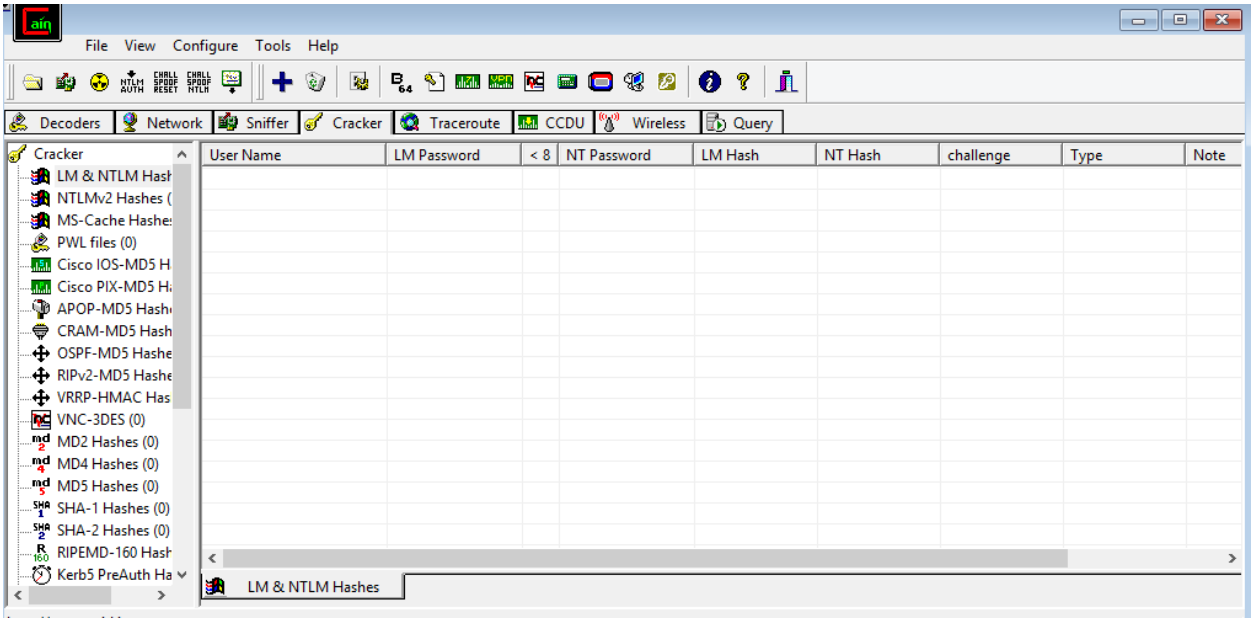
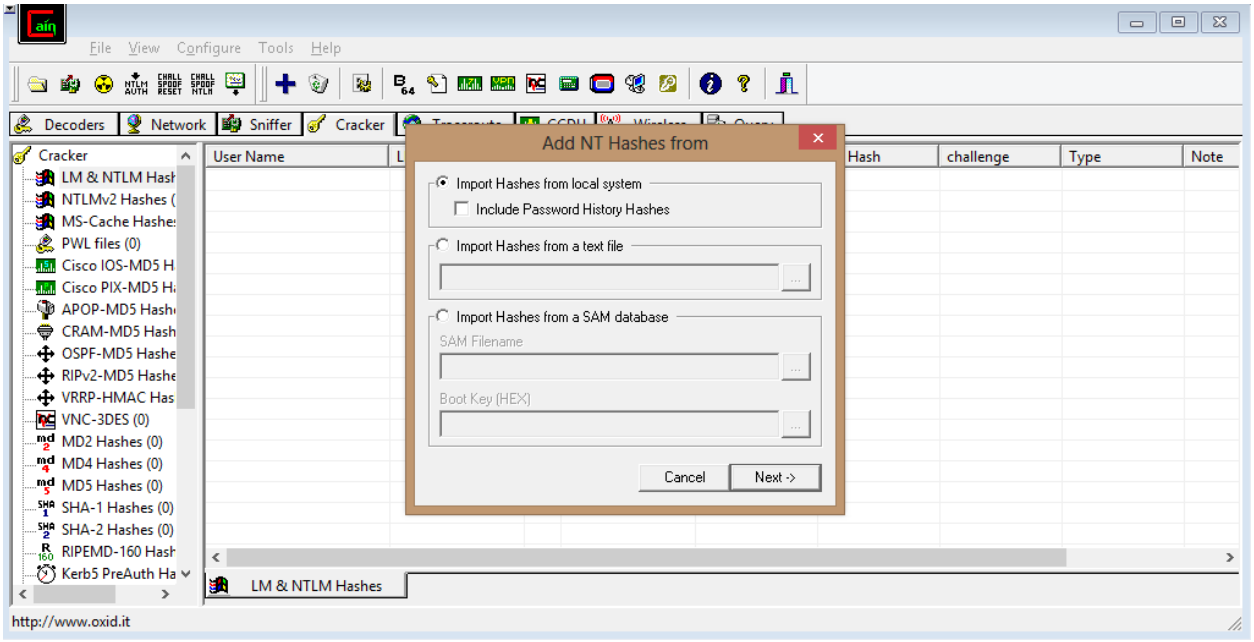
Hack your own windows with cain and abel from inside

