Team 16

19521671 Trần Hoàng Khang

Instruction file

No instruction file available.

Instruction

Username/Password: **root/1**

Team name (WannaOne)
tictoc_neverdie

Công cụ :

Ở đây mình sử dụng **Volatility 2,** ban đầu có một số bước mình demo với bản **standalone** cho Linux, sau đó mình có sử dụng plugin để hỗ trợ forensic nên mình chuyển sang bản **python source**

Lời giải :

Ta có file **dump.zip.** Giải nén ra:

```
ubuntu@ubuntu:~$ unzip dump.zip
Archive:  dump.zip
  inflating: dump.raw
ubuntu@ubuntu:~$ ls
dump.raw  dump.zip
```

Lấy thông tin cơ bản bằng **imageinfo** (chủ yếu lấy thông tin các **profile** :v)

```
./volatility_2.6_lin64_standalone  -f dump.raw --profile=Win7SP1x64
filescan | grep flag
```

```
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_standalone  dump.raw
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : You must specify something to do (try -h)
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_standalone  -f dump.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/ubuntu/volatility_2.6_lin64_standalone/dump.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029f2110L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800029f3d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2022-04-08 19:05:12 UTC+0000
     Image local date and time : 2022-04-08 12:05:12 -0700
```

Challenge 2.1 - dump.raw

“Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra: + Thu thập các file bất thường để ghép mảnh flag.”

Command:

```
./volatility_2.6_lin64_standalone  -f dump.raw --profile=Win7SP1x64 filescan | grep flag
```

```
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_standalone  -f dump.raw --profile=Win7SP1x64 filescan | grep flag
Volatility Foundation Volatility Framework 2.6
0x000000013fb0cf20     16      0 RW-r-- \Device\HarddiskVolume1\Users\TEMP\Desktop\flag.txt.txt
0x000000013fc30070     16      0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\Desktop\flag.txt
0x000000013fc45350     16      0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk
0x000000013ff104b0     16      0 RW-rw- \Device\HarddiskVolume1\Users\TEMP\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk
```

Dump file này tại địa chỉ **0x000000013fc30070** và đọc file :

```
./volatility_2.6_lin64_standalone  -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000013fc30070 -D .
```

```
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_standalone  -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000013fc30070 -D .
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x13fc30070   None   \Device\HarddiskVolume1\Users\NHK-InsecLab\Desktop\flag.txt
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ ls
AUTHORS.txt  CREDITS.txt  dump.raw  file.None.0xfffffa8003f10350.dat  LEGAL.txt  LICENSE.txt  README.txt  resultDump  volatility_2.6_lin64_standalone
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ cat file.None.0xfffffa8003f10350.dat
inseclab{w3lcom3_t0ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ ^C
```

Flag’s segment: **inseclab{w3lcom3_t0**

Dump dữ liệu duyệt web thử:

```
GitHub        5     0 2022-04-08 18:51:33.934445        N/A
    11 https://github.com/goliate/hidden-tear/tree/master/hidden-tear                hidden-tear/hidden-tear/hidden-tear at master · goliate/hidden-tear ·
GitHub        4     0 2022-04-08 18:51:35.373730        N/A
    10 https://github.com/goliate/hidden-tear                                        GitHub - goliate/hidden-tear: ransomware open-sources
               2     0 2022-04-08 18:51:13.252715        N/A
     8 https://pastebin.com/k2HuWZmp                                                 https://drive.google.com/file/d/1TxvMNb...RWjD7wZc/view?usp=shari - Pa
stebin.com      1     0 2022-04-08 18:46:46.246539        N/A
     3 https://www.win-rar.com/download.html?&L=0                                    WinRAR download free and support: WinRAR Download Latest Version
               1     0 2022-04-08 18:05:17.080333        N/A
     2 https://www.win-rar.com/download.html                                         WinRAR download free and support: WinRAR Download Latest Version
               1     0 2022-04-08 18:05:17.080333        N/A
```

Ở đây ta thấy có user có tải phần mềm WinRAR về, có thể là cho mục đích giải nén file rar gì đó (chỉ đoán thôi)

```
ubuntu@ubuntu:~/volatility$ python vol.py  -f /home/ubuntu/dump.raw --profile=Win7SP1x64 filescan | grep -E "\.rar"
```

```
Volatility Foundation Volatility Framework 2.6.1
0x00000000071f3a10     16      0 RW----
\Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
0x000000013feb7f20     16      0 R--rwd
\Device\HarddiskVolume1\Users\NHK-
InsecLab\AppData\Roaming\Microsoft\Windows\Recent\fl4g.rar.lnk
```

```
ubuntu@ubuntu:~/volatility$ python vol.py  -f /home/ubuntu/dump.raw --profile=Win7SP1x64 filescan | grep -E "\.rar"
Volatility Foundation Volatility Framework 2.6.1
0x00000000071f3a10     16      0 RW---- \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
0x000000013feb7f20     16      0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\fl4g.rar.lnk
```

