

ETHICAL HACKING USING JOHN THE RIPPER

A REPORT

Submitted by

AJAY KUMAR (RA2111030010084)

Under the Guidance of

Dr. Jeyaselvi M

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



SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

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 ETHICAL HACKING USING JOHN THE RIPPER

EVEN Semester (2023-2024)

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

Year & Semester : III/VI

Report Title : Ethical hacking using penetration testing tools

Course Faculty : Dr. Jeyaselvi M

Student Name : Ajay Kumar C (RA2111030010084)

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 :

INDEX

CONTENTS:-		
<u>S.no</u>	<u>Particulars</u>	<u>Page no.</u>
1.	Introduction	1
2.	Scope and Objectives	2
3.	About the Tool and Application	3
4.	Tool Installation Procedure	4
5.	Steps Of Ethical Hacking Tool John The Ripper	5
6.	Screenshot	6
7.	Conclusion	11
8.	References	12

CHAPTER-1

1.INTRODUCTION

In the realm of cybersecurity, staying ahead of potential threats requires a proactive stance. This means not only reacting to known vulnerabilities but also anticipating and addressing potential weaknesses before they are exploited. Ethical hacking, or penetration testing, is a vital component of this proactive approach. By simulating attacks from the perspective of a malicious actor, ethical hackers can identify vulnerabilities and help organizations bolster their defenses.

John the Ripper stands out as a valuable tool in the arsenal of ethical hackers. Its ability to crack passwords using various techniques, such as dictionary attacks, brute force attacks, and rainbow table attacks, allows testers to assess the strength of password security measures. By uncovering weak passwords, organizations can take steps to enforce stronger password policies and educate users on better password practices.

The ethical hacking process typically begins with defining the scope and objectives of the test. This involves identifying the systems and applications to be tested, as well as the goals of the testing exercise. Clear communication with stakeholders is crucial to ensure that testing activities align with organizational priorities and concerns.

Once the scope and objectives are established, ethical hackers proceed with reconnaissance, gathering information about the target environment. This may involve scanning for open ports, identifying services running on target systems, and collecting publicly available information about the organization and its employees. This phase lays the groundwork for subsequent testing activities and helps ethical hackers understand the attack surface.

With reconnaissance complete, ethical hackers move on to vulnerability assessment, identifying potential security weaknesses in target systems and applications. This may involve conducting automated scans using tools like Nessus or OpenVAS, as well as manual inspection of system configurations and code review. Vulnerability assessment enables testers to prioritize risks and focus their efforts on areas of greatest concern.

John the Ripper comes into play during the exploitation phase, where ethical hackers attempt to leverage identified vulnerabilities to gain unauthorized access to target systems. By cracking passwords obtained through reconnaissance or exploiting weak authentication mechanisms, testers can demonstrate the impact of security weaknesses and provide recommendations for remediation.

Finally, ethical hackers document their findings and provide actionable insights to stakeholders. This may include detailed reports outlining vulnerabilities discovered, their potential impact, and recommendations for mitigation. Effective communication is key to ensuring that stakeholders understand the significance of the findings and are equipped to take appropriate action to improve cybersecurity posture.

CHAPTER-2

Scope and Objectives

Scope:

1. **Password Security Assessment:** The primary focus of the project is to evaluate the effectiveness of password security measures implemented within a chosen application or system. By leveraging John the Ripper's capabilities, we aim to identify weak passwords that may pose security risks.
2. **Tool Utilization:** This case study provides comprehensive guidance on the installation and utilization of John the Ripper, ensuring that participants gain a thorough understanding of the tool's functionalities and applications in ethical hacking scenarios.
3. **Practical Implementation:** Through practical demonstrations and real-world examples, we aim to illustrate the ethical hacking process step-by-step, enabling participants to apply theoretical knowledge in practical scenarios.
4. **Recommendations for Improvement:** Based on the findings of the ethical hacking exercise, we will provide actionable recommendations for enhancing password security measures. These recommendations may include the adoption of stronger password policies, implementation of multi-factor authentication, and regular password audits.

Objectives:

1. **Identify Vulnerabilities:** Utilize John the Ripper to identify potential vulnerabilities in password security measures, including weak or easily guessable passwords.
2. **Assess Password Strength:** Evaluate the strength of passwords used within the target application or system by analyzing the effectiveness of password hashing and encryption techniques.
3. **Demonstrate Ethical Hacking Techniques:** Provide practical demonstrations of ethical hacking techniques using John the Ripper, empowering participants to apply these techniques in real-world scenarios.
4. **Enhance Cybersecurity Awareness:** Raise awareness about the importance of password security and the role of ethical hacking in strengthening cybersecurity defenses.
5. **Provide Actionable Recommendations:** Offer actionable recommendations for improving password security based on the findings of the ethical hacking exercise, thereby enhancing overall cybersecurity posture.

CHAPTER-3

ABOUT THE TOOL AND THE APPLICATION

John the Ripper is a renowned open-source password cracking tool utilized for ethical hacking purposes. It serves as a valuable asset in the cybersecurity arsenal, enabling security professionals to assess the strength of passwords and uncover vulnerabilities within systems and applications. Developed by Alexander Peslyak, also known as "Solar Designer," John the Ripper is available for various platforms, including Linux, Windows, and macOS, making it accessible to a wide range of users.

