

Nama : Makiyah
NIM : 09011282126093
Mata Kuliah : Keamanan Jaringan Komputer

Dumping and Cracking SAM Hashes to Extract Plain Password

1. Jalankan *Run as administrator* pada *command prompt* di windows



Command Prompt

App

- Open
- Run as administrator
- Open file location
- Pin to Start
- Pin to taskbar

2. Perintah “wmic useraccount get name,sid” digunakan untuk melihat dan menampilkan UserID dengan username serta menampilkan SID.

```
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
defaultuser100000 S-1-5-21-2267913805-2358182439-2120727182-1005
Guest S-1-5-21-2267913805-2358182439-2120727182-501
kiyah S-1-5-21-2267913805-2358182439-2120727182-1002
WDAGUtilityAccount S-1-5-21-2267913805-2358182439-2120727182-504
```

3. File pwdump dan ophcrack yang di download kemudian di ekstraksi

Name	Date modified	Type
Today (2)		
ophcrack-3.8.0-bin	10/13/2024 8:21 PM	File folder
pwdump-master	10/13/2024 8:21 PM	File folder

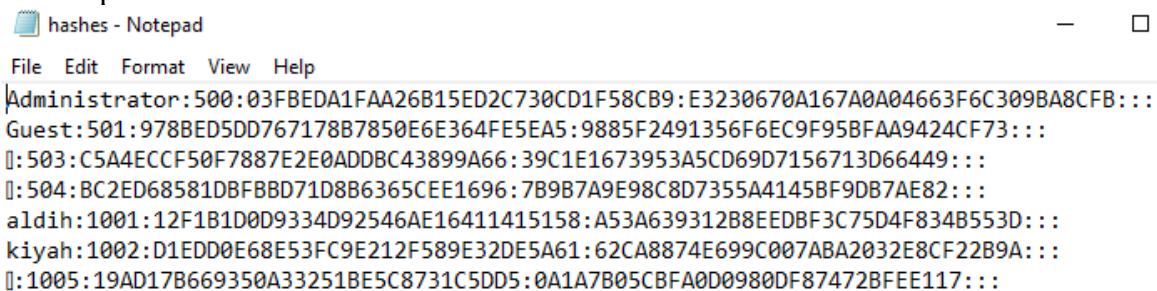
4. Perintah “cd C:\folder\tempat\kita\meletakan\pwdump” untuk masuk ke folder yang telah di buat lalu masukkan Kembali perintah “PwDump7.exe” untuk menampilkan UserID dan password Hashes.

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

5. Perintah “PwDump7.exe > c:\hashes.txt” digunakan untuk memindahkan isi file.

```
C:\Users\kiyah\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. Menampilkan isi file hashes.txt

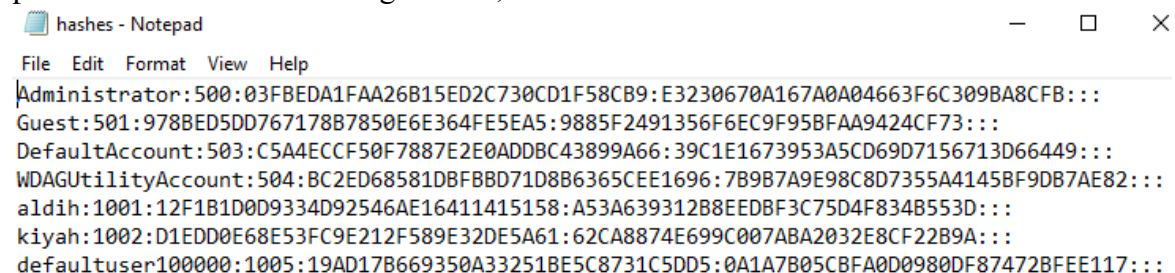


hashes - Notepad

File Edit Format View Help

```
Administrator:500:03FBEDA1FAA26B15ED2C730CD1F58CB9:E3230670A167A0A04663F6C309BA8CFB:::  
Guest:501:978BED5DD767178B7850E6E364FE5EA5:9885F2491356F6EC9F95BFAA9424CF73:::  
[]:503:C5A4ECCF50F7887E2E0ADDBC43899A66:39C1E1673953A5CD69D7156713D66449:::  
[]:504:BC2ED68581DBFBBD71D8B6365CEE1696:7B9B7A9E98C8D7355A4145BF9DB7AE82:::  
aldih:1001:12F1B1D0D9334D92546AE16411415158:A53A639312B8EEDBF3C75D4F834B553D:::  
kiyah:1002:D1EDD0E68E53FC9E212F589E32DE5A61:62CA8874E699C007ABA2032E8CF22B9A:::  
[]:1005:19AD17B669350A33251BE5C8731C5DD5:0A1A7B05CBFA0D0980DF87472BFEE117:::
```

7. Username yang kosong di isi dengan username sebelumnya dengan menggunakan perintah “wmic useraccount get name,sid”

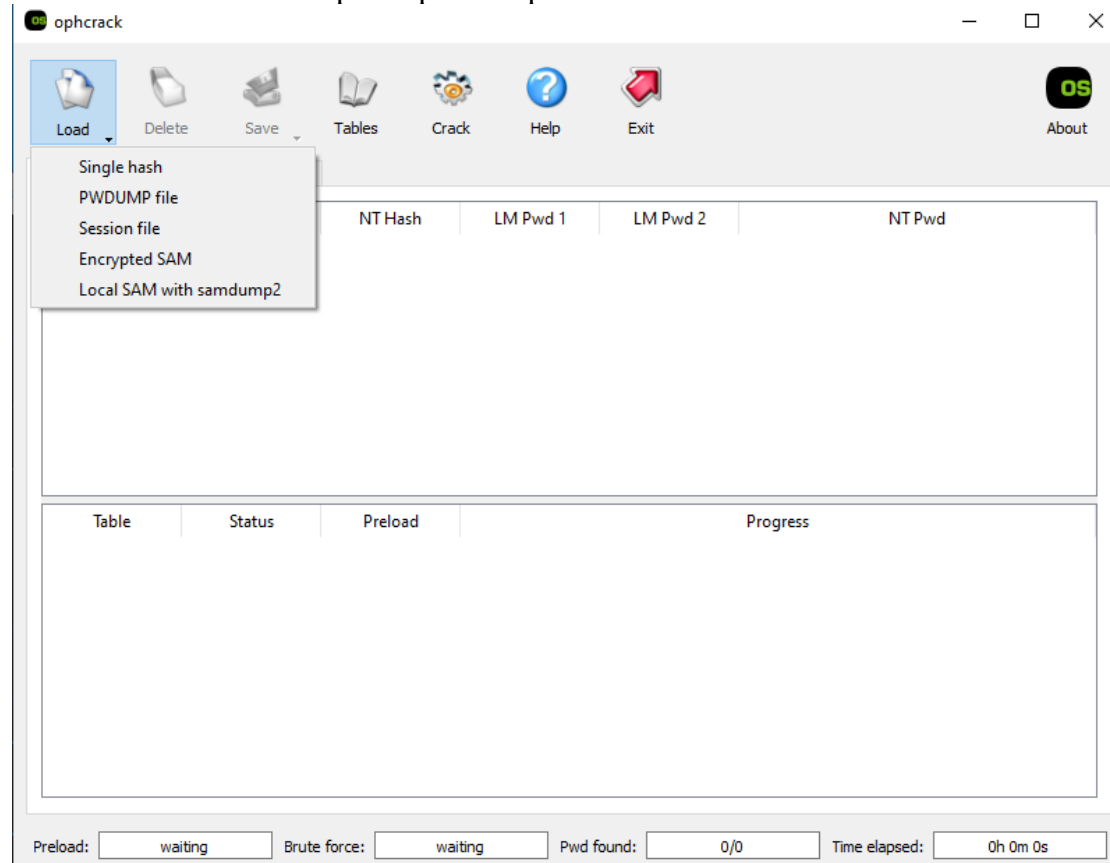


hashes - Notepad

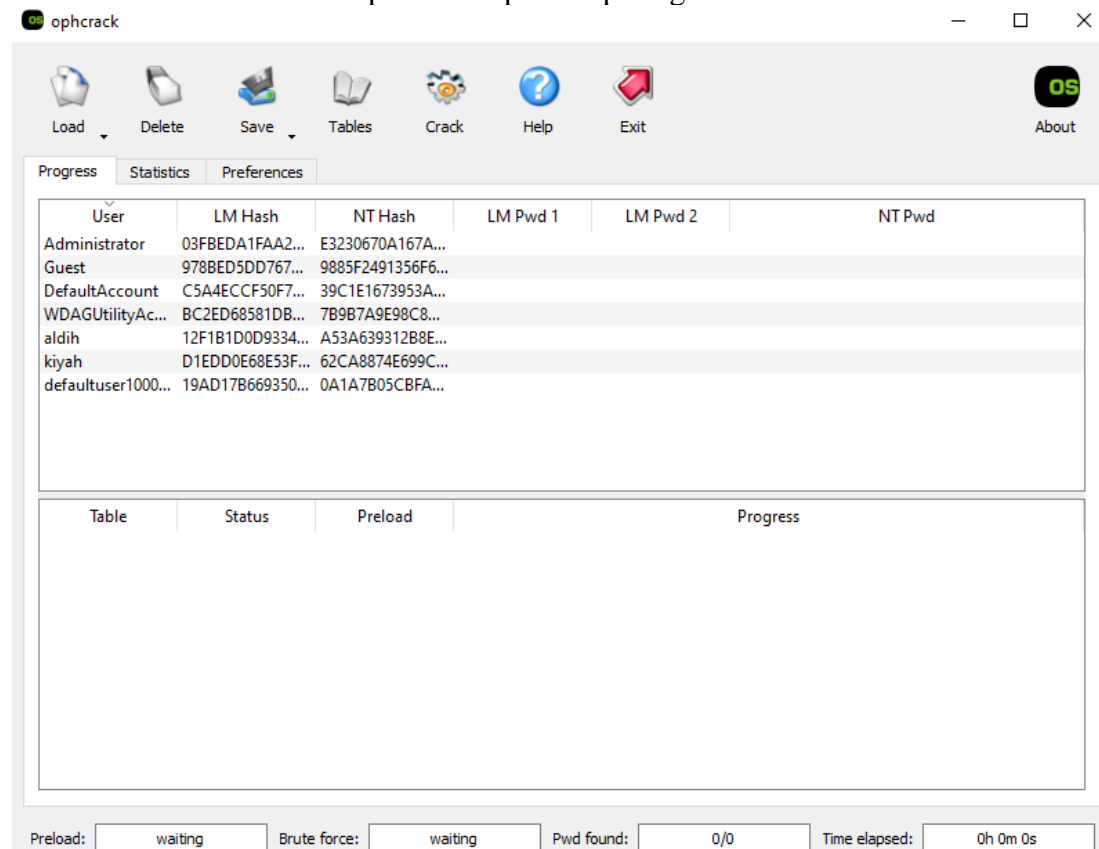
File Edit Format View Help

