

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

# «МИРЭА – Российский технологический университет» РТУ МИРЭА

# РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Прикладные информационные технологии»

Практическая работа № 5

по дисциплине «Безопасность Операционных систем»

«Основы Kali Linux ч.2»

|  |  |
| --- | --- |
|  | Выполнил:  Студент БББО-05-20  Кутьин З.С. |
|  | Проверил:  Абрамов Д.П. |

Москва

2022

**Цель работы**

Продолжить изучение инструментов Kali linux nmap, metasploit.

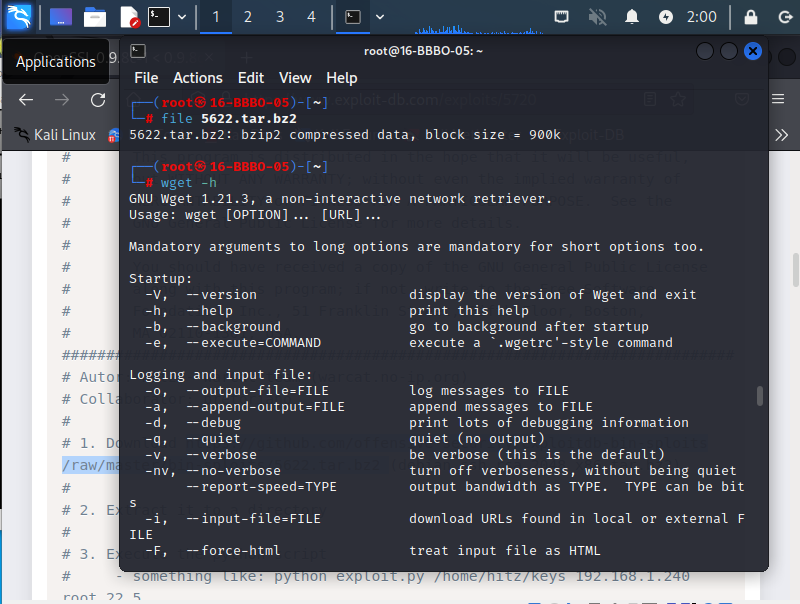
**Время выполнения работы:** 4 академических часа.

**Порядок выполнения работы**

**1. Взламываем SSH**

1) Ссылка на уязвимость в каталоге Mitre AT&T: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2008-0166>

2) Описание основных ключей команды wget:



**-V** - вывести версию программы

**-h** - вывести справку

**-b** - работать в фоновом режиме

**-o файл** - указать лог файл

**-d** - включить режим отладки

**-v** - выводить максимум информации о работе утилиты

**-q** - выводить минимум информации о работе

**-i файл** - прочитать URL из файла

**--force-html** - читать файл указанный в предыдущем параметре как html

**-t** - количество попыток подключения к серверу

**-O файл** - файл в который будут сохранены полученные данные

**-с** - продолжить ранее прерванную загрузку

**-S** - вывести ответ сервера

**--spider** - проверить работоспособность URL

**-T время** - таймаут подключения к серверу

**--limit-rate** - ограничить скорость загрузки

**-w** - интервал между запросами

**-Q** - максимальный размер загрузки

**-4** - использовать протокол ipv4

**-6** - использовать протокол ipv6

**-U** - строка USER AGENT отправляемая серверу

**-r -** рекурсивная работа утилиты

**-l** - глубина при рекурсивном сканировании

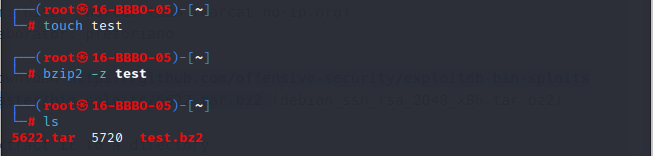
**-k** - конвертировать ссылки в локальные при загрузке страниц

**-P** - каталог, в который будут загружаться файлы

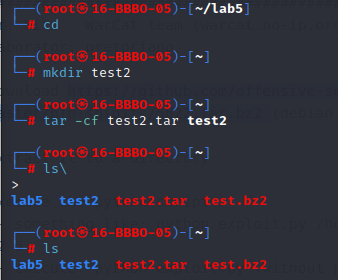
**-m** - скачать сайт на локальную машину

**-p** - во время загрузки сайта скачивать все необходимые ресурсы

3) Создайте файл test и заархивируйте ее с помощью bzip2, результат приложите скриншотом



4) Создайте папку test2 и заархивируйте ее с помощью tar, результат приложите скриншотом. Дайте описание использованным ключам.



