

Dumping And Cracking SAM Hashes To Exstract Plaintext Password

1. Yang pertama mendownload semua file pada link berikut. Setelah itu ekstrak semua filenya.

- Table Vista free

https://sourceforge.net/projects/ophcrack/files/tables/Vista%20free/tables_vista_free.zip/download

- PwDump7

<https://github.com/Seabreg/pwdump>

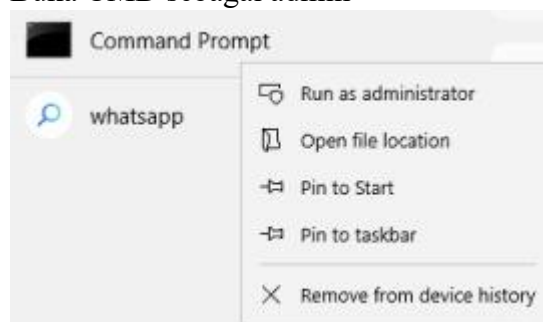
- Ophcrack

<https://ophcrack.sourceforge.io/download.php?type=ophcrack>

tables_vista_free	13/10/2024 14:10	Compressed (zipp...	400.987 KB
pwdump-master	13/10/2024 14:08	Compressed (zipp...	517 KB
ophcrack-3.8.0-bin	13/10/2024 14:07	Compressed (zipp...	15.469 KB

2. Langkah selanjutnya kita akan mengambil file hashes yang berisi username dan password user.

- Buka CMD sebagai admin



- Ketik wmic useraccount get username,id

```
C:\Windows\system32>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-2884404221-3422014549-1795551341-500
DefaultAccount S-1-5-21-2884404221-3422014549-1795551341-503
Guest S-1-5-21-2884404221-3422014549-1795551341-501
tter1 S-1-5-21-2884404221-3422014549-1795551341-1001
WDAGUtilityAccount S-1-5-21-2884404221-3422014549-1795551341-504
```

- Selanjutnya pada cmd buka folder pwdump7

```
C:\Windows\system32>cd C:\Users\tter1\Downloads\pwdump-master\pwdump-master
```

- Jalankan pwdump7.exe untuk melakukan hashes

```
C:\Users\tter1\Downloads\pwdump-master\pwdump-master>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:0F0D1B10B86A75AA5C842F95A12F28D9:64D6344C4EAF22FE11D7BD344A94B857:::
Guest:501:BD5CCC607726B4412B4DA81EDE530737:63FA257F7F949374F5394E5D37973848:::
5:503:AF37D0821596537C085AFD518A5878F3:12B2345B75907D1366D3576082404161:::
5:504:296448AF0D194E3DF778A88CAE01660:982356321E25D2855C69F3BA9F682E90:::
tter1:1001:3B46F6E8B7B22D9C3F0343FA50034C66:E71B22337326B8D6A5F2DA7D9EBD2B0B:::
```

- Selanjutnya akan memindahkan hasil dari pwdump7 tadi ke dalam bentuk txt.

