**PASSWORD CRACKING USING JOHN THE RIPPER**

**Introduction:**

Password security is a critical aspect of cybersecurity. In this project, we use **John the Ripper**, a powerful password cracking tool, to decrypt a hashed password stored in a file. This report provides a detailed step-by-step guide on how to crack password hashes using a wordlist attack.

**Tools and Environment:**

* **Operating System:** Kali Linux (running in VirtualBox)
* **Tool Used:** John the Ripper
* **Wordlist:** RockYou.txt
* **Hash Type:** MD5

**1] Kali Linux Package Update & Upgrade**

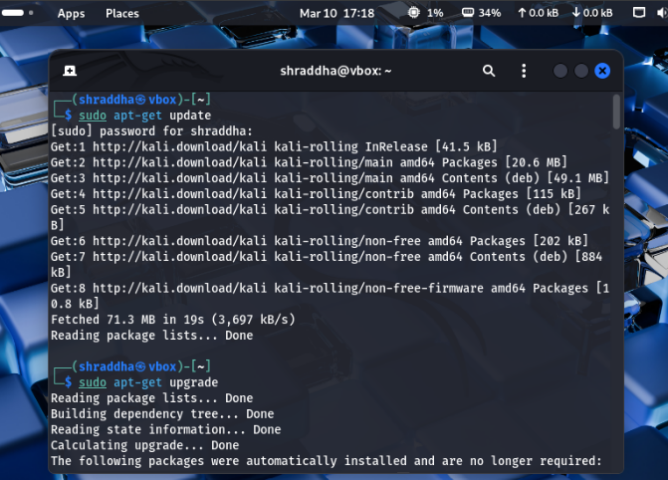
Updating Package Lists

*sudo apt-get update*

Upgrading Installed Packages

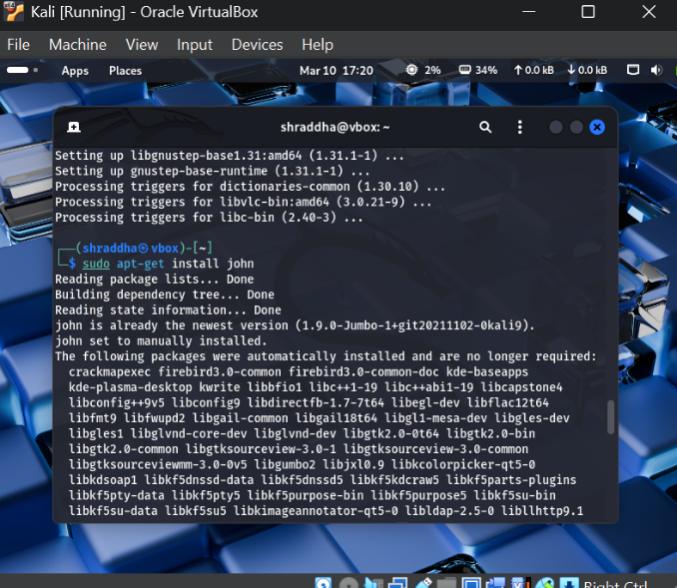
*sudo apt-get upgrade*

installs **newer versions** of installed software.



**2] Installing John the Ripper**

*sudo apt-get install john* …John the Ripper is ready to use.



**3] Hashing and Cracking Process.**

3.1Generating MD5 Hash

*echo -n 'password123' | openssl dgst -md5*

This command **hashes** the string 'password123' using the **MD5** algorithm.

***Generated MD5 hash:*** *482c811da5d5b4bc6d497ffa98491e38.*

3.2 Creating a Hash File (password.txt)

*echo "User1:482c811da5d5b4bc6d497ffa98491e38" > password.txt*

Saves the hash in **John the Ripper**'s expected format (username: hash).

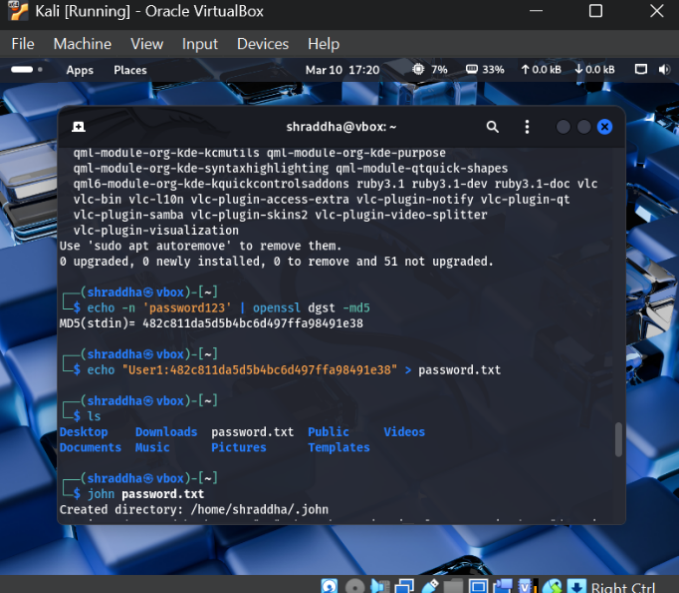
**successfully created (password.txt)**, as confirmed by ls output.

