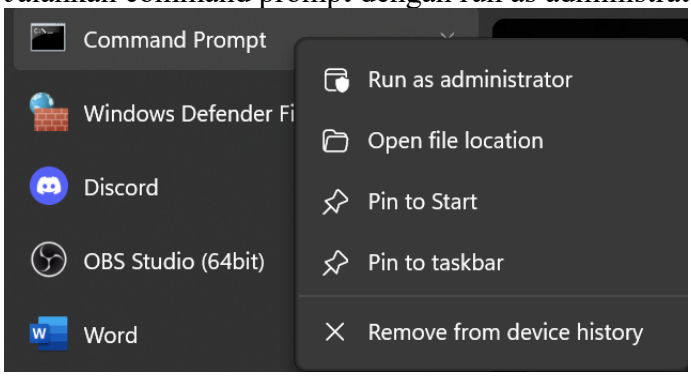
Nama : Muhammad Rafi Rizqullah
NIM : 09011282126091

Tugas Keamanan Jaringan Komputer

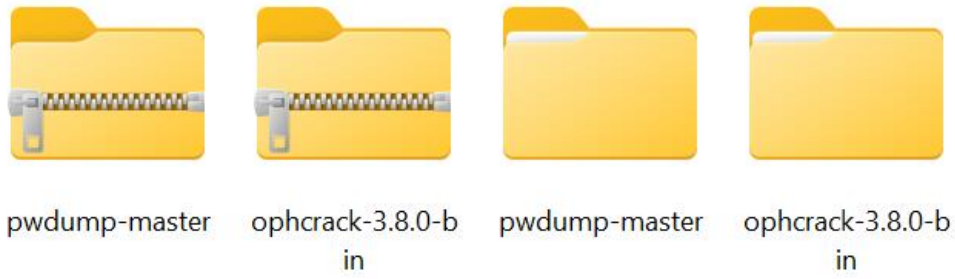
1. Jalankan command prompt dengan run as administrator.



2. Kemudian, agar dapat mengetahui userID dan username, ketik "wmic useraccount get name,sid" pada command prompt, dan akan menampilkan daftar akun yang ada pada sistem beserta SID nya seperti dibawah ini.

```
C:\Windows\System32>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-2656300957-33799841-3255957036-500
asus                S-1-5-21-2656300957-33799841-3255957036-1001
DefaultAccount      S-1-5-21-2656300957-33799841-3255957036-503
Guest               S-1-5-21-2656300957-33799841-3255957036-501
WDAGUtilityAccount  S-1-5-21-2656300957-33799841-3255957036-504
```

3. Download pwdump dan ophcrack, kemudian di ekstrak.



4. Kemudian, buka ke command prompt dan masuk ke folder pwdump yang telah di ekstrak sebelumnya dengan "cd (folder tempat anda meletakkan pwdump". Lalu, ketikkan "PwDump7.exe" agar dapat menampilkan userID, dan password hashes.

```
C:\Windows\System32>cd C:\Users\asus\Downloads\pwdump-master\pwdump-master
```

5. Selanjutnya, lakukan "PwDump7.exe > c:\hashes.txt" untuk memindahkan PwDump7.exe ke file hashes.txt

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

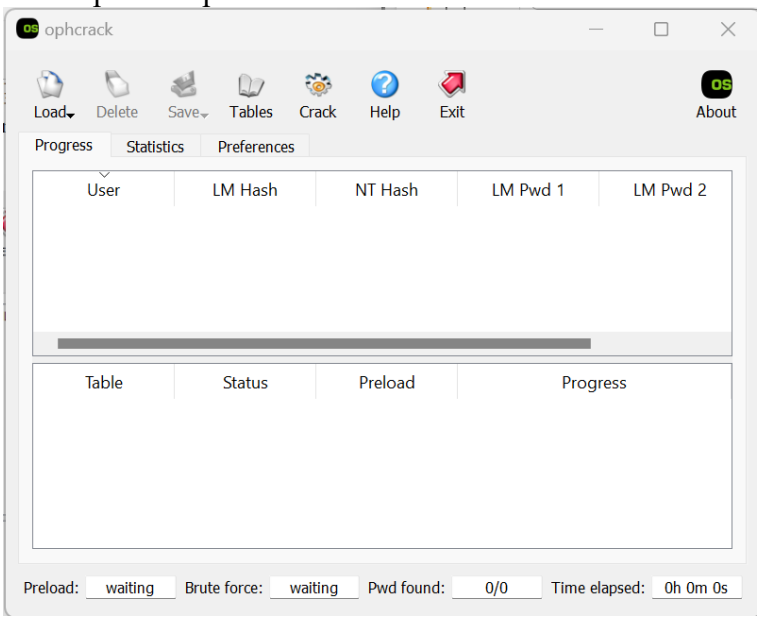
6. Setelah itu buka file hashes.txt yang telah dibuat tadi.

```
Administrator:500:95F584D4608C09D0984A1172E3BDE0A9:EBAD5E068E496D35D530231E9205A58F:::
Guest:501:0C8B00C55AF9B2F354EEA24E4FF89B51:EE27B288D297A79F6DE728EAF685C921:::
[illegible]:503:F39801E2A8F881DB10531302EC0BE8B9:AAE492542E63FACD2DC191D983D8EE60:::
[illegible]:504:1305C15391A757A74F8B84BD2CD895D3:B2FE9F67E7BA9D7E5A18447B7BFFA2DB:::
asus:1001:386EA13B2845191F13EF17E7C9E39ADC:12B244C1FDC7BA7EF9BF0D35D8A29230:::
```

