|  |
| --- |
| 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**

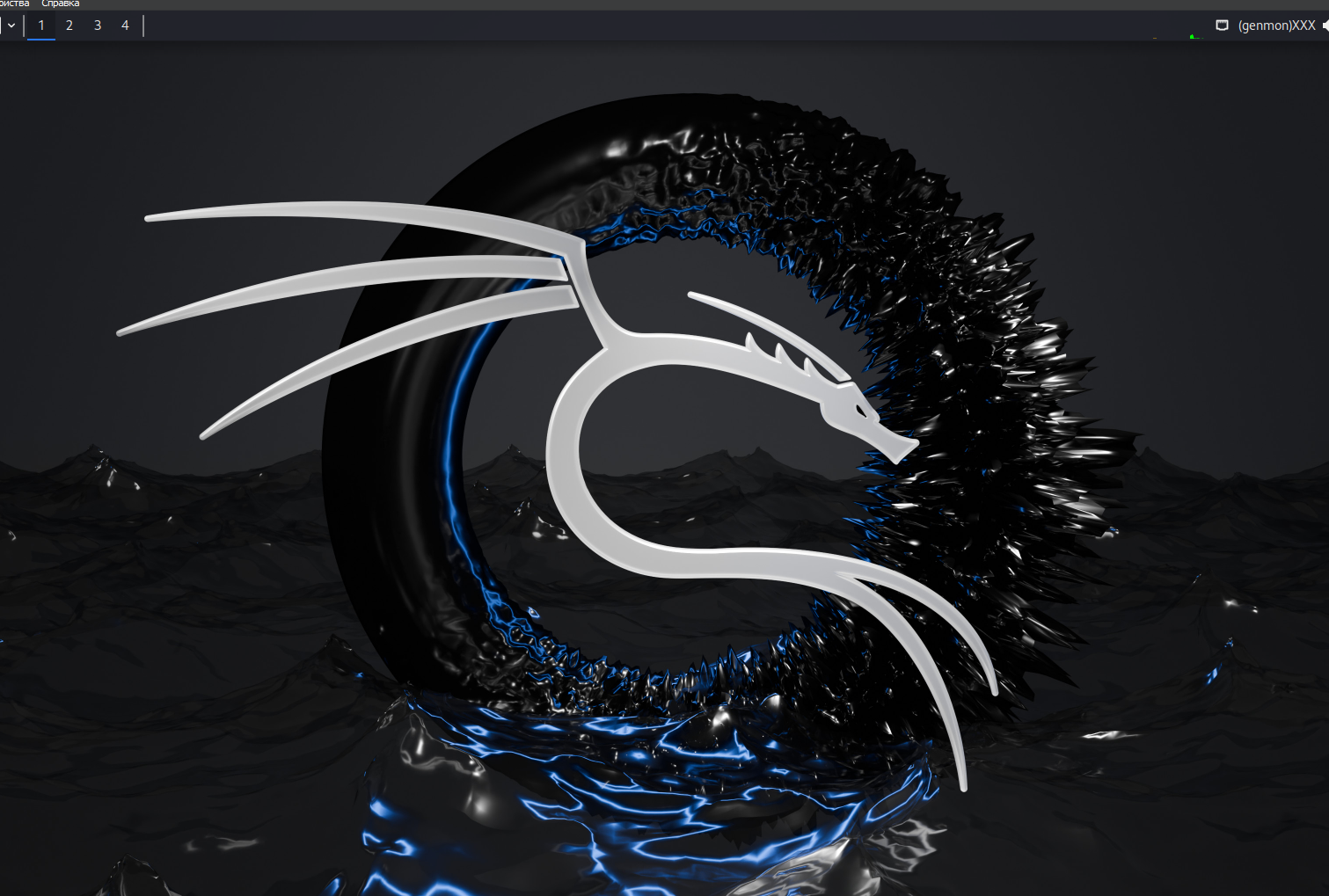
**по дисциплине «Безопасность операционных систем»**