Key Features of John the Ripper:

- **Versatility:** John the Ripper supports a plethora of password cracking techniques, including dictionary attacks, brute-force attacks, and rainbow table attacks. Its flexibility allows security professionals to adapt their approach based on the target system's password hashing algorithms and encryption methods.
- **Speed and Efficiency:** With support for multi-core CPUs and GPU acceleration, John the Ripper can efficiently process large volumes of password hashes, significantly reducing the time required to crack passwords. This speed and efficiency make it an indispensable tool in time-sensitive ethical hacking scenarios.
- **Extensibility:** John the Ripper's modular architecture enables the integration of additional hash algorithms and custom wordlists, further enhancing its capabilities and adaptability to diverse environments. Security professionals can extend John the Ripper's functionality to accommodate unique requirements and challenges.
- **Community Support:** As an open-source project, John the Ripper benefits from a vibrant and active community of contributors and users. This community-driven development model fosters collaboration, innovation, and continuous improvement, ensuring that John the Ripper remains at the forefront of password cracking technology.

About the Chosen Application: Password-Protected RAR File

For the purpose of this case study, we have selected a password-protected RAR file as the target application for testing. RAR (Roshal Archive) is a popular file compression and archival format commonly used to store and transmit files securely. By encrypting RAR archives with passwords, users can protect sensitive information from unauthorized access.

It aims to demonstrate the effectiveness of tools like John the Ripper in evaluating the security posture of systems utilizing this archival format. Through comprehensive testing and analysis, security professionals can uncover vulnerabilities and implement remediation strategies to enhance the overall resilience of systems against unauthorized access and data breaches.

CHAPTER-4

TOOL INSTALLATION PROCEDURE

Prerequisites:

Internet Connection: Ensure that your system is connected to the internet to download necessary packages and dependencies.

Access Permissions: You may need administrative privileges (root access) to install packages and perform system-wide configurations.

Step 1: Update System Repositories:

Open a terminal window and run the following command to update the system repositories:

```
sudo apt update
```

Step 2: Install Dependencies:

John the Ripper may require certain dependencies to be installed on your system. Use the following command to install the necessary packages:

```
sudo apt install build-essential libssl-dev zlib1g-dev yasm pkg-config
```

Step 3: Download John the Ripper:

Navigate to the official John the Ripper GitHub repository to download the source code. You can either clone the repository using Git or download the source code archive directly from the repository page.

To clone the repository using Git, run the following command:

```
git clone https://github.com/magnumripper/JohnTheRipper.git
```

Step 4: Compile and Install John the Ripper:

Once the source code is downloaded, navigate to the directory containing the source code and compile John the Ripper using the following commands:

```
cd JohnTheRipper/src
```

```
./configure && make -s clean && make -sj4
```

Step 5: Verify Installation:

After the compilation is complete, you can verify the installation by running the following command:

```
./john --version
```

This command will display the version information of John the Ripper, confirming that the installation was successful.

CHAPTER-5

STEPS OF ETHICAL HACKING TOOL

JOHN THE RIPPER

STEP 1: Start by creating a text file containing a message or phrase that will serve as the target for the ethical hacking demonstration.

```
nano file.txt  
"The file has been successfully cracked!!"
```

STEP 2: Next, add the text file to a compressed archive (e.g., RAR format) along with other files to simulate a real-world scenario.

```
rar a case.rar file.txt
```

STEP 3: Verify the contents of the compressed archive using the cat command.

```
cat case.rar
```

STEP 4: Secure the compressed archive with a password using appropriate encryption techniques.

```
rar a -hpajaykumar case.rar file.txt
```

STEP 5: Extract the hashed representation of the password from the encrypted archive and save it to a file.

```
rar2john case.rar > casepass.hash
```

STEP 6: Confirm the contents of the generated hash file using the cat command.

```
cat casepass.hash
```

STEP 7: Utilize a password-cracking tool like John the Ripper to compare the hashed password against a wordlist (e.g., rockyou.txt) containing commonly used passwords and previously leaked credentials.

