



# WRITEUP WHITEHAT 11 CTF

**Biên soạn: Đỗ Minh Long**

*26/06/2022*

## 1. Thông tin

Thông tin chi tiết về chương trình:

- Thời gian: Từ 15h00 ngày 20/06/2022 đến 15h00 ngày 27/06/2022
- Hình thức thi: Online CTF - Jeopardy tại <https://wargame.whitehat.vn>




Lĩnh vực tham gia: *Forensics (Tổng số lượng challenge: 06)*

Thông tin tài khoản tham gia:

- Username: *thegun*
- Thông điệp: *CmodC\_T2SumGr*

THÔNG TIN TÀI KHOẢN



Chọn ảnh

Tên tài khoản:

thegun

Quốc gia:

Viet Nam

Điểm:

2432

Xếp hạng:

27

Email:

anhits.hufi@gmail.com

Thông điệp:

CmodC\_T2SumGr

Đổi mật khẩu

## 2. Challenge 1

- Tên Challenge: for06-Beginner forensics (32 points)
- Thông tin đề: When I open this file in notepad, it looks very chaotic. Do you know what file it is?
- Download file:  
<https://drive.google.com/file/d/151mSsV5WKXq751UHAauTOx7Czfxkyqkt/view?usp=sharing>
- Bài này dành cho beginner nên cũng không có gì khó lắm, kiểm tra thông tin file cái đã 😊)

```
kali@kali: ~/Desktop/whitehat11/for06
File Actions Edit View Help

(kali@kali)-[~/Desktop/whitehat11/for06]
$ file for06-Beginner\ forensics.txt
for06-Beginner forensics.txt: PNG image data, 900 x 500, 8-bit/color RGBA, non-interlaced
```

- Nhận thấy đây là file hình ảnh nhưng bị đổi extension → ta đổi extension về đúng extension ban đầu và được kết quả 😊)



- Flag: WhiteHat{SummEr\_1s\_4\_st3te\_of\_m1nd}

## 3. Challenge 2

- Tên Challenge: for05-Corrupt (64 points)
- Thông tin đề: It seems that this file is corrupt. Pls fix it for me!
- Download file:  
[https://drive.google.com/file/d/1wLzWf7fYHtHpozSCQKoA\\_CBBwC7X6mT/view?usp=sharing](https://drive.google.com/file/d/1wLzWf7fYHtHpozSCQKoA_CBBwC7X6mT/view?usp=sharing)

- Cũng tương tự bước đầu ở challenge đầu tiên, ta cũng kiểm tra file, tuy nhiên file này đúng extension hùmmm

```
kali@kali: ~/Desktop/whitehat11/for5
File Actions Edit View Help

(kali@kali)-[~/Desktop/whitehat11/for5]
$ file for05-Corrupt.png
for05-Corrupt.png: SoftQuad DESC or font file binary - version 10303

(kali@kali)-[~/Desktop/whitehat11/for5]
$
```

- Mặc dù đúng extension nhưng header file png này lại sai.

```
$ xxd for05-Corrupt.png | head -n 40
00000000: aaaa 3f28 292f 3920 3b7b 6310 0b79 1c67  .?()/9 ;{c..y.g
00000010: 2b0c 261c 0b18 3b7d 7f0b 2867 3b3d 6332  +.&... ;}..(g;=c2
00000020: a041 4141 4141 4141 4141 4141 4141 4189  .AAAAAAAAAAAAA.
00000030: 706e 670d 1a0a 1a00 0000 0d49 4844 5200  png.....IHDR.
00000040: 0001 0300 0001 0308 0600 0000 31d1 61cb  .....1.a.
00000050: 0000 0001 7352 4742 00ae ce1c e900 0000  ....sRGB.....
00000060: 0467 414d 4100 00b1 8f0b fc61 0500 0000  .gAMA.....a....
00000070: 0970 4859 7300 000e c400 000e c401 952b  .pHYs.....+
00000080: 0e1b 0000 05cf 4944 4154 785e eddd d18e  ....IDATx^....
00000090: 23b7 1140 d1dd fcf7 3f3b ce85 1f3d 4452  #..@....?;...=DR
000000a0: 9e62 5a3d e700 86fd 2235 d92d 5cd0 5bd0  .bZ=...."5.-\.[.
000000b0: eaf7 1f7f fa05 fc78 fffa ebd0 c00f 2706  ....x.....'
000000c0: 40c4 0088 1800 1103 2062 0044 0c80 8801  @..... b.D....
000000d0: 1031 0022 0640 c400 8818 0011 0320 1ff7  .1."@..... ..
```

