TUGAS
KEAMANAN JARINGAN KOMPUTER

Nama : **Ana Emilia Priyanti**

NIM : **09011182126029**

Jurusan : **Sistem Komputer**

Dosen : **Prof. Dr. Deris Stiawan, S.Kom., M.T.**

FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER
UNIVERSITAS SRIWIJAYA
2024

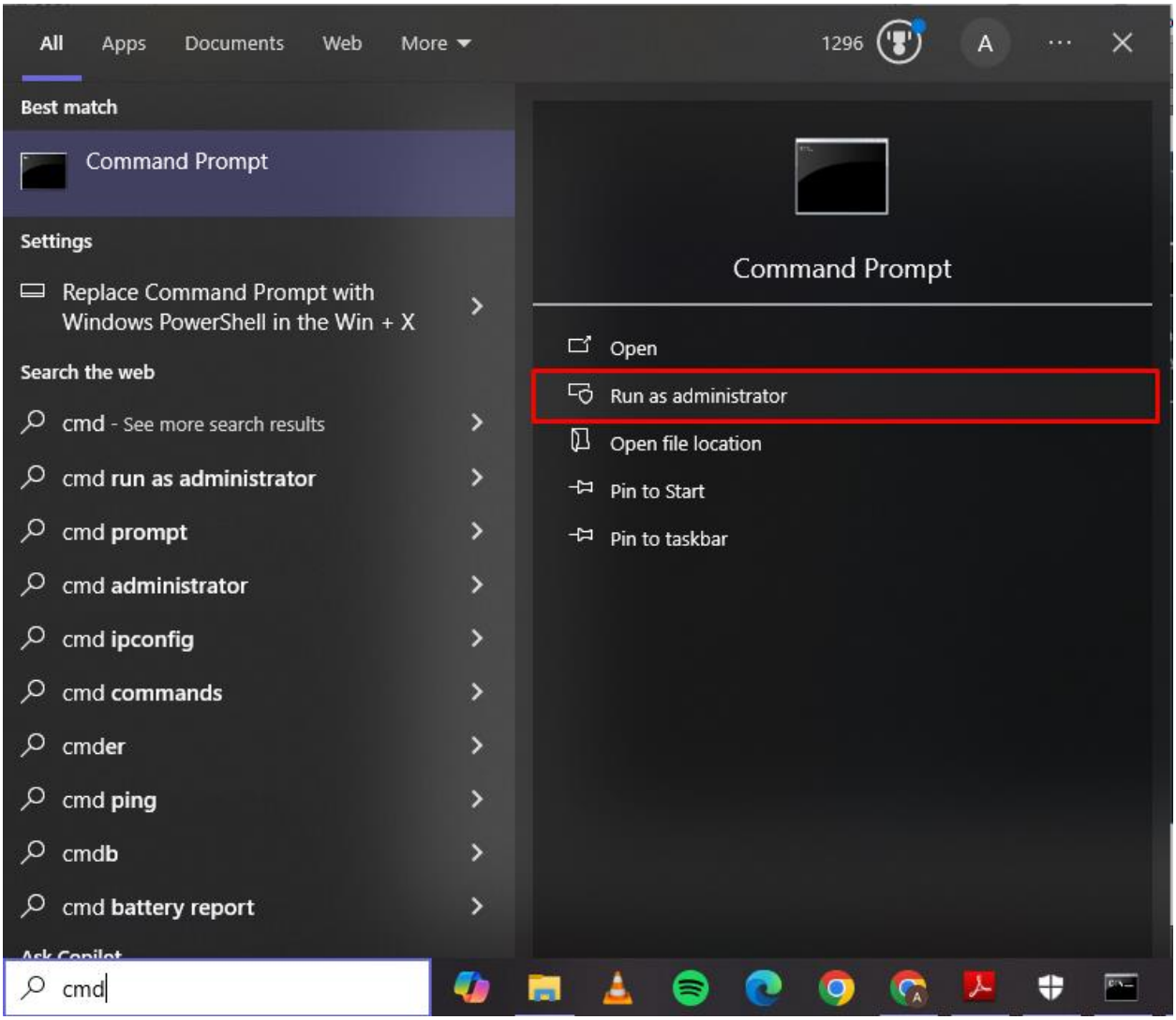
Dumping and Cracking SAM Hashes to Extract PlainText Password

File Security Account Manager (SAM) pada sistem operasi Windows berperan sebagai gudang data yang menyimpan informasi rinci tentang setiap pengguna, termasuk kata sandi yang telah dienkripsi dalam bentuk hash. Meskipun enkripsi ini dirancang untuk mengamankan kata sandi, namun hash tersebut dapat diekstrak oleh penyerang yang berhasil mengakses sistem.

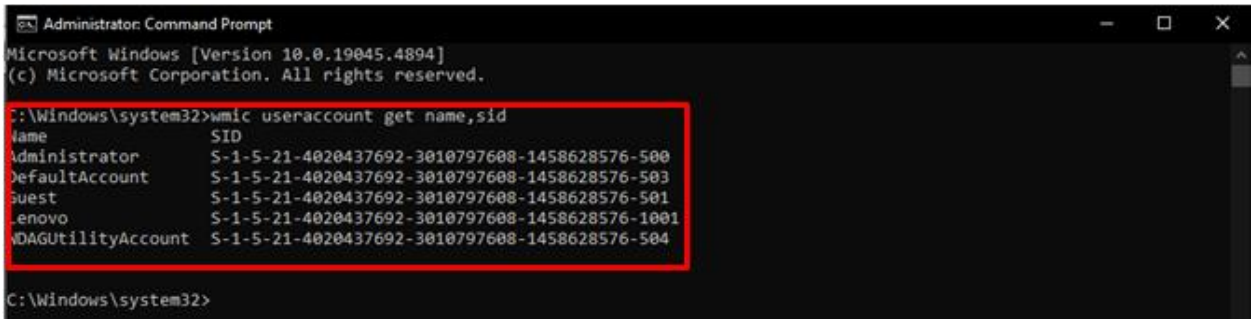
Hash yang telah diekstrak ini kemudian dapat dimanfaatkan untuk melakukan berbagai serangan siber, seperti mencoba menebak kata sandi asli (cracking), menggunakan hash tersebut untuk mengakses sistem lain yang mungkin menggunakan kata sandi yang sama, atau menganalisis pola dalam hash untuk memecahkan kata sandi lainnya.

Untuk dapat mengakses dan mengekstrak data dari file SAM, seseorang memerlukan hak akses administratif pada sistem. Proses ekstraksi hash dan pemecahan kata sandi ini seringkali dilakukan untuk memahami kerentanan sistem dan mencari tahu cara meningkatkan keamanan.

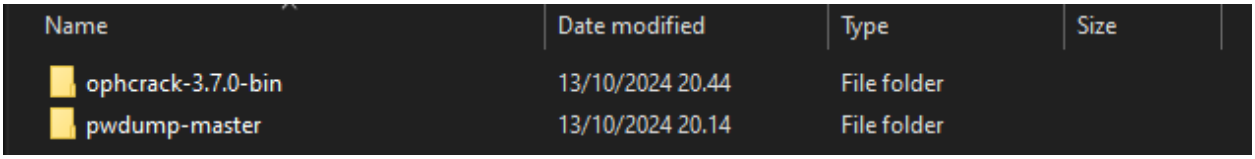
1. Sebelum memulai praktikum ini, kita perlu mencari ID pengguna yang terkait dengan nama pengguna pada mesin Windows 10
2. Nyalakan mesin Windows 10 dan masuk (login)
3. Buka Command Prompt dalam mode Administrator, untuk membukanya ketik “cmd” di kolom pencarian, lalu klik kanan pada “Command Prompt” dan pilih “Run as Administrator” seperti gambar dibawah ini.



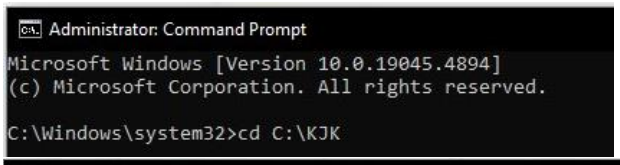
4. Di jendela Command Prompt, ketik **"wmic useraccount get name, sid"** lalu tekan Enter
5. Dengan menjalankan perintah tersebut, kita mendapatkan nama pengguna dan UserID masing-masing. Catat setiap UserID untuk langkah-langkah selanjutnya.

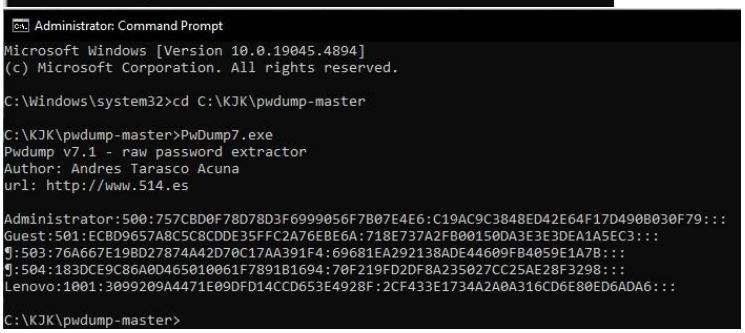


6. Kemudian download dan ekstrak file pwdump dan ophcrack

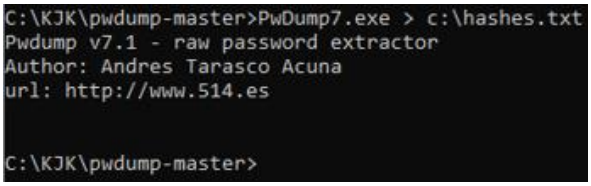


7. Setelah itu buka dan copy lokasi file pwdump dan klik “Enter” untuk masuk ke directory pwdump-master, kemudian ketik **“PwDump7.exe”** untuk mendapatkan dan menampilkan password husnes dan UserID.

