

Nama : Armanda Fathurrahman

NIM : 09011282126055

Kelas : SK7A Indralaya

Dumping and Cracking SAM Hashes to Extract Plain Text Password

Security Account Manager (SAM) adalah komponen penting dalam sistem operasi Windows yang berfungsi sebagai database untuk menyimpan informasi keamanan terkait akun pengguna, termasuk kata sandi dan hak akses. SAM menyimpan hash dari kata sandi pengguna, bukan kata sandi sebenarnya, untuk memastikan keamanan data autentikasi. Ketika pengguna mencoba login ke sistem, Windows akan membandingkan hash kata sandi yang dimasukkan dengan hash yang tersimpan di SAM untuk memastikan identitas pengguna. File SAM, yang biasanya terletak di direktori `C:\Windows\System32\Config\SAM`, dilindungi ketat oleh sistem dan tidak bisa diakses atau dimodifikasi secara langsung saat sistem sedang berjalan, karena Windows menguncinya untuk melindungi integritas dan keamanan data pengguna. SAM memainkan peran vital dalam memastikan bahwa hanya pengguna yang berwenang yang bisa mengakses sumber daya di dalam sistem, dan karena sifat pentingnya, file SAM sering menjadi target serangan bagi peretas yang berusaha mendapatkan akses tidak sah ke akun pengguna. Untuk mencegah akses yang tidak sah, Windows menggunakan beberapa lapisan perlindungan, termasuk enkripsi dan pembatasan akses pada file SAM, sehingga peretas tidak bisa dengan mudah memanipulasi atau mencurinya.

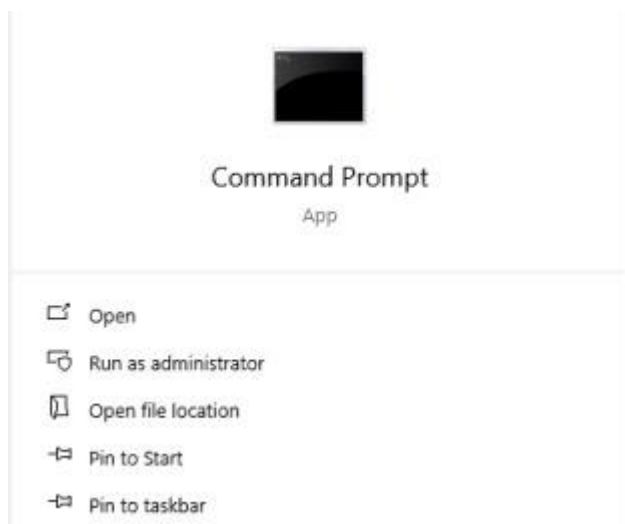
Dumping dan cracking SAM adalah metode yang sering digunakan oleh penyerang untuk mendapatkan akses tidak sah ke akun pengguna pada sistem Windows. Dumping merujuk pada proses mengekstrak data dari file SAM yang berisi hash kata sandi, yang kemudian digunakan untuk melakukan cracking. Karena file SAM dilindungi oleh sistem saat sedang berjalan, penyerang sering menggunakan alat atau teknik khusus, seperti menjalankan sistem dalam mode offline atau menggunakan perangkat lunak seperti Mimikatz atau pwdump untuk mem-bypass perlindungan tersebut. Setelah hash kata sandi diekstrak, langkah berikutnya adalah melakukan cracking, yaitu mencoba memecahkan hash tersebut untuk mendapatkan kata sandi asli. Salah satu teknik yang umum digunakan untuk cracking adalah **brute-force** atau **dictionary attack**, di mana

penyerang mencoba berbagai kombinasi kata sandi atau menggunakan daftar kata sandi yang umum. Meski hash dirancang untuk sulit dipecahkan, jika kata sandi yang digunakan lemah atau tidak aman, proses cracking bisa lebih mudah dan cepat. Oleh karena itu, penggunaan kata sandi yang kuat serta lapisan keamanan tambahan seperti enkripsi file SAM dan penggunaan **salting** pada hash dapat membantu mengurangi risiko dumping dan cracking ini.

Tujuan dari *dumping and cracking SAM* adalah :

1. Mengetahui cara menggunakan alat pwdump7 untuk mengekstrak hash kata sandi.
2. Mengetahui cara menggunakan alat Ophcrack untuk memecahkan kata sandi dan mendapatkan teks biasa.

