

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

# «МИРЭА – Российский технологический университет» РТУ МИРЭА

# РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

Кафедра КБ-2 «Прикладные информационные технологии»

Практическая работа № 6

по дисциплине «Безопасность Операционных систем»

«Основы Kali Linux ч.3»

|  |  |
| --- | --- |
|  | Выполнил:  Студент БББО-05-20  Кутьин З.С. |
|  | Проверил:  Абрамов Д.П. |

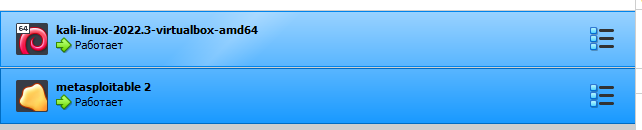
**Цель работы**

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

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

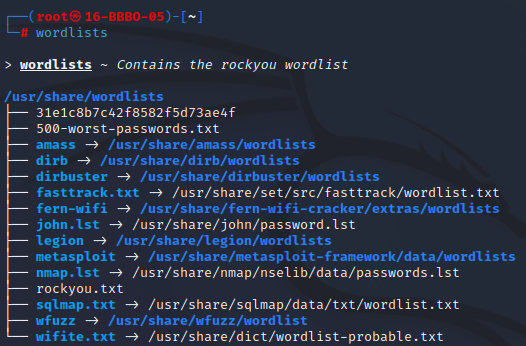
**Порядок выполнения работы**

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

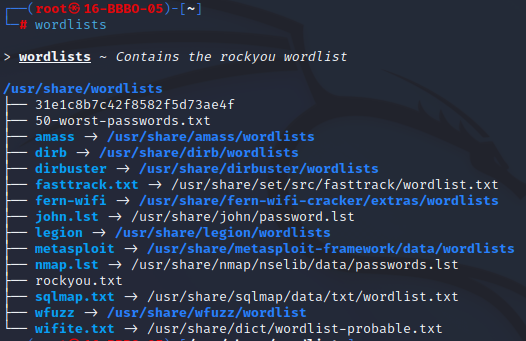


1. **Взламываем базу данных. Атаки на пароли**

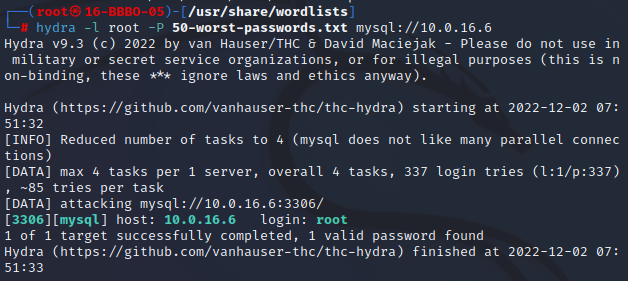
Выполнение команды wordlists



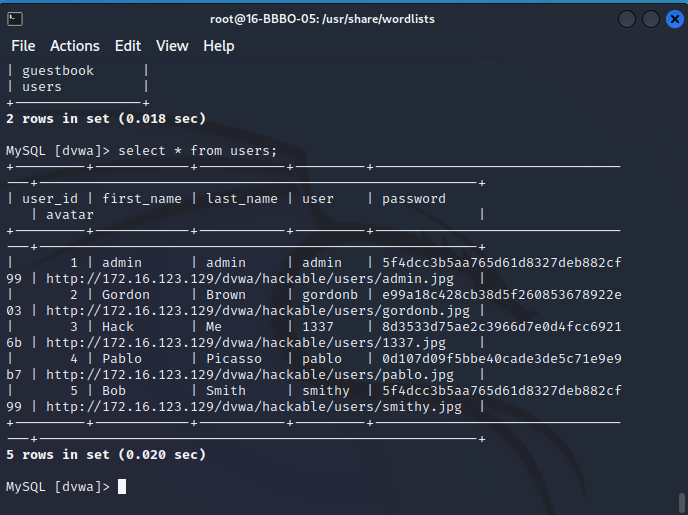
Выполнение команды wordlists после редактирования файла (добавления поля пустого пароля и оставления 50-ти паролей из 500), изменения названия файла

