

Extract password from registry files

Có một người anh giới thiệu mình tool Mimikatz rất là "powerful" để xử chall này (mặc dù là trích xuất dùng tool khác vẫn được) nhưng tụi mình không thể solve được

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #19041 Aug  9 2020 22:45:17
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##  > http://blog.gentilkiwi.com/mimikatz
'## v #'  Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'  > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # lsadump::sam /system:SYSTEM /sam:SAM
Domain : JOHN-PC
SysKey : 97fd831aaa54840800ead7b16fc2413e
Local SID : S-1-5-21-806928618-3257427745-877340488

SAMKey : 1edbf838753ddf7adae5440d5a6ff2b1

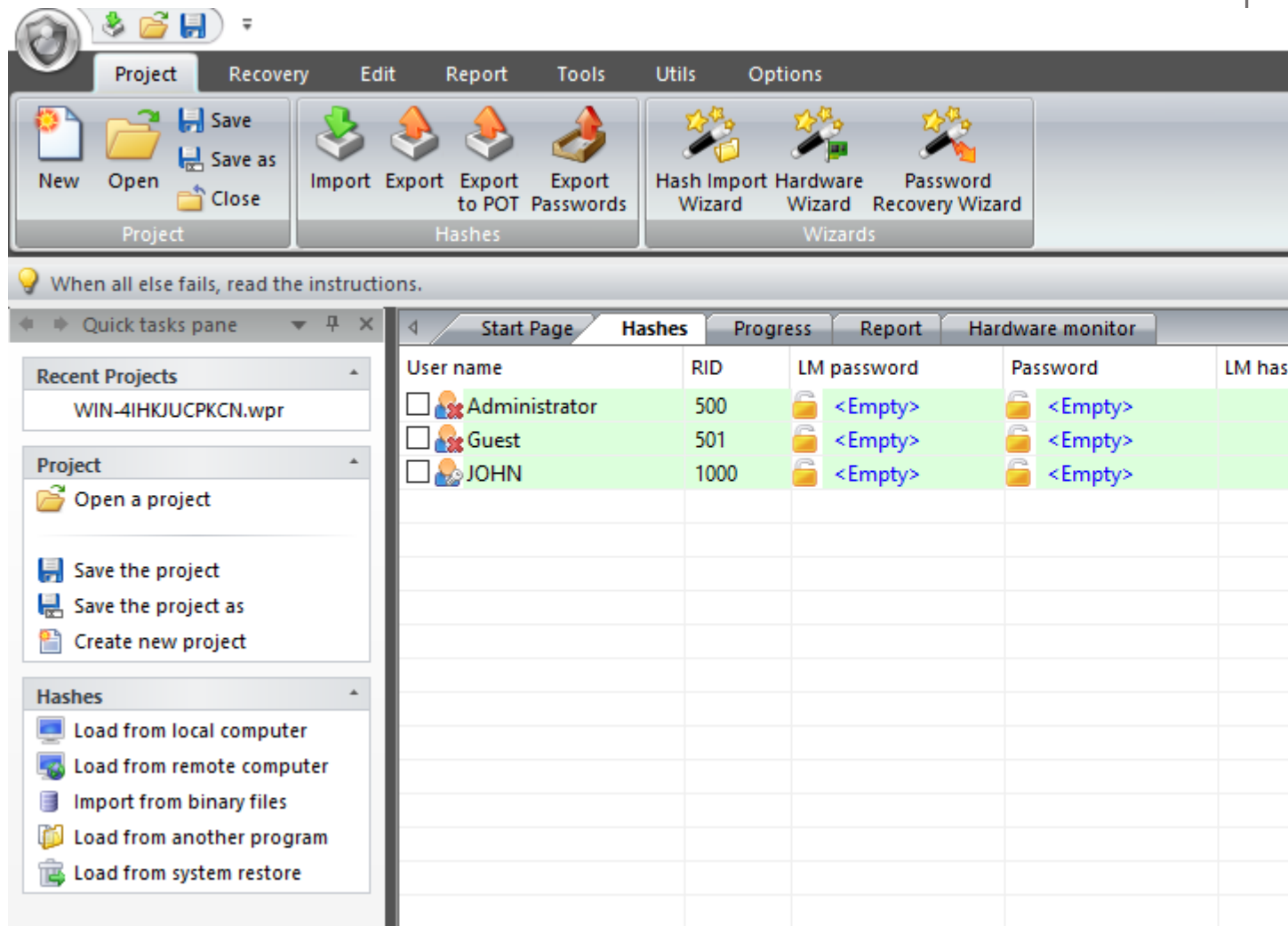
RID : 000001f4 (500)
User : Administrator
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