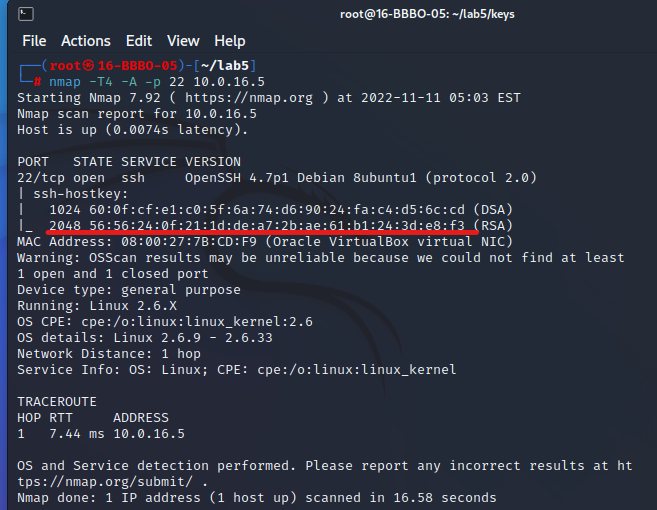
**mkdir** — команда для создания пустых каталогов

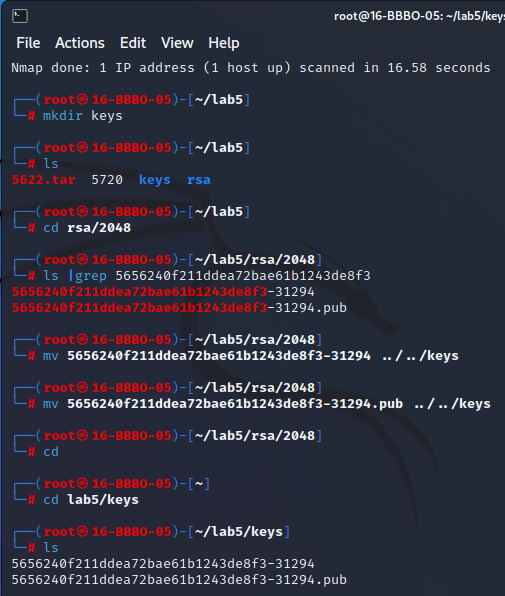
**tar <опции> <архив.tar> <файлы для архивации>** – команда для архивации данных

* **-сf –** создать новый архив для архивации в нем файла

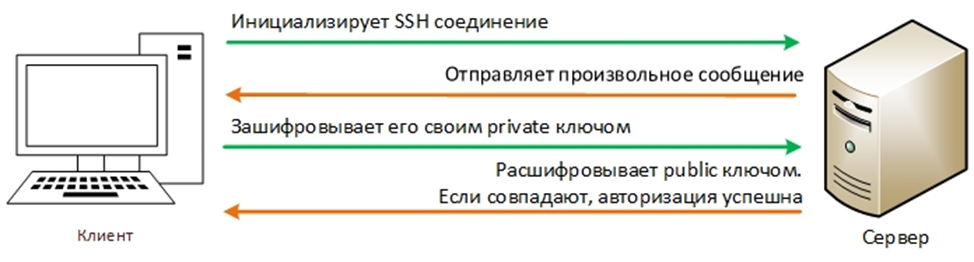
**ls** – вывод информации о содержимом каталога

5) Заново проведите сканирование nmap по порту 22, сохраните название ключа rsa (2048). Используя grep найдите пару ключей в папке rsa/2048/ и переместите их в отдельную папку keys.

****

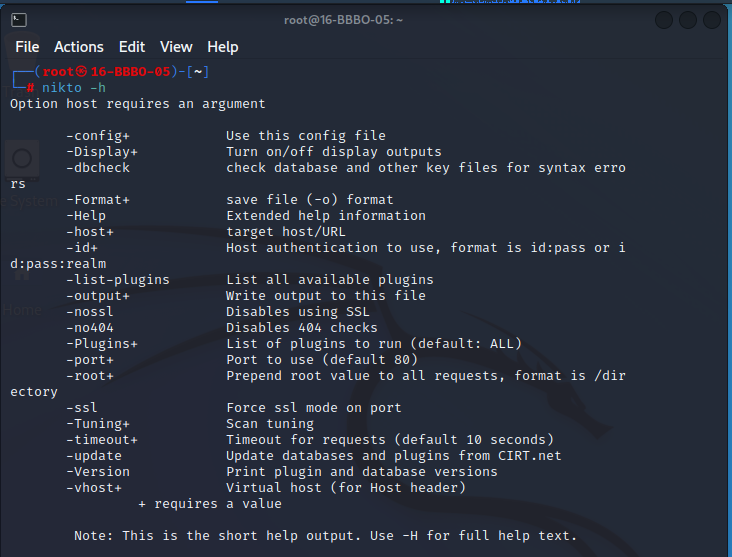


6) Изобразите схему работы OpenSSH.



**2. Взламываем WEB сервис**

1) Описание основных ключей команды nikto



**-ask** – Спрашивать ли о получении обновлений/отправке данных об обнаруженных новых веб-серверах и службах

**-Cgidirs** – Сканировать эти CGI директории: "none", "all" или значения вроде "/cgi/ /cgi-a/"

**-config** – Использовать этот конфигурационный файл

**-Display** – Включить/отключить отображение вывода:

**-dbcheck** – Проверить базу данных и другие ключевые файлы на ошибки синтаксиса

**-Format** – Сохранить файл (-o) в формате:

                            csv   Значения, разделённые запятыми

                            htm   HTML формат

                            nbe   Nessus NBE формат

                            sql   Универсальный SQL

                            txt   Простой текст

                            xml   XML формат

                            (если не указан, формат будет взят из расширения файла, переданного опцией -output)

**-host** – Целевой хост

**-404code** – Игнорировать эти HTTP коды как негативный ответ

**-404string** –Игнорировать эти строки в содержимом теле ответа как негативный ответ (всегда).

**-id** – Использовать аутентификацию на хосте.

**-key** – Файл ключа клиентского сертификата

**-list-plugins** – Список доступных плагинов, тестирование не выполняется

**-maxtime** – Максимальное время тестирования для одного хоста

**-mutate** – Предположить дополнительные имена файлов

**-mutate-options** – Указать информацию для перестановок

**-nointeractive** – Отключить интерактивные функции

**-nolookup** – Отключить DNS преобразования

**-nossl** – Отключить использование SSL

**-no404** – Отключить попытки nikto угадать страницу 404

**-output** – Записать вывод в этот файл

**-Pause** – Пауза между тестами (секунды, целые или с плавающей точкой)

**-Plugins** – Список плагинов, которые нужно запускать (по умолчанию: ALL)

**-port** – Порт для использования (по умолчанию 80)

**-RSAcert** – Клиентский файл сертификата

**-root** – В начало всех запросов добавить корневую величину, формат /directory

**-Save** – Сохранить положительные ответы в эту директорию

**-ssl** – Принудительный ssl режим на порту

**-Tuning** – Тюнинг сканирования

    -**timeout** – Таймаут для запросов (по умолчанию 10 секунд)

    -**Userdbs** – Загрузить только пользовательскую, а не стандартную базу данных

    -**useragent** – Переписать дефолтный useragent

**-until** – Работать на протяжении этого времени

    -**update** – Обновить базы данных и плагины с CIRT.net

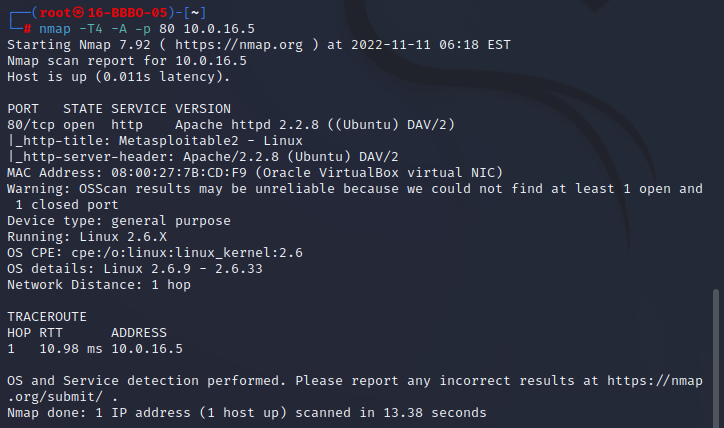
    -**useproxy** – Использовать прокси, установленное в nikto.conf или аргументом http://server:port

