|  |
| --- |
| 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 №6**

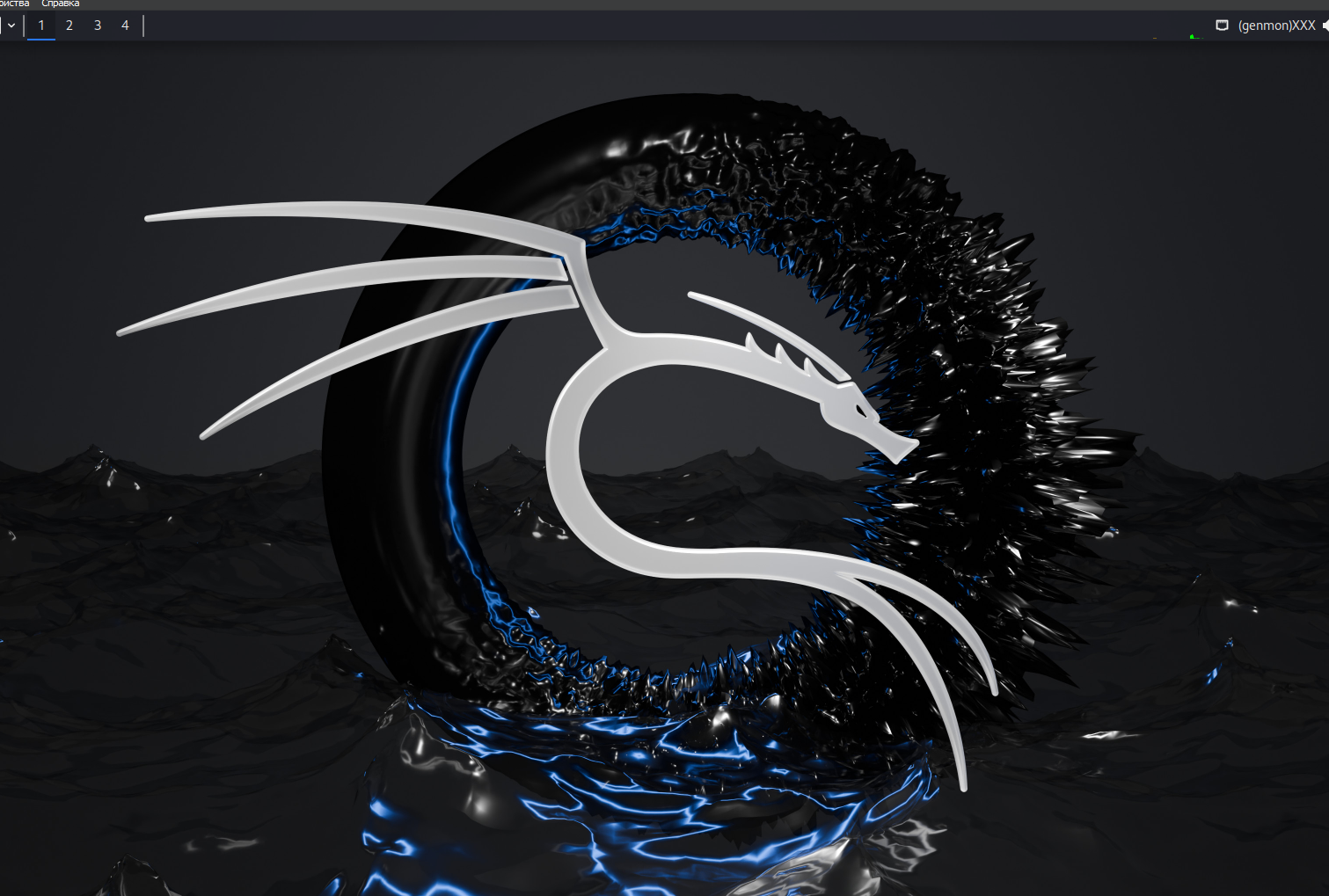
**по дисциплине «Безопасность операционных систем»**

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

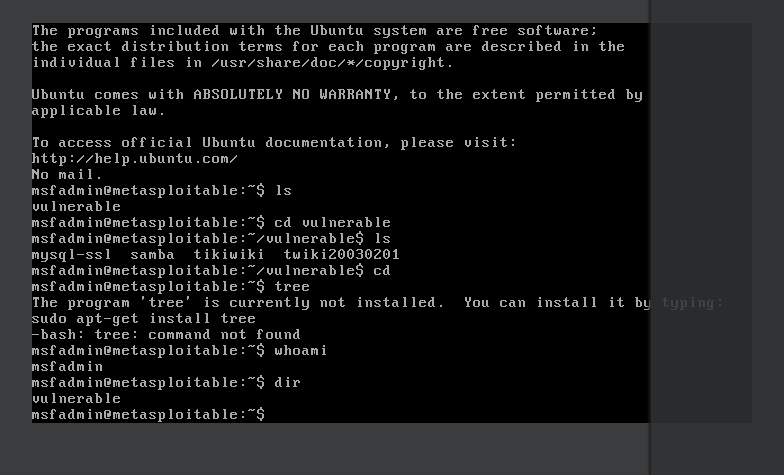
Москва, 2024 г.

1.1.Подготовка учебного стенда

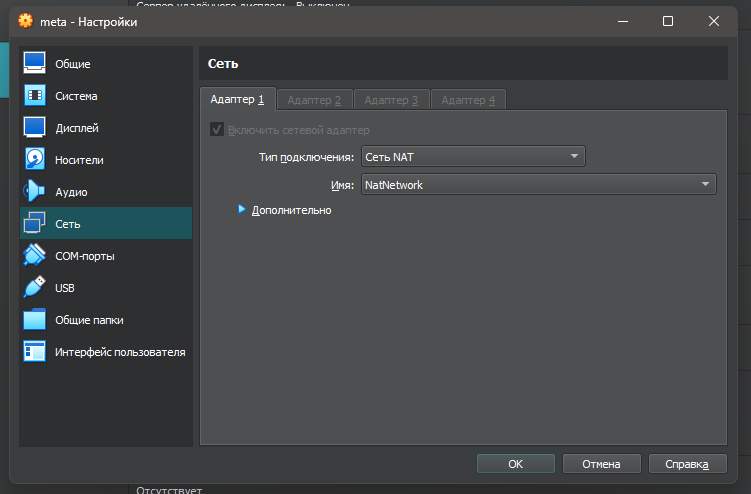
1. Установка Kali Linux

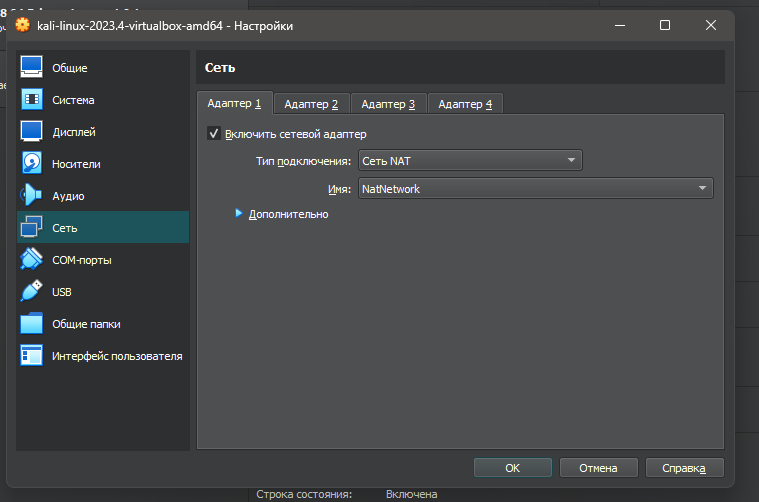


2. Установка Metasploitable 2

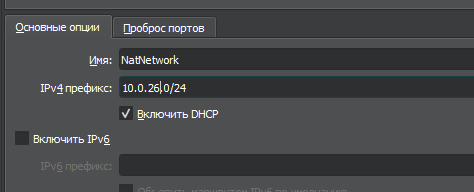


3. Настройка и проверка сетевого взаимодействия

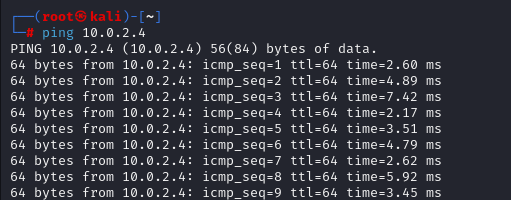




Сеть по порядковому номеру в группе:

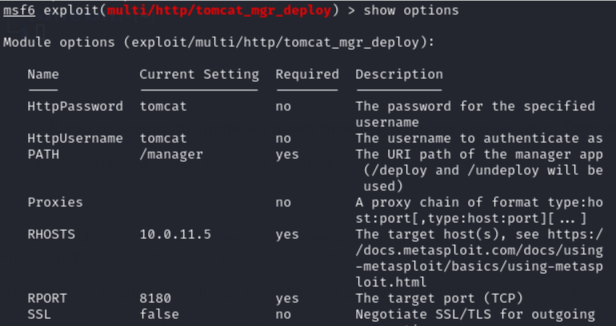


Задание: На ВМ Kali Linux выполните команду ping {ip-адрес ВМ metasploitable 2}

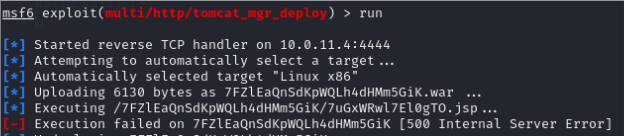


**ГЛАВА 3. ПАРОЛИ**

**3.3. Повышение прав**

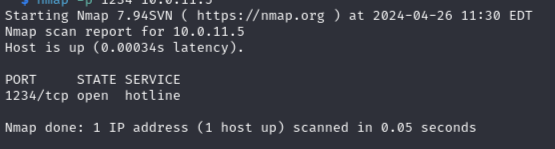


Запуск эксплойта и его неработоспособность



unix-privesc-check - это инструмент для проверки привилегий в Unix-системах, который анализирует текущие привилегии пользователя и определяет возможные уязвимости, которые могут быть использованы для повышения привилегий. Перспективными уязвимостями являются:  
1. Недостаточные настройки системы безопасности. Это может включать наличие слабых паролей, неправильно настроенные ACL (Access Control Lists), отсутствие контроля доступа к важным файлам или службам.  
2. Наличие проблем с правами доступа к критическим файлам и службам. Например, если пользователь имеет доступ к execute команде от имени пользователя с правами администратора, это также может быть использовано для получения повышения привилегий.1. Наличие необходимости повышения привилегий (SUID/SGID файлы и исполняемые). Если у объекта есть права SUID (Set User ID) или SGID (Set Group ID), то это может предоставить доступ к привилегированным действиям, которые могут быть использованы злоумышленником для повышения привилегий.  
3. Наличие локальных уязвимостей в ядрах или установленных программных компонентах системы. Уязвимости в системных компонентах или службах могут быть использованы для выполнения атаки на повышение привилегий.  
**ГЛАВА 4. BIND И REVERSE SHELL В ДЕЙСТВИИ**

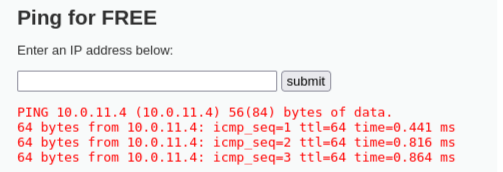
**4.1. Базовые веб-шеллы**



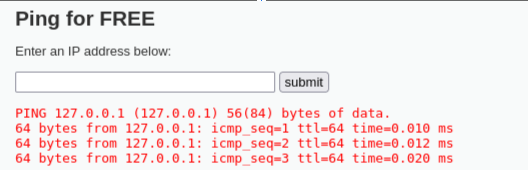
**Результат bind shell**

****

**Создение бекдора в метасплоит**

****

**Результат пинга**

****

**Результат загрузки файлов**

**Что такое bind shell?**это тип shell-а, который прослушивает определенный порт на хосте и ждет подключения от клиента. Когда клиент подключается, они имеют доступ к командной оболочке хоста. **Что такое reverse shell?**это тип shell-а, который устанавливается на цель и подключается к удаленному хосту. Это позволяет удаленному атакующему получить доступ к командной оболочке цели. **Как расшифровывается DVWA?**Damn Vulnerable Web Application. **Мы вручную запускали сервис Apache2. С помощью какой команды можно поставить его в автозагрузку?**update-rc.d apache2 defaults **Как использовать netcat для получения shell цели?**Для использования netcat для получения shell цели, необходимо сначала установить netcat на своем хосте и на цели, затем открыть порт на цели, после чего можно установить соединение с использованием команды:  
nc <цель> <порт>