Ophcrack Howto
(Ophcrack Documentation)

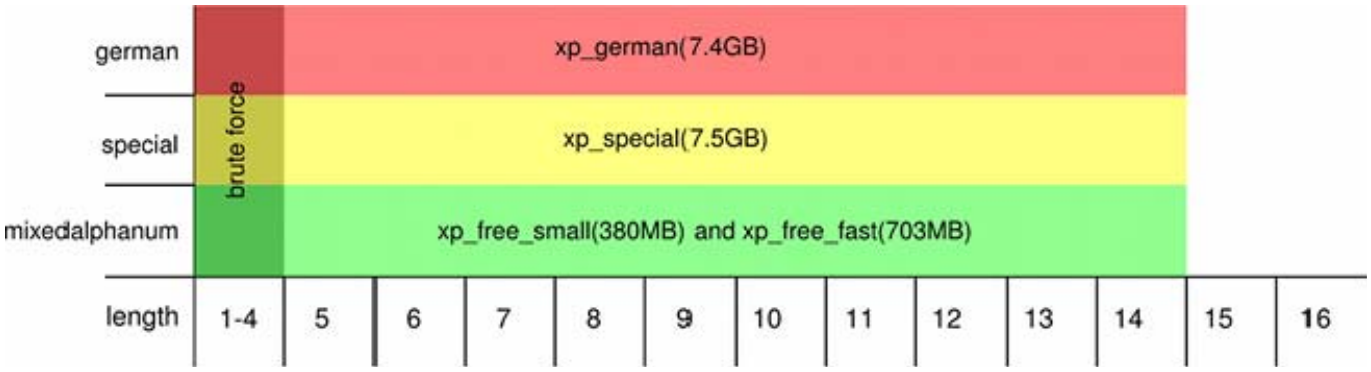
This howto assumes you have already installed ophcrack 3 and downloaded the ophcrack rainbow tables you want to use. It also assumes that you understand how to use third party tools like pwdump or fgdump to dump the SAM of a Windows system.

Ophcrack and the ophcrack LiveCD are available for free at the ophcrack project page.

Ophcrack rainbow tables are avaible at ophcrack rainbow tables page. The XP free small, XP free fast and Vista free rainbow tables are free. The others ophcrack rainbow tables are sold by Objectif Securite.

