Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Тульский государственный университет»

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДЫ АНАЛИЗА АЛГОРИТМОВ ХЕШИРОВАНИЯ

отчет о
лабораторной работе №1

по дисциплине
ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Выполнила: ст. гр. 230711 Павлова В.С.
Проверил: асс. каф. ИБ Греков М.М.

Тула, 2023 г.

ЦЕЛЬ РАБОТЫ

Цель: ознакомиться с основными методами оценки методов хеширования методом подбора заранее известных значений. Получить навыки оценки сложности паролей, используемых пользователями.

ЗАДАНИЕ НА РАБОТУ

1. Скачать и установить приложения JhonTheRipper и HashCat, в случае, если не используется Kali Linux.
2. Скачать словарь RockYou.
3. Скачать задание с https://disk.yandex.ru/d/8Oh9impzdtESLw
4. При помощи утилиты zip2john и команды john файл с хешем --wordlist=rockyou.txt получить доступ к зашифрованному архиву.
5. Получить пароль при помощи утилиты SamDump или ophcrack получить пароль из исходных файлов SAM и SYSTEM. (По сути NTLM хеш).
6. При помощи утилит JhonTheRipper и HashCat, используемой в режим дешифровки хешированной соли, получить пароли из файла shadow

ХОД РАБОТЫ

1. С помощью приложения JhonTheRipper и словаря RockYou.txt подбираем пароль к архиву с зашифрованными данными (рисунок 1). Полученный пароль – zipzip1984.

Рисунок 1 – Получение доступа к архиву

2. Аналогичным образом при помощи утилиты JhonTheRipper, используемой в режим дешифровки хешированной соли, получаем пароля из файла shadow (рисунок 2). Полученный пароль – jskillz83.

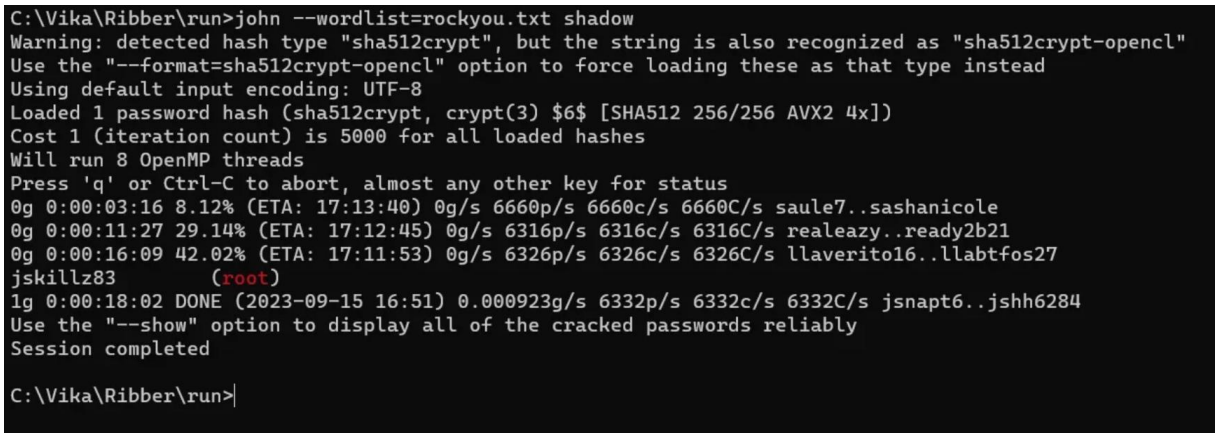

Рисунок 2 – Получение пароля из файла shadow

3. При помощи утилиты ophcrack и ресурса crackstation.net получаем пароль от учётной записи администратора из исходных файлов SAM и SYSTEM (рисунок 3 и 4). Полученный пароль – Passw0rd!

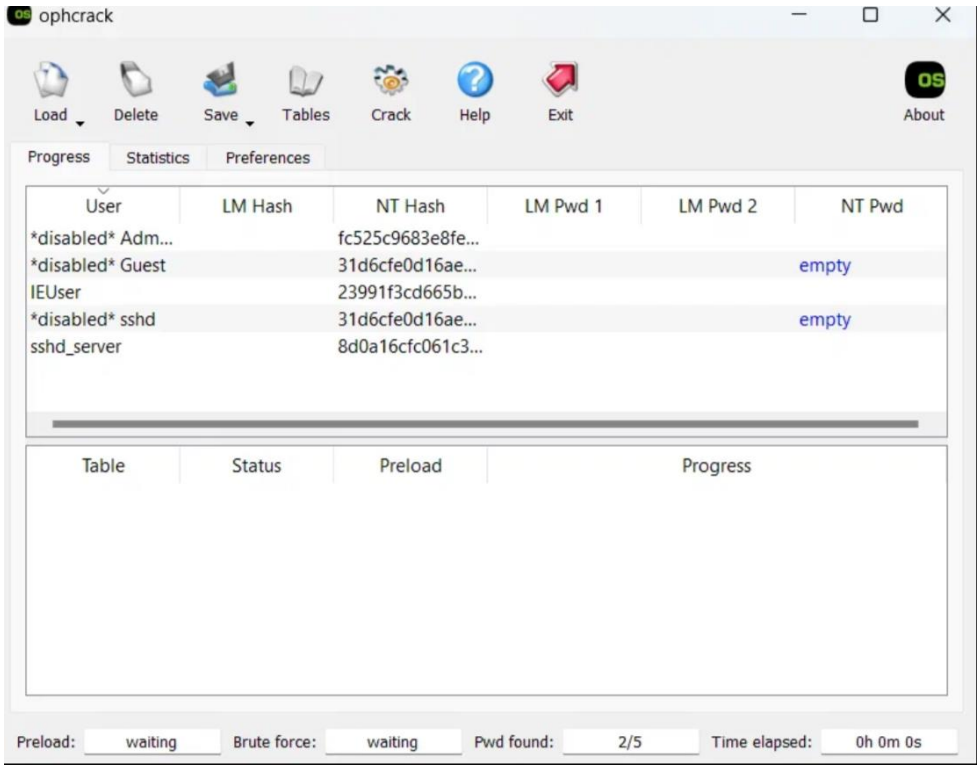

Рисунок 3 – Получение NT (LM) хэшей

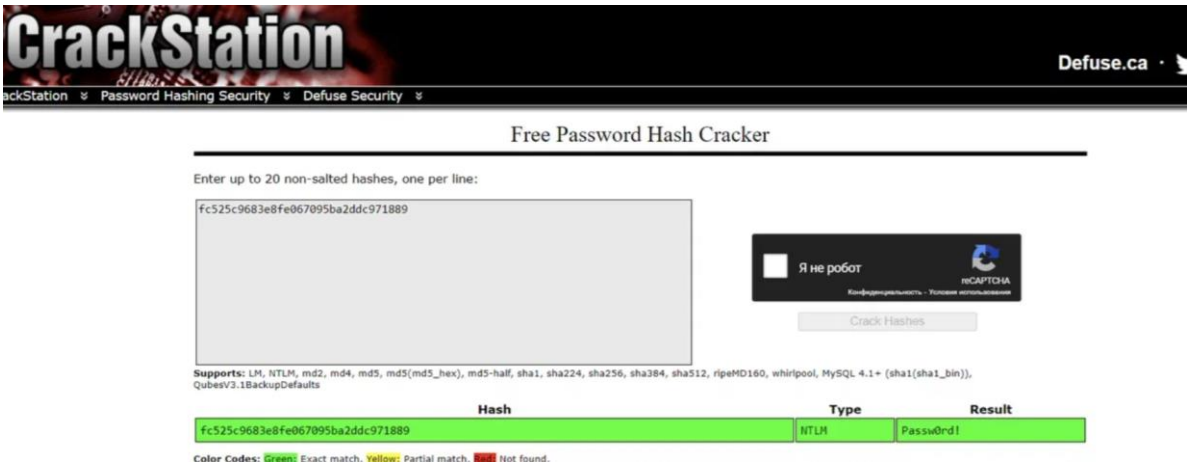

Рисунок 4 – Получение пароля к учётной записи администратора

ВЫВОД

В ходе выполнения данной лабораторной работы я ознакомилась с основными методами оценки методов хеширования методом подбора заранее известных значений.