1. Kita mencari tahu User ID dengan username menggunakan CMD via mode administrator.



2. Masukkan kode **“wmic useraccount get name,sid”** pada CMD 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-1-5-21-573011037-3557357056-4035154767-500
arfat S-1-5-21-573011037-3557357056-4035154767-1002
DefaultAccount S-1-5-21-573011037-3557357056-4035154767-503
defaultuser0 S-1-5-21-573011037-3557357056-4035154767-1001
Guest S-1-5-21-573011037-3557357056-4035154767-501
WDAGUtilityAccount S-1-5-21-573011037-3557357056-4035154767-504
```

3. Download dan extract pwdump dan ophcrack.

 ophcrack-3.8.0-bin.zip	10/13/2024 8:26 PM	WinRAR ZIP archive	15,469 KB
 pwdump-master.zip	10/13/2024 9:00 PM	WinRAR ZIP archive	517 KB

4. Buka dan salin lokasi file pwdump dan klik enter untuk masuk ke directory pwdumpmaster, kemudian ketik PwDump7.exe untuk mendapatkan dan menampilkan password hashes dan userID.

```
C:\Windows\system32>cd C:\Users\arfat\Downloads\pwdump-master
C:\Users\arfat\Downloads\pwdump-master>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:F607941900C13FA5FB04D9F96EB94C4D:F11BFADECB1CE6EF24841E7EED6A915C:::
Guest:501:1356A2636620AA17DC2017B33D5E2A79:27C0E956CD1BF4845B36844DE02D6F0B:::
j:503:1520B8015B8FCFD533D5BFCB44CD4FE3:351755276F6DD1B4E5345DDC55858010:::
j:504:F8BDD5C2337C8E60E9253A5925BB5BEF:89B5E3DE27CBD51F9822F6497AB9ECE0:::
j:1001:D8BF86C591021B16D18B6AD531990B54:907E4F819231E91471AB76C8D9D730AA:::
arfat:1002:B1F40D8470413600A6F749A942DAE6C9:3945F93CC6E8B45D939AF5DFE7282E1A:::
```

5. Pindahkan dan copy semua data hasil dari PwDump7.exe ke hashes.txt menggunakan command PwDump7.exe > c:\hashes.txt

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

Berikut isi dari hashes yang sudah disalin.

