“Dumping And Cracking SAM Hashes to Extract PlainText Password"

Mata Kuliah:

Keamanan Jaringan Komputer

Dosen Pengampu:

Prof. Deris Stiawan, M.T., Ph.D.
Adi Hermansyah, M.T.

Dibuat oleh:

Anya Nur Defitri 09011182126017

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

Pendahuluan

Security Account Manager (SAM) yang artinya Manajer Akun Keamanan merupakan database di Windows yang menyimpan data login pengguna, termasuk kata sandi yang dienkripsi (di-hash). File ini menyimpan kata sandi pengguna dalam bentuk hash (LM dan NTLM). Kata sandi yang tersimpan dalam bentuk hash ini sulit untuk dibaca kembali, sehingga dianggap aman. Namun, hacker bisa mengekstrak hash ini jika berhasil masuk ke komputer. Dengan hash ini, mereka bisa mencoba berbagai cara untuk menebak kata sandi asli, menganalisis pola kata sandi, atau bahkan menggunakannya untuk masuk ke sistem lain. Untuk mengakses SAM, hacker harus memiliki hak akses administrator. Oleh karena itu, mengukur kekuatan kata sandi sangat penting untuk menjaga keamanan sistem. Proses ini melibatkan pengambilan hash dari SAM lalu mencoba untuk mengubahnya kembali ke bentuk kata sandi biasa.

Tujuan

1. Mengekstrak kata sandi terenkripsi: Menggunakan alat pwdump7, kita akan mengambil salinan digital dari kata sandi yang telah diubah menjadi kode rahasia (hash) dan disimpan di dalam sistem operasi Windows.
2. Memecahkan kode rahasia: Dengan bantuan alat Ophcrack, kita akan mencoba menebak kata sandi asli berdasarkan kode rahasia yang telah kita dapatkan sebelumnya. Proses ini sering disebut dengan password cracking.

Praktik

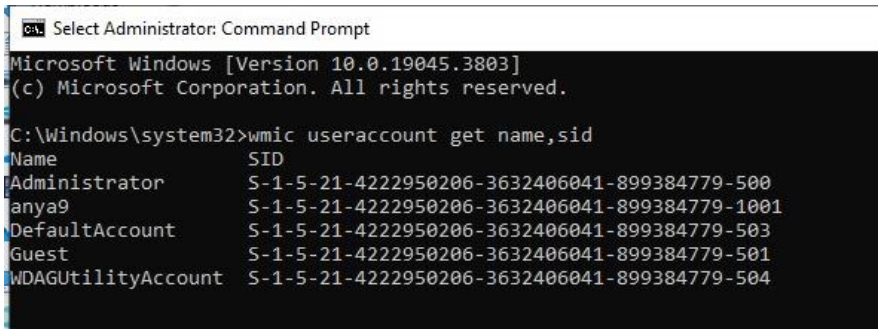
Sebelum memulai praktik, ada beberapa yang perlu dipersiapkan sebagai berikut:

- Persiapan Alat: Anda perlu menyiapkan dua alat utama, yaitu pwdump7 dan Ophcrack. Kedua alat ini digunakan untuk mengekstrak dan memecahkan hash kata sandi.
- Lokasi Alat: Kedua alat tersebut biasanya terletak di dalam folder "Z:\CEH-Tools\CEHv10 Module 06 System Hacking\Password Cracking Tools".
- Sistem Operasi: Praktikum ini dirancang untuk dijalankan pada sistem operasi Windows 10.
- Download: Jika Anda belum memiliki alat-alat tersebut, Anda dapat mengunduhnya dari alamat yang diberikan.
- Hak Akses: Untuk menjalankan alat-alat ini, Anda memerlukan hak akses administrator.

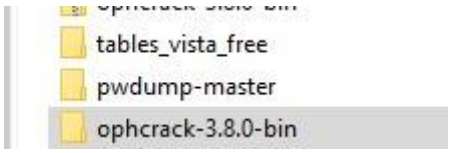
Setelah mempersiapkan alat dan sebagainya, maka kita akan memulai praktik nya. Berikut beberapa caranya:

1. Pertama, kita mencari tahu User ID dengan username menggunakan cmd administrator mode.

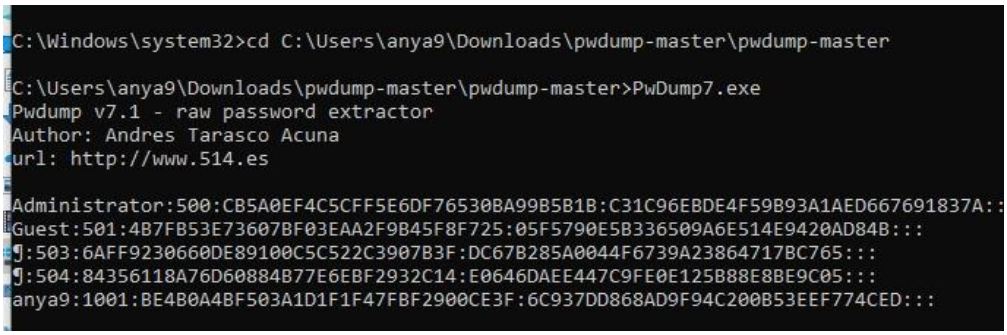
2. Membuat daftar lengkap semua akun pengguna yang ada di sistem dengan mengetikkan perintah wmic useraccount get name,sid di command prompt. Perintah ini akan menampilkan nama pengguna dan SID (nomor identitas unik) dari setiap akun.



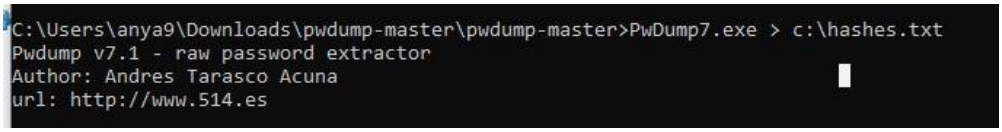
3. Kemudian mendownload dan mengekstrak file pwdump dan ophcrack. File-file ini berisi program yang akan membantu kita dalam menganalisis kata sandi yang tersimpan di sistem.



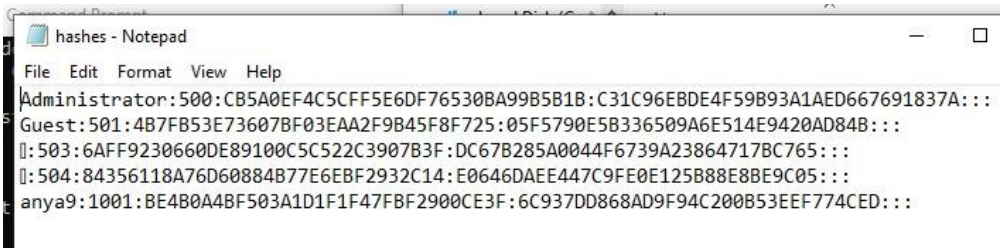
4. Setelah itu buka dan copy lokasi file pwdump dan klik enter untuk masuk ke directory pwdump master , kemudian ketik PwDump7.exe untuk mendapatkan dan menampilkan password hashes dan userID.



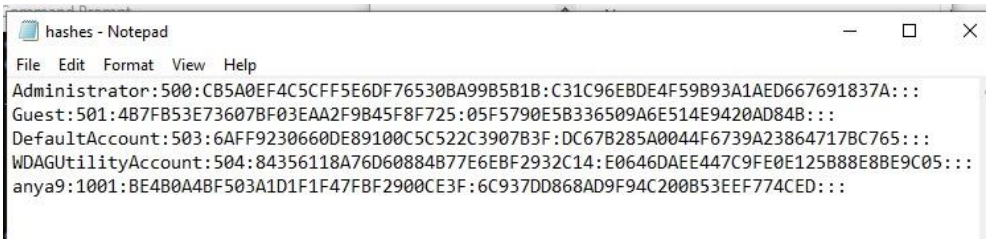
5. Kemudian untuk memindahkan dan men-copy semua data hasil dari PwDump7.exe ke hashes.txt menggunakan command PwDump7.exe > c:\hashes.txt