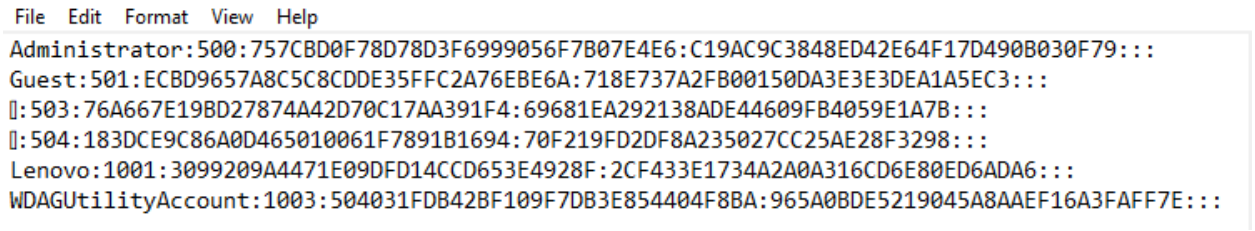




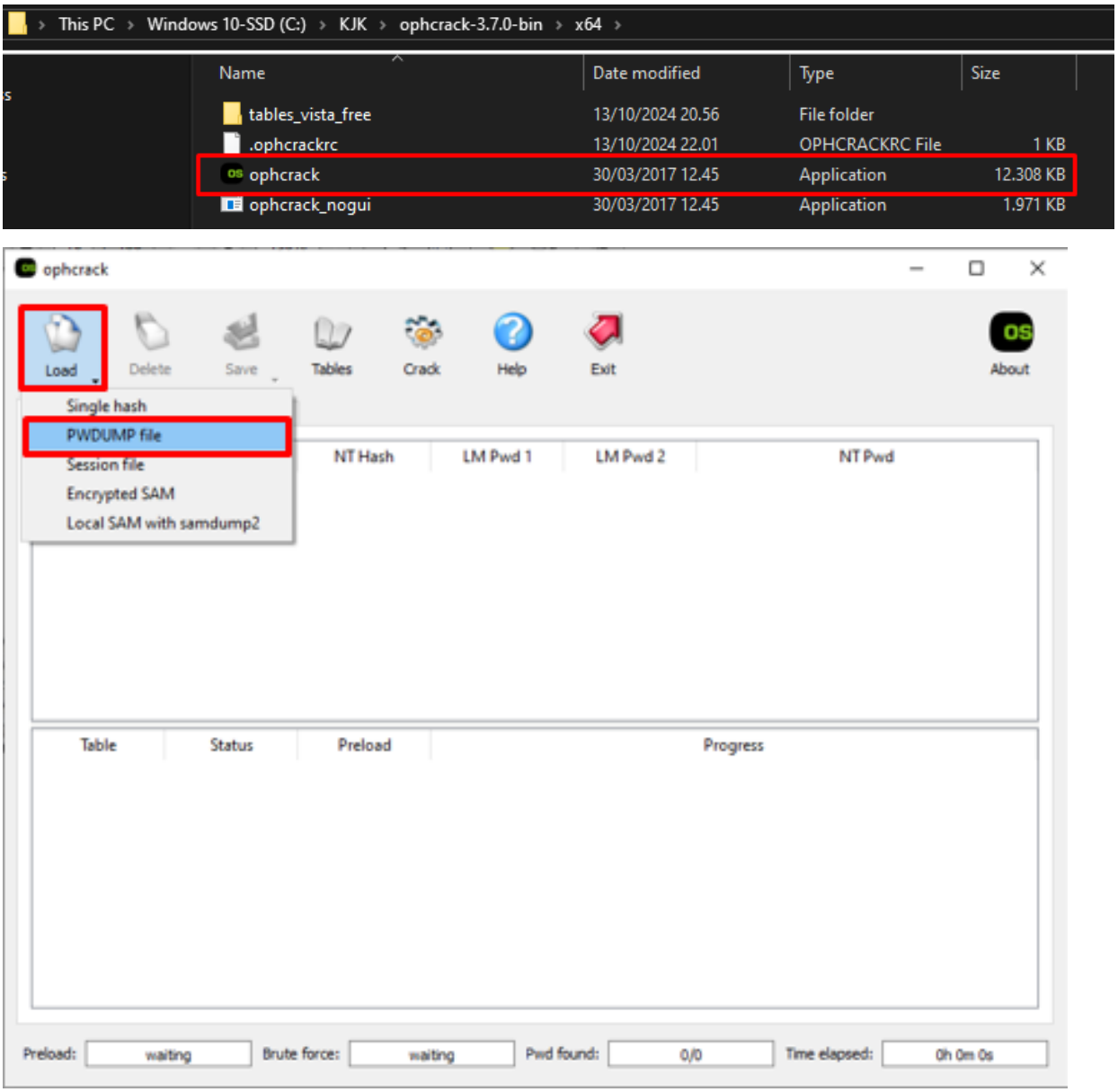
8. Sekarang, pada jendela Command Prompt, ketik **“PwDump7.exe > c:\hashes.txt”** lalu tekan “Enter”.
9. Dengan menjalankan perintah ini, PwDump7.exe akan menyalin semua data dari PwDump7.exe ke file c:\hashes.txt.



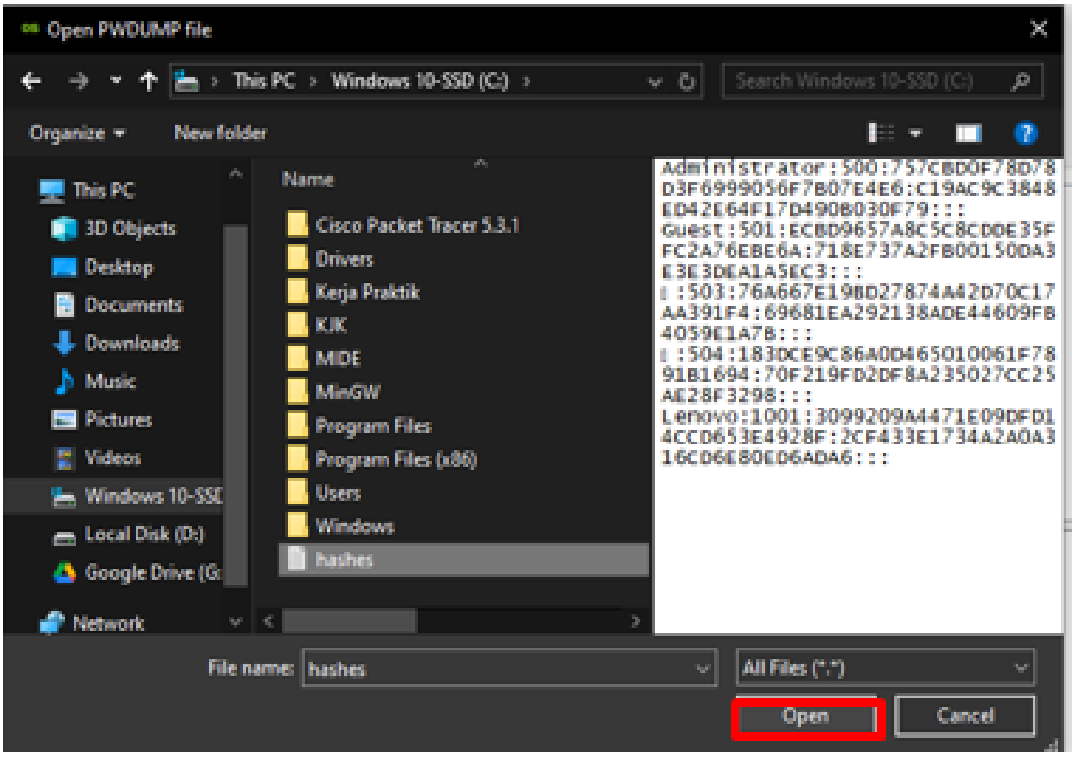
10. Untuk memeriksa hash yang telah dihasilkan, navigasi ke drive c dan buka file hashes.txt dengan Notepad. Lalu, tempatkan nama pengguna di depan UserID masing-masing yang telah dikumpulkan.



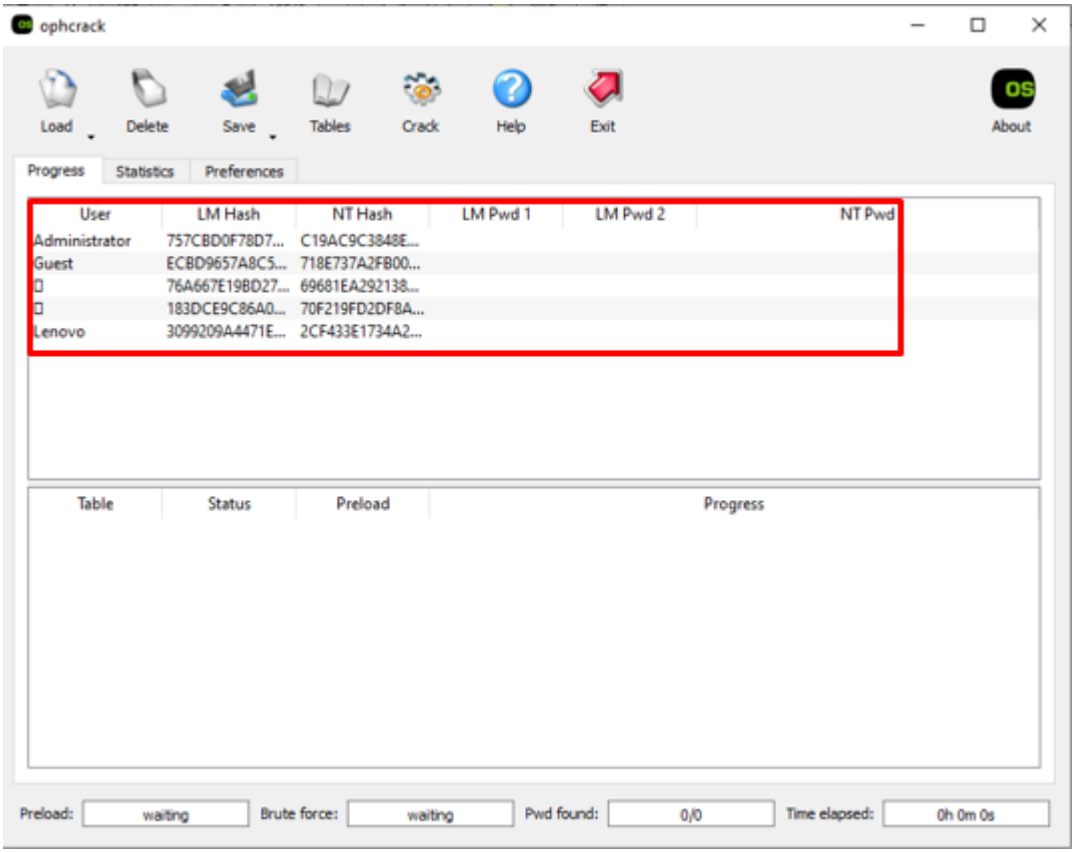
11. Selanjutnya buka ophcrack lalu pilih load PWDUMP file dan pilih file hashes.txt yang tadi.



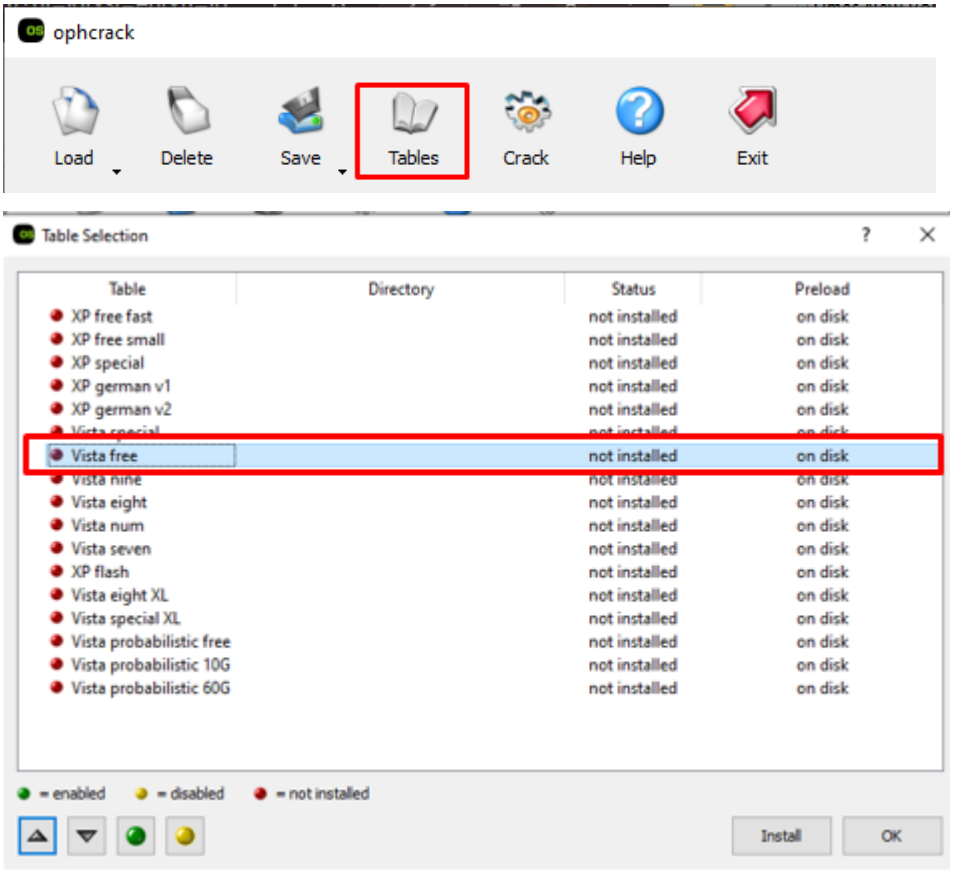
12. Telusuri file hashes.txt tadi lalu klik open



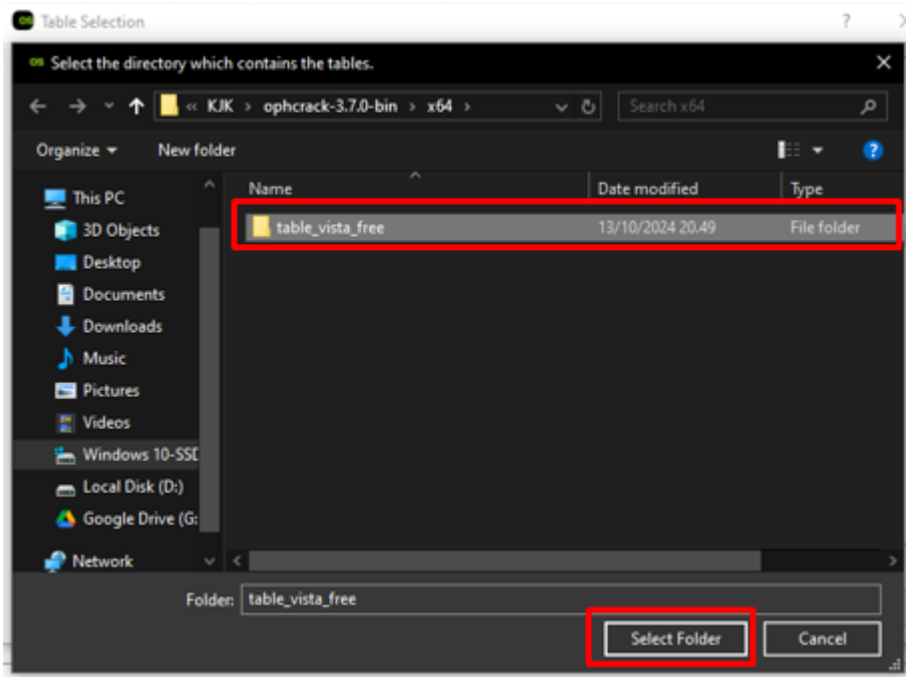
13. Hasil dimuat dalam opcrack, seperti gambar dibawah ini.

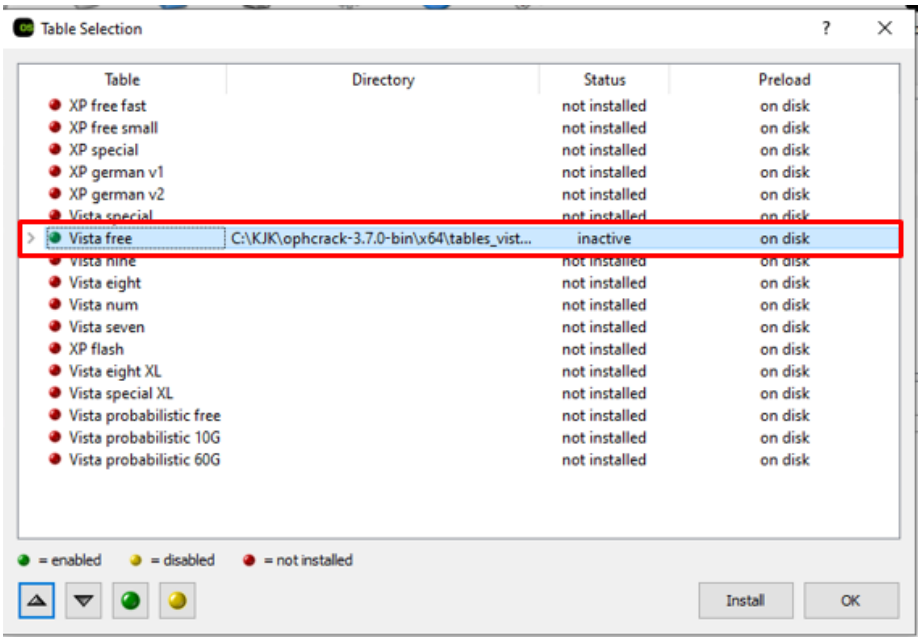


14. Klik “Tables” install “Vista free”

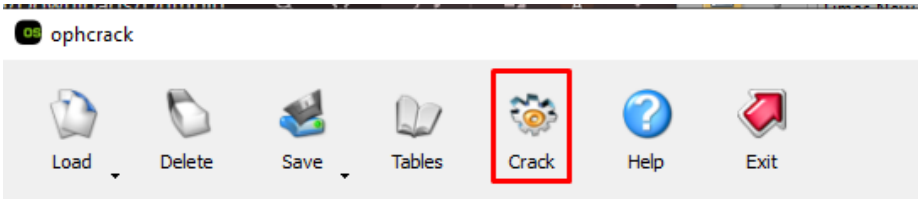


15. Kemudian pilih table vista free yang sudah di download sebelumnya. (table vista free bisa di download menggunakan link : https://ophcrack.sourceforge.io/tables.php)

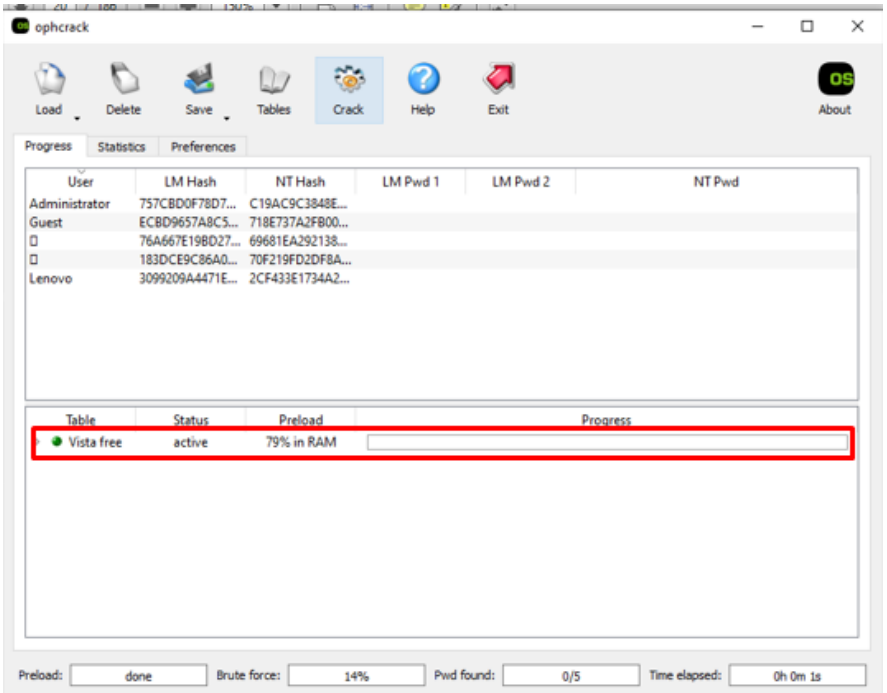




16. Setelah table tampil kemudian klik icon “Crack” untuk memecahkan kata sandi.



17. Ophcrack akan membutuhkan waktu beberapa menit untuk memecahkan kata sandi. Tunggu hingga proses selesai.



18. Setelah selesai maka password akan tampil, jika hasilnya menunjukkan not found maka kemungkinan besar karena Windows 10 terbaru secara default tidak lagi menyimpan password di hash LM karena kurang aman atau bisa juga karena beberapa akun (seperti "Guest" atau "DefaultAccount") mungkin tidak memiliki password atau sedang tidak aktif, sehingga ophcrack tidak menemukan apa-apa.