Project Report

**Title: John the Ripper Password Cracking – Decrypting a Password-Protected File Using RockYou Wordlist**

Submitted By: Manash Choudhury

Course: Cybersecurity

**1. Introduction**

John the Ripper (JtR) is one of the most popular open-source password-cracking tools used in cybersecurity. In this project, we focus on decrypting a password-protected ZIP file using John the Ripper and the well-known rockyou.txt wordlist. This demonstrates how weak passwords can be cracked using dictionary attacks, reinforcing the importance of secure password policies.

**2. Tools and Environment**

* Operating System: Kali Linux
* Password Cracking Tool: John the Ripper
* Wordlist: /usr/share/wordlists/rockyou.txt
* Target: Password-protected ZIP file

**3. Objective**

To decrypt a password-protected file using John the Ripper and the RockYou wordlist, simulating a dictionary attack on a ZIP archive.

**4. Procedure**

**Step 1:** Prepare the Environment

Ensure the RockYou wordlist is extracted:



**Step 2**: Create a Password-Protected ZIP (for testing)



Enter a weak password like: 12345

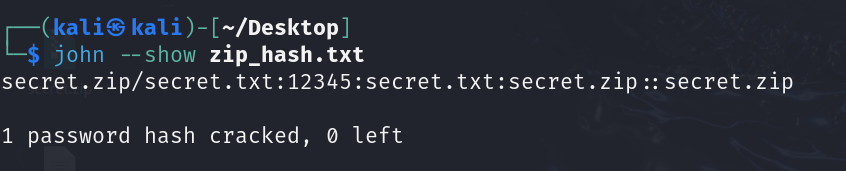
**Step 3**: Convert ZIP File to a Hash Format

Use zip2john to extract the hash: 

**Step 4**: Start Cracking with John the Ripper



**Step 5**: View the Cracked Password



**5. Results and Analysis**

File Name Cracked Password Time Taken Wordlist Used

secret.zip 12345 Few seconds rockyou.txt

The password was successfully recovered using the dictionary attack.

**6. Learnings**

* John the Ripper is extremely powerful for offline password attacks.
* Dictionary attacks are highly effective against common and weak passwords.
* Wordlists like RockYou contain real-world leaked passwords, making them dangerous if users use predictable patterns.
* Always enforce strong, unique passwords and avoid dictionary-based choices.

**7. Ethical Considerations**

* This project was performed in a safe and isolated environment.
* No real user data or unauthorized access was involved.
* The goal is educational awareness on password security.

**8. Conclusion**

This project successfully demonstrated how a password-protected file can be decrypted using John the Ripper and a dictionary attack with RockYou. It underlines the critical need for using secure and complex passwords in real-world scenarios.