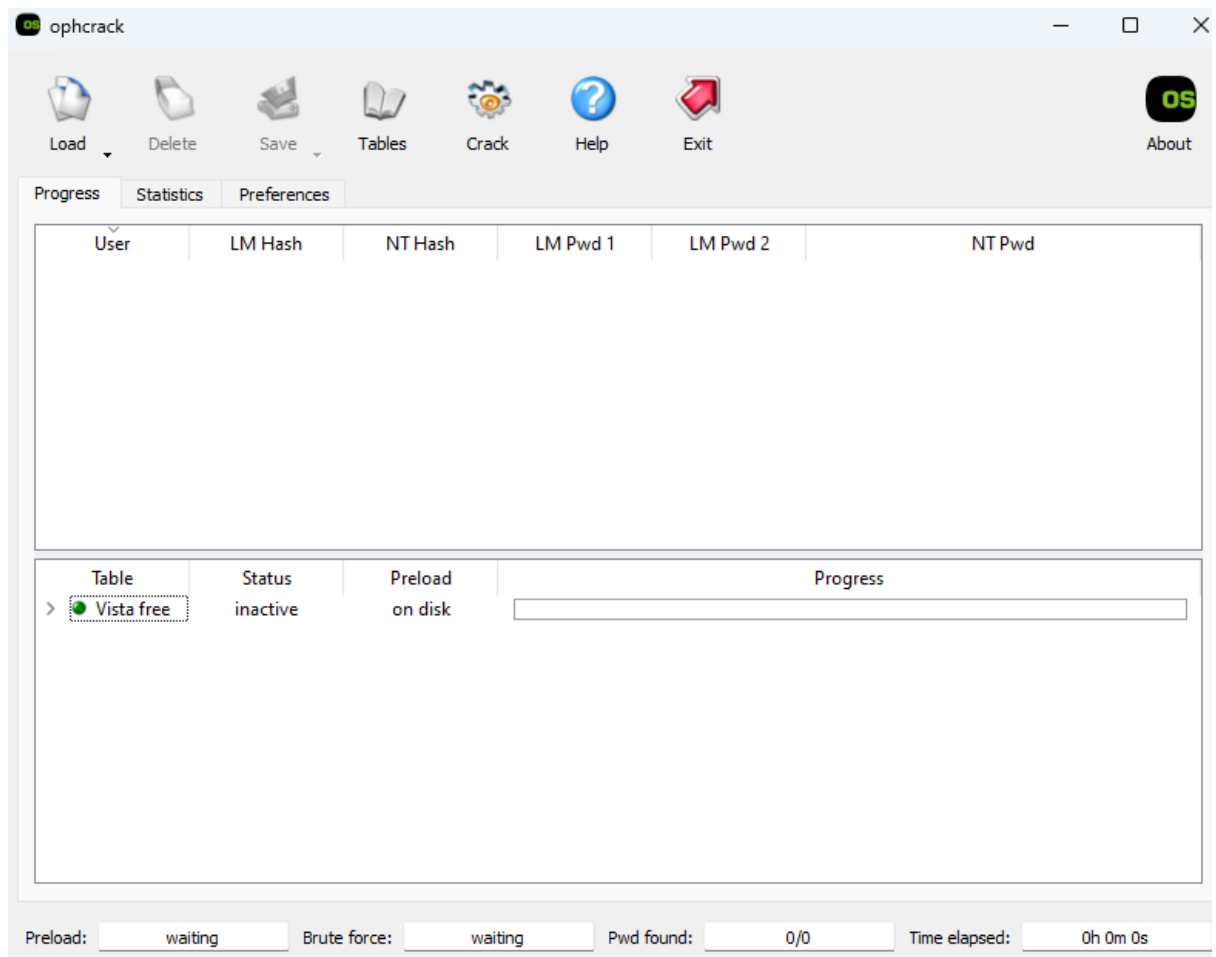
```
C:\Users\tter1\Downloads\pwdump-master\pwdump-master>Pwdump7.exe > hashes.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

- Berikut isi file hashes.txt nya



