KEAMANAN JARINGAN KOMPUTER

Disusun Oleh:

Josua Benfrino Pasaribu

(09011282126056)

PRODI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2024

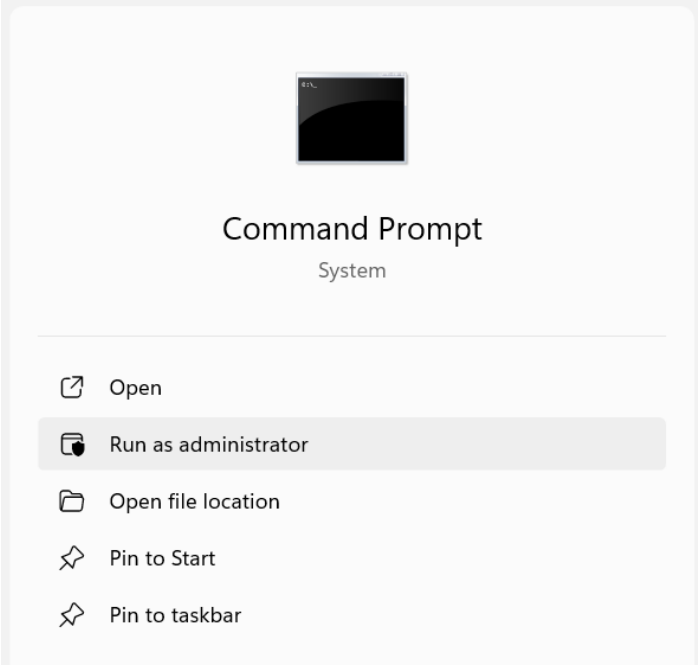
Dumping And Cracking SAM Hashes to Extract PlainText Password

SAM (Security Account Manager) adalah sebuah basis data di sistem operasi Windows yang berfungsi untuk menyimpan informasi penting terkait akun pengguna, seperti nama akun dan hash dari password. Hash ini merupakan representasi dari password asli yang diolah melalui algoritma tertentu, sehingga password tidak disimpan dalam bentuk teks biasa demi meningkatkan keamanan. Saat pengguna mencoba login, sistem akan membandingkan hash dari password yang dimasukkan dengan hash yang tersimpan di SAM untuk memverifikasi keaslian login tersebut.

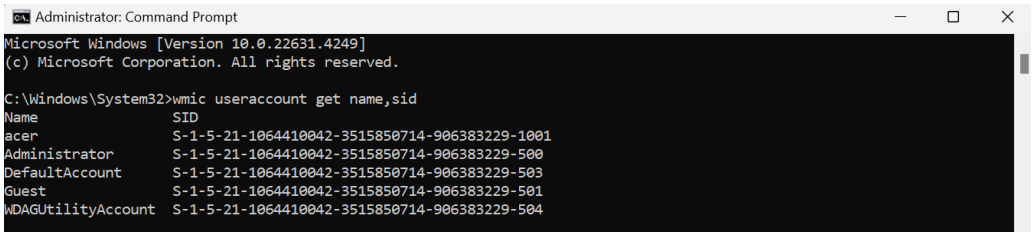
File SAM ini disimpan di direktori sistem Windows dan hanya dapat diakses oleh sistem operasi, yang membantu mencegah akses tidak sah terhadap data sensitif seperti password. Meskipun demikian, jika ada pihak yang memiliki hak akses tinggi (administrator), mereka bisa mencoba untuk mengambil file SAM dan kemudian melakukan proses cracking terhadap hash untuk memperoleh password asli. Oleh karena itu, menjaga keamanan akses terhadap file ini menjadi sangat penting untuk mencegah serangan yang berpotensi membahayakan sistem.

Langkah-langkahnya ialah sebagai berikut:

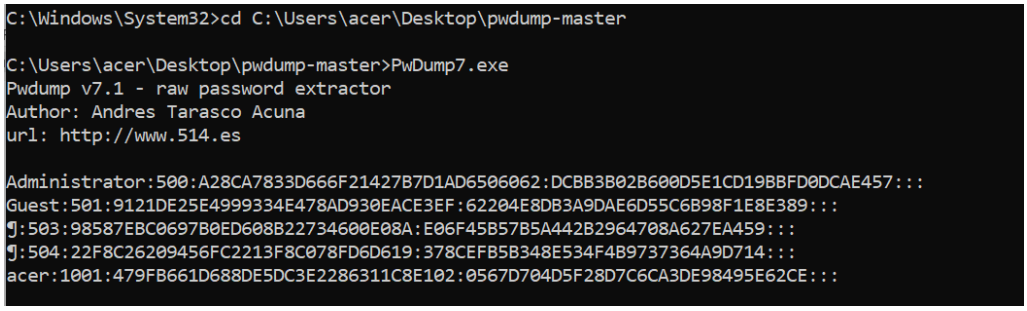
1. Pertama, mencari User ID berdasarkan username dengan menggunakan Command Prompt dalam mode administrator.



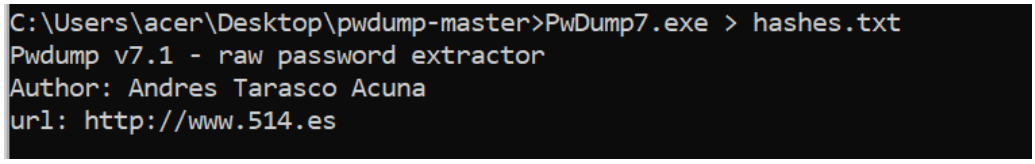
2. Selanjutnya, masukkan kode wmic useraccount get name,sid yang berfungsi untuk menampilkan daftar seluruh akun pengguna di sistem beserta SID (Security Identifier).

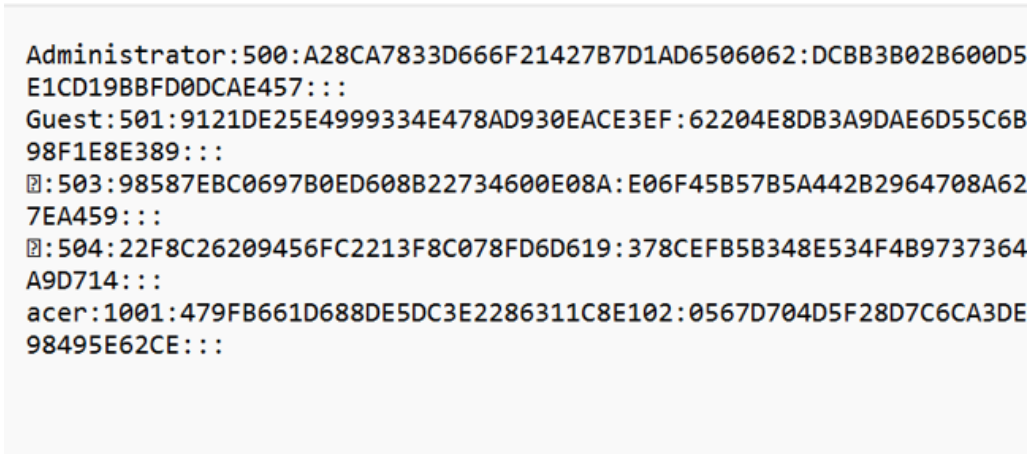


3. Selanjutnya, buka dan salin lokasi file pwdump, lalu tekan Enter untuk masuk ke direktori pwdump-master. Setelah itu, jalankan perintah `PwDump7.exe` untuk mendapatkan dan menampilkan hash password serta User ID.

