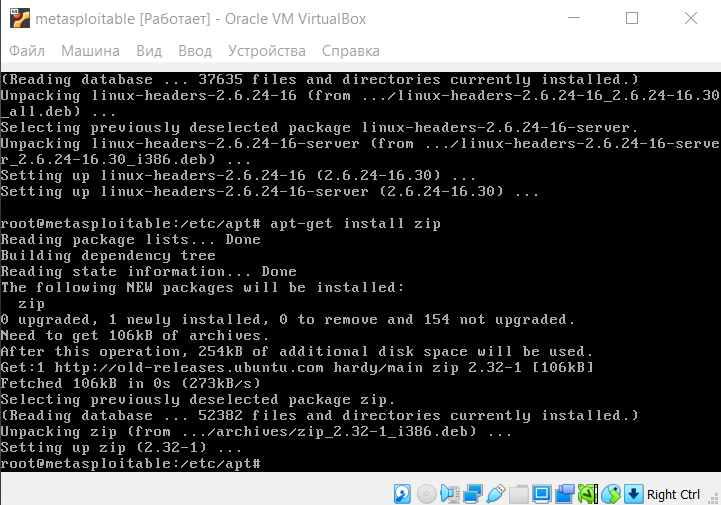
Обновить список репозиториев для менеджера пакетов apt и проверяем версию ядра