```
Administrator:500:0F0D1810B86A75AA5C842F95A12F28D9:64D6344C4EAF22FE11D7BD344A948857:::
Guest:501:BD5CCC6B7726B4412B4DAB1EDE530737:63FA257F7F949374F5394E5D37973848:::
503:AF37D0821596537C085AFD518A5878F3:12B2345B75907D1366D3576082404161:::
504:296448AF0DD194E3DF77BA88CAE01660:982356321E25D2855C69F3BA9F682E90:::
tter1:1001:3B46F6E8B7B22D9C3F0343FA50034C66:E71B22337326B8D6A5F2DA7D9EBD2B0B:::
```

3. Langkah selanjutnya yaitu melakukan crack file hasehes.txt menggunakan tools ophcrack



- Sebelum itu terlebih dahulu menginstal table pada ophcrack dengan cara berikut.
- Buka Tables



Load



Delete



Save



Tables



Crack



Help



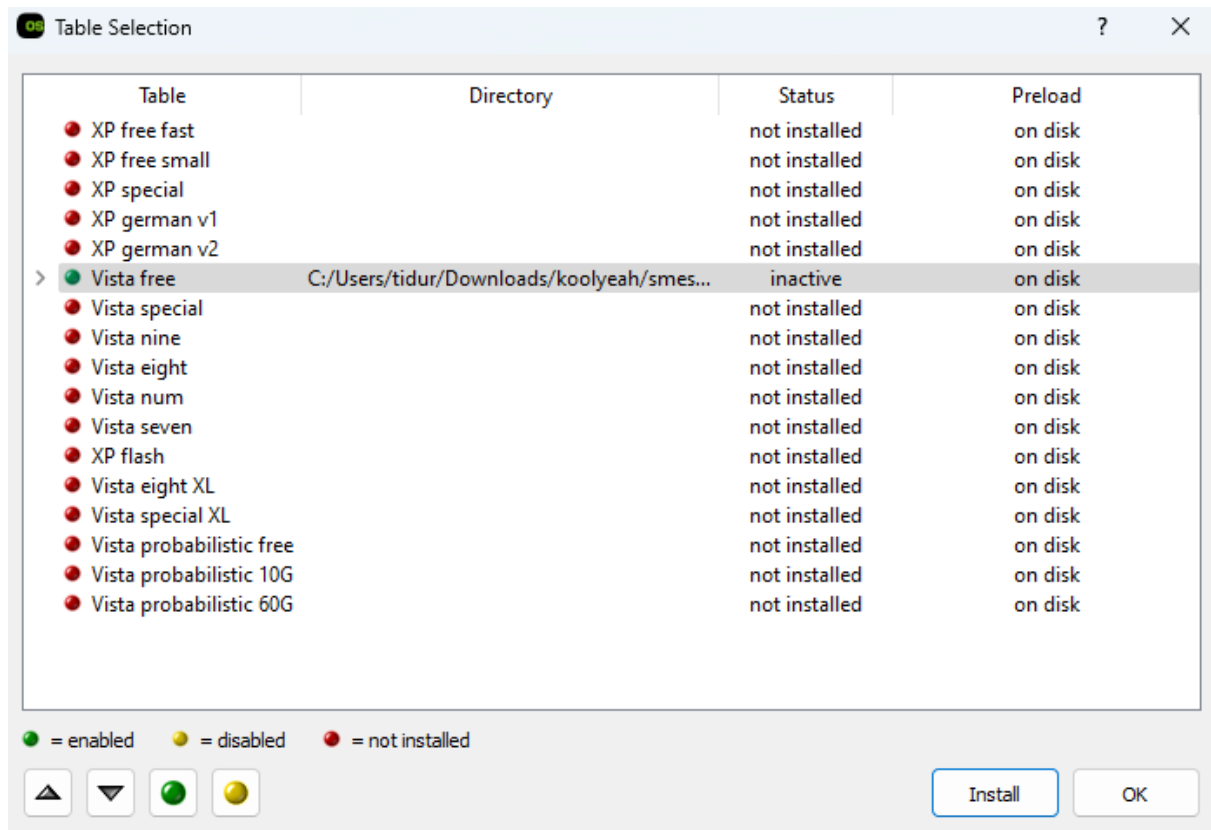
Exit

Progress

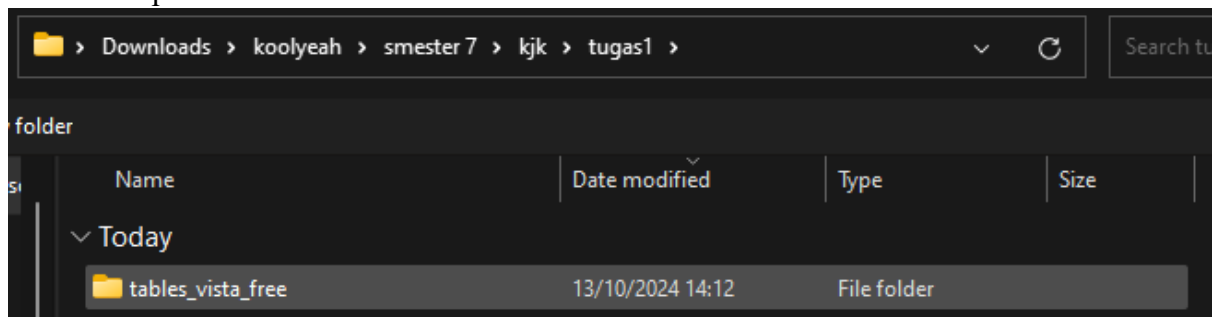
Statistics

Preferences

- Pilih Vista free dan klik install



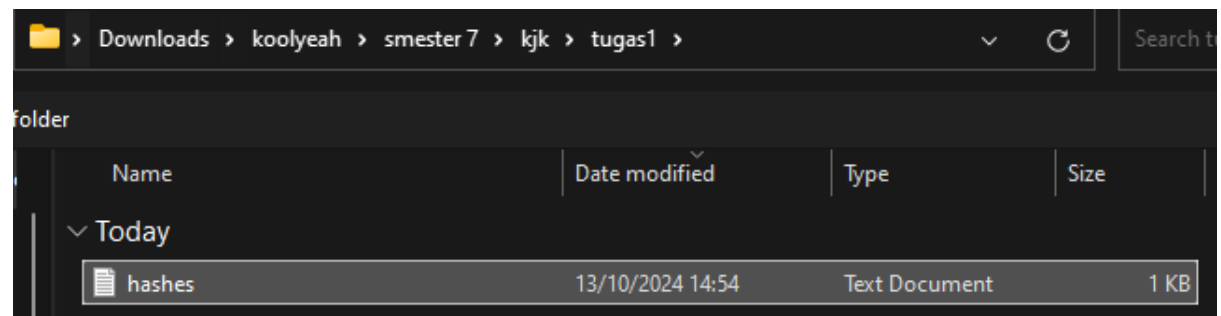
- Setelah itu pilih direktori dimana file vista free di ekstrak



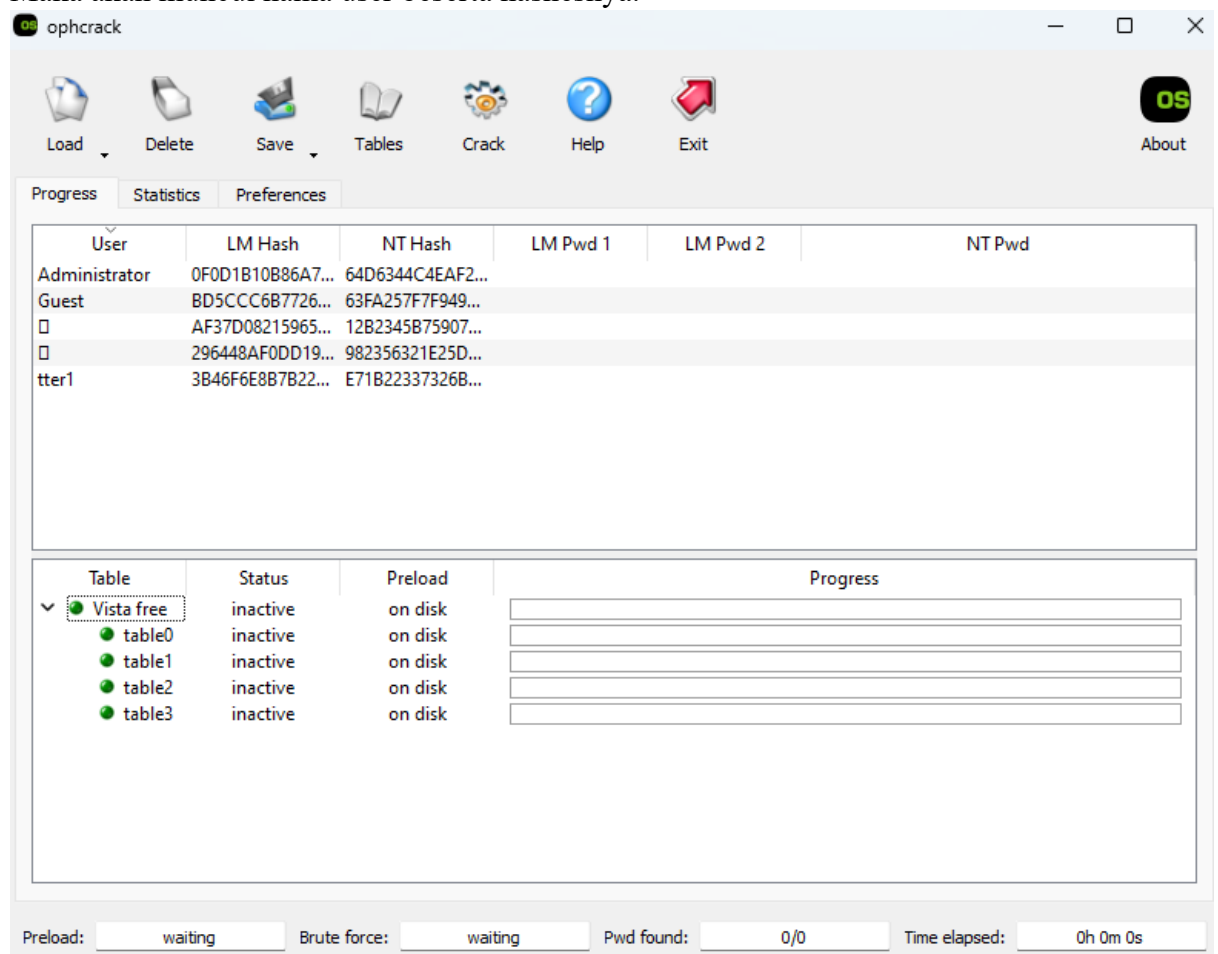
-

- ophcrack
- Load Delete Save Ta
- Single hash
 - PWDUMP file
 - Session file
 - Encrypted SAM
 - Local SAM with samdump2

- Selanjutnya pilih file hashes nya.



- Maka akan muncul nama user beserta hashesnya.



- Selanjutnya click Crack dan tunggu Progress nya sampai selesai.