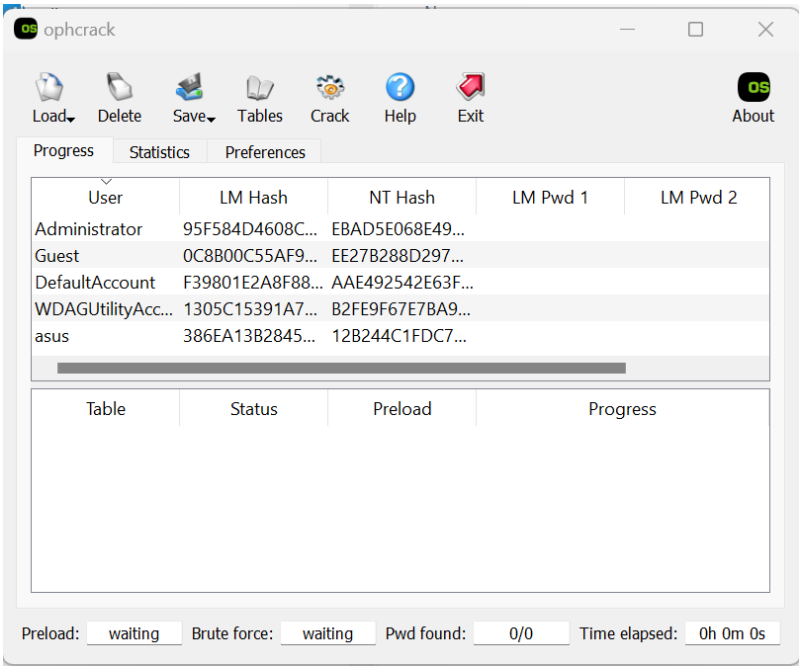
7. Isi username yang kosong tersebut sesuai dengan yang tertera di langkah kedua tadi.

```
Administrator:500:95F584D4608C09D0984A1172E3BDE0A9:EBAD5E068E496D35D530231E9205A58F:::
Guest:501:0C8B00C55AF9B2F354EEA24E4FF89B51:EE27B288D297A79F6DE728EAF685C921:::
DefaultAccount:503:F39801E2A8F881DB10531302EC0BE8B9:AAE492542E63FACD2DC191D983D8EE60:::
WDAGUtilityAccount:504:1305C15391A757A74F8B84BD2CD895D3:B2FE9F67E7BA9D7E5A18447B7BFFA2DB:::
asus:1001:386EA13B2845191F13EF17E7C9E39ADC:12B244C1FDC7BA7EF9BF0D35D8A29230:::
```

