How to crack a password hash with Kali Linux

Cracking hashed passwords refers to the process of attempting to reverse or guess a hashed password to discover the original plaintext value. While this topic is important in cybersecurity education and ethical penetration testing, it must always be approached legally and responsibly; only in environments where you have explicit permission to test security (e.g., penetration testing labs, CTFs, or your own systems).

What Is a Hashed Password?

- A password hash is a **fixed-length encrypted output** generated by a **hash function** (e.g., SHA-256, MD5, etc).
- Hashing is **one-way**: it should not be possible to reverse the hash to get the original password.

Common Hash Cracking Methods (for Educational Use Only):

1. **Brute Force** – Try all possible combinations until a match is found.
2. **Dictionary Attack** – Use a list of common passwords to compare against hashes.
3. **Rainbow Tables** – Precomputed hash tables used to reverse hashes quickly (less useful against salted hashes).
4. **Hybrid Attacks** – Mix of dictionary and brute-force (e.g., adding numbers to common words).
5. **Rule-based Attacks** – Use patterns and transformations on dictionary entries.

It is important to understand that simple passwords are easily cracked. That is why it is always advisable to use a combination of both upper- and lower-case letters, numbers together with other special characters when choosing passwords. Strong passwords cannot be cracked easily or take forever to crack.

STEP1: Open virtual box and open Kali Linux. Go to browser and search for any LM hash generator and generate a simple password hash.

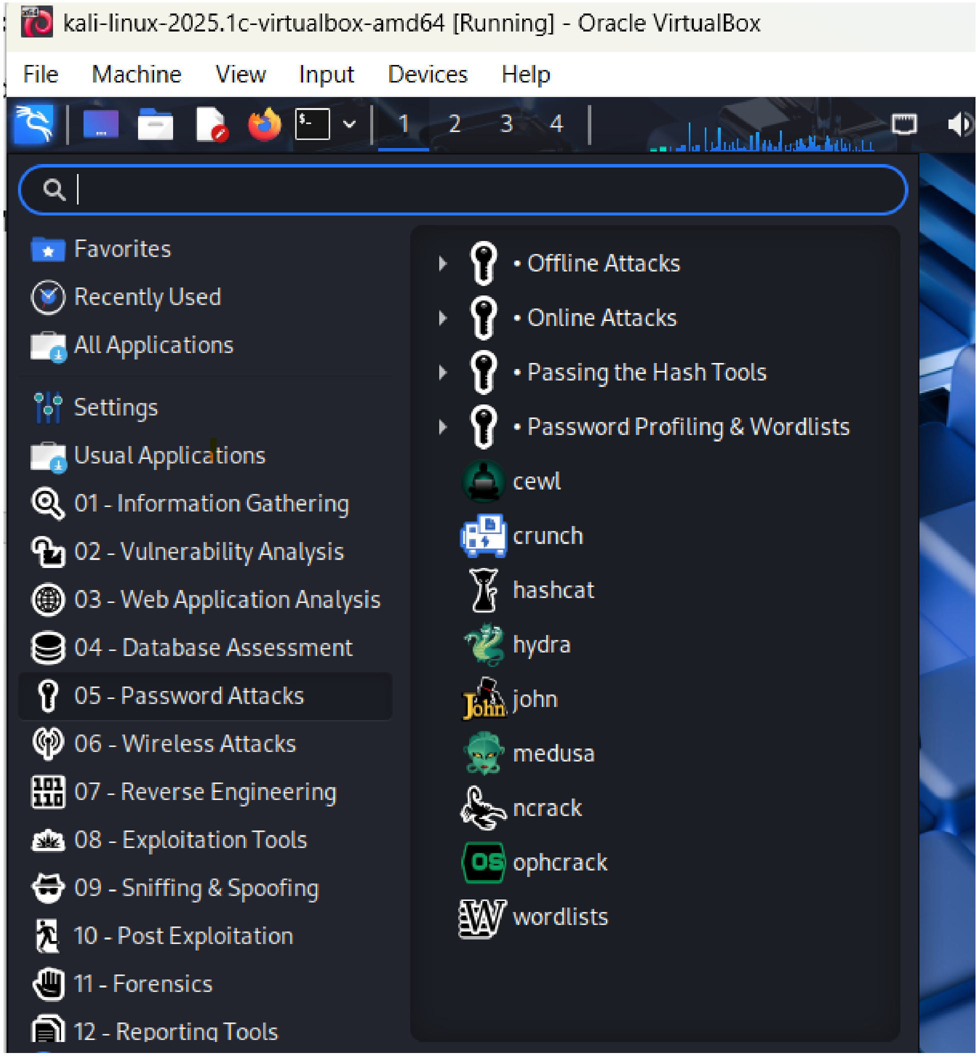
Example:

Password: welc

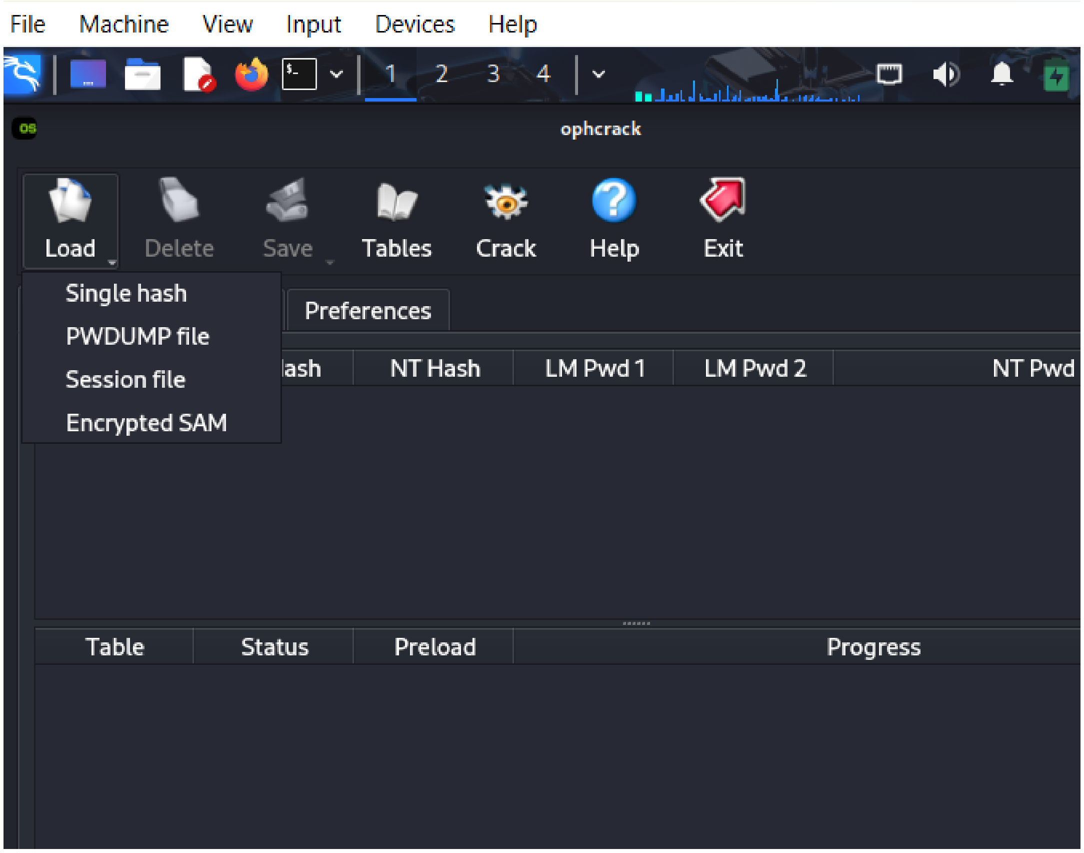
LM hash: E4B0A2BBEABC9B04AAD3B435B51404EE

NOTE: LM HASH is used in older versions on Windows to store passwords.

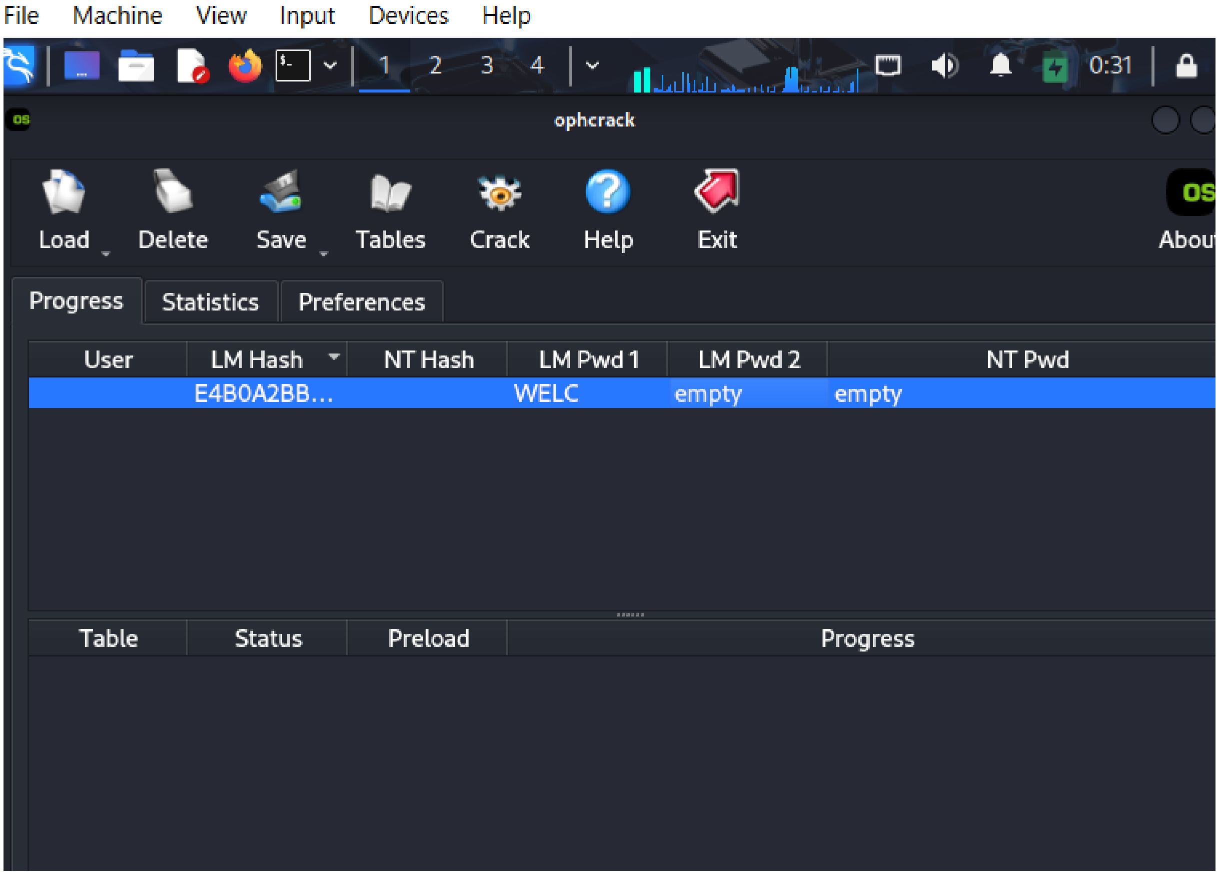
STEP2:



STEP3: Select ophcrack. Click on Load and then select single hash



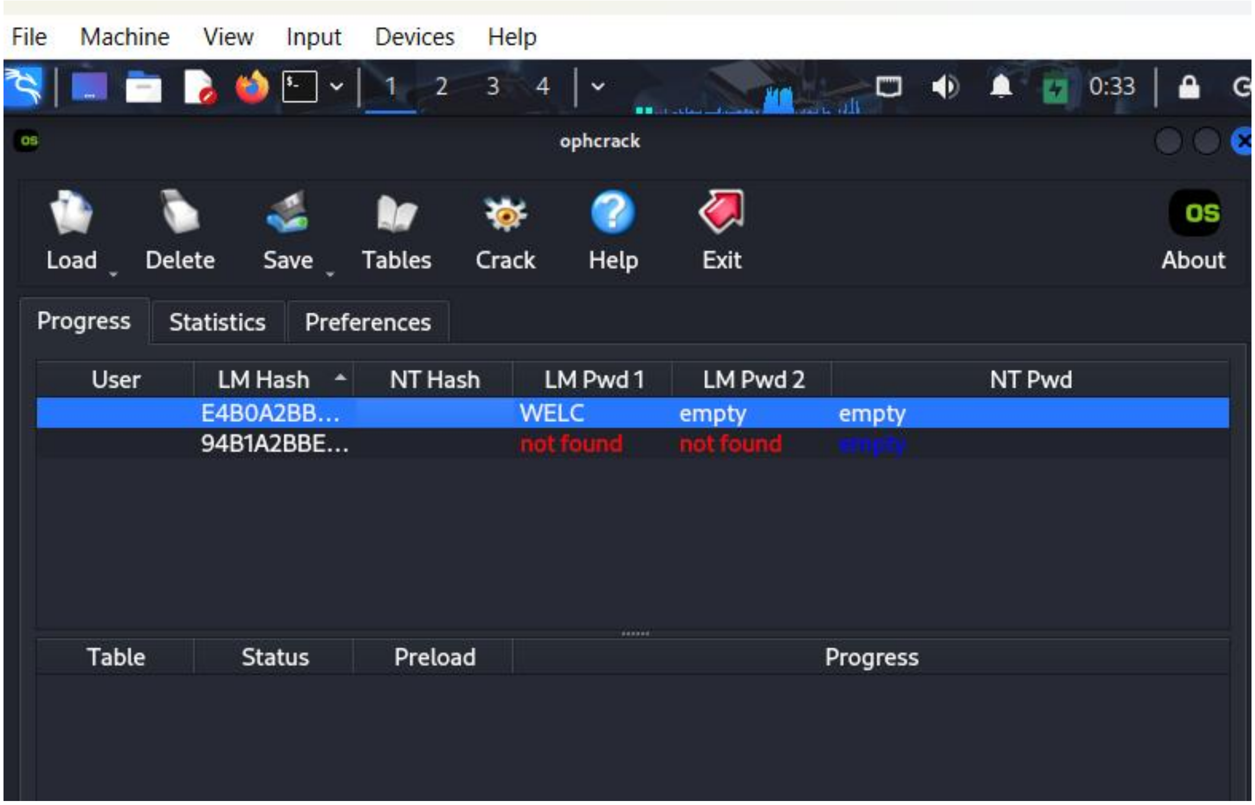
Step4: Paste your LM hash, click ok, and then click on crack



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
	E4B0A2BB...		WELC	empty	empty

Table	Status	Preload	Progress

STEP5: Trying with stronger password will take almost forever to crack. That is why is says “not found.”



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
	E4B0A2BB…		WELC	empty	empty
	94B1A2BBE…		not found	not found	empty

Table	Status	Preload	Progress