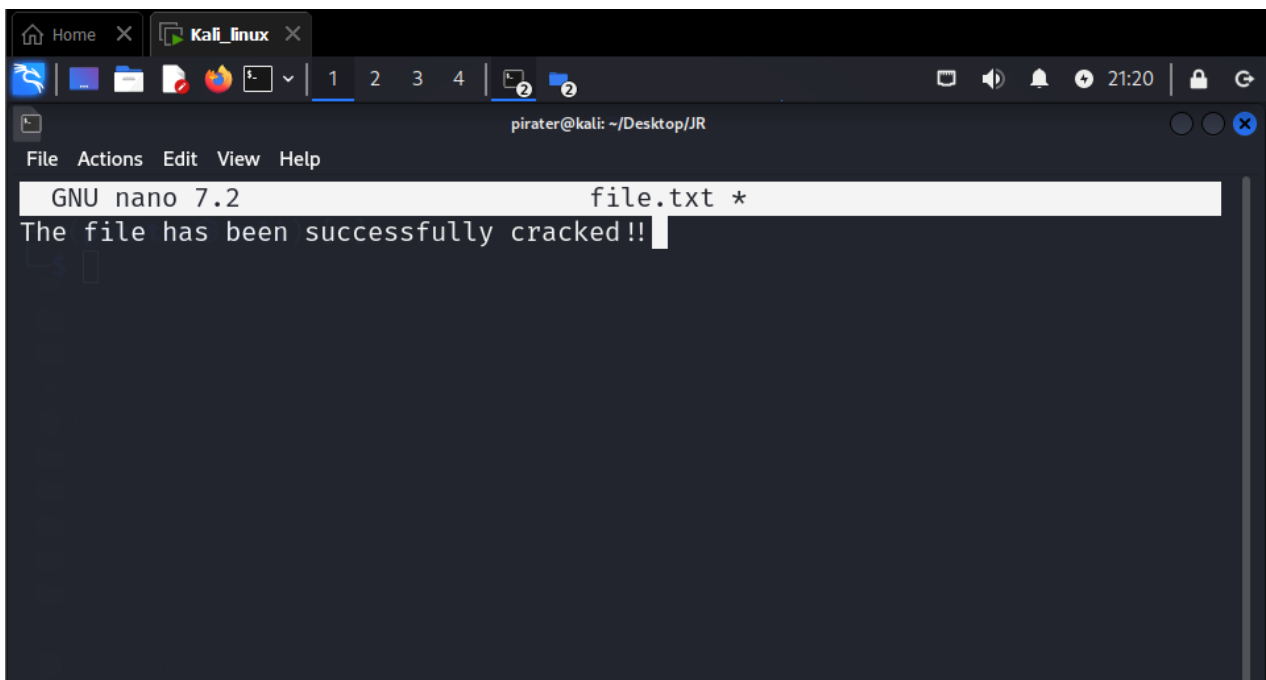
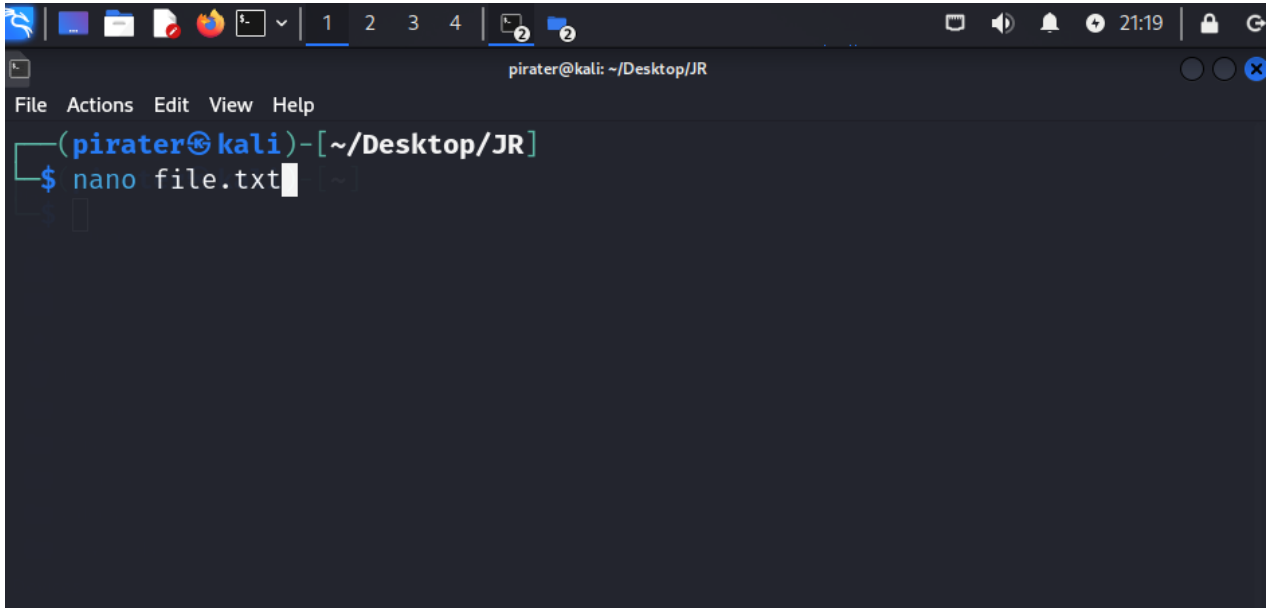
```
john --format=RAR5 --wordlist=rockyou.txt casepass.hash
```

STEP 8: Once the password is successfully identified, it can be used to unlock the encrypted archive.

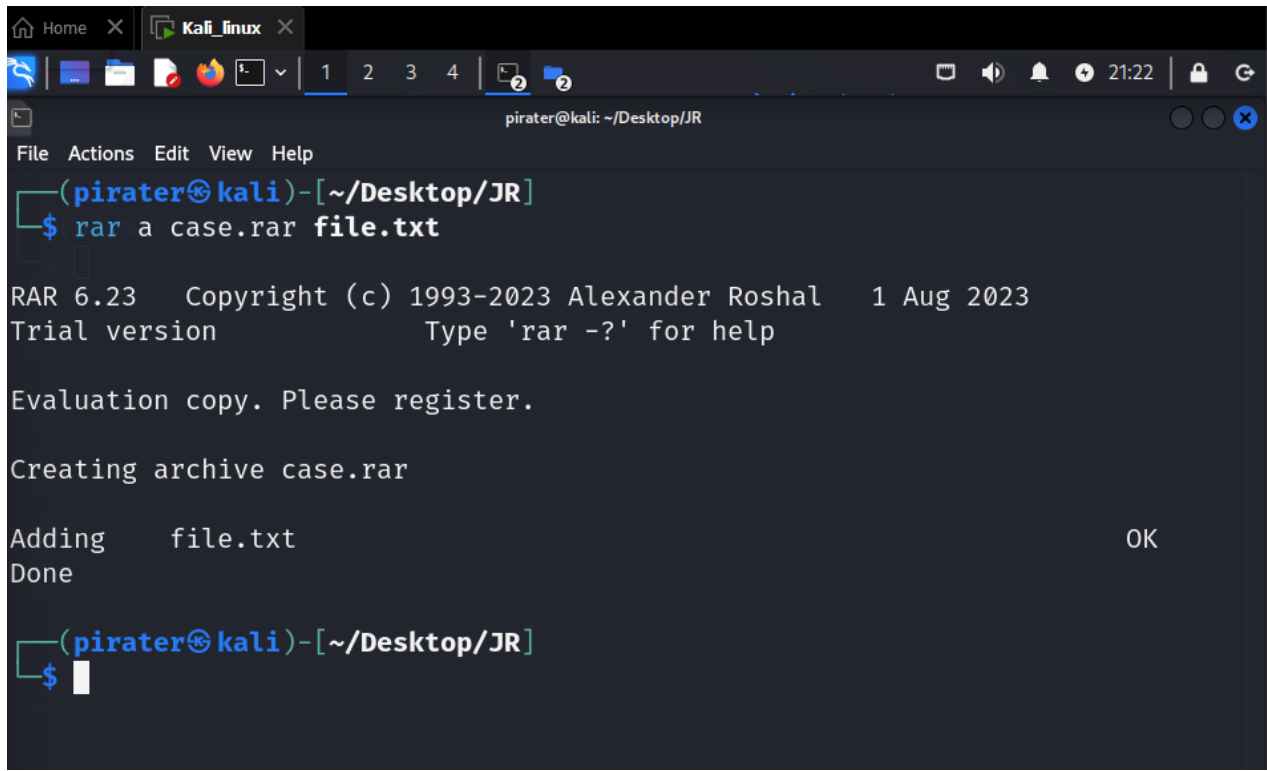
CHAPTER-6

SCREENSHOTS

Text Creation



Compression



A terminal window titled 'Kali_linux' with a tab for 'Home'. The prompt is 'pirater@kali: ~/Desktop/JR'. The user enters the command 'rar a case.rar file.txt'. The terminal displays the RAR 6.23 version information, including copyright (c) 1993-2023 Alexander Roshal, dated 1 Aug 2023, and a trial version notice. It then shows 'Creating archive case.rar' and 'Adding file.txt' with an 'OK' status.

```
pirater@kali: ~/Desktop/JR
File Actions Edit View Help
(pirater@kali)-[~/Desktop/JR]
$ rar a case.rar file.txt

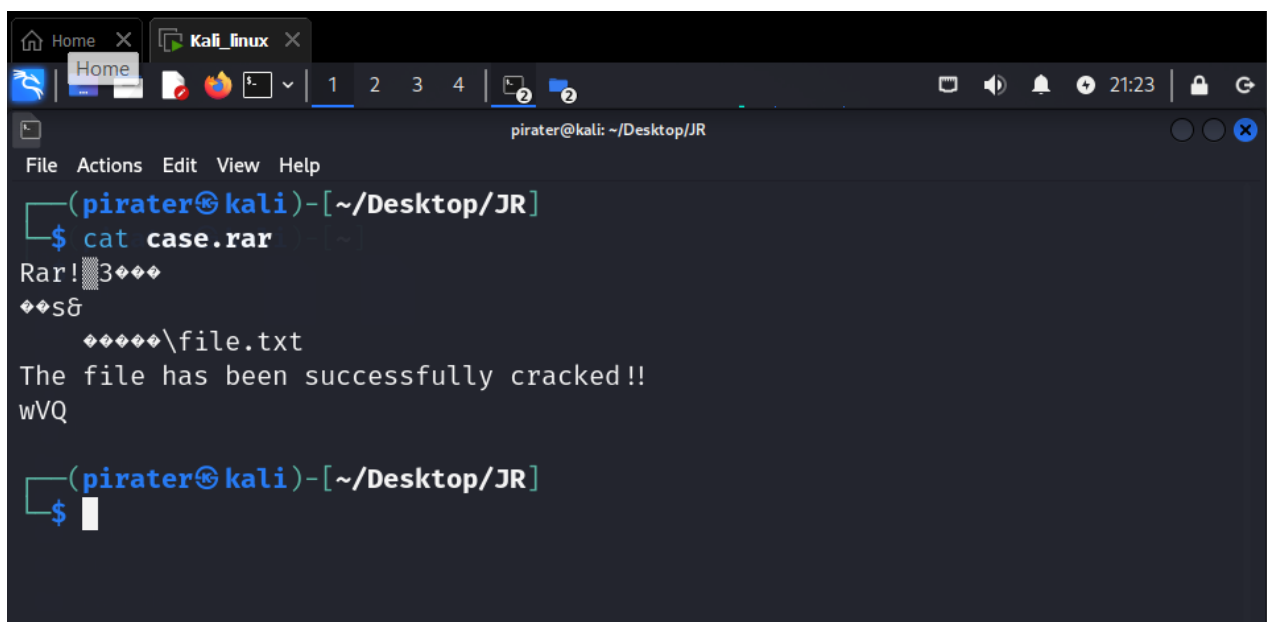
RAR 6.23 Copyright (c) 1993-2023 Alexander Roshal 1 Aug 2023
Trial version Type 'rar -?' for help

Evaluation copy. Please register.

Creating archive case.rar

Adding file.txt OK
Done

(pirater@kali)-[~/Desktop/JR]
$
```



A terminal window titled 'Kali_linux' with a tab for 'Home'. The prompt is 'pirater@kali: ~/Desktop/JR'. The user enters the command 'cat case.rar'. The terminal displays a RAR! error message, followed by a successful extraction message: 'The file has been successfully cracked!!'. The user then enters a command to view the contents of the archive, which shows 'file.txt'.

