

NAMA : PUTRI DANTY APRIANI
NIM : 09011182126005
KELAS : SK7A INDRALAYA
MATA KULIAH : KEAMANAN JARINGAN KOMPUTER

Lab 2

Dumping and Cracking SAM Hashes to Extract Plaintext Passwords

Tools :

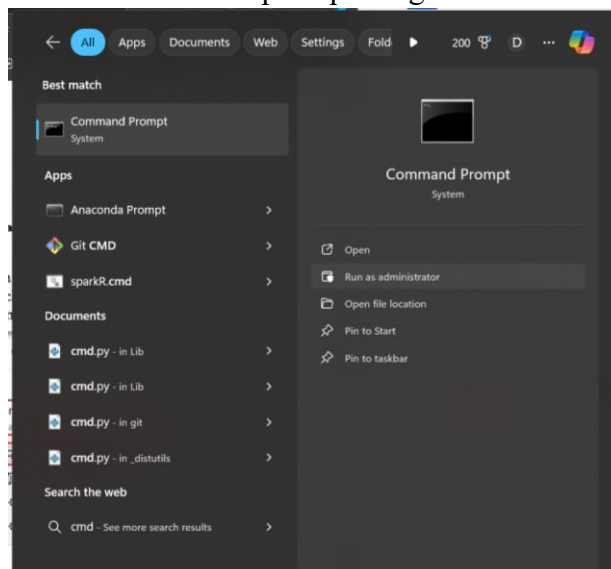
- Windows 11
- Pwdump7
- Ophcrack

Pwdump7 dan Ophcrack adalah alat yang digunakan untuk keamanan dan pemulihan kata sandi pada sistem Windows.

1. Pwdump7: adalah alat yang digunakan untuk mengekstrak kata sandi hash dari file SAM (Security Account Manager) di Windows. Pwdump7 dapat membantu dalam mengumpulkan informasi untuk audit keamanan atau dalam pengujian penetrasi.
2. Ophcrack: adalah alat pemulihan kata sandi yang menggunakan teknik rainbow table untuk memecahkan kata sandi Windows. Ophcrack dapat digunakan untuk mengembalikan akses ke akun pengguna jika kata sandi terlupakan.

Langkah-langkah :

1. Jalankan command prompt dengan mode run as administrator.



2. Masukkan command prompt berikut untuk mengetahui nama pengguna dan UserIDs.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-3221041124-1981190527-2894957778-500
DefaultAccount       S-1-5-21-3221041124-1981190527-2894957778-503
Guest                S-1-5-21-3221041124-1981190527-2894957778-501
user                 S-1-5-21-3221041124-1981190527-2894957778-1001
WDAGUtilityAccount   S-1-5-21-3221041124-1981190527-2894957778-504

C:\Windows\System32>
```

3. Jalankan PwDump7.exe untuk mengumpulkan hashes dan UserIDs.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.4317]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\UNSRI\Sistem Komputer\SEMESTER\Semester 7\Keamanan Jaringan Komputer\tugas

C:\UNSRI\Sistem Komputer\SEMESTER\Semester 7\Keamanan Jaringan Komputer\tugas>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:D0E74D17AF45ACE23CA5D9CC0C740D34:EC5171B72A9604E6A190F321A68749A4:::
Guest:501:EF00C14D3BC709F7C569D1D2A983859A:B635206F2B8B502818E0F75F710A3098:::
j:503:50155FDCBF886043802A004512CA6813:93BAEE4FB5112B48DB4B7A93F170086C:::
j:504:8FC8B9639DCF3250B0DA9371FFA28729:250A02AEFA0BD9B99C27E658017D9A79:::
user:1001:F7E152A5322FBEC90D70BBBD7D643DE4:D17AB383AF60635CDC09A1086A56E0D2:::

C:\UNSRI\Sistem Komputer\SEMESTER\Semester 7\Keamanan Jaringan Komputer\tugas>
```