RID : 000001f5 (501)
User : Guest
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

RID : 000003e8 (1000)
User : JOHN
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

mimikatz #
```

Có thể thấy, hash NTLM của hai user Admin và JOHN là NULL , nên mình thử tool bình thường xem sao



Tool này cũng báo tương tự. Có vài teams đã giải được, nhưng bọn mình bó tay.

Extract cookies from Google Chrome browser

Chall này có một file dump, folder appdata . Lúc mở tool mimikatz ở chall trên thì mình có thấy nó có chức năng đọc dump, và có cái gì đó liên quan DPAPI, sau đó hint có nói về DPAPI nên mình mở thử.

Link mò được về read cookie:

<https://www.ired.team/offensive-security/credential-access-and-credential-dumping/reading-dpapi-encrypted-secrets-with-mimikatz-and-c++>


Thử luận nào:

<https://uit-jfm.github.io/>

dpapi::chrome /in:"D:\Downloads\mimikatz_trunk\x64\AppData\Local\Microsoft\Edge\User Data\Default\Cookies" /unprotect

```
File Select mimikatz 2.2.0 x64 (oe.eo)
Name : _efr
Dates : 7/29/2020 1:40:14 PM -> 7/29/2020 2:40:14 PM
ERROR kuhl_m_dpapi_chrome_decrypt ; No Alg and/or Key handle despite AES encryption
Host : vnexpress.net ( / )
Name : _tb_sess_r
Dates : 7/29/2020 1:40:18 PM -> 7/29/2020 2:10:18 PM
ERROR kuhl_m_dpapi_chrome_decrypt ; No Alg and/or Key handle despite AES encryption
Host : vnexpress.net ( / )
Name : _tb_t_ppg
Dates : 7/29/2020 1:40:23 PM -> 7/29/2020 2:10:23 PM
ERROR kuhl_m_dpapi_chrome_decrypt ; No Alg and/or Key handle despite AES encryption
Host : vnexpress.net ( / )
Name : adAsiaUserIp
Dates : 7/29/2020 1:40:17 PM -> 8/5/2020 1:40:17 PM
ERROR kuhl_m_dpapi_chrome_decrypt ; No Alg and/or Key handle despite AES encryption
Host : vnexpress.net ( / )
Name : trc_cookie_storage
Dates : 7/29/2020 1:40:20 PM -> 7/29/2021 1:40:24 PM
ERROR kuhl_m_dpapi_chrome_decrypt ; No Alg and/or Key handle despite AES encryption
Host : www.bing.com ( / )
Name : MUIDB
Dates : 7/29/2020 1:39:41 PM -> 8/23/2021 1:39:41 PM
ERROR kuhl_m_dpapi_chrome_decrypt ; No Alg and/or Key handle despite AES encryption
mimikatz #
```

À =))) Lí do mà có file dump là vì nó có key để giải mã. Load dump vào nào

 mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::dpapi
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 2807848 (00000000:002ad828)
Session           : Interactive from 2
User Name         : Alice
Domain           : DESKTOP-4D9UVLD
Logon Server      : DESKTOP-4D9UVLD
Logon Time        : 7/29/2020 11:51:15 AM
SID               : S-1-5-21-3734529546-3570587082-1750843553-1001
                  [00000000]
                  * GUID       : {b9820292-310b-4df7-8ff2-1a857a8f1ea5}
                  * Time       : 7/29/2020 1:37:53 PM
                  * MasterKey   : 56b63acd7e2e9004aac16e14322148e8a2a09e3041adb4aa421adb6fd8530f9b8c7
7bc40c5dffd4a4bdccb803a559a2fac9
                  * sha1(key)  : ed634a59b7bb4cca37009449d3ccacec9f073b6f

Authentication Id : 0 ; 2807819 (00000000:002ad80b)
Session           : Interactive from 2
User Name         : Alice
Domain           : DESKTOP-4D9UVLD
```

