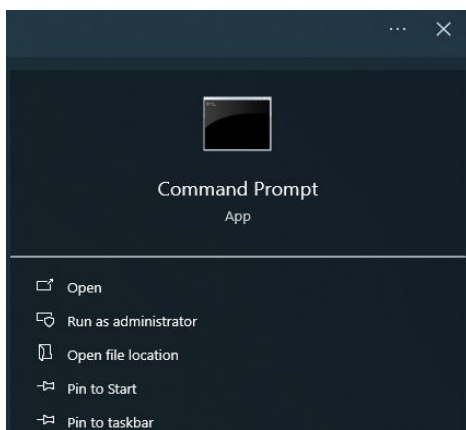


Nama : Fajar Pradika
NIM : 09011282126045
Mata Kuliah : Keamanan Jaringan komputer

Dumping And Cracking SAM Hashes to Extract PlainText Password

Security Account Manager (SAM) adalah basis data di Windows yang menyimpan informasi akun pengguna dan hash kata sandi (LM dan NTLM). Hash ini bersifat satu arah, memberikan perlindungan pada kata sandi. Dalam peretasan, penyerang mengekstrak hash dari SAM setelah mendapatkan akses administrator, kemudian menggunakan hash ini untuk serangan kata sandi atau mengakses sistem lain. Penilaian keamanan dimulai dengan mengekstrak hash dan memecahkannya menjadi kata sandi teks biasa. Tujuannya adalah untuk mempelajari penggunaan pwdump7 untuk ekstraksi hash dan Ophcrack untuk cracking kata sandi.

1. Untuk mengetahui User ID kita menggunakan cmd administrator mode pada windows pada percobaan kali ini saya menggunakan windows 10 pada kali linux.



2. Setelah membuka cmd administrator jalan kan code `wmic useraccount get name,sid` untuk menampilkan nama akun pengguna dan Security Identifier (SID) di Windows yang Outputnya adalah daftar akun pengguna beserta SID, yang merupakan pengenalan unik setiap akun.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>wmic useraccount get name,sid
Name SID
ACER S-1-5-21-713649669-2513938858-2884992973-1000
Administrator S-1-5-21-713649669-2513938858-2884992973-500
DefaultAccount S-1-5-21-713649669-2513938858-2884992973-503
Guest S-1-5-21-713649669-2513938858-2884992973-501
WDAGUtilityAccount S-1-5-21-713649669-2513938858-2884992973-504
```

3. Jalankan perintah dibawah ini untuk menyimpan beberapa bagian penting dari registry Windows (SAM, Security, System) ke file di desktop lalu saya pindahkan ke kali linux.

```
C:\Windows\system32>cd C:\Users\ACER\OneDrive\Desktop
The system cannot find the path specified.

C:\Windows\system32>
C:\Windows\system32>cd C:\Users\ACER\OneDrive\Desktop
The system cannot find the path specified.

C:\Windows\system32>cd C:\Users\ACER\Desktop

C:\Users\ACER\Desktop>reg save hklm\sam sam.save
The operation completed successfully.

C:\Users\ACER\Desktop>reg save hklm\security security.save
The operation completed successfully.

C:\Users\ACER\Desktop>reg save hklm\system systemsave
The operation completed successfully.

C:\Users\ACER\Desktop>reg save hklm\system system.save
The operation completed successfully.
```

4. Masukkan Perintah samdump2 untuk mengekstrak **hash kata sandi** dari file SAM Windows.

```
(kali@kali)-[~]
$ samdump2
samdump2 3.0.0 by Objectif Securite (http://www.objectif-securite.ch)
original author: ncuomo@studenti.unina.it

Usage: samdump2 [OPTION]... SYSTEM_FILE SAM_FILE
Retrieves syskey and extract hashes from Windows 2k/NT/XP/Vista SAM

-d          enable debugging
-h          display this information
-o file     write output to file
```

5. Lalu lakukan langkah dibawah ini ke folder **Downloads** dan menampilkan isinya. Kemudian, dengan perintah samdump2, pengguna mengekstrak hash akun Windows dari file **system.save** dan **sam.save**. Setelah itu, pengguna menggunakan alat **creddump7** dengan perintah pwdump.py untuk mengekstrak hash kata sandi dan menyimpannya dalam file **fajarpass**, lalu menampilkan isinya menggunakan perintah cat.

```
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ samdump2 system.save sam.save
+disabled* Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
+disabled* Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
+disabled* :503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
+disabled* :504:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ACER:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

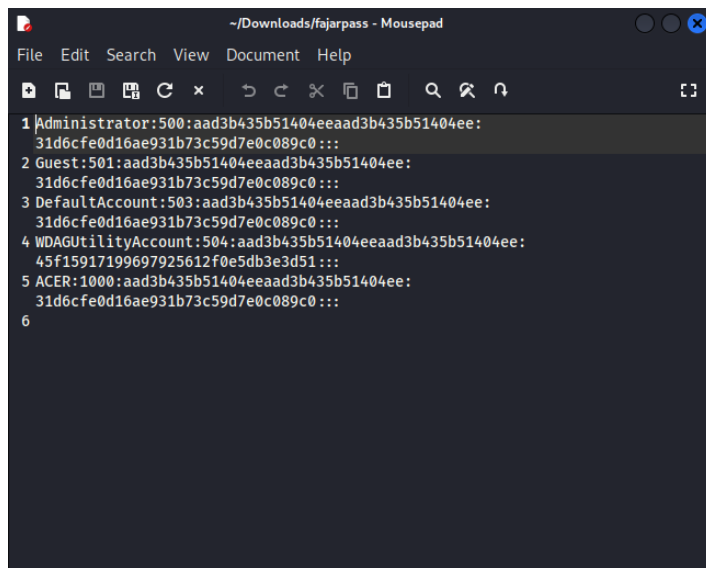
(kali@kali)-[~/Downloads]
$ creddump7
creddump7 - Python tool to extract credentials and secrets from Windows registry hives
/usr/share/creddump7
├── cachedump.py
├── framework
├── lsadump.py
├── pwdump.py
└── pycache
(kali@kali)-[/usr/share/creddump7]
$ python pwdump.py
Command 'python' not found, did you mean:
  command 'python' from deb python-is-python3
  command 'cython' from deb cython3
  command 'jython' from deb jython
Try: sudo apt install <deb name>

