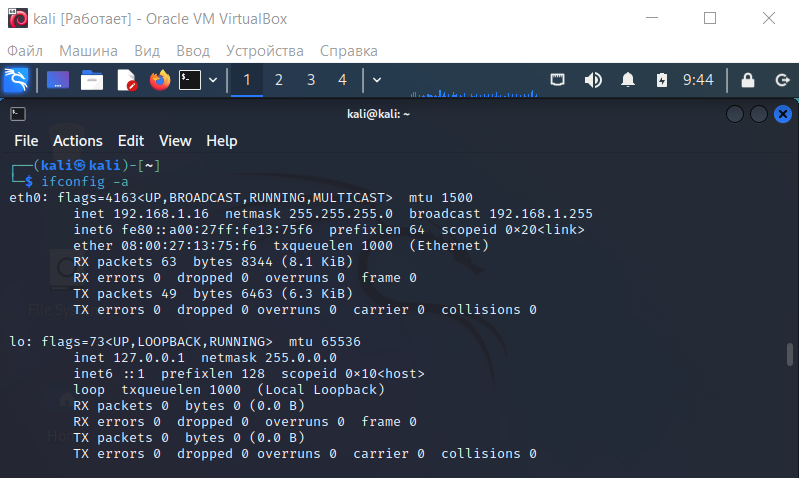
1. Создание виртуальной машины Kali Linux, настройка сети