Giờ chạy lại lệnh trên và ctrl-f thôi

```
Select mimikatz 2.2.0 x64 (oe.eo)
Name : bsc
Dates : 7/29/2020 1:40:42 PM
* using BCrypt with AES-256-GCM
Cookie: fZ4E2LwUbk-Xt3RB2fR7ug

Host : beacon.walmart.com ( / )
Name : btc
Dates : 7/29/2020 1:40:42 PM -> 7/30/2030 1:40:42 AM
* using BCrypt with AES-256-GCM
Cookie: fZ4E2LwUbk-Xt3RB2fR7ug

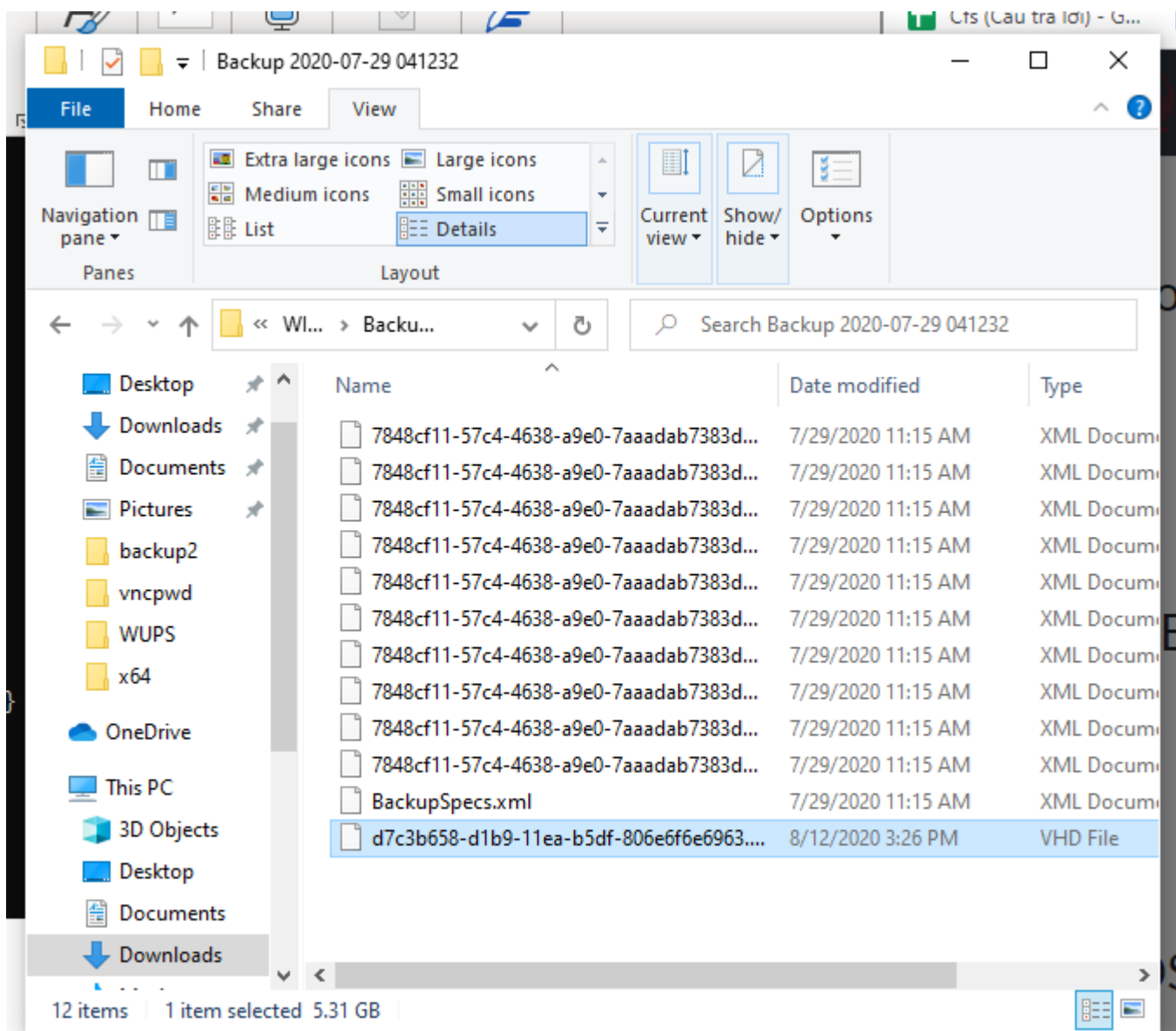
Host : bh.contextweb.com ( / )
Name : INGRESSCOOKIE
Dates : 7/29/2020 1:40:29 PM