- Tra lại format của file png, ta sửa lại header theo format sau

**File header** [\[edit\]](#)

A PNG file starts with an 8-byte [signature](#)<sup>[13]</sup> (refer to hex editor image on the right):

Values (hex)	Purpose
89	Has the high bit set to detect transmission systems that do not support 8-bit data and to reduce the chance that a text file is mistakenly interpreted as a PNG, or vice versa.
50 4E 47	In ASCII, the letters PNG, allowing a person to identify the format easily if it is viewed in a text editor.
0D 0A	A DOS-style line ending (CRLF) to detect DOS/Unix line ending conversion of the data.
1A	A byte that stops display of the file under DOS when the command type has been used—the end-of-file character.
0A	A Unix-style line ending (LF) to detect Unix-DOS line ending conversion.

- Sau khi sửa lại sẽ trông như sau:

```
$ xxd for05-Corrupt.png | head -n 40
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG.....IHDR
00000010: 0000 0103 0000 0103 0806 0000 0031 d161  .....1.a
00000020: cb00 0000 0173 5247 4200 aece 1ce9 0000  ....sRGB.....
00000030: 0004 6741 4d41 0000 b18f 0bfc 6105 0000  ..gAMA.....a...
00000040: 0009 7048 5973 0000 0ec4 0000 0ec4 0195  ..pHYs.....
00000050: 2b0e 1b00 0005 cf49 4441 5478 5eed ddd1  +.....IDATx^...
00000060: 8e23 b711 40d1 ddfc ff3f 3bce 851f 3d44  .#..@....?;...=D
00000070: 529e 625a 3de7 0086 fd22 35d9 2d5c d05b  R.bZ=...."5.-\.[
00000080: d0ea f71f 7ffa 05fc 78ff faeb dfc0 0f27  ....x.....'
00000090: 0640 c400 8818 0011 0320 6200 440c 8088  .@..... b.D...
```

- Sau khi sửa header thì ta nhận dc file như bên dưới, tuy nhiên ta vẫn chưa lấy được flag, do file bị miss:



- Sau khi dùng kỹ thuật khôi phục lại mã QR thì ta nhận dc flag;  
WhiteHat{4a5y\_W4rmup\_ch4lleng3\_f0r\_SUMMER\_RACEEEE}

#### 4. Challenge 3

- Tên challenge: for04-CSIRT (64 point)
- Thông tin đề: Client's company has a mole, he opned the port for this accomplices to steal data. A document sent is encrypted and we don't have the password. At the momment, we have caught the insider but no password. He only admitted haved compressed the file and created password around 21:25-21:35 on April 24th, 2022 ICT Time. Can you help me? We have iocs.
- Download file: <https://drive.google.com/file/d/1FDN8sGy-2nGAe8CF2YYB77idCPA5W4OG/view?usp=sharing>

- Bài này thì ban tổ chức cho ta một file pcap lưu lượng mạng

1572	2022-04-24	14:41:44.753342	91.189.91.39	192.168.17.129	HTTP	415	HTTP/1.1	200	OK	(application/x-debian-package)
1559	2022-04-24	14:41:44.512654	192.168.17.129	91.189.91.39	HTTP	243	GET	/ubuntu/pool/main/c/cyrus-sasl2/libsasl2-modules-c		
1557	2022-04-24	14:41:44.489206	91.189.91.39	192.168.17.129	HTTP	771	HTTP/1.1	200	OK	(application/x-debian-package)
1729	2022-04-24	14:41:31.020128	192.168.17.129	192.168.17.1	HTTP	738	HTTP/1.0	200	OK	(application/zip)
1724	2022-04-24	14:41:31.016975	192.168.17.1	192.168.17.129	HTTP	542	GET	/insider.zip	HTTP/1.1	
1392	2022-04-24	14:41:21.427787	192.168.17.129	192.168.17.1	HTTP	460	HTTP/1.0	200	OK	(text/plain)
1386	2022-04-24	14:41:21.424824	192.168.17.1	192.168.17.129	HTTP	546	GET	/gen_password.py	HTTP/1.1	
1282	2022-04-24	14:41:17.777626	192.168.17.129	192.168.17.1	HTTP	453	HTTP/1.0	200	OK	(text/html)
1279	2022-04-24	14:41:17.776071	192.168.17.1	192.168.17.129	HTTP	493	GET	/	HTTP/1.1	
1359	2022-04-24	14:41:12.083463	192.168.17.129	192.168.17.1	HTTP	523	HTTP/1.0	404	File not found	(text/html)
1356	2022-04-24	14:41:12.080659	192.168.17.1	192.168.17.129	HTTP	505	GET	/password.txt	HTTP/1.1	

