Password Cracking Report Using John the Ripper and Hashcat

Ankush Uday Naik

December 15, 2025

Abstract

This report presents a practical demonstration of password cracking techniques using John the Ripper and Hashcat on a password-protected ZIP archive. The experiment highlights how weak passwords can be compromised using dictionary-based attacks. A ZIP archive was created with a password, its hash was extracted using John the Ripper, and the password was successfully cracked using Hashcat with the RockYou wordlist. The task was performed in a controlled Kali Linux environment for educational purposes only.

Objective

The objective of this experiment is to demonstrate the vulnerability of password-protected ZIP files when weak passwords are used and to analyze the effectiveness of John the Ripper and Hashcat in recovering such passwords.

Tools and Environment

The experiment was conducted on Kali Linux. John the Ripper was used to extract password hashes from the ZIP archive, while Hashcat was used to perform high-speed dictionary-based password cracking. The RockYou wordlist was used as the password dictionary.

Methodology

The experiment was carried out in multiple stages including ZIP file creation, hash extraction, password cracking, and verification of the cracked password. Each step is explained

in detail with supporting screenshots.

1 Creating a Password-Protected ZIP File

A folder named `secret_folder` was created and compressed into a ZIP archive with password protection. This simulates a real-world scenario where users protect sensitive files using archive encryption.

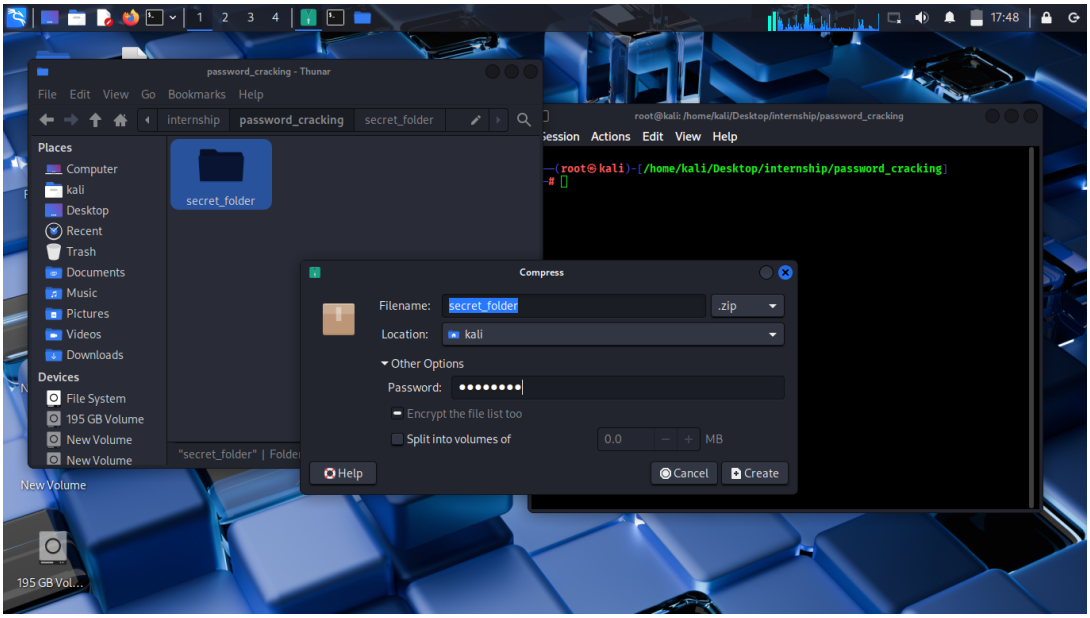

Figure 1: Creating a ZIP folder with password

The archive utility prompts for a password during compression, confirming that encryption is enabled.

2 Extracting ZIP Hash Using John the Ripper

The `zip2john` utility was used to extract the cryptographic hash from the ZIP file. This hash is required for offline password cracking.