* using BCrypt with AES-256-GCM
Cookie: c986591d06542acf

Host : cnsc.uit.edu.vn ( / )
Name : _Flag
Dates : 7/29/2020 1:41:59 PM -> 12/1/2020 7:00:00 AM
* using BCrypt with AES-256-GCM
Cookie: WannaGame{this_challenge_is_created_by_danhph}

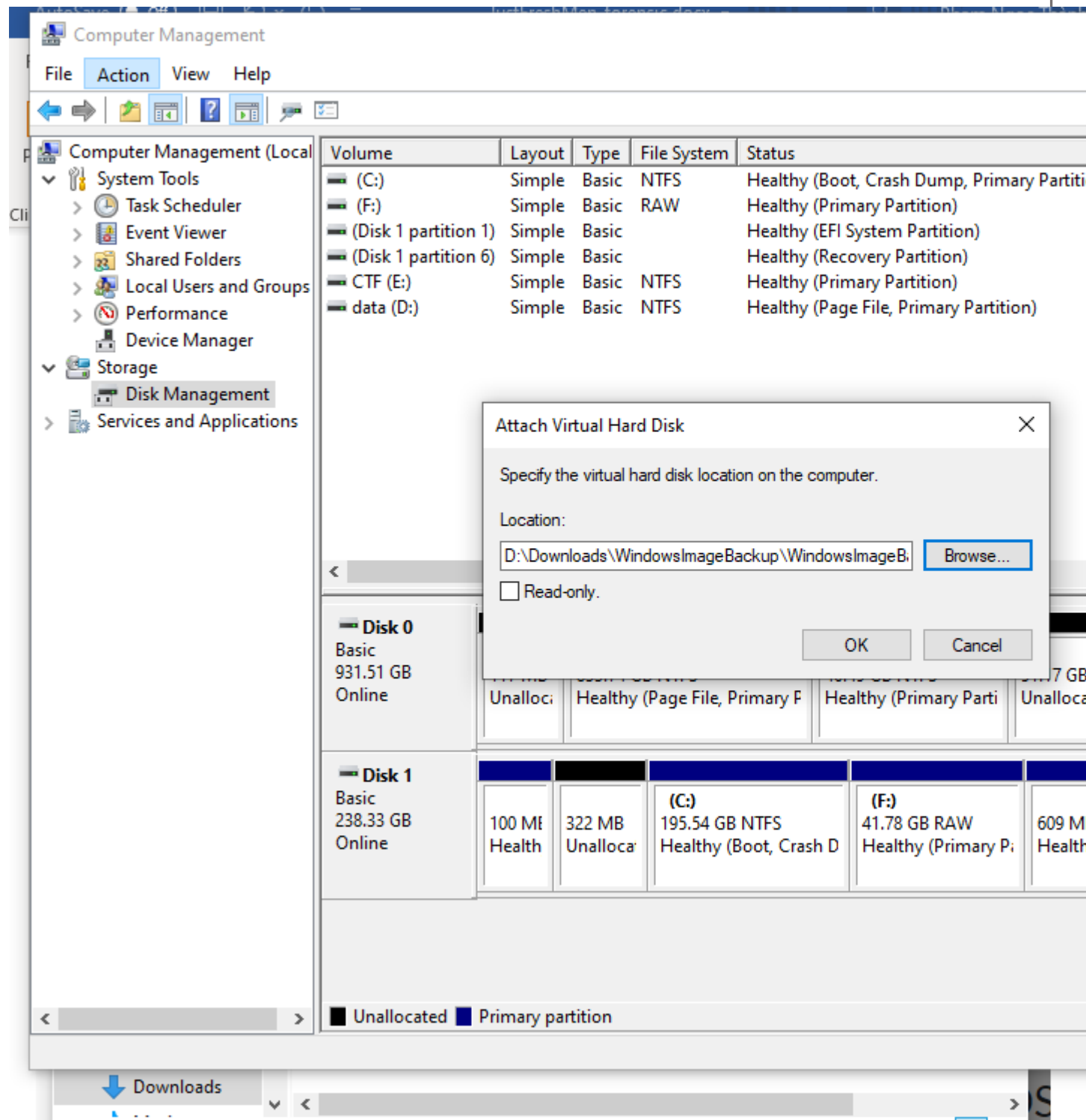
Host : e.serverbid.com ( / )
Name : azk
Dates : 7/29/2020 1:40:29 PM -> 7/29/2021 1:40:29 PM
* using BCrypt with AES-256-GCM
Cookie: ue1-sb1-f36042a8-3459-43e8-8144-adafda0f8836
```

