CASE STUDY: JOHN THE RIPPER
A REPORT

Submitted by

SIDDHARTH SAXENA (RA2111030010029)

Under the Guidance of

DR. M. JEYASELVI
Assistant Professor

DEPARTMENT OF NETWORKING AND COMMUNICATIONS

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING
with specialization in Information Technology

SCHOOL OF COMPUTING
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603203

MAY 2024

DEPARTMENT OF NETWORKING AND COMMUNICATIONS
SCHOOL OF COMPUTING

College of Engineering and Technology
SRM Institute of Science and Technology

CASE STUDY ON "JOHN THE RIPPER"

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester : III/VI

Report Title : Case Study on "John the Ripper" Tool for Password Cracking

Course Faculty **: Dr. M. Jeyaselvi**

Student Name : (Reg.No:RA2111030010029) Siddharth Saxena

Evaluation:

S.No	Parameter	Marks
1	Problem Investigation & Methodology Used	5
2	Tool used for investigation	5
3	Demo of investigation	5
4	Uploaded in GitHub?	5
5	Viva	5
6	Report	5
	Total	**30**

Date :

Staff Name :

Signature :

INTRODUCTION

First released in 1996, John the Ripper (JtR) is a password cracking tool originally produced for UNIX-based systems. It was designed to test password strength, brute-force encrypted (hashed) passwords, and crack passwords via dictionary attacks.

The tool comes in both GNU-licensed and proprietary (Pro) versions. An enhanced “jumbo” community release has also been made available on the open-source GitHub repo. The Pro version, designed for use by professional pen testers, has additional features such as bigger, multilingual wordlists, performance optimizations and 64-bit architecture support.

Some of the key features of the tool include offering multiple modes to speed up password cracking, automatically detecting the hashing algorithm used by the encrypted passwords, and the ease of running and configuring the tool making it a password cracking tool of choice for novices and professionals alike.

OBJECTIVE OF THE PROJECT

The objective of this project is to leverage John the Ripper for password cracking and hash analysis to assess the strength of authentication systems. Through systematic password cracking attempts and comprehensive hash analysis, the project aims to identify weak passwords, evaluate the effectiveness of existing password policies, and recommend enhancements to bolster password security. By gaining insights into common password vulnerabilities and encryption weaknesses, the project seeks to mitigate the risk of unauthorized access and strengthen overall cybersecurity defenses.

INSTALLATION

John the Ripper is a cross-platform tool which is supported on the desktop operating systems Windows, macOS and various Linux distributions.

- To install it on Windows and macOS, we can download it from the link https://www.openwall.com/john/

  Alternatively, for macOS, the Homebrew package manager can be used as well with the following command:

  $ brew install john

- On Linux, the following commands can be given for various distributions for installing John the ripper:

  $ sudo apt install john (Debian/Ubuntu/Kali Linux and derivatives)

  $ sudo dnf install john (RedHat/Fedora and derivatives)

  $ sudo pacman –S john (Arch Linux and derivatives)

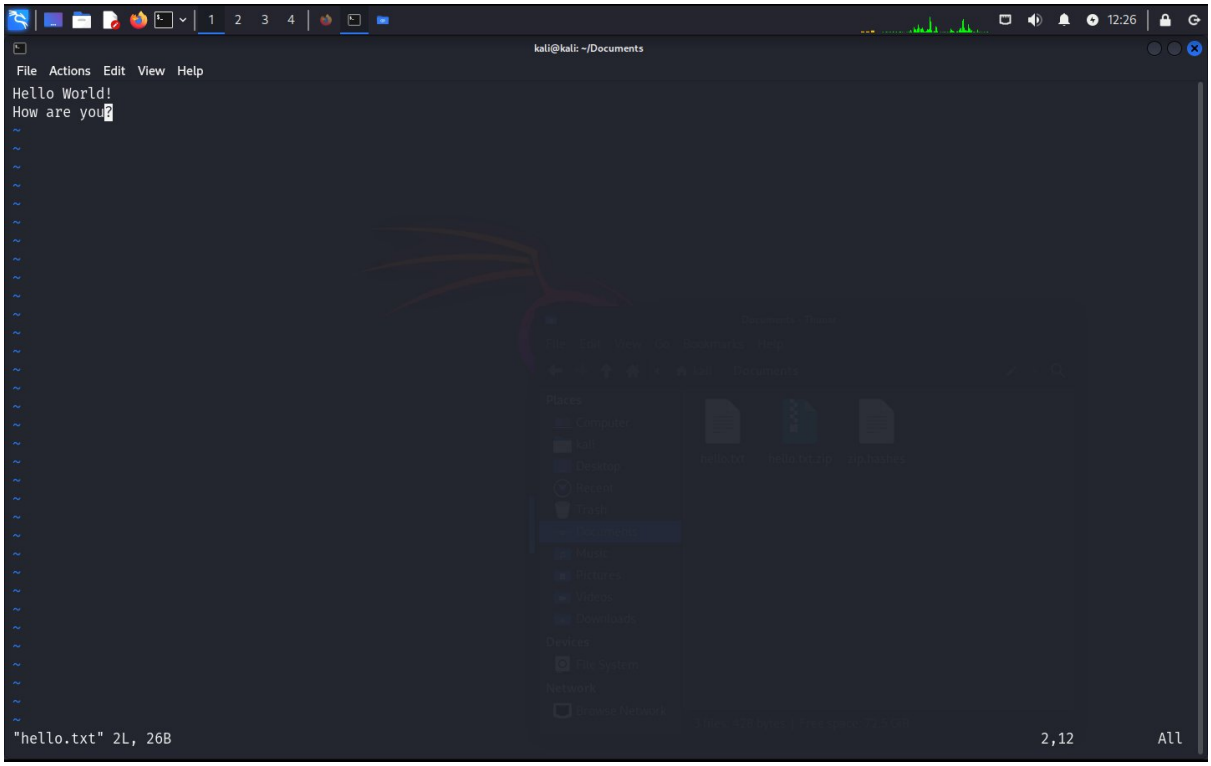
  For other Linux distributions, their package repositories can be referred.