Установка заголовочных файлов ядра



Установка утилиты zip

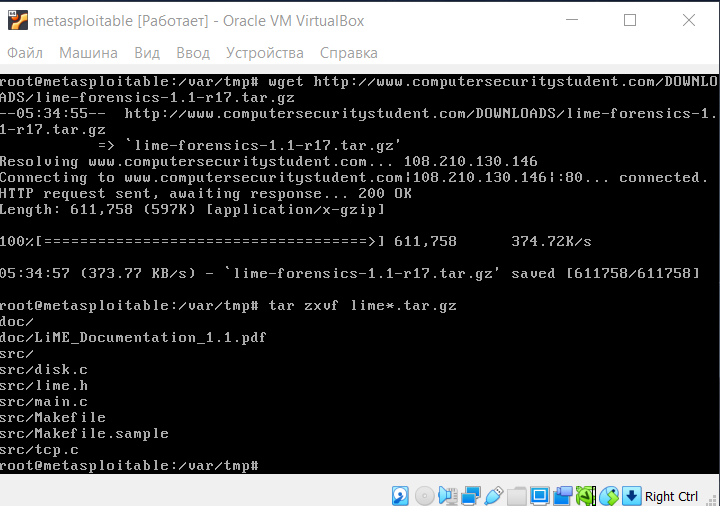


Итог: по обновлено

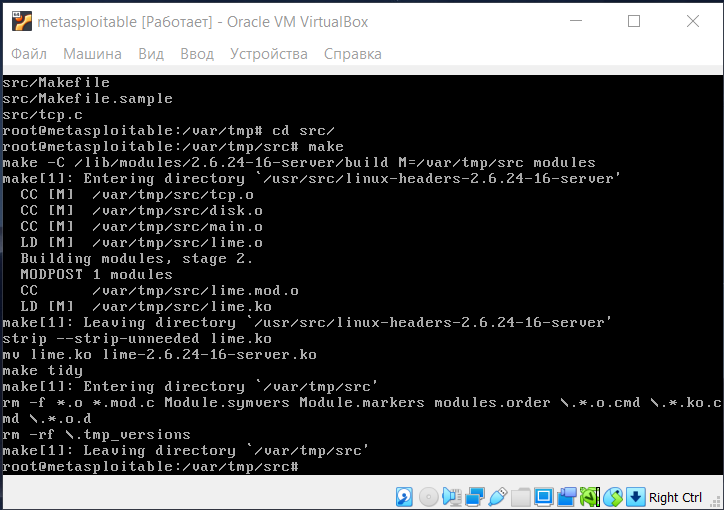
1. Установка LIME

Цель: установить LIME  
 Исходная ситуация: LIME не установлен

Скачивание архива с исходными текстами Lime и распаковка



Билд



Итог: LIME установлен

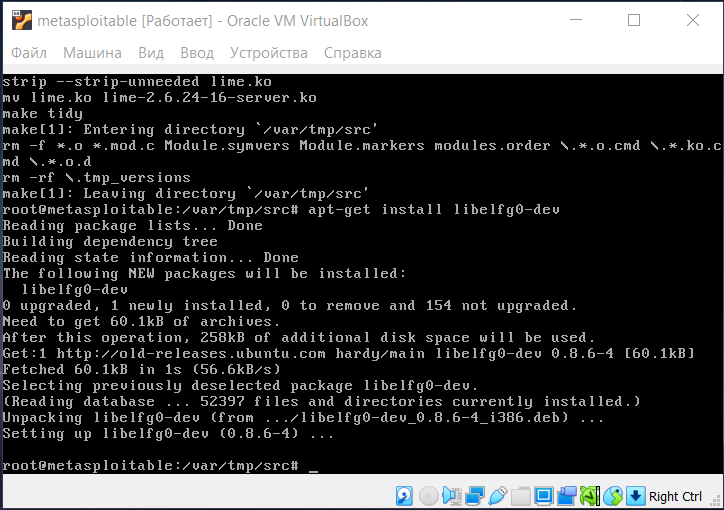
1. Установка вспомогательных библиотек

Цель: Установить вспомогательные библиотеки

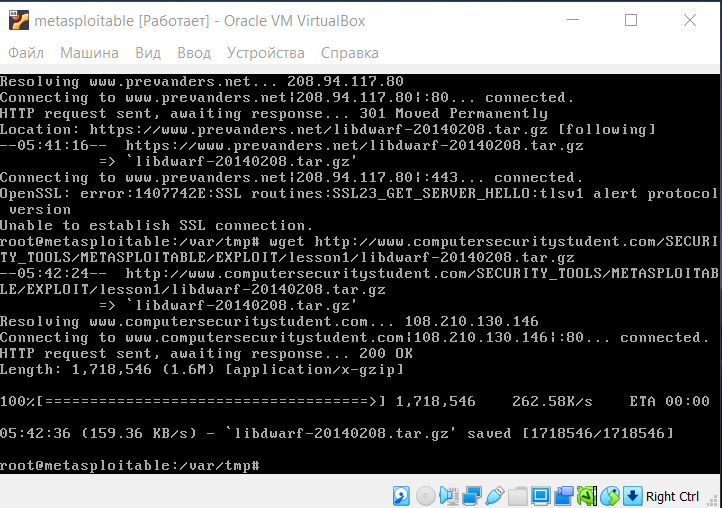
Исходная ситуация: библиотеки не установлены

Алгоритм:

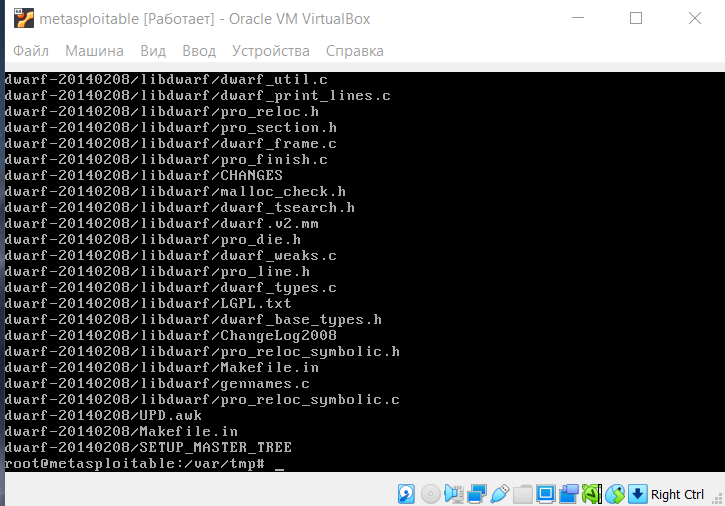
Установка заголовочных файлов библиотеки libelf



