Nama: Dhani Medianto Saputra

Nim : 09011282126067

Keamanan Jaringan Komputer

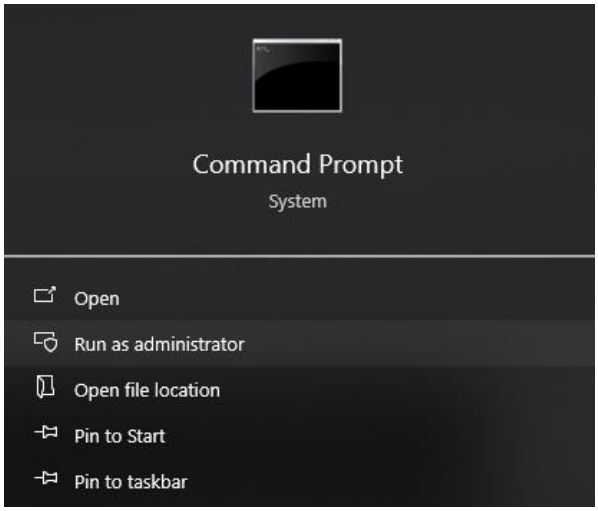
Dumping And Cracking SAM Hashes to Extract PlainText Password

Security Account Manager (SAM) adalah basis data di sistem operasi Windows yang menyimpan informasi akun pengguna dan deskriptor keamanannya. File ini menyimpan kata sandi pengguna dalam bentuk hash (LM dan NTLM). Karena proses hashing bersifat satu arah, ini memberikan tingkat keamanan dalam penyimpanan kata sandi.Dalam konteks peretasan, penyerang biasanya akan mengekstrak hash kata sandi setelah berhasil mengakses komputer target. Hash ini memungkinkan mereka untuk melakukan berbagai serangan, seperti peretasan kata sandi, menggunakan hash untuk mengakses sistem lain, menganalisis kata sandi, dan mengidentifikasi pola untuk memecahkan kata sandi lain dalam lingkungan yang sama.Untuk dapat mengekstrak isi file SAM, diperlukan hak akses administrator. Menilai kekuatan kata sandi adalah langkah penting dalam penilaian keamanan. Proses ini dimulai dengan mengekstrak hash SAM dan kemudian menggunakan metode dekripsi untuk mendapatkan kata sandi dalam bentuk teks biasa.

Tujuan dari dumping dan cracking ini adalah untuk membantu mempelajari cara:

- Mengetahui cara mengunakan alat pwdump7 untuk mengekstrak hash kata sandi
- Mengetahui cara mengunakan alat Ophcrack untuk memecahkan kata sandi dan mendapatkan teks biasa

1. Pertama, kita mencari tahu User ID dengan username menggunakan cmd administrator mode.



2. Kemudian ketik code wmic useraccount get name,sid yang memiliki fungsi menampilkan daftar semua akun pengguna yang ada di sistem beserta SID-nya masing-masing.

```
C:\Windows\system32>wmic useraccount get name,sid
Name               SID
Administrator      S-1-5-21-3056085304-78094005-505501463-500
danim              S-1-5-21-3056085304-78094005-505501463-1001
DefaultAccount     S-1-5-21-3056085304-78094005-505501463-503
defaultuser100001  S-1-5-21-3056085304-78094005-505501463-1003
Guest              S-1-5-21-3056085304-78094005-505501463-501
WDAGUtilityAccount S-1-5-21-3056085304-78094005-505501463-504
```

3. Kemudian mendownload dan mengekstrak file pwdump dan ophcrack

4. 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 hashes dan userID.

```
C:\Windows\system32>cd C:\Users\danim\Desktop

C:\Users\danim\Desktop>cd pwdump-master
```

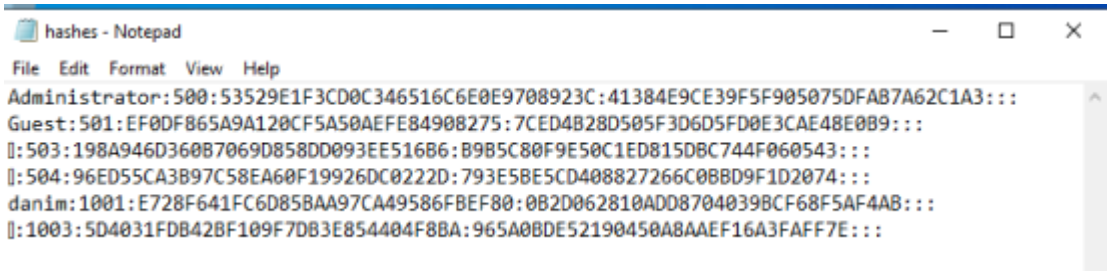
```
C:\Users\danim\Desktop\pwdump-master>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:53529E1F3CD0C346516C6E0E9708923C:41384E9CE39F5F905075DFAB7A62C1A3:::
Guest:501:EF0DF865A9A120CF5A50AEFE84908275:7CED4B28D505F3D6D5FD0E3CAE48E0B9:::
¶:503:198A946D360B7069D858DD093EE516B6:B9B5C80F9E50C1ED815DBC744F060543:::
¶:504:96ED55CA3B97C58EA60F19926DC0222D:793E5BE5CD408827266C0BBD9F1D2074:::
danim:1001:E728F641FC6D85BAA97CA49586FBEF80:0B2D062810ADD8704039BCF68F5AF4AB:::
¶:1003:5D4031FDB42BF109F7DB3E854404F8BA:965A0BDE52190450A8AAEF16A3FAFF7E:::
```

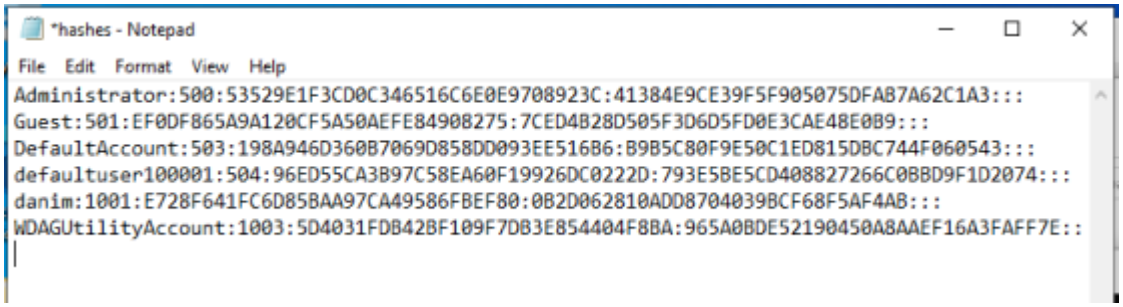
5. Kemudian untuk memindahkan dan men-copy semua data hasil dari PwDump7.exe ke hashes.txt menggunakan command PwDump7.exe > c:\hashes.txt

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

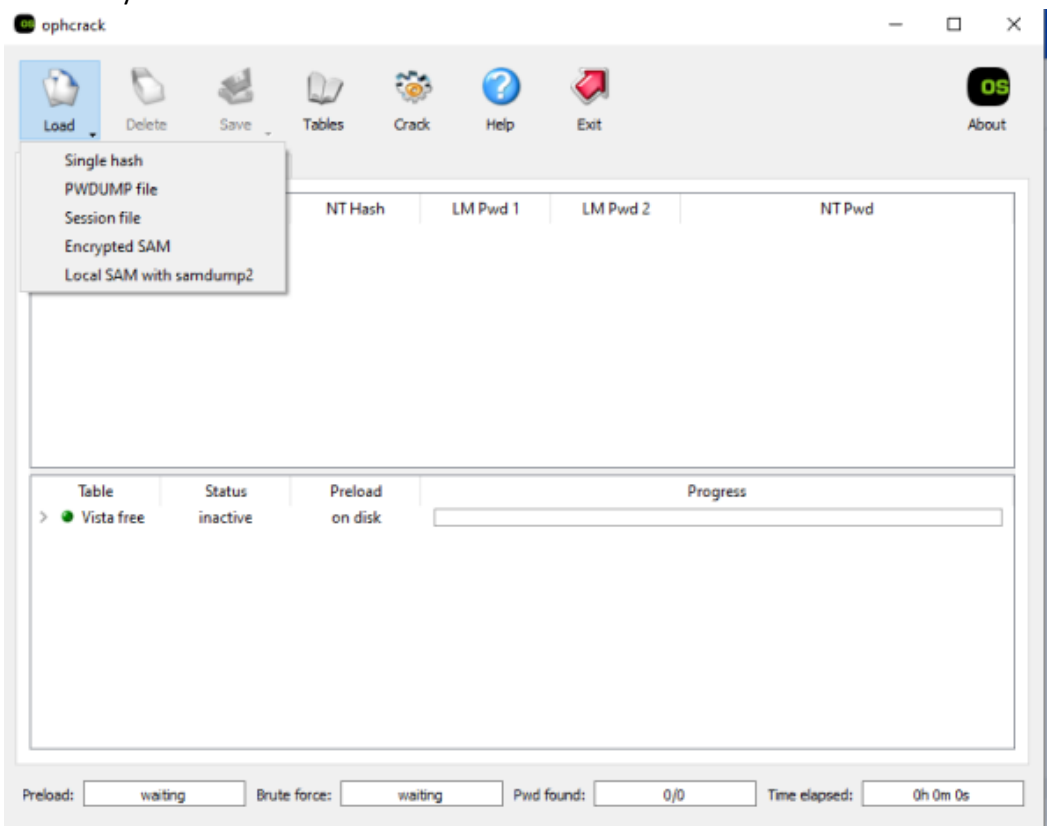
6. Berikut ini adalah isi file dari hashes.txt.



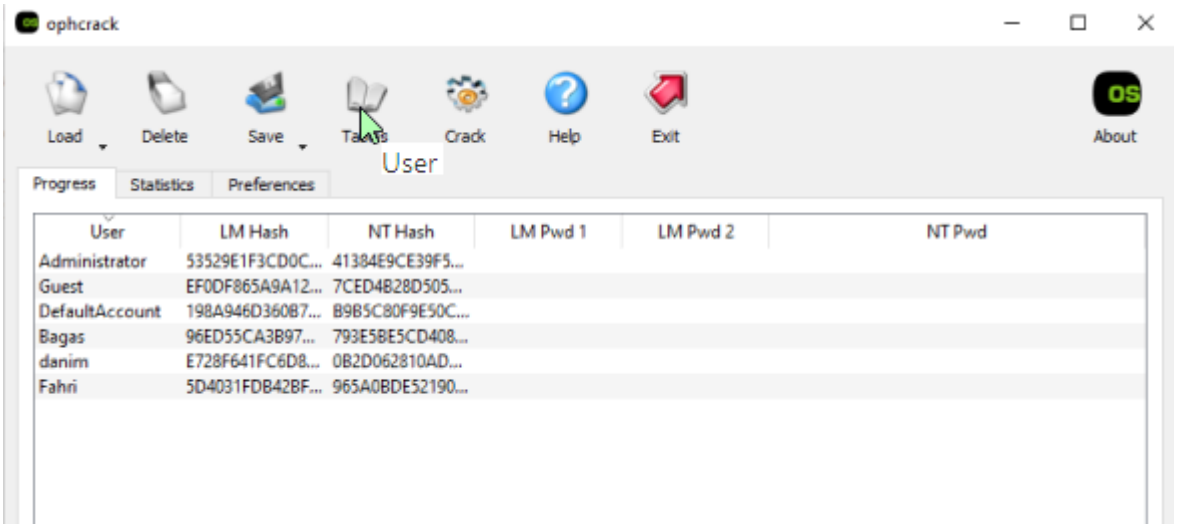
7. Selanjutnya mengisi semua username yang kosong sesuai dengan username pengguna pada step 2 kemudian save file hashes.txt