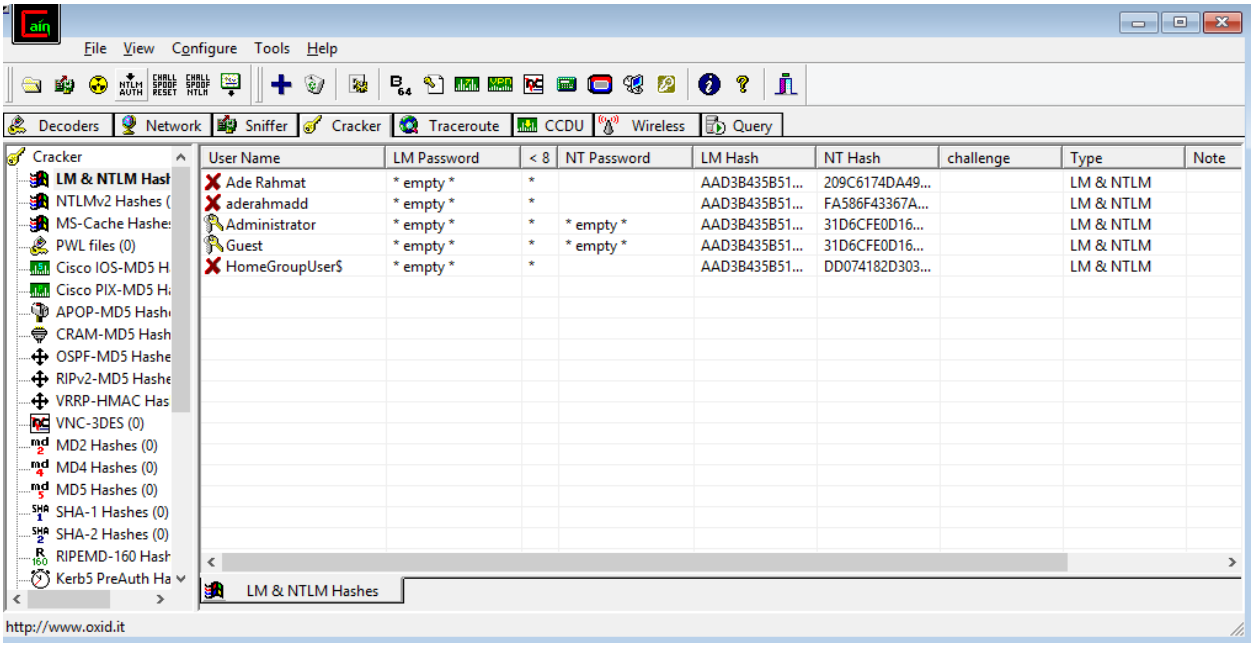
1. Install dan buka aplikasi cain and abel. Pilih tab Cracker dan pilih bagian LM & NTLM Hash