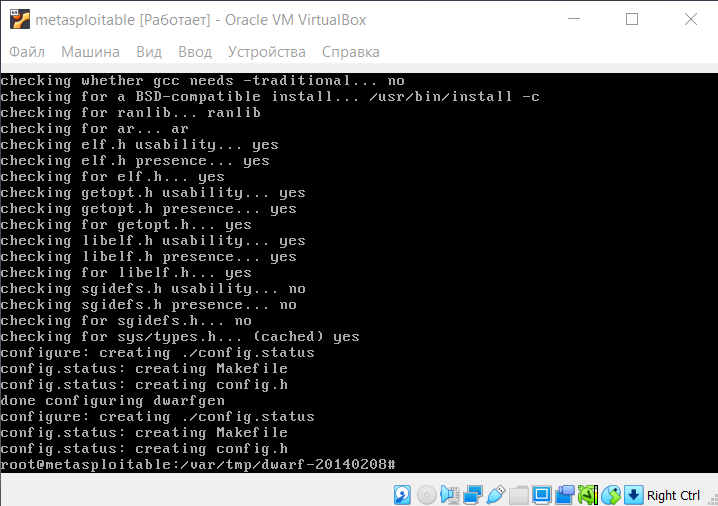
Скачивание, настройка и установка библиотеки libdwarf



Распаковка



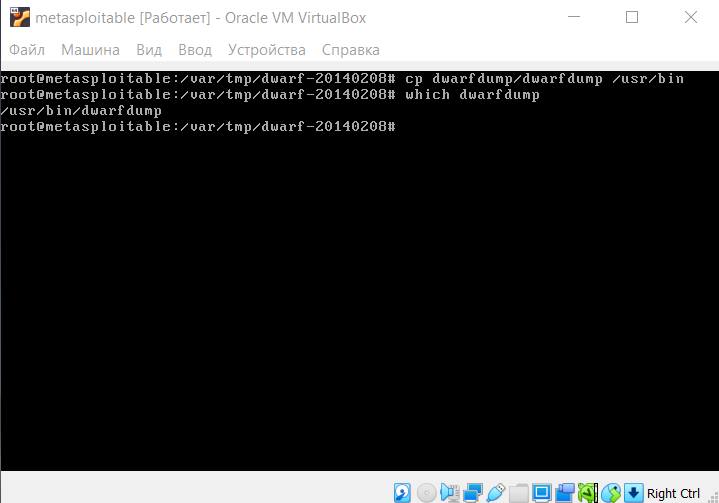
Подготовить пакеты к сборке



Билд (make)

Перемещаем утилиту

Проверяем что перенос успешен



Итог: все установлено

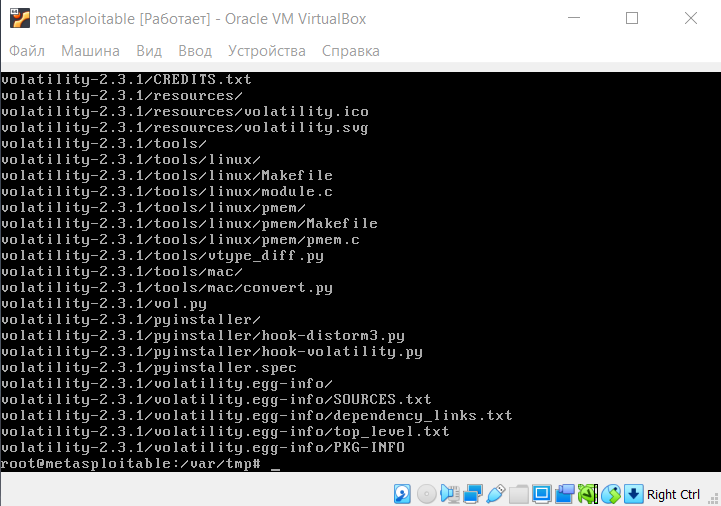
1. Скачивание, настройка и установка фреймворка Volatility