4. Menampilkan isi dari file hashes.txt

```
C:\UNSRI\Sistem Komputer\SEMESTER\Semester 7\Keamanan Jaringan Komputer\tugas>PwDump7.exe > c:\hashes.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\UNSRI\Sistem Komputer\SEMESTER\Semester 7\Keamanan Jaringan Komputer\tugas>
```

```
File Edit View

Administrator:500:D0E74D17AF45ACE23CA5D9CC0C740D34:EC5171B72A9604E6A190F321A68749A4:::
Guest:501:EF00C14D3BC709F7C569D1D2A983859A:B635206F2B8B502818E0F75F710A3098:::
j:503:50155FDCBF886043802A004512CA6813:93BAEE4FB5112B48DB4B7A93F170086C:::
j:504:8FC8B9639DCF3250B0DA9371FFA28729:250A02AEFA0BD9B99C27E658017D9A79:::
user:1001:F7E152A5322FBEC90D70BBBD7D643DE4:D17AB383AF60635CDC09A1086A56E0D2:::
```

5. Ganti nama pengguna sebelum UserIDs masing-masing yang telah didapatkan pada Langkah 2.

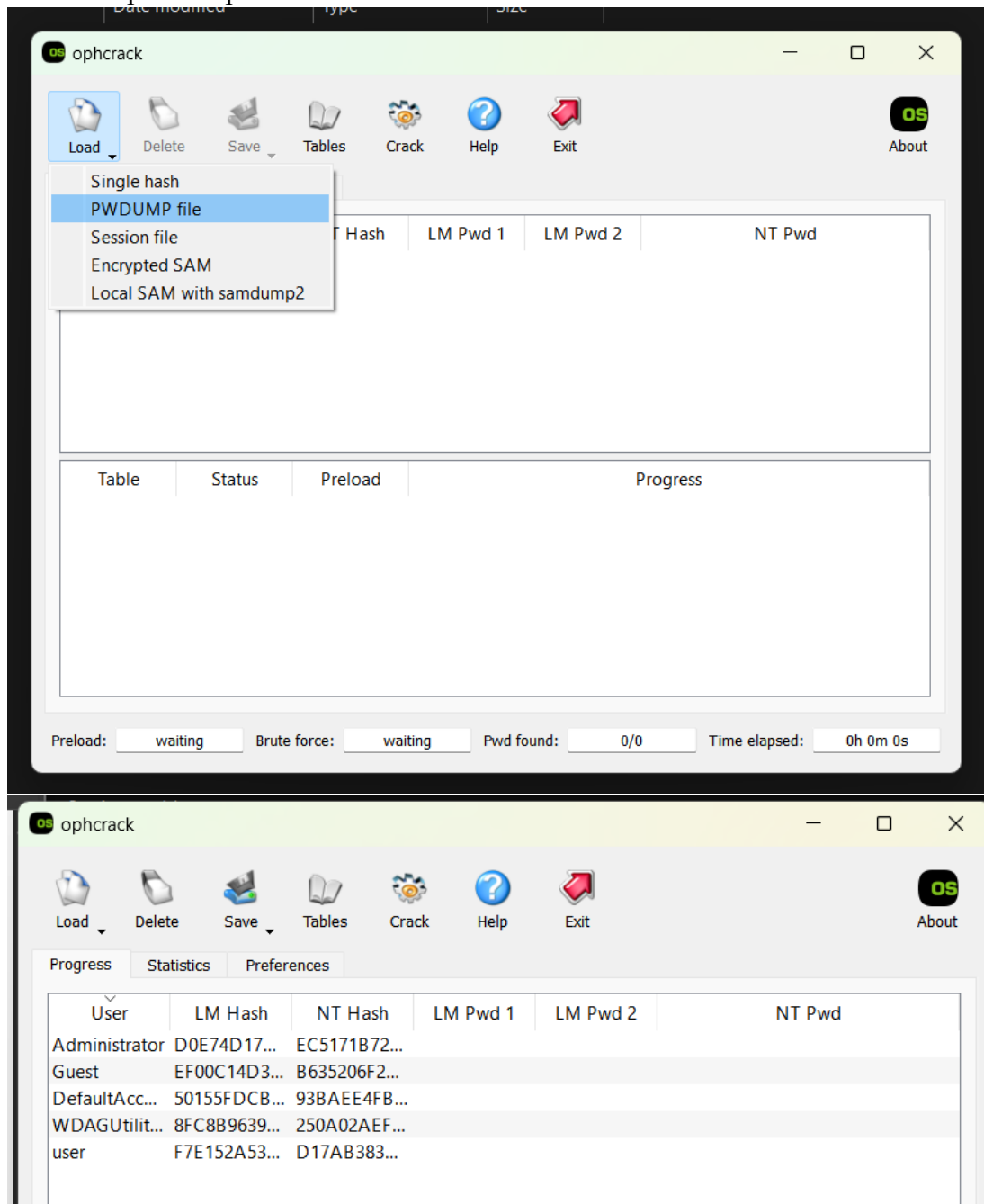
```

File Edit View


Administrator:500:D0E74D17AF45ACE23CA5D9CC0C740D34:EC5171B72A9604E6A190F321A68749A4:::
Guest:501:EF00C14D3BC709F7C569D1D2A983859A:B635206F2B8B502818E0F75F710A3098:::
DefaultAccount:503:50155FDCBF886043802A004512CA6813:93BAEE4FB5112B48DB4B7A93F170086C:::
WDAGUtilityAccount:504:8FC8B9639DCF3250B0DA9371FFA28729:250A02AEFA0BD9B99C27E658017D9A79:::
user:1001:F7E152A5322FBEC90D70BBBD7D643DE4:D17AB383AF60635CDC09A1086A56E0D2:::

