Cracking Windows Passwords with Ophcrack and Kali

@mmar

Ophcrack is a free Windows password cracker based on rainbow tables. It comes with a Graphical User Interface and runs on multiple platforms.

Rainbow tables are precomputed hashes of a dictionary which makes cracking much faster than a dictionary attack

Attacks

Scenorio

- You have physical access to a system which is **password locked**. The tool can be used to quickly **crack** the password

We are actually cracking the password and not bypassing it

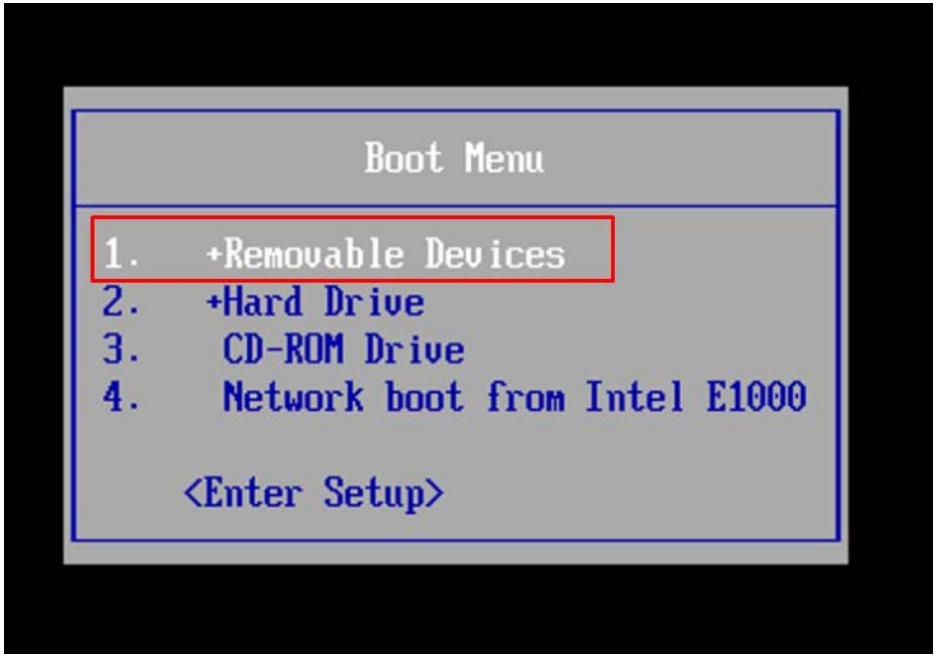
We need to have Kali Live boot USB

(Check the lecture “Kali Linux as a bootable USB Drive”)

Step- 1

- Boot from Kali Linux USB drive

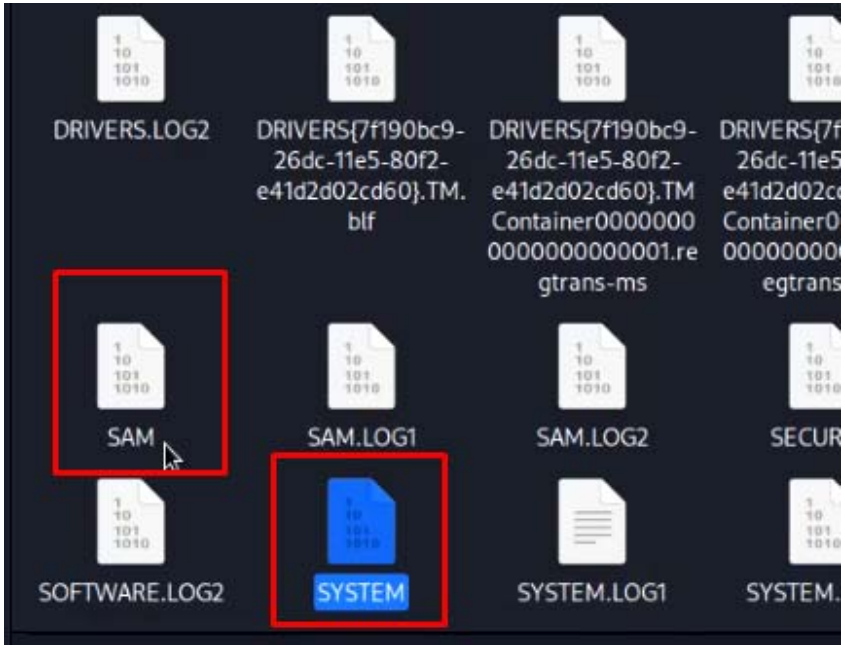
Plug in USB to target PC and Boot from USB



