

Nama : Febiyona Melista Tarigan

NIM : 09011282126087

MK : Keamanan Jaringan Komputer

“Dumping And Cracking SAM Hashes to Extract Plain Text Password “

Security Account Manager (SAM) adalah database dalam sistem operasi Windows yang digunakan untuk menyimpan informasi akun pengguna serta deskriptor keamanan terkait. File SAM menyimpan kata sandi pengguna dalam bentuk hash, menggunakan algoritma seperti LM (Lan Manager) dan NTLM (NT LAN Manager). Meskipun proses hashing bersifat satu arah, yang berarti hash tidak bisa langsung dikonversi kembali menjadi kata sandi asli, hash tetap memberikan lapisan keamanan karena kata sandi tidak disimpan secara langsung.

Namun, dalam konteks keamanan dan peretasan, penyerang yang berhasil mendapatkan akses ke sistem dengan hak administrator dapat mengekstrak hash kata sandi dari file SAM. Setelah hash ini diekstraksi, penyerang dapat melakukan berbagai jenis serangan, seperti serangan brute force untuk memecahkan kata sandi, serangan pass-the-hash untuk mengakses sistem lain tanpa memerlukan kata sandi asli, atau menganalisis pola kata sandi dalam organisasi yang sama.

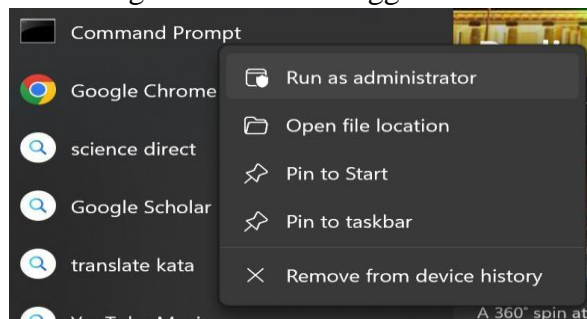
Untuk melakukan ekstraksi file SAM, diperlukan hak akses level administrator. Setelah hash didapatkan, langkah selanjutnya adalah menggunakan teknik cracking atau dekripsi untuk mendapatkan kata sandi dalam bentuk teks asli (plaintext). Salah satu alat yang umum digunakan untuk mengekstrak hash SAM adalah pwdump7, sementara alat seperti Ophcrack digunakan untuk memecahkan hash tersebut dan mengubahnya kembali menjadi teks biasa.

Tujuan dari proses dumping dan cracking hash ini antara lain:

- Mempelajari cara menggunakan alat pwdump7 untuk mengekstrak hash kata sandi dari file SAM.
- Mempelajari cara menggunakan Ophcrack untuk memecahkan hash kata sandi dan mengubahnya menjadi teks biasa.

Adapun Langkah-langkah yang harus dilakukan sebagai berikut :

1. Mencari tahu User ID dengan username menggunakan cmd administrator mode



- Setelah itu, 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-1-5-21-1272325986-2949973955-3825535459-500
DefaultAccount       S-1-5-21-1272325986-2949973955-3825535459-503
Guest                S-1-5-21-1272325986-2949973955-3825535459-501
USER                  S-1-5-21-1272325986-2949973955-3825535459-1001
WDAGUtilityAccount   S-1-5-21-1272325986-2949973955-3825535459-504
```

- Kemudian mendownload dan mengekstrak file `pwdump` dan `ophcrack`



- 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\USER\Downloads\pwdump-master\pwdump-master

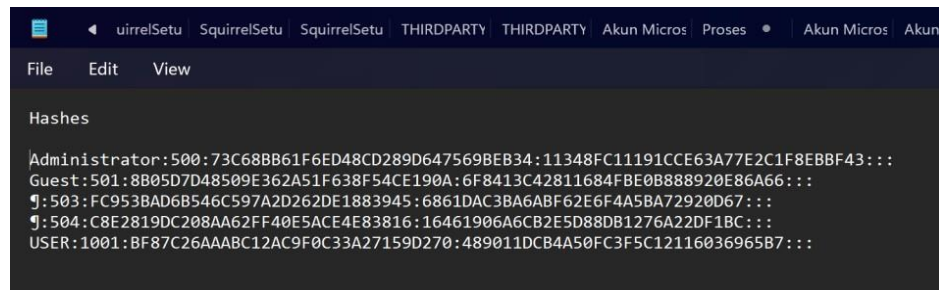
C:\Users\USER\Downloads\pwdump-master\pwdump-master>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:73C68BB61F6ED48CD289D647569BEB34:11348FC11191CCE63A77E2C1F8EBBF43:::
Guest:501:8B05D7D48509E362A51F638F54CE190A:6F8413C42811684FBE0B888920E86A66:::
j:503:FC953BAD6B546C597A2D262DE1883945:6861DAC3BA6ABF62E6F4A5BA72920D67:::
j:504:C8E2819DC208AA62FF40E5ACE4E83816:16461906A6CB2E5D88DB1276A22DF1BC:::
USER:1001:BF87C26AAABC12AC9F0C33A27159D270:489011DCB4A50FC3F5C12116036965B7:::
```

