

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОЙ РАБОТЫ №5**

# **В РАМКАХ ДИСЦИПЛИНЫ «БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»**

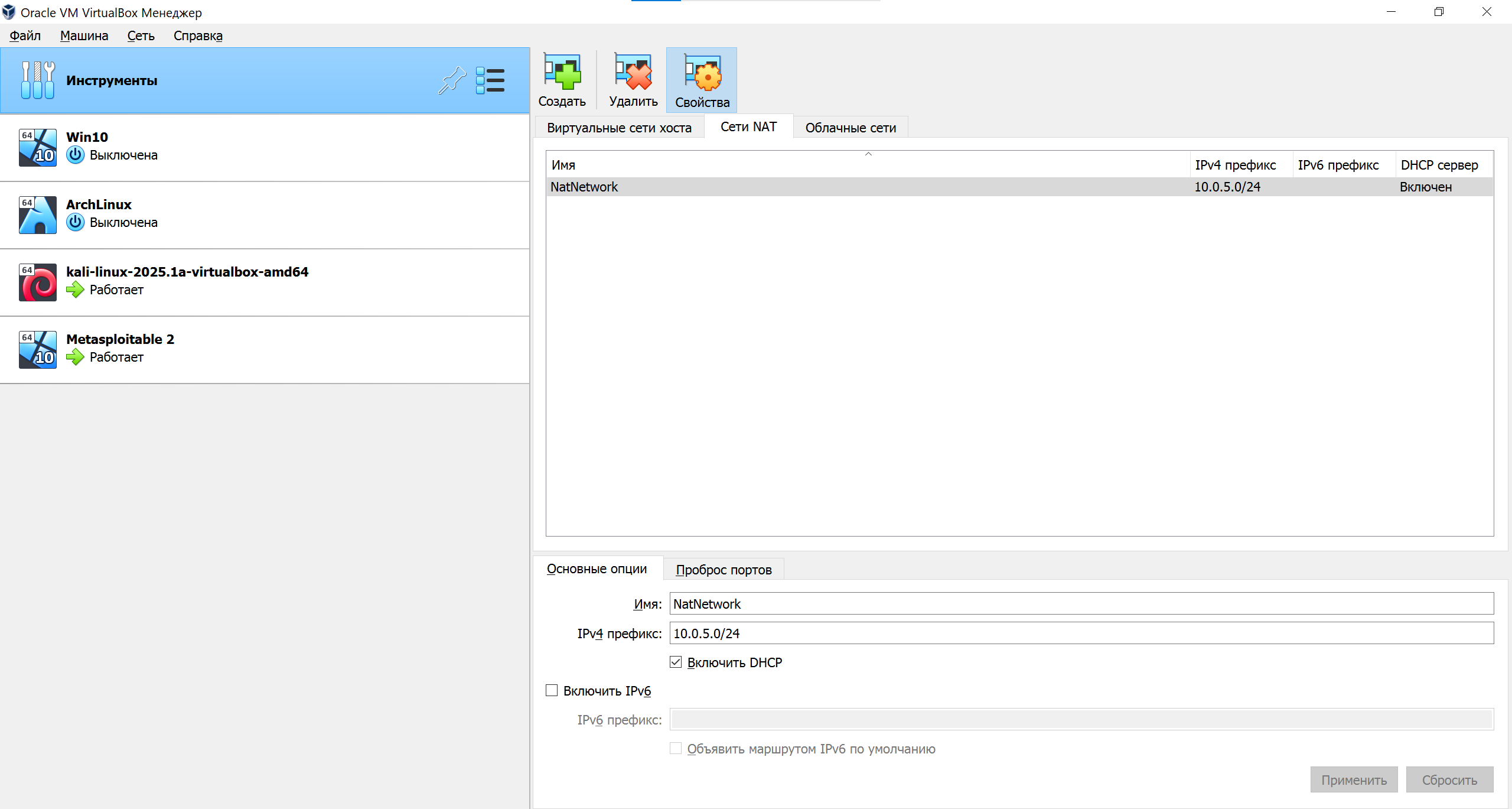
Выполнил:

Студент 3-ого курса

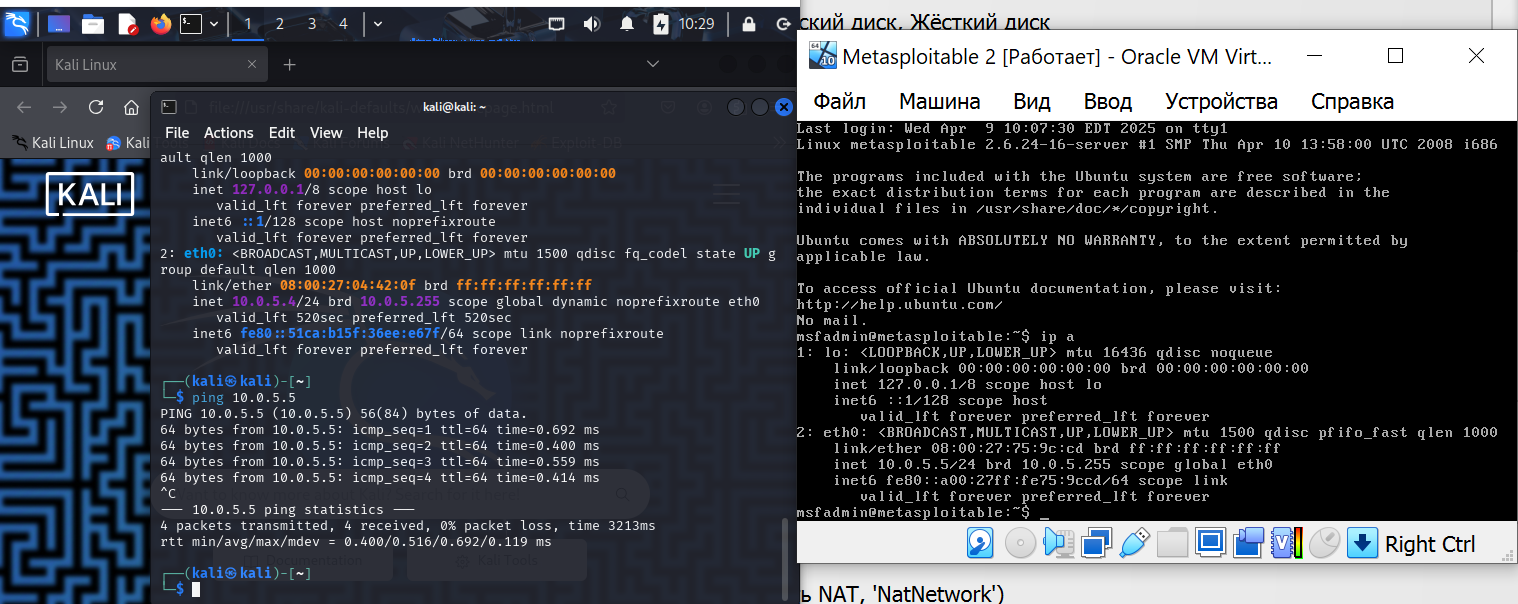
Учебной группы БИСО-02-22

Зубарев В.С.

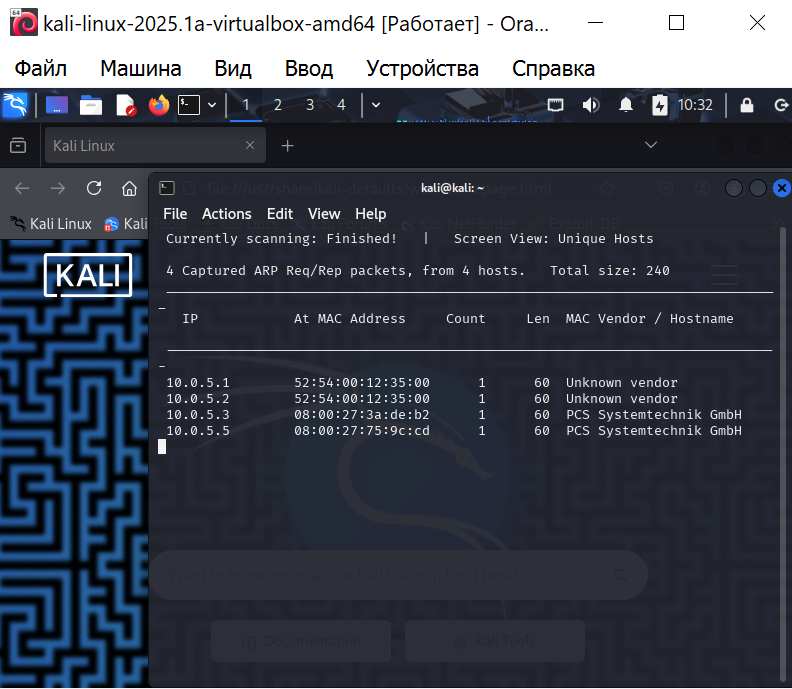
Создание сети NAT



Проверка настроек сети NAT



Поиск цели с помощью инструмента netdiscover

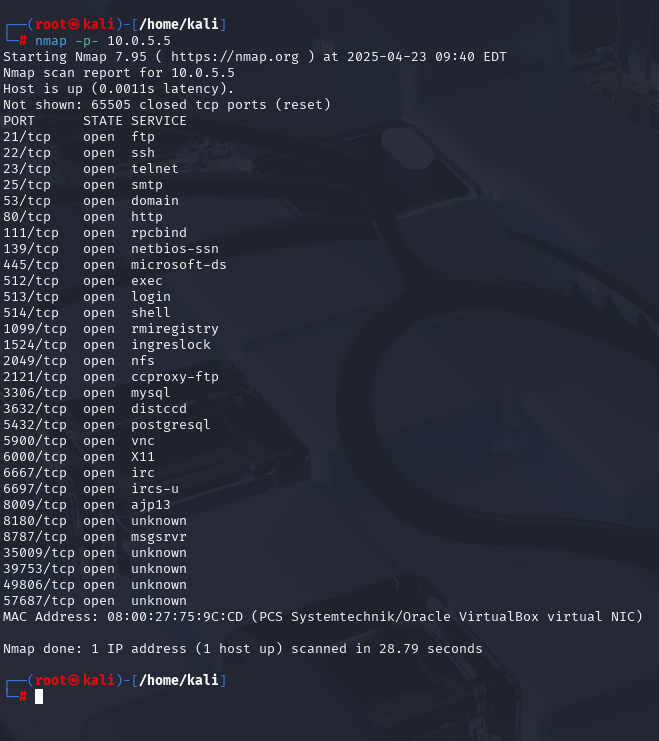


Перечень известных систем виртуализации, их отличительные особенности.  
Oracle VirtualBox, VMWare Workstation  
**VirtualBox** — это бесплатное решение с открытым исходным кодом для виртуализации, которое поддерживает широкий спектр операционных систем, включая Windows, macOS, Linux и Solaris. Подходит для личного использования и тестирования. [1](https://www.securitylab.ru/blog/personal/xiaomite-journal/354260.php)

