Crack Windows Passwords with Ophcrack on Windows

@mmar

Attacks

Scenorio

- You have physical access to a system which is **password locked**. We can copy the file hashes and then use the tool to **crack** the password in an offline attack
- It may also be possible **to crack other users' passwords** on the same system

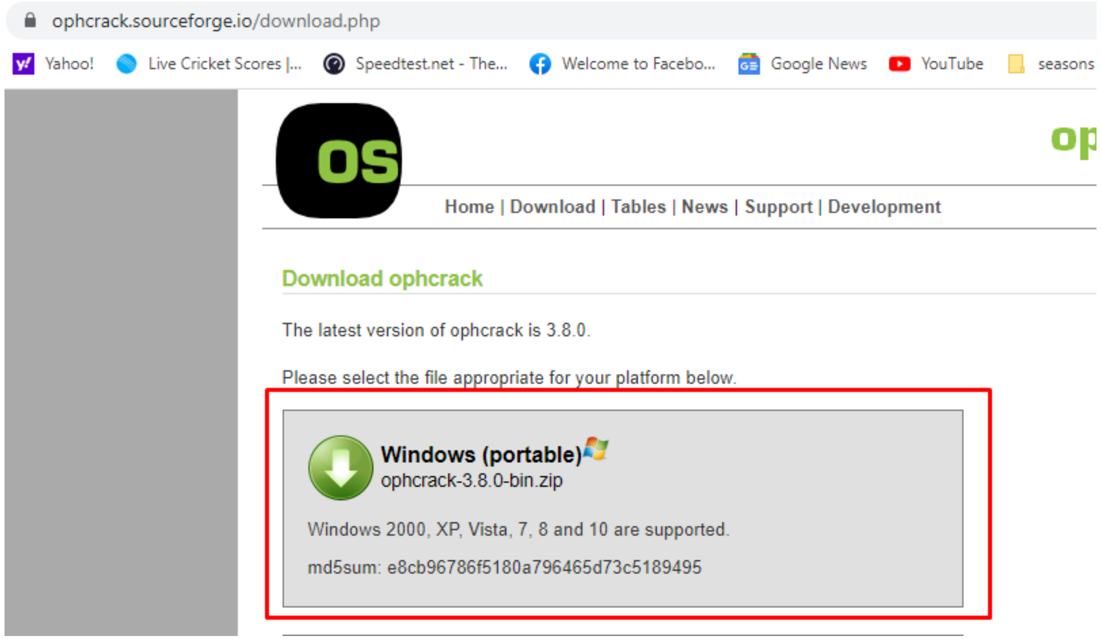
Obtaining Hashes

1. Copy SAM and System files after booting from the live kali USB drive(recommended)
2. Directly dump the hashes with ophcrack
3. Use commands to dump hashes from the registry

Step- 1

- Download Ophcrack from official website

https://ophcrack.sourceforge.io



Download ophcrack

The latest version of ophcrack is 3.8.0.

Please select the file appropriate for your platform below.

