# ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования

# МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

Кафедра «Математическая кибернетика и информационные технологии»

# ОТЧЁТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ № 4

по дисциплине «СПОЗИС»

# «hashcat»

Выполнил студент группы БПЗ1801:

Тимошенко А.С.

Проверила Алексанян Д. А.

Москва, 2021

# Цель работы:

* Научиться работать с утилитой HashCat.

# Задача:

**Задача 1**

Каким-то образом у вас оказался хэш пароля. Необходимо выполнить следующее:

* По длине хэша попробовать угадать его тип;
* Запустить hashcat для подбора пароля.

Индивидуальный вариант задания:

35602208E86AC7D6B3A63780A9538A9D1763A646D5B9F3930A0548E0983E0CA6

20

# Задача 2

У вас есть фрагмент записи из файла /etc/shadow:

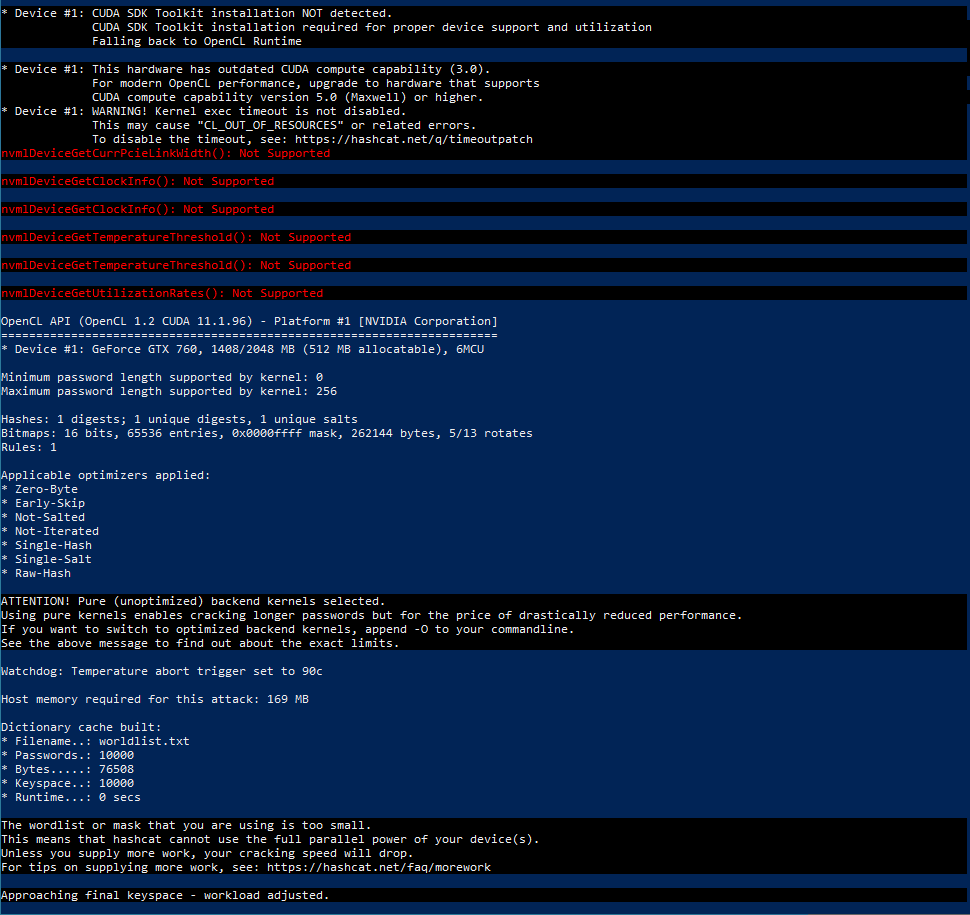
# hackme:$6$iMDxXB6C.bGVPgP/$dzNU7.0TSuoY8LUBKInul8kkDbjNsTEJWC6ake4pBi9Mf8icvzTm7aydpgs7ciJsRur ui/SVBHsKWP0Ji4f7U1:....

Подберите с помощью Hashcat пароль пользователя по хэшу из /etc/shadow.

