Сабирзянова А.М.

11-901

ИСПОЛЬЗОВАНИЕ DISTCC ДЛЯ ПОЛУЧЕНИЯ ПРАВ ROOT. СОЗДАНИЕ ДАМПА ПАМЯТИ LIME И ЕГО АНАЛИЗ.

Содержание:

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

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

[**3. Расширение прав доступа до root**](#_kvgvvl48ll8n) **4**

[**4. Форензика**](#_wcwh4bdc6sdc) **5**

[**5. Создание дампа памяти с помощью LiME**](#_bxrpyqmimdxa) **7**

[**6. Создание файлов для форензического анализа**](#_ib4aapyggno0) **7**

[**8. Оформление результатов работы**](#_bu6s7szbj78l) **9**

## 1. Настройка сети между Metasploitable и Kali Linux

Цель: объединить машины в одну сеть

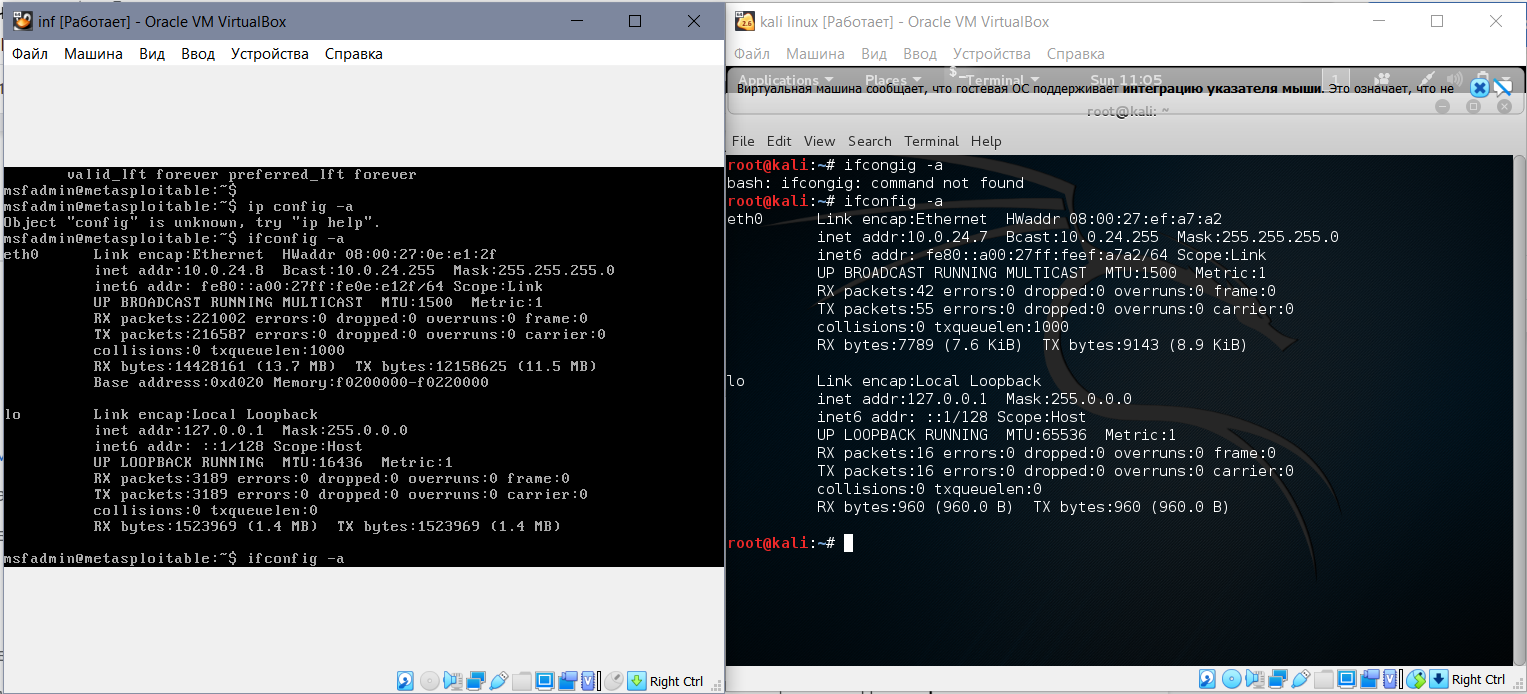
Начальная ситуация: между машинами связи нет