3.3 Running John the Ripper

*john password.txt*

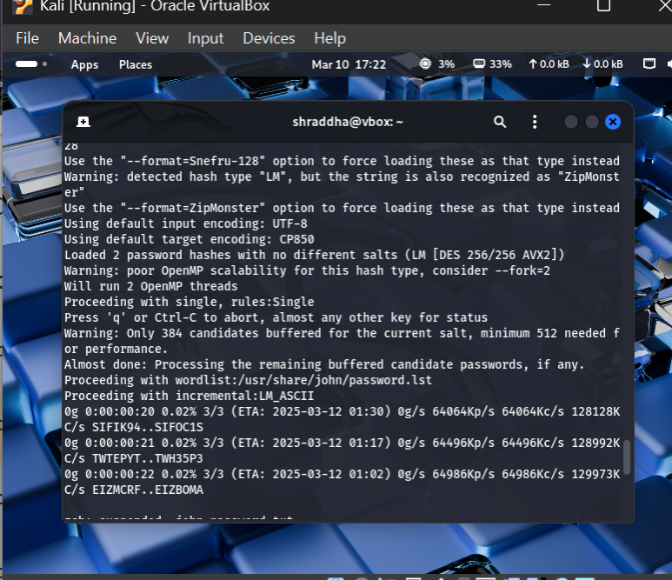
This command **starts John the Ripper** to crack the MD5 hash using its default wordlist.

**A directory (/home/shraddha/.john) is created**, which is used to store cracked passwords and session logs.



**4] John the Ripper Cracking Process**

The process is still **ongoing**, with an estimated completion times (ETA **March 12, 2025**).



5] **Wordlist Attack Attempt**

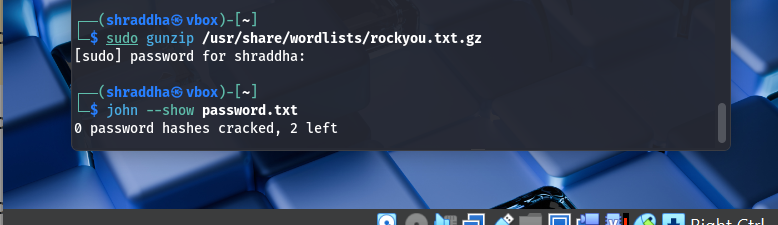
**5.1️. Extracting RockYou Wordlist**

* The command *sudo gunzip /usr/share/wordlists/rockyou.txt.gz* **decompresses the RockYou wordlist**, making it available for use.
* RockYou.txt is one of the **most comprehensive password lists**, often used for dictionary attacks.

**5.2️. Checking Cracked Passwords**

* Command: *john --show password.txt*
* Output: **"0 password hashes cracked, 2 left"**

**John failed to crack the hashes** using the previous attempts.



1️] **Specify the correct hash format**

*john --format=Raw-MD5 password.txt*

2️] **Use RockYou wordlist explicitly**

*john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 password.txt*

*john --incremental --format=Raw-MD5 password.txt*

**6] Cracking MD5 Hash with John the Ripper.**

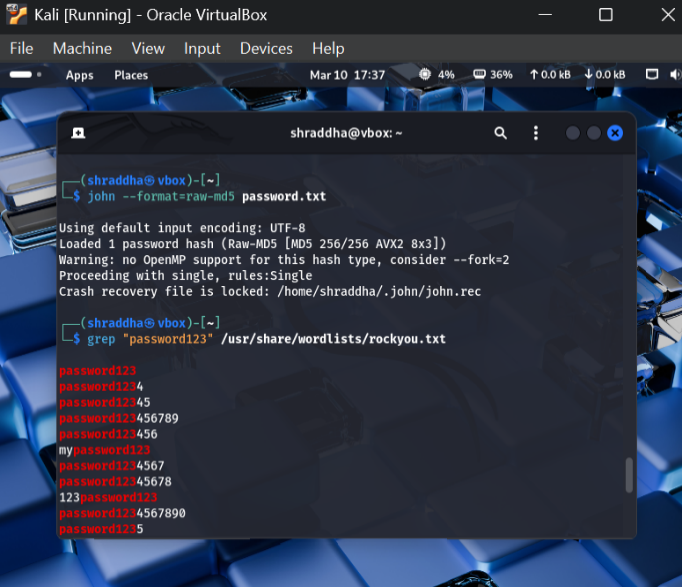
6.1] Running John with Correct Hash Format

