Farid Wazdi
09111001047
Keamanan Jaringan Komputer

TASK

1. Crack password windows.

Cracking atau meretas password windows dapat menggunakan tools-tools yang sudah ada pada saat ini, namun pada tugas kali ini salah satu tools yang digunakan adalah “pwdump” dan “cain and abel”.

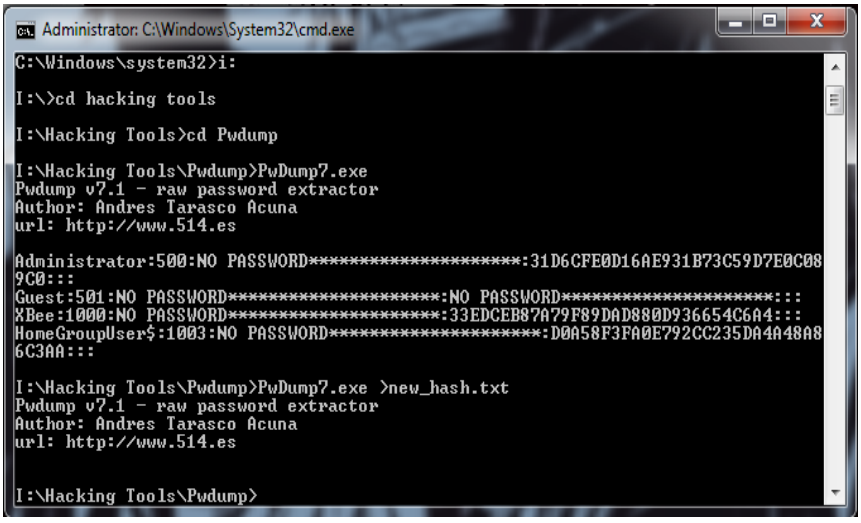
Pwdump adalah nama dari berbagai program Windows yang output LM dan password NTLM hash dari akun pengguna lokal dari Account Manager Security (SAM). Dalam rangka untuk bekerja, itu harus dijalankan di bawah account Administrator, atau dapat mengakses account Administrator pada komputer di mana hash harus dibuang. Pwdump bisa dikatakan membahayakan keamanan karena bisa memungkinkan administrator berbahaya untuk mengakses password pengguna. Sebagian besar program-program ini open-source.

Sedangkan cain and abel adalah alat pemulihan password untuk Microsoft Sistem Operasi. Hal ini memungkinkan pemulihan mudah berbagai jenis password dengan mengendus jaringan, cracking password terenkripsi menggunakan Dictionary, Brute-Force dan serangan pembacaan sandi, rekaman percakapan VoIP, decoding password orak-arik, memulihkan kunci jaringan nirkabel, mengungkapkan kotak password, mengungkap password cache dan menganalisis routing yang protokol. Program ini tidak mengeksploitasi kerentanan software atau bug yang tidak dapat diperbaiki dengan sedikit usaha. Ini mencakup beberapa aspek keamanan / kelemahan hadir dalam standar protokol, metode otentikasi dan mekanisme caching; tujuan utamanya adalah pemulihan disederhanakan password dan kredensial dari berbagai sumber, namun juga kapal beberapa "non standard" utilitas untuk pengguna Microsoft Windows.

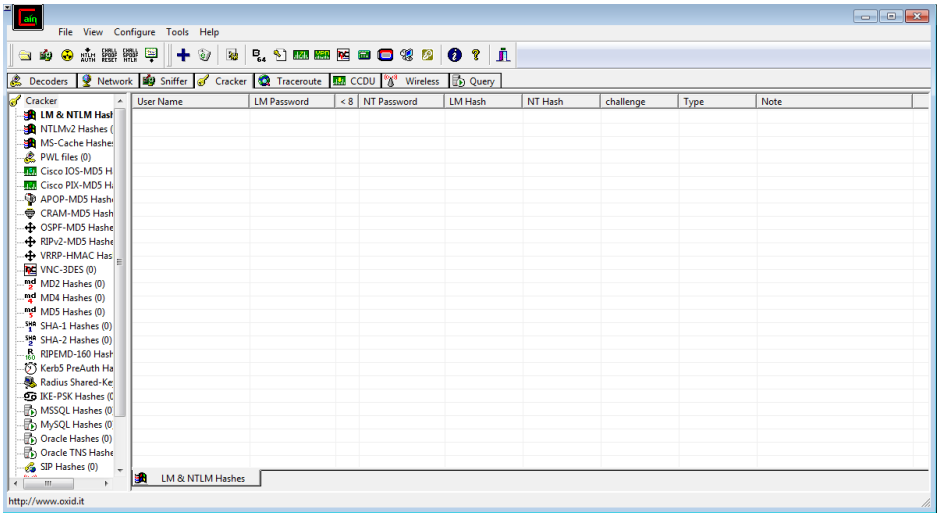
Farid Wazdi
09111001047
Keamanan Jaringan Komputer

Langkah-langkah cracking password windows :