USAGE OF THE TOOL

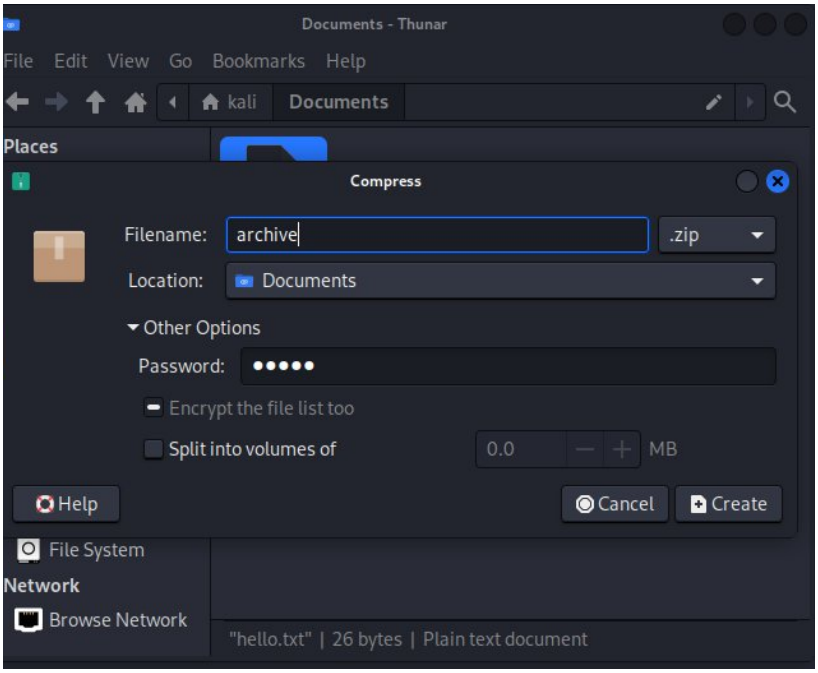
1. Password cracking of a .zip archive

A .zip archive is a compressed file format commonly used for storing and transferring multiple files or directories. It employs lossless compression algorithms to reduce the overall size of the files, making them more manageable for storage and transmission. ZIP archives can contain a variety of file types and are widely supported across different operating systems and software applications. They offer benefits such as faster file transfers, reduced storage space requirements, and the ability to preserve the original file structure. Additionally, .zip archives support encryption, password protection, and metadata storage, enhancing security and organization for archived data.

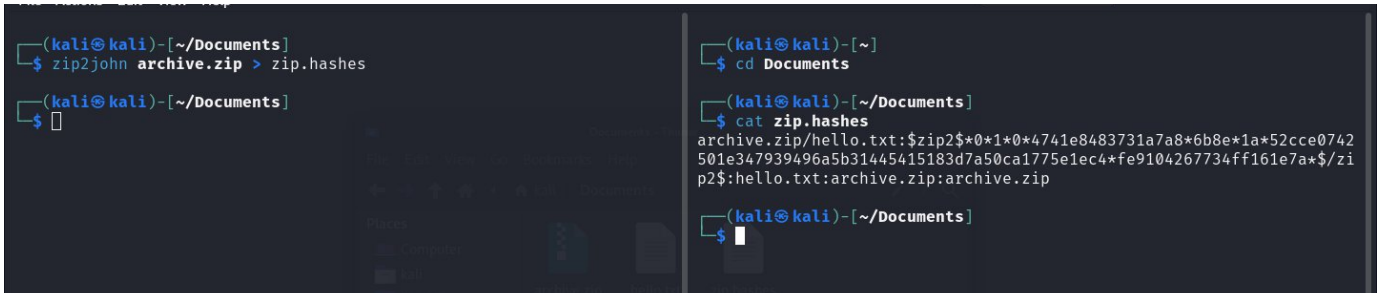
In this scenario, we will be creating a .zip archive containing a file named hello.txt, which will be password protected.