    -**Version** – Напечатать версии плагинов и базы данных

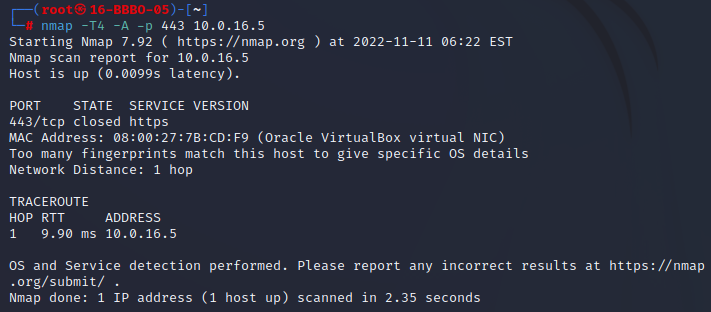
**-vhost** – Виртуальный хост (для Host header)

2)Какие сервисы занимают порты 80 и 443 у атакуемой машины?

80 – HTTP



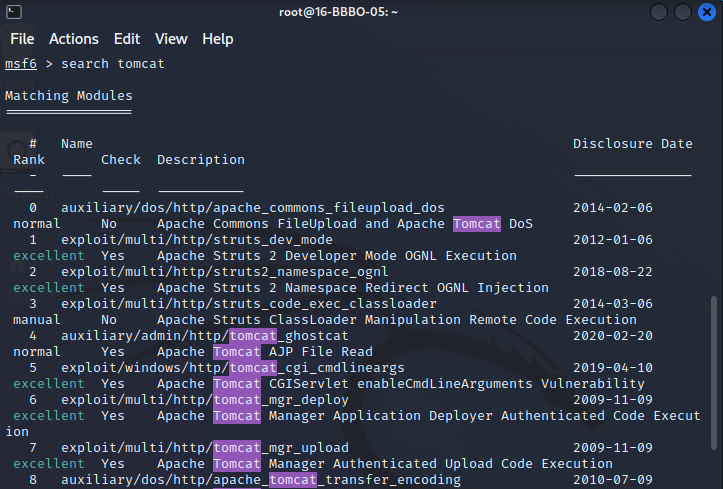
443 – HTTPS

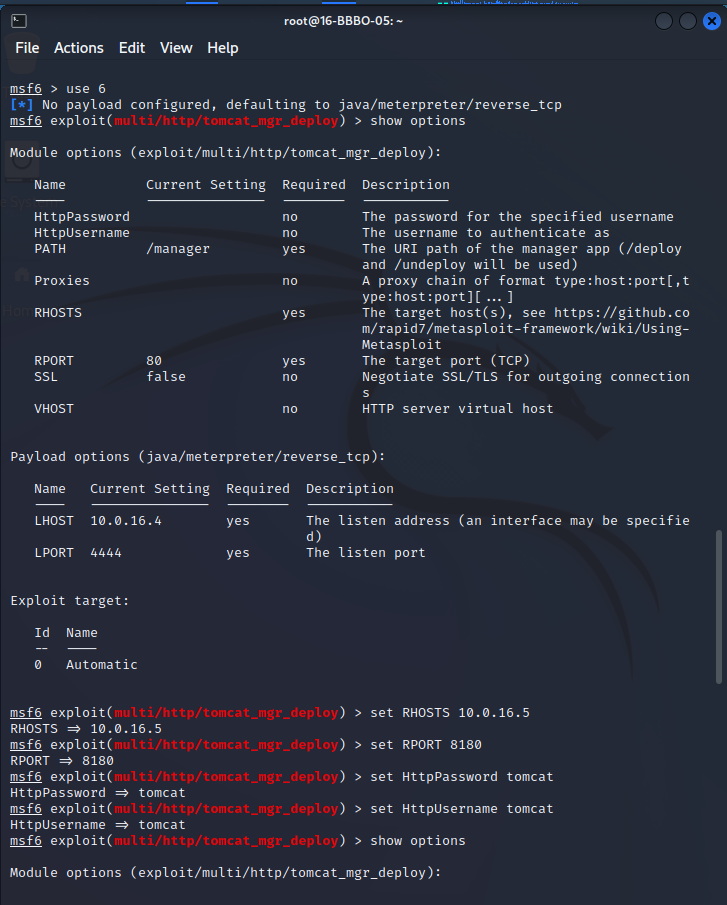


3) Подключитесь к атакуемой машине используя tomcat\_mgr\_deploy, опишите переменные, которые будете изменять.