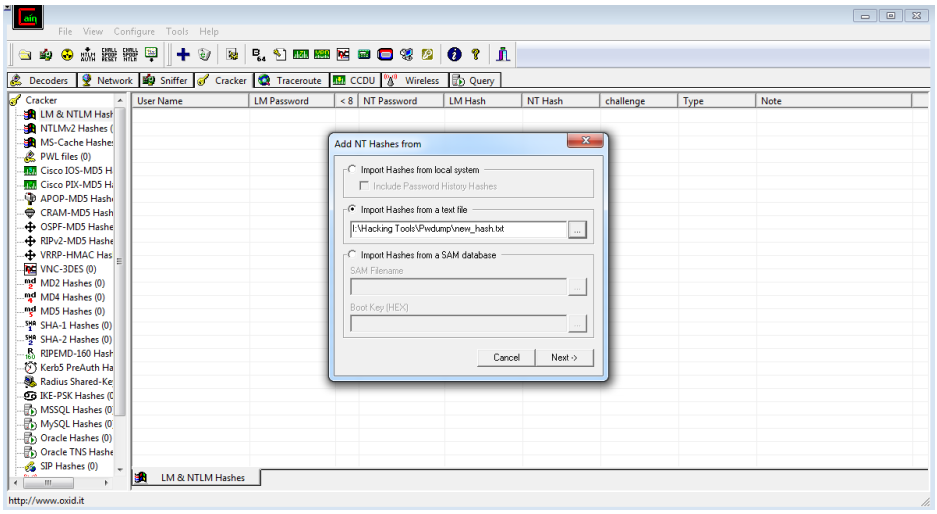
1. Langkah pertama adalah menggunakan pwdump yang dipanggil lewat command prompt (CMD) untuk mendapatkan hash. CMD dibuka dengan cara “run administrator”. Ketikkan perintah seperti gambar berikut : perintah pertama adalah untuk masuk ke direktori atau tempat penyimpanan pwdump. Lalu jalankan pwdump.exe lewat command prom dan buat hash dalam bentuk .txt.



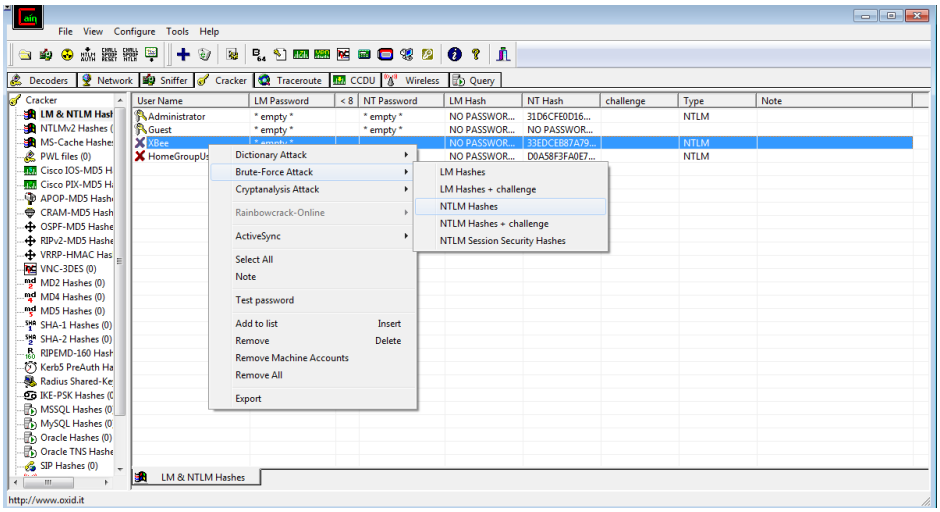
2. Langkah kedua setelah di dapatkan hash, buka aplikasi cain and abel yang sudah diinstall terlebih dahulu. Lalu pilih menu cracker seperti pada gambar dan pilih LM & NTML Hash.



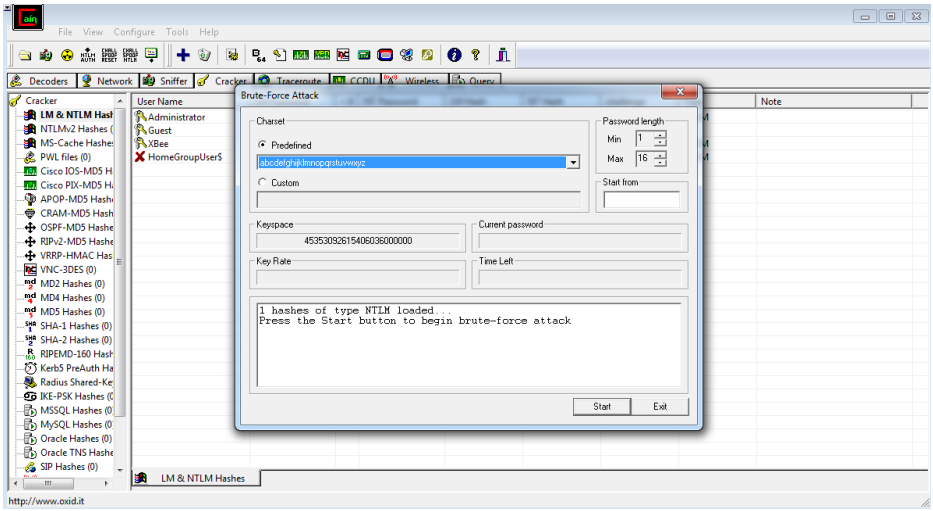
3. Langkah ketiga adalah klik tanda “plus” di atas, untuk membuka tempat penyimpanan hash yang tadi sudah di dapatkan. Jika berhasil, tampilan akan berubah seperti gambar di bawah :



4. Langkah keempat adalah klik next dan tampilan akan tampak seperti gambar di bawah. Lalu pilih user mana yang tadi kita ingin crack passwordnya. Setelah itu pilih brute force attack dan NTLM Hashes.



5. Langkah kelima setelah muncul tampilan seperti gambar di bawah adalah mengisi beberapa kemungkinan yang di dapat dari instuisi seperti password length atau start from lalu klik start.



6. Langkah terakhir adalah menunggu sampai di dapatkan password seperti gambar di bawah.