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

```
C:\Users\USER\Downloads\pwdump-master\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.

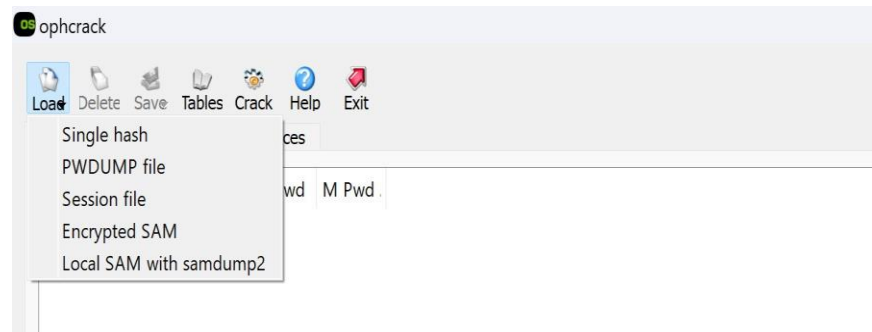


```
Administrator:500:73C68BB61F6ED48CD289D647569BEB34:11348FC11191CCE63A77E2C1F8EBBF43:::  
Guest:501:8B05D7D48509E362A51F638F54CE190A:6F8413C42811684FBE0B888920E86A66:::  
j:503:FC953BAD6B546C597A2D262DE1883945:6861DAC3BA6ABF62E6F4A5BA72920D67:::  
j:504:C8E2819DC208AA62FF40E5ACE4E83816:16461906A6CB2E5D88DB1276A22DF1BC:::  
USER:1001:BF87C26AAABC12AC9F0C33A27159D270:489011DCB4A50FC3F5C1211603696587:::
```

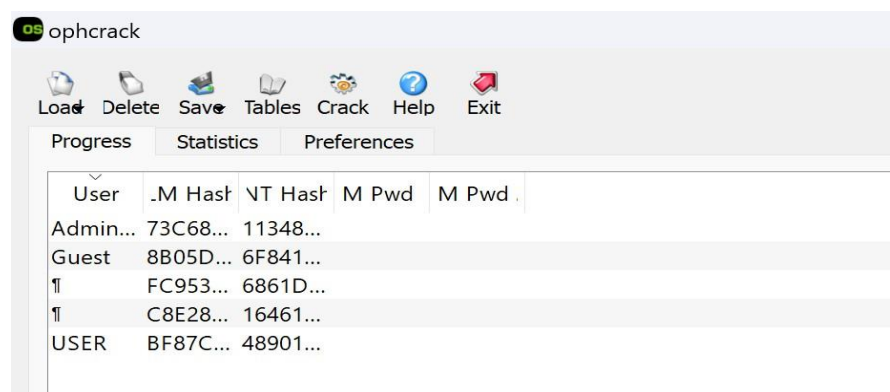
7. Selanjutnya mengisi semua username yang kosong sesuai dengan username pengguna pada step 2 kemudian save file hashes.txt