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

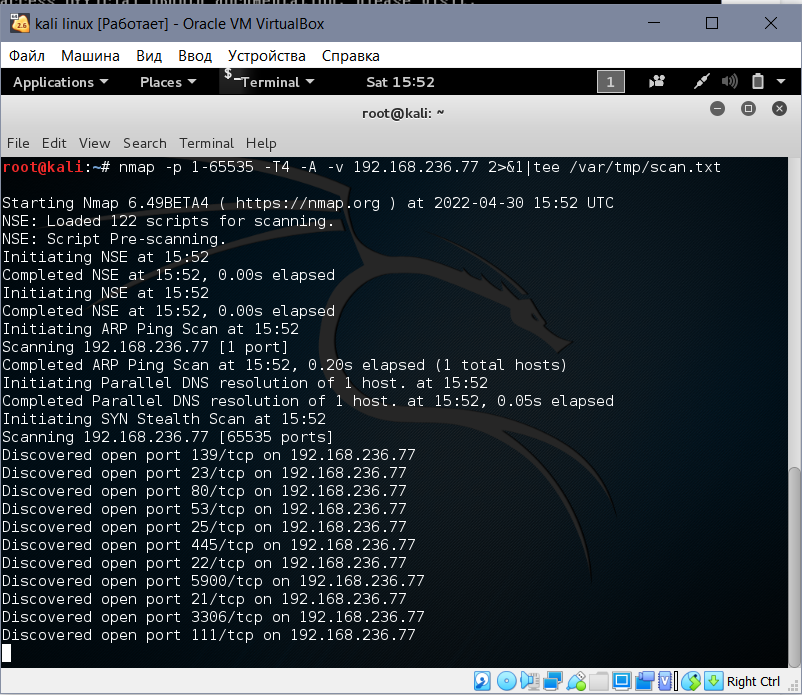


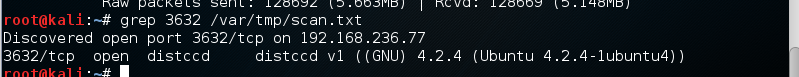
Результаты: полученные ip

## 2. Атака Metasploitable

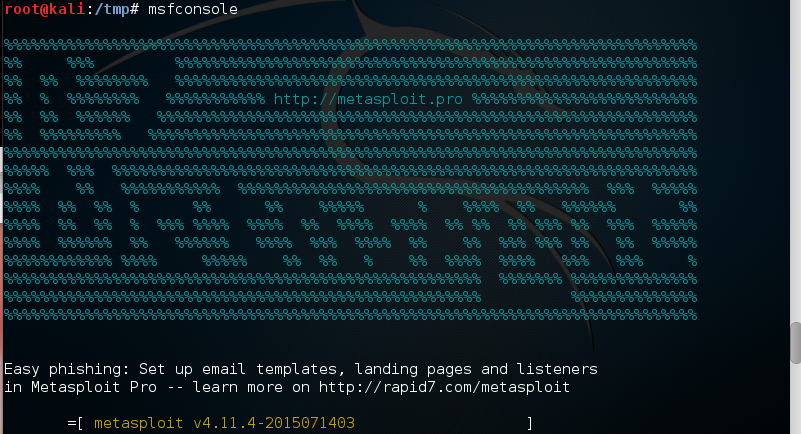
Цель: получить доступ к консоли на Metasploitable

Алгоритм:

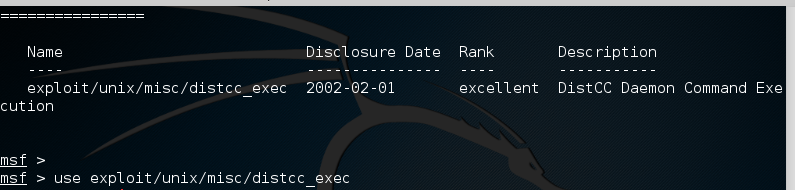
1. Сканируем порты машины Metasploitable с помощью команды **nmap**.
2. Находим distccd на 3632 порту