Подключение к атакаемой машине с испоьзованием **tomcat\_mgr\_deploy**







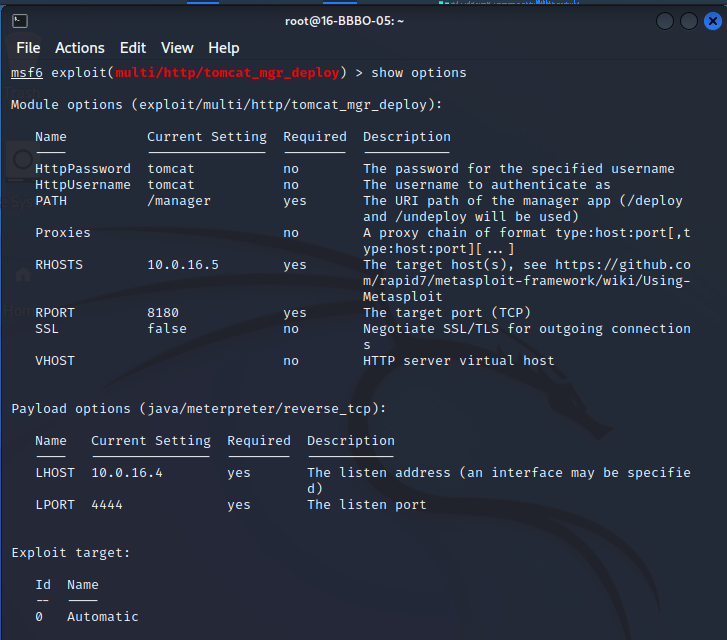
Были изменены параметры:

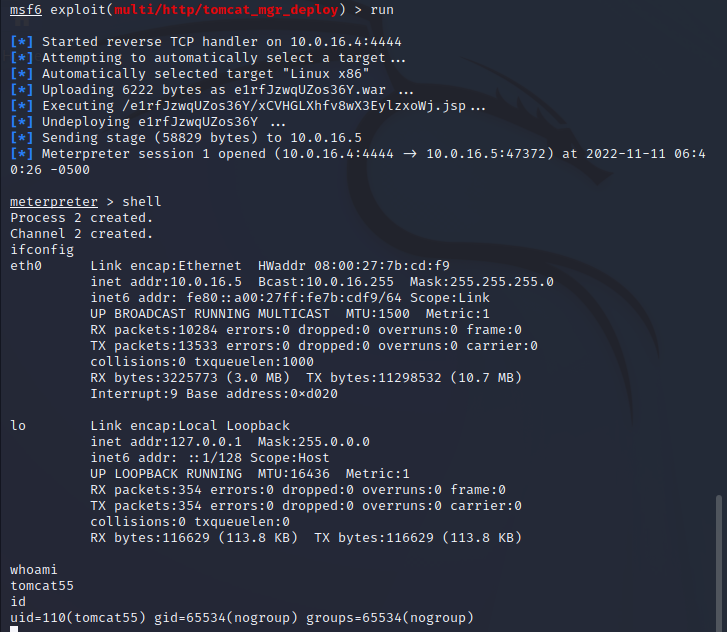
RHOST – 10.0.16.5 – хост атакуемой машины

RPORT – 8180 – порт, используемый веб-сервером Apache Tomcat

HttpPassword – tomcat – пароль для входа на сервер

HttpUsername – tomcat – имя пользователя для входа на сервер





4) Какая команда meterpreter используется для повышения прав в windows? – getsystem

**Вывод:** Я закрепил знания полученные после выполнения четвертой практической работы такие как: nmap в Kali Linux. Я научился работать с файловой системой Linux, создавать файлы и директории, а также архивировать их. Изучил взлом SSH и WEB сервиса.