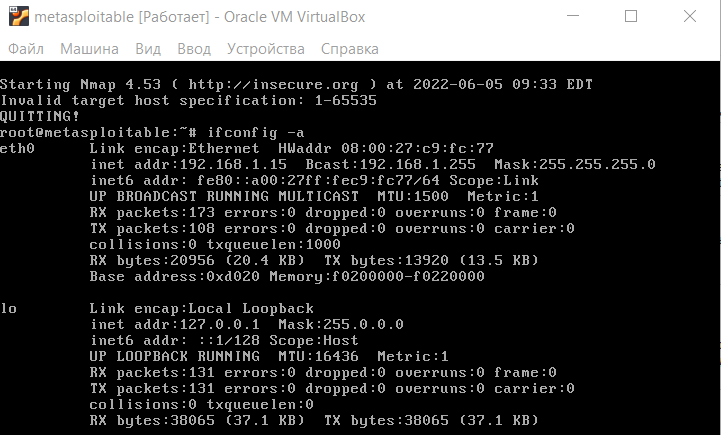
Цель: настроить сеть

Исходная ситуация: сетьь не настроена

KL\_IP = 192.168.1.16



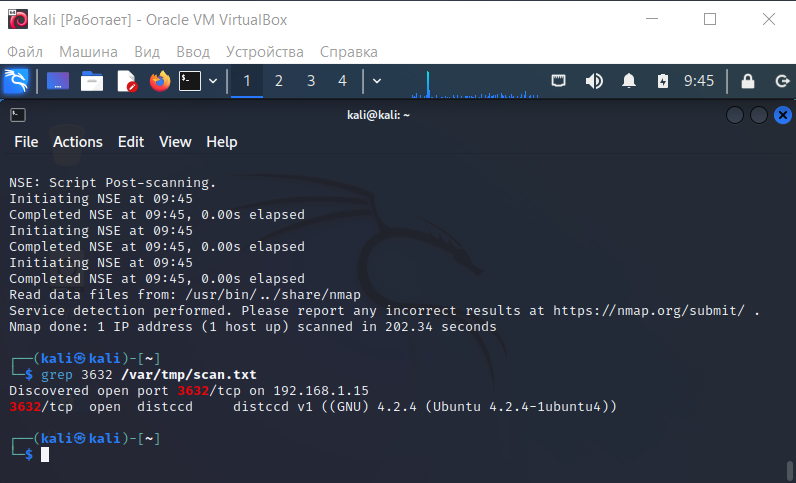
MS\_IP = 192.168.1.15



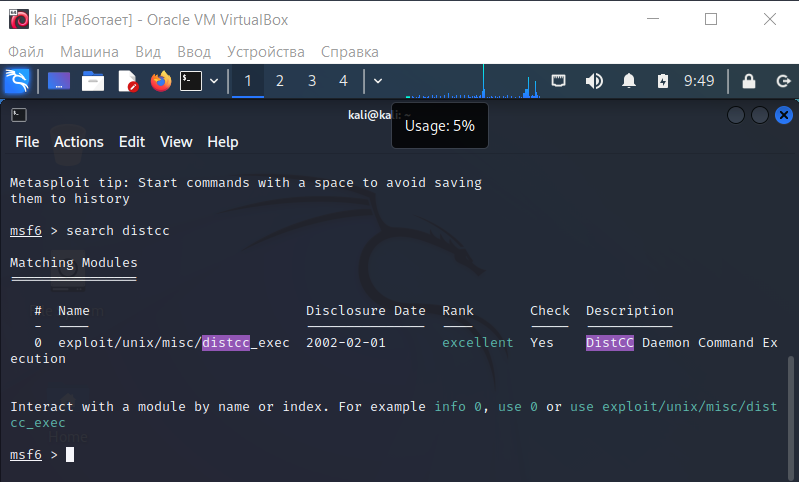
Итог: сеть настроена

1. Атака на metasploitable

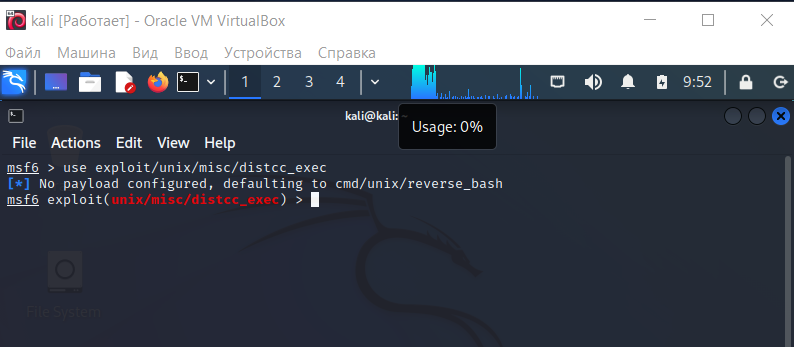
Сканирование портов