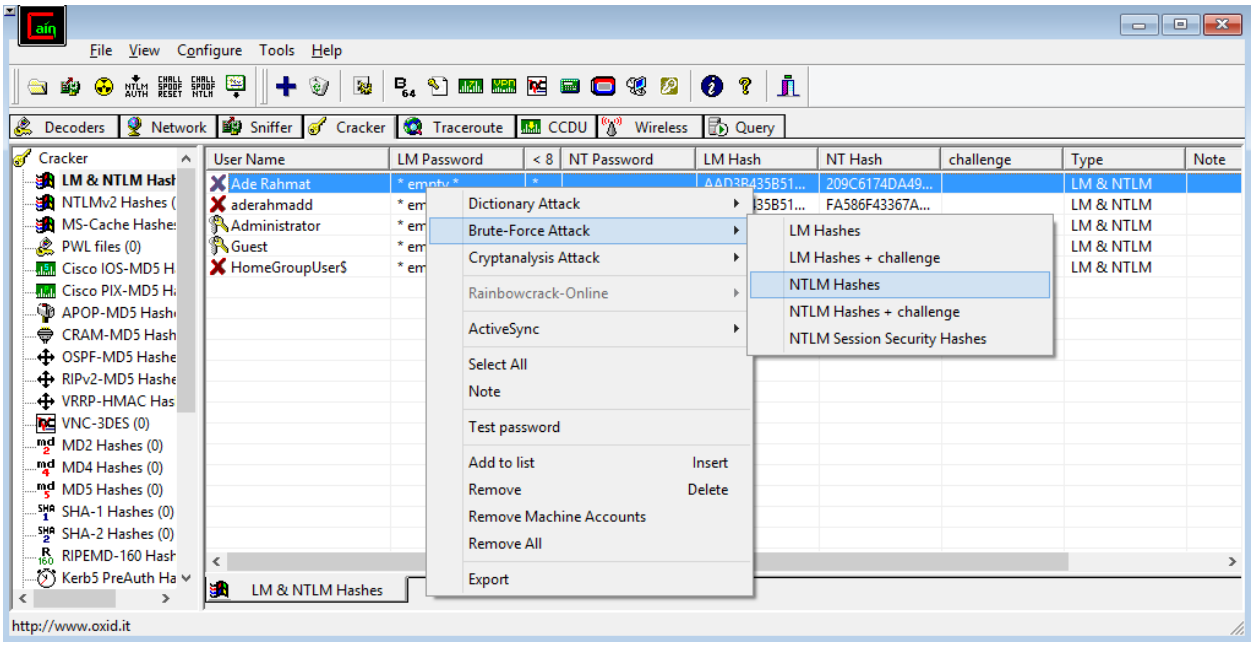
2. Klik tombol plus warna biru yang berada di bawah tab Tools. Kemudian pilih option “import hashes from local system” dan klik next



3. Setelah next diklik, maka akan tampil informasi mengenai user yang ada pada windows tersebut. kemudian pilih salah satu user yang akan kita hack (dalam hal ini user Ade Rahmat)