Windows (portable)
ophcrack-3.8.0-bin.zip

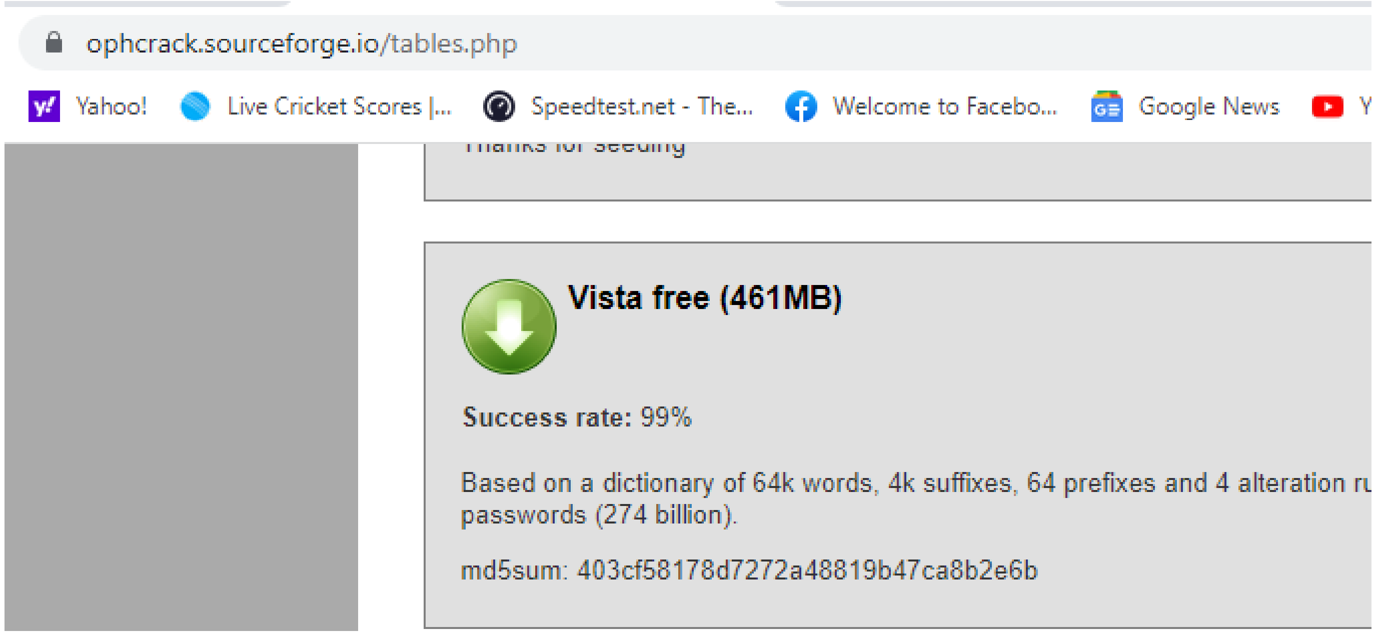
Windows 2000, XP, Vista, 7, 8 and 10 are supported.

md5sum: e8cb96786f5180a796465d73c5189495

Step- 2

- Download vista free rainbow tables and extract them

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



Thanks for seeding

Vista free (461MB)

Success rate: 99%

Based on a dictionary of 64k words, 4k suffixes, 64 prefixes and 4 alteration ru
passwords (274 billion).