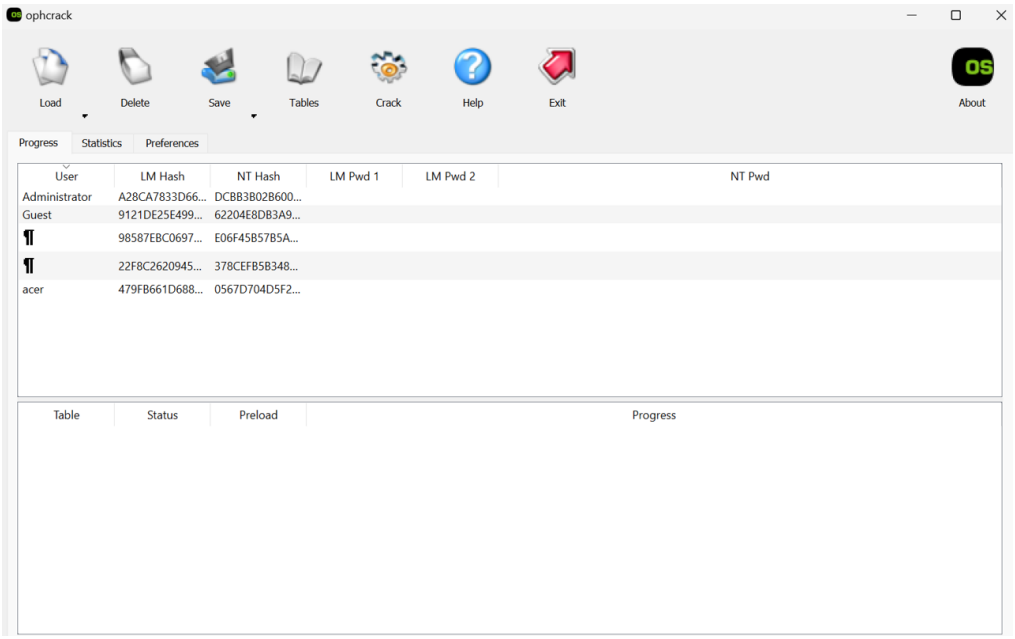


4. Selanjutnya, untuk memindahkan dan mengcopy semua data hasil dari PwDump7.exe ke file hashes.txt, gunakan perintah PwDump7.exe > c:\hashes.txt.

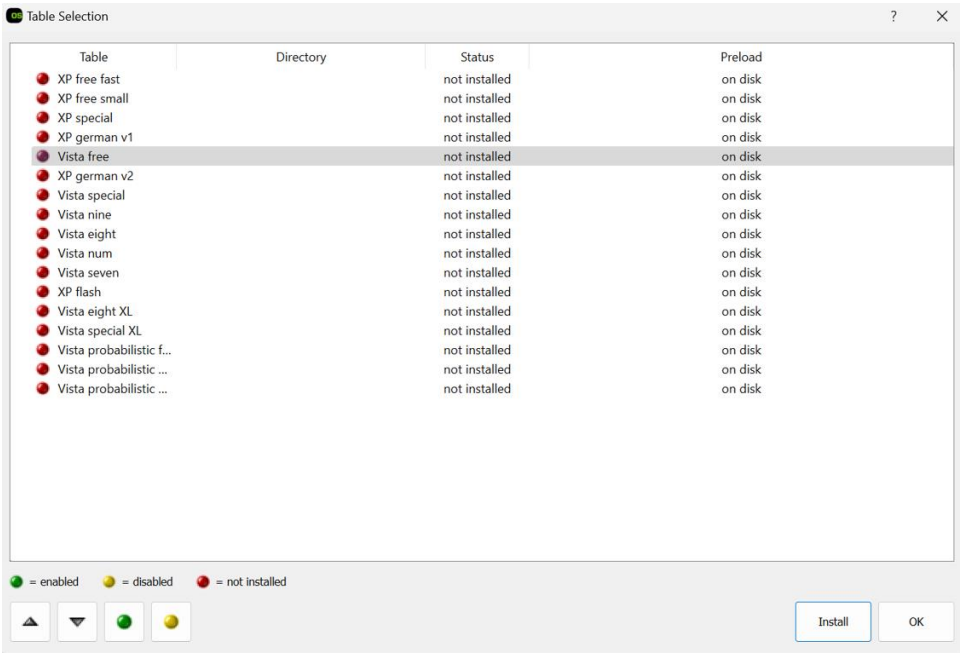




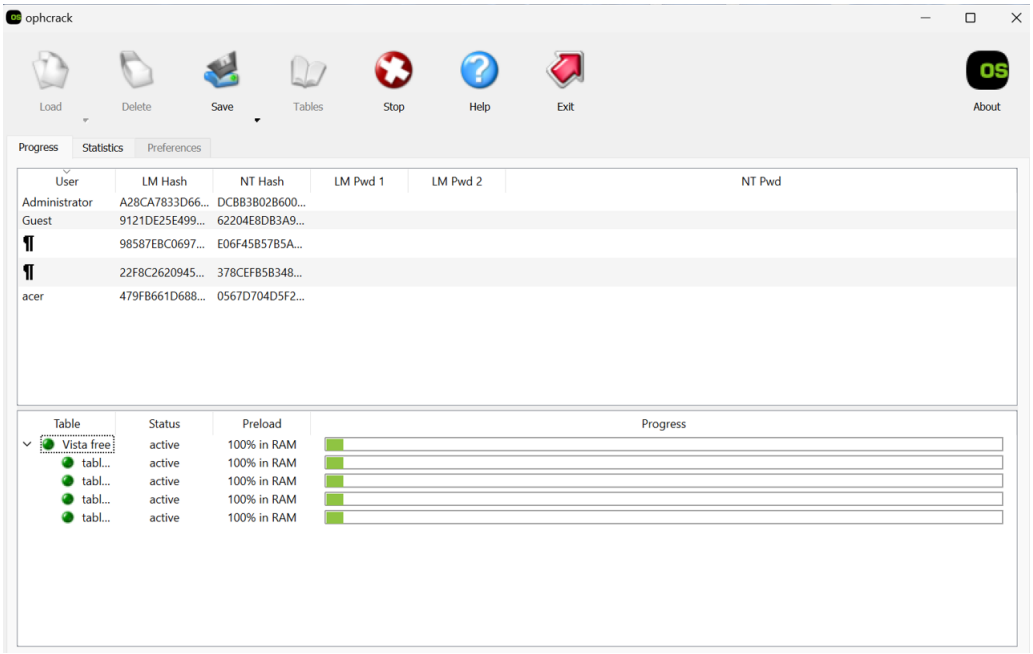
5. Lalu, buka Ophcrack, lalu pilih pada bagian load PWDUMP file dan pilih file hashes.txt yang telah dibuat sebelumnya. Pilih file hash tersebut, maka akan tampil dengan LM hash dan NT hash, masing masing sesuai dengan username pengguna.