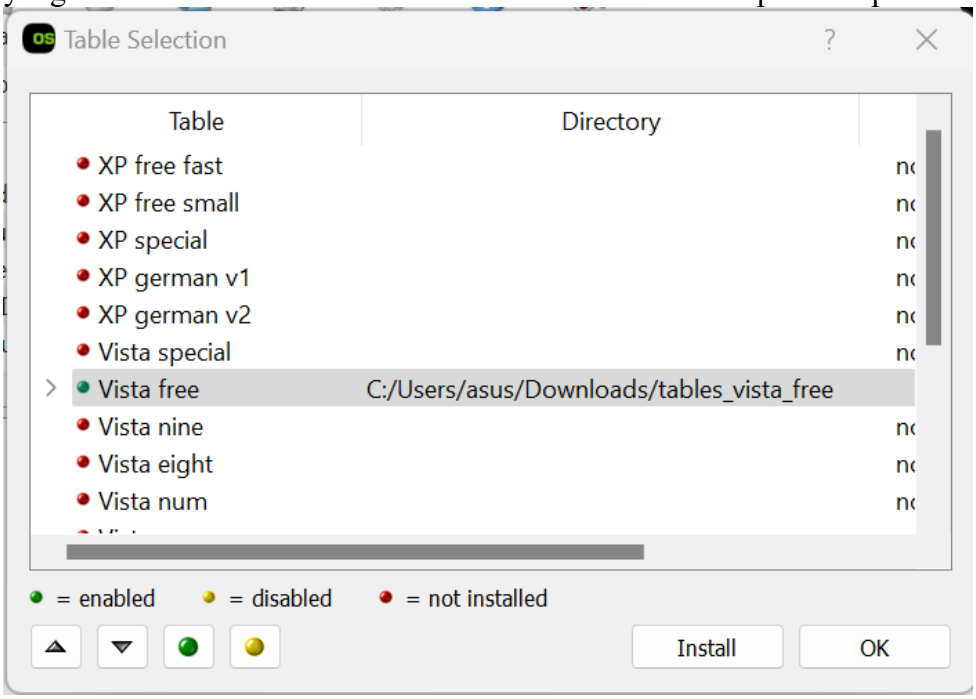
8. Buka aplikasi ophcrack.



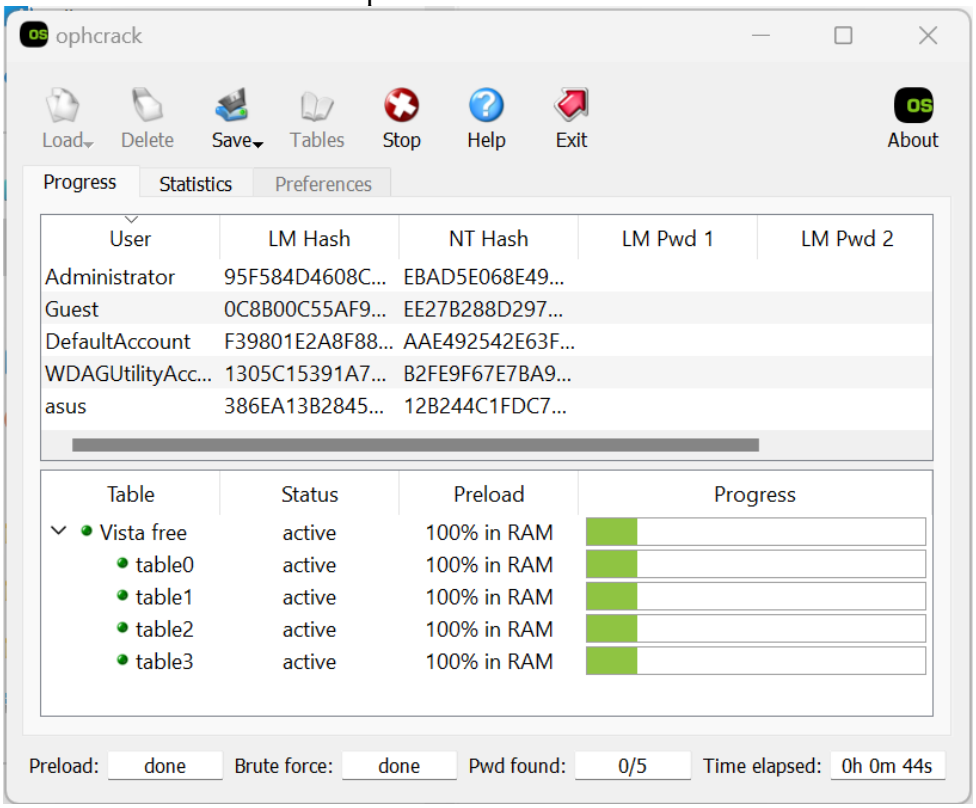
9. Kemudian klik menu Load > PWDUMP file > Pilih file hashes.txt yang telah dibuat.



10. Kemudian download vista free di browser anda > ekstrak file vista free > klik menu Tables di bagian atas > pilih bagian vista free > klik install > pilih folder vista free yang telah di ekstrak > klik select folder. Dan akan menampilkan seperti ini.



11. Setelah itu klik vista free dan klik ok. Kemudian akan tampil menu crack di bagian atas, kemudian klik menu crack tersebut agar dapat memecahkan kata sandi dengan membutuhkan waktu beberapa menit.



12. Jika sudah selesai maka password akan tampil. Untuk windows 10 terbaru, secara default tidak lagi menyimpan kata sandi di bash LM karena kurang aman dan beberapa akun seperti Guest dan DefaultAccount bisa jadi tidak memiliki kata sandi atau sedang tidak aktif, maka dari itu seluruh hasilnya adalah not found.