```
Administrator:500:73C68BB61F6ED48CD289D647569BEB34:11348FC11191CCE63A77E2C1F8EBBF43:::  
Guest:501:8B05D7D48509E362A51F638F54CE190A:6F8413C42811684FBE0B888920E86A66:::  
j:503:FC953BAD6B546C597A2D262DE1883945:6861DAC3BA6ABF62E6F4A5BA72920D67:::  
j:504:C8E2819DC208AA62FF40E5ACE4E83816:16461906A6CB2E5D88DB1276A22DF1BC:::  
USER:1001:BF87C26AAABC12AC9F0C33A27159D270:489011DCB4A50FC3F5C1211603696587:::
```

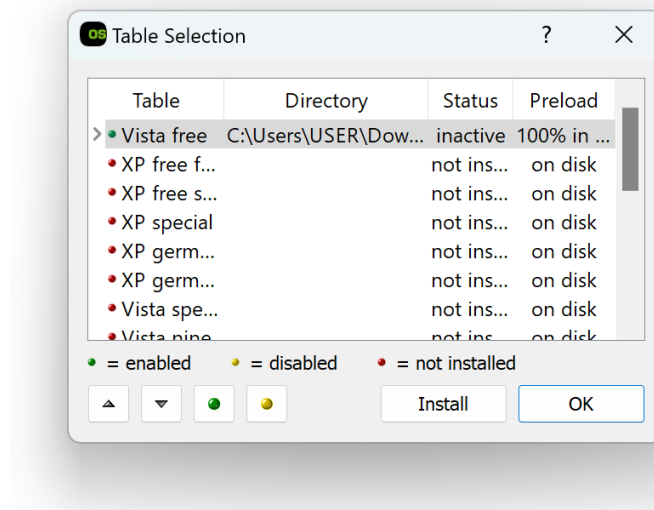
8. Setelah itu, buka oph crack kemudian pilih load PWDUMP file dan pilih file hashes.txt sebelumnya.



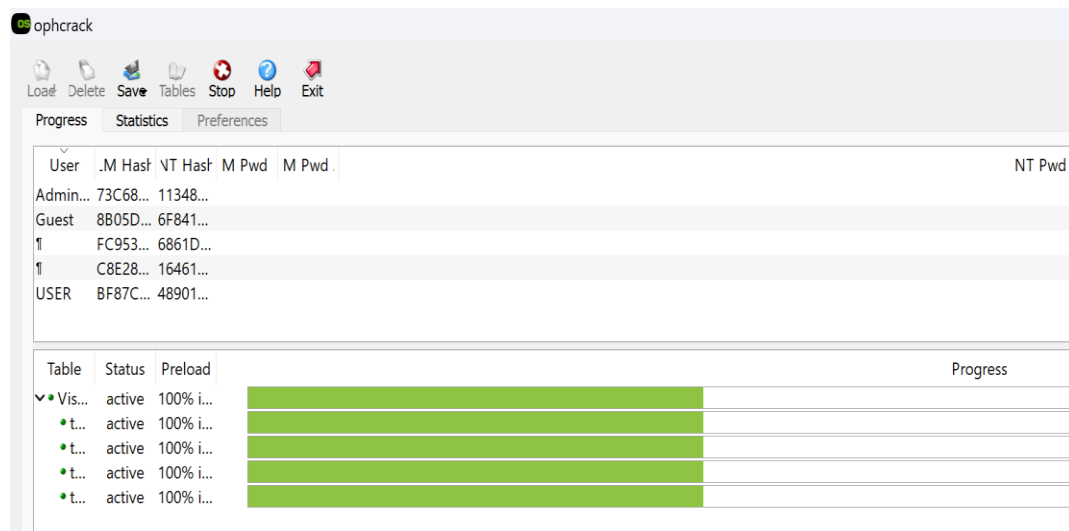
9. File Hashes tersebut akan tampil denan Im hash sesuai username user.



10. Kemudian 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](https://ophcrack.sourceforge.io/tables.php))



11. Setelah table tampil 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.