```

6. Jalankan aplikasi ophcrack.exe dan masukkan file hashes.txt melalui PWDUMP file



7. Selanjutnya klik menu Tables, install file Vista free dan menginstallnya


Vista free (461MB)

Success rate: 99%

Based on a dictionary of 64k words, 4k suffixes, 64 prefixes and 4 alteration rules for a total of 2^{38} passwords (274 billion).

md5sum: 403cf58178d7272a48819b47ca8b2e6b

ophcrack

Table Selection

Table	Directory	Status	Preload
XP free fast		not installed	on disk
XP free small	C:\UNSRI\Sistem Komputer\SE...	inactive	on disk
XP special		not installed	on disk
XP german v1		not installed	on disk
XP german v2		not installed	on disk
Vista special		not installed	on disk
Vista free		not installed	on disk
Vista nine		not installed	on disk
Vista eight		not installed	on disk
Vista num		not installed	on disk
Vista seven		not installed	on disk
XP flash		not installed	on disk
Vista eight XL		not installed	on disk
Vista special XL		not installed	on disk
Vista probabilis...		not installed	on disk

enabled

disabled

not installed

Install

OK

Preload:

waiting

Brute force:

waiting

Pwd found:

0/0

Time elapsed:

0h 0m 0s

Vista free

XP free fast

XP special

XP german v1

XP german v2

Vista special

Vista nine

Vista eight

Vista num

Vista seven

XP flash

Vista eight XL

Vista special XL

C:\UNSRI\Sistem Komputer\SE...