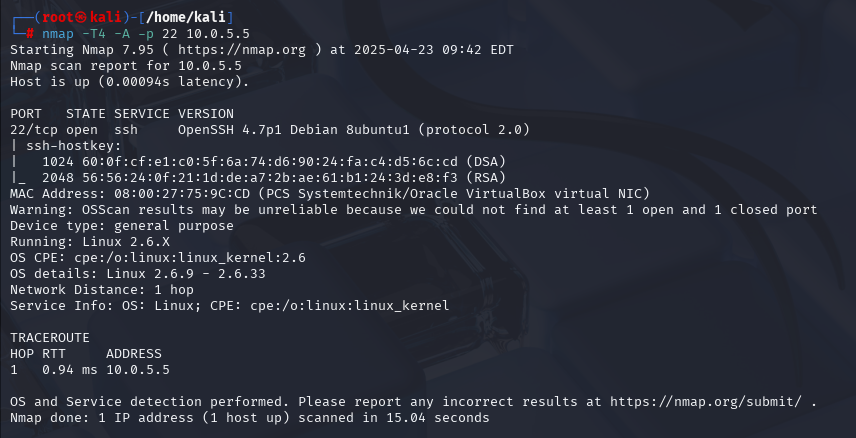
**VMware** — это платное решение для профессиональной виртуализации, которое часто используют в корпоративной среде. Предлагает высокую производительность и поддержку сложных сетевых инфраструктур.

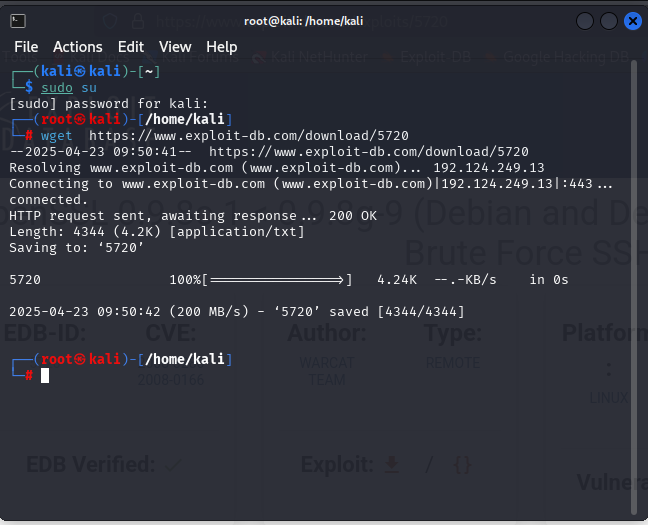
**Тестирование сервиса SSH**

Получите список открытых портов на целевой машине, сделайте screenshot.



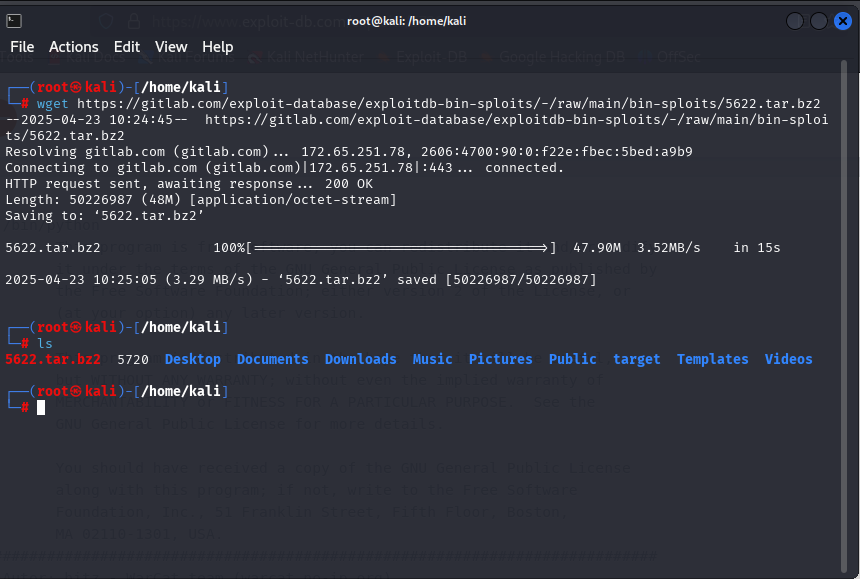
Сделайте более углубленное сканирование этого порта.



