

ФГБОУ ВО «Московский технологический университет»

Институт комплексной безопасности и специального приборостроения

Кафедра КБ-1 «Защита информации»

**Дисциплина:** «Безопасность операционных систем»

**Отчет по практической работе №7**

**Тема:** «Основы Kali Linux ч.4»

**Выполнил:**

Студент группы БББО-05-20

Кутьин З.С.

**Проверил:**

Абрамов Д.П.

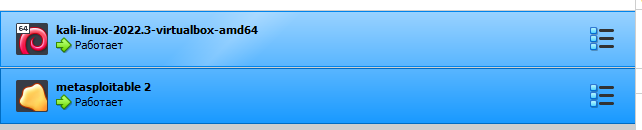
**Цель работы**

Продолжить изучение инструментов Kali linux nmap, metasploit. Утилита для тестирования веб сервисов nikto.

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

**Порядок выполнения работы**

1. **Установить Kali linux, metasploitable 2**

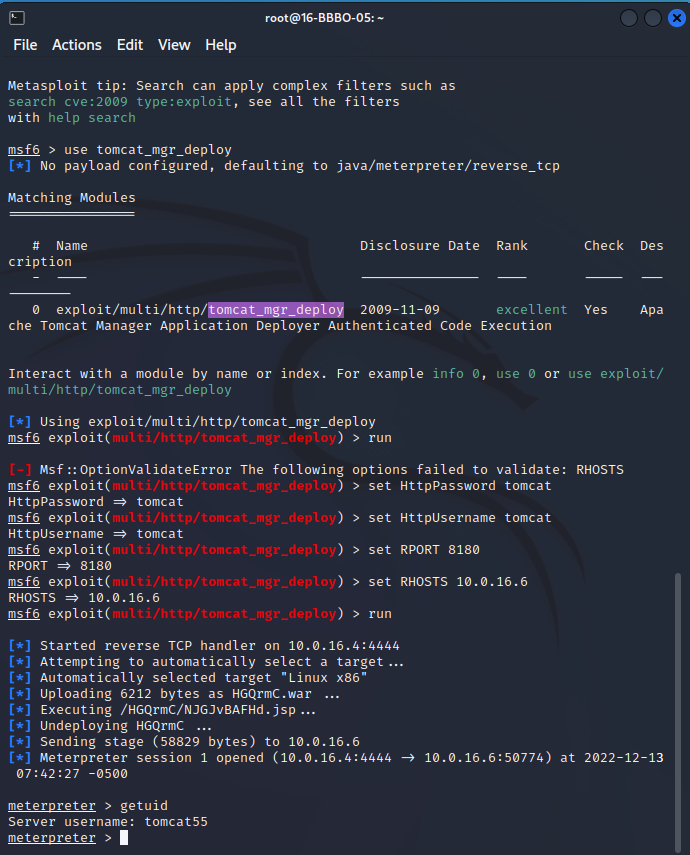


1. **Повышение прав**

Настрока опций эксплойта tomcat\_mgr\_deploy:

* HttpPassword = tomcat
* HttpUsername = tomcat
* RPORT = 8180
* RHOSTS = 10.0.16.6

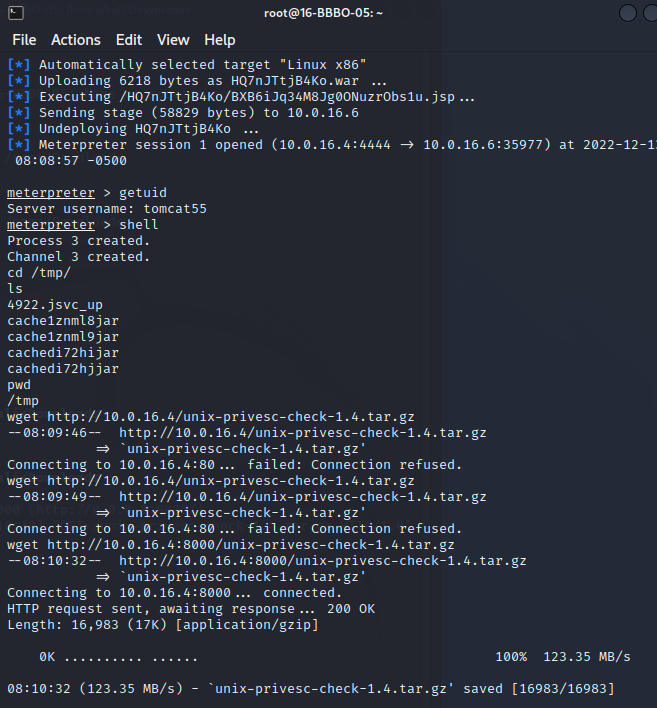
А так же проверка под каким пользователем мы авторизовались.



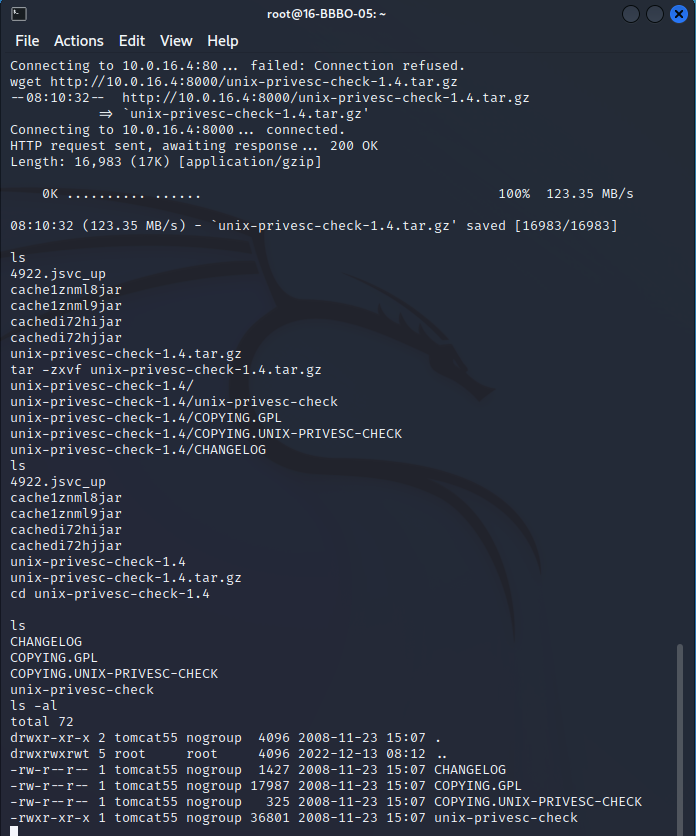
Скачал и установил скрипт, запустил веб-сервер



Зашёл в линукс-шелл и запустил скачанный ранее скрипт



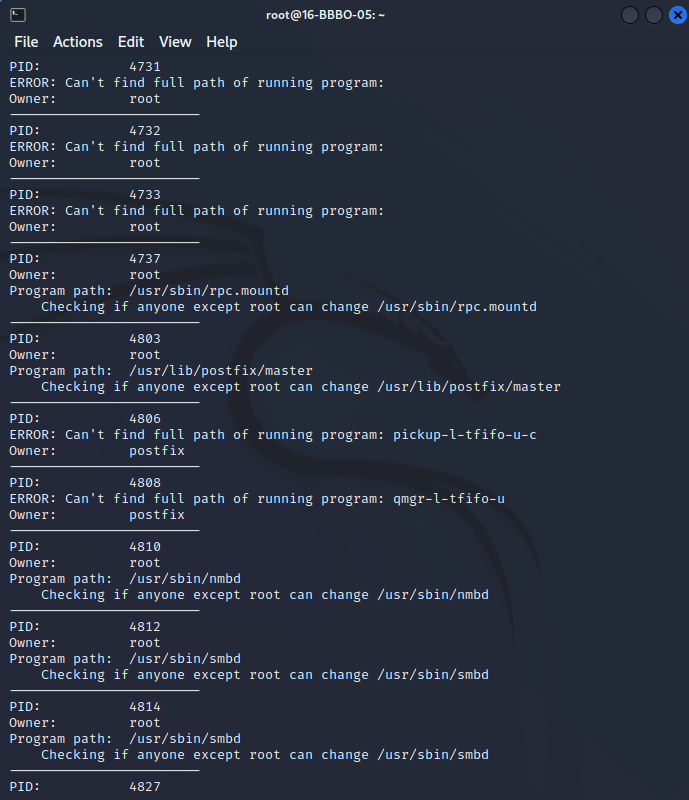
Убеждаемся, что файл скачался. Распаковываем его. Просматриваем права файлов.



Запускаю скрипт



Повторно запускаю скрипт, с добавлением режима standard



**Перспективные уязвимости:**

* Домашние директории с правом записи

В домашний каталог можно положить ssh-ключи или добавить файл rhosts и сразу войти в систему.

* Читаемые файлы в домашних каталогах

Как и в первом пункте, это является риском, т.к. в домашних каталогах могут лежать пароли, списки доступа и т.д. Это может дать доступ к локальным приложениям или другим учетным записям.

* Читаемый /etc/shadow

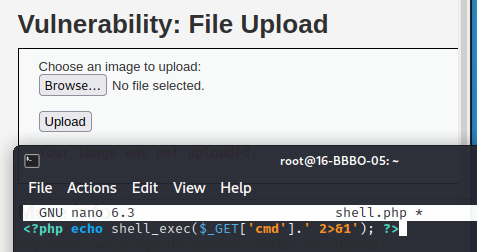
Позволит прочитать хэши паролей, которые затем можно будет декодировать и войти под другими учетками.

1. **Разбираемся с базовыми веб-шеллами**

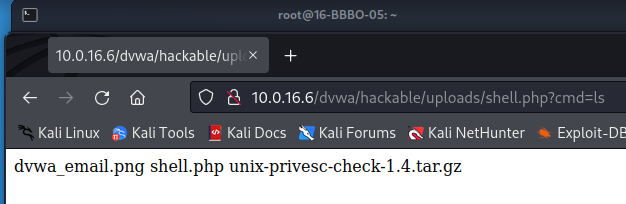
Получаем веб сервер с 80-го порта командой get



Тестирую DVWA на уязвимость внедрения PHP скрипта в поле для отправки файлов. Создал файл со скриптом.

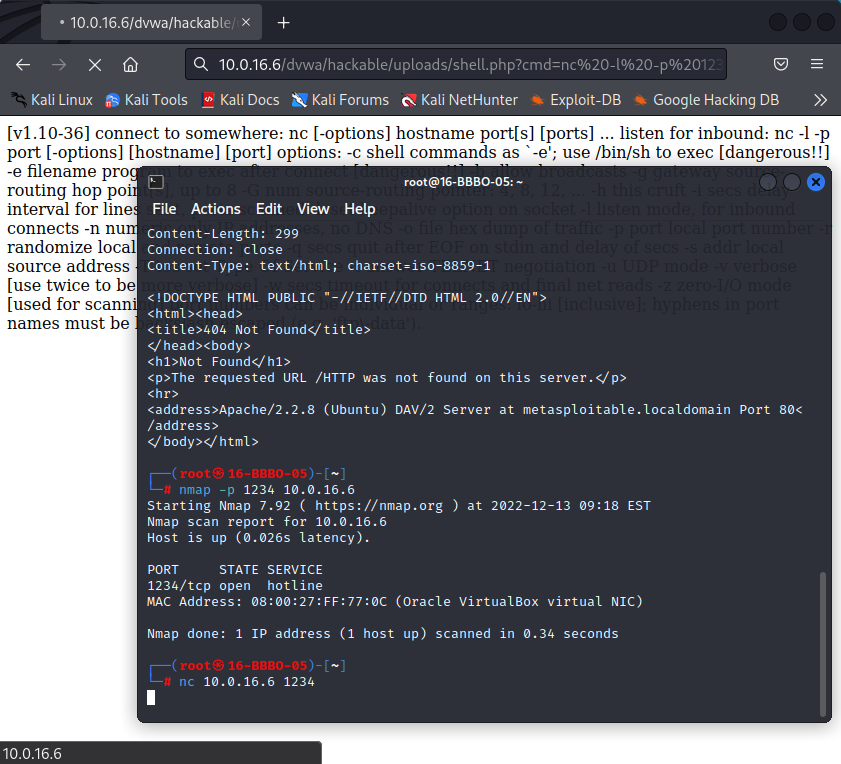


Загрузил файл со скриптом на сайт, пробую прописать команду. Видим вывод на странице сайта.

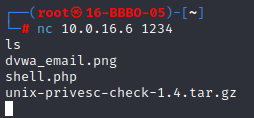


1. **Что такое Blind Shell**

Открыл порт 1234 на прослушивание, сканирую Ip с помощью nmap

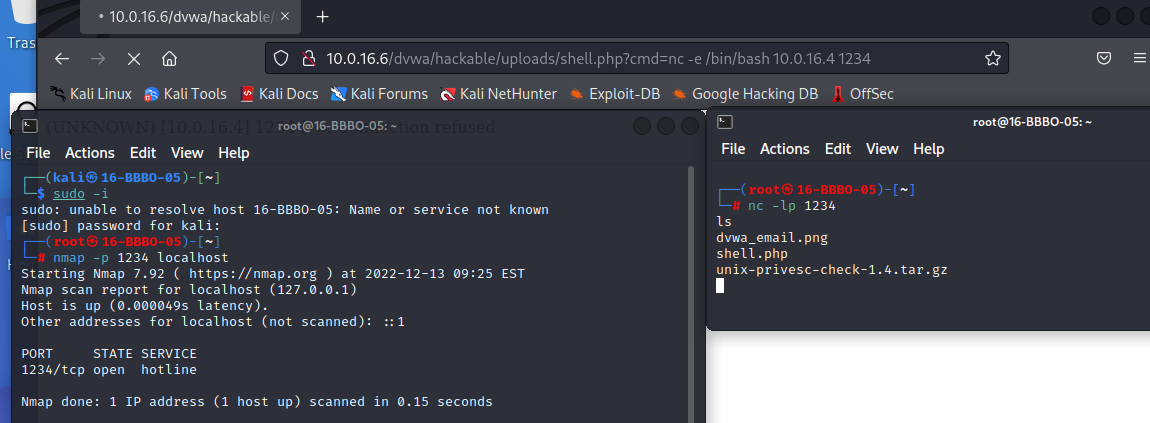


Прослушивание работает, получил вывод



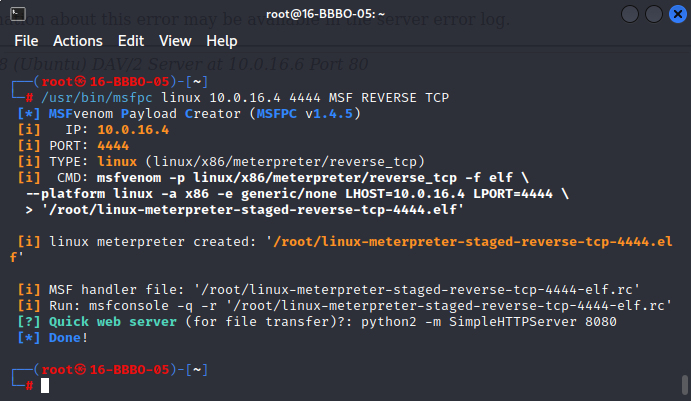
1. **Что такое Reverse Shell?**

Прослушиваем исходящее соединение от metasploitable машины, параллельно сканируя их nmap’ом. Порт 1234 открыт. Вывод ls.

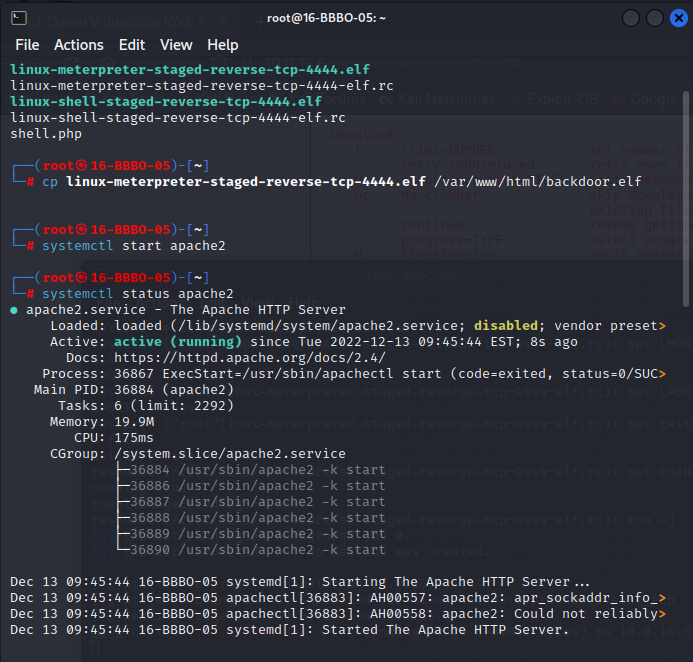


1. **Создаём бэкдор Metasploitable**

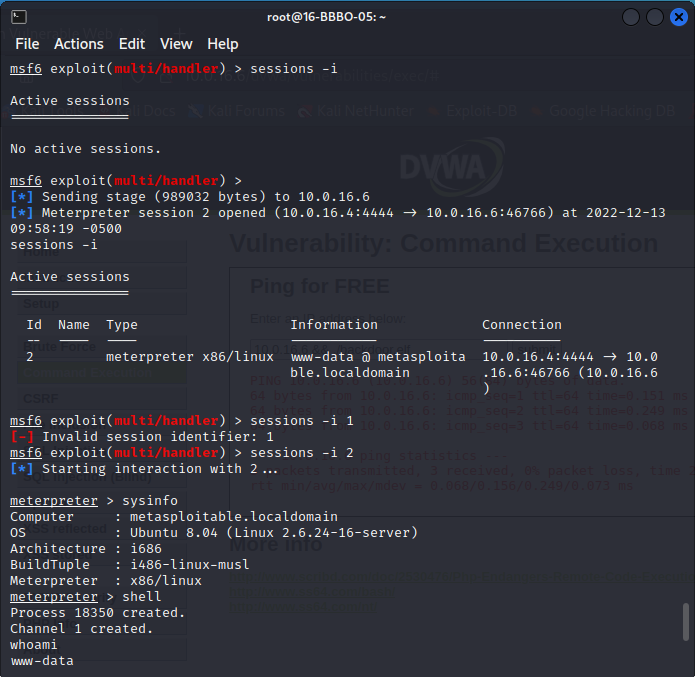
Создаю исполняемый файл, который позвонил использовать шелл meterpreter, воспользуясь скриптом msfpc. Запуск инструмента.



Запускаю сервер Apache2



Обнаруживаю открытую сессию и подключаюсь к ней. Теперь meterpreter позволяет взаимодействовать с Metasploitable2.



**Shell** – это программа, которая интерпретирует наши команды и отдает их операционной системе.

Она действует как интерфейс между пользователем и операционной системой.

Она принимает ввод с клавиатуры и отдает его ОС, а терминал позволяет вводить команды и взаимодействовать с оболочкой.

**1) Bind shell** – это своего рода настройка, при которой удаленные консоли устанавливаются с другими компьютерами по сети.

* В Bind shell злоумышленник запускает на целевом компьютере службу, к которой злоумышленник может подключиться.
* В bind shell злоумышленник может подключиться к целевому компьютеру и выполнять команды на нем.
* Чтобы запустить bind shell, злоумышленник должен иметь IP-адрес жертвы для доступа к целевому компьютеру.

**2) Reverse shell или connect-back** – это схема, при которой атакующий должен сначала запустить сервер на своей машине, а целевая машина должна выступить в роли клиента, который подключается к серверу, обслуживаемому атакующим.

* После успешного соединения злоумышленник может получить доступ к оболочке целевого компьютера.
* Для запуска Reverse shell злоумышленнику не нужно знать IP-адрес жертвы, чтобы получить доступ к целевому компьютеру.

**3) Damn Vulnerable Web Application (DVWA)** — это веб-приложение на PHP/MySQL, которое чертовски уязвимо. Его главная цель — помочь профессионалам по безопасности протестировать их навыки и инструменты в легальном окружении, помочь веб-разработчикам лучше понять процесс безопасности веб-приложений и помочь и студентам и учителям в изучении безопасности веб-приложений в контролируем окружении аудитории.

**4) sudo systemctl enable apache2** – команда для постановки apache2 в автозагрузку.

**5)** Использовать **bind** либо **reverse shell**. Конкретно netcat используется для создания шелла на удаленном устройстве, для подключения к нему, прослушивания портов и подключения к ним.

Например, ncat -l -e "/bin/bash" 1