(kali@kali)-[/usr/share/creddump7]
$ python pwdump.py
usage: pwdump.py <system hive> <SAM hive>

(kali@kali)-[/usr/share/creddump7]
$ python pwdump.py '/home/kali/Downloads/system.save' '/home/kali/Downloads/sam.save' > ~/Downloads/fajarpass

(kali@kali)-[/usr/share/creddump7]
$ cat '/home/kali/Downloads/fajarpass'
```

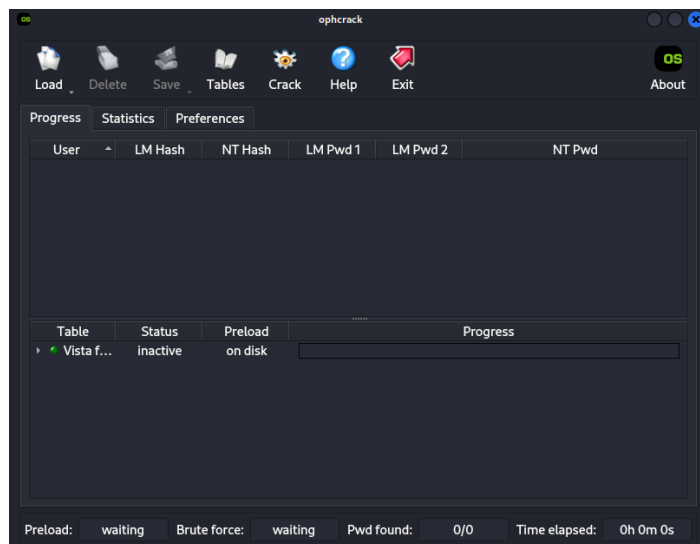
6. Berikut isi dari hashes.txt.



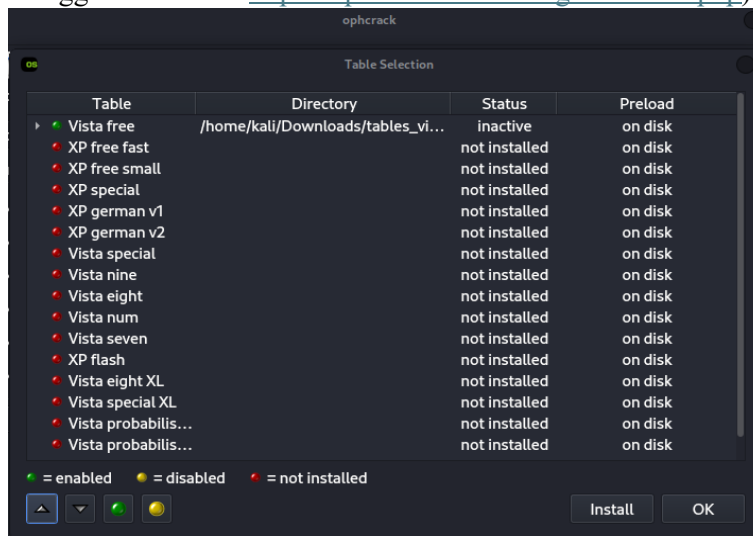
A screenshot of a text editor window titled "~Downloads/fajarpass - Mousepad". The window contains a list of six entries, each representing a user account and its corresponding hash. The entries are numbered 1 through 6. The first entry is "1 administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::". The second entry is "2 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::". The third entry is "3 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::". The fourth entry is "4 WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:45f15917199697925612f0e5db3e3d51:::". The fifth entry is "5 ACER:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::". The sixth entry is "6".

```
1 administrator:500:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
2 Guest:501:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
3 DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
4 WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:
45f15917199697925612f0e5db3e3d51:::
5 ACER:1000:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
6
```

7. Jalankan perintah ophcrack pada terminal dan gunakan tools ophcrack pada kali linux



8. Lalu 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. Berikut hasil penggunaan Ophcrack untuk memecahkan hash kata sandi Windows. Terdapat beberapa akun pengguna, termasuk Administrator, Guest, DefaultAccount, dan ACER, yang memiliki hash NT yang sama (31d6cfe0d1...) tetapi tidak ada kata sandi yang ditemukan (dinyatakan sebagai "empty"). Akun WDAGUtilityAccount juga tidak berhasil ditemukan. Dalam proses pemecahan, tabel rainbow Vista free telah dimuat 100% ke dalam RAM, tetapi statusnya masih inactive. Dari total 5 hash yang diuji, 4 berhasil ditemukan, namun tidak satu pun dapat direkonstruksi menjadi kata sandi. Proses pemecahan ini memakan waktu selama 54 detik. Meskipun ada 4 hash yang berhasil ditemukan, semua kata sandi tetap tidak dapat diterjemahkan menjadi teks biasa.

