

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.

```
C:\Vika\Ribber\run>zip2john LabData.zip > LabData.hash
ver 81.9 LabData.zip/SAM is not encrypted, or stored with non-handled compression type
ver 81.9 LabData.zip/SYSTEM is not encrypted, or stored with non-handled compression type
ver 81.9 LabData.zip/shadow is not encrypted, or stored with non-handled compression type

C:\Vika\Ribber\run>john --wordlist=rockyou.txt LabData.hash
Warning: detected hash type "ZIP", but the string is also recognized as "ZIP-openc1"
Use the "--format=ZIP-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
zipzip1984 (LabData.zip/SAM)
1g 0:00:00:22 DONE (2023-09-15 16:31) 0.04436g/s 111218p/s 111218c/s 111218C/s zoefarina..zettykmj
Use the "--show" option to display all of the cracked passwords reliably
Session completed

C:\Vika\Ribber\run>
```

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.

```
C:\Vika\Ribber\run>john --wordlist=rockyou.txt shadow
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-openc1"
Use the "--format=sha512crypt-openc1" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:03:16 8.12% (ETA: 17:13:40) 0g/s 6660p/s 6660c/s 6660C/s saule7..sashanicole
0g 0:00:11:27 29.14% (ETA: 17:12:45) 0g/s 6316p/s 6316c/s 6316C/s realeazy..ready2b21
0g 0:00:16:09 42.02% (ETA: 17:11:53) 0g/s 6326p/s 6326c/s 6326C/s llaverito16..llabtfos27
jskillz83 (root)
1g 0:00:18:02 DONE (2023-09-15 16:51) 0.000923g/s 6332p/s 6332c/s 6332C/s jsnapt6..jshh6284
Use the "--show" option to display all of the cracked passwords reliably
Session completed

C:\Vika\Ribber\run>
```

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!

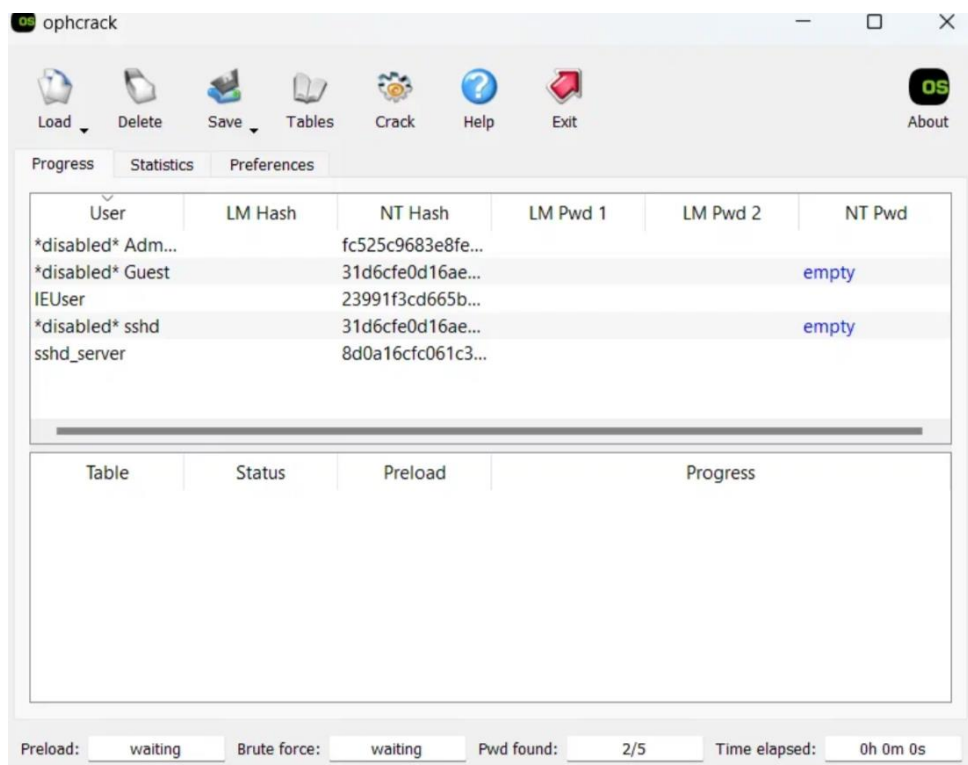


Рисунок 3 – Получение NT (LM) хэшей



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.