```
Administrator:500:F607941900C13FA5FB04D9F96EB94C4D:F11BFADECB1CE6EF24841E7EED6A915C:::
Guest:501:1356A2636620AA17DC2017B33D5E2A79:27C0E956CD1BF4845B36844DE02D6F0B:::
j:503:1520B8015B8FCFD533D5BFCB44CD4FE3:351755276F6DD1B4E5345DDC55858010:::
j:504:F8BDD5C2337C8E60E9253A5925BB5BEF:89B5E3DE27CBD51F9822F6497AB9ECE0:::
j:1001:D8BF86C591021B16D18B6AD531990B54:907E4F819231E91471AB76C8D9D730AA:::
arfat:1002:B1F40D8470413600A6F749A942DAE6C9:3945F93CC6E8B45D939AF5DFE7282E1A:::
```

6. Isi semua username yang kosong sesuai dengan username pengguna pada step 2 kemudian save file hashes.txt

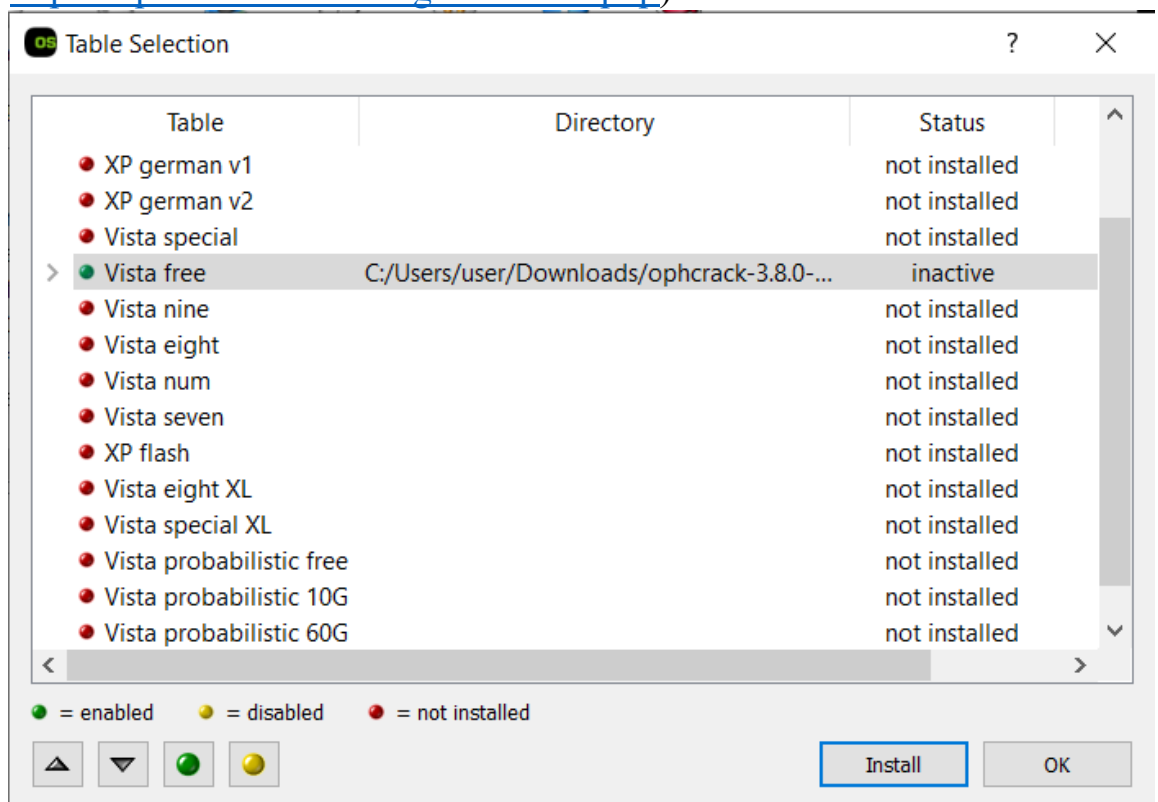
```
Administrator:500:F607941900C13FA5FB04D9F96EB94C4D:F11BFADECB1CE6EF24841E7EED6A915C:::
Guest:501:1356A2636620AA17DC2017B33D5E2A79:27C0E956CD1BF4845B36844DE02D6F0B:::
DefaultAccount:503:1520B8015B8FCFD533D5BFCB44CD4FE3:351755276F6DD1B4E5345DDC55858010:::
WDAGUtilityAccount:504:F8BDD5C2337C8E60E9253A5925BB5BEF:89B5E3DE27CBD51F9822F6497AB9ECE0:::
defaultuser0:1001:D8BF86C591021B16D18B6AD531990B54:907E4F819231E91471AB76C8D9D730AA:::
arfat:1002:B1F40D8470413600A6F749A942DAE6C9:3945F93CC6E8B45D939AF5DFE7282E1A:::