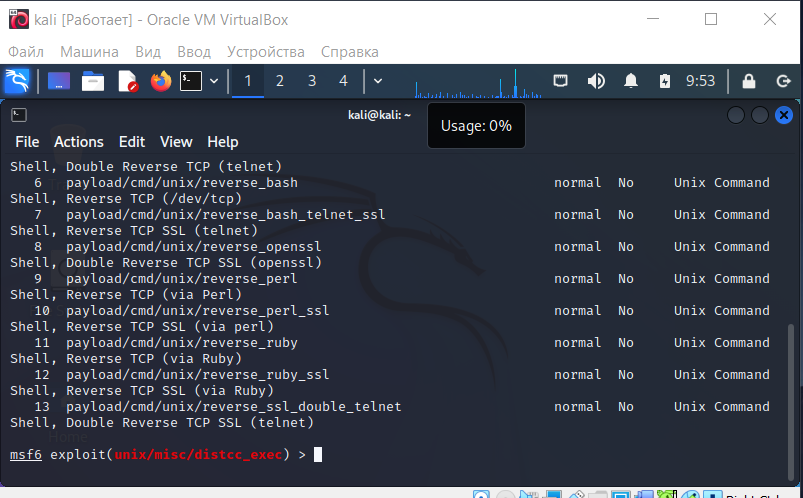
Поиск эксплоита



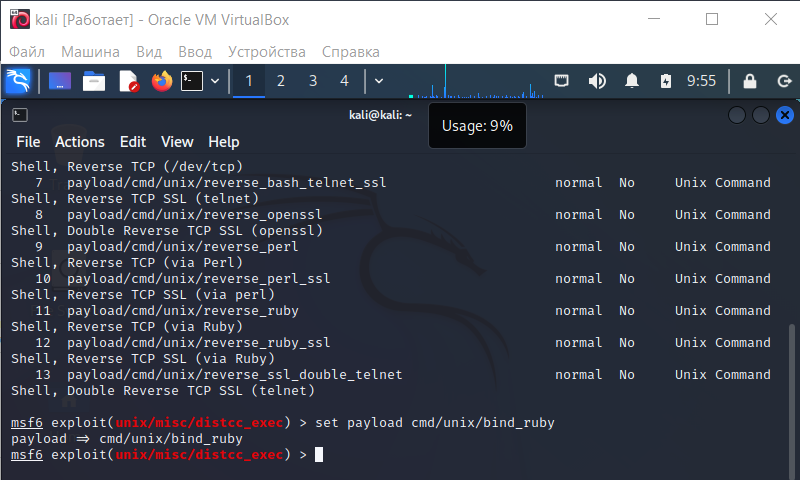
Запуск

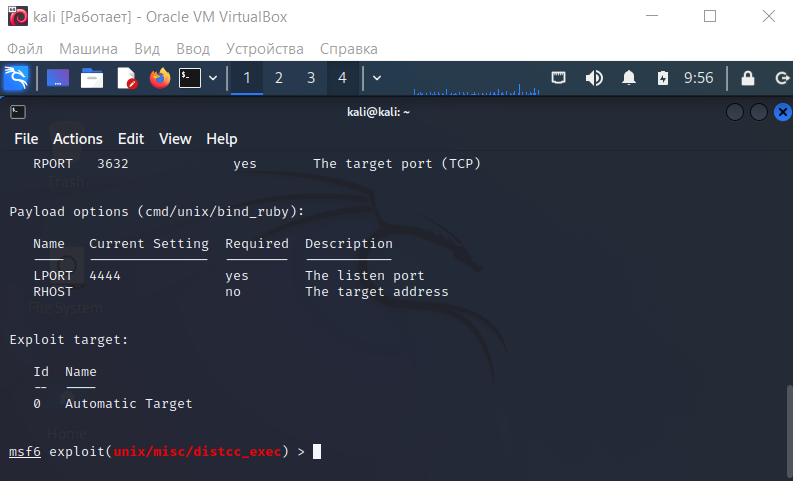


Доступные загрузчики

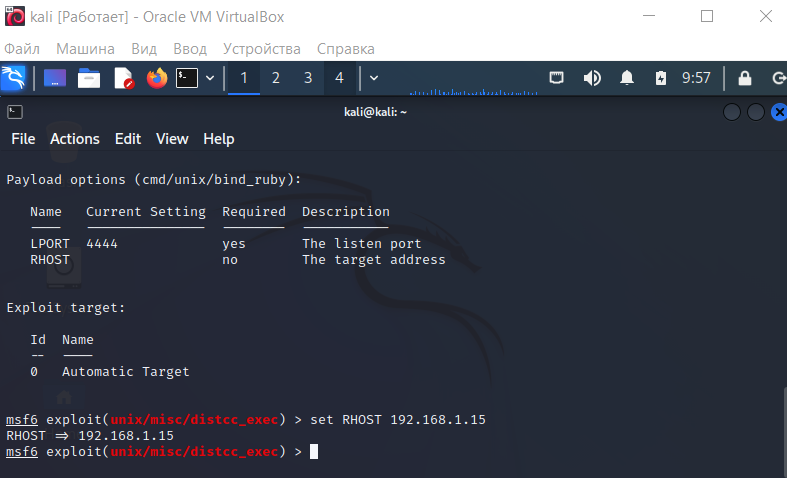


Выбор загрузчика

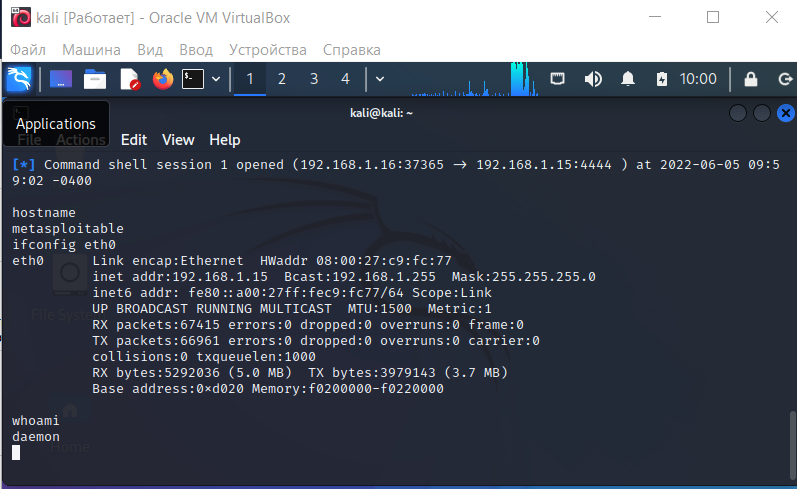


Список настроек  


Установка ip адреса жертвы



Получение доступа к Metasploitable