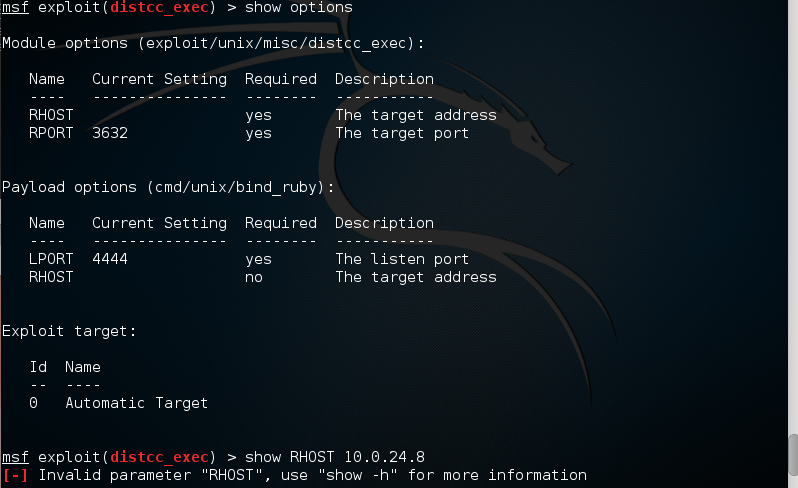
1. Запускаем консоль msfconsole



1. Ищем эксплоит для distcc

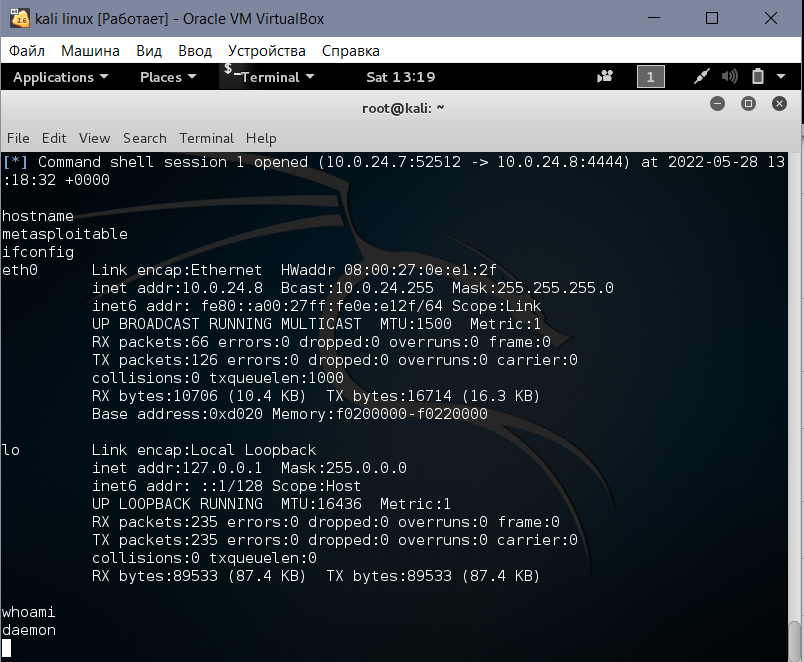


1. Настраиваем эксплоит для атаки на Metasploitable





1. Запускаем эксплоит командой **exploit**.



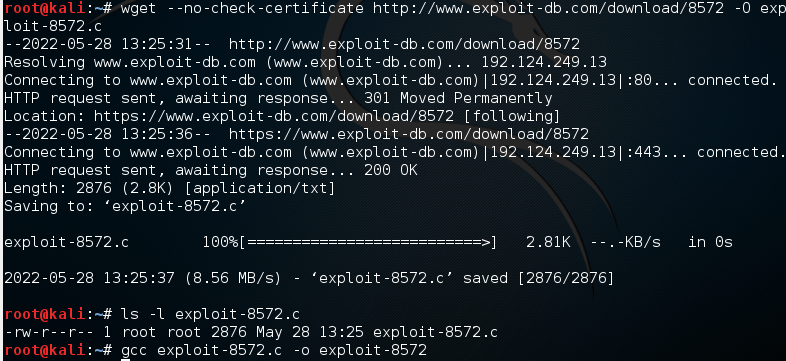
## 3. Расширение прав доступа до root

Цель: получить права root пользователя

Изначальная ситуация: имеем права пользователя daemon

Алгоритм:

1. Скачиваем эксплоит
2. Выполняем сборку командой **gcc**
3. Запускаем прослушивание порта 4444 на kali командой **netcat**
4. Создаём скрипт для подключения консоли по netcat на Metasploitable
5. Выясняем pid менеджера устройств (2412)
6. Проверяем работу



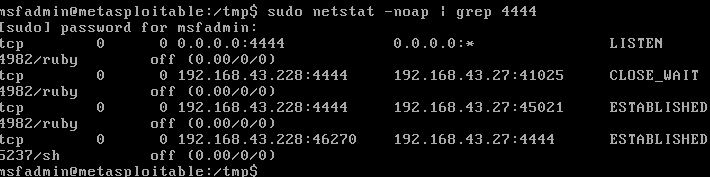
Результат: доступ к root пользователю получен.

## 4. Форензика

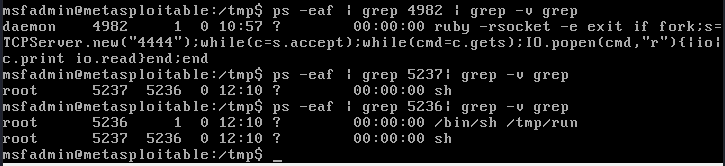
Цель: выявить проникновение в систему

Алгоритм:

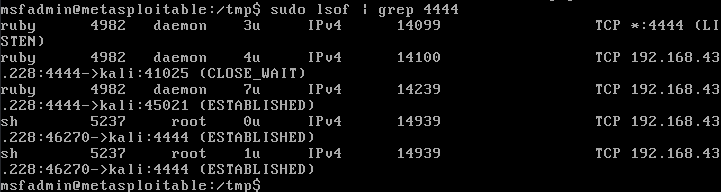
1. Смотрим открытые сетевые соединения



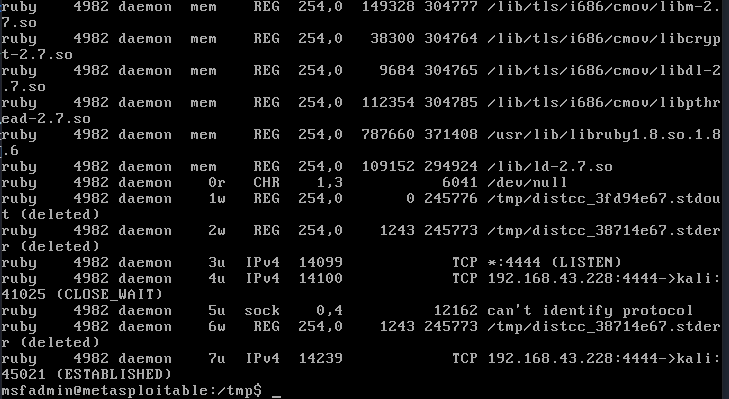
1. Просматриваем процессы, использующие соединения



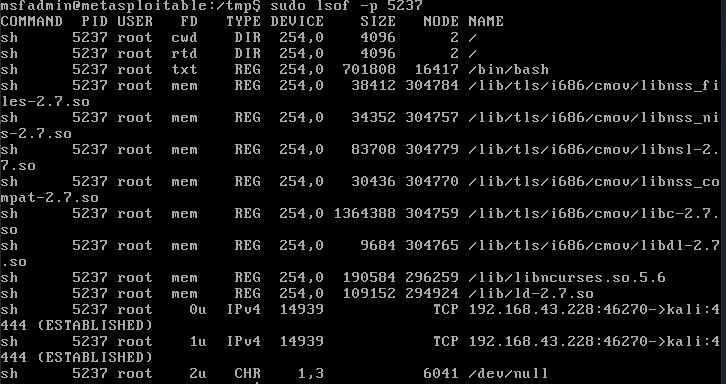
1. Смотрим информацию о запущенных соединениях



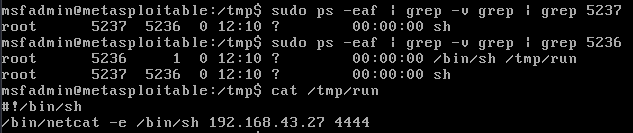
1. Анализируем работу на RUBY\_PID



1. Анализируем работу SH\_PID



1. Анализируем подозрительные процессы с root правами.