Ы

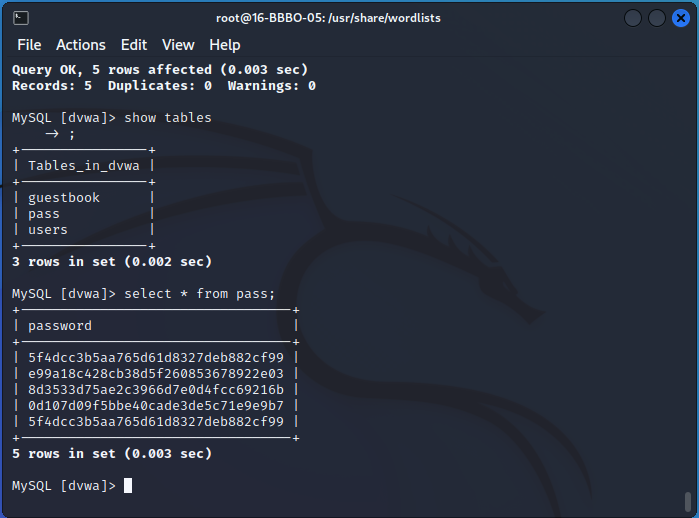
Перебор по словарю с помощью команды hydra –l root –P 50-worst-passwords.txt mysql://10.0.16.6



Вывод таблицы users из MySQL базы данных



Создание новой таблицы с украденными хэш-паролями и вывод её на экран

****

Вывод содержания txt файла с хэш-паролями и исходными паролями

****

**Основные ключи команды hydra с описанием**

****

$ hydra опции логины пароли -s порт адрес\_цели модуль параметры\_модуля

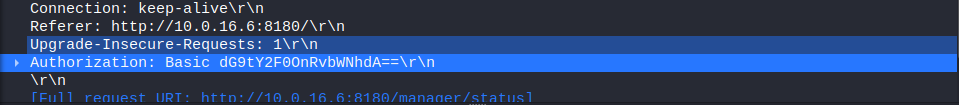
* -R - восстановить ранее прерванную сессию Hydra;
* -S - использовать SSL для подключения;
* -s - указать порт;
* -l - использовать логин;
* -L - выбирать логины из файла со списком;
* -p - использовать пароль;
* -P - использовать пароль из файла со списком;
* -M - взять список целей из файла;
* -x - генератор паролей;
* -u - по умолчанию hydra проверяет все пароли для первого логина, эта опция позволяет проверить один пароль для всех логинов;
* -f - выйти, если правильный логин/пароль найден;
* -o - сохранить результат в файл;
* -t - количество потоков для программы;
* -w - время между запросами в секундах;
* -v - подробный вывод;
* -V - выводить тестируемые логины и пароли.

1. **Сниффим пароли**

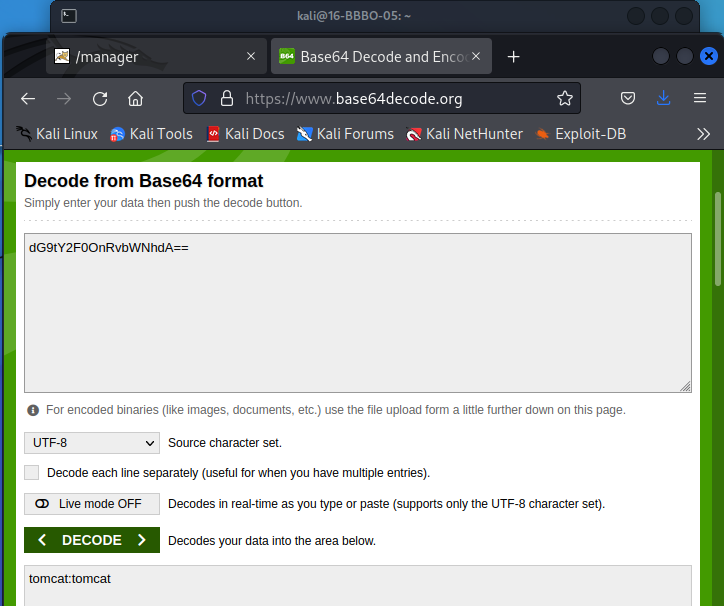
Вывод пакета HTTP 481 (авторизация на сайте)



Значение в поле Authorization. Данная строка зашифрована с помощью легко декодируемого метода base64



Декодирование значения из поля Authorization. Ниже видим данные в формате логин:пароль



**Вывод**: Я закрепил знания об инструментах Kali linux: nmap, Metasploit, утилиты для тестирования веб-сервисов nikto. Освоил атаку на пароли через wordlists и hydra. А также сниффинг паролей с помощью программы WireShark.