md5sum: 403cf58178d7272a48819b47ca8b2e6b

Step- 3

- In Ophcrack click on tables, and install the tables

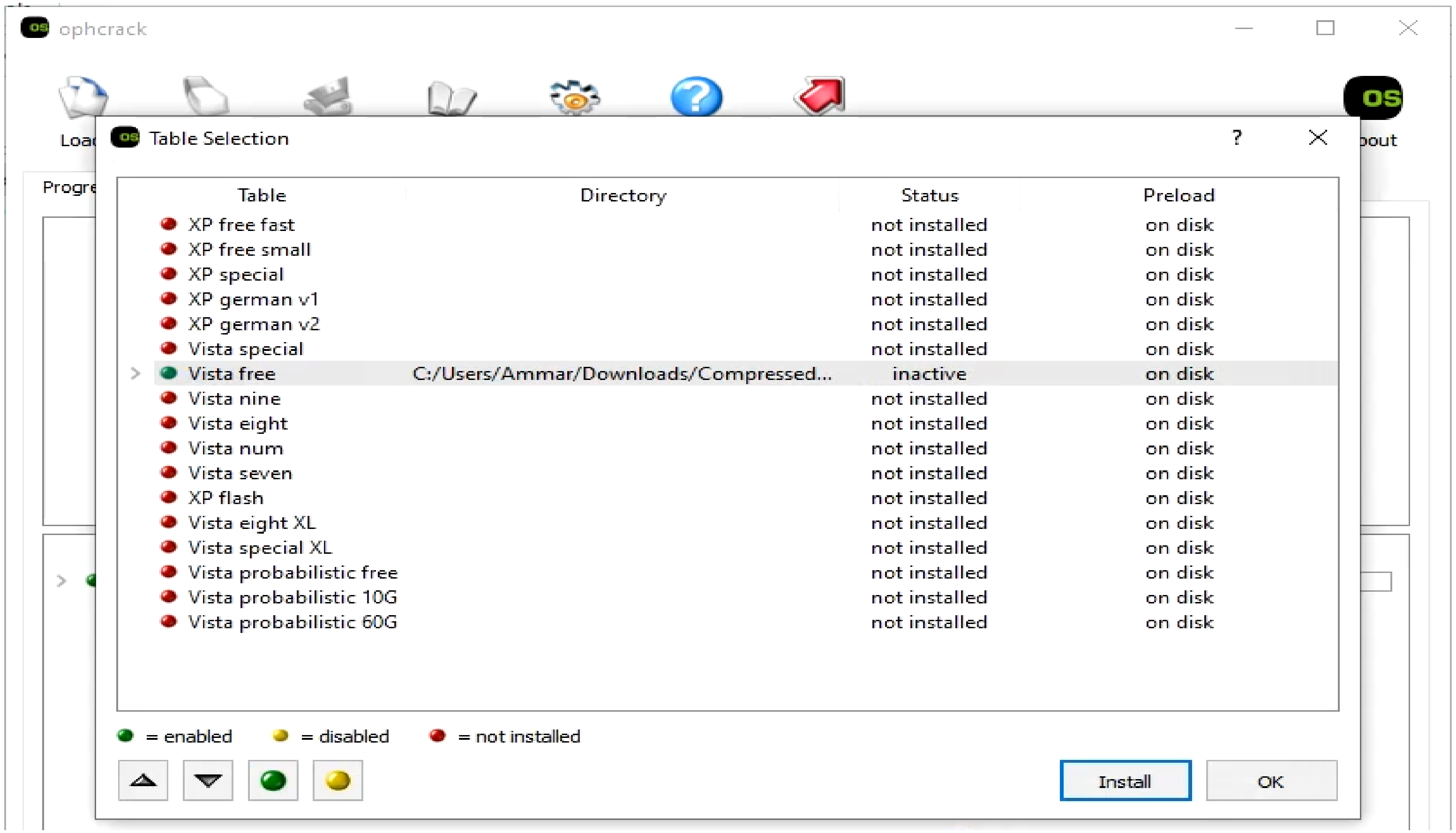


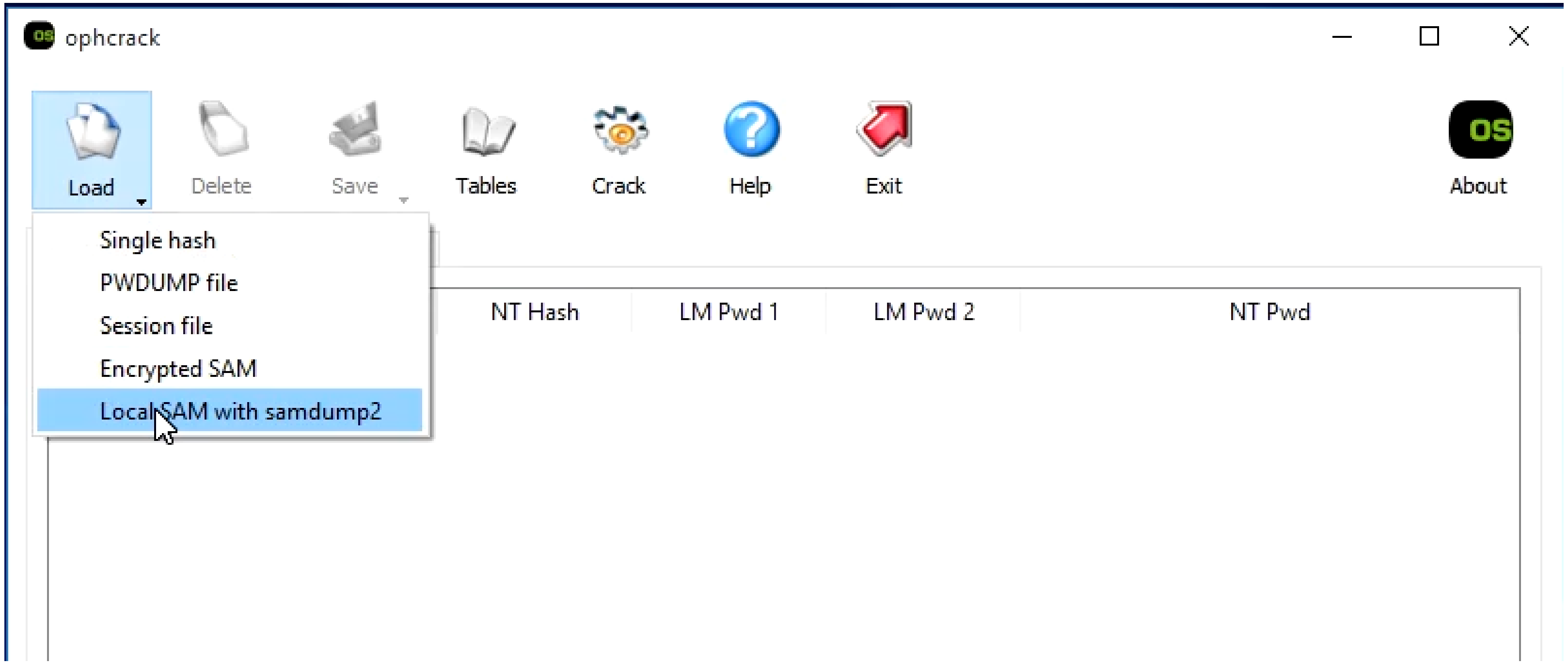
Table	Directory	Status	Preload
🟥 XP free fast		not installed	on disk
🟥 XP free small		not installed	on disk
🟥 XP special		not installed	on disk
🟥 XP german v1		not installed	on disk
🟥 XP german v2		not installed	on disk
🟥 Vista special		not installed	on disk
🟩 Vista free	C:/Users/Ammar/Downloads/Compressed...	inactive	on disk
🟥 Vista nine		not installed	on disk
🟥 Vista eight		not installed	on disk