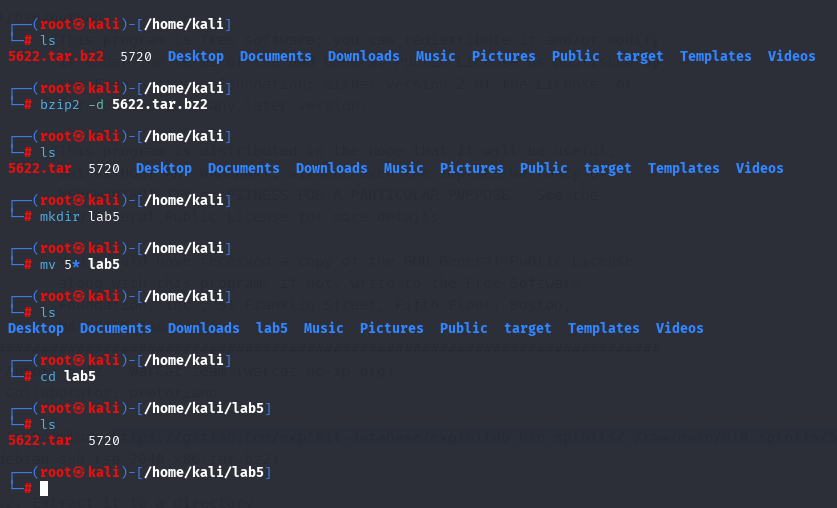
Загрузка эксплойта  


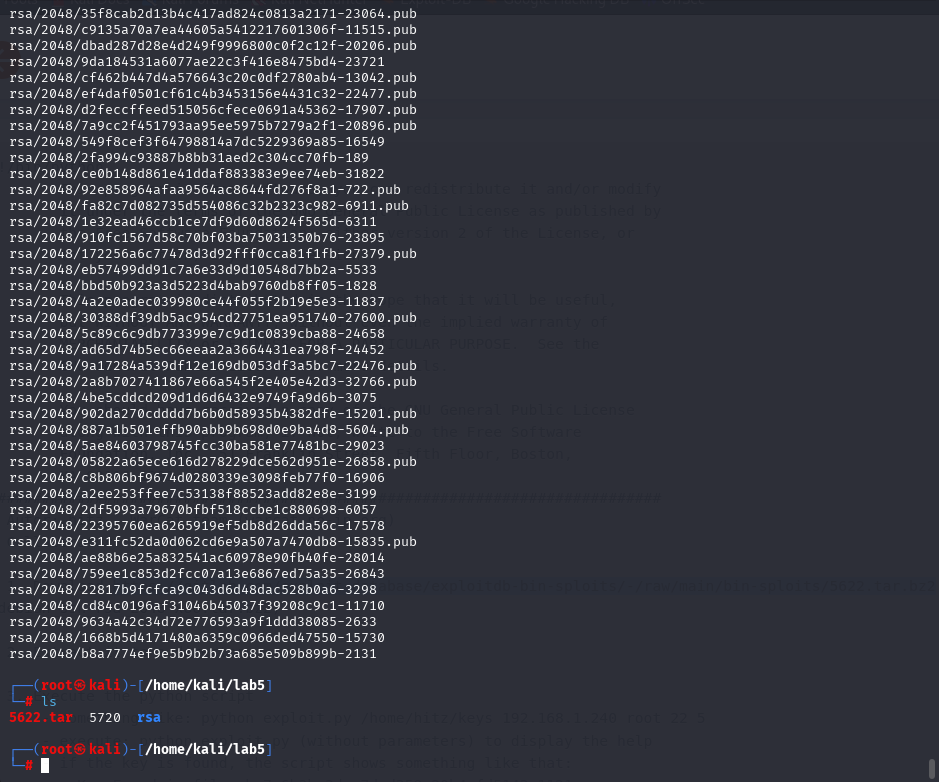
Скачивание файла

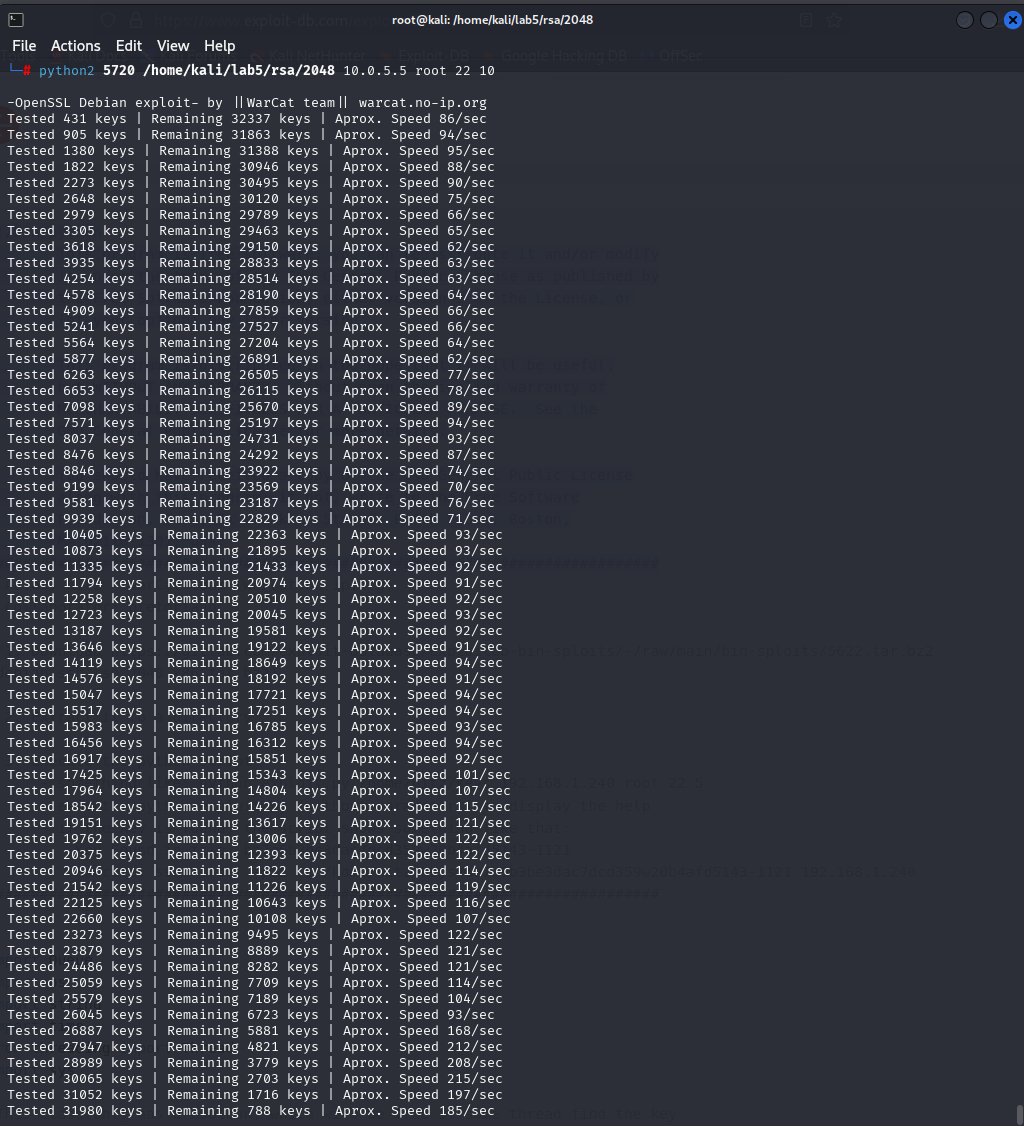
Актуальная ссылка   
https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/5622.tar.bz2



