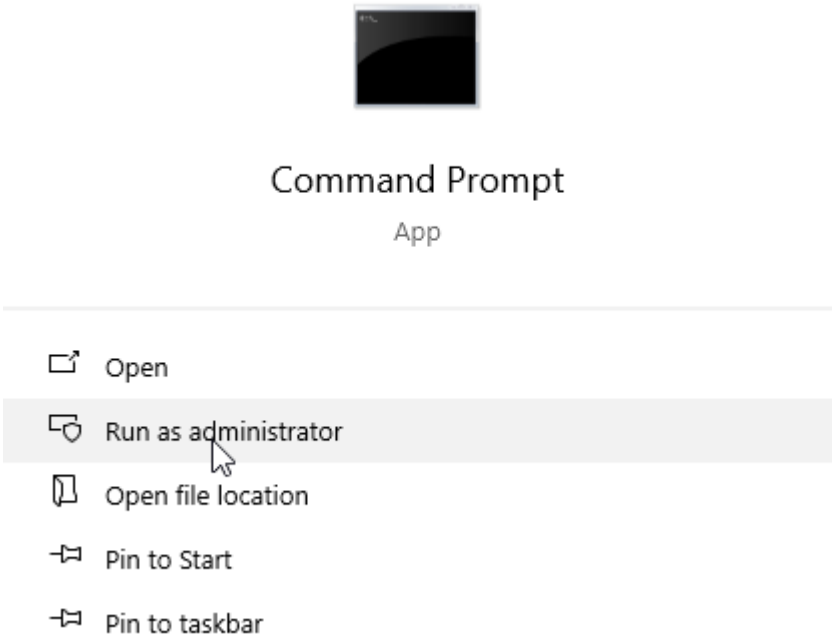
Nama: Aldi Hoirul Fatih
NIM: 09011282126069

KEAMANAN JARINGAN KOMPUTER

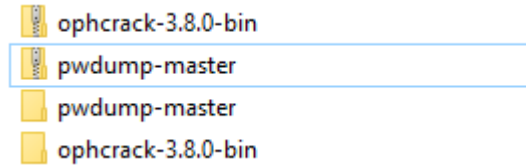
1. Cari command prompt dan jalankan dengan *run as administrator*.



2. Untuk kita mengetahui userID dengan username milik kita, dengan menggetikan “wmic useraccount get name,sid” maka akan menampilkan daftar akun yang ada di sistem kita beserta SID nya.

```
C:\Windows\system32>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-2267913805-2358182439-2120727182-500
aldih               S-1-5-21-2267913805-2358182439-2120727182-1001
DefaultAccount      S-1-5-21-2267913805-2358182439-2120727182-503
Guest               S-1-5-21-2267913805-2358182439-2120727182-501
WDAGUtilityAccount  S-1-5-21-2267913805-2358182439-2120727182-504
```

3. Disini kita akan mendownload dan mengekstrak file pwdump dan ophcrack .



4. Buka kembali cmd dan kita masuk ke dalam folder pwdump yang telah dibuat sebelumnya dengan cara “cd C:\folder\tempat\kita\meletakan\pwdump”. Setelah itu ketik “PwDump7.exe” untuk mendapatkan dan menampilkan password hashes dan userID.

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

5. Setelah itu kita memindahkan isi file dari PwDump7.exe ke dalam file hashes.tst dengan cara “PwDump7.exe > c:\hashes.txt”.

```
C:\Users\aldih\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. Isi file didalam hashes.txt

hashes - Notepad

File Edit Format View Help