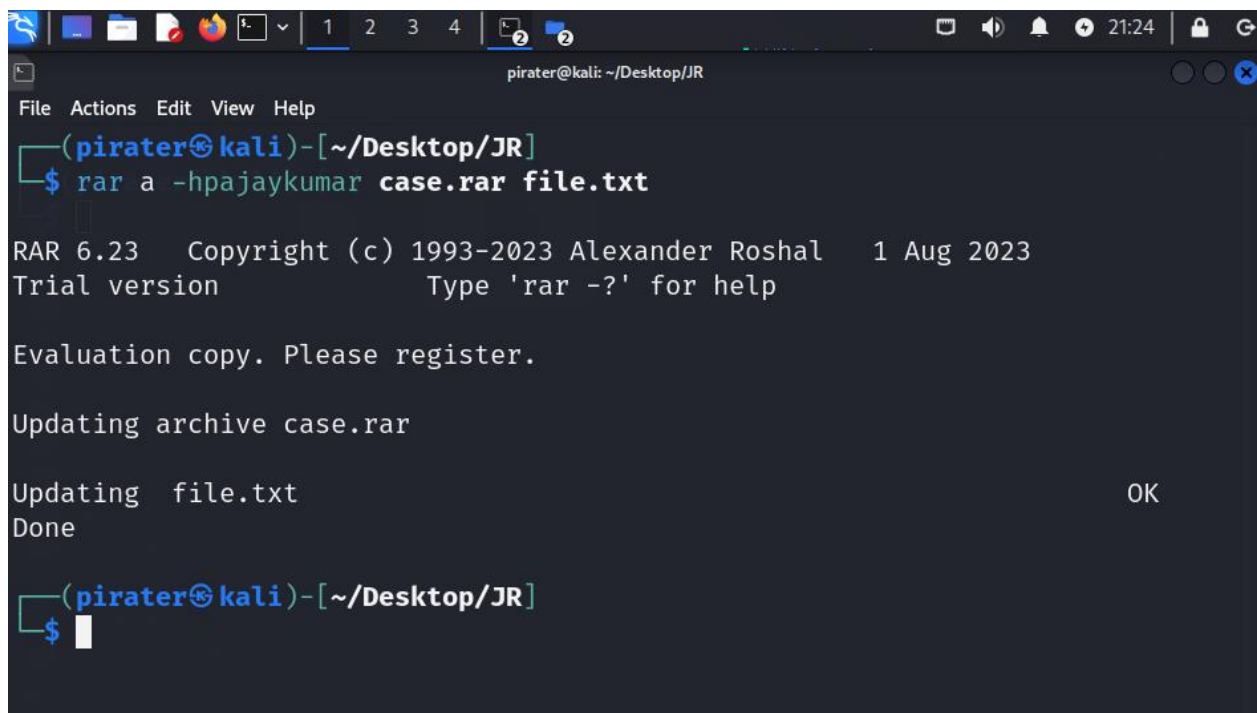
```
pirater@kali: ~/Desktop/JR
File Actions Edit View Help
(pirater@kali)-[~/Desktop/JR]
$ cat case.rar

Rar! 3
s
\file.txt

The file has been successfully cracked!!
wVQ

(pirater@kali)-[~/Desktop/JR]
$
```

Password Protection



A terminal window titled 'pirater@kali: ~/Desktop/JR' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(pirater@kali)-[~/Desktop/JR]'. The command '\$ rar a -hpajaykumar case.rar file.txt' is entered. The output shows 'RAR 6.23 Copyright (c) 1993-2023 Alexander Roshal 1 Aug 2023 Trial version Type 'rar -?' for help Evaluation copy. Please register. Updating archive case.rar Updating file.txt Done'. An 'OK' dialog box is visible on the right.

```
(pirater@kali)-[~/Desktop/JR]
$ rar a -hpajaykumar case.rar file.txt

RAR 6.23 Copyright (c) 1993-2023 Alexander Roshal 1 Aug 2023
Trial version Type 'rar -?' for help

Evaluation copy. Please register.

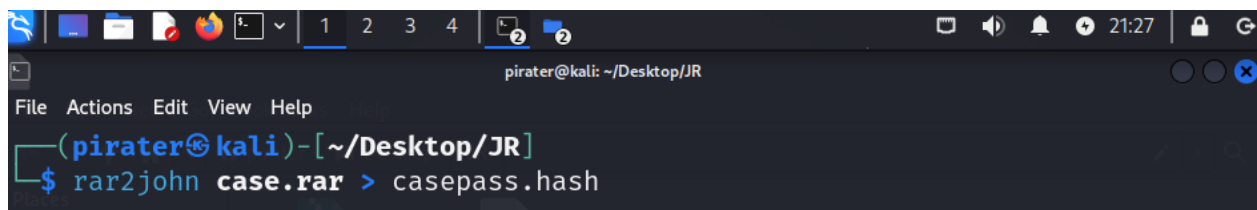
Updating archive case.rar

Updating file.txt
Done

OK

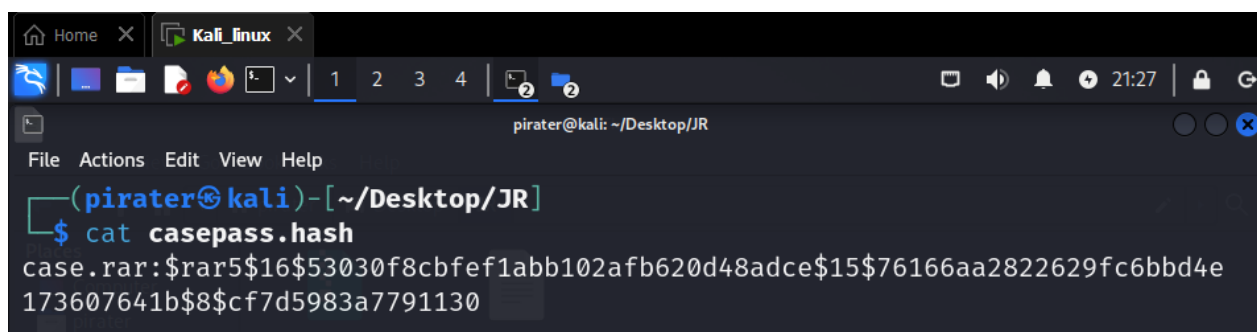
(pirater@kali)-[~/Desktop/JR]
$
```

Hash Extraction



A terminal window titled 'pirater@kali: ~/Desktop/JR' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(pirater@kali)-[~/Desktop/JR]'. The command '\$ rar2john case.rar > casepass.hash' is entered.

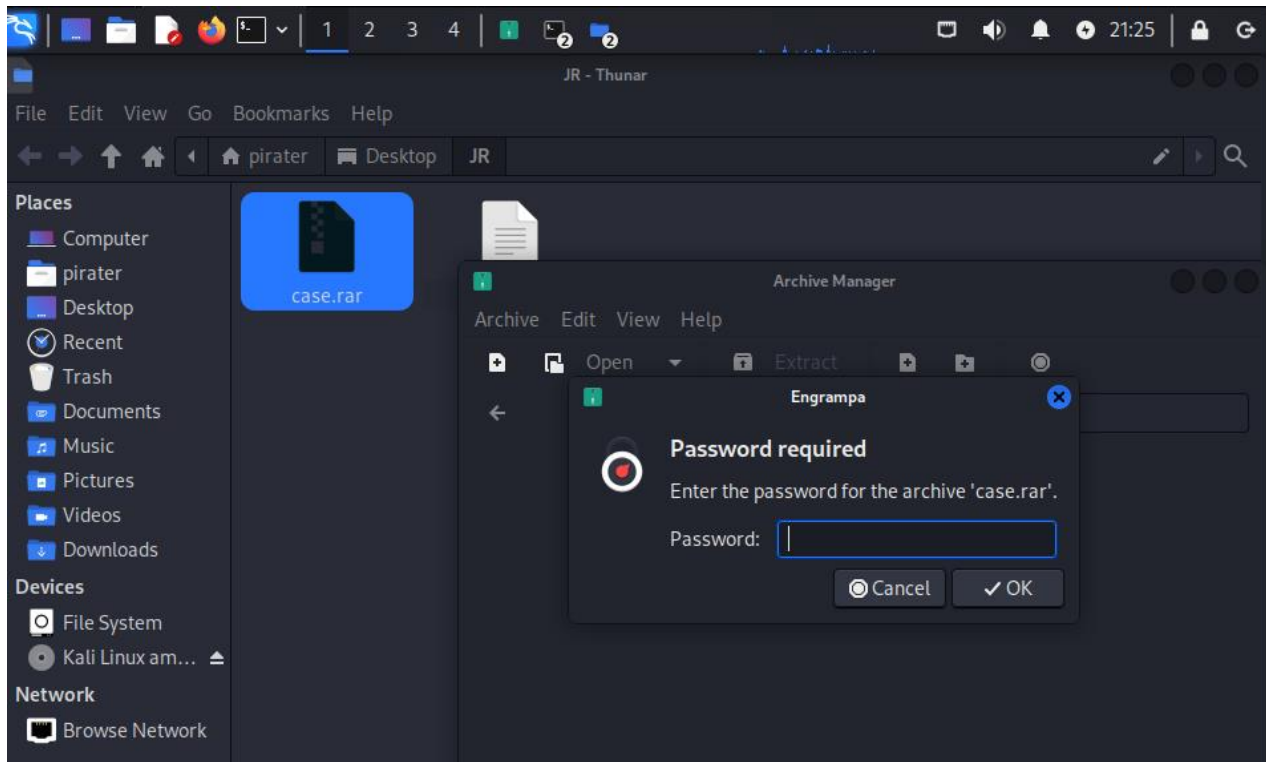
```
(pirater@kali)-[~/Desktop/JR]
$ rar2john case.rar > casepass.hash
```



A terminal window titled 'pirater@kali: ~/Desktop/JR' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(pirater@kali)-[~/Desktop/JR]'. The command '\$ cat casepass.hash' is entered. The output is a long alphanumeric string.

```
(pirater@kali)-[~/Desktop/JR]
$ cat casepass.hash
case.rar:$rar5$16$53030f8cbfef1abb102afb620d48adce$15$76166aa2822629fc6bbd4e
173607641b$8$cf7d5983a7791130
```

