|  |
| --- |
| 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**

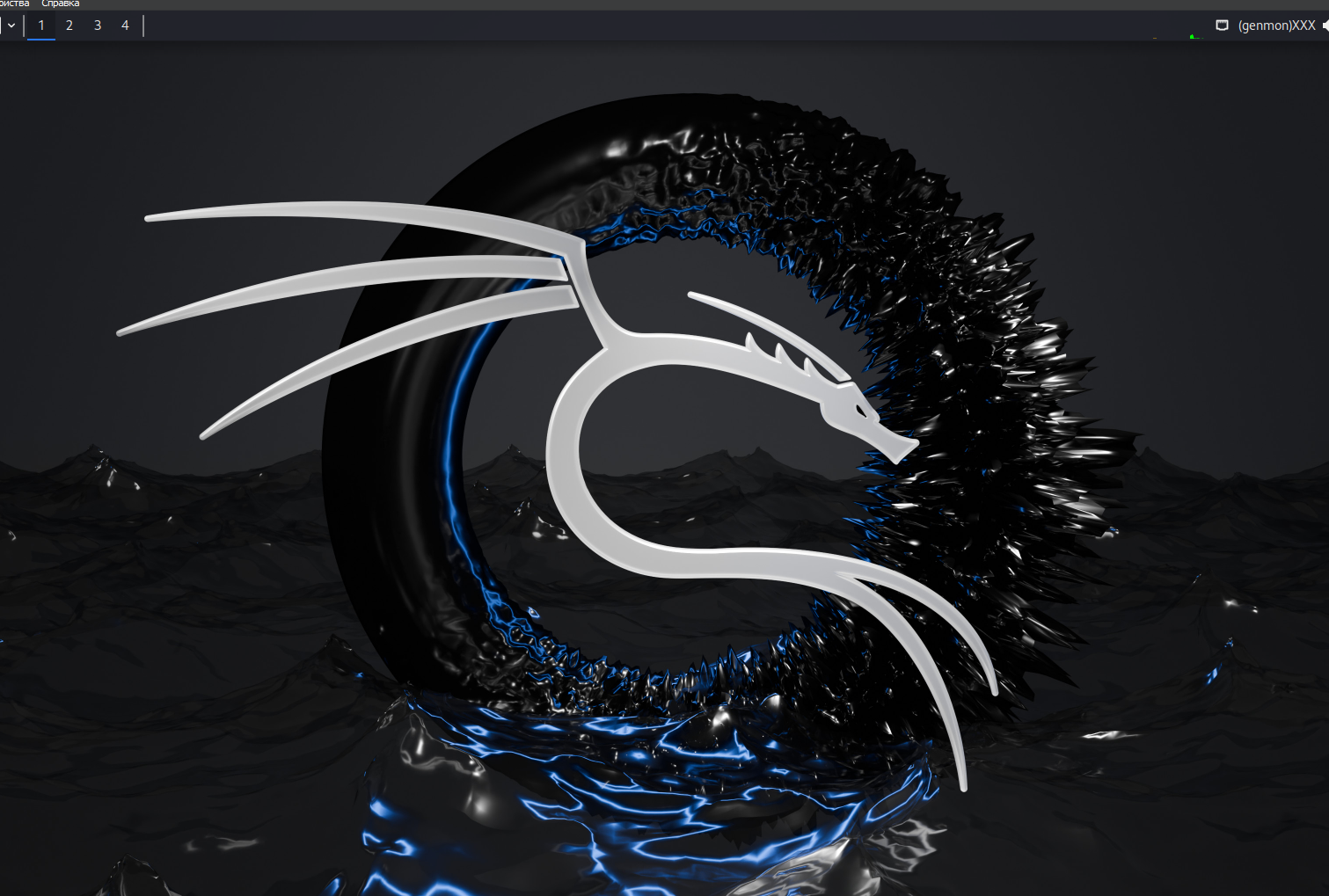
**по дисциплине «Безопасность операционных систем»**

|  |  |  |  |
| --- | --- | --- | --- |
| 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. |