Цель: установить Volatility

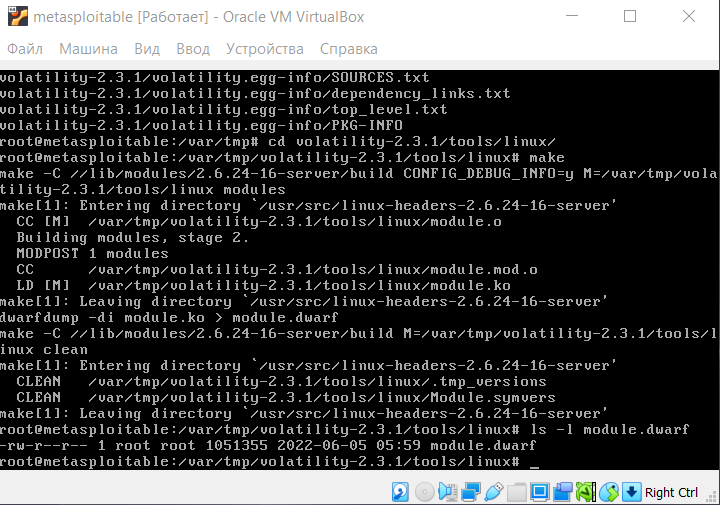
Исходная ситуация: фреймворк не установлен

Алгоритм:

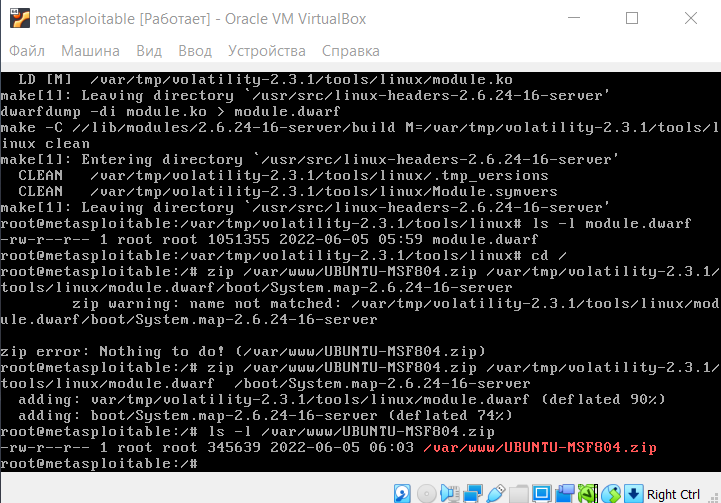
Установка и распаковка



Создание файла с отладочной информацией модуля ядра Metasploitable – module.dwarf



