Password Cracking with John the Ripper

Objective:

To familiarize the intern with password cracking techniques and tools.

Introduction:

John the Ripper, commonly referred to as **John**, is one of the most popular and widely-used open-source password cracking tools available today. Originally developed for Unix-based systems, John the Ripper has evolved into a powerful and versatile tool that can operate on a variety of operating systems including Linux, macOS, and Windows.

John the Ripper is primarily used by security professionals and system administrators to test the strength of passwords and identify weak password policies. However, its functionality extends far beyond simple password cracking; it supports a vast array of cryptographic hash types, such as DES, MD5, SHA-1, bcrypt, and more. This flexibility makes John the Ripper suitable for cracking not only operating system passwords but also database passwords, compressed files, and more.

Install John the Ripper:

First, you need to install John the Ripper. Depending on your operating system, you can use the following commands:

- **For Debian/Ubuntu:**

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

- **For macOS:**

  ```
  brew install john
  ```

- **For Windows:**

Download the Windows binaries from the official John the Ripper website.

Prepare the Hashed Password List:

Ensure you have a file containing the hashed passwords. Let's assume the file is named *hashed_passwords.txt*.

Cracking the Passwords:

To crack the passwords using John the Ripper, follow these steps:

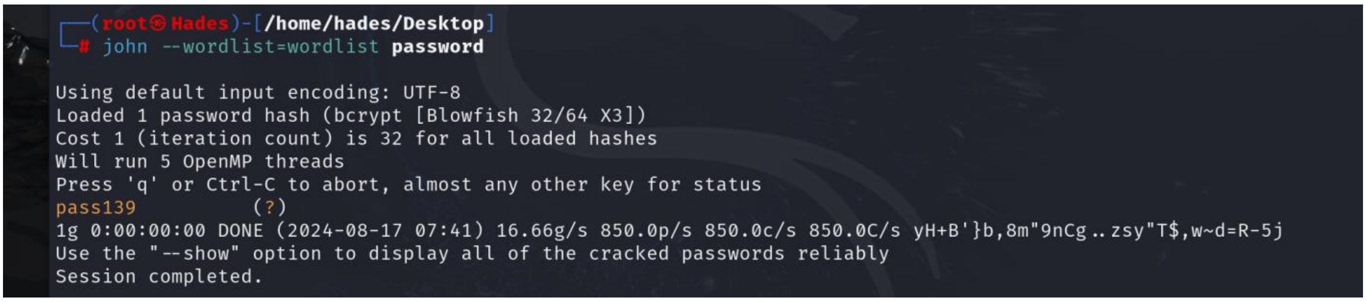
a) **Open the terminal or command prompt.**

b) **Navigate to the directory containing the *password*.txt file.**

```
cd /Desktop
```

c) **Run John the Ripper:**

```
john --wordlist=wordlist password
```



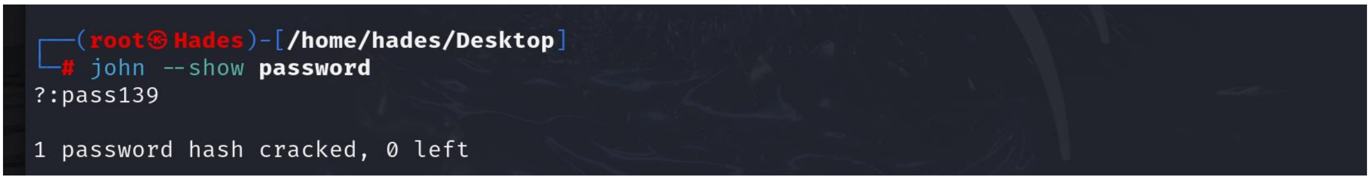
```
┌──(root㉿Hades)-[/home/hades/Desktop]
└─# john --wordlist=wordlist password

Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pass139          (?)
1g 0:00:00:00 DONE (2024-08-17 07:41) 16.66g/s 850.0p/s 850.0c/s 850.0C/s yH+B'}b,8m"9nCg..zsy"T$,w~d=R-5j
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

d) **Document the Process:**

- Note the time you start the cracking process.
- John will automatically start trying to crack the passwords using its default wordlist.
- To see the progress or results while it's running, you can use:

  john --show password



```
┌──(root㉿Hades)-[/home/hades/Desktop]
└─# john --show password
?:pass139

1 password hash cracked, 0 left
```

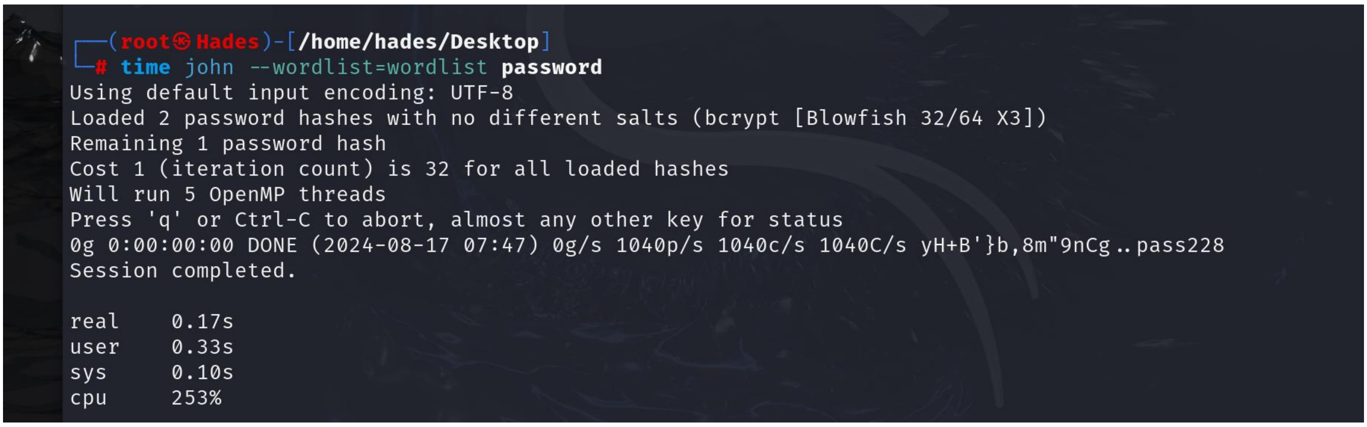
e) **Measuring Time Taken:**

You can measure the time taken to crack each password by noting the start and end times or by using the time command:

- **Using the time Command:**

  time john --wordlist=wordlist password

The time command will give you the total time taken for the process once John has finished running.



```
┌──(root㉿Hades)-[/home/hades/Desktop]
└─# time john --wordlist=wordlist password
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (bcrypt [Blowfish 32/64 X3])
Remaining 1 password hash
Cost 1 (iteration count) is 32 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-08-17 07:47) 0g/s 1040p/s 1040c/s 1040C/s yH+B'}b,8m"9nCg..pass228
Session completed.

real    0.17s
user    0.33s
sys     0.10s
cpu     253%
```

f) **Summary:**

Cracked Hashes:

- **Hash Type**: bcrypt (Blowfish 32/64 X3)
- **Password Hashes:**
  - $2b$05$saltsaltsaltsaltsaltsOp2JsfNz77jYSRItqsfKYWBtHvrr10Qq
  - $2b$05$saltsaltsaltsaltsaltsOoSE6kip4muty61kd/Ko1yPqd.SM/H6.

- **Decrypted Passwords:**
  - **First Password**: pass139
  - **Second Password**: pass228