InSkill-5

Step 1: Install John the Ripper

1. **Linux Installation**:
   - If you are using a Linux distribution like Kali Linux, John the Ripper is usually pre-installed.
   - If not, install it using:

     ```
     sudo apt-get install john
     ```

2. **Windows Installation**:
   - Download John the Ripper from the official website.
   - Extract the contents and navigate to the installation directory using the command prompt.

Step 2: Extract the Hash from the ZIP File

John the Ripper needs the password hash to perform the cracking. To extract the hash from the ZIP file:

1. **Use `zip2john` to Extract the Hash**:
   - `zip2john` is a utility that comes with John the Ripper and is used to extract the password hash from a ZIP file.
   - Run the following command in the terminal:

     ```
     zip2john yourfile.zip > hash.txt
     ```

   - Replace `yourfile.zip` with the actual name of the ZIP file.
   - This command will output the hash to a file called `hash.txt`.

Step 3: Crack the Password Using John the Ripper

1. **Use John to Crack the Password**:
   - Now that you have the hash, use John the Ripper to crack it:

     ```
     john hash.txt
     ```

   - John will start attempting to crack the password using its default wordlist and methods.
2. **View the Cracked Password**:
   - If John successfully cracks the password, it will display it on the screen.
   - You can also view it later by running:

     ```
     john --show hash.txt
     ```

Step 4: Access the ZIP File

1. **Use the Recovered Password**:

- Once the password is recovered, use it to unzip the file:

  ```
  unzip yourfile.zip
  ```

- Enter the cracked password when prompted.