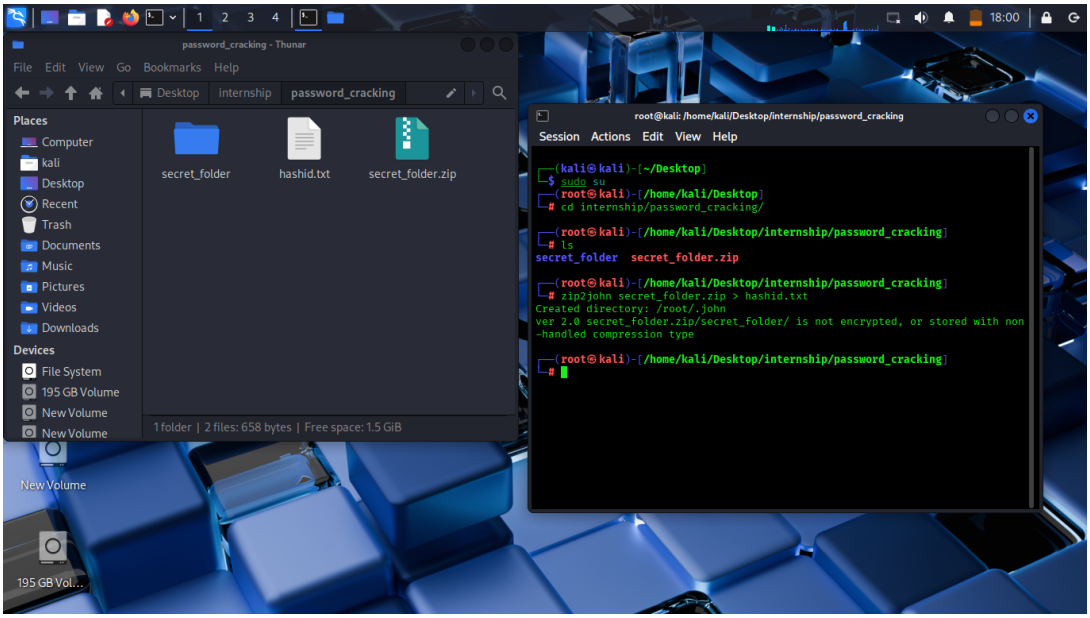

Figure 2: Extracting ZIP hash using zip2john

The extracted hash was saved into a file named `hashid.txt`.

3 Preparing the Hash File

The extracted hash file was reviewed and modified to ensure compatibility with Hashcat. Unnecessary metadata was removed, leaving only the valid ZIP hash entry.

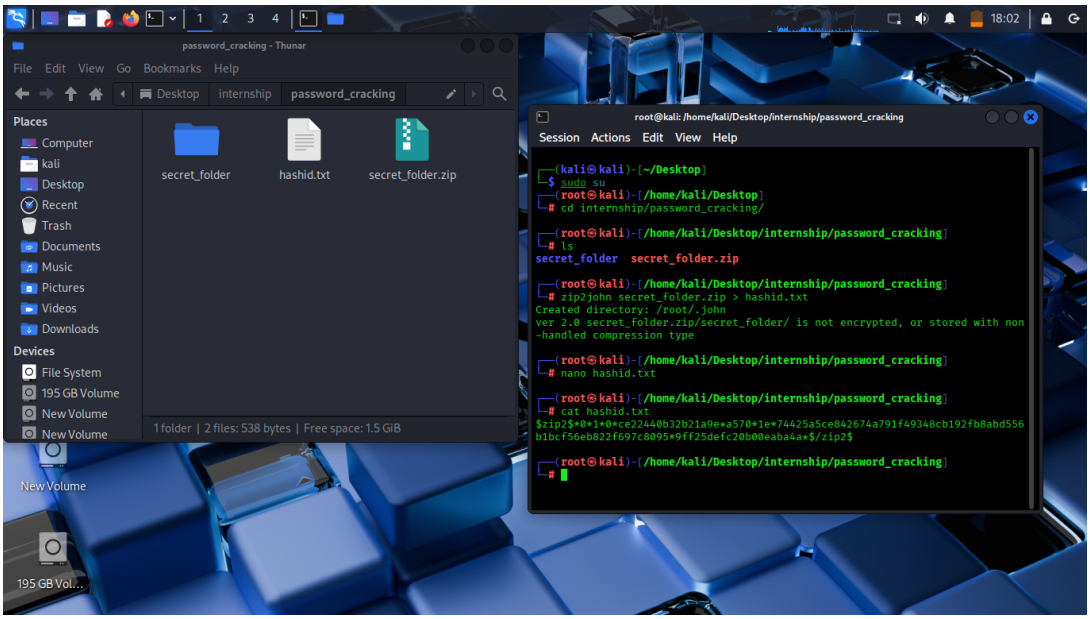

Figure 3: Modified hash file for password cracking

4 Password Cracking Using Hashcat

Hashcat was executed using ZIP hash mode `13600` along with the RockYou wordlist. A dictionary attack was performed to test commonly used passwords.

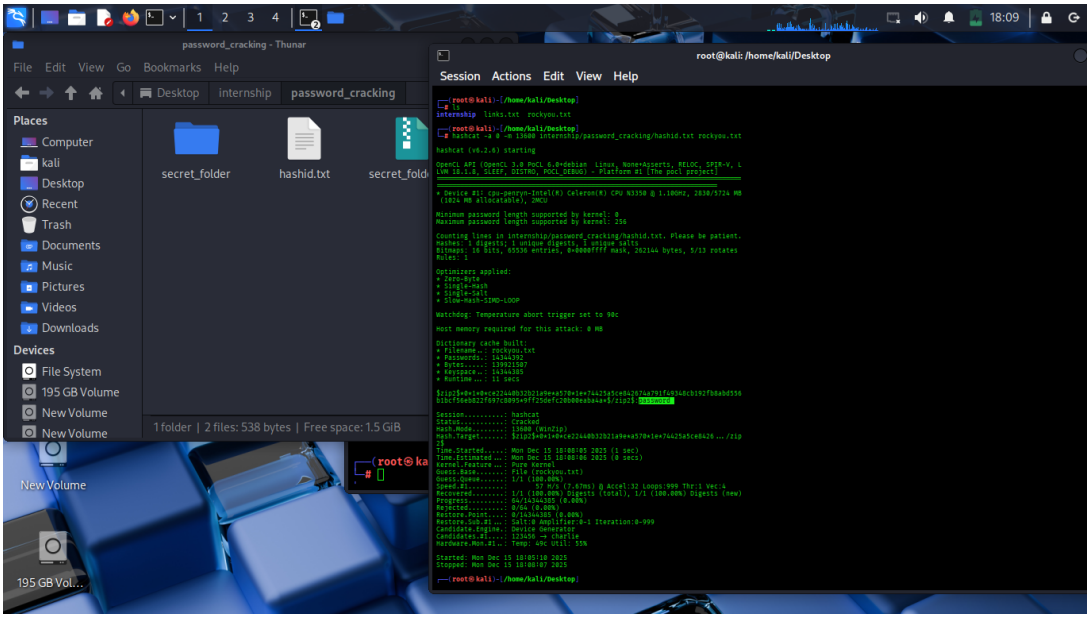

Figure 4: Hashcat cracking ZIP password using RockYou wordlist

The output indicates that the password was successfully cracked, and the status is shown as *Cracked*.

5 Use of RockYou Wordlist

The RockYou wordlist contains millions of leaked real-world passwords and is highly effective against weak password policies.

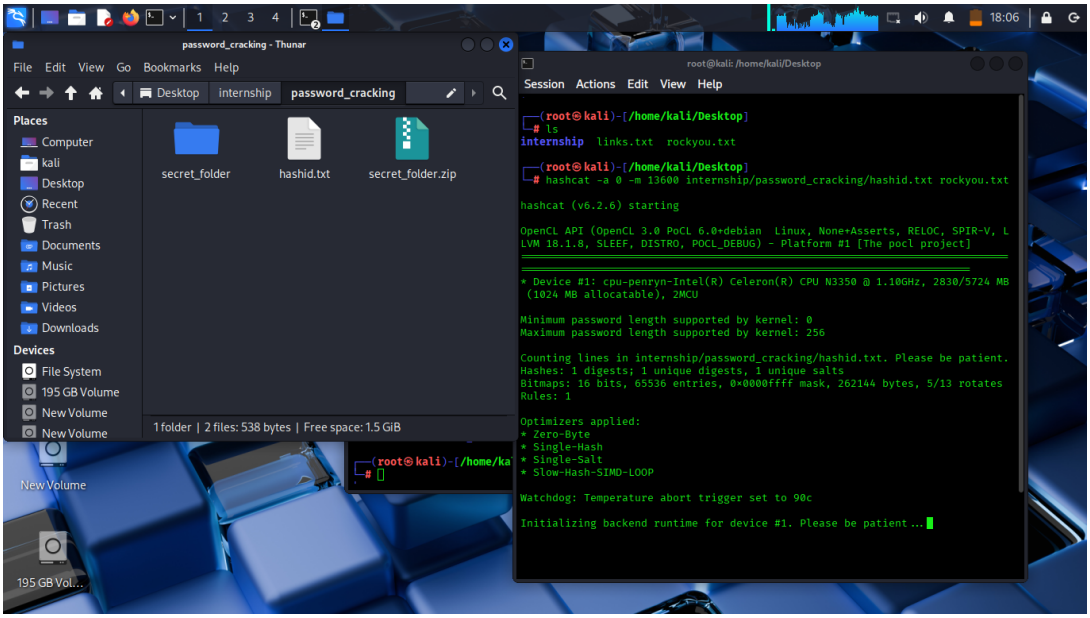

Figure 5: RockYou wordlist used for dictionary attack

This demonstrates how easily predictable passwords can be compromised.

6 Verification of Cracked Password

After cracking the password, the ZIP file was opened using the recovered password to verify its correctness.