Dump file này ra tại địa chỉ **0x00000000071f3a10.**

```
python vol.py  -f /home/ubuntu/dump.raw --profile=Win7SP1x64 dumpfiles -
Q 0x00000000071f3a10 -D resultDump/
```

Kiểm tra file dump được đúng signature không:

```
ubuntu@ubuntu:~/volatility/resultDump$ file
file.None.0xfffffa8003d61f10.dat
file.None.0xfffffa8003d61f10.dat: RAR archive data, vd, os: MS-DOS
```

Yes. Đúng là file RAR, đổi lại tên file thành hidden.rar cho đẹp. Chúng ta dùng unrar để extract file thì bị đòi mật khẩu

```
ubuntu@ubuntu:~$ unrar e ~/volatility/resultDump/hidden.rar

UNRAR 5.30 beta 2 freeware      Copyright (c) 1993-2015 Alexander Roshal


Extracting from /home/ubuntu/volatility/resultDump/hidden.rar

Enter password (will not be echoed) for h4lf-fl4g.txt:

Extracting  h4lf-fl4g.txt
The specified password is incorrect.
Total errors: 2
```

Lên mạng search “crack rar password file” thì thấy suggest dùng tool **rar2john** để lấy hash password file RAR trong bộ tool “John The Ripper”. Cài toàn bộ tool tất tần tật của “họ nhà John” [tại đây]

Cài đặt line-by-line và cd vào thư mục **~/src/john/run** :

```
./rar2john ~/volatility/resultDump/hidden.rar > ~/volatility/resultDump/hidden.txt
```

Có hash **hidden.txt**

Hash password rar có dạng như này:

```
ubuntu@ubuntu:~$ cat ~/volatility/resultDump/hashedpass.txt
```

```
hidden.rar:$rar5$16$7a3f367e550900d03550fdaaa0937470$15$6cff83d489ca5fef8
c6ae8fc7abd4168$8$2948156db3e079b9
```

Sau đó dùng john để crack này, lưu ý rar có 2 version là RAR3 thì dùng **--format=rar**, trường hợp này là RAR5 thì dùng **--format=RAR5 .** Sử dụng wordlist [rockyou.txt]

```
./john --wordlist=rockyou.txt --format=RAR5 ~/volatility/resultDump/hashedpass.txt
```

```
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 128/128 SSE2 4x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:18 0.01% (ETA: 2022-04-19 12:43) 0g/s 133.1p/s 133.1c/s 133.1C/s leonel..778899
0g 0:00:00:23 0.02% (ETA: 2022-04-19 12:47) 0g/s 134.3p/s 134.3c/s 134.3C/s marita..candycane
0g 0:00:00:27 0.02% (ETA: 2022-04-19 12:22) 0g/s 135.7p/s 135.7c/s 135.7C/s doggy..misael
r0cky0u          (hidden.rar)
1g 0:00:01:58 DONE (2022-04-18 00:32) 0.008431g/s 127.3p/s 127.3c/s 127.3C/s rangga..love2dance
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Mật khẩu file là **r0cky0u**. Giải nén file với mật khẩu này ta được file h4lf-fl4g.txt. Đọc file này ra ta có flag:

Flag's segment**: _th3_w0rld_NHK}**

Flag: inseclab{w3lcom3_t0_th3_w0rld_NHK}

Challenge 2.2 - dump.raw

"Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra: + Liệu họ có để lại những dấu vết trên trình duyệt web?."

Dùng một số plugin mở rộng tại: [superponible/volatility-plugins: Plugins I've written for Volatility (github.com)]

Trong đó có hỗ trợ "chiết xuất" thông tin từ history browser trên *chrome, firefox, …*

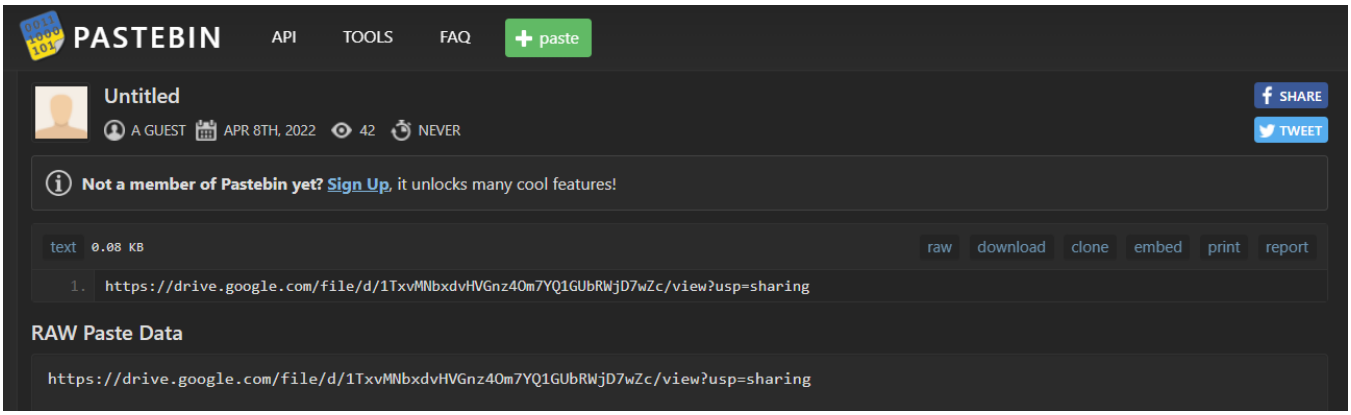
Command:

```
python vol.py --plugins=volatility-plugins/ -f /home/ubuntu/dump.raw --
profile=Win7SP1x64 chromehistory
```

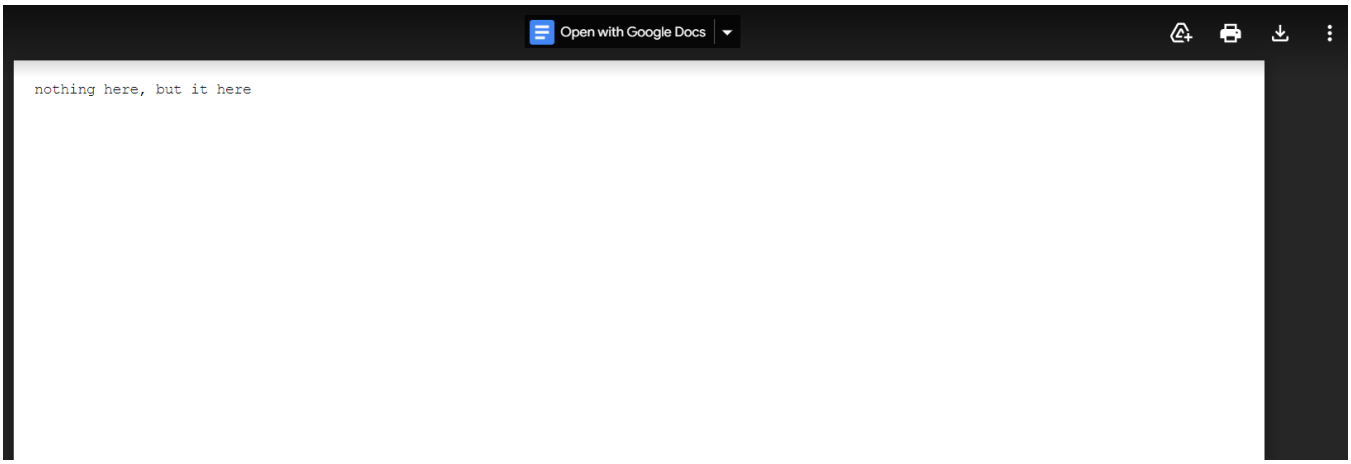
Output (để ý đoạn cuối)