Step- 2

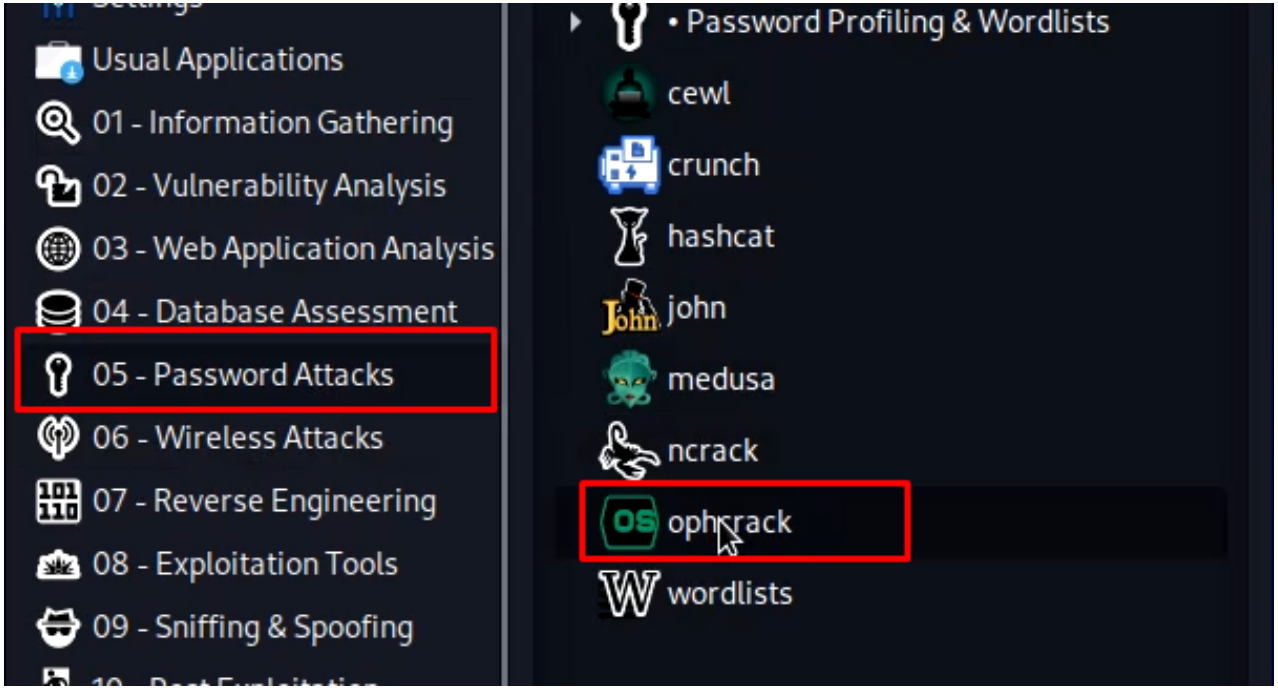
- Navigate to windows/system32/config folder and copy these files to Kali Desktop