🟥 Vista num		not installed	on disk
🟥 Vista seven		not installed	on disk
🟥 XP flash		not installed	on disk
🟥 Vista eight XL		not installed	on disk
🟥 Vista special XL		not installed	on disk
🟥 Vista probabilistic free		not installed	on disk
🟥 Vista probabilistic 10G		not installed	on disk
🟥 Vista probabilistic 60G		not installed	on disk

🟩 = enabled 🟨 = disabled 🟥 = not installed

DUMPING HASHES

Extract hashes with ophcrack

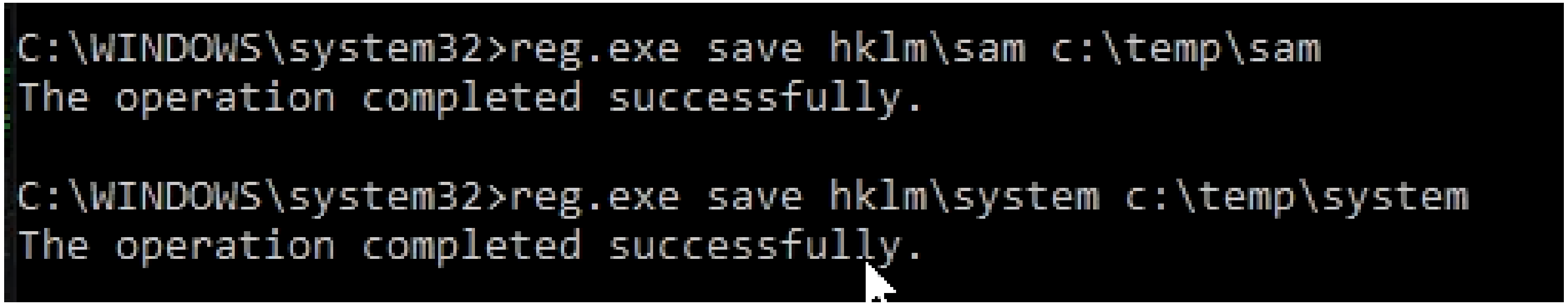
- In Ophcrack, click on load and choose the option to load from SAM with SAMDUMP2 (may not work on latest windows 10/11)