```
Administrator:500:03FBEDA1FAA26B15ED2C730CD1F58CB9:E3230670A167A0A04663F6C309BA8CFB:::
Guest:501:978BED5DD767178B7850E6E364FE5EA5:9885F2491356F6EC9F95BFAA9424CF73:::
[illegible]:503:C5A4ECCF50F7887E2E0ADDBC43899A66:39C1E1673953A5CD69D7156713D66449:::
[illegible]:504:BC2ED68581DBFBBD71D8B6365CEE1696:7B9B7A9E98C8D7355A4145BF9DB7AE82:::
aldih:1001:12F1B1D0D9334D92546AE16411415158:A53A639312B8EEDBF3C75D4F834B553D:::
```

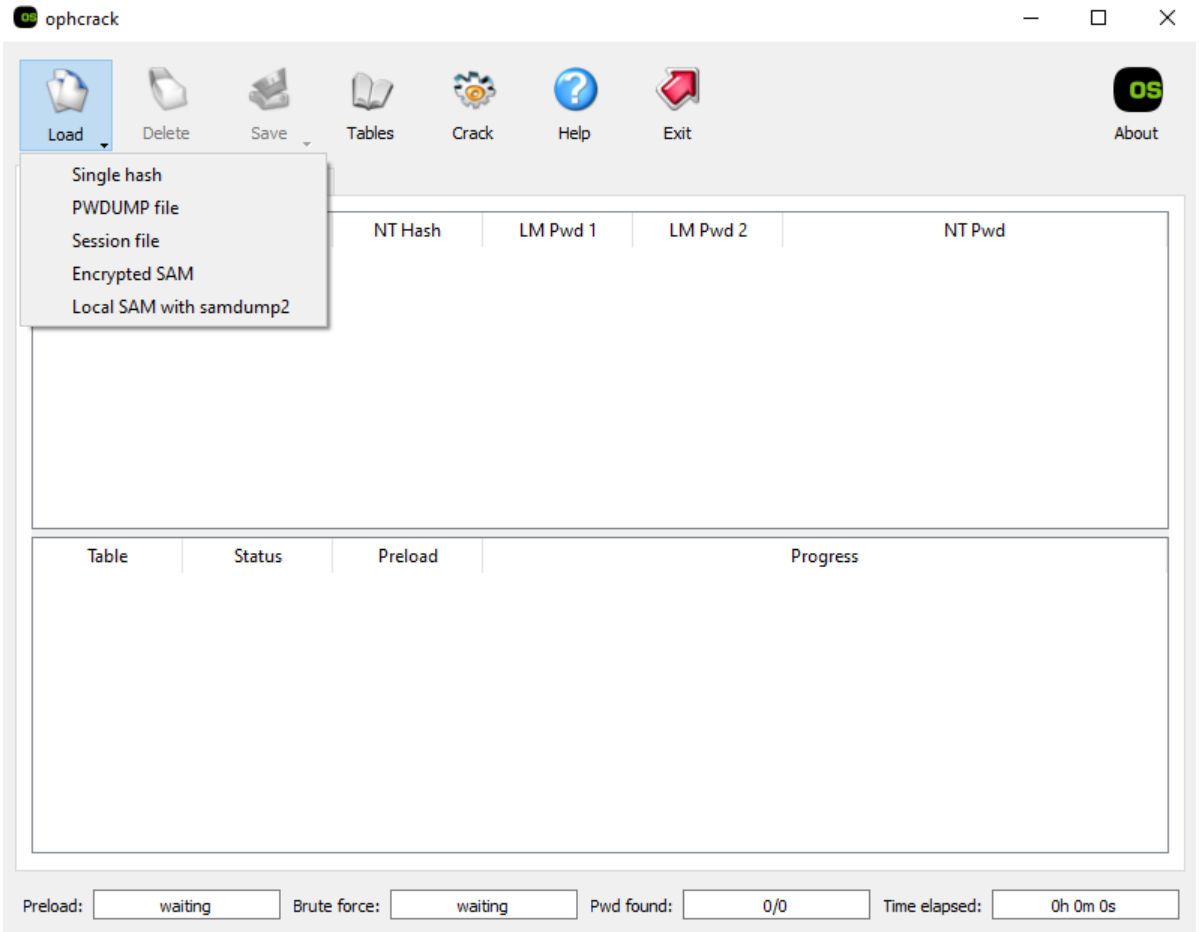
7. Setelah itu kita mengisi username yang kosong pada file tersebut dengan username yang telah kita lihat sebelumnya dengan cara “wmic useraccount get name,sid”.

hashes - Notepad

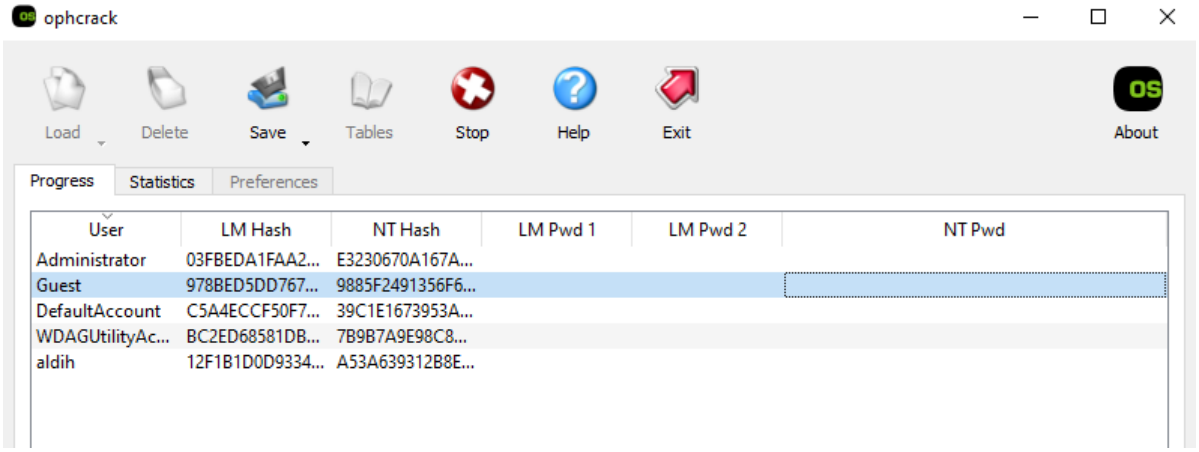
File Edit Format View Help