Расширение прав до root

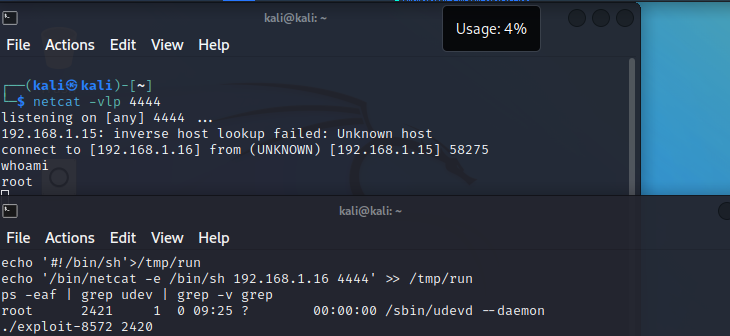
Цель: получить рут права

Исходная ситуация: прав нет

Скачивание эксплоита *exploit-8572 *

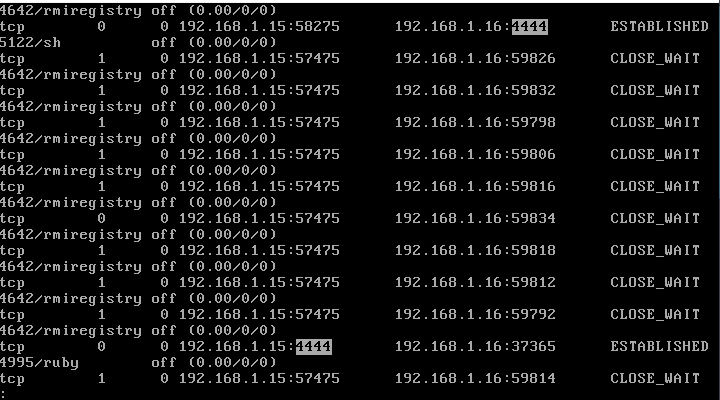
Создание netcat сессии для удаленного управления

Использование *exploit-8572* для предоставления удаленной консоли с правами root по netcat