```
    14 https://github.com/goliate/hidden-tear/...ster/hidden-tear/hidden-
tear/bin/Debug hidden-tear/hidden-tear/hidden-tear/bin...aster · goliate/hidden-tear
· GitHub      2     0 2022-04-08 18:51:33.424394        N/A
    13 https://github.com/goliate/hidden-tear/...ter/hidden-tear/hidden-
tear/Properties hidden-tear/hidden-tear/hidden-tear/Pro...aster · goliate/hidden-
tear
· GitHub      2     0 2022-04-08 18:51:21.710010        N/A
    12 https://github.com/goliate/hidden-tear/tree/master/hidden-tear/hidden-tear
hidden-tear/hidden-tear/hidden-tear at master · goliate/hidden-tear ·
GitHub        5     0 2022-04-08 18:51:33.934445        N/A
    11 https://github.com/goliate/hidden-tear/tree/master/hidden-tear
hidden-tear/hidden-tear/hidden-tear at master · goliate/hidden-tear ·
GitHub        4     0 2022-04-08 18:51:35.373730        N/A
    10 https://github.com/goliate/hidden-tear
GitHub - goliate/hidden-tear: ransomware open-sources
               2     0 2022-04-08 18:51:13.252715        N/A
     8 https://pastebin.com/k2HuWZmp
https://drive.google.com/file/d/1TxvMNb...RWjD7wZc/view?usp=shari - Pa
stebin.com      1     0 2022-04-08 18:46:46.246539        N/A
     3 https://www.win-rar.com/download.html?&L=0
WinRAR download free and support: WinRAR Download Latest Version
               1     0 2022-04-08 18:05:17.080333        N/A
     2 https://www.win-rar.com/download.html
WinRAR download free and support: WinRAR Download Latest Version
               1     0 2022-04-08 18:05:17.080333        N/A
```

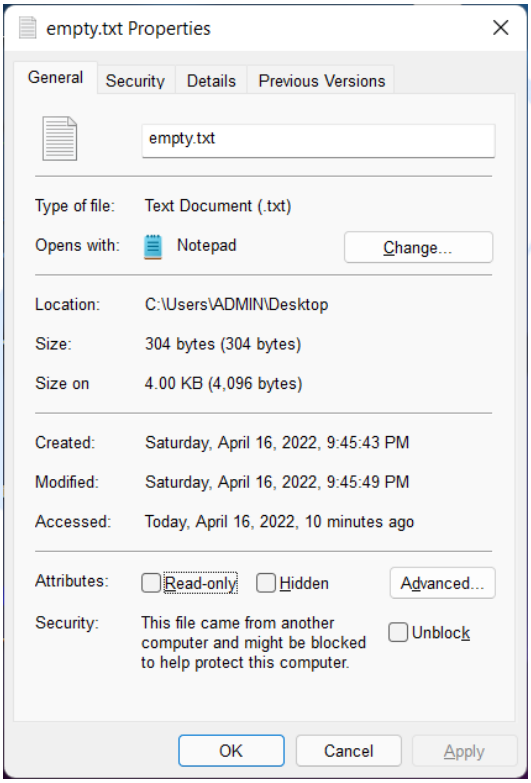
Truy cập vào đường dẫn https://pastebin.com/k2HuWZmp.



Tại đây **PASTEBIN** lưu một đường dẫn khác. Truy cập vào đường dẫn trên https://drive.google.com/file/d/1TxvMNbxdvHVGnz4Om7YQ1GUbRWjD7wZc/view?usp=sharing



Một file text với message **“nothing here, but it here”.** Có lẽ đây là hint của một loại *steganography* đang được giấu trong đây. Kiểm tra sơ bộ thông tin:



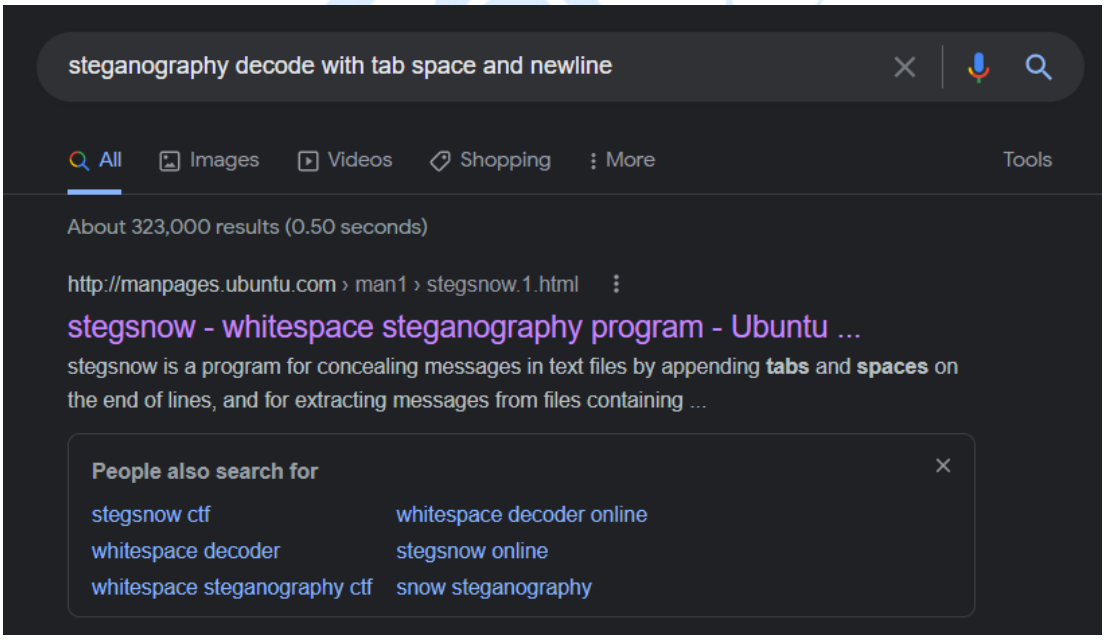
File có mấy chữ mà size tới **304** bytes thì “ảo thuật” luôn. Quẳng đại vào **HxD** xem file raw có chứa flag ẩn không (bỏ thẳng luôn cũng được khỏi phân tích file size, vì mình hơi nghi ngờ thôi :-P) :

empty.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   6E 6F 74 68 69 6E 67 20 68 65 72 65 2C 20 62 75  nothing here, bu
00000010   74 20 69 74 20 68 65 72 65 09 20 20 20 20 09 20  t it here.    .
00000020   09 20 20 09 09 20 20 20 09 20 20 20 20 20 20 0A  . ..   .      .
00000030   20 20 20 20 20 20 20 09 20 20 20 20 09 20 20 20        .    .
00000040   20 20 20 09 20 20 09 20 09 20 09 20 20 20 09 20     .  . . .   .
00000050   09 20 20 20 20 20 20 20 09 20 0A 20 20 20 20 09  .       . .    .
00000060   09 09 20 20 09 09 20 20 20 09 20 20 20 20 20 20  ..  ..   .
00000070   20 09 20 20 20 20 20 09 20 20 20 20 20 20 20 09   .     .       .
00000080   20 20 20 20 20 20 20 0A 20 20 20 20 09 20 20 20         .    .
00000090   20 20 09 20 09 20 20 09 20 09 20 20 20 09 20 20    . .  . .   .
000000A0   20 20 09 20 20 20 20 20 09 20 20 20 20 20 20 20    .      .
000000B0   09 20 20 20 20 20 20 20 0A 09 09 20 20 20 20 09  .       ...    .
000000C0   20 20 09 20 20 20 20 20 09 20 20 20 20 09 20 20    .     .    .
000000D0   09 20 20 20 20 20 09 20 20 20 20 20 09 20 20 20  .     .     .
000000E0   20 20 20 20 0A 20 20 20 20 20 20 20 20 09 20 20      .       .
000000F0   20 09 20 20 09 20 09 20 20 20 20 20 20 20 09 20   .  . .       .
00000100   09 20 20 20 20 20 09 20 20 20 20 20 09 20 20 20  .     .    .
00000110   20 09 20 20 20 0A 20 20 20 20 20 09 20 20 20 20   .   .     .
00000120   09 20 20 20 09 20 20 20 20 20 20 20 09 20 20 0A  .   .       .  .
```