```
Administrator:500:03FBEDA1FAA26B15ED2C730CD1F58CB9:E3230670A167A0A04663F6C309BA8CFB:::  
Guest:501:978BED5DD767178B7850E6E364FE5EA5:9885F2491356F6EC9F95BFAA9424CF73:::  
DefaultAccount:503:C5A4ECCF50F7887E2E0ADDBC43899A66:39C1E1673953A5CD69D7156713D66449:::  
WDAGUtilityAccount:504:BC2ED68581DBFBBD71D8B6365CEE1696:7B9B7A9E98C8D7355A4145BF9DB7AE82:::  
aldih:1001:12F1B1D0D9334D92546AE16411415158:A53A639312B8EEDBF3C75D4F834B553D:::  
kiyah:1002:D1EDD0E68E53FC9E212F589E32DE5A61:62CA8874E699C007ABA2032E8CF22B9A:::  
defaultuser100000:1005:19AD17B669350A33251BE5C8731C5DD5:0A1A7B05CBFA0D0980DF87472BFEE117:::
```

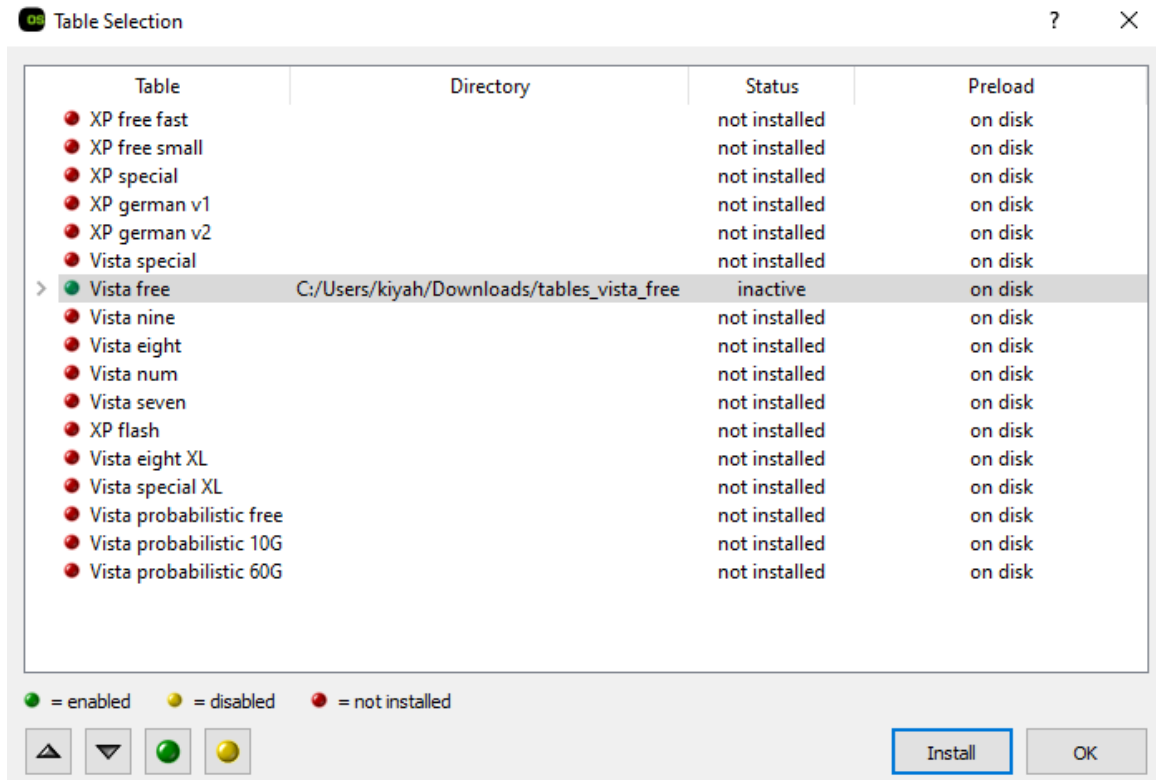
8. Membuka file hashes.txt pada aplikasi ophcrack



9. File hashes.txt akan menampilkan tampilan seperti gambar dibawah ini.



10. Install *vista free* pada aplikasi ophcrack



11. Jika icon crack dipilih akan langsung memecahkan kata sandi. Butuh waktu beberapa menit untuk ophcrack memecahkan kata sandi. Jika proses selesai kata sandi akan ditampilkan jika tidak artinya windows 10 terbaru secara default tidak lagi menyimpan password di hash LM karena kurang aman atau bisa juga karena beberapa mungkin tidak memiliki password atau sedang tidak aktif, sehingga ophcrack akan menampilkan pesan “not found”.

