**ЛАБОРАТОРНАЯ РАБОТА №1. LiME и Volatility. Форензика.**

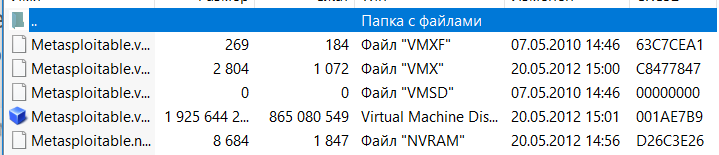
**Кондратьев Артем 11-901**

1. **Создание виртуальной машины Metasploitable**

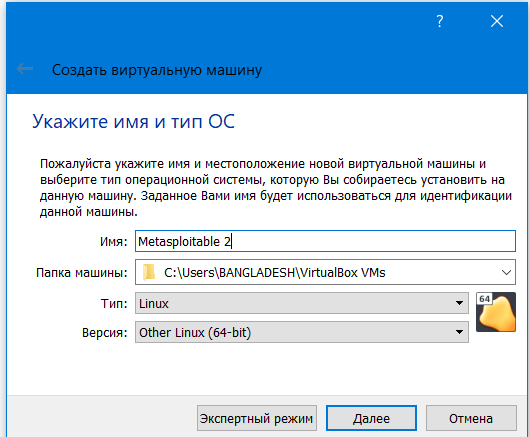
Для выполнения лабораторной работы была установлена операционная система Metasploitable 2 в качестве виртуальной машиной с использование программы VirtualBox.

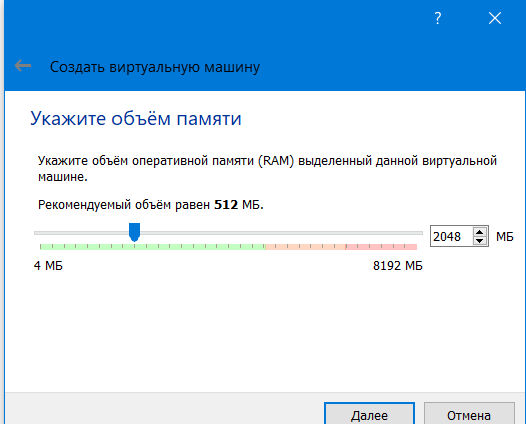
**1) Этапы создания виртуальной машины Metasploitable 2:**

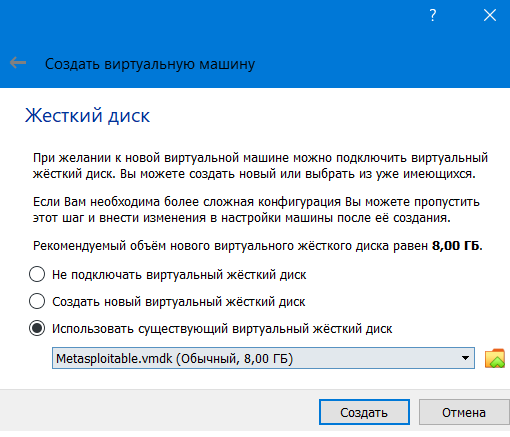
1. Зайти на сайт: <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>
2. Скачать metasploitable-linux-2.0.0.zip и разархировать файл Metasploitable.vmdk