Trong file chứa message và có "hiện tượng lạ ở đây". Các ký tự *"không đọc được" (dấu chấm)* được phân cách khá lạ, để ý kỹ thì đoạn sau chỉ có các byte như **09(tab**) → parse thành ký tự **".", 20(space**) → khoảng trắng, **0A(new line – xuống dòng**) → ký tự "."

Search Google với các từ khóa tương tự, vì mình newbie có hiểu cái này là gì đâu (@-@)

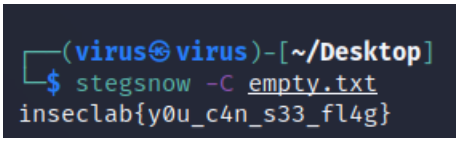


Được đề xuất dùng **stegsnow**, có sẵn trong gói package của linux. Tham khảo thêm công cụ tại đây. Tool này vừa có tác dụng reveal và cả hide message. Đọc *manual* sẽ biết rõ:

```
OPTIONS
       -C     Compress the data if concealing, or uncompress it if extracting.
```

Command:

```
stegsnow -C empty.txt
```



Flag: inseclab{y0u_c4n_s33_fl4g}

Challenge 2.3 - dump.raw

“Dường như đã có hành vi bất thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra: + Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK. Hãy tìm password đó.”