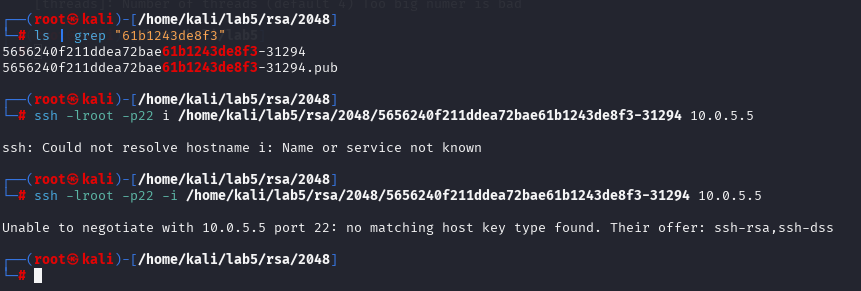
Разархивирование архива



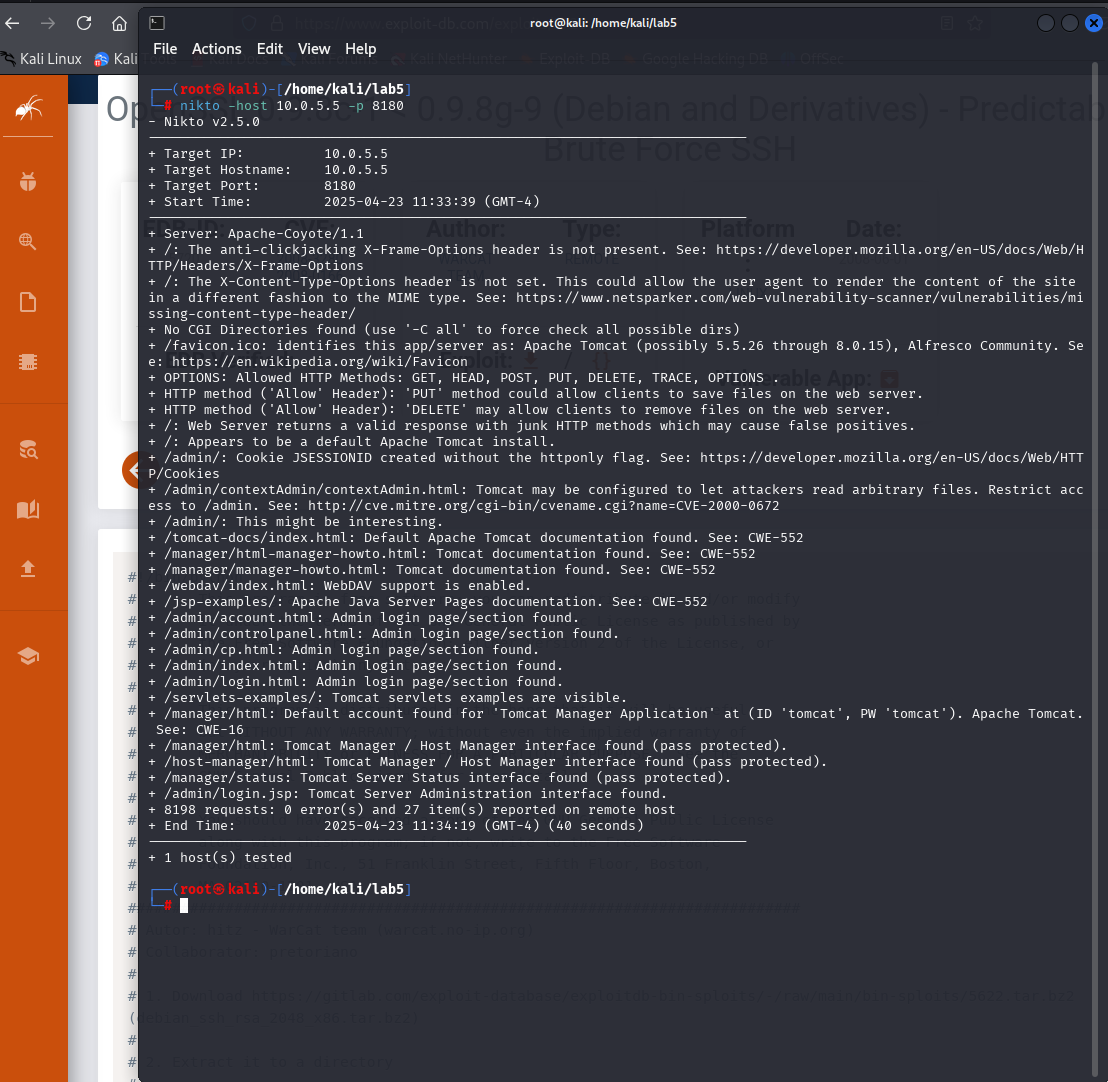
Все возможные ключи RSA  


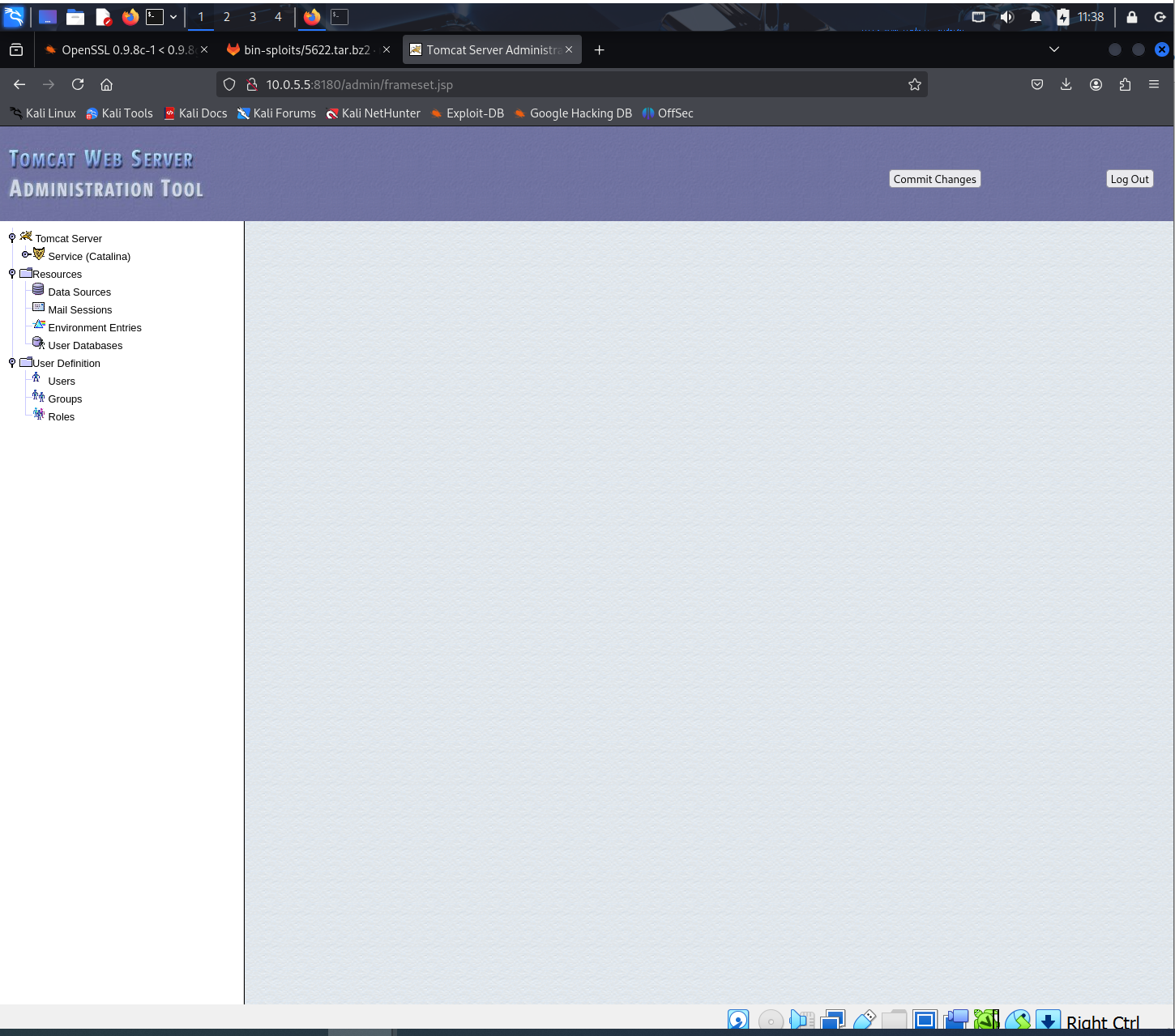