```
Administrator:500:03FBEDA1FAA26B15ED2C730CD1F58CB9:E3230670A167A0A04663F6C309BA8CFB:::
Guest:501:978BED5DD767178B7850E6E364FE5EA5:9885F2491356F6EC9F95BFAA9424CF73:::
DefaultAccount:503:C5A4ECCF50F7887E2E0ADDBC43899A66:39C1E1673953A5CD69D7156713D66449:::
WDAGUtilityAccount:504:BC2ED68581DBFBBD71D8B6365CEE1696:7B9B7A9E98C8D7355A4145BF9DB7AE82:::
aldih:1001:12F1B1D0D9334D92546AE16411415158:A53A639312B8EEDBF3C75D4F834B553D:::
```

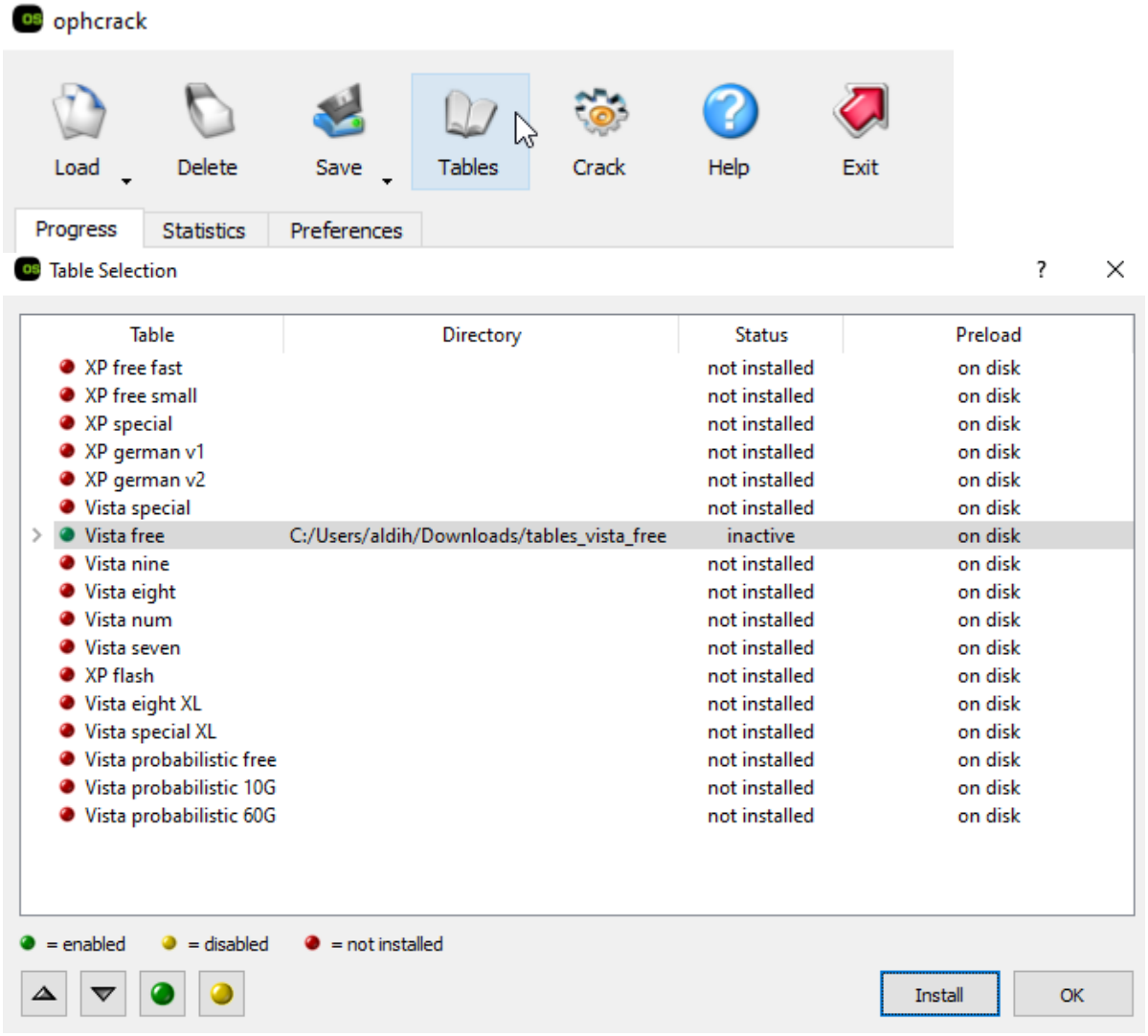
8. Membuka aplikasi ophcrack dan setelah itu memilih load -> PWDUMP file -> memilih file hashes.txt yang telah dibuat sebelumnya.