Lấy mật khẩu thì basic rồi, thường thì mình crack **NTML** hash của user thôi. Xem thông tin registry bằng **hivelist**:

```
python vol.py  -f /home/ubuntu/dump.raw --profile=Win7SP1x64 hivelist
```

```
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a0012a6010 0x000000009e18b010 \??\C:\Users\sshd_server\ntuser.dat
0xfffff8a0012bb270 0x000000004829e270 \??\C:\Users\sshd_server\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0017f4010 0x0000000019cda010 \??\C:\Users\TEMP\ntuser.dat
0xfffff8a001882410 0x0000000021a41410 \??\C:\Users\TEMP\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0032eb010 0x000000011ff7a010 \??\C:\Windows\AppCompat\Programs\Amcache.hve
0xfffff8a00484c010 0x00000000a8ca5010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a004ecd010 0x00000000529bb010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a004ed7010 0x0000000052913010 \SystemRoot\System32\Config\SAM
0xfffff8a00000e010 0x00000000a9537010 [no name]
0xfffff8a000024010 0x00000000a9742010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a000063010 0x00000000a9683010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0005dc010 0x0000000054799010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0005e6010 0x0000000013a00010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000e2b010 0x00000000a4cc8010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a000e61010 0x000000000dc00010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000ef1010 0x000000004b8d9010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
```

Trích xuất hash bằng hashdump tại địa chỉ ảo từ **0xfffff8a000024010** (\REGISTRY\MACHINE\SYSTEM) đến **0xfffff8a004ed7010** (\SystemRoot\System32\Config\SAM)

```
python vol.py  -f /home/ubuntu/dump.raw --profile=Win7SP1x64 hashdump -y
0xfffff8a000024010 -s 0xfffff8a004ed7010
```

```
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
NHK-InsecLab:1000:aad3b435b51404eeaad3b435b51404ee:141be588e38b145c4e1f274b646898eb:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cfc061c3359db455d00ec27035:::
```

Cố gắng crack mã hash của NHK-InsecLab 141be588e38b145c4e1f274b646898eb bằng [CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc.] và dùng cả "John Đù Ripper" nhưng không được. Bắt đầu thấy khoai rồi đó

Cố dùng plugin xịn hơn là **lsadump** để dump ra password hoặc LSA secret key, …

```
python vol.py  -f /home/ubuntu/dump.raw --profile=Win7SP1x64 lsadump
```

```
Volatility Foundation Volatility Framework 2.6.1
NL$KM
0x00000000  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   @...............
0x00000010  ef 8e 01 77 ad a5 85 29 da 7c 46 c4 d1 5b a7 d4   ...w...).|F..[..
0x00000020  10 38 2d d7 b5 84 7d 93 45 5d 7b e7 28 5f e9 c1   .8-...}.E]{.(_..
0x00000030  fe be 9e 6a 42 d8 a5 6b 47 99 30 67 fc a7 5c 6c   ...jB..kG.0g..\l
0x00000040  49 ea 4c 1e 2b 89 21 56 a2 33 01 bd e6 71 fa 4d   I.L.+.!V.3...q.M
0x00000050  90 36 4c e1 5f a5 29 5a 13 12 08 90 4d 7c 15 67   .6L._.)Z....M|.g

DefaultPassword
0x00000000  12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  50 00 61 00 73 00 73 00 77 00 30 00 72 00 64 00   P.a.s.s.w.0.r.d.
0x00000020  21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   !...............

_SC_OpenSSHd
0x00000000  14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  44 00 40 00 72 00 6a 00 33 00 33 00 6c 00 31 00   D.@.r.j.3.3.l.1.
0x00000020  6e 00 67 00 00 00 00 00 00 00 00 00 00 00 00 00   n.g.............

DPAPI_SYSTEM
0x00000000  2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ,...............
0x00000010  01 00 00 00 4a b5 78 3e 9b 1a 62 d6 52 08 75 86   ....J.x>..b.R.u.
0x00000020  13 a2 3b 36 3c 96 ad 6e 74 1e 31 1d bf e1 89 85   ..;6<..nt.1.....
0x00000030  49 ac 51 cf ca 28 97 2d 8d c6 a4 b6 00 00 00 00   I.Q..(.-........
```