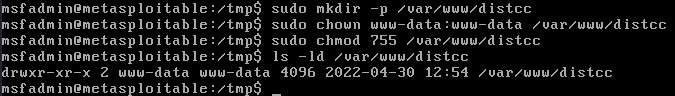
Результат: мы выявили проникновение

## 5. Создание дампа памяти с помощью LiME

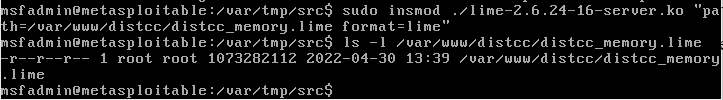
Цель: создать дамп памяти

Алгоритм:

1. Создаём папку для дампа



1. Создаём дамп памяти с помощью LiME



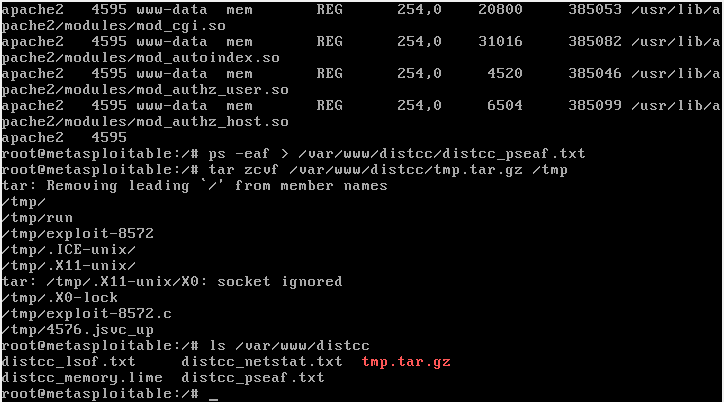
Результат: мы создали дамп памяти

## 6. Создание файлов для форензического анализа

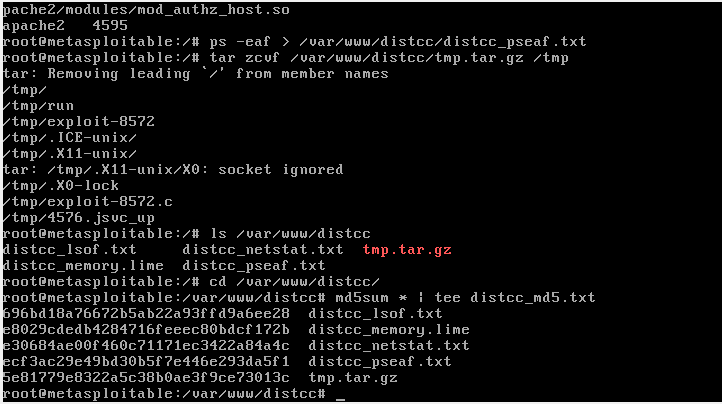
Цель: создать файлы для форензического анализа

Алгоритм:

1. Переходим в корневой каталог
2. Создаём файлы с данными о соединениях, процессах, используемых ими файлах, файлы в /tmp

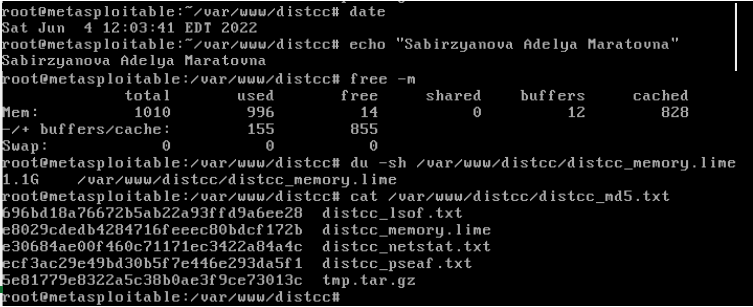


1. Создаём хеш-суммы файлов



Результат: мы создали файлы для форензического анализа

## 8. Оформление результатов работы



### 