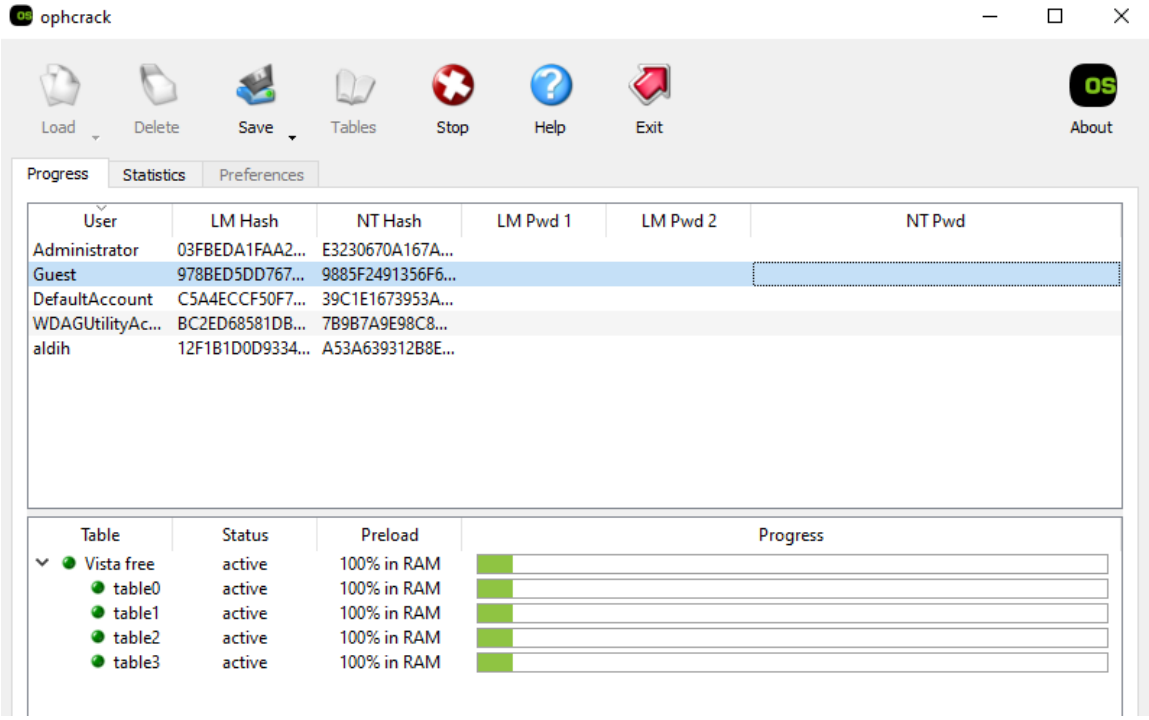
9. Maka akan tampil seperti dibawah ini setelah memilih file hashes.txt sbebelumnya.



10. Setelah itu klik tables dan pada halaman table tersebut pilih *vista free* kemudian download *vista free* tersebut di web ophcrack.



11. Setelah memilih table sebelumnya maka akan muncul icon crack disebelah tables, kemudian ketika kita memilih icon tersebut maka akan langsung memecahkan kata sandi. Butuh waktu beberapa menit untuk ophcrack memecahkan kata sandi.



12. 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.