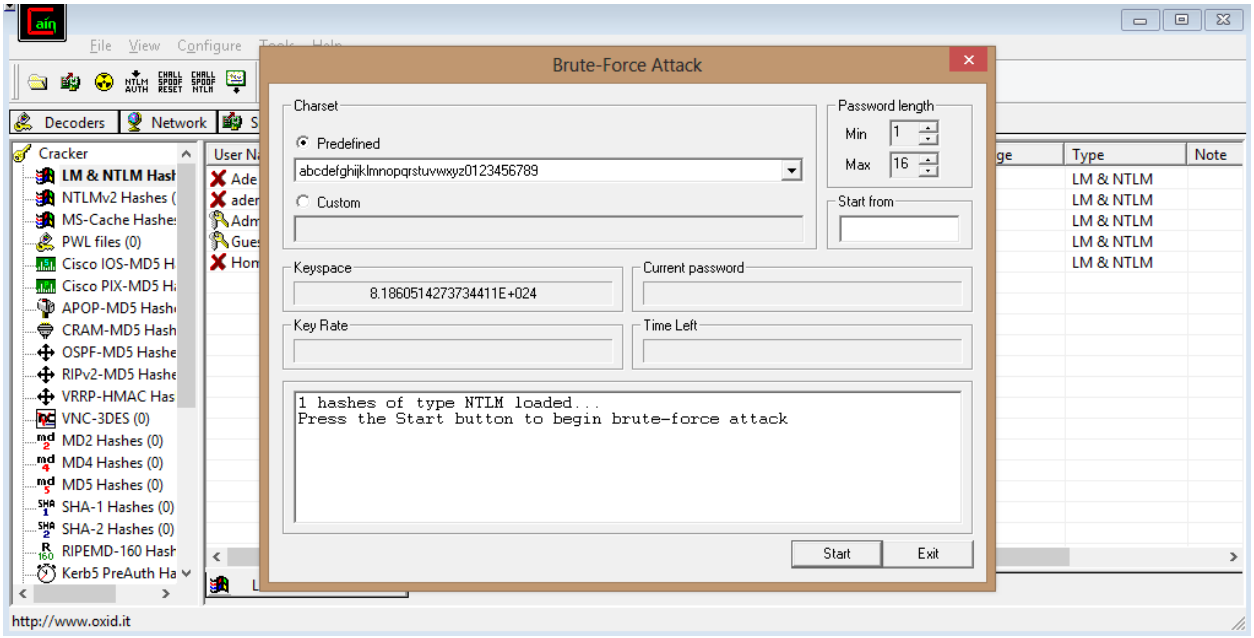


4. Klik kanan pada user yang akan kita hack dan pilih option NTLM Hashes pada bagian Brute-force attack

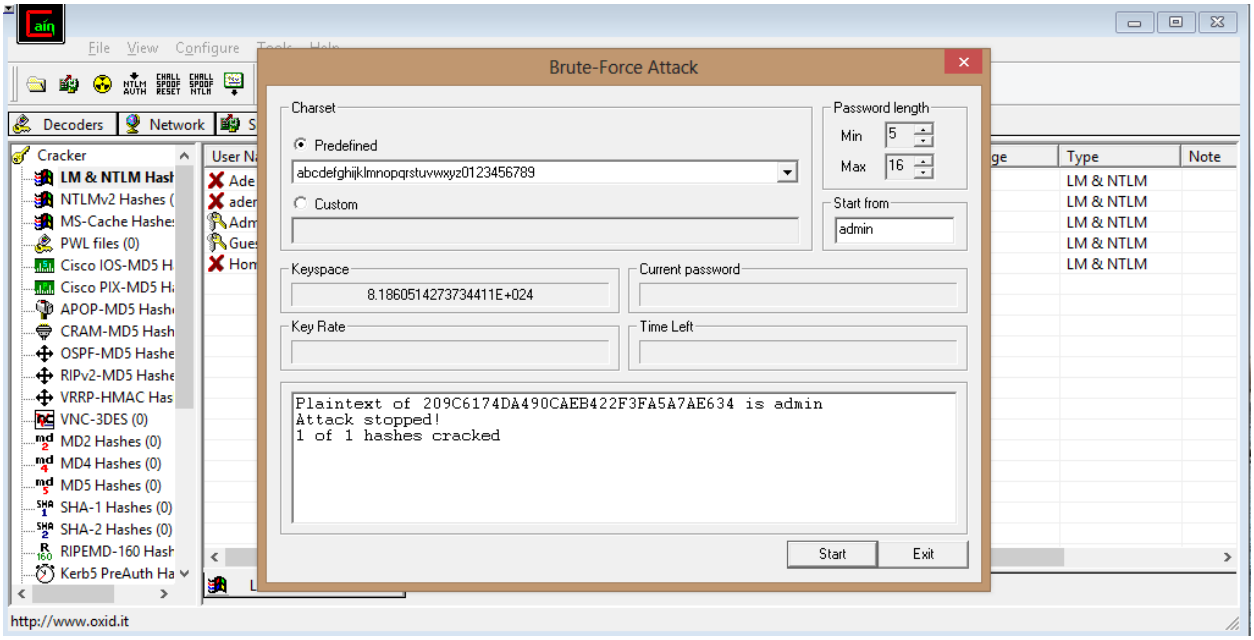


5. Akan muncul tampilan seperti gambar dibawah dengan option yang banyak. Kita bisa menentukan password yang akan dicari terdiri dari alfabet,alfabet angka, alfabet simbol dan lain-lain. kita juga bisa menentukan berapa panjang minimal dan maksimal password

yang akan kita cari. Jika selesai menyetting option password klik tombol start. Serangan brute force akan dimulai.



6. Apabila password yang dicari sudah dapat maka akan ditampilkan seperti informasi dibawah. User Ade Rahmat mempunyai password admin. Proses serangan brute force ini akan bergantung dengan kerumitan password, semakin rumit password yang dicari maka semakin lama serangan ini berhasil.



Hack your own windows password with usb bootable

1. Buat bootable linux(kali) dengan aplikasi bootable seperti rufus.
2. Restart laptop dan masuk dengan bootable yang kita buat tadi.
3. Pilih mode live agar kali linux dapat langsung digunakan tanpa proses instalasi.
4. Mount partisi windows agar dapat dibuka dengan command:
   Sudo mkdir /mnt/Hasil_Mount
   Sudo mount /dev/sda1 /mnt/Hasil_Mount
5. Kemudian buka folder Windows/System32/config, copy file SAM dan SYSTEM yang ada didalam folder tersebut ke folder root kita.
6. Kemudian jalankan samdump2 untuk mengekstrak file SYSTEM dan SAM tadi dengan command:
   Samdump2 SYSTEM SAM –o hasil.txt
7. Buka john untuk mencari password dari user windows yang telah kita ekstrak menjadi hasil.txt dengan command:
   John –format=LM hasil.txt