SAM & SYSTEM



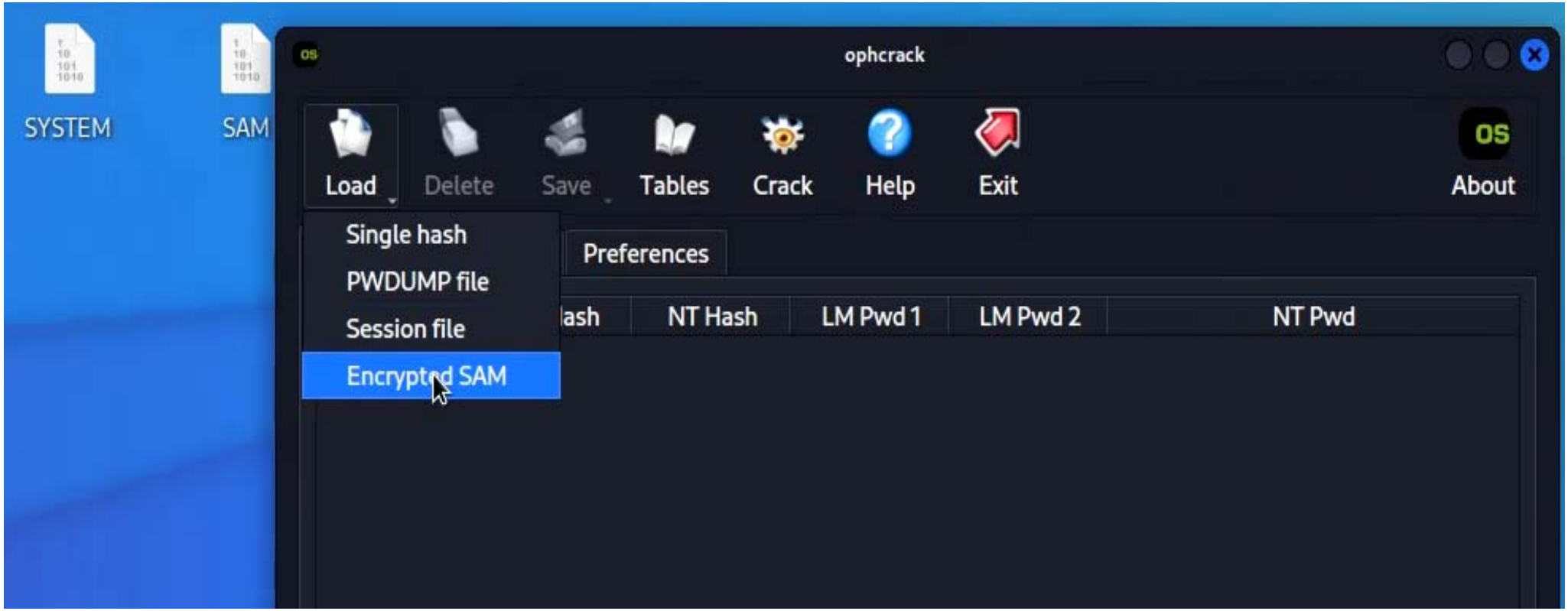
Step- 3

- Run Ophcrack from Applications/password attacks



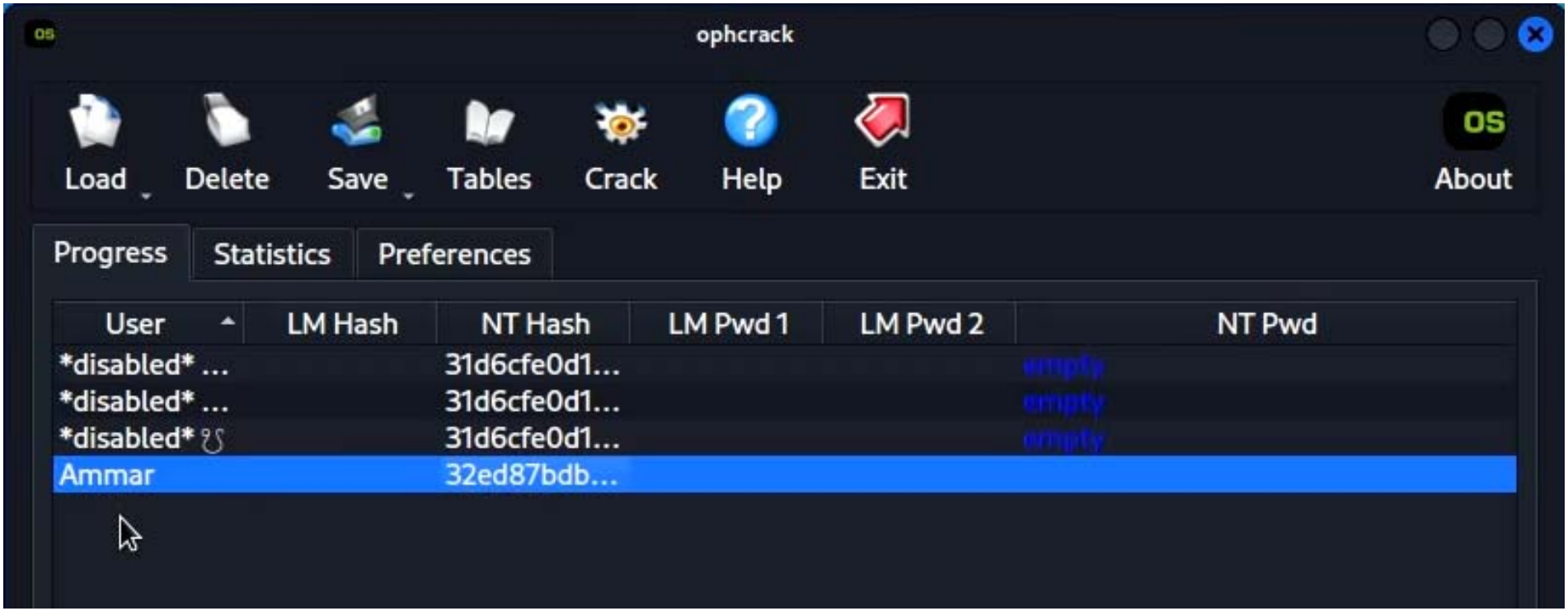
Step- 4