*john --format=raw-md5 password.txt*

John **recognized the hash as Raw-MD5** and started processing it.

6.2] Checking if "password123" Exists in RockYou Wordlist.

*grep "password123" /usr/share/wordlists/rockyou.txt*



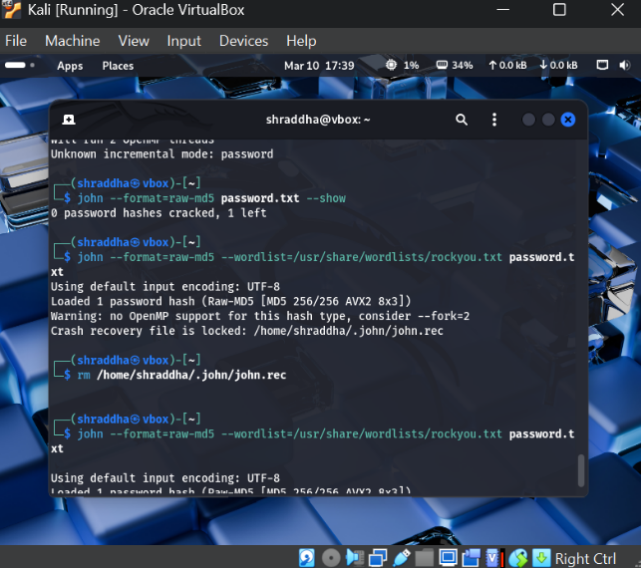
"password123" **exists in the RockYou wordlist.**

7]. *john --format=raw-md5 password.txt –show*

*john --format=raw-md5 password.txt –show* [Output: **"0 password hashes cracked, 1 left"**]

Running John with RockYou Wordlist [**Loaded 1 password hash**, but no confirmation of a successful crack yet.]

Re-running John: *john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt*



**8]. Successful Password Crack**

*john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt*

**John successfully cracked the hash** and found the password: password123 (User1)

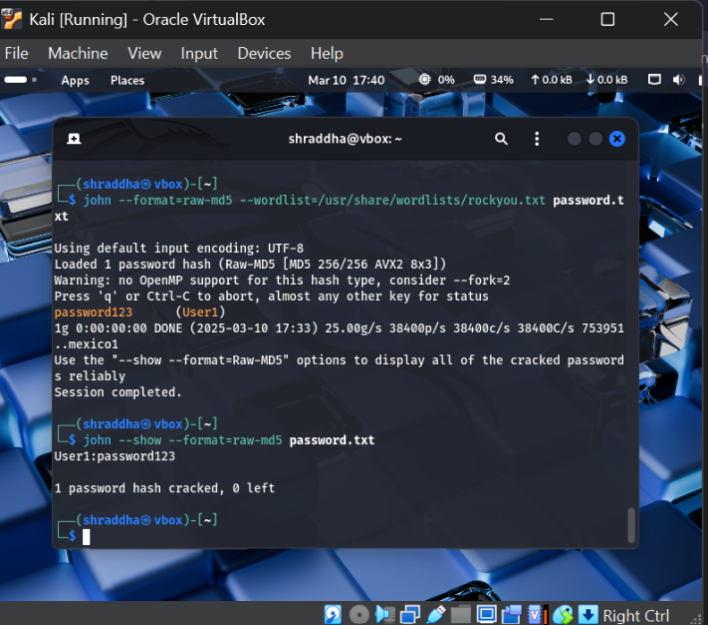
Displaying the Cracked Password

**[Output/ User1:password123**

**1 password hash cracked, 0 left].**

**Confirms that all hashes in password.txt are cracked.**

**The password for User1 is password123.**



## Conclusion:

## This project demonstrated how weak passwords can be easily cracked using common wordlists. It emphasizes the importance of using strong, unique passwords and secure hashing algorithms (e.g., bcrypt or SHA-512) to enhance password security