Vẫn không có được **password** của *NHK*. Này hơi căng rồi, nhưng không sao. Hồi chơi mấy giải CTF mình có biết một tool là **Mimikatz** giúp lấy được **password**, một trong những cách để nó retrieve là tiến trình lsass.exe phải tồn tại trong file dump. Mình kiểm tra bằng **pslist** thì thấy có tiến trình này:

```
python vol.py  -f /home/ubuntu/dump.raw --profile=Win7SP1x64 pslist
```

```
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8003c71b10 System                    4      0     91      546 ------      0 2022-04-08 17:44:21 UTC+0000
0xfffffa8005334620 smss.exe                264      4      2       29 ------      0 2022-04-08 17:44:21 UTC+0000
0xfffffa800584d060 csrss.exe               340    332      9      502      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa800cdfc570 wininit.exe             392    332      3       76      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa800bdfa880 csrss.exe               404    384     16      279      1      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a1cb10 services.exe            456    392      7      223      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a276f0 lsass.exe               464    392      7      598      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a1f750 lsm.exe                 472    392      9      157      0      0 2022-04-08 17:44:22 UTC+0000
0xfffffa8005a248f0 winlogon.exe            496    384      3      110      1      0 2022-04-08 17:44:22 UTC+0000
```

Khá thuận tiện. Giờ mình download plugin tại: [community/FrancescoPicasso at master · volatilityfoundation/community (github.com)]

Khi chạy cần thư viện Construct, python2 của server chưa có thư viện này. Cài với pip thì lỗi nhiều do conflict phiên bản. Tham khảo Google với từ khóa “install construct in python2.7 “ và tham khảo tại link [How to install python2.7-construct ubuntu package on Ubuntu 20.04/Ubuntu 18.04/Ubuntu 19.04/Ubuntu 16.04 (zoomadmin.com)], Ta cài với lệnh

```
sudo apt-get install -y python2.7-construct
```

Chạy **mimikatz** để extract password

```
python vol.py --plugins=/home/ubuntu/community/FrancescoPicasso/ -f
/home/ubuntu/dump.raw --profile=Win7SP1x64 mimikatz
```

```
ubuntu@ubuntu:~/volatility$ python vol.py --plugins=/home/ubuntu/commu
Volatility Foundation Volatility Framework 2.6.1
Module   User             Domain           Password
-------- ---------------- ---------------- ----------------------------
wdigest  NHK-InsecLab     IEWIN7           AntiNHK
wdigest  sshd_server      IEWIN7           D@rj33l1ng
wdigest  IEWIN7$          WORKGROUP
```

Flag: inseclab{AntiNHK}

Challenge 1 - memory.dmp

“Có một command chứa thông báo lạ trong bash history, liệu bạn có thể khôi phục thông báo đó? Bạn phải xây dựng volatility và tìm profile.”

Ta có file **dump.zip.** Giải nén ra

Dùng **imageinfo** để lấy thông tin về image (bao gồm cả *profile*)

```
./volatility_2.6_lin64_standalone -f ../memory.dmp imageinfo
```

```
ubuntu@ubuntu:~$ cd volatility_2.6_lin64_standalone/
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$ ./volatility_2.6_lin64_standalone -f ../memory.dmp imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : No suggestion (Instantiated with no profile)
                     AS Layer1 : LimeAddressSpace (Unnamed AS)
                     AS Layer2 : FileAddressSpace (/home/ubuntu/memory.dmp)
                      PAE type : No PAE
ubuntu@ubuntu:~/volatility_2.6_lin64_standalone$
```

Trong file image chưa có **profile**. Vậy ta sẽ build cái mới:

- Xác Định OS (Hệ Điều Hành)

```
ubuntu@ubuntu:~$ strings memory.dmp | grep -i 'Linux version' | uniq
Linux version 4.15.0-112-generic (buildd@lcy01-amd64-021) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.12)) #113~16.04.1-Ubuntu SMP Fri Jul 10 04:37:08 UTC 2020 (Ubuntu 4.15.0-112.113~16.04.1-generic 4.15.18)
```

Các bước build:

Search với từ khóa “linux memory build profile” . Link tham khảo: build profile

Bước 1: Tải image và header với phiên bản chính xác của kernel trong file dump được xác định ở trên:

```
sudo apt install linux-image-4.15.0-112-generic linux-headers-4.15.0-112-generic
```

Sau đó khởi động lại và kernel sẽ được upgrade lên:

```
reboot
```

```
ubuntu@ubuntu:~$ uname -r
4.15.0-112-generic
ubuntu@ubuntu:~$
```

Bước 2: Tải các gói dependencies cần thiết cho việc cài đặt và tạo Profile:

NOTE: Tìm profile mặc định trong repo của Volatility Foundation nhưng không có kernel trùng khớp

```
sudo apt install build-essential dwarfdump
```