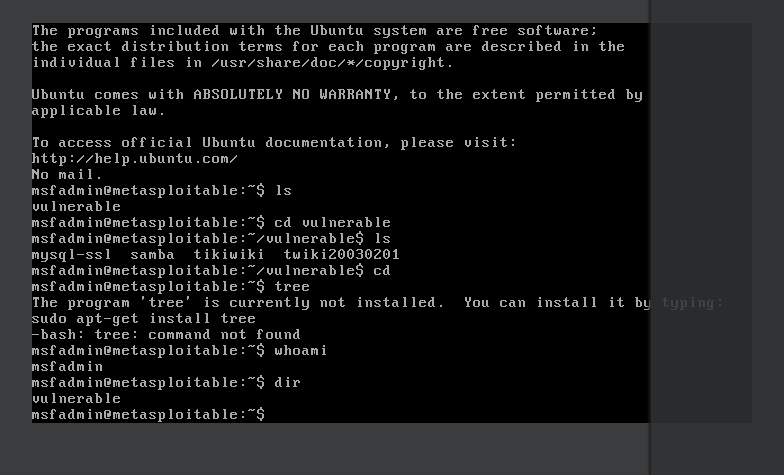
Москва, 2024 г.

1.1.Подготовка учебного стенда

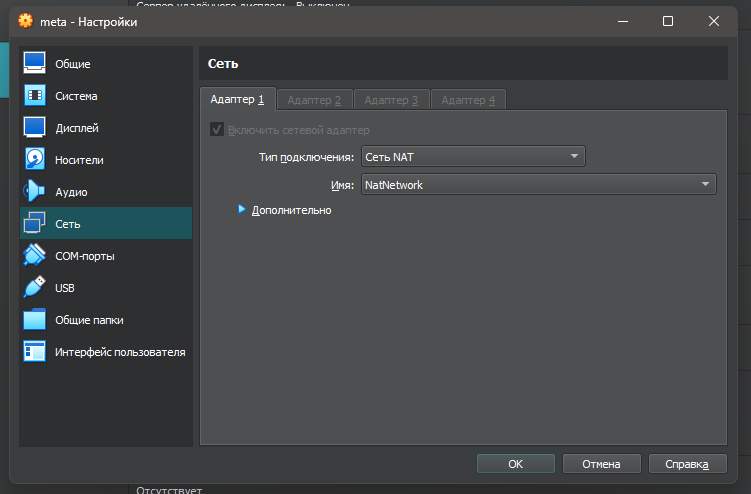
1. Установка Kali Linux

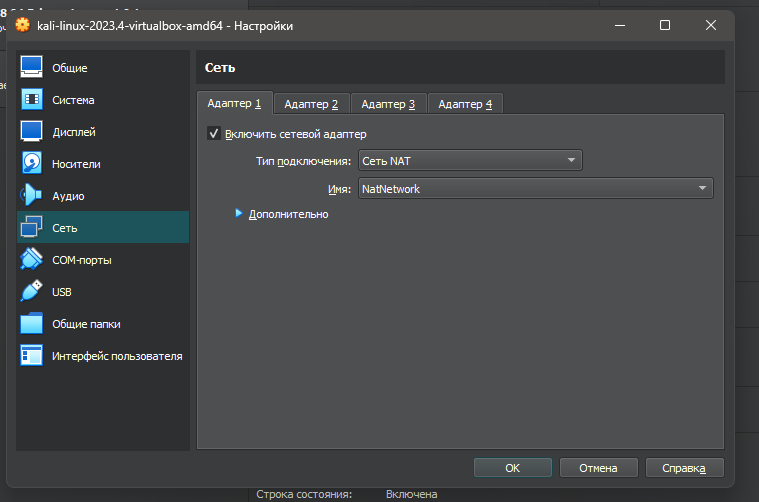


2. Установка Metasploitable 2

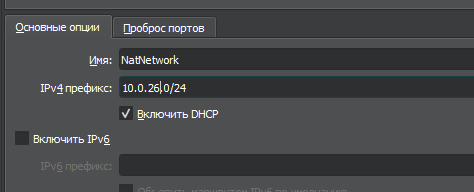


3. Настройка и проверка сетевого взаимодействия

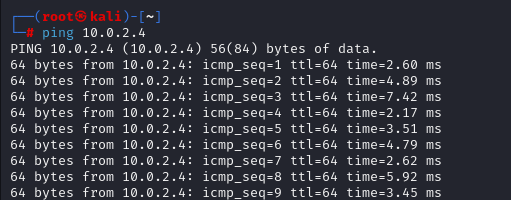




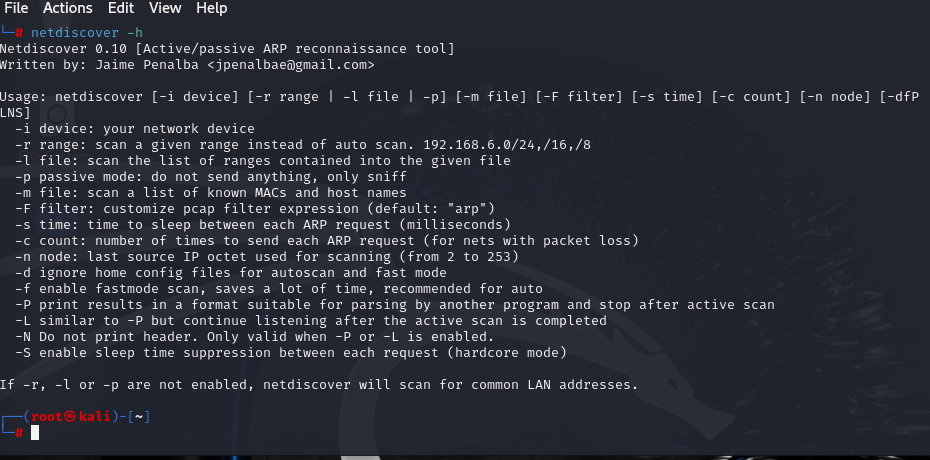
Сеть по порядковому номеру в группе:



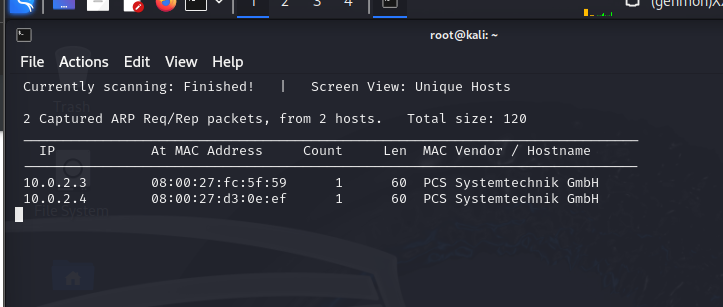
Задание: На ВМ Kali Linux выполните команду ping {ip-адрес ВМ metasploitable 2}



1.2.Настройка цели



Результат выполнения команды



Сканирование сети