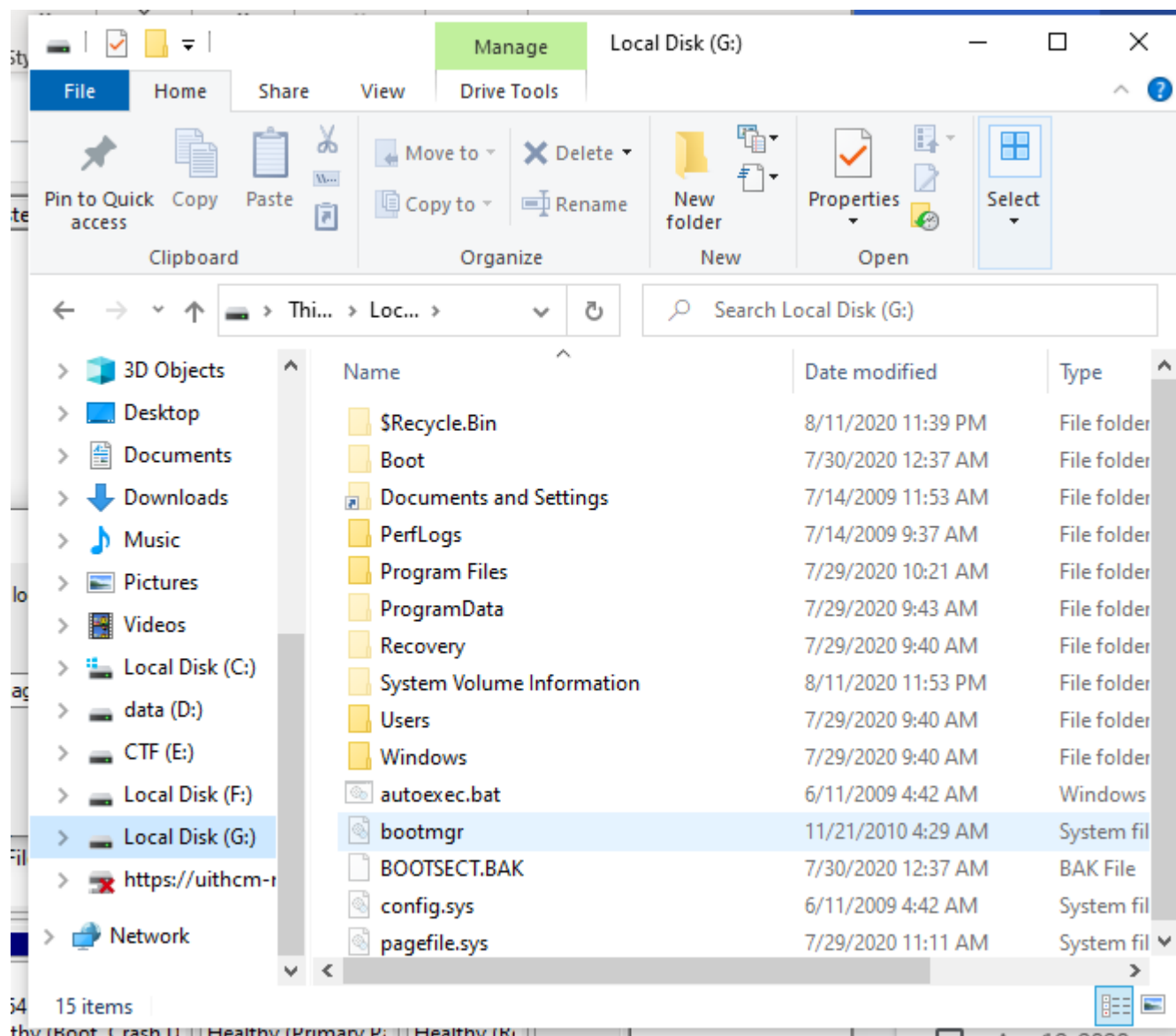
Backup Leaked #1: SoS

Ở chall này và chall 2, tụi mình được 1 file backup windows Giải nén ra thì có file VHD.



