PostSkill Task:-

1. Security Auditing

Objective: Assess the strength of password hashes and identify weak passwords.

Steps:

1. **Install John the Ripper**: Download and install John the Ripper from its official website.
2. **Prepare Password Hashes**: Obtain password hashes in a format supported by John the Ripper (e.g., MD5, SHA-1).
3. **Run John the Ripper**: Use the following command to start the audit:

   ```
   john --format=<hash_format> <hash_file>
   ```

   Replace `<hash_format>` with the hash type (e.g., `raw-md5`, `sha256crypt`) and `<hash_file>` with the file containing the hashes.

4. **Analyze Results**: Review the output for cracked passwords and assess the strength of the passwords used.

---

2. Penetration Testing

Objective: Test the security of systems by attempting to crack password hashes.

Steps:

1. **Install John the Ripper**: Ensure the latest version is installed.
2. **Obtain Password Hashes**: Extract password hashes from the target system (ensure legal authorization).
3. **Choose an Attack Mode**: Depending on the complexity, select a suitable attack mode (e.g., dictionary attack, brute force).
4. **Execute the Attack**:
   - For a dictionary attack:

     ```
     john --wordlist=<wordlist_file> --format=<hash_format>
     <hash_file>
     ```

   - For a brute-force attack:

     ```
     john --incremental --format=<hash_format> <hash_file>
     ```

5. **Review Results**: Check which passwords were cracked and assess the system's vulnerability.

---

3. Password Recovery

Objective: Recover lost or forgotten passwords by cracking password hashes.

Steps:

1. **Install John the Ripper**: Install and ensure it's up-to-date.
2. **Prepare the Hash File**: Obtain the file containing the password hashes to recover.
3. **Select a Cracking Mode**: Choose between dictionary, brute-force, or hybrid attack based on the expected password complexity.
4. **Run the Cracking Command**:
    - For a dictionary attack:

      ```
      john --wordlist=<wordlist_file> --format=<hash_format>
      <hash_file>
      ```

    - For a brute-force attack:

      ```
      john --incremental --format=<hash_format> <hash_file>
      ```

5. **Recover Passwords**: Check the output for recovered passwords.