●Перечень известных систем виртуализации, их отличительные

особенности:

VirtualBox - бесплатная система виртуализации, подходит для

домашнего использования.

VMware - у компании огромное количество продуктов и разными

фичами.

Docker - платформа для доставки и запуска приложений в

контейнерах.

●Краткое описание установленных ОС с описанием их назначения.

Полный перечень использованных команд с кратким описанием их

назначения:

Kali Linux: Kali Linux — операционная система для тестирования на

проникновение.

Metasploitable2 — уязвимая виртуальная машина, предназначенная

для обучения тестированию на проникновение.

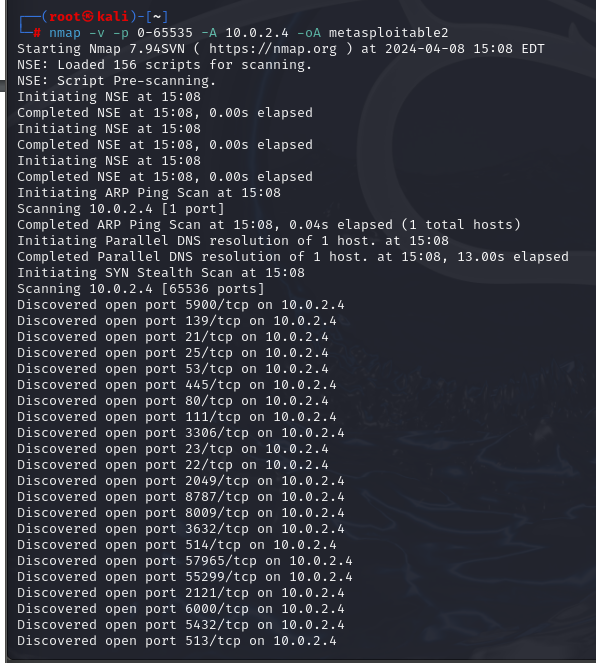
●Основные ключи и их описание.