Commands

- Use the following commands to dump hashes

```
C:\> reg.exe save hklm\sam c:\temp\sam
C:\> reg.exe save hklm\system c:\temp\system
```



```
C:\WINDOWS\system32>reg.exe save hklm\sam c:\temp\sam
The operation completed successfully.

C:\WINDOWS\system32>reg.exe save hklm\system c:\temp\system
The operation completed successfully.
```

Commands

- Now load encrypted hashes in ophcrack

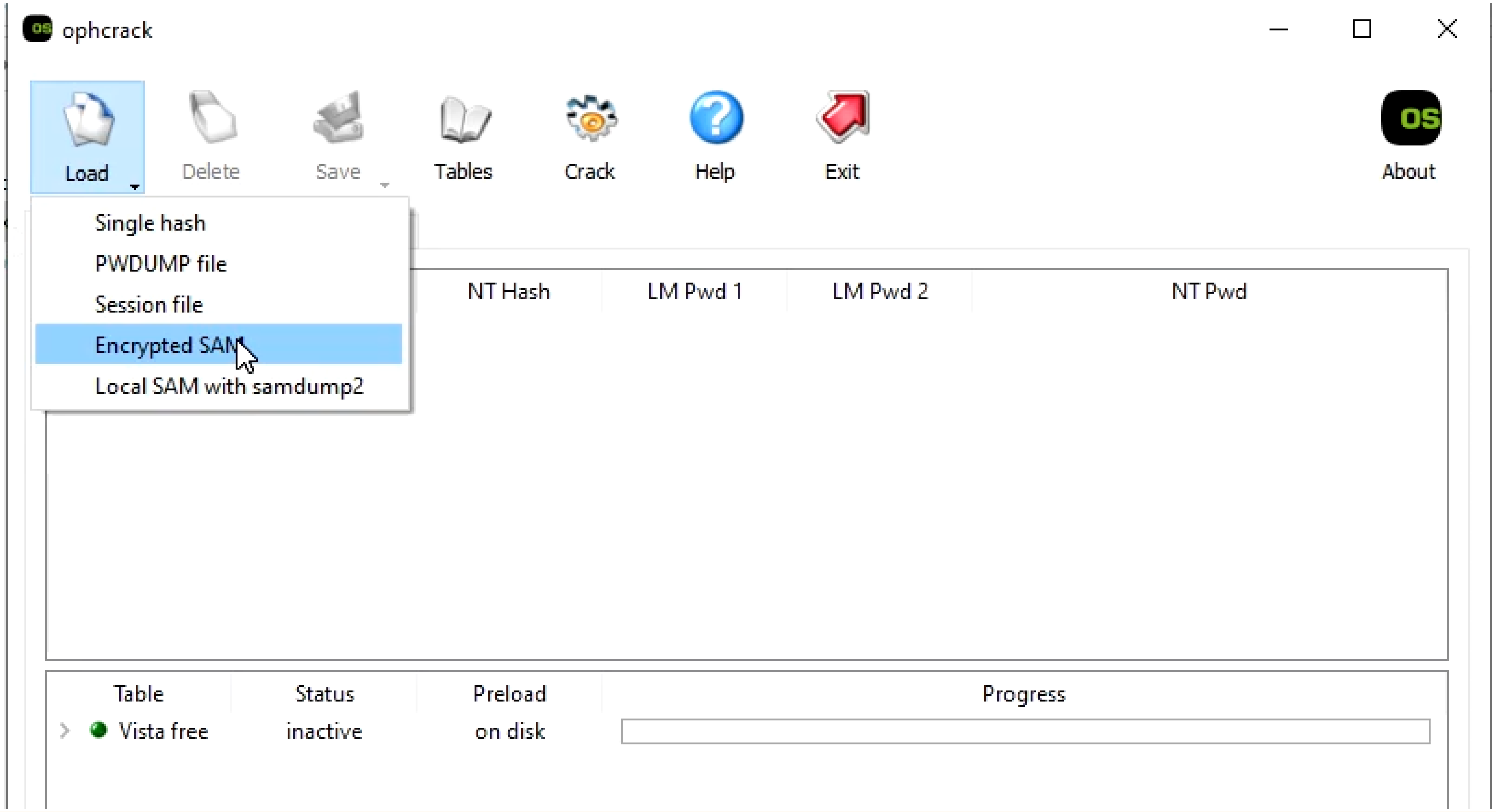
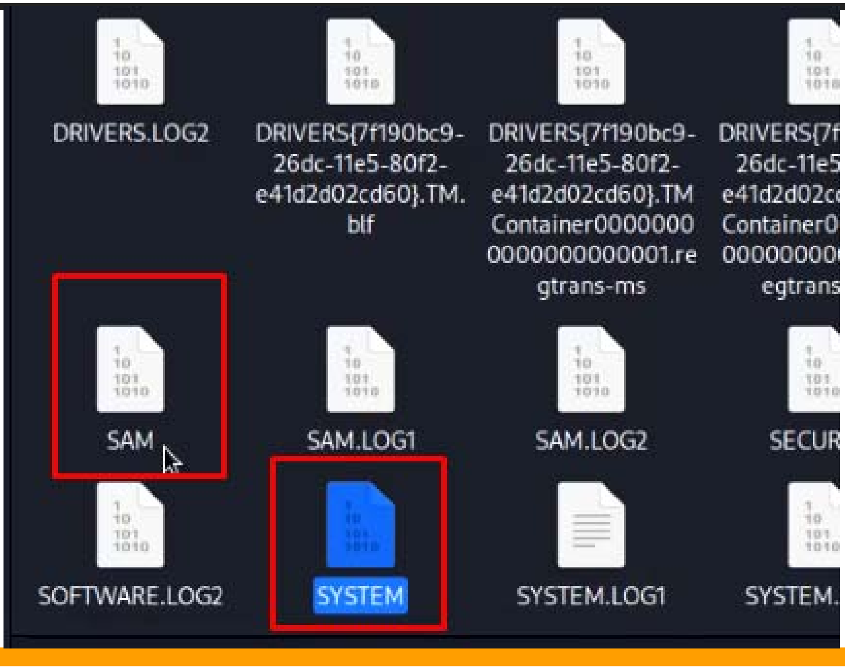


Table	Status	Preload	Progress
Vista free	inactive	on disk	

Kali live USB

- Boot from kali live USB. Navigate to the windows/system32/config folder and copy these files to your main machine

SAM & SYSTEM



DRIVERS.LOG2

DRIVERS{7f190bc9-26dc-11e5-80f2-e41d2d02cd60}.TM.blf

DRIVERS{7f190bc9-26dc-11e5-80f2-e41d2d02cd60}.TMContainer00000000000000000001.regtrans-ms

DRIVERS{7f 26dc-11e5 e41d2d02c Container0 00000000 egtrans

SAM

SAM.LOG1

SAM.LOG2

SECUR

SOFTWARE.LOG2

SYSTEM

SYSTEM.LOG1

SYSTEM.