Time 14789: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface \Device\NPF\_{96AF9599-C54C-43BE-888D-92967B49712A}, id 0

- Sau khi kiểm tra, thì ta phát hiện, nội gián đã tải file insider.zip, và gen\_password.py về máy. Tiến hành trích xuất file dựa trên lưu lượng mạng. Tuy nhiên ta không có



password để giải nén file insider.zip, thật may mắn ta biết dc thuật toán mà nội gián sử dụng để đặt passwd.

```
1 import random
2 import hashlib
3 import datetime
4
5
6 def gen_Pass(key):
7     password = ''
8     password = hashlib.md5(str(key).encode())
9     password = password.hexdigest()
10    password += '-'
11    password += 'bjAwYg=='
12    return password
13
14 if __name__ == '__main__':
15     seed_ = int(datetime.datetime.utcnow().timestamp())
16     random.seed(seed_)
17     key = random.randint(1,1000000000)
18     password = gen_Pass(key)
19     print('Password:', password)
20
```

- Okay ta viết ngược lại thuật toán của nó, và tiến hành giải nén thôi 😊)

```
1 import random
2 import hashlib
3 import datetime
4
5 def gen_Pass(key):
6     password = ''
7     password = hashlib.md5(str(key).encode())
8     password = password.hexdigest()
9     password += '-'
10    password += 'bjAwYg=='
11    return password
12
13 if __name__ == '__main__':
14     fileout=open("passwd.txt","a")
15     start = datetime.datetime(2022, 4, 24, 14, 25, 0, 0).timestamp()
16
17     end = datetime.datetime(2022, 4, 24, 14, 35, 0, 0).timestamp()
18
19     for seed_ in range(int(start),int(end)):
20         print(random.seed(seed_))
21         key = random.randint(1,1000000000)
22         print(key)
23         password = gen_Pass(key)
24         print('Password:', password)
25         fileout.write(password+"\n")
26     fileout.close()
27
```

- Okay, run nó và tiến hành crack passwd thì ta dc thông tin sau:

insider.zip/insider/database.txt:b8126bb646aa957307685a4216a46b23-  
bjAwYg==:insider/database.txt:insider.zip:insider.zip  
insider.zip/insider/flag.txt:b8126bb646aa957307685a4216a46b23-  
bjAwYg==:insider/flag.txt:insider.zip:insider.zip

- Giải nén file và nhận flag thôi 😊)

- Flag: WhiteHat{start\_again\_https://www.youtube.com/watch?v=O0StKIRHVeE}

- Tên challenge: for03-S1mple Obfuscation (256 points)
- Thông tin đề: The flag has 2 parts. Part 2 has been encode and saved somewhere. Can you find it?
- Download file: <https://drive.google.com/file/d/1ZmWZiTTqL62wjZvhgcZabrt59W-Mq7uQ/view?usp=sharing>
- Password: wargame