netdiscover: Инструмент для обнаружения активных устройств в

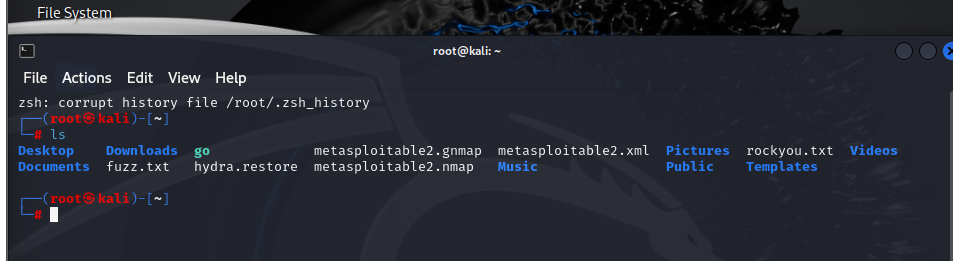
сети. Основной ключ: -r: Позволяет указать диапазон IP-адресов для

сканирования.

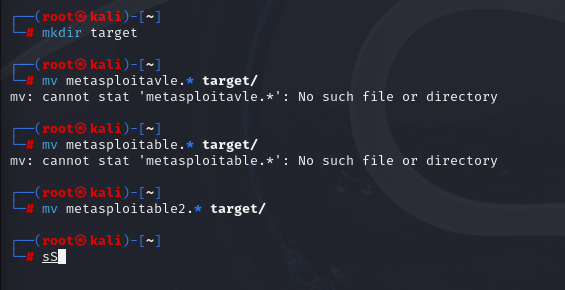
1.3.Сканирование портов



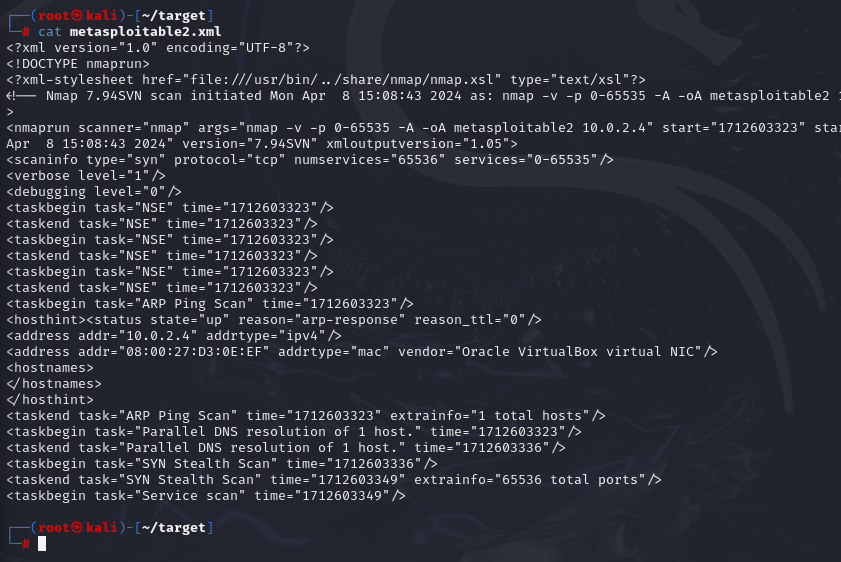
Результат сканирования портов



Отчеты о сканировании



Результаты перемещения



Просмотр отчета о сканировании

Полный перечень использованных команд с кратким описанием их

назначения. Основные ключи и их описание:

nmap

Основные ключи:

-v, -vv, -vvv: Устанавливают уровень подробности вывода.

-p: Указывает диапазон портов для сканирования.

-A: Выполняет детальное сканирование и отображает версии сервисов.

-oA: Определяет формат вывода отчета.

-T: Устанавливает скорость сканирования (от 1 до 5, где 1 - это очень

медленное сканирование.).

Примеры выполнения команд, которые были использованы в ходе

работы с описанием их результатов.

nmap -v -p 0-65535 -A 10.0.2.5 -oA metasploitable2

Перечень открытых портов, названия и версии сервисов, которые их

используют.

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:

WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup:

WORKGROUP)

512/tcp open exec netkit-rsh rexecd

513/tcp open login?

