Сабирзянова А.М.

11-901

**ИСПОЛЬЗОВАНИЕ УЯЗВИМОСТИ ПРОТОКОЛА SAMBA: CVE - 2007 - 2447. СЕТЕВАЯ ФОРЕНЗИКА**

Содержание:

[**1. Настройка сети между Metasploitable и Kali Linux**](#_mgp1vn336u97) **1**

[**2. Атака Metasploitable**](#_9k3b2j8fsodb) **1**

[**3. Форензика**](#_wcwh4bdc6sdc) **3**

[**4. Оформление результатов работы**](#_bu6s7szbj78l) **4**

## 1. Настройка сети между Metasploitable и Kali Linux

Цель: объединить машины в одну сеть

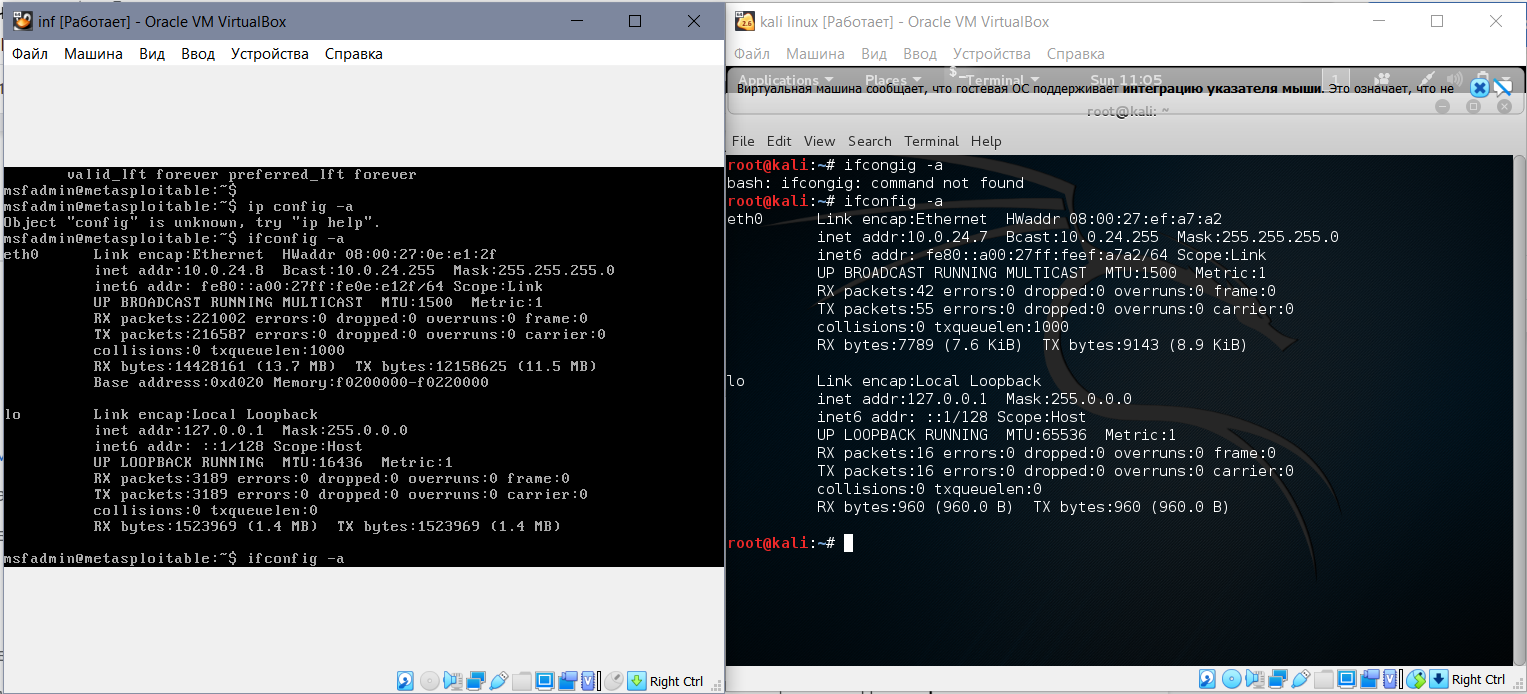
Начальная ситуация: между машинами связи нет