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

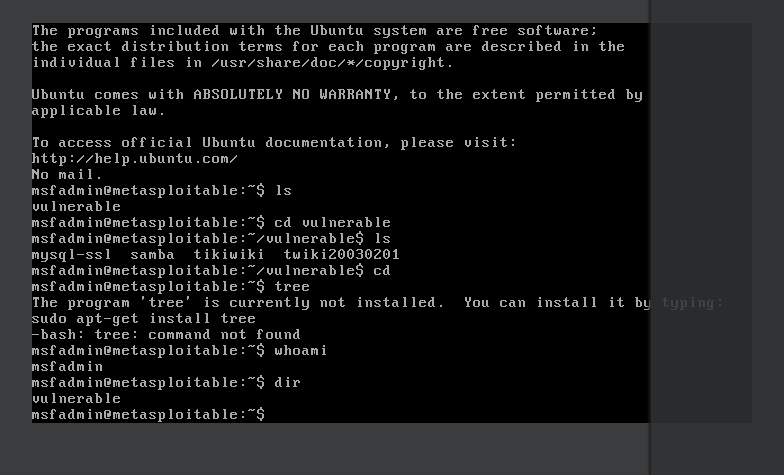
Москва, 2024 г.

1.1.Подготовка учебного стенда

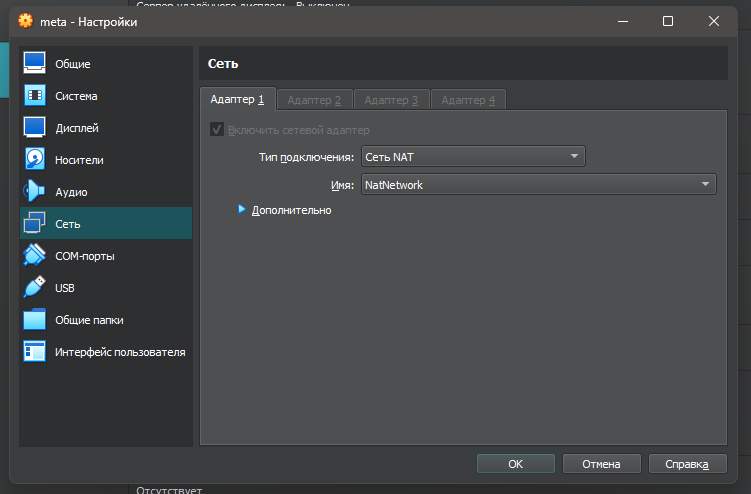
1. Установка Kali Linux

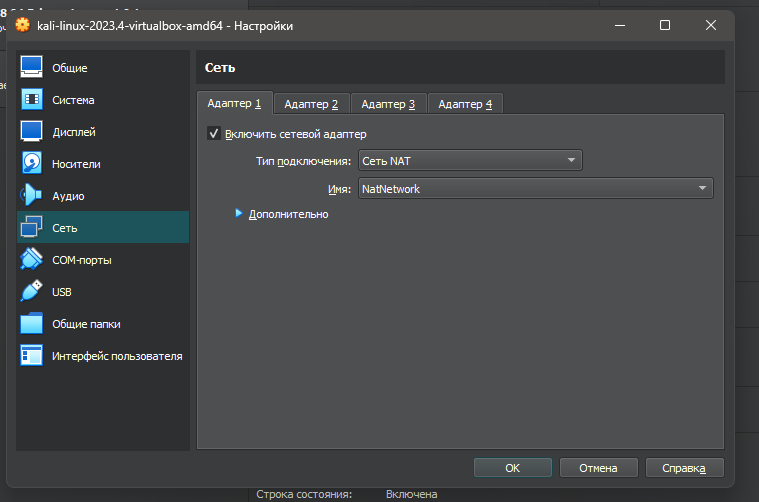


2. Установка Metasploitable 2

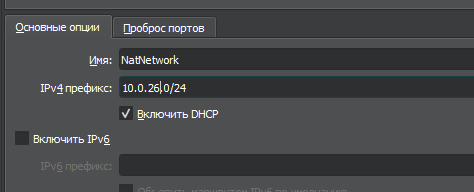


3. Настройка и проверка сетевого взаимодействия

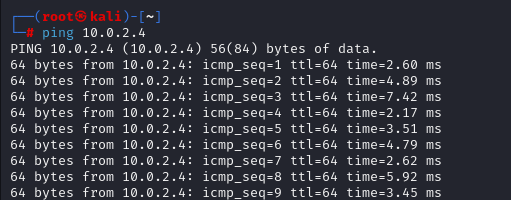




Сеть по порядковому номеру в группе:



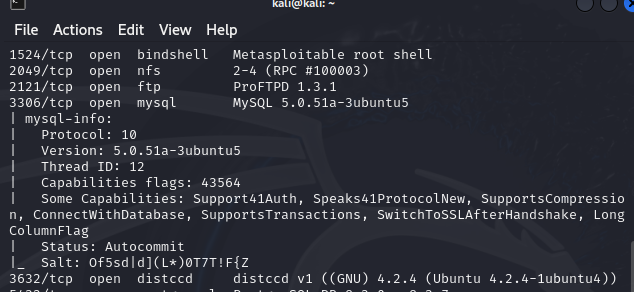
Задание: На ВМ Kali Linux выполните команду ping {ip-адрес ВМ metasploitable 2}



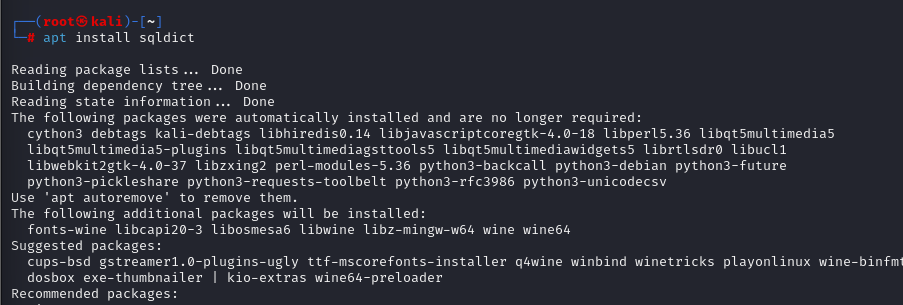
ГЛАВА 3. ПАРОЛИ

3.1 Тестирование баз данных, Атаки на пароли

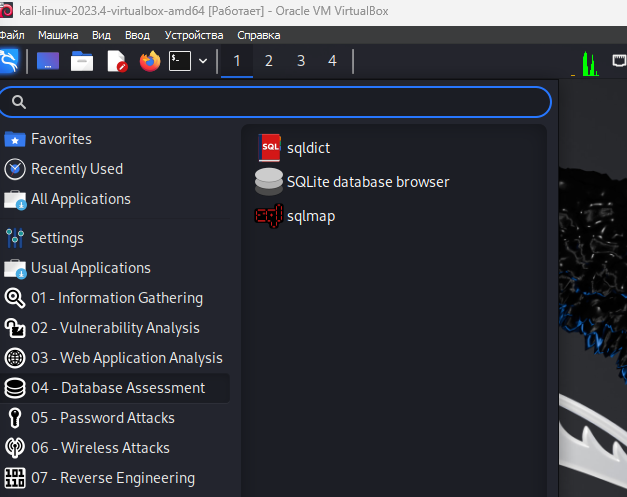
nmap -p- -T4 -A 10.0.17.5



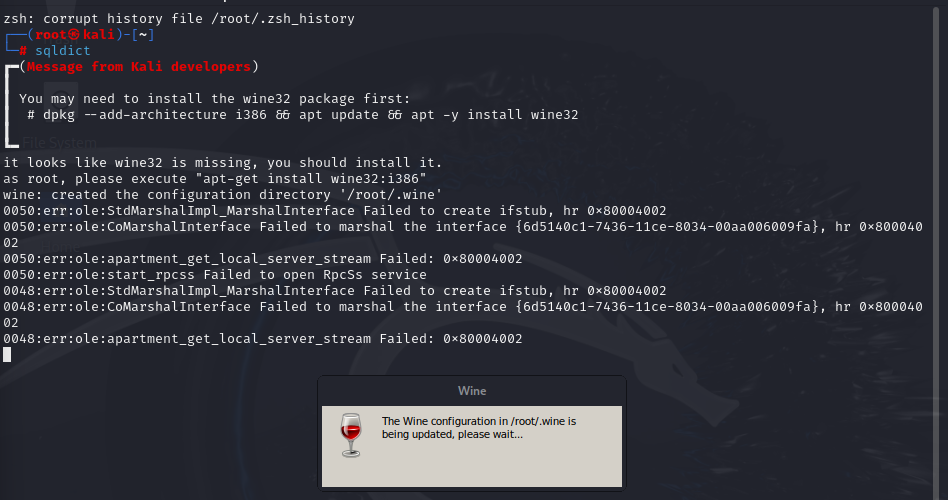
apt install sqldict



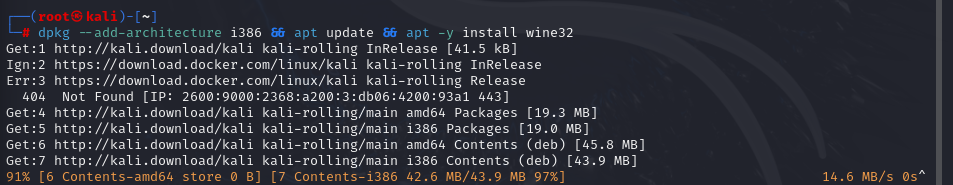
Обратите внимание, что в меню Application в разделе 04 - Database Assessment появилось приложение Sqldict.



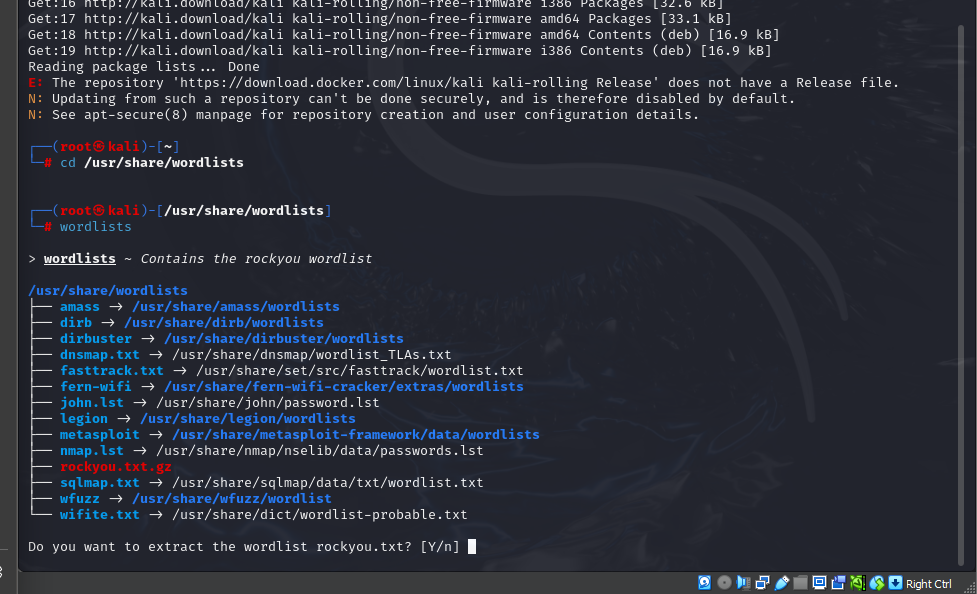
С помощью sqldict можно производить подбор паролей, и данный процесс называется «атака по словарю». Другими словами, создается список возможных паролей. При первом запуске sqldict в терминале появляется ошибка, так как сперва нужно выполнить установку «wine32»

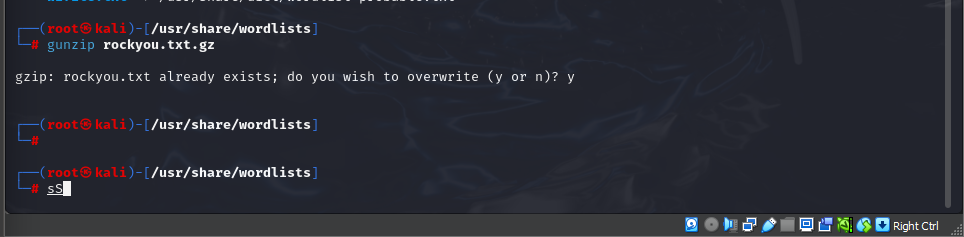


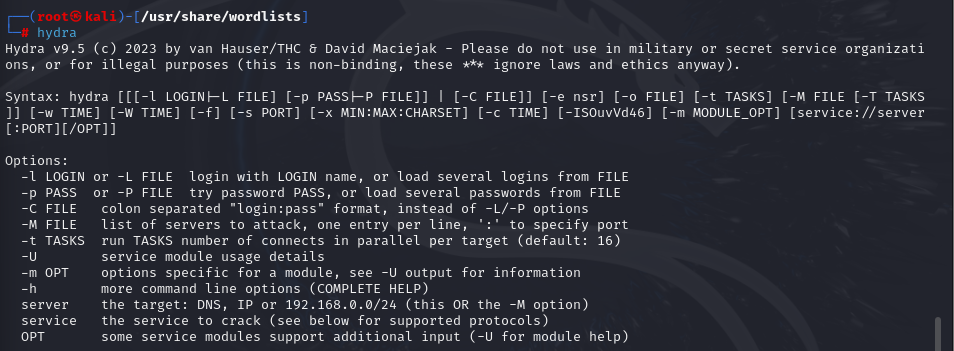
Wine32 – это программа на Kali и других дистрибутивах Linux, которая позволяет запускать программы для Windows в линукс системах. В Windows программы имеют расширение «.exe». Это исполняемые файлы, и они созданы для работы в Windows. В отобразившейся информации при запуске в терминале есть команда для установки wine32. Она выглядит как dpkg --add-architecture i386 &&

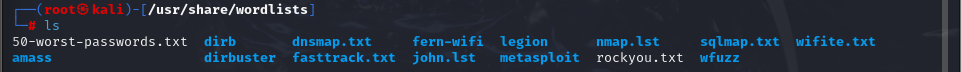


Рассмотрим еще один инструмент, который можно использовать для достижения той же самой цели. Его можно найти в разделе «Passwords Attacks», и он называется «wordlists». Найдите его и сделайте screenshot. В разделе «Атаки на пароли» существует несколько инструментов для этого, но нас интересует тестирование онлайн сервисов. Ранее мы уже тестировали запущенные сервисы SSH и FTP. Как правило, для этих них существует подбор имени пользователя и пароля. Вашей целью будет сервис mysql, который запущен на целевой машине. Вам нужно подобрать имя пользователя и пароль. Это называется онлайн-атака на пароли. Перейдите в директорию «worldlists»

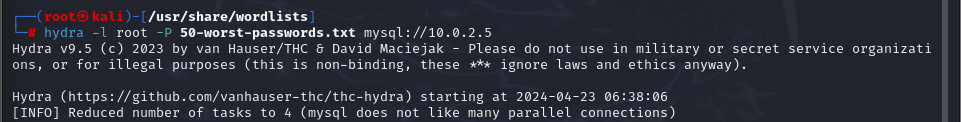




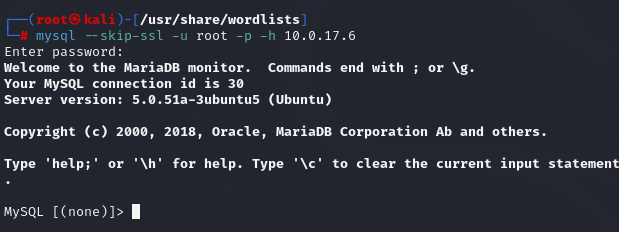




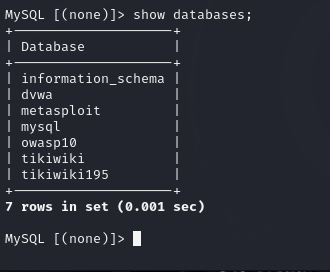
hydra -l root -P 50-worst-passwords.txt mysql://10.0.2,5



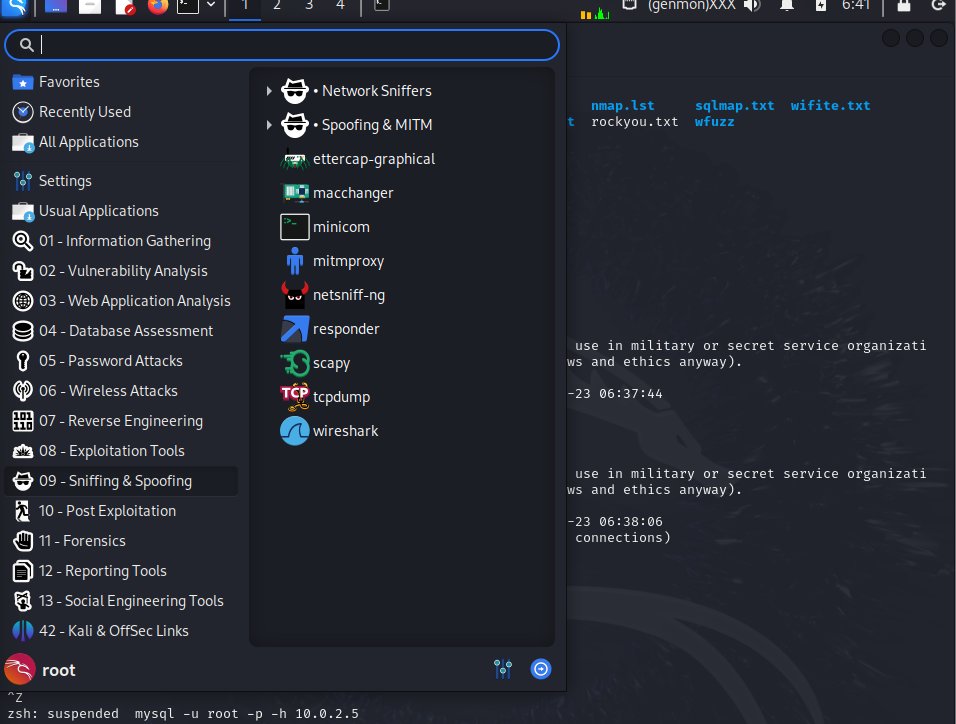
mysql –skip-ssl -u root -p -h 10.0.17.7



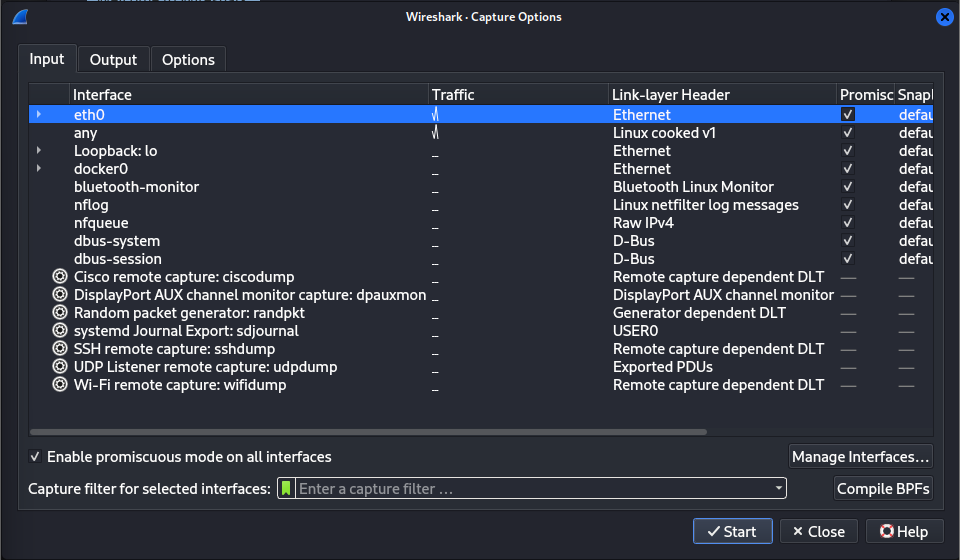
show databases;

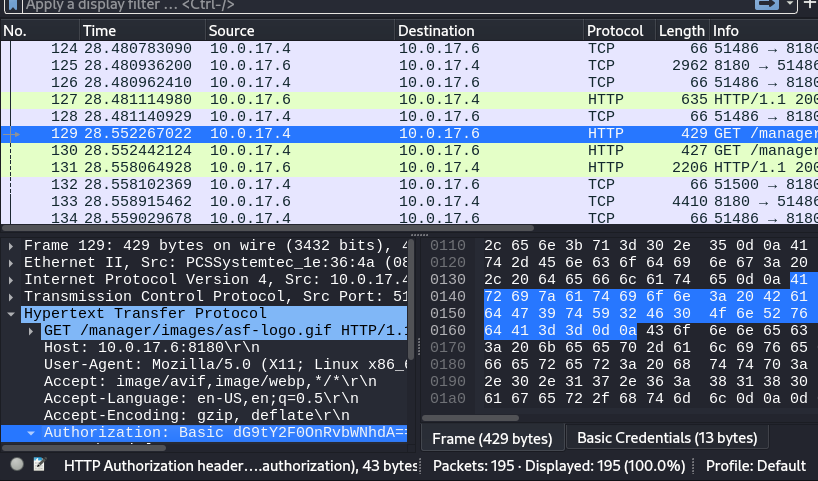


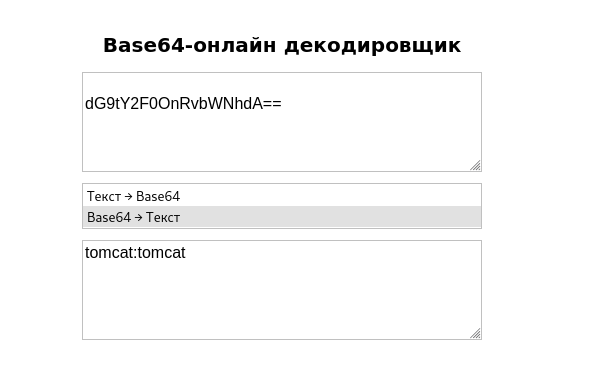
**3.2. Сниффинг паролей**



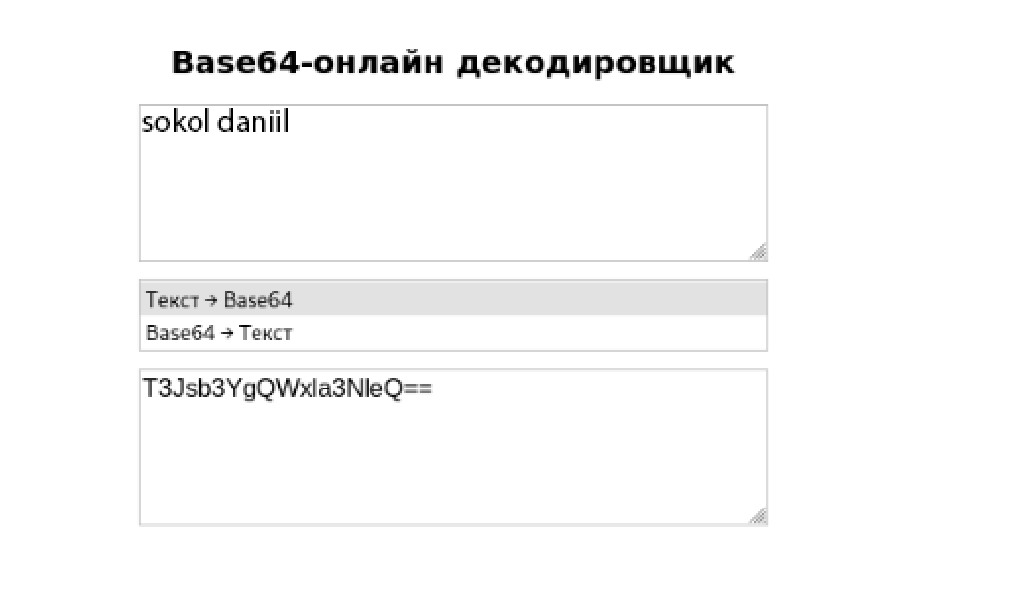
Этот инструмент работает на вашем компьютере, анализируя сетевой трафик и перехватывая все пакеты. Также можно указать, какие пакеты перехватывать. Рассмотрим wireshark более детально, научимся искать имена пользователей и пароли, которые передаются в вашей сети. Для начала выбираете меню «Capture», далее «Options»:



****

****

● Закодируйте свое имя с помощью base64. Сделайте screenshot результата.



● Опишите основной функционал программы wireshark. Какие из его модулей используются наиболее часто?

● Захват пакетов: Wireshark позволяет захватывать пакеты данных, передаваемые по сети.

● Анализ пакетов: После захвата пакетов Wireshark предоставляет мощные средства для анализа каждого пакета в отдельности.

● Фильтрация пакетов: Позволяет применять различные фильтры для отображения только тех пакетов, которые соответствуют определенным критериям.

● Декодирование пакетов: Wireshark автоматически декодирует пакеты, отображая содержимое пакетов в удобочитаемом формате.

● Статистика: Wireshark предоставляет различные статистические данные о захваченном сетевом трафике