- Now load encrypted hashes by clicking load and then choosing encrypted SAM. Choose the desktop folder



Step- 5

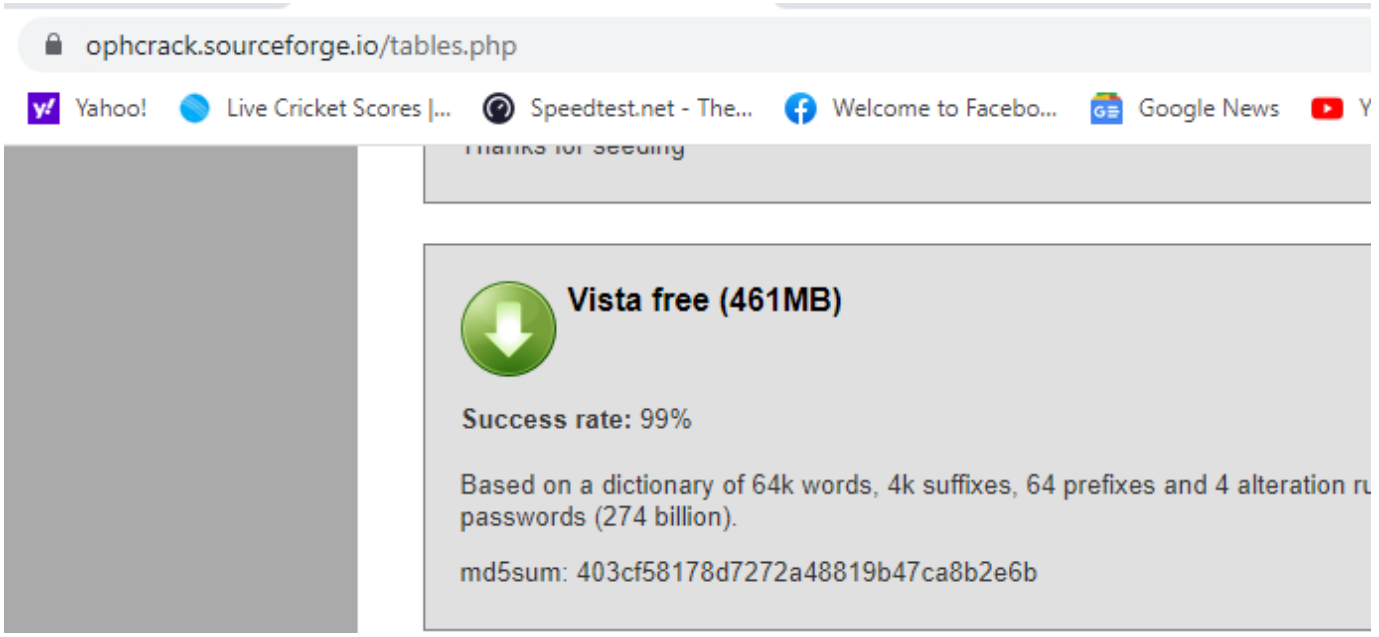
- All accounts and their Hashes will be loaded