- Nhìn tên challenge thì ta dễ dàng đoán được đây là file office có chứa malicious code được viết bằng macro. Vậy thì trích xuất đoạn macro xem thử 😊 )

```
LineCont 0x001C 03 00 00 05 00 00 00 00 00 00 09 00 00 0B 00 00 00 00 00 00 0F
LitStr 0x03E0 "PowerShell.exe -WindowStyle Hidden -no -ENCOD JABFGACUGBJADKJAGyBgAGnQBTA
AnAE44z03C80AVB1AG0wJwArACcAAnLAcSjwBVhAHIAyQByCAcKwAnAHKAgBwAgWzACnAcKcAfJAmACAAKAgACQcAC
AnWw0A0F0AKwAKHAHAcwbTAE8ABQBFAFsAmw0A0F0AKwAnAFgAJwApAdSajABHAeWASAB0AGUAMABVAFIAbwB0ACAAPQAgACgAf
DEALALxADAADANAASADEAMAA4CwAnWwAzACwAnAyAcWc0A0AyACwAMQAwADQALASADCAQ7ACQARwBGdGAgVBQZHAHYA9B3AE
ACIAeAw0A0H0Aewz4H0AewAyAH0Aewz4H0Aeww1AHOAewAxH0AewAwH0AeGA0Ck07ACQARwAGwAB0AAGEAB0B1ACCLAAAnA
gB1ACALAAAFIAJwJasACwZAAwAnACJwB0FAAnWwBFACALAAAnG0AJwAdASCSAQ5AGTJwApAcKcAIAGcAQ0AcgB1AFATAT
ADAB0D4C4JwJasAF5ASQwBTAGEAUgbdADMAngApAhWzJgAgCgAKAnAGUASACnADAT1AFYQAQByAEK4Q0QBCEwZ0QAgACkBgTAE0AQ
E4YQBNAEUAWwAzACwAMQAxAcwMgBdAC0AagBPAEKATgACwAnACKQ7ACQARwBMAEGATgB1ADAAYQBSAG8AaAgAgACsAPQAgACg
ADKDLALAAxADAMAAwASAdKAOAASADUAMAAASAdgAOQASADEAMAAZACwAMQAwADAAALAA3ADEALAAxADAADANAASADEAMAA4CwAnWwAz
QAwACwAMQAwADUALAA4ADKAL"
LitStr 0x03B1 "AA4ADACADQ7ACQARwBMAEGATgB1ADAAYQBSAG8AaAgAgACsAPQAOADKAOQASADEAMAAZACwAnWwAz
3ADQALAAxADAADANAASAdKAAwASAdCmGASADEAMGAgACwAMQAwADAAALAA3ADEALAAxADAADANAASADEAMAA4CwAnWwAz
AnWwAzACwAMQAwADTALAA4ADKALAA4ADCLAAAXADTIAAMASADEEMAAyACwAQOQ3ACwAnWwAxACwAnWwAzACkAOwAKAEUwZ0AOHC
GKATIAACG4ACAAKAAOAcADJwArAFMAJwArACcAVwB4AHTAawB1AGQATIAAnACsJwBwZHGATIA0AGMAyQAnACsJwBkACsAKwAnAH
SACAAZGB4C0AcKwAnAHIAJwArACcAZwB4HQJwArACcATIA0A0HgAJwArACcAdwAGHQAeAHQeAHYAJwArACcAYwBhAGQAYwBj
AB0AGkAEAB0ACsJwBwBUCFAJwArACcAIQAnACsJwAhACEAdABYcCAcKwAnAFMALGBSAGUAJwArACcAUAAAnACsJwBwSEEEYw
ADJwArAFMAAEAB0AHIAJwArACcAUwASACkAnAnAHQcAGBTADA0ABAFYAFMAKQACwKwAnAFIAJwArACcAZQAnACsJwBwBQAGw
ACkAWAnAHIAJwArACcAUwAnACsJwBjGAGEJwArACcADZAD0ACkAWAnAHIAUwASAHQcAGCwKwAnACsJwBTAGEADAnACsJwByAF
NACKAIIAGcAC0cGB1AHAATbAHnEMARAgAcCdABYAFMAJwASAFsAQwBIAEEcGbdADMAOQAPACAAfAAGAC4ATA"
Concat
```

- Đúng như dự đoán, vậy ta chỉ cần giải hết đoạn malicious code này thôi 😊))
- Mớ hỗn độn trên là base64 → decode base64 ta sẽ ra đoạn code mà hacker sử dụng như sau:

[illegible]

- Nhận thấy hacker sử dụng kỹ thuật Obfuscation code, nhìn có vẻ căng đây 😊), nhưng không sao 😊))



- Okay flag: Whitehat{hustl3 h4rd hustl3 r3al hard}

## 6. Challenge 05

- Tên challenge: for02-Think DFIRently
- Thông tin đề: We need your help to investigate a suspected computer, can you answer the following questions?
- Yêu cầu để tìm các thông tin sau:
  1. How many times has the user turned on their default browser and when was the last time it was launched from the taskbar?  
\*Format: X\_DDMMYYYY-HH:MM:SS (X is an integer, no time conversion needed)
  2. What is the ID,hostname connected by remote access tool?  
\*Format: 111222444\_hostname
  3. What version does the messaging app use?
- Download file:  
<https://drive.google.com/file/d/1VgsksoWPSz6OA2dMvLn9q07SD5FugDzi/view?usp=sharing>

- Đối với bài Memory forensics này ta sử dụng volatility để giải.
- Đầu tiên, lấy thông tin default browser bằng cách dump registry:  
"Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice".

```
Values:
REG_SZ      Progid      : (S) FirefoxURL
```

[+] Default Browser: Firefox.

- Số lần mở default browser dưới taskbar và lần cuối cùng
- + Mở ở phía taskbar:

```
REG_BINARY  %APPDATA%\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Mozilla Firefox.lnk :
Count:      3
Focus Count: 0
Time Focused: 0:00:00.503000
Last updated: 2022-04-12 07:14:55 UTC+0000
```

+ Mở bình thường ngoài Desktop

```
REG_BINARY  C:\Users\Public\Desktop\Mozilla Firefox.lnk :
Count:      4
Focus Count: 0
Time Focused: 0:00:00.504000
Last updated: 2022-04-12 07:16:12 UTC+0000
Raw Data:
```

[+] Tổng số lần mở Firefox (Default Browser): 7 lần.  
[+] Lần cuối cùng mở: 2022-04-12 07:14:55



- What is the ID,hostname connected by remote access tool?

Bước này ta chưa biết thông tin ứng dụng Remote Access là gì, xác định nó cái đã 😊)

```
$ vol -i 10102.raw pstree | grep -i Teamviewer
Volatility Foundation Volatility Framework 2.6
.. 0xfffffa8003527990:TeamViewer_Ser      1452    500    23    390 2022-04-12 07:12:59 UTC+0000
WARNING : volatility.debug      : PID 888 PPID 3068 has already been seen
WARNING : volatility.debug      : PID 2708 PPID 3068 has already been seen
. 0xfffffa8001f75760:TeamViewer.exe      3840    2864    0    2022-04-12 07:13:46 UTC+0000
```

- Okay là Teamview, vậy thì dễ rồi 😊), phân tích log của nó ta phát hiện

```
(kali@kali)-[~/Desktop/whitehat11/10102]
$ strings Teamviewer15 Logfile.Log1 | grep "CreateClassicSession::Start:"
2022/04/12 14:14:08.974 1452 1500 S0 CreateClassicSession::Start: RequestRoute request BCommand: RequestRouteRequestDataControlID=
edRemoteAccessType=0 ClientType=TV TargetId=282087703 PartnerBuddyId=0 RAApiData=0000000000000000 RAApiKey=00000000-0000-0000-0000-000
ff204d56f186db612c0d8bc244e99b38000c29e99b3895d8ad0157492ec4dd1096b2607fe135<~~~~~0dd0c5b4e712d7cef7750d93b
dRouter: TerminalServerUserId:0 SourceId:361820239 DisplayName:WIN-QK3QHP1566V SmartAccessData Access=0 Account=0 TargetBuddy=0 Paswwo
000000000000 SessionId=0 LicenseCode= SupportsLimiter=1 CBFeatures=[UseCaseCB_MVP]
2022/04/12 14:14:31.692 1452 1500 S0 CreateClassicSession::Start: RequestRoute request BCommand: RequestRouteRequestDataControlID=
edRemoteAccessType=0 ClientType=TV TargetId=282087703 PartnerBuddyId=0 RAApiData=0000000000000000 RAApiKey=00000000-0000-0000-0000-000
ff204d56f186db612c0d8bc244e99b38000c29e99b3895d8ad0157492ec4dd1096b2607fe135<~~~~~0dd0c5b4e712d7cef7750d93b
dRouter: TerminalServerUserId:0 SourceId:361820239 DisplayName:WIN-QK3QHP1566V SmartAccessData Access=0 Account=0 TargetBuddy=0 Paswwo
000000000000 SessionId=0 LicenseCode= SupportsLimiter=1 CBFeatures=[UseCaseCB_MVP]

CPersistentParticipantManager::AddParticipant: [361820239,923252946] type=6 name=WIN-QK3QHP1566V
CPersistentParticipantManager::AddParticipant: [282087703,-1269226870] type=3 name=longnte
CPersistentParticipantManager::AddParticipant: [361820239,923252946] type=6 name=WIN-QK3QHP1566V
SessionStateParticipants::AddParticipant: pid: [361820239,923252946] and timestamp: 1649747681107
SessionStateParticipants::AddParticipant: pid: [282087703,-1269226870] and timestamp: 1649747681439
```

[+] ID: 282087703

[+] Hostname: longnte

- What version does the messaging app use?

```
data\Local\Programs\Zalo\Zalo-21.2.1\Zalo.exe
data\Local\Programs\Zalo\Zalo-21.2.1\locales\en-US.pak
data\Local\Programs\Zalo\Zalo-21.2.1\resources\app.asar
data\Local\Programs\Zalo\Zalo-21.2.1\resources\app.asar
data\Local\Programs\Zalo\Zalo-21.2.1\chrome_100_percent.p
data\Local\Programs\Zalo\Zalo-21.2.1\chrome_200_percent.p
data\Local\Programs\Zalo\Zalo-21.2.1\v8_context_snapshot.
data\Local\Programs\Zalo\Zalo-21.2.1\resources.pak
```

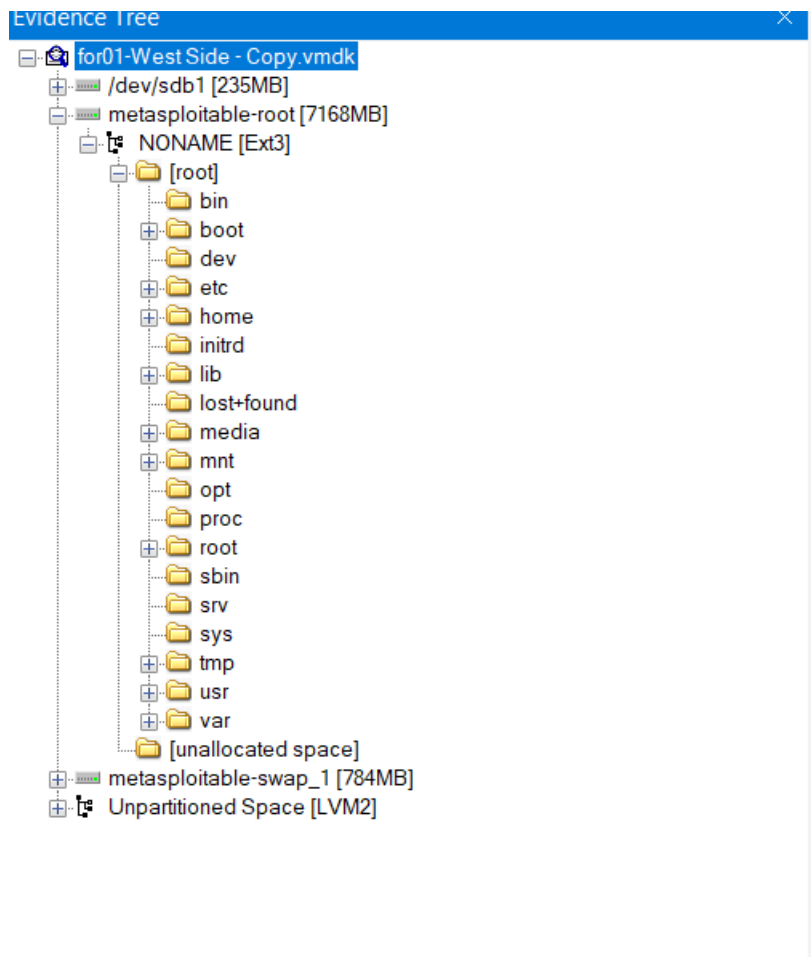
App chat được sử dụng là Zalo.

[+] Version: 21.2.1

⇒ Flag: WhiteHat{7\_12042022-07:14:55\_282087703\_longnte\_21.2.1}

## 7. Challenge 06

- Tên challenge: for01-West Side (128 points)
- Thông tin đề: We are investigating a person who often creates phishing websites. This is his virtual machine. Please help us
- Download file:  
[https://drive.google.com/file/d/1GV87Cood6h7ne0x\\_PJ4ljKuchRI35MuG/view?usp=sharing](https://drive.google.com/file/d/1GV87Cood6h7ne0x_PJ4ljKuchRI35MuG/view?usp=sharing)
- Đây là một bài về OS Forensics. Đánh giá sơ bộ về challenge này thì ta được cung cấp 1 disk của tội phạm, nhưng đã bị tội phạm format và delete các paratition nhân gây khó dễ trong quá trình forensics. Tuy nhiên ta tên tội phạm đã không clear được hết chứng cứ, nên ta có thể dễ dàng khôi phục lại các paratition trên disk, cũng như các file dữ liệu trên đó.



- Sau một thời gian đọc log và dựng lại máy của tội phạm vô ích, ta chợt phát hiện flag nằm trong /var/www
- Flag: WhiteHat{Mu4\_h3\_s0i\_d0n9}