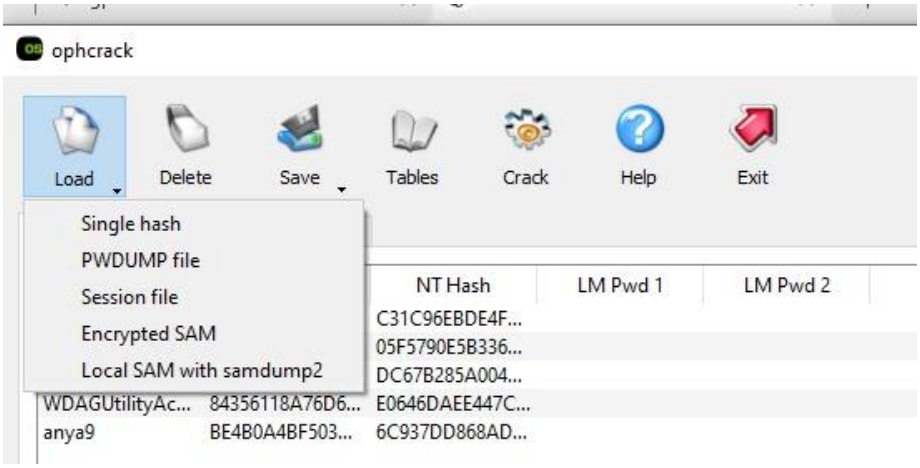
6. Berikut ini adalah isi file dari hashes.txt.



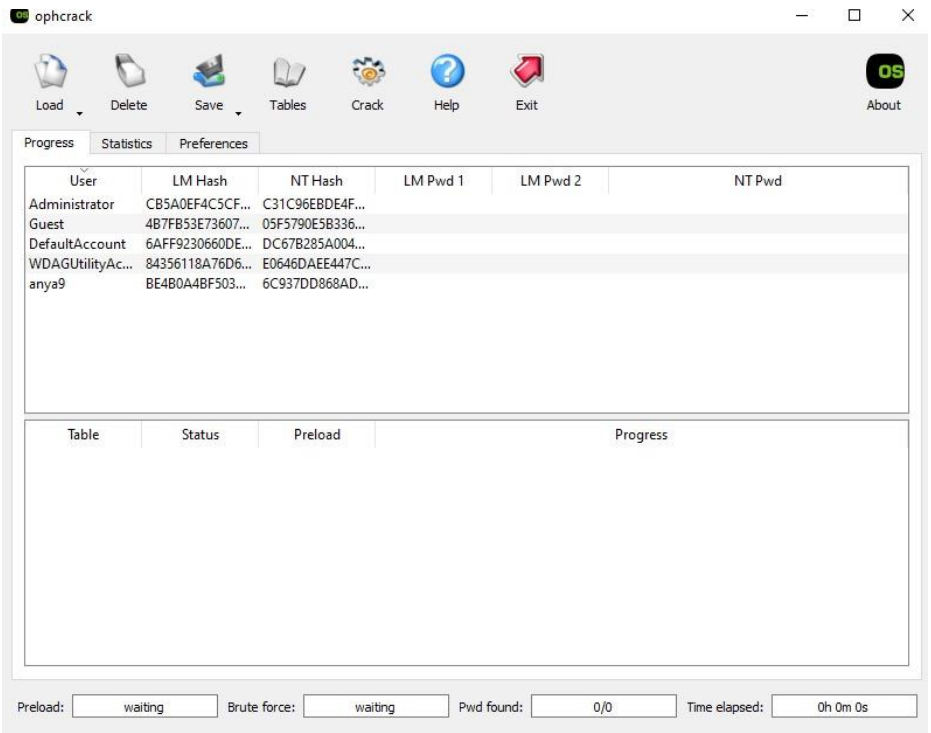
7. Dilanjutkan dengan mengisi semua username yang kosong sesuai dengan username pengguna pada step 2 kemudian save file hashes.txt



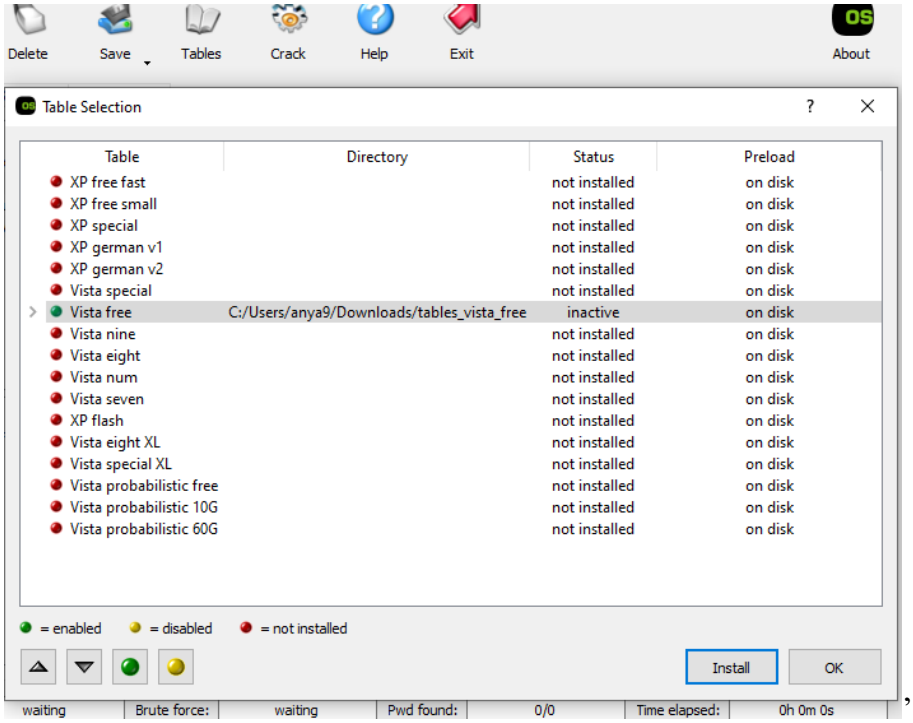
8. Kemudian buka oph crack kemudian pilih load PWDUMP file dan pilih file hashes.txt sebelumnya.



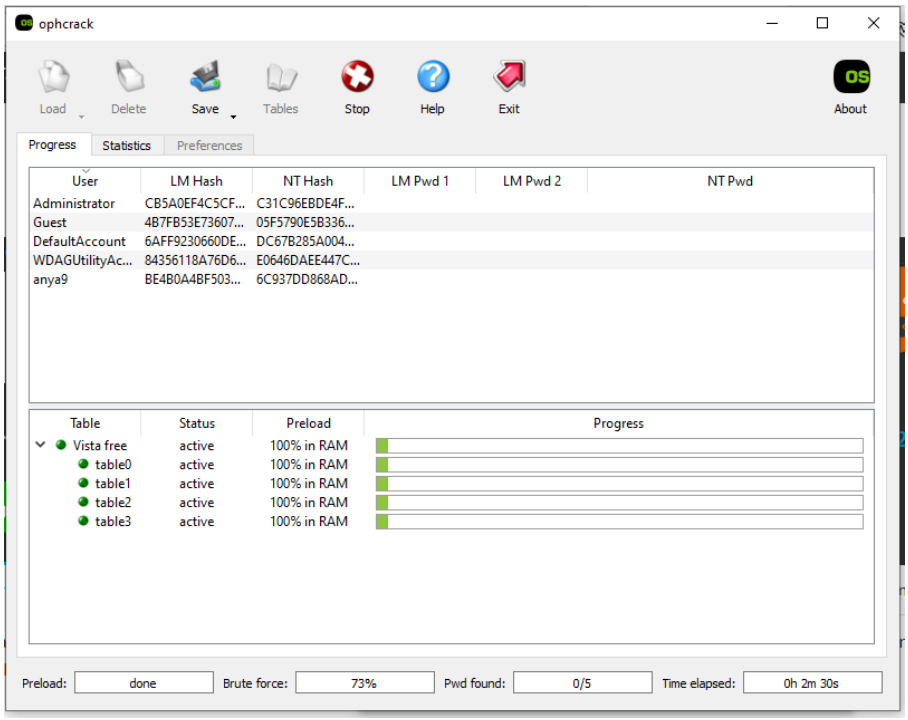
9. File Hashes tersebut akan tampil dengan LM Hash dan NT Hash sesuai username user.



10. Kemudian, klik table dan opsi pemilihan table, pilih “vista free”. Setelah itu, klik “Install”, lalu pindah table “Vista free” yang sudah diunduh sebelumnya. Tabel "vista free" bisa diunduh melalui tautan: (https://ophcrack.sourceforge.io/tables.php).



11. Setelah tabel ditampilkan, klik ikon crack di samping ikon untuk memulai proses pemecahan kata sandi. Ophcrack akan membutuhkan beberapa menit untuk menyelesaikan pemecahan kata sandi. Tunggu hingga proses selesai.



12. Setelah selesai, password akan ditampilkan. Jika hasilnya menunjukkan "not found," kemungkinan besar hal ini terjadi karena Windows 10 versi terbaru secara default tidak lagi menyimpan password dalam bentuk hash LM karena alasan keamanan. Selain itu, beberapa akun seperti "Guest" atau "DefaultAccount" mungkin tidak memiliki password atau sedang tidak aktif, sehingga Ophcrack tidak menemukan apapun.