Step- 6

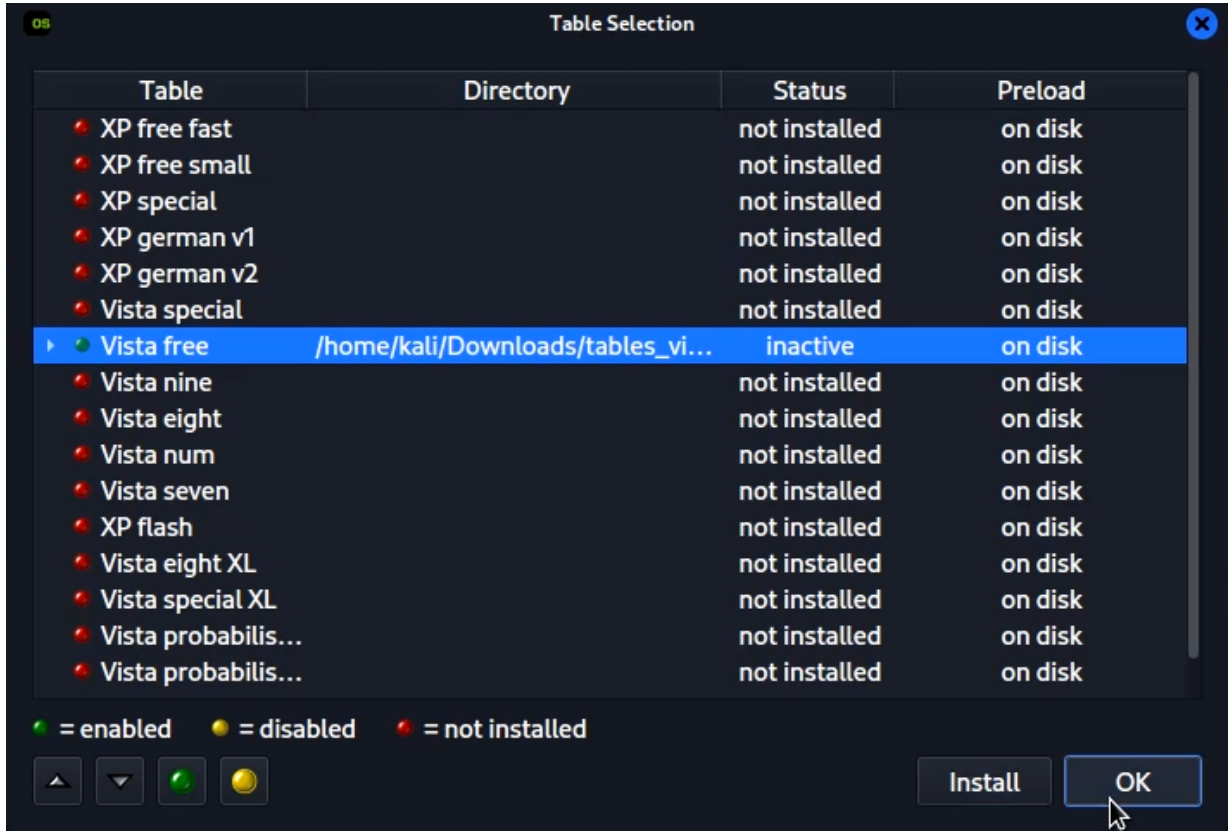
- Now visit following website and download vista free rainbow tables and extract them