Mount file này vào nào

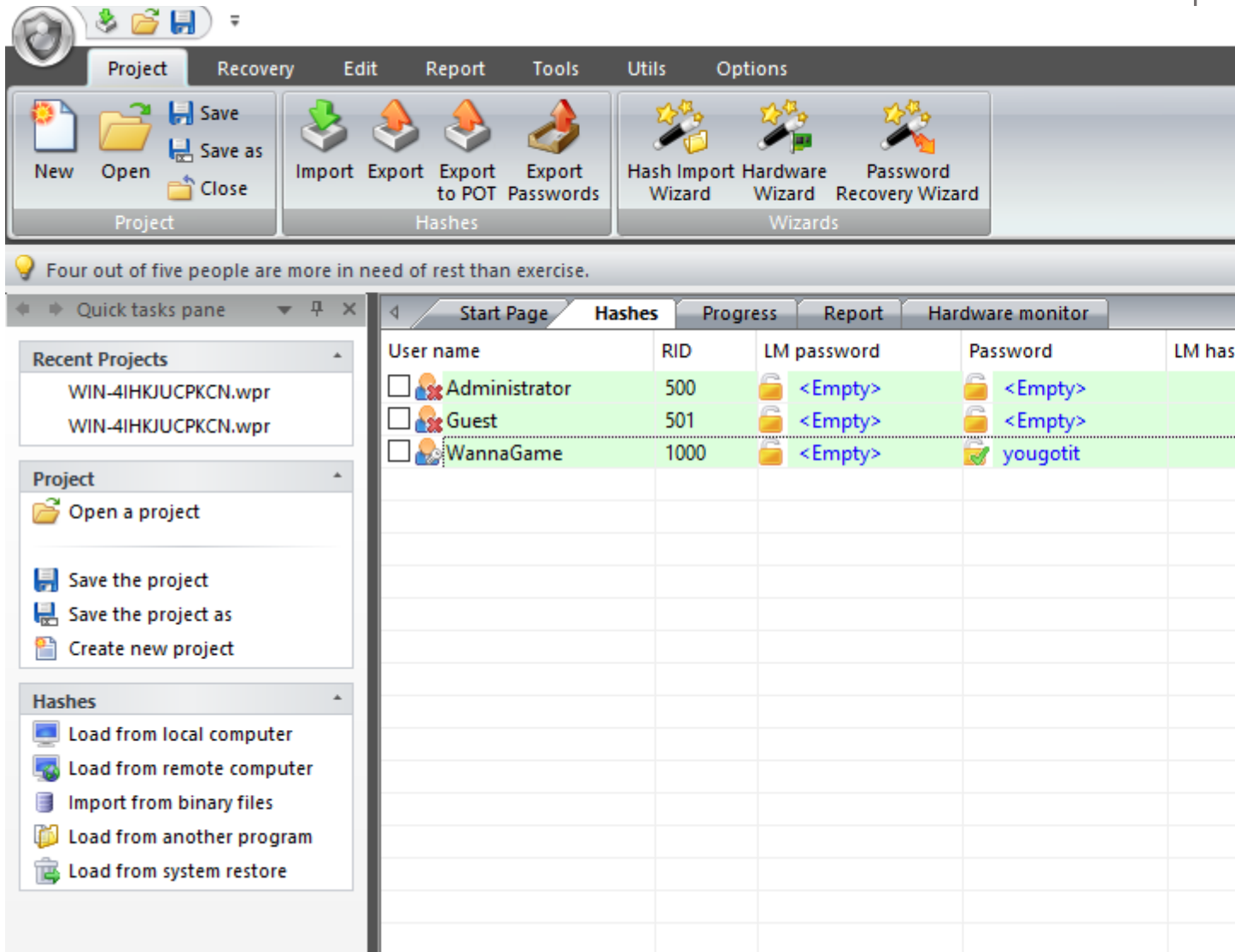




Đầu tiên, mình sẽ dùng tool **Autopsy**, một tool dùng để pháp chứng để check xem có file nào đáng nghi không.

[illegible]

Trong lúc đợi nó quét thì mình đi quét password



OK ==))) cái account này có password nè. Solve ra yougotit. Hash nó với SHA1 là OK

Backup Leaked #2: Beehive

<https://uit-jfm.github.io/>

Khi dùng tool autopsy, mình có thấy hint là “Do you believe that the service password that is saved on the server is encrypted securely”

Challenge

2 Solves

×

Backup Leaked #2: Beehive 200

Do you believe that the service password that is saved on the server is encrypted securely? **File** Flag format:
wannagame{SHA1(your_answer)} Author: **CNSC team**

Mình scan dùng Autopsy thì chỉ có app VNC là đáng nghi nhất

sac - Autopsy 4.15.0

Case View Tools Window Help

Add Data Source
 Images/Videos
 Communications
 Geolocation
 Timeline
 File Discovery
 Generate Report

←
→

- [-] Data Sources
 - [+] G:
- [-] Views
 - [+] File Types
 - [+] Deleted Files
 - [+] MB File Size
- [-] Results
 - [-] Extracted Content
 - EXIF Metadata (10)
 - Encryption Suspected (5)
 - Extension Mismatch Detected (3)
 - Installed Programs (18)
 - Operating System Information (2)
 - Operating System User Account (6)
 - Recent Documents (5)
 - Shell Bags (14)
 - USB Device Attached (7)
 - User Content Suspected (10)
 - Web Bookmarks (18)
 - Web History (1668)
 - Keyword Hits
 - [+] Single Literal Keyword Search (0)
 - [+] Single Regular Expression Search (0)
