Министерство науки и высшего образования Российской Федерации Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ДОПОЛНИТЕЛЬНЫЕ МЕТОДЫ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ НА ОБЪЕКТЕ ЗАЩИТЫ ИНФОРМАЦИИ**

отчет о   
лабораторной работе №5

по дисциплине

*ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ*

***ВАРИАНТ 13***

|  |  |  |
| --- | --- | --- |
| Выполнила: | ст. гр. 230711 | Павлова В.С. |
| Проверил: | асс. каф. ИБ | Греков М.М. |

Тула, 2023 г.

# **ЦЕЛЬ РАБОТЫ**

**Цель:** ознакомиться с дополнительными средствами эксплуатации уязвимостей, используемых для упрощения автоматизации контроля степени защищённости объекта защиты информации.

# **ЗАДАНИЕ НА РАБОТУ**

1. Настройте сеть и запустите обе ОС.
2. В системе Windows отключите защитника и фаервол, а также включите сетевое обнаружение.
3. В системе Linux запустить сервер базы данных командой sudo service postgresql start.
4. В системе Linux запустить Armitage командой sudo Armitage.
5. В системе Linux подключите базу данных Metasploit. Если она была использована в предыдущей работе, то БД инициализируется автоматически, если нет, но настройте подключение к ней и повторите процедуру.
6. Используя msfvenom скомпилируйте файл с полезной нагрузкой meterpreter с расширением .exe , указав lhost (IP адрес машины Linux). Рекомендуется использовать модуль Metasploit под названием reverce tcp, запущенных при помощи Armitage.
7. С помощью python3 -m http.server разместите вредоносный файл на web-интерфейсе Kali Linux (запускается из каталога с файлом).
8. Скачайте файл и запустите его с правами администратора на Windows.
9. Скопируйте хеши паролей пользователей ОС Windows.
10. Отправить полученных хеши паролей на расшифровку в ПО JhonTheRipper и получить пароль администратора.

**ХОД РАБОТЫ**

1. Создание полезной нагрузки payload.exe в Kali через GUI Armitage (рисунок 1):

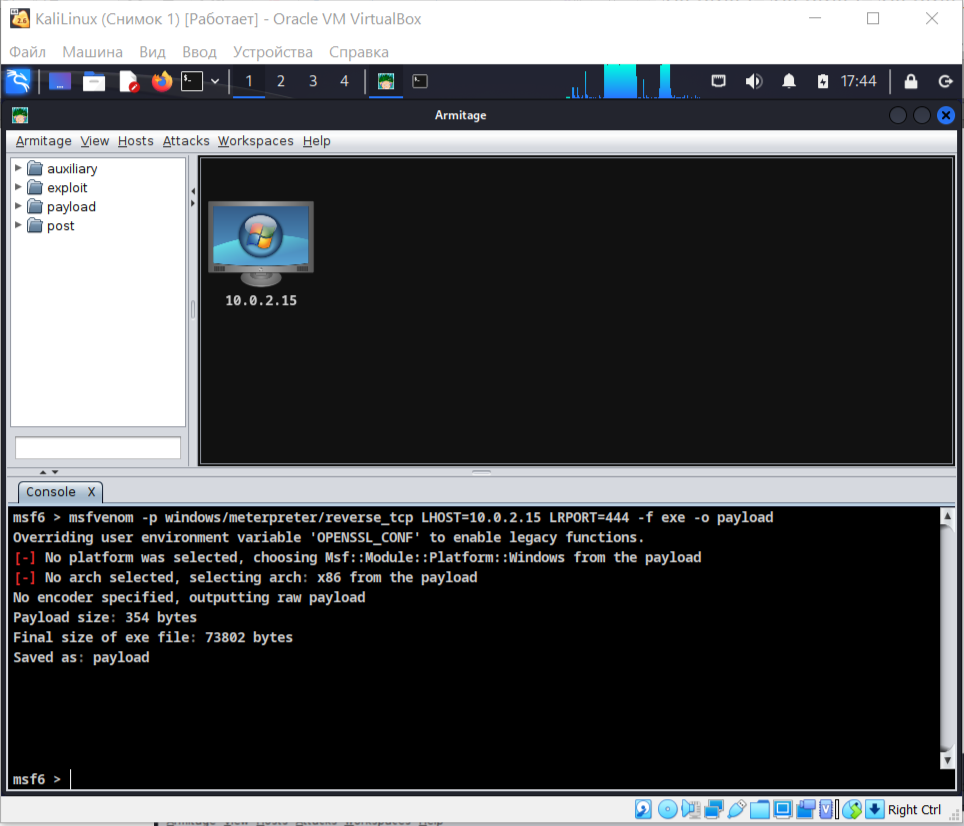
****

Рисунок 1 – Создание нагрузки через Armitage

1. Размещение вредоносного файла на целевой ОС (рисунок 2)

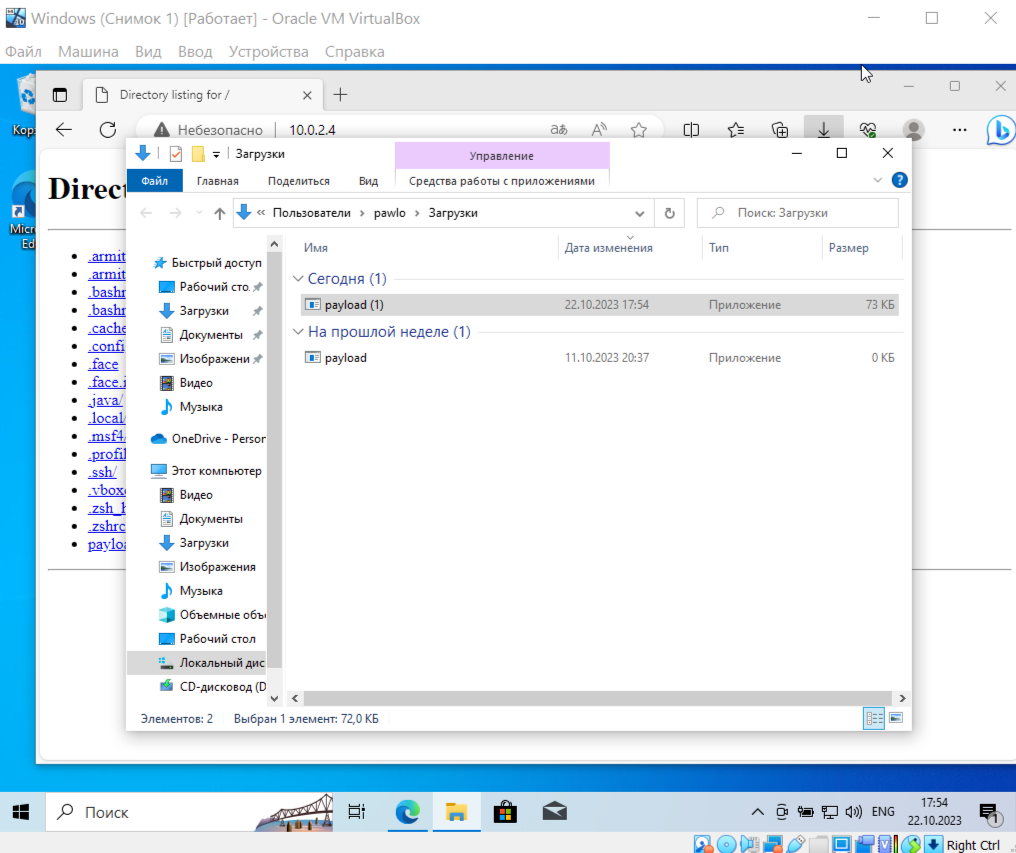


Рисунок 2 – Скачивание payload.exe

1. Подключение к целевой ОС (рисунок 3)

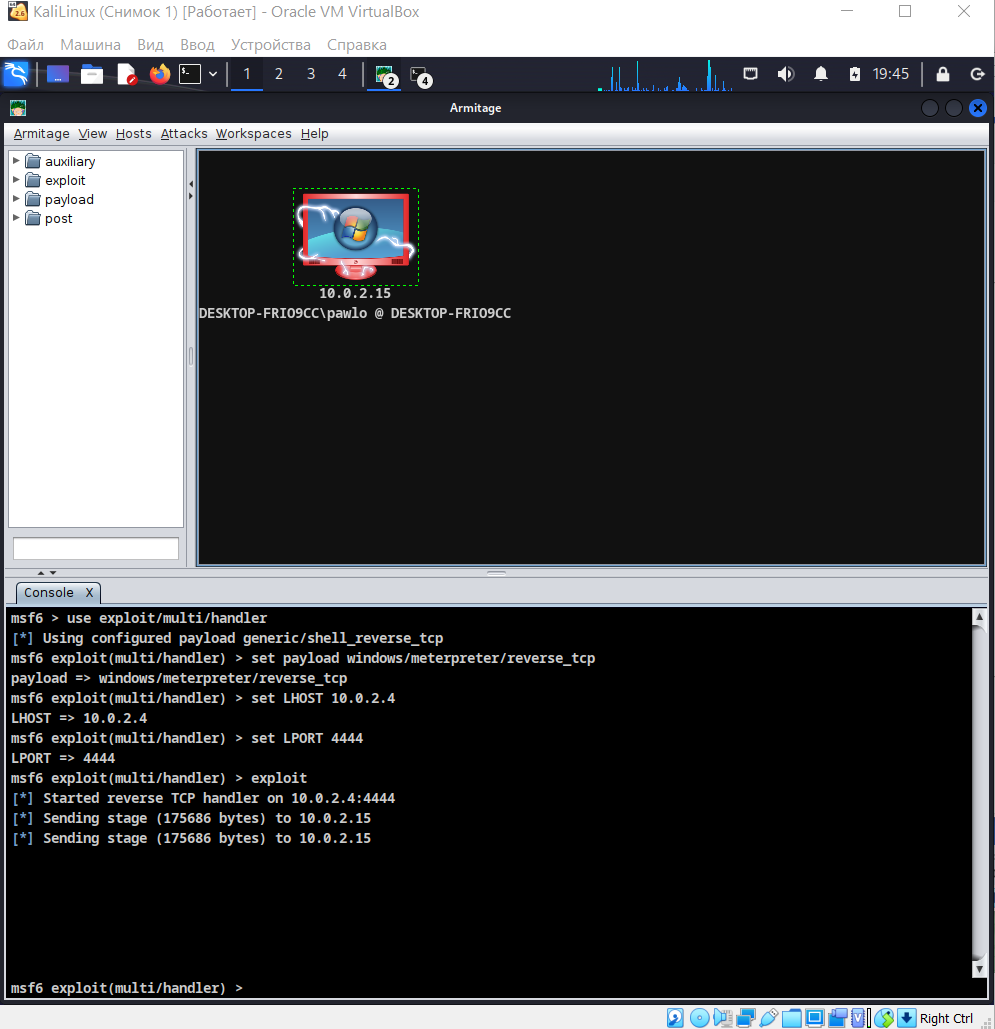


Рисунок 3 – Подключение к целевой ОС

1. Получение NTLM-хэшей (рисунок 4):

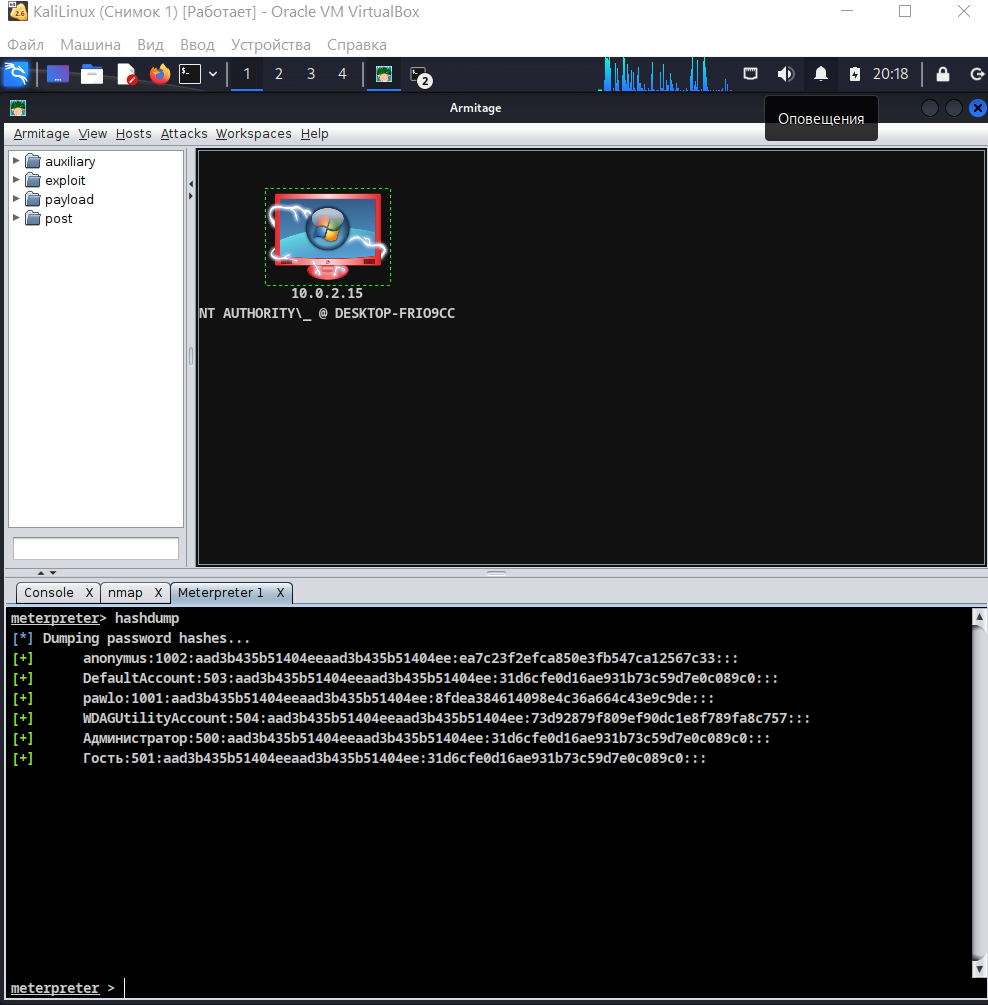


Рисунок 4 – Результат выполнения hashdump

1. Получение пароля администратора (с помощью JohnTheRipper):

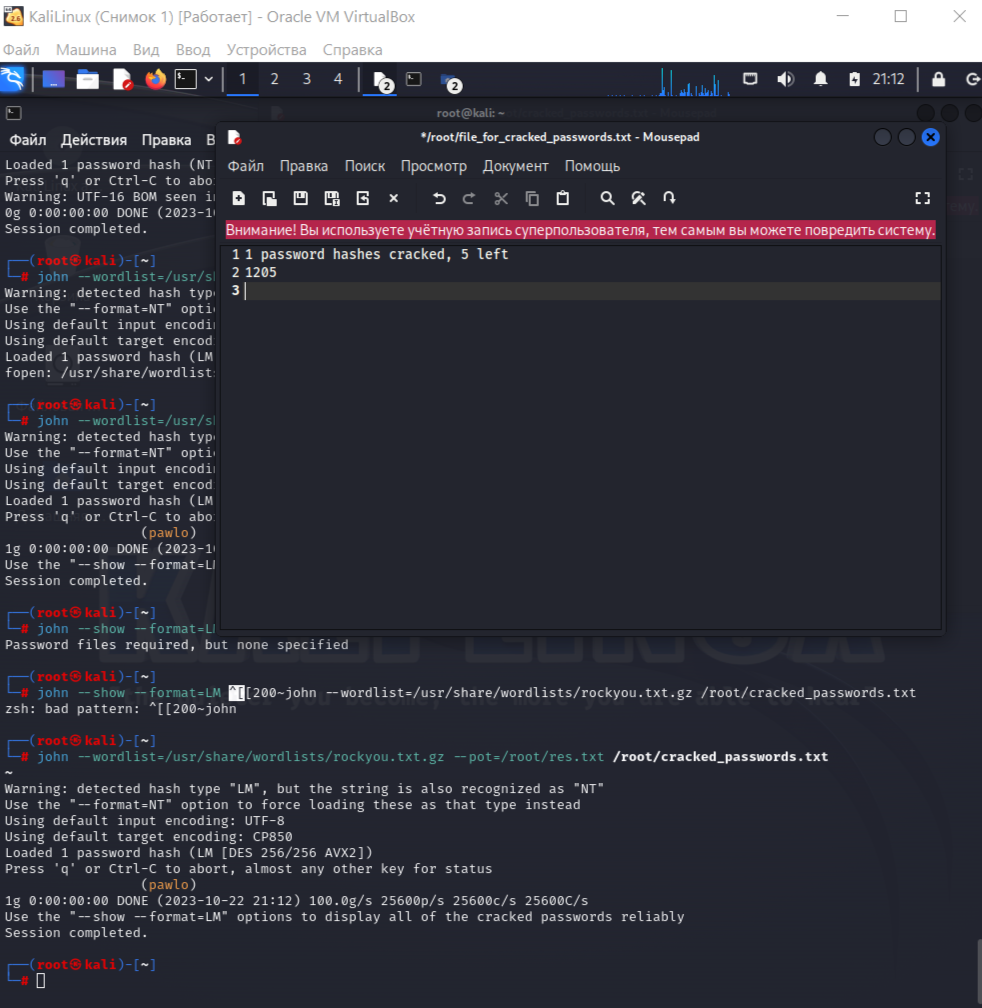


Рисунок 5 – Получение пароля администратора

# **ВЫВОД**

В ходе выполнения данной лабораторной работы я ознакомилась с дополнительными методами эксплуатации уязвимостей на объекте защиты информации.