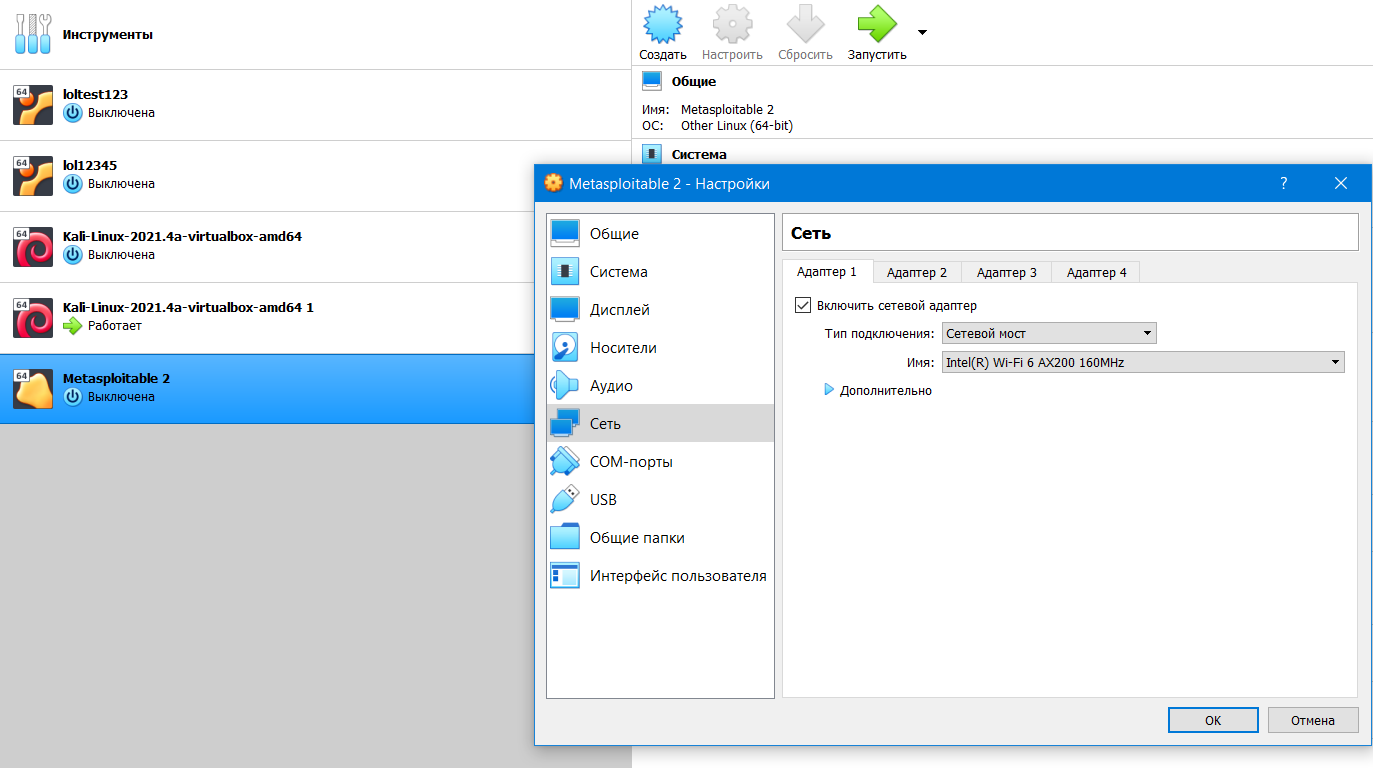
1. После загрузки зайти в VirtualBox и создать новую машину (Linux 64-bit):



1. Указать любой удобный объем оперативной памяти (например: 2048)
2. Указать Metasploitable.vmdk в качестве жесткого диска:

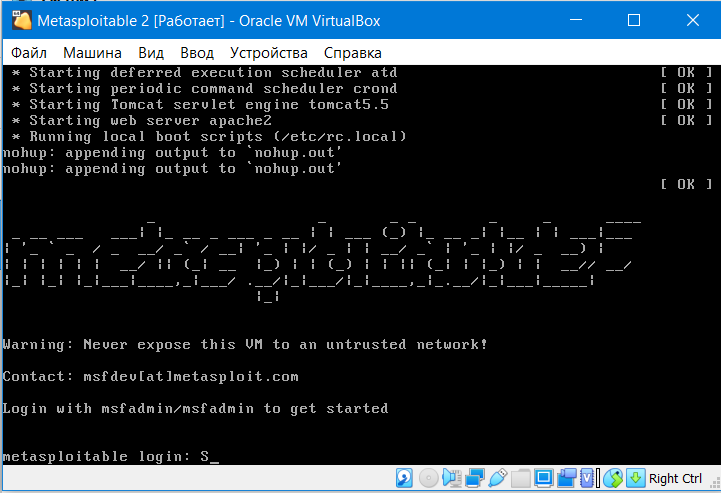


1. Поменять настройки сети на Сетевой мост и сохранить настройки

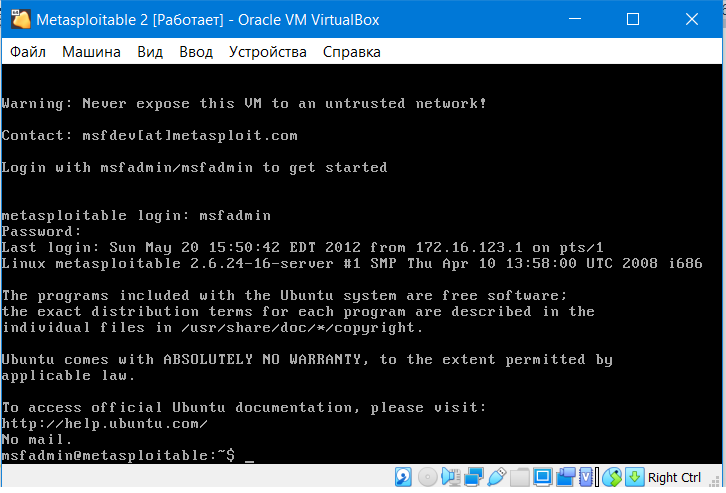


**2) Этапы первичной настройки Metasploitable 2:**

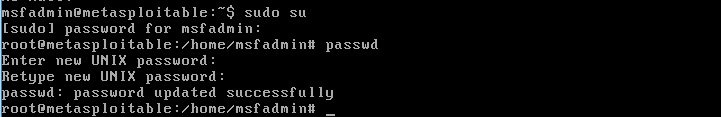
1. После настройк в VirtualBox нужно запустить Metasloitable 2 и подождать конца установки:



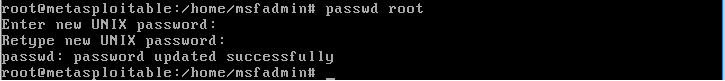
1. Необходимо ввести логин и пароль: *msfadmin/msfadmin*



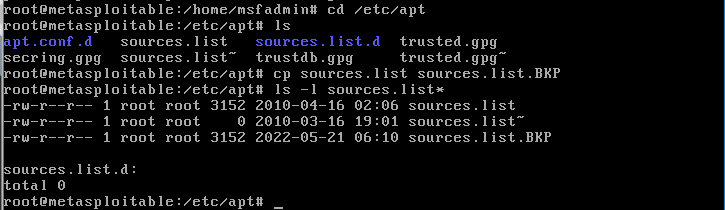
1. Далее дать права от root через команду: *sudo su*. И поменять пароль через команду: *passwd* и задать любой пароль:



1. Также можно поменять пароль root пользователя через команду: *passwd root* и задать любой пароль:



**3) Обновление источников пакетов и создание backup-файла репозиториев:**

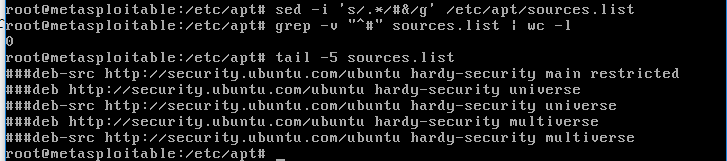
1. Обновление источников пакетов и создание backup-файла репозиториев

**4) Работа с репозиториями и установка заголовочных файлов ядра:**

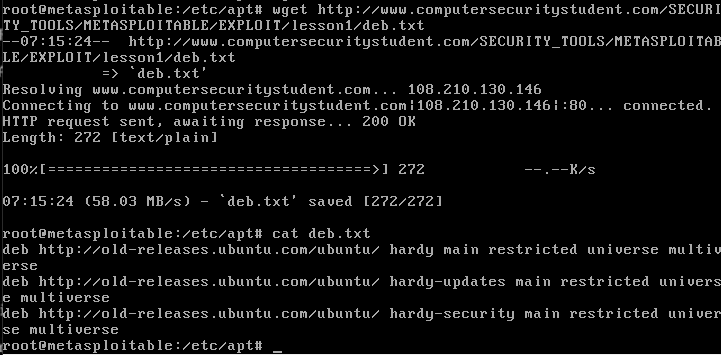
1. Просмотр списка репозиториев, используя команду:



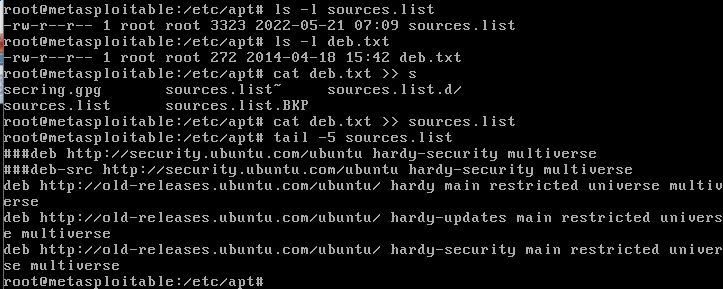
1. Отключение репозиториев, используя команду:



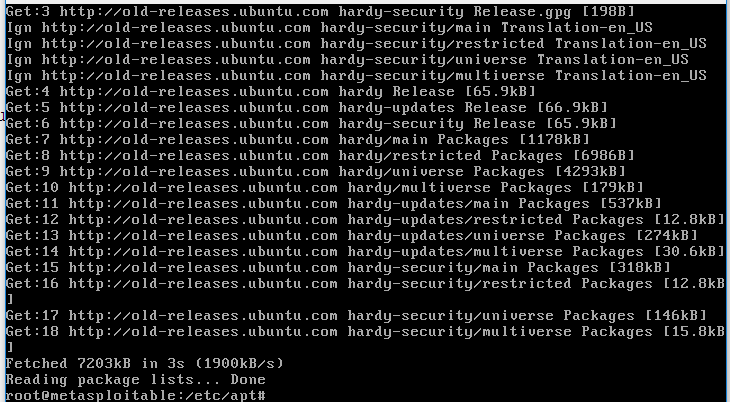
1. Добавление репозиториев из файла deb.txt в список репозиториев, используя команду:



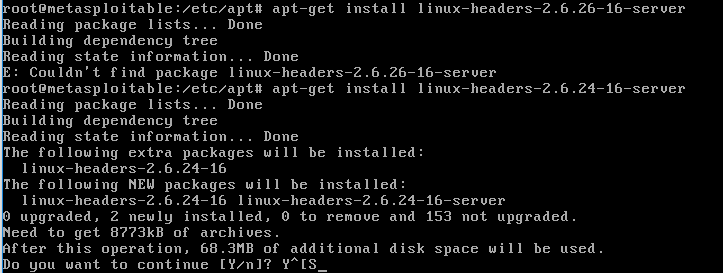
1. Выполнить команду: *cat deb.txt >> sources.list*. При этом файлы deb.txt и sources.list должны находиться в одной директории:



1. Обновить список репозиториев для менеджера пакетов apt, используя команду: *apt-get update*

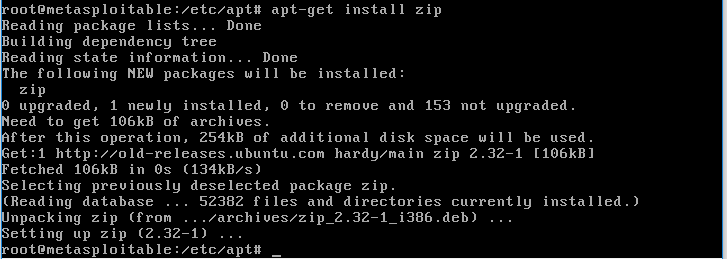


1. Установка заголовочных файлов ядра

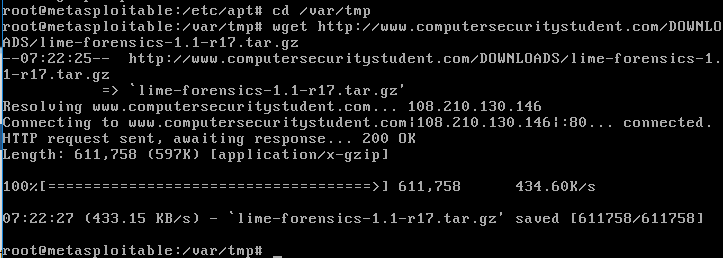


**5) Установка zip и Lime:**

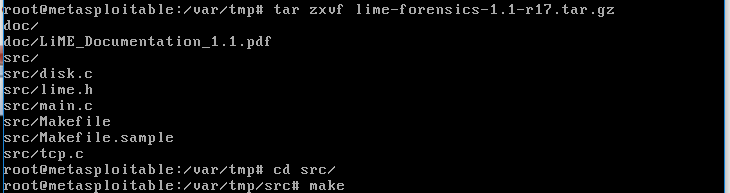
1. Выполнить команду: *apt-get install zip*