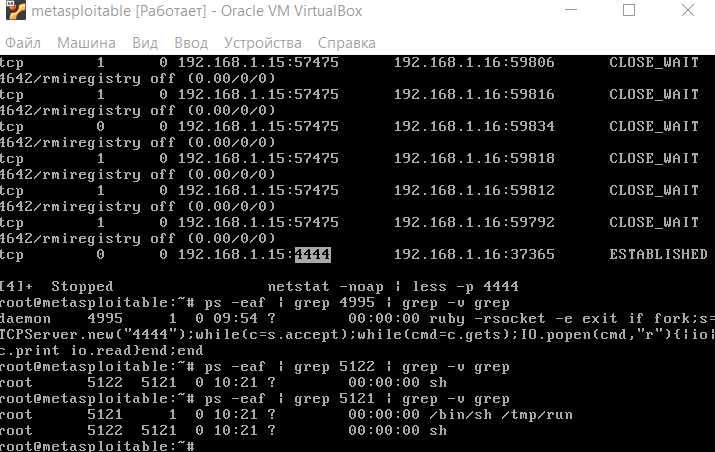


5. Форензика

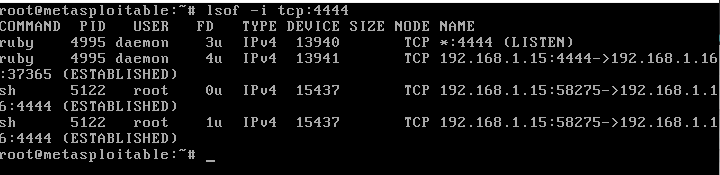
Выявление аномальной активности



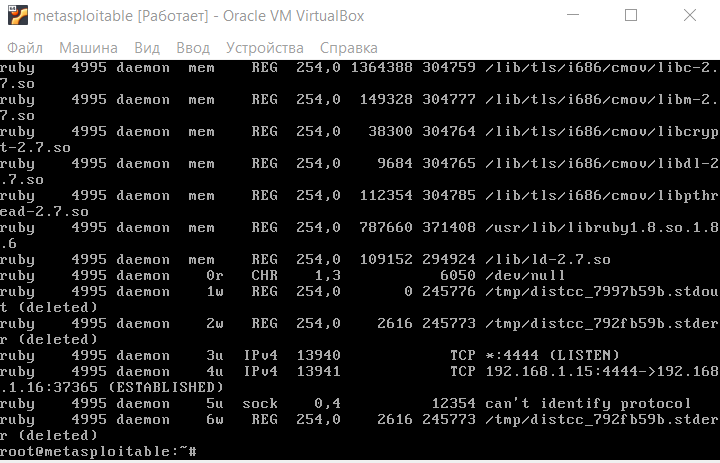
ps -eaf | grep RUBY\_PID | grep -v grep



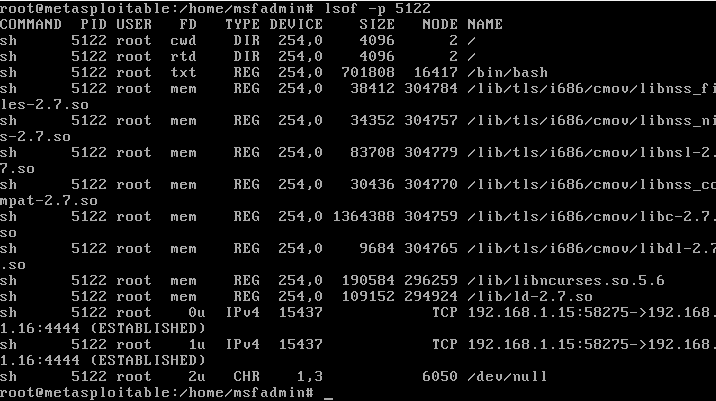
Какие файлы используются netcat сессией на порту 4444



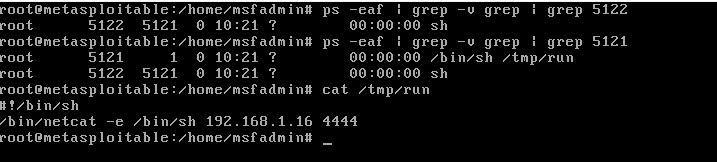
Используем lsof для анализа демона с процессом RUBY\_PID



Используем lsof для анализа netcat сессии c процессом SH\_PID и root правами

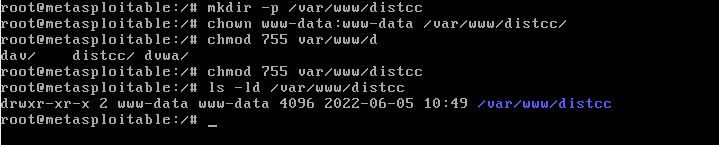


Используем ps для анализа netcat сессии с процессом SH\_PID и root правами.

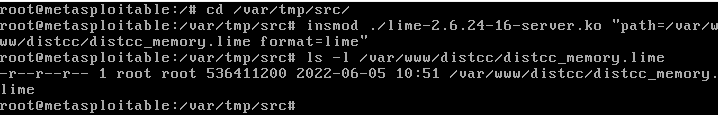


6. Создание дампа памяти с помощью LiME

Подготовка директории

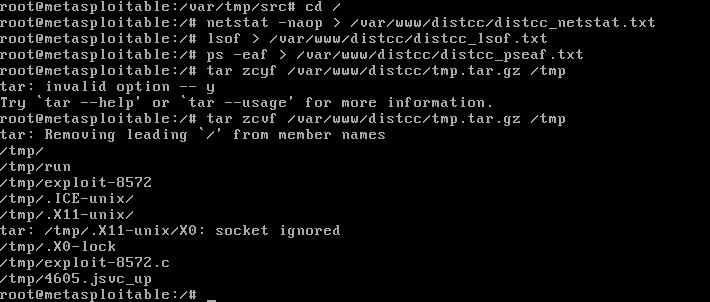


Создание дампа

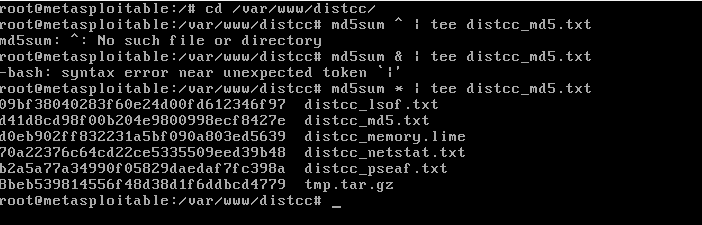


7. Создание файлов для форензического анализа

Сохранение сведений о системе



Создание MD5 хеш-суммы



8. Оформление

