**SMK7 CYBER SECURITY**

**LKSN [2022]**

|  |  |
| --- | --- |
|  |  |
|  | SMK Negeri 7 Samarinda - Wikipedia bahasa Indonesia ... |

|  |  |  |
| --- | --- | --- |
| Nama Lengkap | : | M.rizqullah ar rahman |
| Jurusan | : | XI TJKT 3 |
| NIM | : | - |
| Username | : | - |

Daftar Isi

Forensic  **3**

Memdump 3

shoulder surfing

**Anda telah mendapati teman sekantor Anda tengah melakukan sesuatu yang cukup "malicious" pada victim host computer teman Anda dari CCTV. Sebelumnya, dia sedang melakukan shoulder surfing terhadap victim dan tim forensik mengira jika dia ingin mengingat kombinasi password temannya. Tatkala dikira itu sangatlah tidak mungkin, ternyata dia dapat mengakses komputernya dengan mudah. Beberapa menit kemudian, teman sekantor Anda tertangkap basah dan melarikan diri**

**Dapatkah Anda mendapatkan \*\*password logon OS\*\* yang memang telah "diingat" oleh si penyerang? Tim Digital Forensik telah melakukan akuisisi memori pada laptop korban dan mereka meminta Anda untuk mengetes jika password tersebut bahkan \*\*sangat mudah untuk didapatkan\*\*. 4**

