

Hack Password Windows XP SP2 dengan Ophcrack

Contributed by Chaidir
Tuesday, 15 April 2008

Sebelumnya saya pernah membuat tutorial mengenai Hack Windows XP (SP2) Passwords menggunakan pwdump6. Namun, cara tersebut mengharuskan user dengan status admin agar dapat “dump” file HASH dari Windows. Sekarang saya akan menyampaikan cara lain untuk “cracking” password Windows XP (semua versi) dengan menggunakan Ophcrack.

Ophcrack is a Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a GTK+ Graphical User Interface and runs on Windows, Mac OS X (Intel CPU) as well as on Linux.

Hebatnya lagi, Ophcrack tersedia dalam bentuk LiveCD, sehingga tidak diperlukan proses instalasi dan tidak perlu password admin, hanya butuh akses agar komputer dapat booting dari CD (biasanya urutan booting default BIOS komputer saat ini dimulai dari CD/DVD ROM, so don’t worry) . Ophcrack LiveCD merupakan Linux yang berbasis SLAX (turunan dari Slackware) dan sudah terdapat Ophcrack dan Rainbow Table untuk cracking password alphanumerik.

Intinya hampir sama dengan cara kerja pwdump6, namun karena Ophcrack menggunakan linux LiveCD sehingga dapat langsung mount file sistem Windows tanpa perlu login ke Windows serta membaca file Hash (windows\system32\config) dan melakukan dump ke file text biasa yang kemudian dapat langsung di crack. Dan hebatnya, tidak perlu Tools seperti JTR lagi, karena crack dilakukan dengan Ophcrack menggunakan Rainbow Table dan memberikan hasil yang sangat cepat.

Ok.. langsung aja kita praktek, tapi sebelumnya pasang disclaimer dulu ah… biar bisa “lepas” tanggung jawab kalau tutorial ini disalahgunakan oleh pihak lain

Disclaimer:

This document was written in the interest of education and care of awareness for unaware people. The author cannot be held responsible for how the topics discussed in this document are applied.

Lets Begin

Pertama kali anda harus mendownload file ISO Ophcrack LiveCD dari sini. Lalu burn ke dalam CD. Dan selanjutnya boot Komputer “target” dari Ophcrack LiveCD, maka akan tampak seperti ini :

Tekan Enter dan biarkan proses Booting berlangsung. Ophcrack akan otomatis masuk ke windows manager menggunakan fluxbox dan langsung menjalankan Ophcrack. Proses pertama adalah mendapatkan file HASH dari partisi yang berisi file Windows kemudian di dump ke file /tmp/ophcrack.tmp

Kemudian tunggu beberapa saat untuk melakukan cracking.

Saya melakukan pengujian menggunakan spesifikasi sebagai berikut : Processor AMD +2000 1.6 Ghz, Memori 256 Mb dan dijalankan menggunakan VM-Ware.

Lalu saya menggunakan password yang sangat sederhana, yaitu “password123′ dan “password”. Hasilnya, Ophcrack mampu menebak kedua password dengan tepat dan hanya membutuhkan waktu 1 Menit!!

Lalu saya coba untuk mengkombinasikan huruf, angka dan simbol dengan memberikan password : “p4ssw0rd” dan “p4ssw0rd~!@#”. Hasilnya, Ophcrack mampu menebak “p4ssw0rd” dengan waktu 8 menit dan tidak dapat menemukan “p4ssw0rd~!@#”.

Selain menggunakan CD, dengan sedikit modifikasi, Ophcrack juga dapat dijalankan melalui USB Flashdisk. Caranya dengan menginstall SLAX ke dalam USB Flashdisk dan menambahkan modul ophcrack di SLAX serta menyalin Rainbow Tables ke dalam USB, maka Ophcrack LiveUSB sudah dapat dijalankan

Selain itu, untuk mempersingkat waktu, kita dapat mengambil file HASH terlebih dahulu yang terletak di /tmp/ophcrack.tmp kemudian baru di crack di tempat lain tanpa perlu menunggu lagi di komputer target.

Saran

Ibarat pisau bermata dua, Ophcrack dapat menjadi sangat berguna ketika ada seseorang yang lupa password Windows dan ingin me-recovery password dengan cepat dan mudah. Namun disisi lain, Ophcrack dapat jugamenjadi ’senjata’ ampuh bagi cracker untuk menjebol Windows dengan carayang sangat mudah dan cepat. Bahkan kabarnya Ophcrack ini merupakan tools yang paling cepat untuk crackpassword Windows. Untuk itu ada beberapa hal yang dapat mengurangiresiko agar password komputer kita tidak ‘dibobol’ dengan mudah.

1. Setting password BIOS komputer dan atur urutan boot agar tidak melakukan booting pertama kali dari CD atau USB.
2. Gunakan password yang terdiri dari huruf+angka+simbol agar tidak mudah di crack.

Oph… Crack!!

NB :Cara lain menggunakan ophcrack di Windows dapat dilihat disini