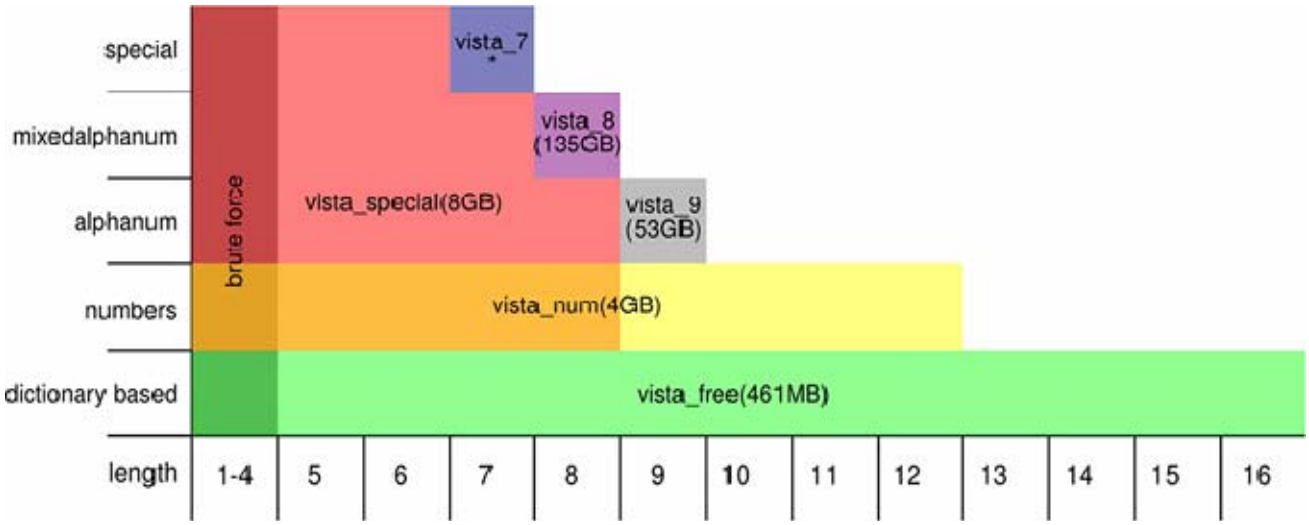
XP Rainbow tables

These tables can be used to crack Windows XP passwords (LM hashes). They CANNOT crack Windows Vista passwords (NT hashes).



Vista Rainbow tables

These tables can be used to crack Windows Vista passwords (NT hashes).



First step

This step is optional but will speed up the cracking process.

Run ophcrack and set the number of threads under the Preferences tab to the number of cores of the computer running ophcrack plus one.For example, for an old processor set the number of threads to 2,

for a Core 2 Duo to 3 and for a Core 2 Quad to 5. If you change this value, you have to exit ophcrack and to restart it in order to save the change. If you don't exit and restart, the new number of threads will not be taken into account by the program.

Second step

This step is mandatory.

Load hashes using the Load button. You can either enter the hash manually (Single hash option), import a text file containing hashes you created with pwdump, fgdump or similar third party tools (PWDUMP file option), extract the hashes from the SYSTEM and SAM files (Encrypted SAM option), dump the SAM from the computer ophcrack is running on (Local SAM option) or dump the SAM from a remote computer (Remote SAM option).

For the Encrypted SAM option, the SAM is located under the Windows system32/config directory and can only be accessed for a Windows partition that is NOT running. For the Local SAM and Remote SAM options, you MUST logged in with the administrator rights on the computer you want to dump the SAM.

Third step

This step is optional but will speed up the cracking process.

Delete with the Delete button every user account you are not interested in (for exemple the Guest account). You can use the Ctrl key to make multiple selection. Ctrl-a will select every loaded hash.
Keep in mind that the time needed to crack password hashes with rainbow tables is proportional to the number of hashes loaded. With a brute force attack the cracking time is NOT dependant on the number of unsalted hashes loaded. That's why it's advisable to remove any unnecessary user account with the Delete button.

Fourth step

This step is mandatory.

Install (Tables button), enable (green and yellow buttons) and sort wisely (up and down arrows) the rainbow tables your are going to use. Keep in mind that storing the rainbow tables on a fast medium like a hard disk will significantly speed up the cracking process.

Here are a few guidelines :

- If you want to crack LM hashes as found on Windows XP by default (the LM Hash column is never empty on the ophcrack main window), first install and enable either the XP free small (if you have less than 512MB of free RAM) or the XP free fast (if you have more than 512MB of free RAM). Do NOT enable both of them since this is generally useless and will slow down the cracking process. Then install and enable the Vista free tables set. Finally install and enable the other XP rainbow tables you may have (XP special, XP german) and Vista one (Vista special). Sort the rainbow tables with the up and down arrows the following way : first the XP free then the Vista free then the XP special after that the Vista special and finally the XP german.

- If you want to crack NT hashes as found on Windows Vista by default (the LM Hash column is always empty on the ophcrack main window), first install and enable the Vista free tables set. Then install and enable the Vista special tables set. Disable every other XP tables sets since they are useless and slow down the cracking process. Sort the enabled rainbow tables with the up and down arrows the following way : first the Vista free then the Vista special.

- If you want to crack a mix of LM and NT enabled hashes (some accounts have their LM column empty, others have both the LM and NT columns filled with hashes) proceed the same way as "If you want to crack LM enabled hashes".

Fifth step

This step is mandatory.

Click on the Crack button to start the cracking process. You'll see the progress of the cracking process in the bottom boxes of the ophcrack window. When a password is found, it will be displayed in the NT Pwd field. You can then save the results of a cracking session at any time with the Save button.