Contents of the file hello.txt



Using John the Ripper, we can first initialize one of its components `zip2john` to copy the hashes to another file, zip.hashes



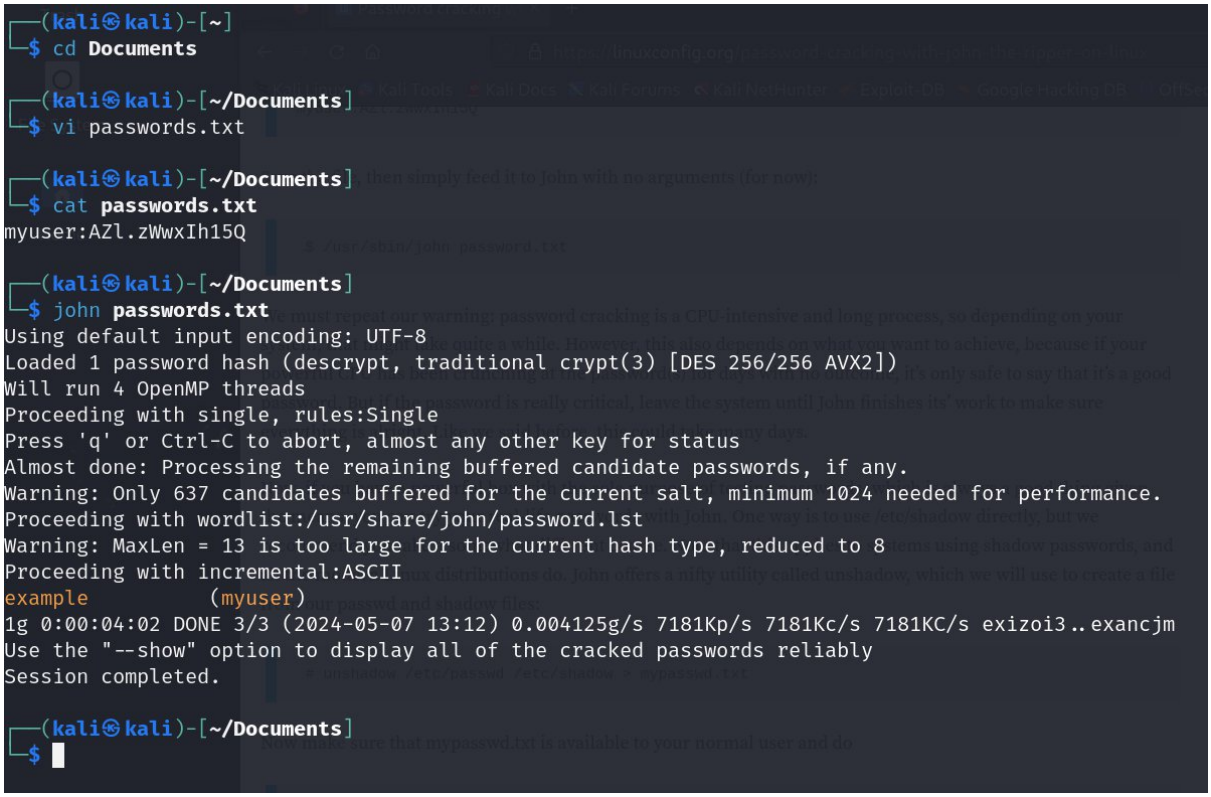
Creation of zip.hashes and its contents

The above command will get the hash from the zip file and store it in the zip.hashes file. We can then use John to crack the hash.

John the Ripper comparing the hashes and cracking the password.

2. Checking Strength of a Password

In this test case, we will enter a password inside a text file, passwords.txt, and analyze it's strength using John the Ripper.



We can see that the passwords.txt file contains the following string

myuser:AZl.zWmxIh15Q

where myuser is the username and the string after the colon is the password. Scanning this file through John the Ripper shows that the password is strong, however due to the high strength of the password, cracking it can take a long time as it depends on the processing power of the system on which the tool is running on.

CONCLUSION

In conclusion, we can analyze that John the Ripper is a powerful and highly-configurable tool to utilize for password strength testing that can work on any desktop platform, however due to the complexity of passwords especially in the modern age, the tool requires high processing power to run efficiently and performant.

GITHUB REPOSITORY

https://github.com/sid3425/JohnTheRipper-Case_Study

RESOURCES

https://www.openwall.com/john/

https://en.wikipedia.org/wiki/John_the_Ripper

https://github.com/openwall/john