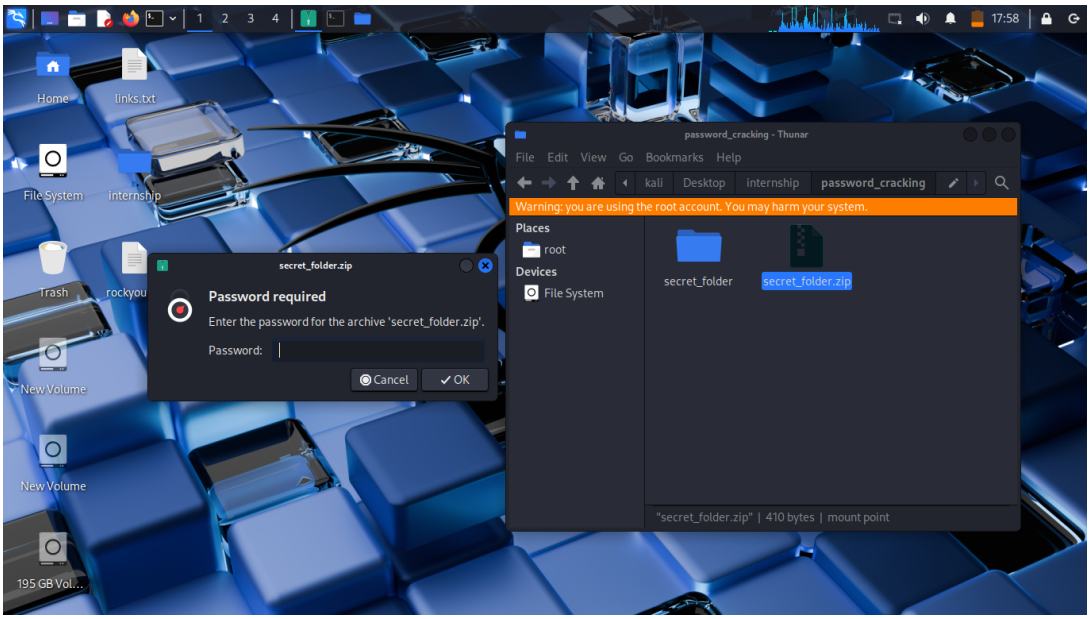

Figure 6: ZIP file prompting for password during extraction

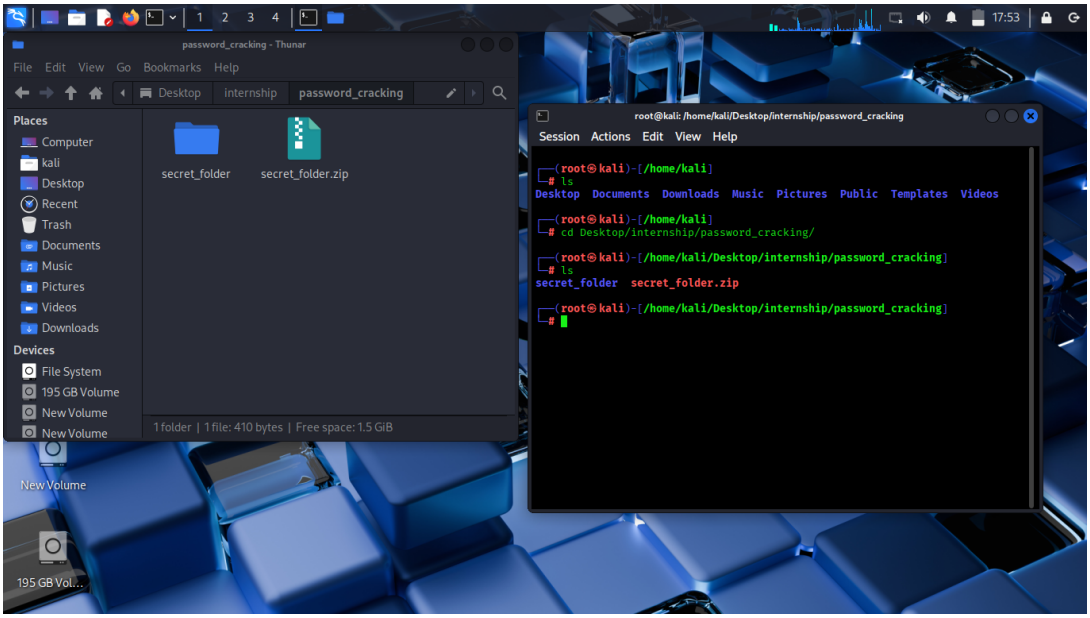

Figure 7: Successful extraction of ZIP file using cracked password

The successful extraction confirms that the cracked password is valid.

Results and Analysis

The experiment clearly demonstrates that ZIP files protected with weak passwords are vulnerable to dictionary attacks. John the Ripper effectively extracted the hash, while Hashcat efficiently cracked the password using optimized algorithms. The RockYou wordlist significantly reduced cracking time.

Security Implications

This experiment highlights the importance of strong password policies. Weak passwords can be easily cracked using readily available tools and publicly leaked wordlists. Users should employ complex passwords and additional encryption mechanisms to protect sensitive data.

Conclusion

The password cracking task was successfully completed using John the Ripper and Hashcat. The results emphasize that password strength plays a critical role in data security. Weak passwords provide minimal resistance against modern cracking tools, making strong password practices essential.

Ethical Disclaimer

All activities performed in this experiment were conducted in a controlled environment for academic and educational purposes only. Unauthorized password cracking is illegal and unethical.