https://ophcrack.sourceforge.io/tables.php



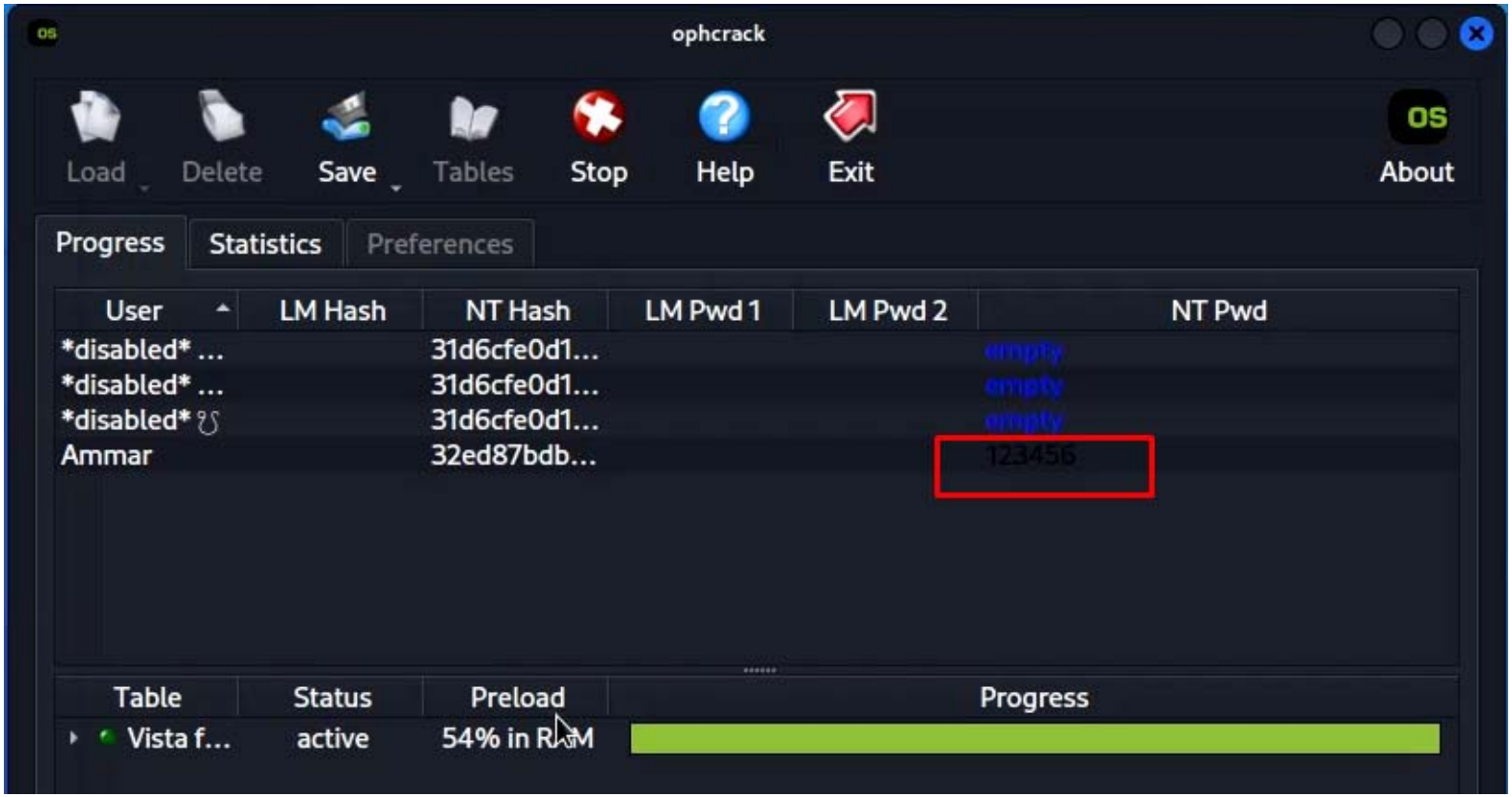
Step- 7

- In Ophcrack click on tables, and install the tables



Step- 8

- Click on crack and the utility will crack your password



DEMO

THANKS