Pre-Skill Task:

1.**What is password cracking, and why is it important from a security perspective?**

Password cracking is the process of deciphering encrypted passwords to access systems. It's important for identifying weak passwords and enhancing security measures.

2.**Explain the working principle of John the Ripper.**

John the Ripper attempts to crack passwords by comparing hashed values against generated plaintext passwords using various algorithms and attack methods.

3.**What are the different types of password cracking techniques supported by John the Ripper?**

Techniques include brute force (trying all combinations), dictionary attacks (using word lists), hybrid attacks (dictionary plus patterns), and rule-based attacks (modifying dictionary entries).

4.**How does a dictionary attack work, and what are its limitations?**

A dictionary attack uses a list of common passwords to guess the correct one. Limitations include its reliance on pre-defined words, which may not cover complex or unique passwords.

5.**Describe the process of configuring John the Ripper for password cracking.**

Install John the Ripper, prepare password hashes, select and configure attack modes, run the tool with appropriate commands, and monitor the progress and results.

Viva questions:

1.**What are the commonly used password hash formats supported by John the Ripper?**

Common formats include MD5, SHA-1, SHA-256, SHA-512, and NTLM. John the Ripper supports various other formats and can handle custom hash types.

2.**How does John the Ripper handle salted password hashes?**

John the Ripper processes salted hashes by incorporating the salt into the cracking process, ensuring that each attempt accounts for the unique salt value used in the hash.

3.**What is the difference between a brute-force attack and a dictionary attack?**

A brute-force attack tries all possible combinations of characters, while a dictionary attack uses a predefined list of common passwords or words.

4.**Explain the concept of a hybrid attack and its advantages over other cracking techniques.**

A hybrid attack combines dictionary words with additional modifications (e.g., appending numbers or special characters). It is advantageous because it targets common variations of passwords not covered by simple dictionary attacks.

5.**What are the countermeasures that can be taken to defend against password cracking?**

Use strong, complex passwords with a mix of characters, implement multi-factor authentication, and employ password hashing with strong algorithms and salts to increase resistance to cracking attempts.