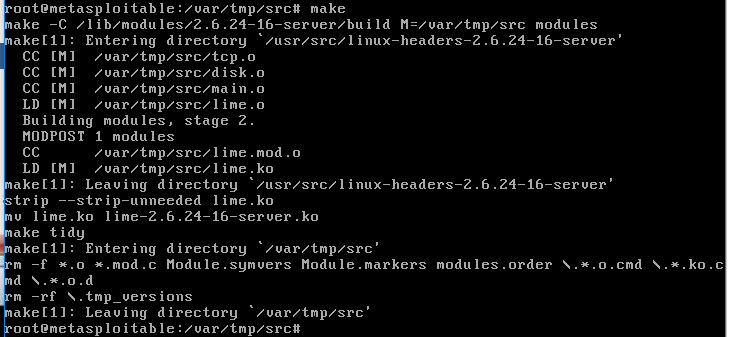
1. Выполнить команду: *cd /var/tmp* и выполнить команду: *wget http://www.computersecuritystudent.com/DOWNLOADS/lime-forensics-1.1-r17.tar.gz*



1. Распаковать архив, выполнив команду: *tar zxvf lime\*.tar.gz*

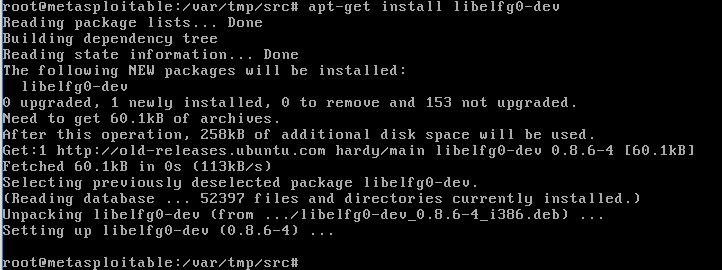


1. Выполнить сборку командой: *make*



**6) Установка вспомогательных библиотек**

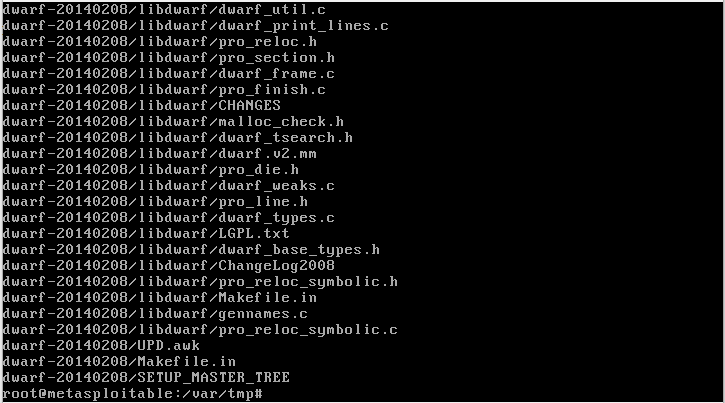
1. Установка заголовочных файлов библиотеки libelf. Выполнить команду: *apt-get install libelfg0-dev*



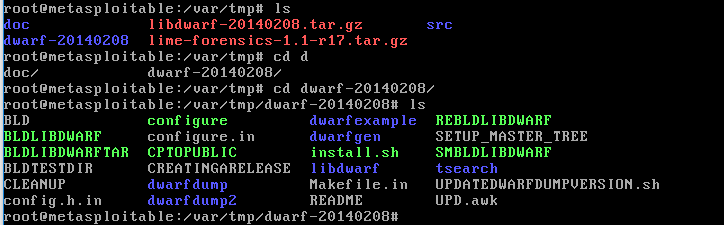
1. Скачивание, настройка и установка библиотеки libdwarf. Выполнить команду *cd /var/tmp* и выполнить команду: *wget http://www.computersecuritystudent.com/SECURITY\_TOOLS/METASPLOITABLE/EXPLOIT/lesson1/libdwarf-20140208.tar.gz*



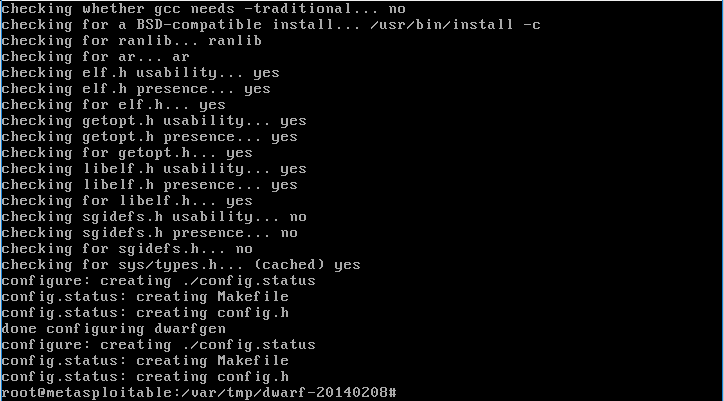
1. *Распаковать архив, выполнив команду: tar zxfy libdwarf-20140208.tar.gz*



