

|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |
| **Институт комплексной безопасности и специального приборостроения** |

Кафедра КБ-1 «Защита информации»

**Электронный отчет**

По теме «Обеспечение криптографической защиты информации

в современных операционных системах. Linux.»

По дисциплине “Основы информационной безопасности”

Выполнил:

Студент 1 курса

Группа БАСО-02-20

Шифр 20Б0852

Чугаев Никита

Сергеевич

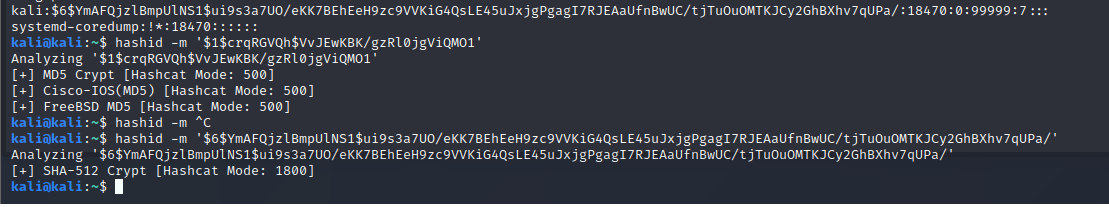
Проверил:

**Оглавление**

1. Определения типа хэш пароля. ………………………………………..3
2. Добавление нового пользователя в систему. ……………….………...4
3. Проверка контрольных сумм. Контрольные суммы используются для целостности файлов. …………………………………………………....5
4. Отправление зашифрованного письма с помощью Tunderbird. ……..7
5. **Определения типа хэш пароля.**

В терминале операционной системе Linux с помощью команды

sudo cat /etc/shadow мы можем узнать хэш пароли всех пользователей системы.

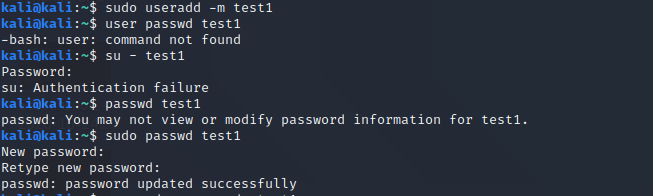


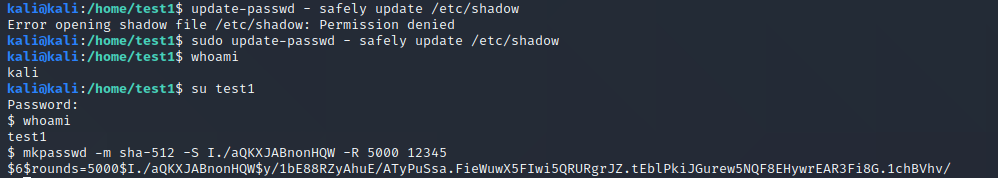
После того как я узнал хэш пароль пользователя kali с помощью команды hashid -m [хэш] мы можем узнать тип хэша. В моем случае тип – sha-512 [hashcat Mode; 1000]

Так же мне требуется определить соль хэша, она находится между знаками $. Моя соль YmAFQjzlBmpUlNS1

1. **Добавление нового пользователя в систему.**

С помощью команды sudo useradd -m test1 создал пользователя с именем test1. А с помощью команды sudo passwd test1 обновил пароль пользователя test1.

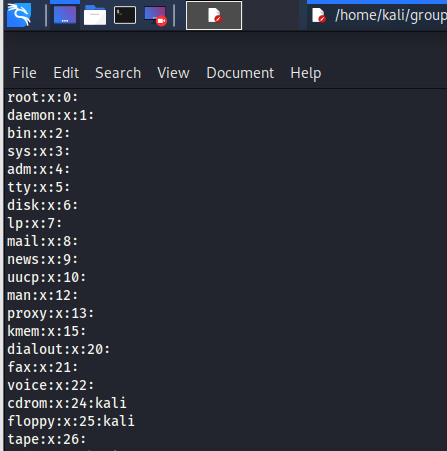




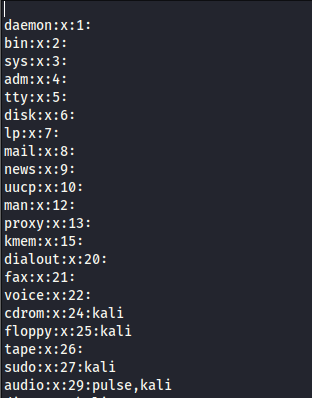
Далее я сменил пользователя командой su test1, после чего проверил с помощью whoami.

Следом с помощью команды mkpasswd -m sha-512 -S [хэш пароля пользователя test1] я смог рассчитать хэш пароль пользователя.

1. **Проверка контрольных сумм. Контрольные суммы используются для целостности файлов.**

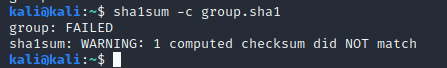
Поместил файл “Group” в домашнюю папку. 

Следом внес в него изменения



Далее с помощью команды sha1sum -c group.sha1 проверил контрольную сумму с исходным файлом.

Warning: 1 computed checksum did NOT match говорит нам о том, что контрольные суммы не совпали. Это означает, что в файл были внесены изменения.



1. **Отправление зашифрованного письма с помощью Tunderbird.**

Письмо было зашифровано и отправлено вам с моего почтового адреса nikchugaev220@gmail.com