Commands

- Now load encrypted hashes in ophcrack and select the folder

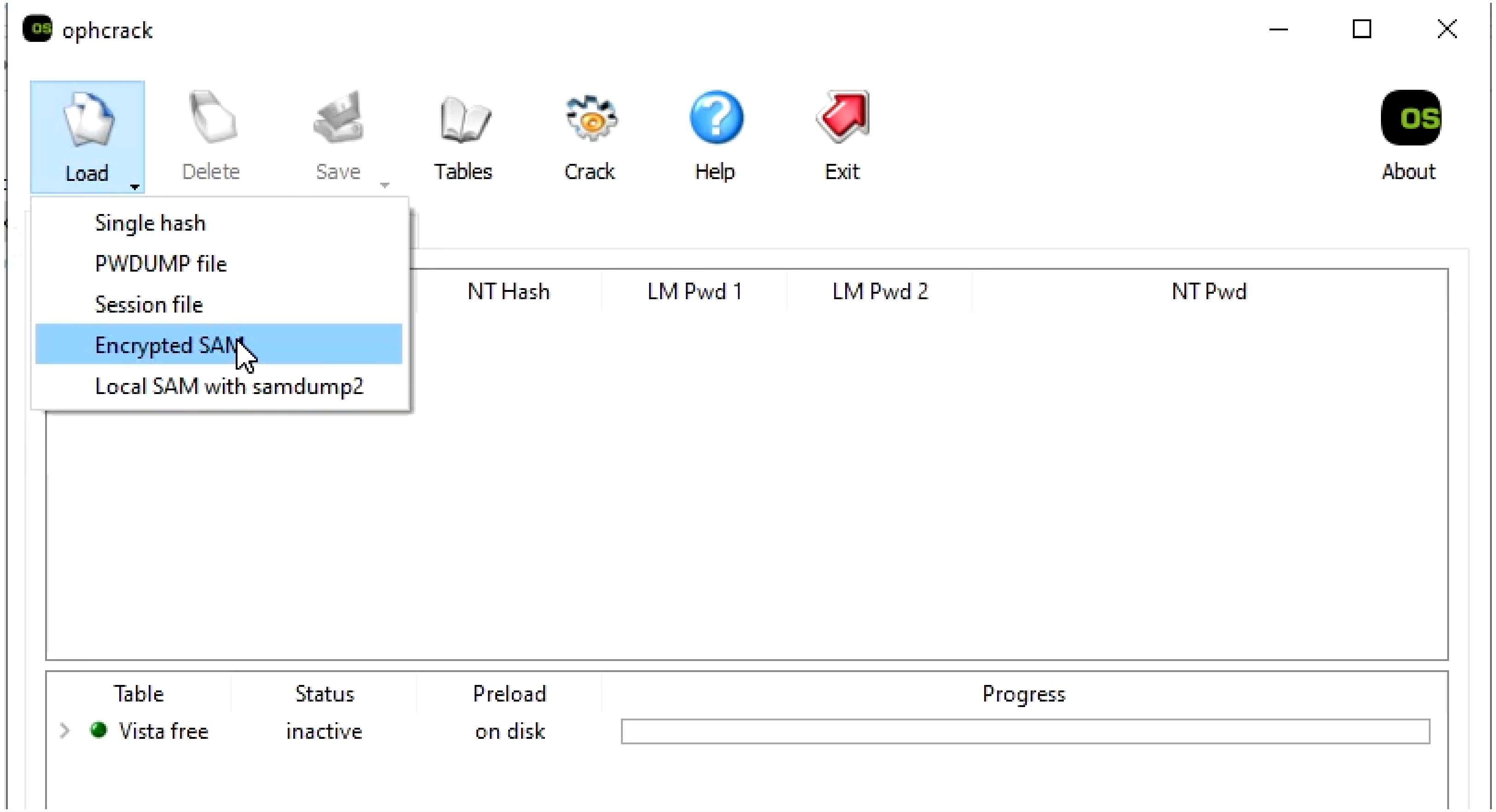
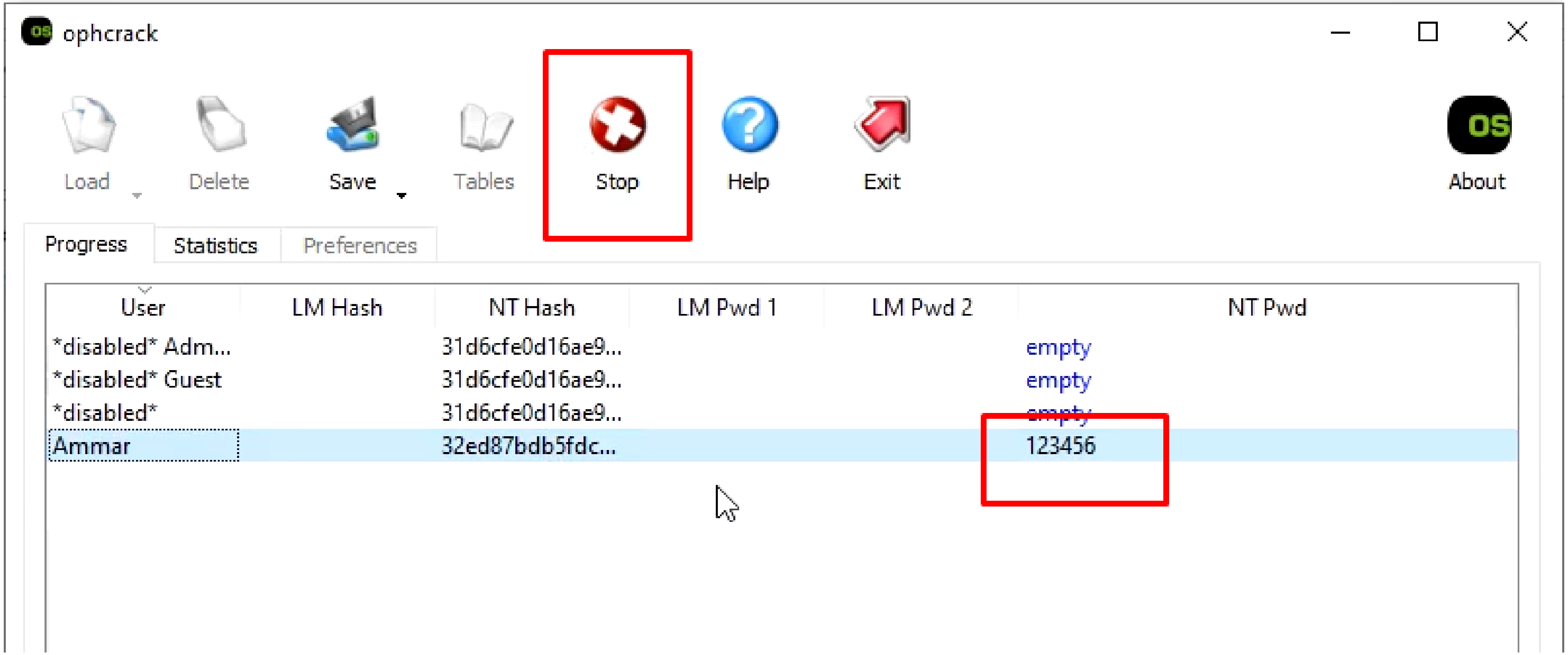


Table	Status	Preload	Progress
● Vista free	inactive	on disk	

CRACKING HASHES

OPHCRACK

- Once we have the hash and rainbow tables installed, you can click crack and the password will be cracked



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
disabled Adm...		31d6cfe0d16ae9...			empty
disabled Guest		31d6cfe0d16ae9...			empty
disabled		31d6cfe0d16ae9...			empty
Ammar		32ed87bdb5fdc...			123456

DEMO

THANKS