4

# 

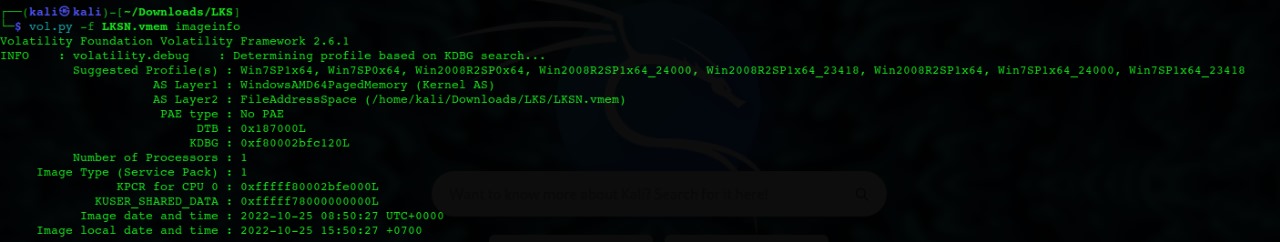
# **Memdump**

## Shoulder surfing

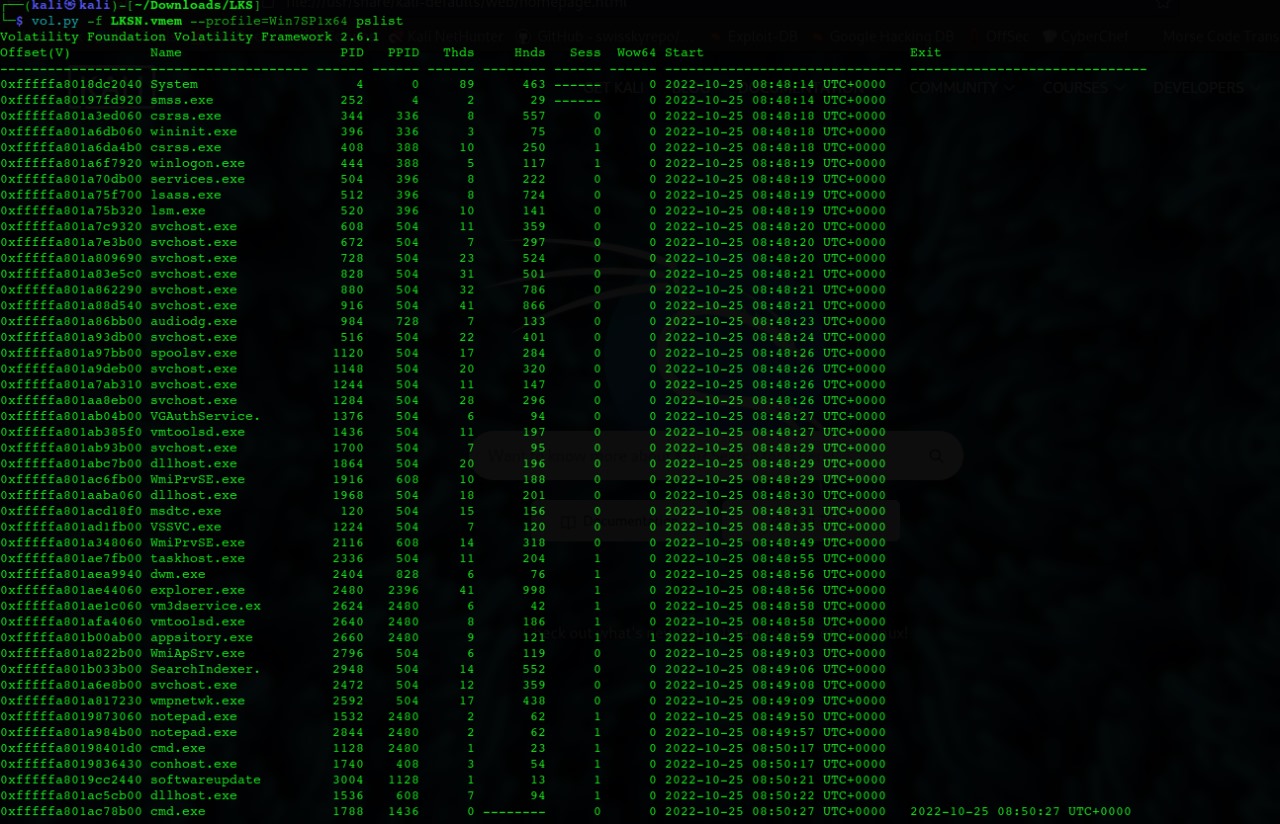
**Langkah Penyelesaian:**

Kita menggunakan tools yang bernama volatility

1.Yang perlu kita tau di awal adalah menemukan profile yang di curigai



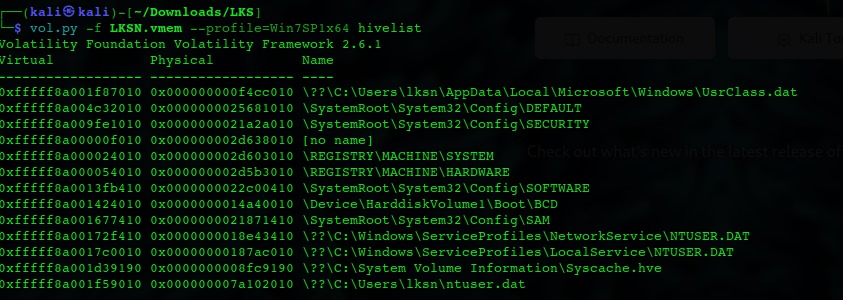
2.dan setelah mengetahui profile yang kita dapat, kita memerlukan proses dari profile tersebut



Dan disini saya mencurigai salah satu program karna tidak seperti biasanya



3. Untuk menemukan alamat virtual kumpulan registri di memori, dan jalur lengkap ke kumpulan terkait di disk, gunakan perintah hivelist.



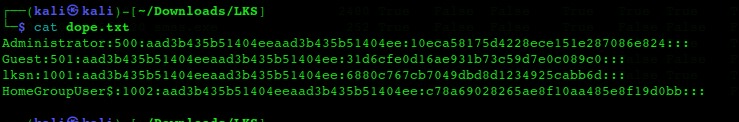
Dan kita mendapatkan sebuah tujuan yang ada SAM(Security Account Manager)



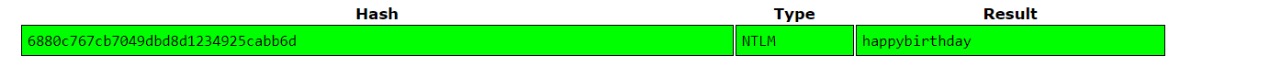
4.Setelah kita mendapatkan alamat tmpt nya jadi kita hashdump untuk mendapat kan jawaban soal nomor 1



Lalu kita cat file tersebut untuk melihat hash nya



5. yang terakhir kita memerlukan website <https://crackstation.net/>



6.**flag : happybirthday**