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

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

отчет о   
лабораторной работе №4

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 основными средствами эксплуатации уязвимостей, используемых для контроля степени защищённости объекта защиты информации.

# **ЗАДАНИЕ НА РАБОТУ**

1. Скачайте виртуальную машину Linux и операционную систему Windows
2. Настройте сеть и запустите обе ОС.
3. В системе Windows отключите защитника и фаервол, а также включите сетевое обнаружение.
4. В системе Linux инициализируйте базу данных Metasploit.
5. 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.
6. С помощью python3 -m http.server разместите вредоносный файл на web-интерфейсе Kali Linux (запускается из каталога с файлом).
7. Скачайте файл и запустите его с правами администратора на Windows.
8. Установите сессию и создайте пользователя.
9. Получите скриншот подтверждения наличия пользователя и скриншот логов.
10. Удалить логи из журнала событий Windows, Windows Event Log.
11. Проверить подключение к ОС Windows при помощи созданного пользователя.

**ХОД РАБОТЫ**

1. Создание полезной нагрузки payload.exe в Kali



Рисунок 1 – Создание нагрузки через root-консоль

1. Подготовка атакуемой ОС: отключение защитника и брандмауэра

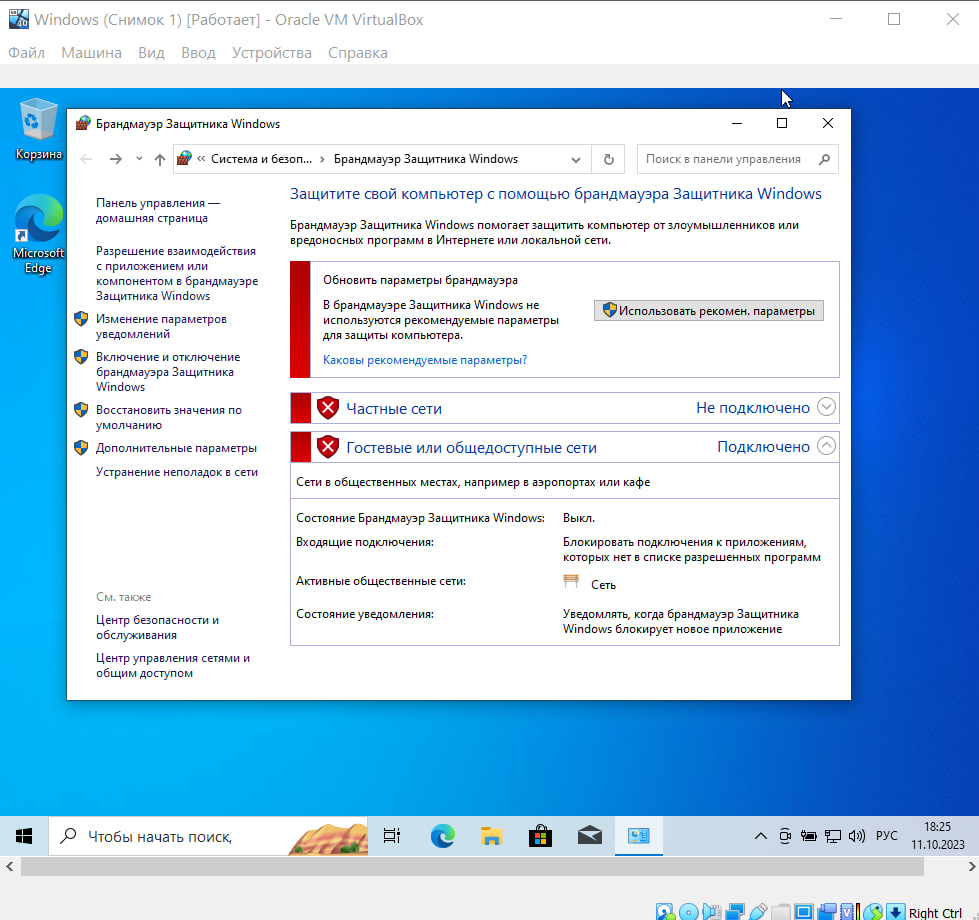


Рисунок 2 – Подготовка целевой ОС

1. Скачивание вредоносного файла на целевую ОС через сетевой мост:

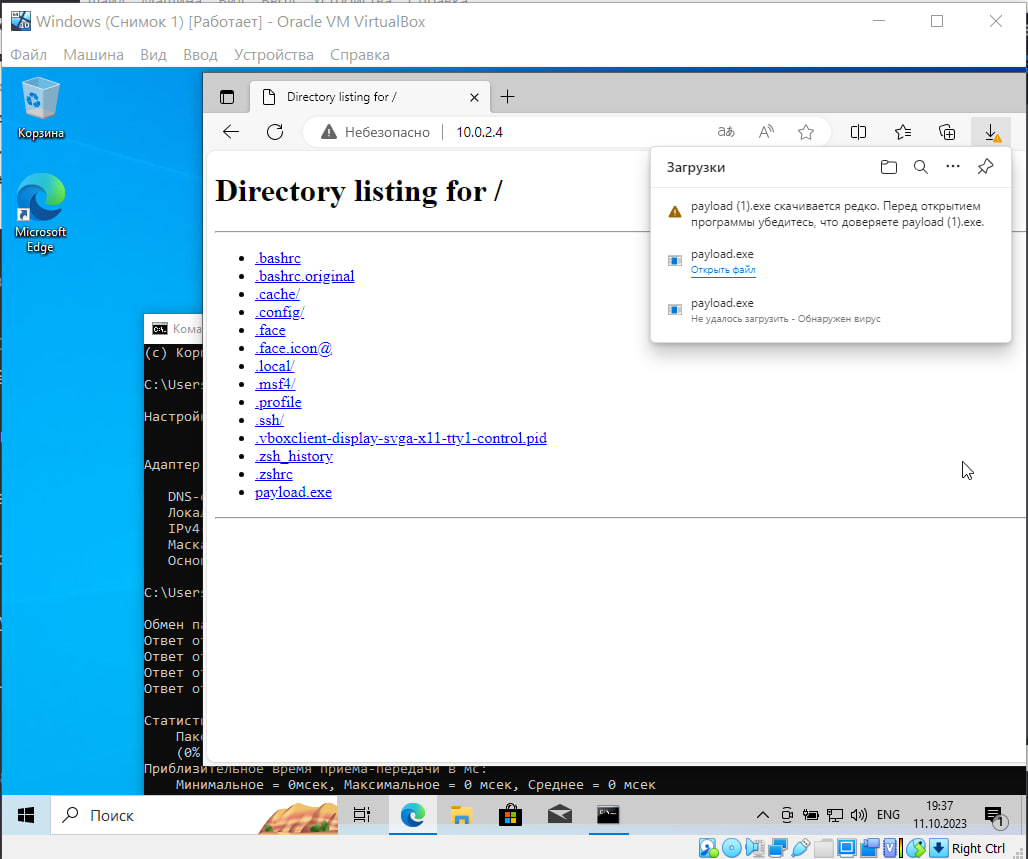


Рисунок 3 – Скачивание payload.exe

1. После запуска команд в Kali создаём нового пользователя в Windows и добавляем его в группу администраторов:

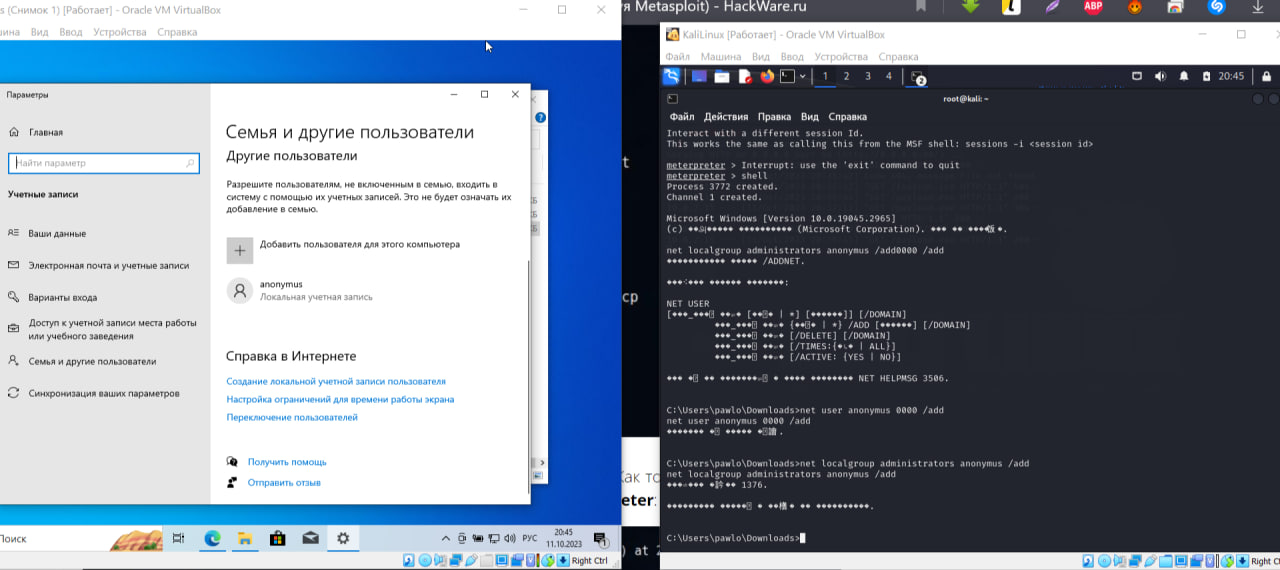


Рисунок 4 – Создание пользователя в Windows

1. Пользователь создан, теперь можно осуществить вход:

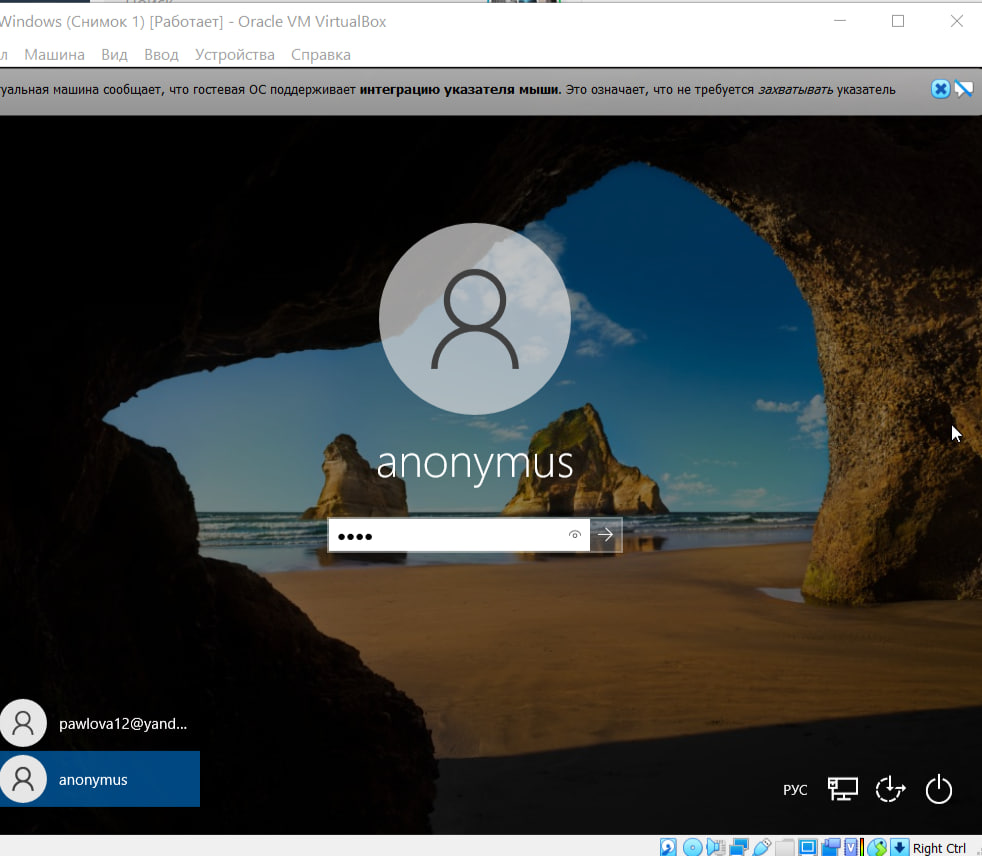


Рисунок 5 – Вход в систему с помощью созданного пользователя

# **ВЫВОД**

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