Clone repo và cài đặt gói theo volatility chính hãng :

```
git clone https://github.com/volatilityfoundation/volatility.git
cd volatility/tools/linux
make
sudo chown -R ubuntu /boot/System.map-4.15.0-112-generic
cd ~/
```

```
zip Ubuntu_4.15.0-112-generic.zip volatility/tools/linux/module.dwarf
/boot/System.map-4.15.0-112-generic
```

Bước 3: Đến đoạn này là mình đã có profile dưới dạng zip. Mình xóa repo cũ đi, tải lại cái mới và copy file zip trong output trên đưa vào path **volatility/volatility/plugins/overlays/linux/**

```
rm -rf volatility
git clone https://github.com/volatilityfoundation/volatility.git
cp Ubuntu_4.15.0-112-generic.zip volatility/volatility/plugins/overlays/linux/
```

Bước 4: Kiểm tra các profile hiện hành, xác nhận có profile vừa tạo hay chưa:

```
python volatility/vol.py --info | grep Linux
```

Profile được tạo thành công:

```
ubuntu@ubuntu:~$ python volatility/vol.py --info | grep Linux
Volatility Foundation Volatility Framework 2.6.1
LinuxUbuntu_4_15_0-112-genericx64 - A Profile for Linux Ubuntu_4.15.0-112-generic x64
linux_aslr_shift            - Automatically detect the Linux ASLR shift
linux_banner                - Prints the Linux banner information
linux_yarascan              - A shell in the Linux memory image
LinuxAMD64PagedMemory           - Linux-specific AMD 64-bit address space.
```

Profile có tên là **LinuxUbuntu_4_15_0-112-genericx64.** Sử dụng cái này để thao tác với file dump. Mình đã xong đoạn cài đặt profile theo hint (bài này chỉ dẫn khá rõ) và bây giờ mình xử lý đoạn “command chứa thông báo lạ trong bash history”. Mình xem thử lịch sử command , dùng **consoles** plugin cho chi tiết.

- Thử dùng **consoles** hay **cmdline** đều không được, profile này không hỗ trợ. Ta xem lại các lệnh khả dụng đối với profile này. Dùng lệnh trên nhưng không sử dụng **grep**

```
python volatility/vol.py --info
```

Xem các lệnh bắt đầu bằng chuỗi “linux”:

```
limeinfo                    - Dump Lime file format information
linux_apihooks              - Checks for userland apihooks
linux_arp                   - Print the ARP table
linux_aslr_shift            - Automatically detect the Linux ASLR shift
linux_banner                - Prints the Linux banner information
linux_bash                  - Recover bash history from bash process memory
linux_bash_env              - Recover a process' dynamic environment variables
linux_bash_hash             - Recover bash hash table from bash process memory
```

Có plugin **linux_bash** hợp hoàn toàn với yêu cầu đề luôn. Sử dụng thử xem:

```
ubuntu@ubuntu:~/volatility$ python vol.py -f ../memory.dmp --profile=LinuxUbuntu_4_15_0-112-genericx64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
    5775 bash                 2022-04-10 18:13:58 UTC+0000   uname -r
    5775 bash                 2022-04-10 18:13:58 UTC+0000   echo "aW5zZWNsYWJ7dzNsYzBtM190MF9MMW51WF9tM20wcllfZjByM25zMWM1fQ==" >> Un33dt0r3@dth1s.txt
    5775 bash                 2022-04-10 18:13:58 UTC+0000   ls
    5775 bash                 2022-04-10 18:14:05 UTC+0000   chmod 755 avml
    5775 bash                 2022-04-10 18:14:08 UTC+0000   ./avml
    5775 bash                 2022-04-10 18:14:20 UTC+0000   sudo ./avml memory.dmp
```

Ta thấy có dòng lệnh khả nghi đưa dữ liệu vào file **Un33dt0r3@dth1s.txt** (nhìn là thấy giống flag format rồi)

Ta decode **base64** với chuỗi trên.

```
ubuntu@ubuntu:~/volatility$ echo "aW5zZWNsYWJ7dzNsYzBtM190MF9MMW51WF9tM20wcllfZjByM25zMWM1fQ==" | base64 -d
```

```
inseclab{w3lc0m3_t0_L1nuX_m3m0rY_f0r3ns1c5}ubuntu@ubuntu:~/volatility$
```

Flag: inseclab{w3lc0m3_t0_L1nuX_m3m0rY_f0r3ns1c5}