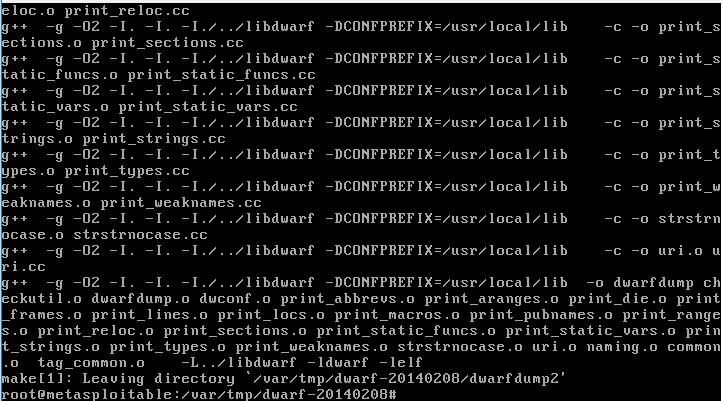
1. Перейти в каталог с исходными текстами, выполнив команду: *cd /var/tmp/dwarf-20140208*



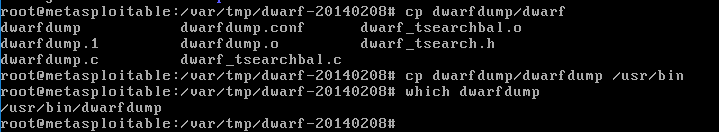
1. Подготовить исходные тексты к сборке, запустив исполняемый файл: *./configure*



1. Выполнить сборку командой: *make*



1. Переместить утилиту dwarfdump в каталог исполняемых файлов командой: *cp dwarfdump/dwarfdump /usr/bin* и с помощью команды: *which dwarfdump* удостовериться в правильности переноса утилиты dwarfdump.

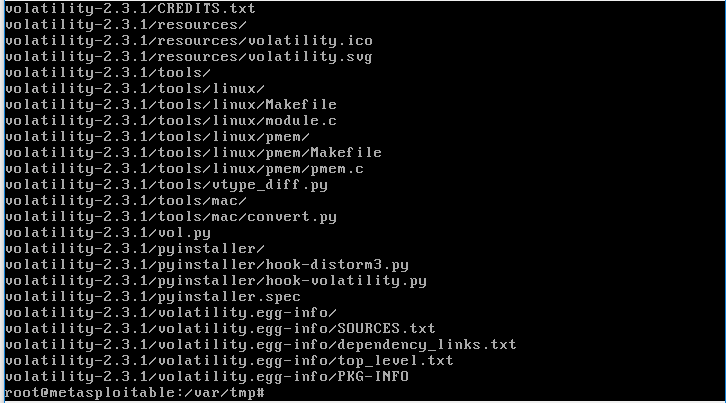


**7) Скачивание, настройка и установка фреймворка Volatility**

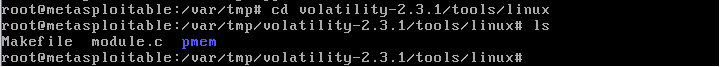
1. Скачивание Volatility. Необходимо перейти в раздел: *cd /var/tmp/* и использовать команду: *wget --no-check-certificate http://www.computersecuritystudent.com/SECURITY\_TOOLS/METASPLOITABLE/EXPLOIT/lesson1/volatility-2.3.1.tar.gz*



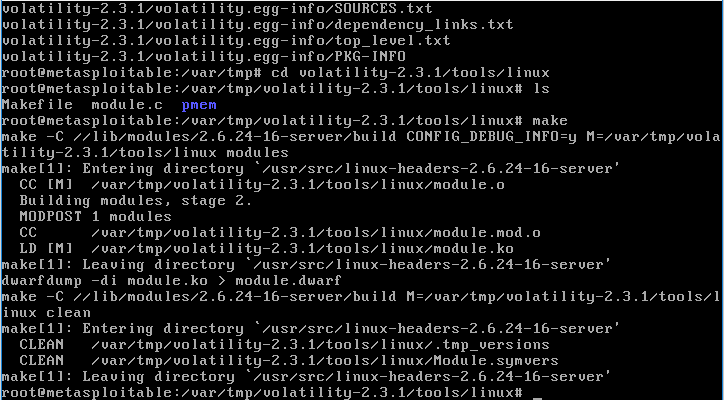
1. Распаковать архив, выполнив команду: *tar zxvf volatility-2.3.1.tar.gz*