inactive

not installed

not installed

not installed

not installed

not installed

not installed

not installed

not installed

not installed

not installed

not installed

not installed

100% in RAM

on disk

on disk

on disk

on disk

on disk

on disk

on disk

on disk

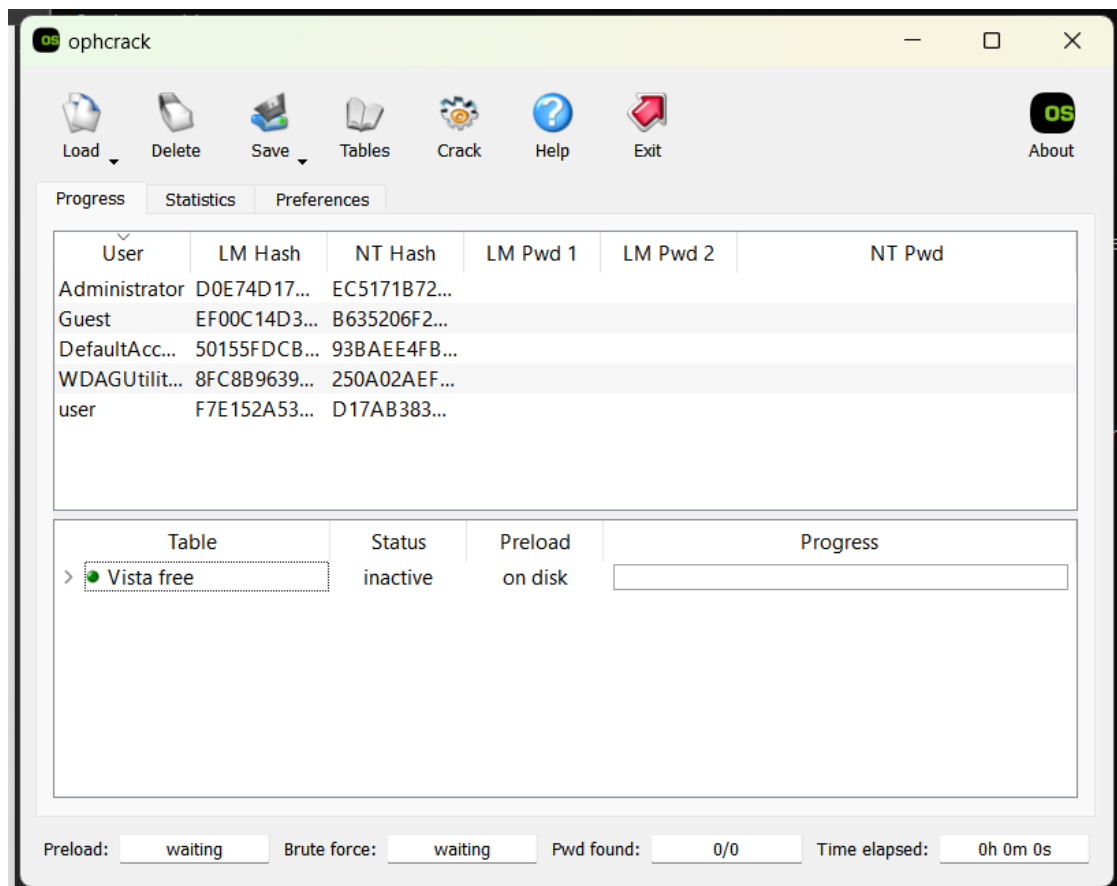
on disk

on disk

on disk

on disk

8. Langkah terakhir melakukan Crack.



9. Dapat dilihat bahwa tidak ada password yang dipakai, seperti yang ditampilkan hasil percobaan berikut ini.

ophcrack

Load

Delete

Save

Tables

Crack

Help

Exit

OS

About

Progress

Statistics

Preferences

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	D0E74D17AF45ACE23...	EC5171B72...	not found	not found	not found
Guest	EF00C14D3BC709F7C5...	B635206F2...	not found	not found	not found
DefaultAccount	50155FDCBF88604380...	93BAEE4FB...	not found	not found	not found
WDAGUtilityAccount	8FC8B9639DCF3250B0...	250A02AEF...	not found	not found	not found
user	F7E152A5322FBEC90D...	D17AB383...	not found	not found	not found

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

Preload:

done

Brute force:

done

Pwd found:

0/5

Time elapsed:

0h 31m 32s