Checking

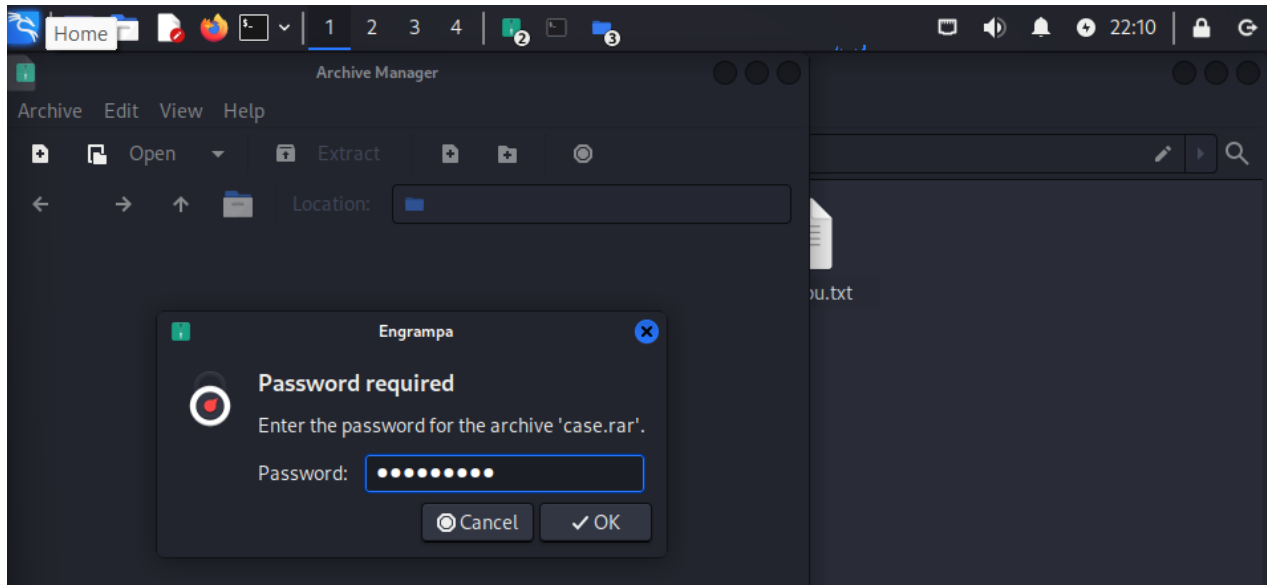


Password Cracking

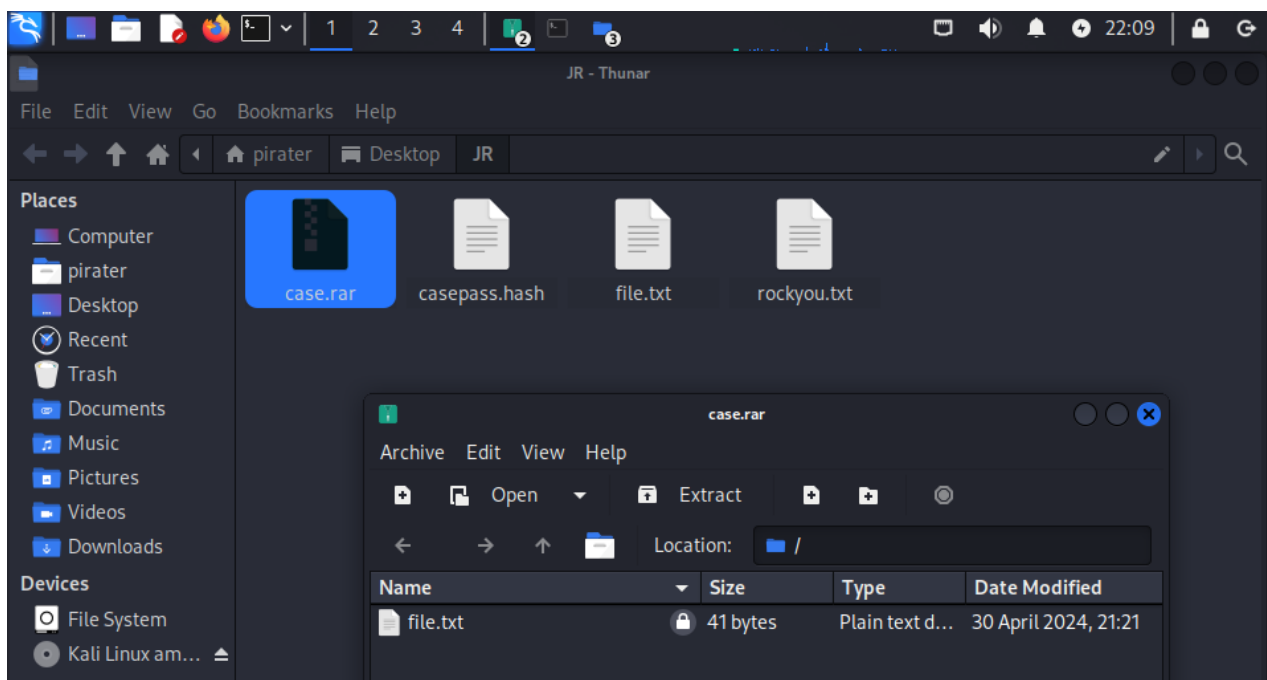
```
pirater@kali: ~/Desktop/JR
File Actions Edit View Help
(pirater@kali)-[~/Desktop/JR]
$ john --format=RAR5 --wordlist=rockyou.txt casepass.hash

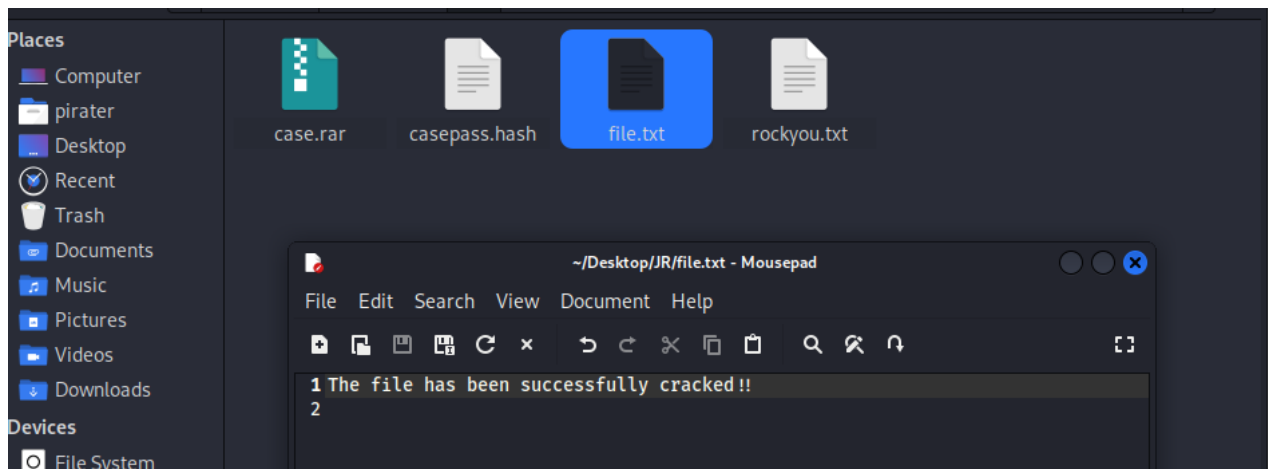
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ajaykumar (case.rar)
1g 0:00:00:00 DONE (2024-04-30 22:07) 2.127g/s 817.0p/s 817.0c/s 817.0C/s 12
3456..sabrina
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Testing

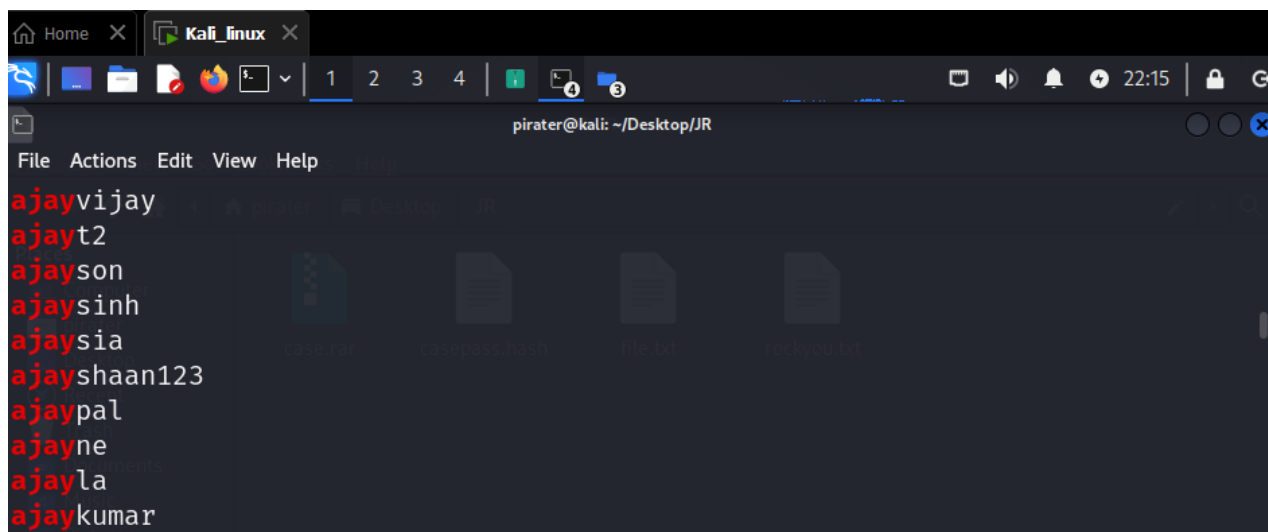
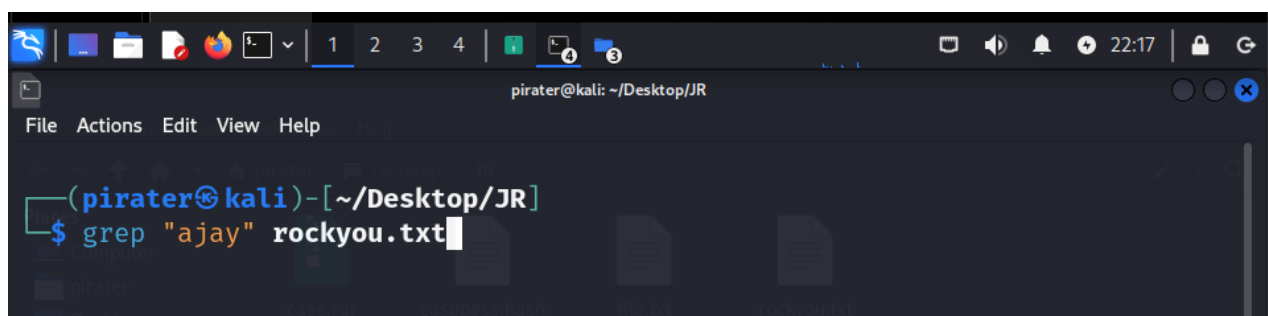


Successful





List of names already in wordlist



CHAPTER-7

CONCLUSION

In this project, we embarked on an ethical hacking journey using John the Ripper to assess password security measures and identify vulnerabilities within a password-protected RAR file. Through a systematic approach, we outlined the steps involved in the ethical hacking process, from identifying the target to analyzing the results and interpreting the findings.

By leveraging John the Ripper's powerful password cracking capabilities, we were able to effectively extract the hash of the password from the target RAR file and subsequently crack the password using a wordlist. This process provided valuable insights into the strength of the password and the effectiveness of password security measures implemented within the target system.

The findings of our ethical hacking exercise underscore the importance of robust password management practices in safeguarding sensitive information against unauthorized access. Weak or easily guessable passwords pose significant security risks and can serve as entry points for malicious actors seeking to exploit vulnerabilities in password security measures.

Moving forward, organizations and individuals must prioritize password security as a fundamental aspect of cybersecurity. This entails adopting strong password policies, implementing multi-factor authentication, and conducting regular password audits to identify and mitigate potential weaknesses.

Furthermore, ethical hacking exercises like the one conducted in this project play a crucial role in raising awareness about cybersecurity threats and enhancing cyber resilience. By proactively identifying and addressing vulnerabilities, organizations can strengthen their defenses and mitigate the risk of data breaches and cyber attacks.

Ethical hacking using tools like John the Ripper serves as a valuable strategy for assessing and improving password security measures. Through continuous vigilance, education, and collaboration, we can fortify our digital defenses and create a safer online environment for individuals and organizations alike.

CHAPTER-8

REFERENCES

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

<https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/>

<https://www.kali.org/tools/john/>

<https://www.esecurityplanet.com/products/john-the-ripper/>