ophcrack

Load Delete Save Tables Stop Help Exit About

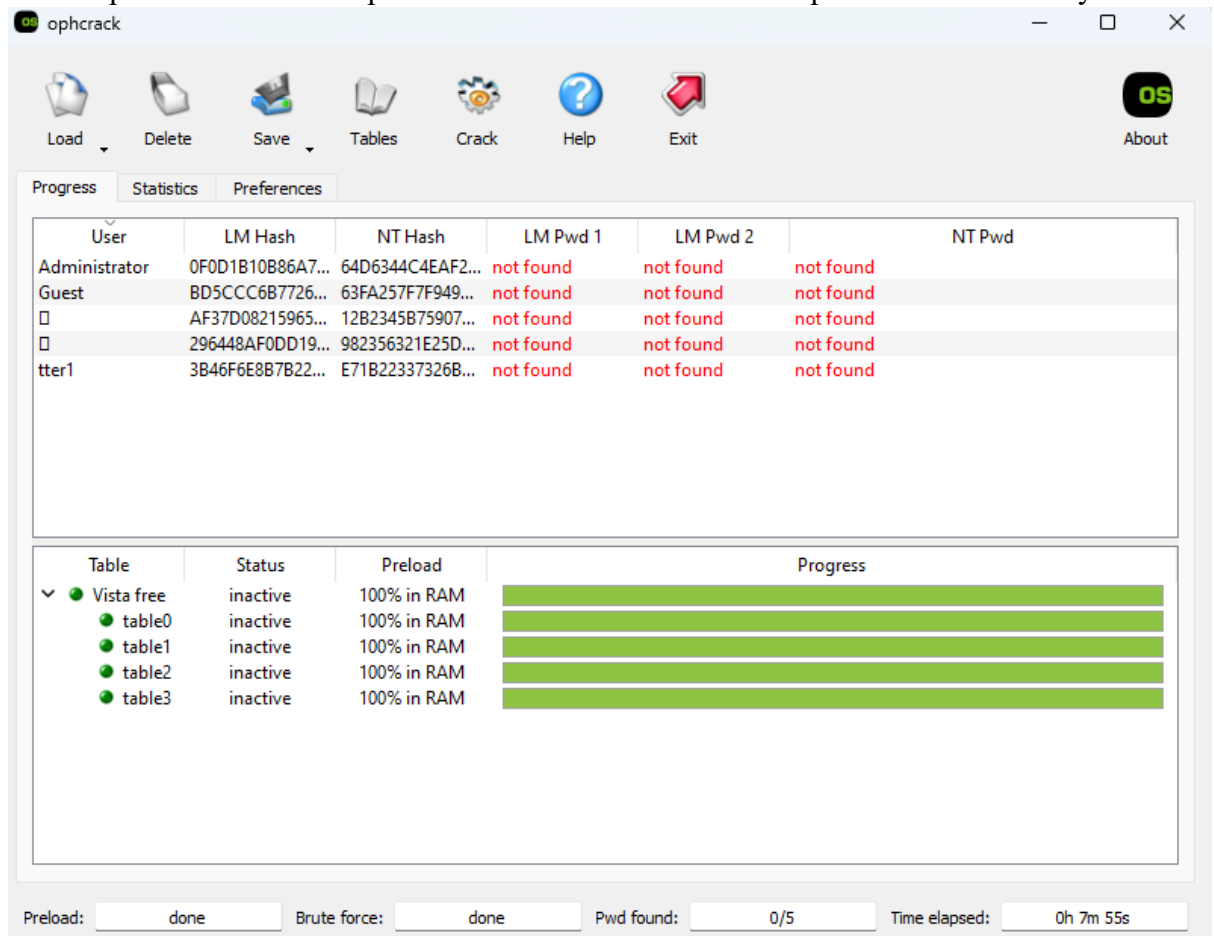
Progress Statistics Preferences

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	0F0D1B10B86A7...	64D6344C4EAF2...			
Guest	BD5CCC6B7726...	63FA257F7F949...			
	AF37D08215965...	12B2345B75907...			
	296448AF0DD19...	982356321E25D...			
ttter1	3B46F6E8B7B22...	E71B22337326B...			

Table	Status	Preload	Progress
<input checked="" type="checkbox"/> Vista free <input checked="" type="checkbox"/> table0 <input checked="" type="checkbox"/> table1 <input checked="" type="checkbox"/> table2 <input checked="" type="checkbox"/> table3	active	100% in RAM	<div><div></div></div>
	active	100% in RAM	<div><div></div></div>
	active	100% in RAM	<div><div></div></div>
	active	100% in RAM	<div><div></div></div>
	active	100% in RAM	<div><div></div></div>

Preload: done Brute force: done Pwd found: 0/5 Time elapsed: 0h 5m 36s

- Setelah proses selesai maka pada LM Pwd 1 dan 2 akan keluar password dari usernya.



Pada percobaan diatas kenapa not found mungkin karena sistem protection pada windows sudah makin bagus. Jadi untuk model hacking ini tidak akan bisa. Dan juga mungkin pada library tables nya kurang karena menggunakan yang free.