|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение высшего образования **«МИРЭА − Российский технологический университет»**  **РТУ МИРЭА** |

**Институт кибербезопасности и цифровых технологий**

**Кафедра КБ-2 «Информационно-аналитические системы кибербезопасности»**

**ОТЧЁТ ПО ПРАКТИЧЕСКОМУ ЗАНЯТИЮ №4**

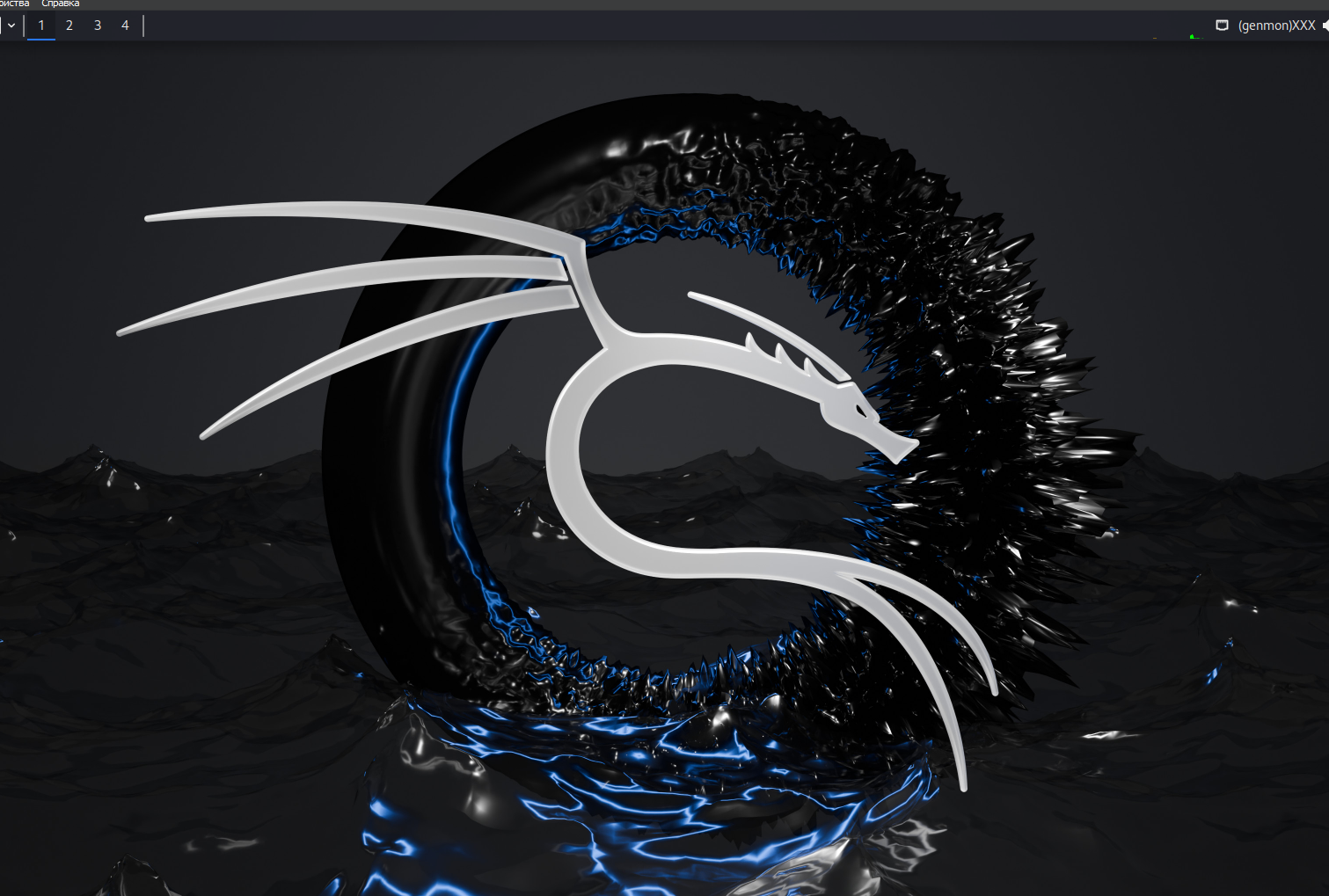
**по дисциплине «Безопасность операционных систем»**

|  |  |  |  |
| --- | --- | --- | --- |
| Отчет представлен к  рассмотрению:  Студент группы БББО-07-22 | «2» апреля 2024 г. | (подпись) | Сокол Д.М. |
|  |  |  |  |
| Преподаватель | «2» апреля 2024 г. | (подпись) | Абрамов Д.П. |

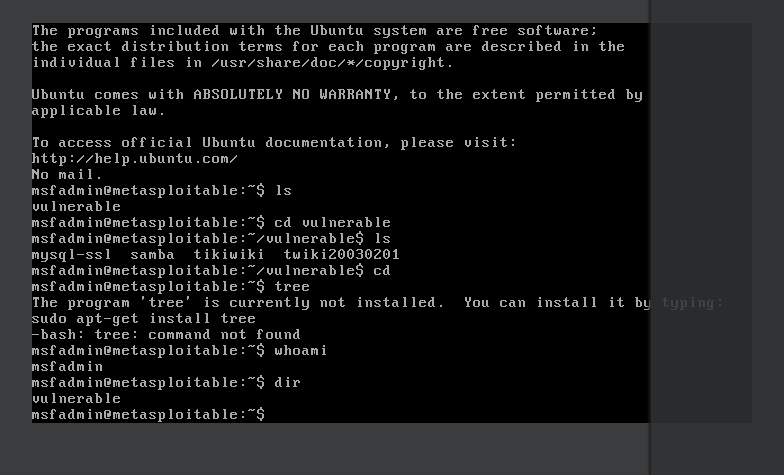
Москва, 2024 г.

1.1.Подготовка учебного стенда

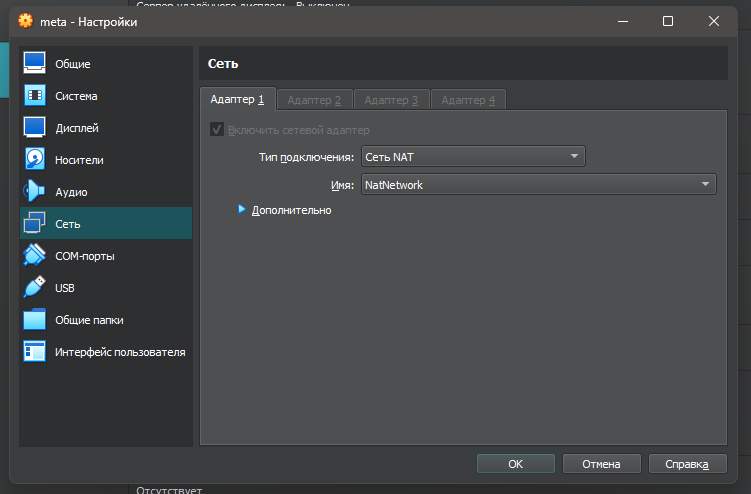
1. Установка Kali Linux

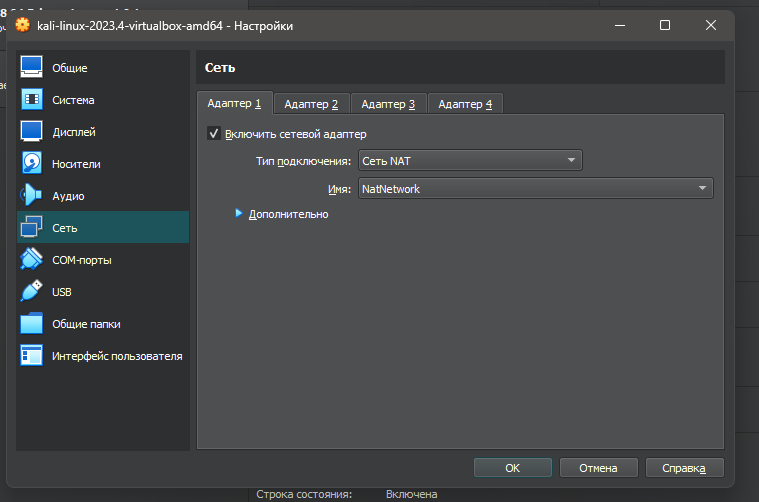


2. Установка Metasploitable 2

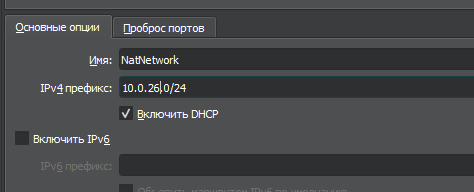


3. Настройка и проверка сетевого взаимодействия

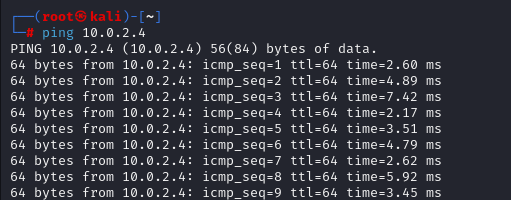




Сеть по порядковому номеру в группе:

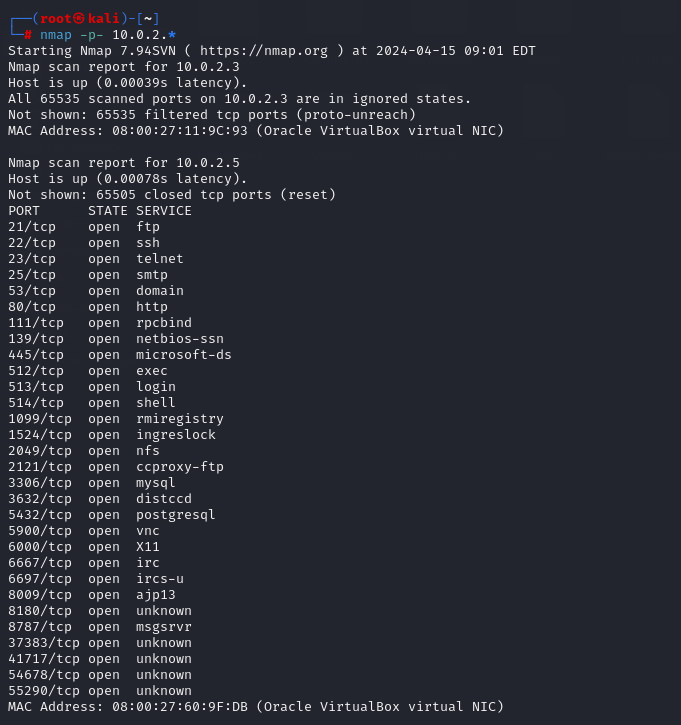


Задание: На ВМ Kali Linux выполните команду ping {ip-адрес ВМ metasploitable 2}

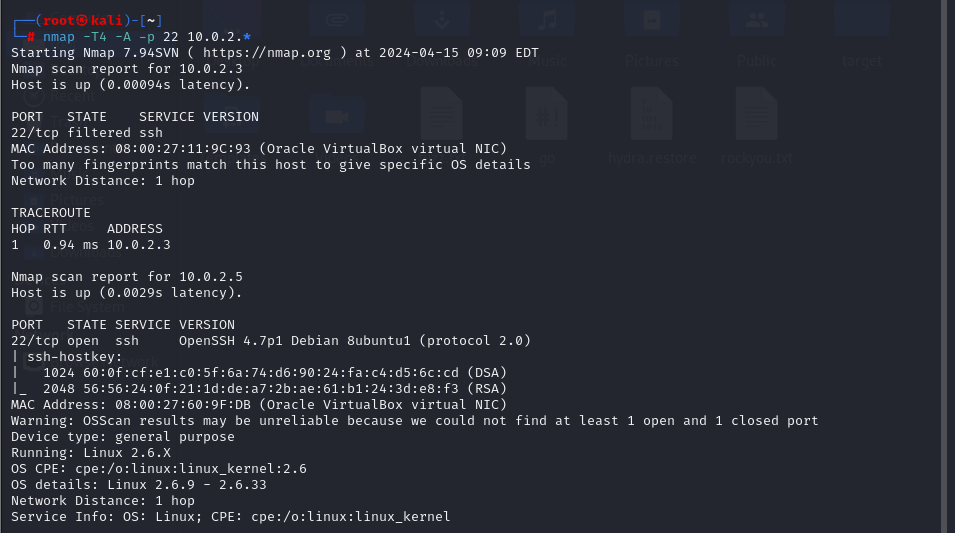


ГЛАВА 2. ТЕСТИРОВАНИЕ СЕРВИСОВ

2.2. Тестирование сервиса SSH

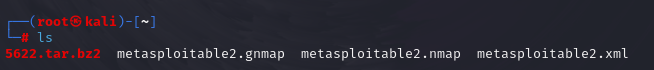


Список открытых портов на metasploitable2

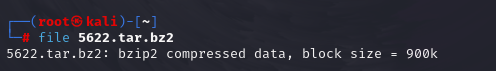


Более углубленное сканирование порта 22

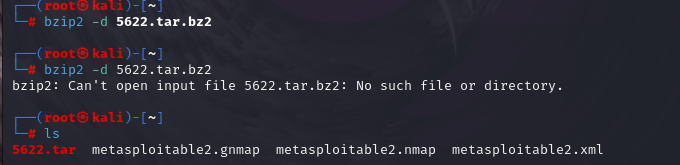
Скачиваю файл, который просят загрузить



file 5622.tar.bz2



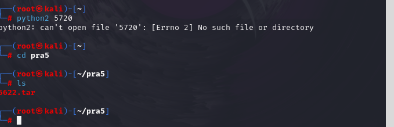
bzip2 -d 5622.tar.bz2



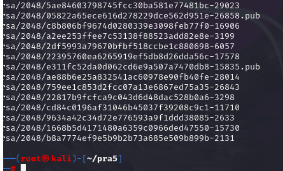
Описание уязвимости(CVE-2008-0166) и решения по ликвидации уязвимости:  
OpenSSL 0.9.8c-1 до версий до 0.9.8g-9 в операционных системах на базе Debian использует генератор случайных чисел, который генерирует предсказуемые числа, что упрощает удаленным злоумышленникам проведение атак методом перебора криптографических ключей.  
Решения по ликвидации:  
1. Обновление до последней версии  
2. Установка дополнительных источников случайности  
3. Конфигурация генератора случайных чисел:  сконфигурируйте генератор случайных чисел в OpenSSH и OpenSSL, чтобы использовать наиболее надежные и безопасные методы генерации случайных чисел.

Описание основных ключей команды wget:  
1. -r загрузить файлы рекурсивно, включая все поддиректории.  
2. -P указать директорию, в которую следует сохранить загруженные файлы.  
3. -O сохранить файл с определенным именем.  
4. –np  не переходить на родительский каталог при загрузке.  
5. -c возобновить загрузку файла, если она была прервана.  
6. - работать в тихом режиме, без вывода лишних сообщений.

1. Перемещаю файлы в новую директорию lab5

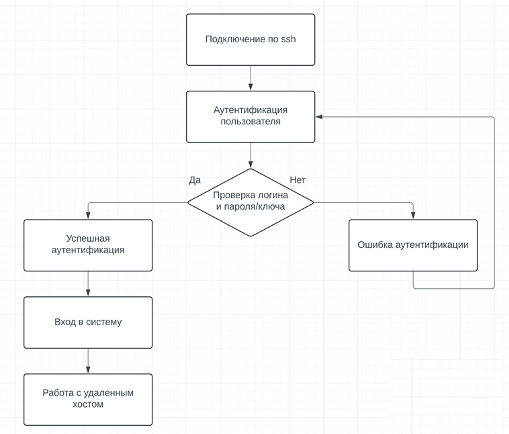


1. Не удалось подобрать.



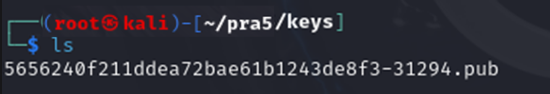
**Задание 1**

Схема работы open-ssh

****

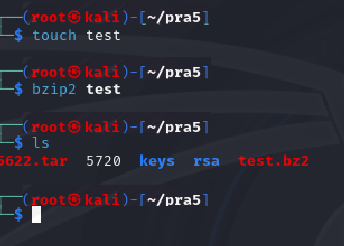
**Задание 2**

Перетащил ключ в папку keys



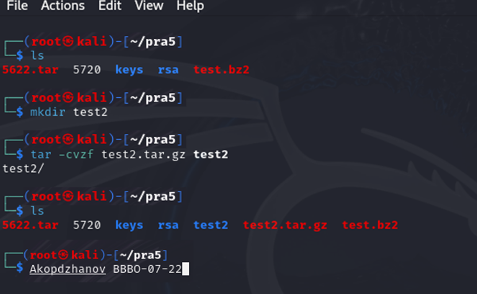
**Задание 3**

Создал файл test и заархивировал его при помощи bzip2

****

**Задание 4**

Создал папку test2 и заархивировал ее при помощи gzip



Описание ключей:

-c Создать новый архив.

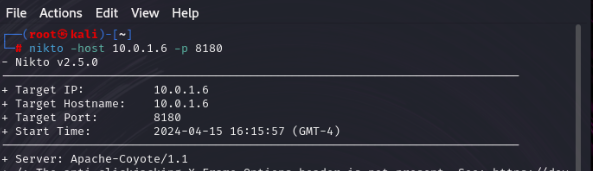
-v Вывод о процессе архивации.

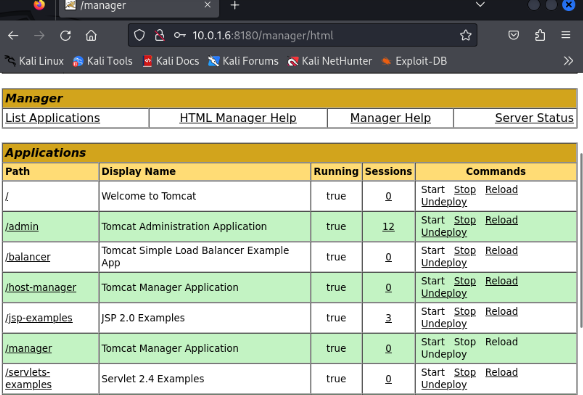
-z Архивировать файлы с помощью gzip.

-f  Указать имя для архива.

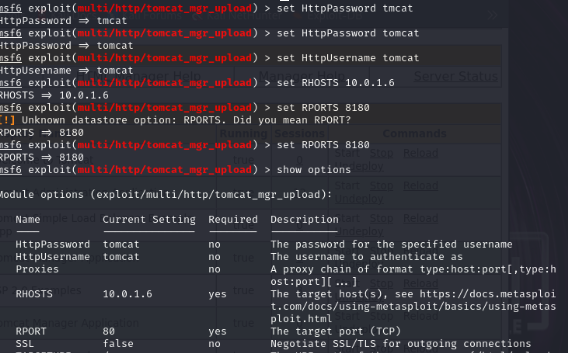
**2.3 Тестирование WEB сервиса**

1. nikto -host 10.0.1.6 -p 8180





Установка опций



HttpPassword - Пароль, используемый для аутентификации при доступе к HTTP-ресурсу.

HttpUsername - имя пользователя, используемое для аутентификации при доступе к HTTP-ресурсу.

RHOSTS - IP-адрес удаленного хоста, с которым взаимодействует приложение или инструмент.

RPORT - Порт, на котором работает целевое приложение или сервис на удаленном хосте.ne

**Задание 2**

getsystem

**Задание 3**

**80 - apache2**

**443 - порт закрыт.**

**Задание 4**

-h Определяет целевой хост (веб-сервер), который будет сканироваться.

-p Определяет порт, на котором работает веб-сервер. По умолчанию 80.

-ssl Включает сканирование по защищенному протоколу HTTPS на порту 443.