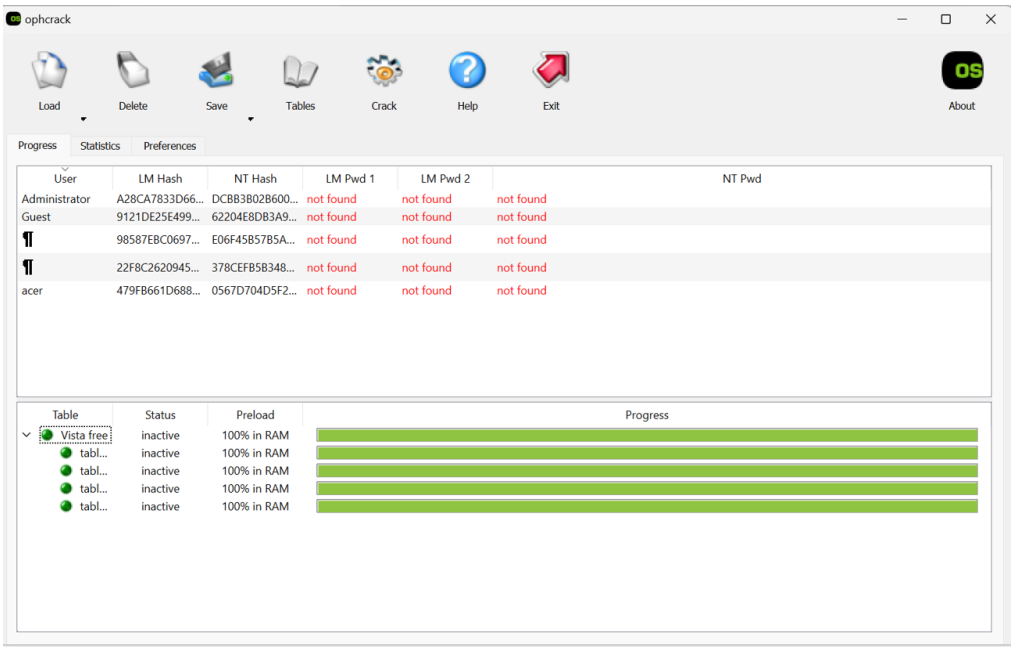
6. Selanjutnya, klik pada table dan pilih Vista Free di bagian table selection, lalu klik install. Setelah itu, pilih tabel Vista Free yang telah didownload sebelumnya.



7. Setelah tabel muncul, klik ikon crack yang terletak di samping ikon untuk memulai proses pemecahan kata sandi. Ophcrack akan membutuhkan beberapa menit untuk menyelesaikan pemecahan kata sandi, jadi tunggu hingga proses tersebut selesai.



8. Setelah proses selesai, kata sandi akan ditampilkan. Jika hasilnya menunjukkan "not found", kemungkinan besar hal ini disebabkan oleh versi terbaru Windows 11 yang secara default tidak lagi menyimpan kata sandi dalam hash LM demi alasan keamanan. Selain itu, beberapa akun seperti Guest atau Administrator mungkin tidak memiliki kata sandi atau sedang tidak aktif, sehingga Ophcrack tidak dapat menemukan apa pun.



KESIMPULAN

Kesimpulannya, SAM (Security Account Manager) adalah basis data penting di Windows yang menyimpan hash password dan informasi akun pengguna dengan tujuan menjaga keamanan sistem. File SAM tidak menyimpan password dalam bentuk teks biasa, melainkan dalam bentuk hash yang lebih sulit untuk disalahgunakan. Meski file ini dilindungi oleh sistem, pengguna dengan hak akses tinggi masih berpotensi mencurinya dan memecahkan hash untuk mendapatkan password asli. Oleh karena itu, keamanan akses ke file SAM sangat penting untuk mencegah risiko serangan terhadap sistem.