 - [+] Email Addresses (317)
 - [+] Hashset Hits
 - E-Mail Messages
 - Interesting Items
 - Accounts
 - [+] Tags
 - Reports

Listing
Installed Programs

Table
Thumbnail

Source File
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE
SOFTWARE

Hex
Text
Application
M

Result: 4
of 23

Type

Program Name

Date/Time

Source File Path

Artifact ID

Mình có biết rằng VNC store pass trên registry . Dùng tool để đọc pass là ra

MiTeC Windows Registry Recovery - [SOFTWARE]

File Options Explore Windows Help

SAM SYSTEM SOFTWARE

NAVIGATOR

- File Information
- Security Records
- SAM
- Windows Installation
- Hardware
- User Data
- Startup Applications
- Services and Drivers
- Network Configuration
- Windows Firewall Settings
- Environment
- Shell Folders
- Outlook Express
- Raw Data**

Value Type

Password	REG
SecurityTypes	REG
ReverseSecurityTypes	REG
UserPasswdVerifier	REG
QueryConnect	REG
QueryOnlyIfLoggedIn	REG
GuestAccess	REG
RSA_Private_Key	REG

Result panel

Key	Type	Value
-----	------	-------

Search trên mạng thì có tool tên vncpwd . Xài thử nào

```
Press RETURN to exit

PS D:\Downloads\vncpwd> ./vncpwd.exe 968e4d3e3f2e2493972ca46e9299a3

*VNC password decoder 0.2.1
by Luigi Aurieremma
e-mail: aluigi@autistici.org
web:    aluigi.org

- your input password seems in hex format (or longer than 8 chars)

Password:  h3llo_w4nn4g4m3

Press RETURN to exit
```

P/s: Khi làm, mình có thấy trong folder %temp%/VMWARE có những file phá pass này, nhưng k để ý lắm, tưởng là của vmware. Chắc là hint của BTC mà bị bỏ qua hihi