Алгоритм:

1. На обоих машинах выбираем тип адаптера - сетевой мост
2. На обоих машинах вводим **ifconfig -a**

KL\_IP = 10.0.24.7

MS\_IP = 10.0.24.8

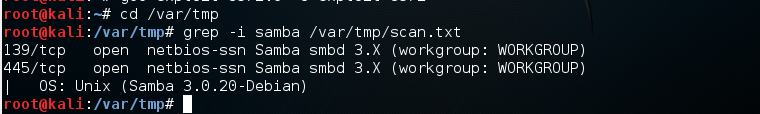


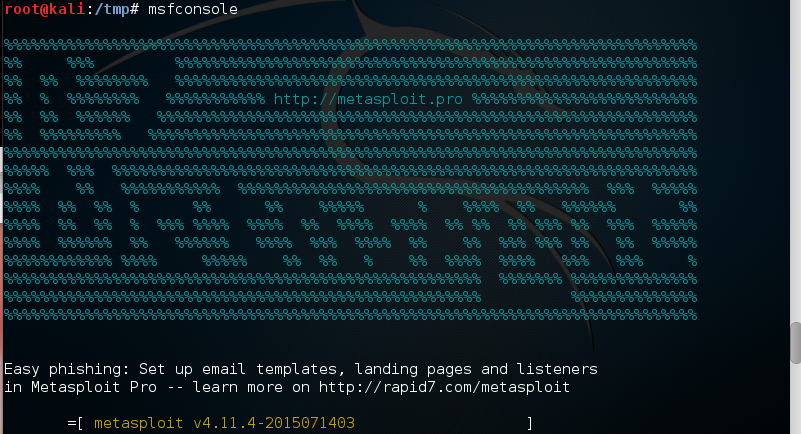
Результаты: полученные ip

## 2. Атака Metasploitable

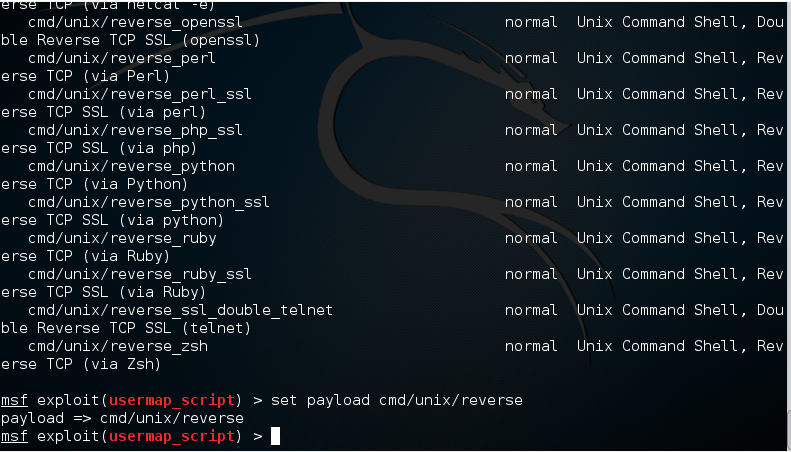
Цель: получить доступ к консоли на Metasploitable

Алгоритм:

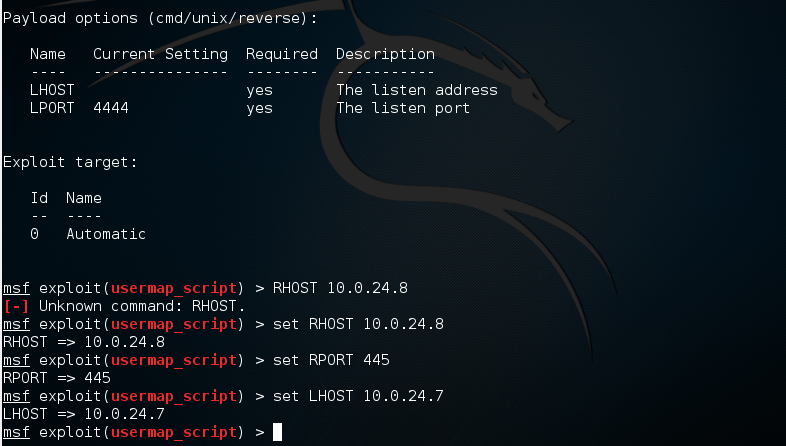
1. Сканируем порты машины Metasploitable с помощью команды **nmap**.
2. Находим samba
3. Запускаем консоль msfconsole



