Comprehensive Tutorial on John the Ripper in Kali Linux

Introduction

John the Ripper (JtR) is a powerful open-source password cracking tool used primarily for password security testing. It supports numerous encryption formats and password hash types, making it an essential tool for ethical hacking and penetration testing. Kali Linux includes John the Ripper by default, along with various useful scripts and extensions.

Key Concepts and Definitions

1. **Password Hash**
   A password hash is a cryptographic representation of a password. John the Ripper works by attempting to guess the password that, when hashed, matches the stored hash.
2. **Cracking Modes**
   - **Single Crack Mode**: Uses information about the user (username, home directory, etc.) to generate guesses.
   - **Wordlist Mode**: Utilizes a predefined list of possible passwords (wordlist).
   - **Incremental Mode**: Attempts all possible password combinations based on character sets.
   - **External Mode**: Custom modes defined by the user using scripts.
3. **Wordlist**
   A file containing potential passwords. Wordlists are commonly used for brute-force attacks and are available in /usr/share/wordlists in Kali Linux.
4. **Rule-Based Attacks**
   Allows modifications to wordlist entries, like appending numbers, reversing words, or leetspeak transformations.
5. **Format**
   Specifies the type of hash (e.g., MD5, SHA-1, bcrypt) John is attempting to crack.

Setting Up John the Ripper

1. **Install John the Ripper**
   If not already installed, use:

```
sudo apt update

sudo apt install john
```

2. **Verify Installation**
   Check if John is installed:

```
john --help
```

Using John the Ripper

1. **Identify Hash Type**
   Use the hashid tool in Kali to identify the type of a given hash:

```
echo "yourhashhere" | hashid
```

2. **Basic Usage**
   a. Prepare a hash file containing the password hash.
   Example: Create hash.txt with a sample hash.
   b. Run John on the hash:

```
john hash.txt
```

3. **Wordlist Mode**
   Specify a wordlist for cracking:

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

4. **Incremental Mode**
   Use incremental mode for brute-forcing:

```
john --incremental hash.txt
```

5. **Show Cracked Passwords**
   Display already cracked passwords:

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

Practical Examples

1. **Cracking a Linux Password Hash**
   Extract hashes from /etc/shadow using unshadow:

```
unshadow /etc/passwd /etc/shadow > hash.txt
```

```
john hash.txt
```

2. **Cracking Zip File Passwords**
   Use the zip2john utility:

```
zip2john file.zip > hash.txt
```

```
john hash.txt
```