Проверка ключей  


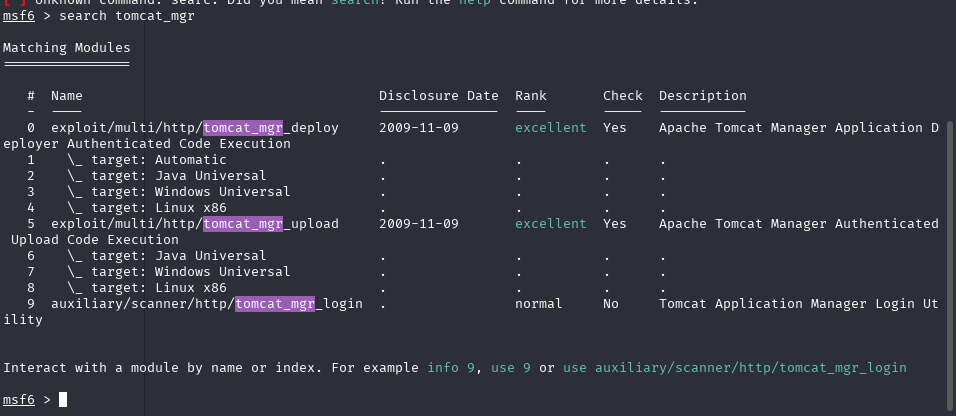
Скрипт не обнаружил нужной пары ключей

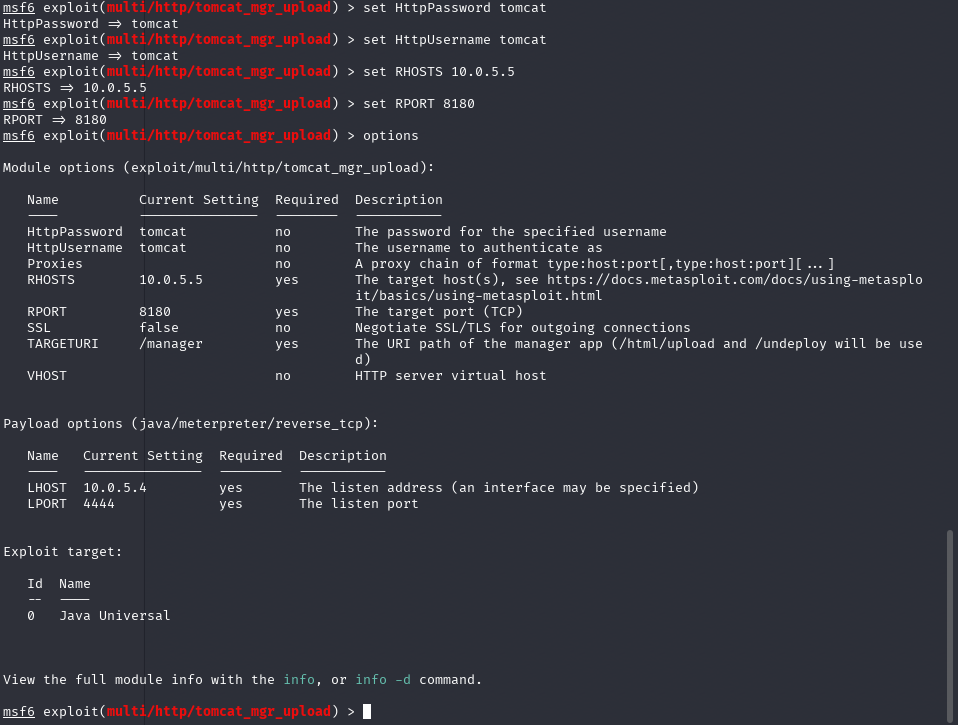
На основании сканирования выявлены пары ключей  