Создание профиля Volatility для Metasploitable



Итог: Volatility установлен

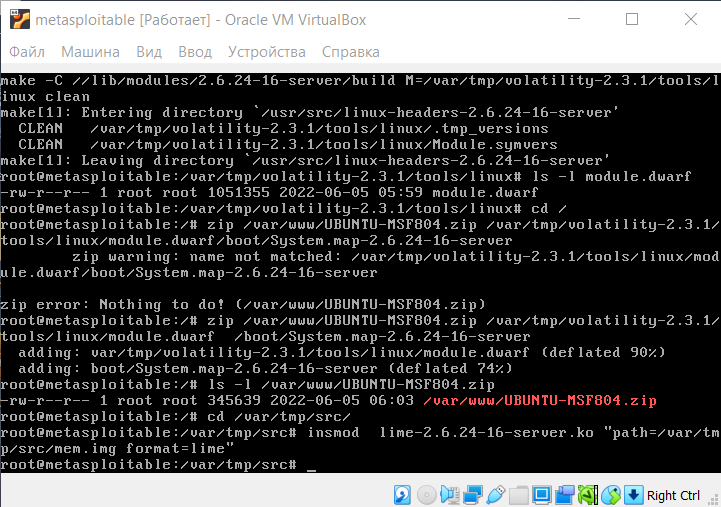
1. Форензика

Цель: создать дамп ОЗУ и проанализировать

Исходная ситуация: LIME & Volatility установлены

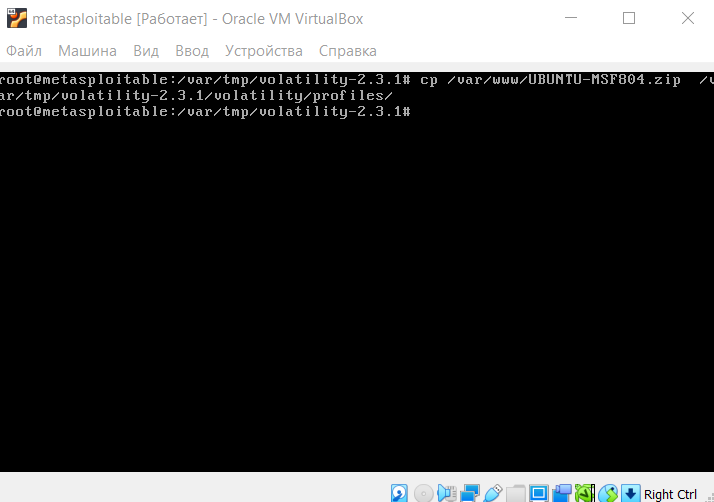
Алгоритм:

Создание дампа памяти с помощью LiME

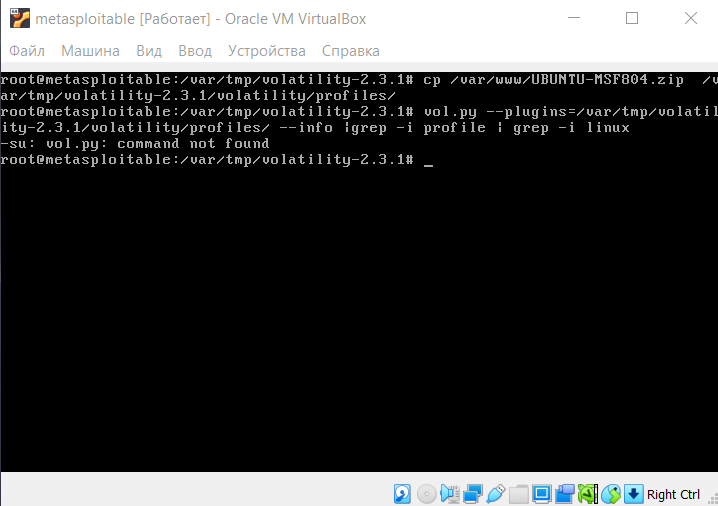


Просмотр активности в памяти в момент снятия дампа с помощью Volatility

переместить архив UBUNTU-MSF804.zip в подготовленный каталог

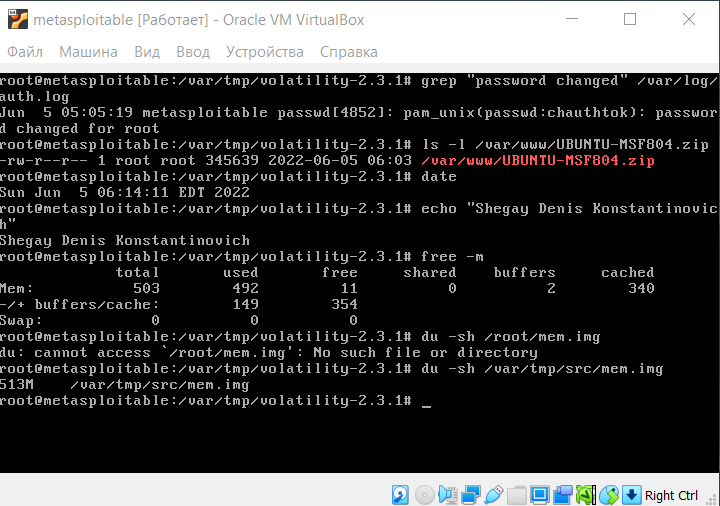


убедиться в том, что volatility успешно распознала новую директорию (питон не работает)



Итог: дамп вроде создан, проанализировать не вышло

Оформление результатов работы



(vol.py не работает)