Cryptography Challenge with Hashcat - Detailed Summary

This project focuses on practical applications of cryptography and password-cracking techniques using tools like Hashcat and John the Ripper. It simulates scenarios where penetration testers or forensic analysts encounter encrypted files. Below is a comprehensive breakdown of the steps, tools, and methods used in the project.

Objective

To crack the passwords of a ZIP file and a PDF file using Hashcat and other supporting tools.

Tools and Setup

1. **John the Ripper**: Used to identify the hash of the ZIP and PDF files.
2. **Hashcat**: Used to crack the hashes and decode the passwords.
3. **Perl Strawberry Perl**: Used for processing the hash of the PDF file.
4. **Notepad++**: For fixing UTF encoding issues.
5. **rockyou.txt Wordlist**: A commonly used wordlist for password cracking.
6. **ZIP File**: Downloaded from the provided Google Drive link.
7. **Environment**: Configured all tools in a Windows environment.

Steps to Complete the Project

Step 1: Initial Setup

1. Download and install the required tools:
    a. John the Ripper
    b. Hashcat
    c. Perl Strawberry Perl
    d. Notepad++
2. Download the password-protected ZIP file from the provided link.
3. Place all tools and the rockyou.txt wordlist in the appropriate directories.
4. Configure the Windows environment for seamless execution.

Step 2: Cracking the ZIP File Password

1. **Identify the Hash**
    a. Use John the Ripper to extract the hash of the ZIP file: `zip2john.exe filename.zip > hash.txt`

    b. Save the extracted hash in a file named `hash.txt` inside the Hashcat folder.
2. **Determine the Hash Mode**
    a. Match the hash format from the Hashcat Example Hashes page.
    b. The hash mode for ZIP files is identified as **13600**.
3. **Crack the Password**
    a. Use Hashcat with the following command: `hashcat.exe -a 0 -m 13600 hash.txt rockyou.txt --force`

    b. Hashcat processes the hash using the rockyou.txt wordlist and reveals the password after a few minutes.

Step 3: Cracking the PDF File Password

1. **Identify the Hash**
    a. Use Perl with John the Ripper to extract the hash of the PDF file: `perl pdf2john.pl filename.pdf > hash.txt`

    b. Save the hash in a file named `hash.txt` inside the Hashcat folder.
2. **Determine the Hash Mode**
    a. Match the hash format from the Hashcat Example Hashes page.
    b. The hash mode for PDF files is identified as **10500**.
3. **Crack the Password**
    a. Use Hashcat with the following command: `hashcat.exe -a 0 -m 10500 hash.txt rockyou.txt --force`

    b. Hashcat processes the hash using the rockyou.txt wordlist and reveals the password after a short time.

Summary of Commands

ZIP File

- Identify hash: `zip2john.exe filename.zip > hash.txt`
- Crack password: `hashcat.exe -a 0 -m 13600 hash.txt rockyou.txt --force`

PDF File

- Identify hash: `perl pdf2john.pl filename.pdf > hash.txt`
- Crack password: `hashcat.exe -a 0 -m 10500 hash.txt rockyou.txt --force`

Outcome

- Successfully cracked the password of the ZIP file and extracted the password-protected PDF file.
- Using the same methodology, successfully cracked the password of the PDF file.

This project demonstrates the effective use of cryptographic tools and techniques, showcasing their importance in cybersecurity and forensic analysis.