# Выполнение: Задача 1



Рис. 1 Выполнение утилиты hashcat



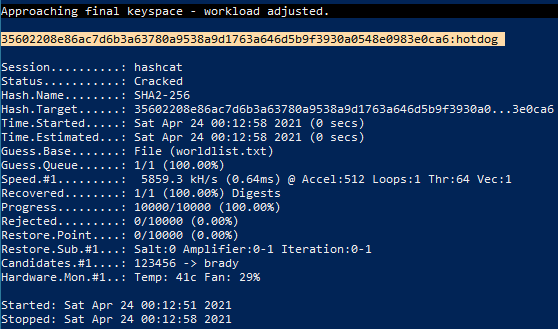


Рис. 2,3 Результат выполнения утилиты hashcat

Как видно, атака прошла успешно. Результат тип хэша **SHA2-256,** пароль – **hotdog**

# Задача 2

**Дано:**

hackme:$6$iMDxXB6C.bGVPgP/$dzNU7.0TSuoY8LUBKInul8kkDbjNsTEJWC6ake4pBi 9Mf8icvzTm7aydpgs7ciJsRurui/SVBHsKWP0Ji4f7U1:....

Начиная с первого символа $ до второго символа $ идёт информация об алгоритме хэширования. В нашем случае алгоритм хэширования - **$6$ - SHA-512**

Со второго $ до следующего $ идёт «соль» - **iMDxXB6C.bGVPgP/**

От последнего $ до : идёт сам хэш (от «соленного пароля») -

# dzNU7.0TSuoY8LUBKInul8kkDbjNsTEJWC6ake4pBi9Mf8icvzTm7aydpgs7ciJsRurui

**/SVBHsKWP0Ji4f7U1**

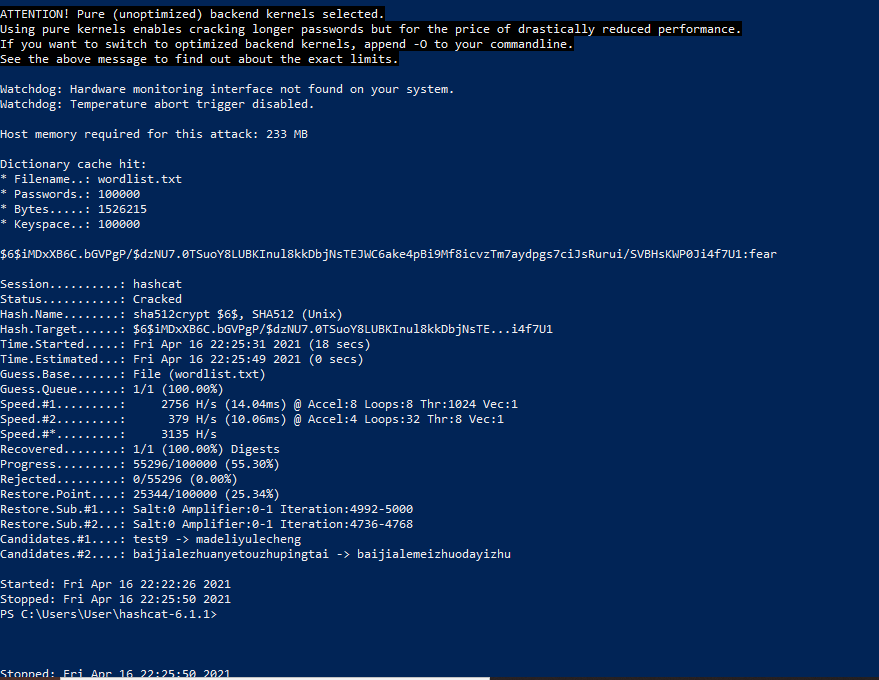
В hashcat хэширование **SHA-512** для **Unix** систем соответствует номер **1800**.

1. Запускаем утилиту hashcat.



*Рис 3 — Выполнение утилиты hashcat.*

1. Получаем результат.



*Рис 4 — Результат выполнения утилиты hashcat.*

Пароль соответствующий фрагменту записи из файла /etc/shadow – **fear**.