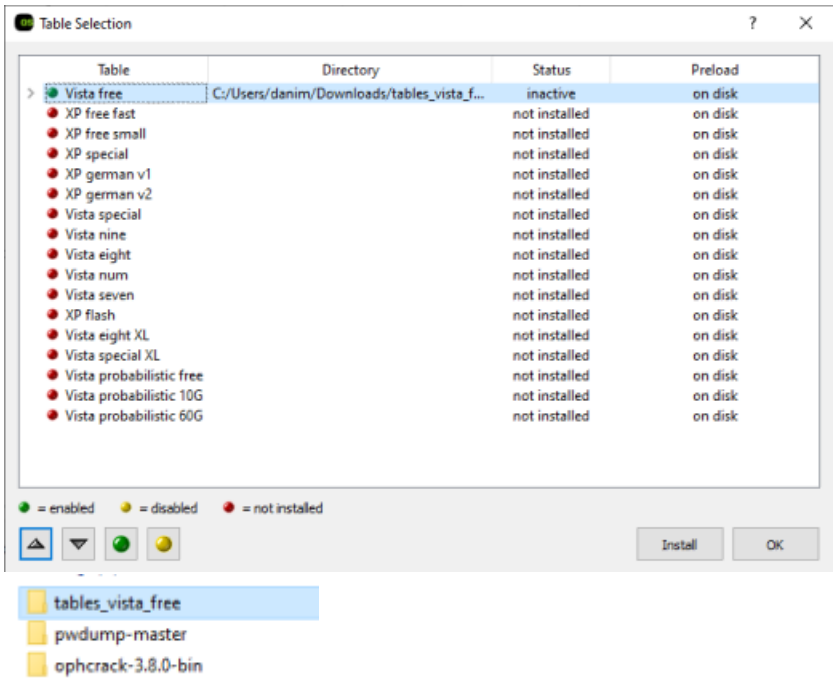
8. Selanjutnya buka oph crack kemudian pilih load PWDUMP file dan pilih file hashes.txt sebelumnya.



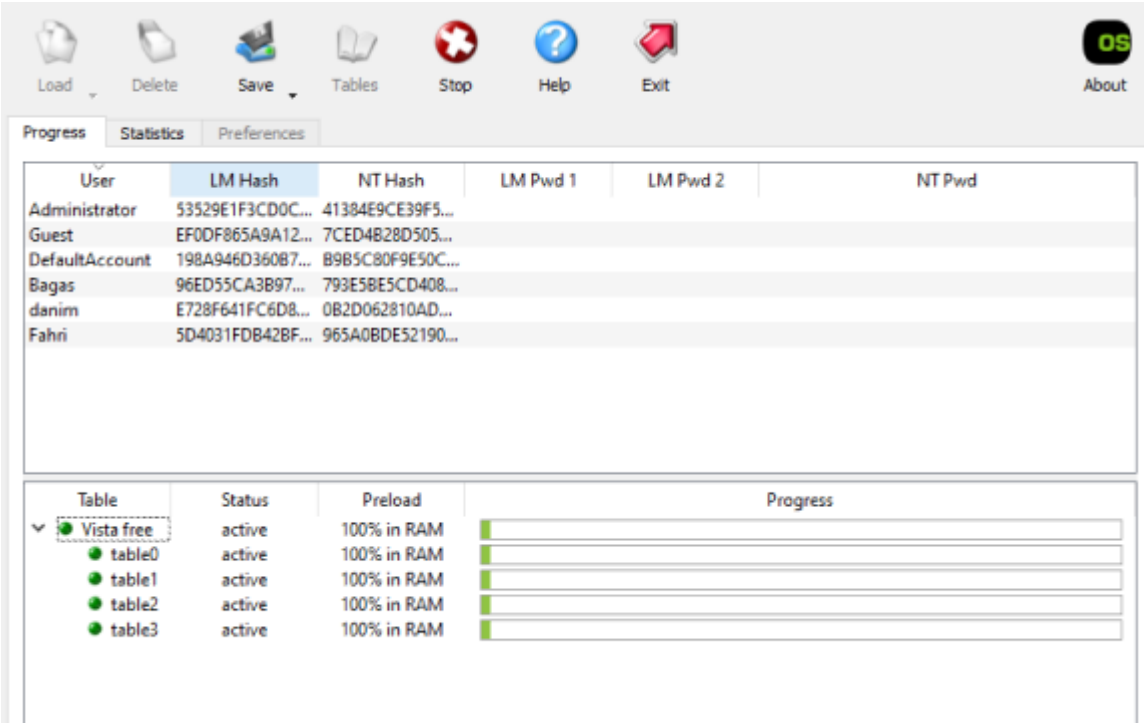
9. File Hashes tersebut akan tampil dengan lm hash dan nt hash sesuai username user.



10. Kemudia klik table dan pada table selection pilih vista free kemudian klik install, kemudian pilih table vista free yang sudah di download sebelumnya . (table vista free bisa di download menggunakan link : https://ophcrack.sourceforge.io/tables.php)



11. Setelah table tambil kemudian klik icon crack disamping icon untuk mulai memecahkan kata sandi. Ophcrack akan membutuhkan waktu beberapa menit untuk memecahkan kata sandi. Tunggu hingga proses pemecahan kata sandi selesai.



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.