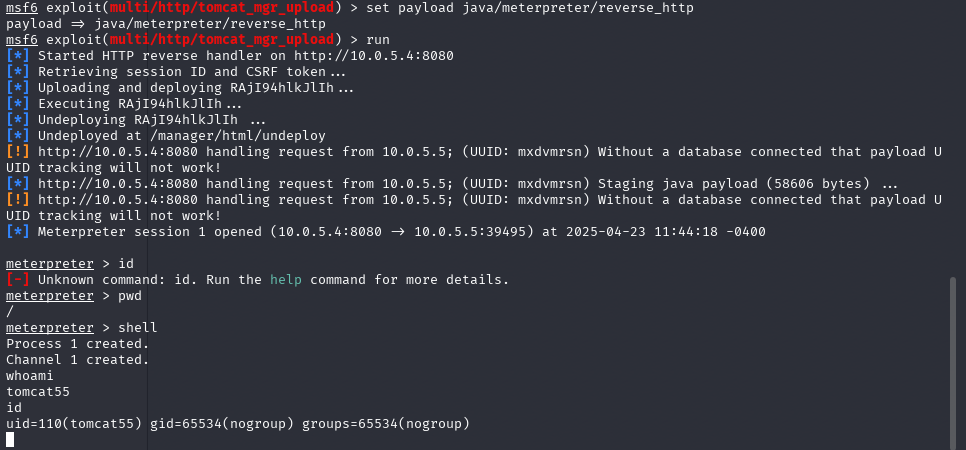
**Тестирование сервисов WEB**

Сканирование утилитой Nikto  


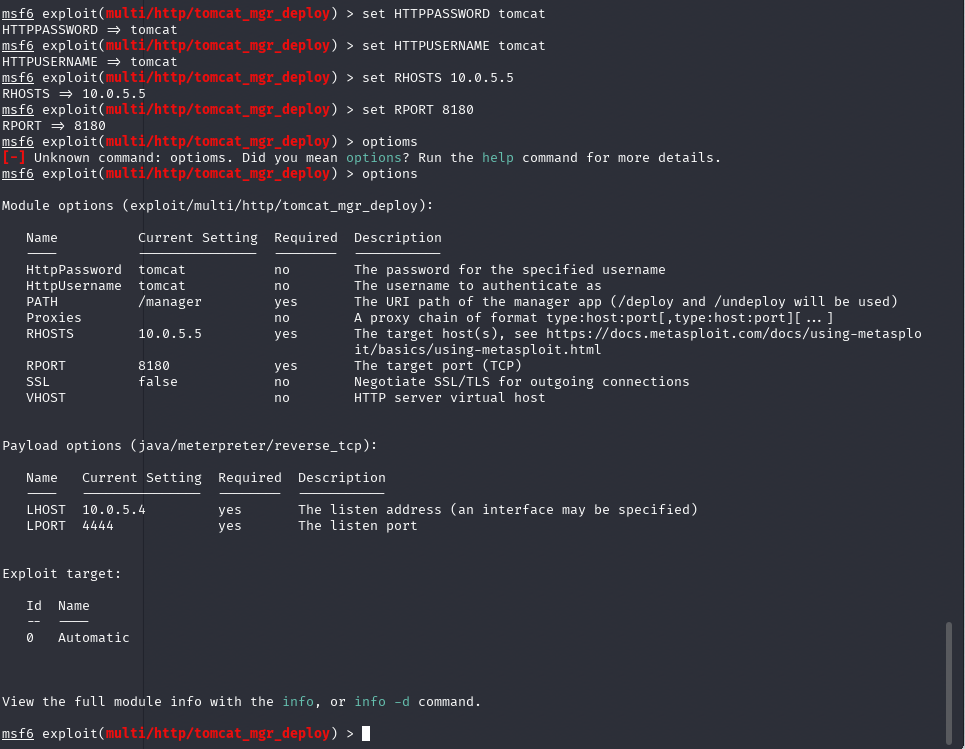
Авторизация на сервере  


Поиск эксплойтов  


Установка параметров  


Установка полезной нагрузки, получение доступа к вебсерверу  


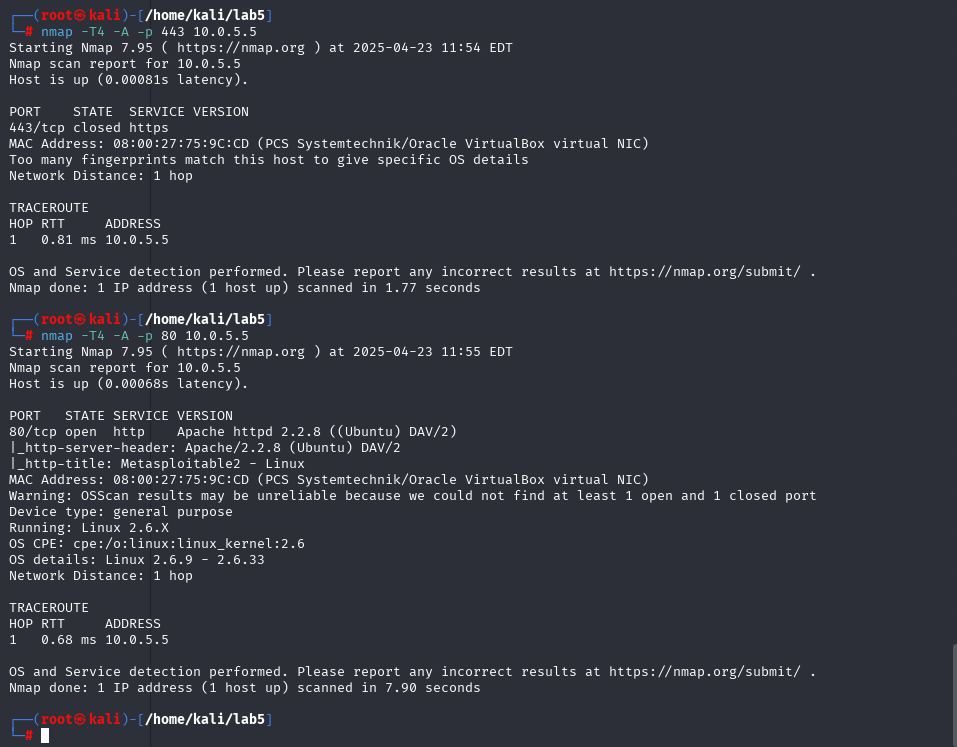
Подключитесь к атакуемой машине используя tomcat\_mgr\_deploy, опишите переменные, которые будете изменять;



Замена параметровpassword, username, rhosts, payload  
Какая команда meterpreter используется для повышения прав в   
windows?

getsystem

Какие сервисы занимают порты 80 и 443 у атакуемой цели?

  
Описание основных ключей команды nikto

* **-Display**. Позволяет контролировать вывод информации Nikto. Можно указать тип вывода с помощью номера или буквы. Например, 1 — показать перенаправления, 2 — полученные файлы cookie, 3 — все ответы 200/OK и т. д..
* **-evasion**. Указывает технику кодировки LibWhisker. Можно указать несколько вариантов.
* **-findonly**. Позволяет обнаружить только порты HTTP(S), не выполняя сканирование безопасности.
* **-Format**. Указывает формат сохранения выходного файла. Возможные варианты: csv — список, разделённый запятыми, htm — отчёт в формате HTML, txt — текстовый отчёт, xml — отчёт в формате XML.
* **-host**. Указывает цель сканирования. Это может быть IP-адрес, имя хоста или текстовый файл с именами хостов.
