**ФИО:** Степанищева Анастасия Андреевна

**Группа:** 11–902

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

**Содержание:**

1. подготовка виртуальной машины

2. обновление источников пакетов (работа с репозиториями)

3. установка Zip утилиты и заголовочных файлов ядра

4. Скачивание и установка Lime

5. Установка дополнительных библиотек (libelf, libdwarf)

6. Скачивание, установка и настройка фреймворка Volatility

7. Форензика

8. Результат работы

**Отчет:**

1. **подготовка виртуальной машины**

Создание виртуальной машины с указанными параметрами, с использованием файла виртуального жесткого диска Metasploitable.vmdk; смена паролей.

Виртуальная машины подготовлена для выполнения лабораторной работы

2. **обновление источников пакетов (работа с репозиториями)**

Создание back-up -файла репозиториев (cp sources.list sources.list.BKP)

Просмотр списка репозиториев + отключение их

Добавление репозиториев из файла deb.txt в список репозиториев. **Проблема:** указанного файла нет. Решение: использовать файл sources.list. Открываем в консольном текстовом редакторе и меняем префиксы на old-archives.

Обновление списка репозиториев для менеджера пакетов (apt-get update)

3. **установка Zip утилиты и заголовочных файлов ядра**

Установка заголовочный файлов ядра (uname -r; apt-get install linux-headers-$(uname -r);)

Установка Zip утилиты (apt-get install zip)

4. **Скачивание и установка Lime**

Скачивание архива с исходниками Lime. Примечание: команда (wget http://lime-forensics.googlecode.com/files/) не работает, т.к. ссылка нерабочая. Можно заменить на актуальную ссылку с архивом или воспользоваться скачанным архивом из каталога /csc/tools. Выбрала первый вариант.

Распаковка архива (unzip -x lime.zip)

Сборка в каталоге исходных текстов (make)

5. **Установка дополнительных библиотек (libelf, libdwarf)**

Установка заголовочных файлов библиотеки libelf (apt-get install libelfg0-dev)

Скачивание библиотеки libdwarf. Примечание: ссылка в инструкции к лабораторной работе нерабочая. Решение: найти актуальную ссылку на архив и скачать его.

Распаковка (unzip -x libdwarf.zip)

Подготовка исходных текстов к сборке (./configure)

Сборка (make)

Перенос утилиты в каталог исполняемых файлов (cp dwarfdump/dwarfdump /usr/bin)

6. **Скачивание, установка и настройка фреймворка Volatility**

Скачивание исходных текстов фреймворка. Примечание: нерабочая ссылка. Используем данные из каталога /csc/tools

Распаковка (tar zxvf volatility-2.3.1.tar.gz)

Создание файла с отладочной информацией. Выполнить сборку (make) из директории с linux-утилитами фреймворка (cd /var/tmp/volatility-2.3.1/tools/linux)

Подготовка архива с файлами профиля ядра Metasploitable c помощью zip команды (/var/www/UBUNTU-MSF804.zip /var/tmp/volatility-2.3.1/tools/linux/module.dwarf /boot/System.map-2.6.24-16-server). Результат: создан архив (проверка: ls -l /var/www/UBUNTU-MSF804.zip)

7. **Форензика**

Создание дампа оперативной памяти Metasploitable из каталога с собранным для ядра модулем Lime. (insmode lime-2.6.24-16-server.ko “ path=/var/tmp/src/mem.img format=lime”)

Создание отдельного каталога и перемещение туда архива

Примечание: для использования следующих команд необходимо установить pycripto, а для него python.

Проверка, что volatility распознает новую директорию с профилями (python ./vol.py --plugins=/var/tmp/volatility-2.3.1/volatility/profiles/ --info | grep -i profile | grep -i linux). **Результат**: LinuxUBUNTU-MSF804x86

Анализ дампа памяти (mem.img). Запускаем плагин linux\_lsof из состава volatility (--plugins=/var/tmp/volatility-2.3.1./volatility/profiles/ --profile=LinuxUBUNTU-MSF804x86 linux\_lsof -f /var/tmp/src/mem.img | tail -20 ) Примечание: ( --profile=LinuxUBUNTU-MSF804x86 ) значение полученное при проверке на предыдущем шаге.

8. **Результат работы**

**Вывод результата выполнения команд**

1) grep "password changed" /var/log/auth.log;

2) ls -l /var/www/UBUNTU-MSF804.zip;

3) date;

4) echo "Ф.И.О. проделавшего работу";

5) free –m;

6) du –sh /root/mem.img;

7) команды:

vol.py --plugins=/var/tmp/volatility-2.3.1./volatility/profiles/ --profile=LinuxUBUNTU-MSF804x86 linux\_lsof -f /var/tmp/src/mem.img | tail -20