514/tcp open shell Netkit rshd

1099/tcp open java-rmi GNU Classpath grmiregistry

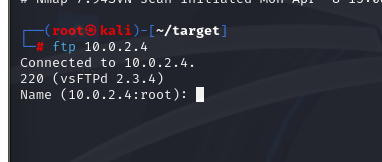
1524/tcp open bindshell Metasploitable root shell

2049/tcp open nfs 2-4 (RPC #100003)

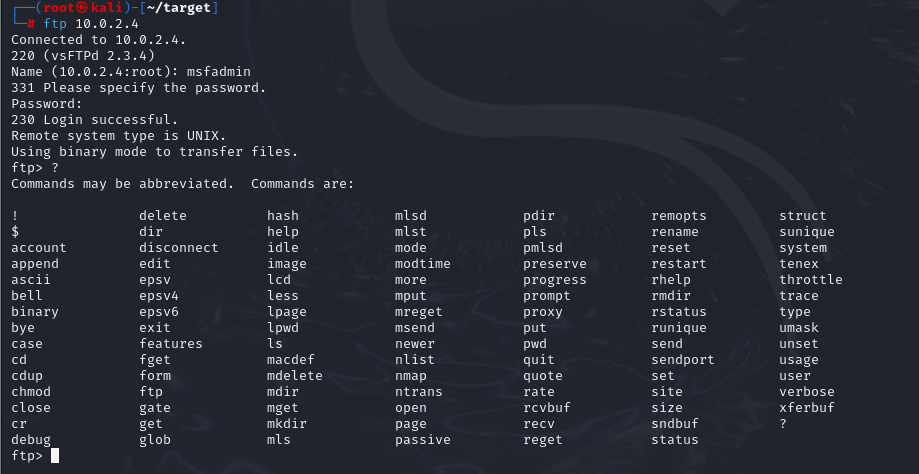
2121/tcp open ftp ProFTPD 1.3.1

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

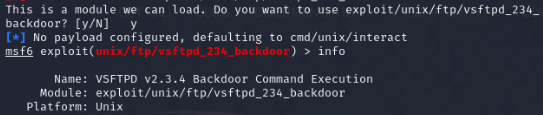
2.1.Тестирование сервиса FTP



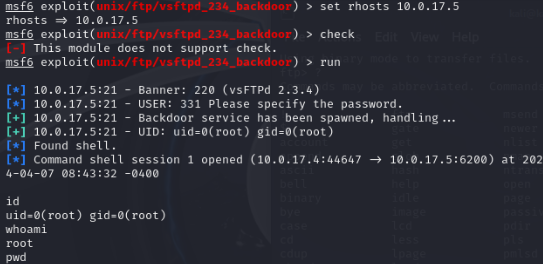
Подключение к сервису ftp



Отображение доступных команд



Использование эксплойта



Выход из метасплойт

**Полный перечень использованных команд с кратким описанием их**

назначения. Основные ключи и их описание:

ftp {ip-адрес цели} - подключение к FTP-серверу по указанному IP-адресу.

? - отображение списка доступных команд в FTP-сессии.

ls - просмотр содержимого текущей директории на FTP-сервере.

exit - завершение сессии FTP.

msfconsole - вход в Metasploit

info - отображение информации о выбранном модуле в Metasploit.

check - проверка наличия уязвимости, соответствующей выбранному

модулю в Metasploit.

run - запуск эксплойта в Metasploit.

id - отображение текущего пользователя в системе.

pwd - отображение текущей рабочей директории.

exit - завершение сессии Metasploit.

**Примеры выполнения команд, которые были использованы в ходе работы с описанием их результатов.**

**Описание модулей metasploit.**

Metasploit - фреймворк для тестирования на проникновение, включающий

в себя множество модулей для проведения атак и эксплуатации

уязвимостей. Модули Metasploit предоставляют возможность

автоматизировать процессы тестирования безопасности, включая поиск

уязвимостей, эксплуатацию, обход защиты и многое другое.

**Перечень и описание основных команд FTP сервиса.**

PWD - отображение текущей рабочей директории.

CWD - смена текущей рабочей директории.

LS - отображение содержимого директории.

RETR - загрузка файла с FTP-сервера на клиент.

STOR - загрузка файла с клиента на FTP-сервер.

EXIT - завершение сеанса FTP.