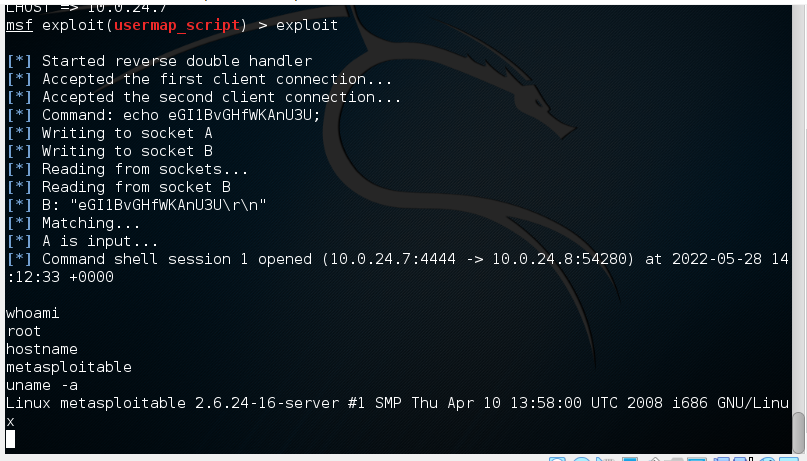
1. Устанавливаем payload



1. Устанавливаем значение параметров



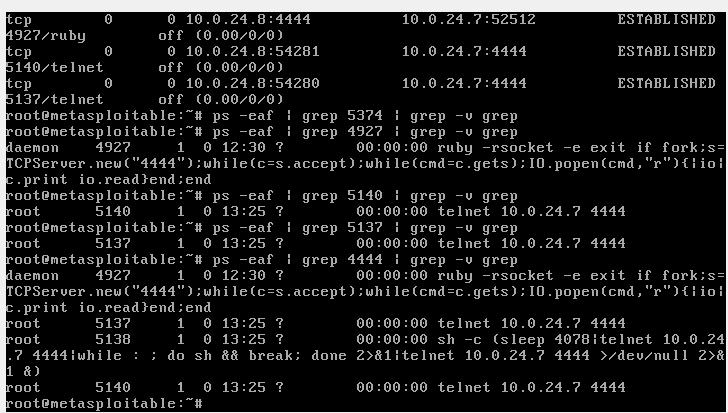
1. Настраиваем эксплоит для атаки на Metasploitable
2. Запускаем эксплоит командой **exploit**.



## 3. Форензика

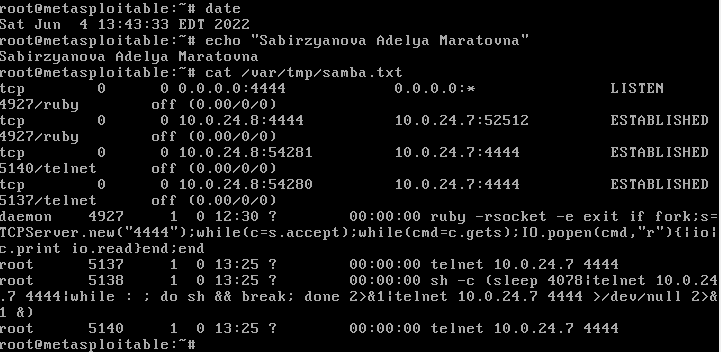
Цель: выявить проникновение в систему

Алгоритм:

1. Осуществляем поиск аномальной активности с помощью утилиты netstat
2. Анализируем подозрительные процессы

Результат: мы выявили проникновение

## 4. Оформление результатов работы



### 