* **-Help**. Выводит расширенную информацию о помощи.
* **-id**. Указывает ID и пароль для использования на хосте. Формат: «id».
* **-list-plugins**. Выводит список всех плагинов, которые Nikto может запускать против целей, и выходит без выполнения сканирования.
* **-Pause**. Указывает секунды (целое число или число с плавающей точкой) для задержки между каждым тестом.
* **-root**. Добавляет указанное значение в начало каждого запроса. Это полезно для тестирования приложений или веб-серверов, которые имеют все свои файлы в определённом каталоге.
* **-ssl**. Проверяет только SSL на указанных портах. Использование этого параметра значительно ускоряет запросы к портам HTTPS.
* **-Single**. Выполняет один запрос к целевому серверу. Nikto запрашивает все возможные опции, а затем предоставляет подробный вывод.
* **-timeout**. Указывает секунды, которые нужно ждать перед истечением срока запроса. По умолчанию время ожидания — 10 секунд.
* **-Tuning**. Позволяет контролировать тесты, которые Nikto использует против цели.
* **-useproxy**. Использует HTTP-прокси, определённый в файле конфигурации или данный в качестве аргумента в формате «[http://server:port»](http://server:port%C2%BB/).
* **-update**. Обновляет плагины и базы данных напрямую с cirt.net.
* **-Version**. Выводит версии программного обеспечения Nikto, плагинов и баз данных.