Тыщенко Леонид Михайлович, 11-902

Лабораторная работа №1. LIME и Volatility.

1. Создание виртуальной машины.

Цель: создание виртуальной машины на основе образа Metasploitable для дальнейшей работы.

Алгоритм выполнения: установка необходимых приложений(VMWire Player), образа виртуальной машины (*Metasploitable.vmdk*), и конфигурация настроек.

1. Сменить пароль для стандартного пользователя

Цель: смена пароля у пользователя на любой другой

Алгоритм выполнения: войти в систему под стандартным логином и паролем, выполнить команду passwd, которая сменит пароль

1. Сменить источники пакетов

Цель: подменить источники пакетов, чтобы загружать из необходимых для нас репозиториев

Алгоритм выполнения: создать бекап и закомментировать содержимое файла sources.list, скачать файл deb.txt, содержащий необходимые для нас ссылки на репозитории, и вставить содержимое скачанного файла в sources.list, после чего необходимо скомпилировать ядро linux с изменениями.

1. Создание дампа памяти с помощью LIME.

Цель: просмотр памяти (запущенных приложений, процессов) в момент снятия дампа памяти для дальнейшего анализа, получение ссылок на необходимые участки памяти.

Алгоритм выполнения: установить LIME, volatility, снять дамп памяти с помощью LIME и просмотреть дамп памяти с помощью volatility.

1. Результаты выполненной работы:

