

# Основы Kali Linux. Хеширование. Hashcat.

Клуб компьютерной безопасности  
Студенческих Клубов Разработки  
2022

# На пути в Linux

- Зачем?
- Что такое «дистрибутив» и почему выбран Kali?
- Насколько это сложно?
- А на Windows можно?

# Базовые команды терминала

| <code>pwd</code>   | выводит директорию, в которой на данный момент находится шелл;              |
|--------------------|---|
| <code>ls</code>    | выводит директории и файлы, находящиеся в текущей директории;               |
| <code>cd</code>    | меняет текущую директорию на ту, которая указана в качестве аргумента;      |
| <code>mkdir</code> | создаёт пустую директорию;  |
| <code>cat</code>   | выводит в консоль содержимое файла;   |
| <code>less</code>  | открывает файл в псевдографическом интерфейсе для удобного просмотра;       |
| <code>mv</code>    | перемещает (или переименовывает) файл;                                      |
| <code>cp</code>    | создаёт копию файла;  |
| <code>rm</code>    | удаляет файл;   |
| <code>nano</code>  | консольный текстовый редактор;  |
| <code>sudo</code>  | позволяет временно повысить привелегии для выполнения некоторой команды     |
| <code>ssh</code>   | позволяет подключиться к другому компьютеру, на котором запущен ssh-сервер. |

# Полезные команды (программы)

| <code>wc -l &lt;file&gt;</code>            | Считаем количество строк в файле   |
|--|--|
| <code>wc -c</code>                         | Считаем количество символов в файле  |
| <code>grep</code>                          | Поиск в файле строк, соответствующих заданному регулярному выражению             |
| <code>xxd</code>                           | Выводим файл в шестнадцатеричном виде (что может быть полезно для неизв. файлов) |
| <code>md5sum</code>                        | Получить хеш из строки, используя алгоритм MD5                                   |
| <code>unzip -P password zipfile.zip</code> | Распаковать zip-архив с паролем  |

<https://securityonline.info/some-useful-linux-command-for-your-penetration-testinglinux-command/>



<https://github.com/sociopart/ctf>

(условия для задач и команды со слайдов – тут)



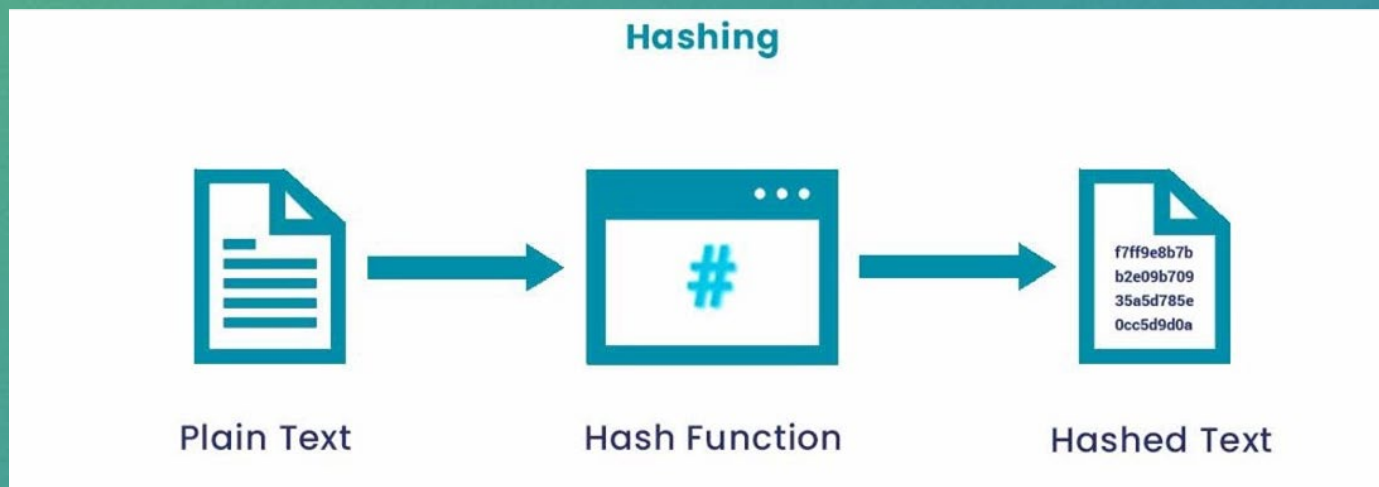
# Задание 0. Проверяем работу всего

1. `echo "Hello World"`
2. Посчитаем количество строк в файле `sample.txt`
3. Покопаемся в бинарном файле:

```
cat calc.exe | xxd
```

# Хеширование

- Хеширование — это процесс, преобразовывающий произвольный массив данных в состоящую из букв и цифр строку фиксированной длины.



- Преобразовывает массив данных в строку фиксированной длины хеш-функция, которая представляет собой математический алгоритм.

# Пример генерации хеша

➤ <http://www.sha1-online.com/>

| Data               | Hash                                     |
|--------------------|--|
| Vince              | 27b7c809b569e2a89c84826e023cba4db292066a |
| SomeVeryBigDataOMG | 17057c0f66c5d3e9fee5a6117774cc0176d9dd27 |
| 1                  | 356a192b7913b04c54574d18c28d46e6395428ab |



# Хеширование VS Шифрование

- Является необратимым процессом и исходные данные получить невозможно
- Данные можно восстановить в исходном виде с помощью ключа.

## Общее:

- Их часто путают между собой 😊
- В некоторых случаях данные можно получить, используя данные из открытых источников (соответствие хеша паролю, базы популярных паролей)

# Области применения

- Шифрование должно использоваться, когда существует необходимость расшифровать получаемое сообщение

Пример: архивы и другие данные для чтения, защищенные паролем.

- Хеширование предпочтительно использовать тогда, когда сами данные не должны быть известны в исходном виде

Пример: хранение паролей в базе данных

# HashCat

- Самая быстрая и передовая утилита для восстановления паролей, поддерживающая пять уникальных режимов атаки для более чем трёхсот алгоритмов хеширования.



# Перебор по словарю

- Скачиваем популярный «словарь» для перебора:

```
> wget http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt
```

- Запускаем программу

```
> hashcat -m 0 -a 0 53ab0dff8ecc7d5a18b4416d00568f02 rockyou.txt
```

- **-m 0** устанавливает тип хеша для взлома (здесь – MD5)
- **-a 0** устанавливает тип «атаки» (здесь – по словарю)



# Задание 1. Перебор по словарю

- Прочитайте содержимое файла `solve.txt`, находящегося внутри архива `task1.zip`, защищенного паролем.
- К сожалению, о пароле неизвестно ничего, кроме его хеша – `6f6f48c6a47626924c38cf9eeb590abd`. Говорят, что он в формате MD5.
- Внутри текстового файла, который находится внутри архива, лежит флаг – он и является ответом на задачу.



# Пароли неизвестной длины

- Представим, что цель – вычислить пароль от Wi-Fi роутера.
- Как правило, его длина 8 символов, но мы точно знаем, что его изменяли неоднократно.
- Попробуем взять и перебрать пароль в окрестности числа 8 (от 6 до 10 =  $8 \pm 2$ )

```
> hashcat -m 0 -a 3 -i --increment-min=6 --increment-max=10 53ab0dff8ecc7d5a18b4416d00568f02
```

- Параметр `-i` нужен для работы параметров `increment-min` и `increment-max`.

## Задание 2. Флаг неизвестной длины

- Взломайте архив `task2.zip`, зная следующее:
- Есть хеш – `9fbe2a6408c62afb10a3e5381ee4e6ef`
- Пароль, вроде как, был или 5 символов... или 8...
- Результат работы Hashcat будет ответом на задачу.

# Маски для паролей

? | Charset

===+=====

l | abcdefghijklmnopqrstuvwxyz

u | ABCDEFGHIJKLMNOPQRSTUVWXYZ

d | 0123456789

h | 0123456789abcdef

H | 0123456789ABCDEF

s | !"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~

a | ?l?u?d?s

b | 0x00 - 0xff

# Перебор по маске

- `hashcat.exe -m 0 -a 3 53ab0dff8ecc7d5a18b4416d00568f02 ?1?1?1?1?1?1?1?1`
- `hashcat.exe -m 0 -a 3 -i --increment-min=6 --increment-max=10 53ab0dff8ecc7d5a18b4416d00568f02 hac?1?1?1?1?1?1?1`

# Задание 3. Перебор по маске


- Взломайте архив `task3.zip`.
- Известно, что пароль состоит из 5 символов шестнадцатеричной системы счисления, записанной маленькими буквами.
- Хеш - `97cb30d0ac8277287b27ce7064afa1b4b830b740`
- Формат - `sha1`
- Пароль к архиву является ответом на задачу.



# Задание 4. Гибридная атака

- Вычислите пароль для архива `task4.zip`, зная, что:
- Его можно найти в словаре;
- Также он содержит только символы шестнадцатеричной системы счисления, записанные большими буквами.
- Подсказка: параметр `-a` будет равняться `6`.

```
- [ Attack Modes ] -  
  
# | Mode  
====+=====  
0 | Straight  
1 | Combination  
3 | Brute-force  
6 | Hybrid Wordlist + Mask  
7 | Hybrid Mask + Wordlist  
9 | Association
```



THANK

YOU

ALL