1. Перейти в каталог с linux-утилитами фреймворка, выполнив команду *cd /var/tmp/volatility-2.3.1/tools/linux*



1. Выполнить сборку командой: *make*

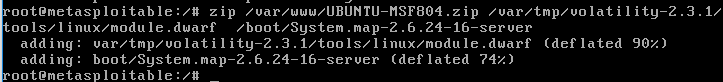


1. С помощью команды: *ls -l module.dwarf* проверить успешность получения структуры ядра Metasploitable.

image10.png

**8) Создание профиля Volatility для Metasploitable**

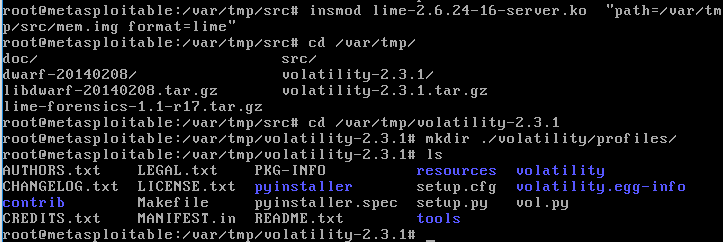
1. Подготовить архив с файлами профиля ядра Metasploitable с помощью команды: *zip /var/www/UBUNTU-MSF804.zip /var/tmp/volatility-2.3.1/tools/linux/module.dwarf /boot/System.map-2.6.24-16-server*



1. Убедиться в успешности создания архива, выполнив команду: *ls -l /var/www/UBUNTU-MSF804.zip*

image22.png

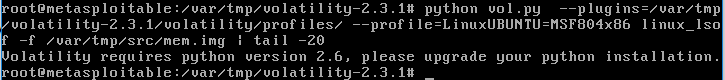
1. Создание дампа памяти с помощью LiME перейти в раздел: *cd /var/tmp/src/* и выполнить команду: *insmod lime-2.6.24-16-server.ko "path=/var/tmp/src/mem.img format=lime*"
2. После этого перейти в каталог с фреймворком с помощью команды: *cd /var/tmp/volatility-2.3.1*и создать отдельный каталог для архива UBUNTU-MSF804.zip c помощью команды *mkdir ./volatility/profiles/*



1. Переместить архив UBUNTU-MSF804.zip в подготовленный каталог с помощью команды: *cp /var/www/UBUNTU-MSF804.zip /var/tmp/volatility-2.3.1./volatility/profiles/*

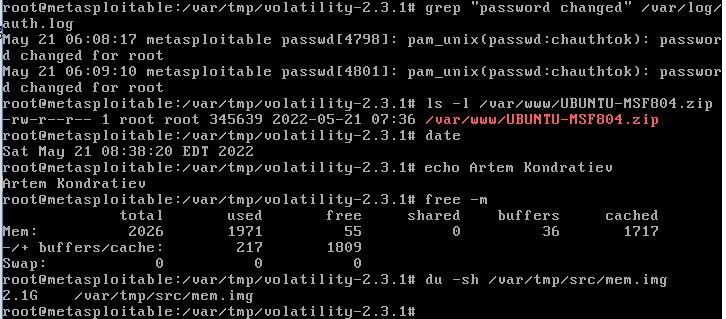
**9) Оформление результатов работы:**

1. Команда: *python vol.py --plugins=/var/tmp/volatility-2.3.1./volatility/profiles/ --profile=LinuxUBUNTU-MSF804x86 linux\_lsof -f /var/tmp/src/mem.img | tail -20* НЕ РАБОТАЕТ из-за версии python

****

***Не получилось обновить версию python до 2.6, некорректно оформлено задание***

1. Список команд:

* *grep "password changed" /var/log/auth.log*
* *ls -l /var/www/UBUNTU-MSF804.zip*
* *date*
* *echo "Ф.И.О"*
* *free –m;*
* *du –sh /var/tmp/src/mem.img*