```

7. Buka ophcrack, kemudian pilih Load > PWDUMP file dan pilih file hashes.txt sebelumnya.

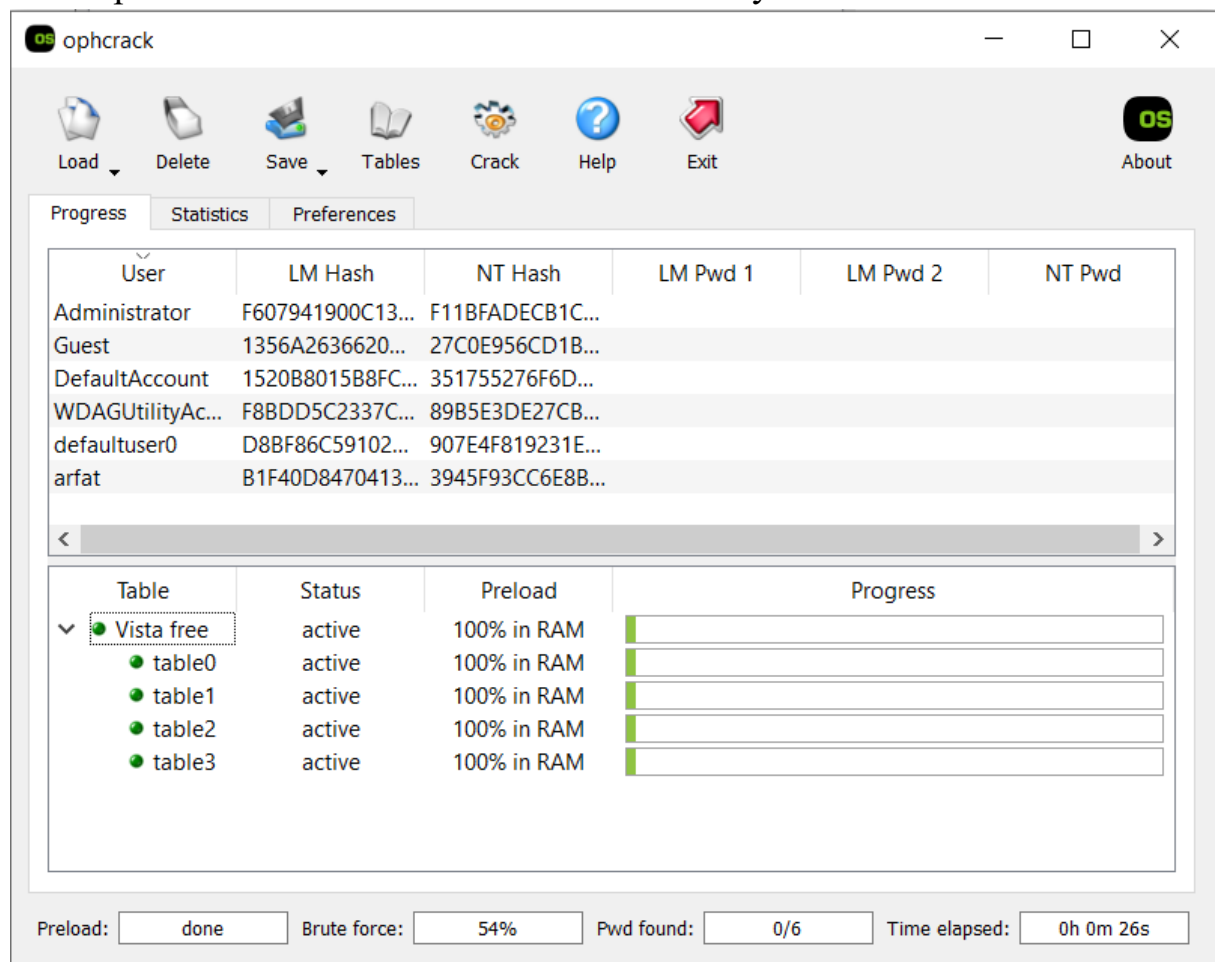
Berikut tampilan file hashes pada ophcrack.

Progress Statistics Preferences					
User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	F607941900C13...	F11BFADECB1C...			
Guest	1356A2636620...	27C0E956CD1B...			
DefaultAccount	1520B8015B8FC...	351755276F6D...			
WDAGUtilityAc...	F8BDD5C2337C...	89B5E3DE27CB...			
defaultuser0	D8BF86C59102...	907E4F819231E...			
arfat	B1F40D8470413...	3945F93CC6E8B...			

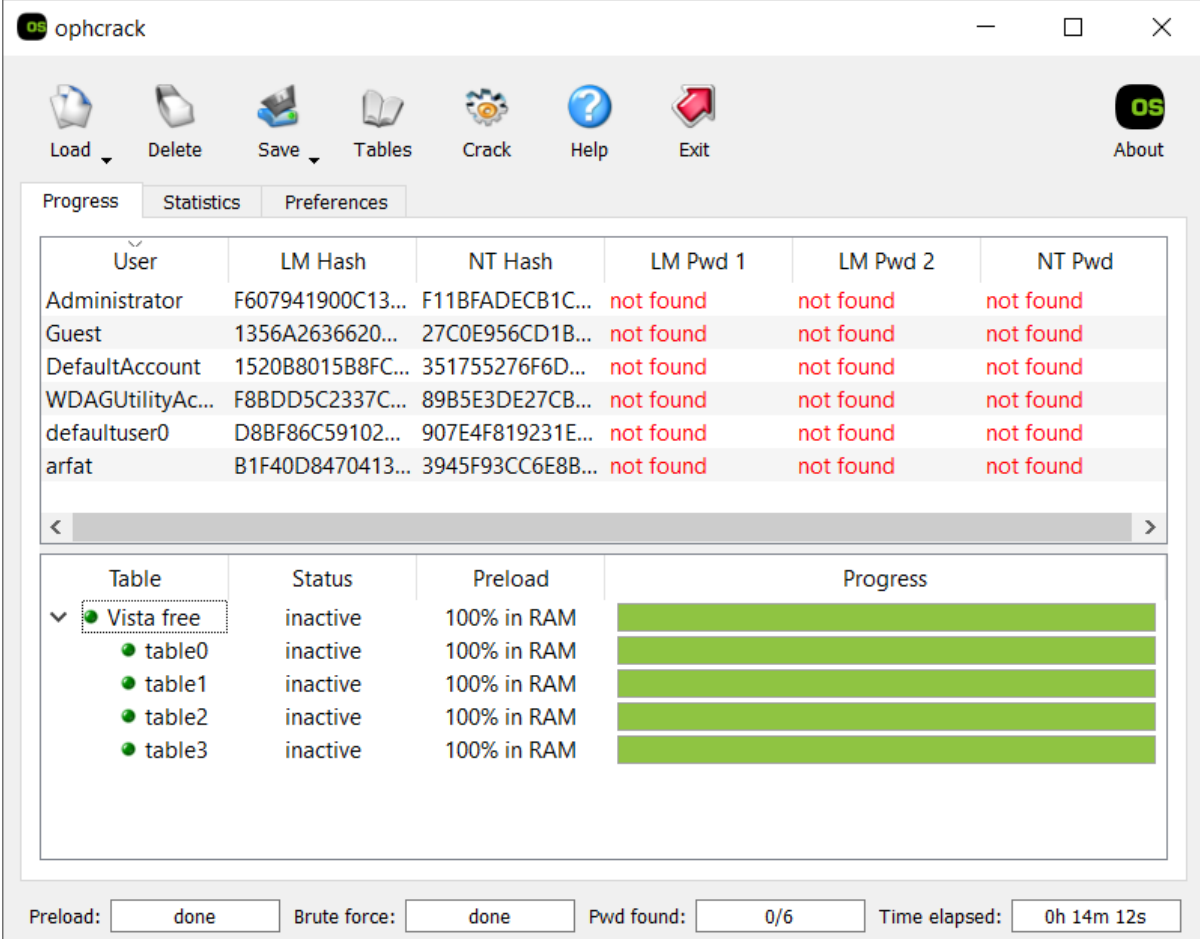
8. Klik Table, dan pada table selection pilih **vista free** kemudian klik install, kemudian pilih table vista free yang sudah di download sebelumnya. (table vista free bisa di download menggunakan link : <https://ophcrack.sourceforge.io/tables.php>)



9. Klik crack setelah menginstall tables sebelumnya untuk memecahkan kata sandi yang ada. Tunggu hingga selesai, OPHCrack akan memakan beberapa waktu untuk memecahkan kata sandinya.



10. 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.



The screenshot shows the Ophcrack application window. The main table displays the results of the password search for various users. All results are 'not found'. Below this table, there is a section for 'Vista free' tables, which are all 'inactive' and '100% in RAM'. At the bottom, the status bar shows 'Preload: done', 'Brute force: done', 'Pwd found: 0/6', and 'Time elapsed: 0h 14m 12s'.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	F607941900C13...	F11BFADECB1C...	not found	not found	not found
Guest	1356A2636620...	27C0E956CD1B...	not found	not found	not found
DefaultAccount	1520B8015B8FC...	351755276F6D...	not found	not found	not found
WDAGUtilityAc...	F8BDD5C2337C...	89B5E3DE27CB...	not found	not found	not found
defaultuser0	D8BF86C59102...	907E4F819231E...	not found	not found	not found
arfat	B1F40D8470413...	3945F93CC6E8B...	not found	not found	not found

Table	Status	Preload	Progress
▼ Vista free	inactive	100% in RAM	<div></div>
● table0	inactive	100% in RAM	<div></div>
● table1	inactive	100% in RAM	<div></div>
● table2	inactive	100% in RAM	<div></div>
● table3	inactive	100% in RAM	<div></div>

Preload: Brute force: Pwd found: Time elapsed: