

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**  
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

-----o0o-----



**BÁO CÁO NỘI DUNG 4**  
**XÂY DỰNG LAB THỰC HÀNH**  
**FORMAT64\_3 – Nhóm 08**

Môn học: Chuyên đề an toàn phần mềm

Giảng viên: ThS. Ninh Thị Thu Trang

Thành viên: Phạm Thị Thu Hương – B19DCAT098

Đỗ Đức Quốc Anh – B19DCAT003

Đoàn Việt Hưng – B19DCAT094

Bùi Thanh Phong – B19DCAT135

**Hà Nội - 2023**

## MỤC LỤC

MỤC LỤC .....	1
DANH MỤC CÁC HÌNH VẼ VÀ BẢNG.....	2
I. Nội dung và hướng dẫn thực hiện bài thực hành.....	3
1. Mục đích.....	3
2. Yêu cầu đối với sinh viên.....	3
3. Nội dung thực hành .....	3
II. Phân tích, thiết kế bài thực hành .....	4
1. Phân tích yêu cầu bài thực hành.....	4
2. Thiết kế bài thực hành .....	5
III. Cài đặt và cấu hình các máy ảo .....	7
IV. Thử nghiệm lab và kết quả .....	13
V. Triển khai bài lab.....	13
TÀI LIỆU THAM KHẢO .....	14

## DANH MỤC CÁC HÌNH VẼ VÀ BẢNG

Hình 1. Sơ đồ thiết kế bài thực hành .....	5
Hình 2. Kết quả chấm điểm.....	7
Hình 3. Tạo lab với tên format64_3 .....	7
Hình 4. Tạo container attacker .....	8
Hình 5. Tạo container server .....	9
Hình 6. Tạo container ghidra .....	10
Hình 7. Tạo mạng mới cho lab .....	11
Hình 8. Cài đặt service binary tại port 1810.....	12
Hình 9. Chỉnh sửa file treataslocal trên máy attacker .....	12
Hình 10. Cài đặt chấm điểm tự động.....	12
Hình 11. build lab và chạy bài lab .....	12
Hình 12. Run lab và thực hiện check work trước khi thực hiện bài lab.....	13
Hình 13. Thực hiện bài lab sau đó check work .....	13
Hình 14. Đẩy bài lab lên git.....	13
Hình 15. Các images của vùng chứa được đẩy lên DockerHub.....	14
Hình 16. Tạo file Imodule tra chứa bài thực hành .....	14

## **I. Nội dung và hướng dẫn thực hiện bài thực hành**

### **1. Mục đích**

- Giúp sinh viên hiểu về lỗ hổng bảo mật format string thông qua việc thực hiện tấn công dịch vụ chứa lỗi.

### **2. Yêu cầu đối với sinh viên**

- Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách chủ
- Có kiến thức cơ bản về ngôn ngữ assembly và C/C++
- Có kiến thức cơ bản về lỗ hổng bảo mật format string
- Lý thuyết về calling convention
- Lý thuyết về thanh ghi

### **3. Nội dung thực hành**

- Khởi động bài lab: `labtainer -r ptit-format64_3`

#### **a. Trigger bug**

*Mục đích: Tìm được index trỏ đến đầu buffer*

##### **Các bước thực hiện:**

- Thực hiện debug tiến trình:
- Tiến hành tạo một khối với nội dung chứa chuỗi format string
- In ra khối đó để trigger bug
- Output sẽ in ra giá trị trên stack
- Tìm phần tử %p tương ứng khi thấy bắt đầu có sự lặp lại các giá trị in ra

#### **b. Find free\_hook**

*Mục đích: Tìm được địa chỉ hàm free\_hook*

##### **Các bước thực hiện:**

Mở lại tiến trình debug:

- Thực hiện chạy lệnh in địa chỉ để in ra địa chỉ của \_\_free\_hook
- Lưu địa chỉ này lại để tính offset của \_\_free\_hook so với libc base

#### **c. Find system**

*Mục đích: Tìm được địa chỉ hàm system*

##### **Các bước thực hiện:**

- Thực hiện chạy lệnh in địa chỉ để in ra địa chỉ của system
- Lưu địa chỉ này lại để tính offset của system so với libc base

#### **d. VM MAP**

*Mục đích: Tìm được offset của địa chỉ leak, offset system và offset free\_hook*

##### **Các bước thực hiện:**

- Tại cửa sổ đang debug thực hiện câu lệnh vmmap để in ra thông tin phân vùng bộ nhớ
- Địa chỉ ở cột start tại dòng đầu tiên trỏ tới libc là địa chỉ base của libc
- Tính địa chỉ offset của system và free\_hook bằng cách lấy 2 địa chỉ ở trên tìm được sau đó trừ đi địa chỉ libc\_base

#### **e. Overwrite**

*Mục đích: Tìm được param thích hợp để tấn công*

##### **Các bước thực hiện:**

- Gõ stack và ấn enter thêm vài lần để hiện thêm thông tin của stack:
- Tìm ô địa chỉ sao cho ô địa chỉ đó chứa giá trị là một danh sách liên kết đơn có ít nhất 2 node
- Địa chỉ của ô đó và địa chỉ của ô mà nó chứa là 2 địa chỉ cần
- Xác định 2 ô địa chỉ đó là phần tử %p thứ bao nhiêu 2 số đó sẽ lần lượt là param1 và param2

#### **f. Secret**

*Mục đích: Tìm được nội dung flag được giấu trên server*

##### **Các bước thực hiện:**

- Thay đổi payload để thực hiện tấn công lên server
- Đọc file secret sau đó copy chuỗi số bí mật:
- Thoát khỏi chương trình sau đó submit flag tại cửa sổ terminal của attacker
  - o echo “flag <secret number>”

## **II. Phân tích, thiết kế bài thực hành**

### **1. Phân tích yêu cầu bài thực hành**

Bài thực hành cần có ba máy tính, trong đó có hai máy tính nằm trong cùng mạng LAN, một máy tính đóng vai trò là công cụ hỗ trợ. Cụ thể như sau, trong mạng LAN gồm có 2 máy, máy attacker là nơi mà sinh viên sẽ tương tác chủ yếu nhằm khai thác thành công binary, máy server sẽ chạy service là binary mà sinh viên cần khai thác, máy ảo còn lại là công cụ hỗ trợ decompile file binary. Để hoàn thành bài thực hành, sinh

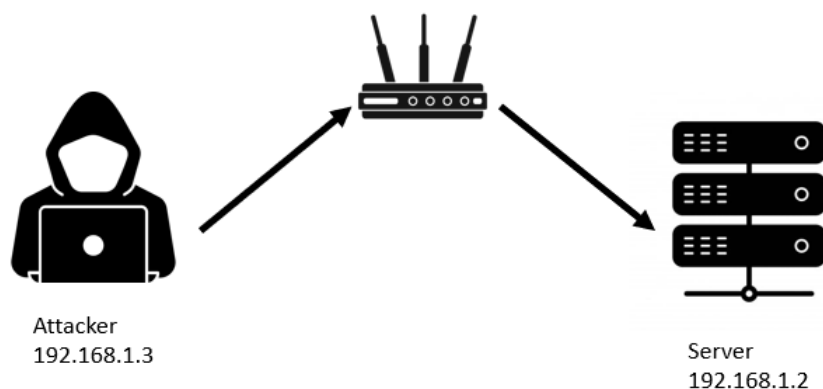
viên cần sử dụng máy attacker tiến hành khai thác thành công lỗ hổng buffer overflow trên máy chủ để lấy được chuỗi số bí mật.

Để đáp ứng yêu cầu bài thực hành, cần cung cấp 3 container docker. Trong đó, một container đóng vai trò là server, một container đóng vai trò là attacker, container còn lại đóng vai trò là công cụ hỗ trợ, sinh viên có thể dùng đến hoặc không (trong trường hợp sinh viên muốn dùng công cụ decompiler trực tiếp trên máy attacker). Hệ thống cần ghi lại được thao tác sử dụng các lệnh trên terminal container của sinh viên để tạo ra được kết quả đánh giá. Hệ thống yêu cầu sinh viên nhập email gắn liền với danh tính của sinh viên để thực hiện việc cá nhân hóa cho từng sinh viên.

Để bắt đầu bài thực hành sinh viên cần phải sử dụng các câu lệnh khởi tạo (labtainer -r <tên bài lab>) và câu lệnh kết thúc (stoplab <tên bài lab>) để hệ thống chạy bài lab cũng như lưu lại kết quả.

## 2. Thiết kế bài thực hành

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker tạo ra 3 container: 1 container mang tên “format643” đóng vai trò là attacker và 1 container mang tên “server” đóng vai trò là server, 2 máy đều được mở các cổng cần thiết. Hình 1 mô tả sơ đồ thiết kế bài thực hành.



*Hình 1. Sơ đồ thiết kế bài thực hành*

- Tạo mạng LAN “TEST” có cấu hình: 192.168.1.0/24 và gateway 192.168.1.1
- Cấu hình docker gồm có:
  - Buf64\_3: Lưu cấu hình cho máy attacker, trong đó gồm có:
    - Tên máy: attacker
    - Địa chỉ trong mạng LAN: 192.168.1.3

- Gateway: 192.168.1.1
- Server: Lưu cấu hình cho máy server, trong đó gồm có:
  - Tên máy: server
  - Địa chỉ trong mạng LAN: 192.168.1.2
  - Gateway: 192.168.1.1
- Ghidra: sử dụng để decompile binary:
  - Tên máy: ghidra-vm
  - Địa chỉ trong mạng LAN: N/A
- Config: Lưu cấu hình hoạt động của hệ thống
- Dockerfiles: Mô tả cấu hình của 3 container: attacker, ghidra và server, trong đó:
  - Attacker sử dụng base image cần cài thêm netcat và git để setup tools
  - Server sử dụng network base image cần cài thêm rsync để setup service xinetd
  - Ghidra sử dụng ghidra base image không cần config gì thêm
- Docs: Lưu phần mô tả hướng dẫn làm bài thực hành cho sinh viên
- Instr\_config: Lưu cấu hình cho phần nhận kết quả và chấm điểm
- Thiết lập hệ thống mạng sao cho 2 container cùng một mạng LAN.
- Để đánh giá được sinh viên đã hoàn thành bài thực hành hay chưa, cần chia bài thực hành thành các nhiệm vụ nhỏ, mỗi nhiệm vụ cần phải chỉ rõ kết quả để có thể đưa vào đó đánh giá, chấm điểm. Do vậy, trong bài thực hành này hệ thống cần ghi nhận các thao tác, sự kiện được mô tả và cấu hình:

```

_create_pattern = format64_3:*.stdout : CONTAINS : > C
_enter_pattern = format64_3:*.stdout : FILE_REGEX : (%p).+
vmmap = format64_3:*.stdout : CONTAINS : ld-2.31.so
find_freehook = format64_3:*.stdout : FILE_REGEX : e48.*__free_hook
find_system = format64_3:*.stdout : FILE_REGEX : 290.*__libc_system
overwrite = format64_3:*.stdout : CONTAINS : e48 (__free_hook)
_echo = format64_3:echo.stdout : TOKEN : LAST : STARTSWITH : flag

```

- Sau khi có đầu vào thao tác, tiến hành kiểm tra để cho ra kết quả cuối ‘Goal result’:

*trigger\_bug = boolean : (\_create\_pattern and \_enter\_pattern)*

*secret = matchany : string\_contains : \_echo : parameter.secret\_*

- Sau khi nhận được file đóng gói từ sinh viên, giảng viên sử dụng chức năng chấm điểm để xem kết quả được thiết kế dưới dạng bảng trong đó có ghi rõ email của sinh viên thực hiện, từng tiêu chí chấm điểm được ghi nhận (ví dụ: ‘Y’ là đã hoàn thành, nếu không có là chưa hoàn thành) và kết luận là sinh viên đã hoàn thành bài thực hành đó hay chưa. Kiểm tra bài thực hành đúng do sinh viên làm bằng cách kiểm tra email

```
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/format64_3
Labname format64_3

Student | trigger_bug | secret | vmmap | find_freehook | find_system | overwrite |
=====|=====|=====|=====|=====|=====|=====|
test123 | Y | Y | Y | Y | Y | Y |
What is automatically assessed for this lab:

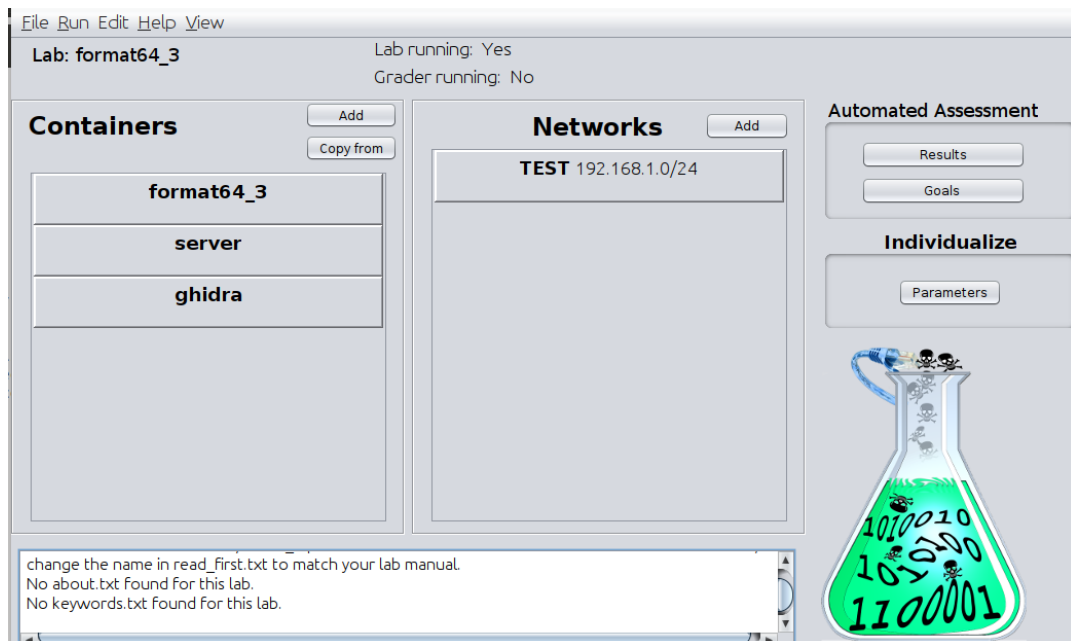
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$
```

Hình 2. Kết quả chấm điểm

Y: đã hoàn thành

### III. Cài đặt và cấu hình các máy ảo

- Cần chạy file update-designer.sh để cập nhật bản mới nhất của labedit
- Từ đường dẫn bất kì trên terminal gõ lệnh labedit
- Thực hiện tạo lab mới: File -> New Lab và đặt tên cho bài lab



Hình 3. Tạo lab với tên format64\_3



- Sau khi lab được khởi tạo, tạo 3 container với base image lần lượt là: base2, network2, ghidra

Container Config: format64\_3

Edit

General Docker Hosts GNS3 Other

**Container: format64\_3 Base: labtainer.base2**

User name  
attacker

Password

Lab Gateway  
192.168.1.1

nameserver

Terminal quantity  
2

Terminal group

☒ X11 enabled  
☐ No external gateway  
☐ No resolv.conf server

Add

**Networks**

TEST	192.168.1.3	Delete
------	-------------	--------

OK Cancel

Hình 4. Tạo container attacker

Container Config: server

Edit

General Docker Hosts GNS3 Other

**Container: server Base: labtainer.network2**

User name  
server

Password  
supersecretbassword

Terminal quantity  
0

Terminal group

Lab Gateway  
192.168.1.1

nameserver

☒ X11 enabled  
☐ No external gateway  
☐ No resolv.conf server

Add

**Networks**

Network	IP	Action
TEST	192.168.1.2	Delete

OK Cancel

Hình 5. Tạo container server

Container Config: ghidra

Edit

General Docker Hosts GNS3 Other

**Container: ghidra Base: labtainer.ghidra**

User name  
ghidra-vm

Password  
1

Terminal quantity  
1

Terminal group

Lab Gateway

nameserver

☒ X11 enabled  
☐ No external gateway  
☐ No resolv.conf server

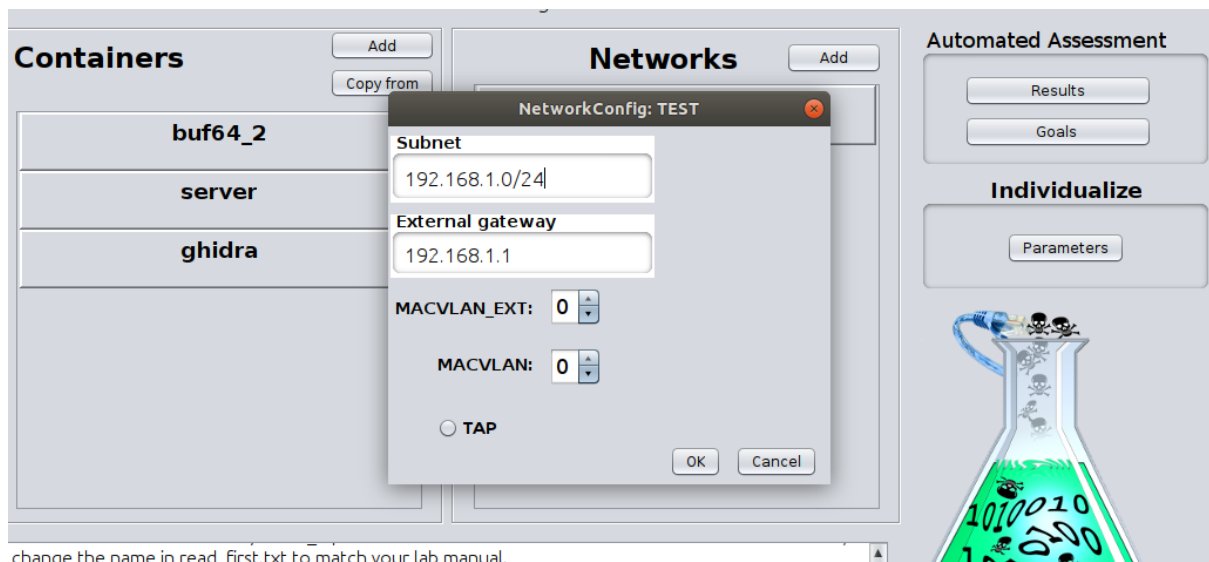
Add

Networks

OK Cancel

*Hình 6. Tạo container ghidra*

- Tạo networks mới cho lab, đặt tên network, cài đặt giải mạng con và gateway cho mạng



Hình 7. Tạo mạng mới cho lab

- Cấu hình mạng cho Attacker và Server:
  - o Attacker:
    - IP: 192.168.1.3/24
    - GW: 192.168.1.1
  - o Server:
    - IP 192.168.1.2/24
    - GW: 192.168.1.1
    - Service port: 1810
- Cài đặt thêm công cụ pwntools và extension pwndbg cho container attacker
- Cài đặt service binary cho container server

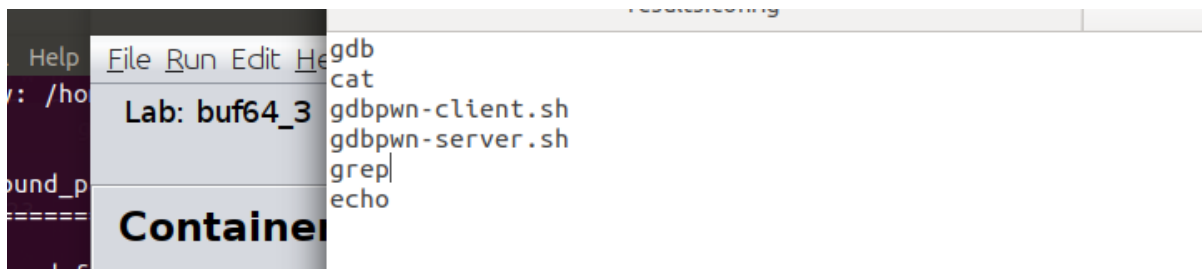
```

service test
{
  disable = no
  socket_type = stream
  protocol = tcp
  wait      = no
  user      = root
  type      = UNLISTED
  port      = 1810
  bind      = 0.0.0.0
  server    = /usr/sbin/chroot
  # replace helloworld to your program
  server_args = --userspec=1000:1000 /home/server ./format64_3
  banner_fail = /etc/banner_fail
  # safety options
  per_source = 10 # the maximum instances of this service per source IP address
  rlimit_cpu = 20 # the maximum number of CPU seconds that the service may use
  #rlimit_as = 1024M # the Address Space resource limit for the service
  #access_times = 2:00-9:00 12:00-24:00
}

```

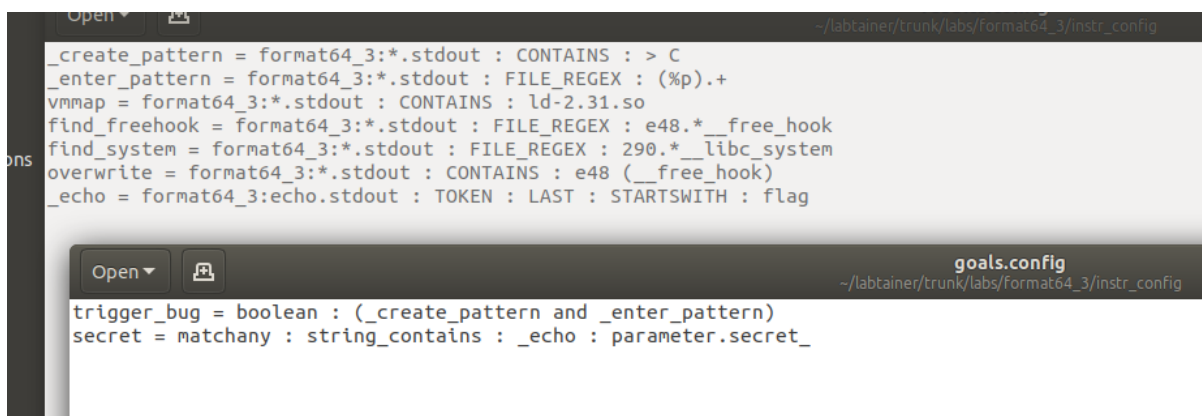
Hình 8. Cài đặt service binary tại port 1810

- Chỉnh sửa file treataslocal để tạo task đánh giá cho từng container bằng cách chỉnh sửa file treataslocal từ labedit hoặc chỉnh sửa trực tiếp theo đường dẫn `~/labtainer/trunk/labs/<tên-lab>/<tên-container>/_bin/treataslocal`



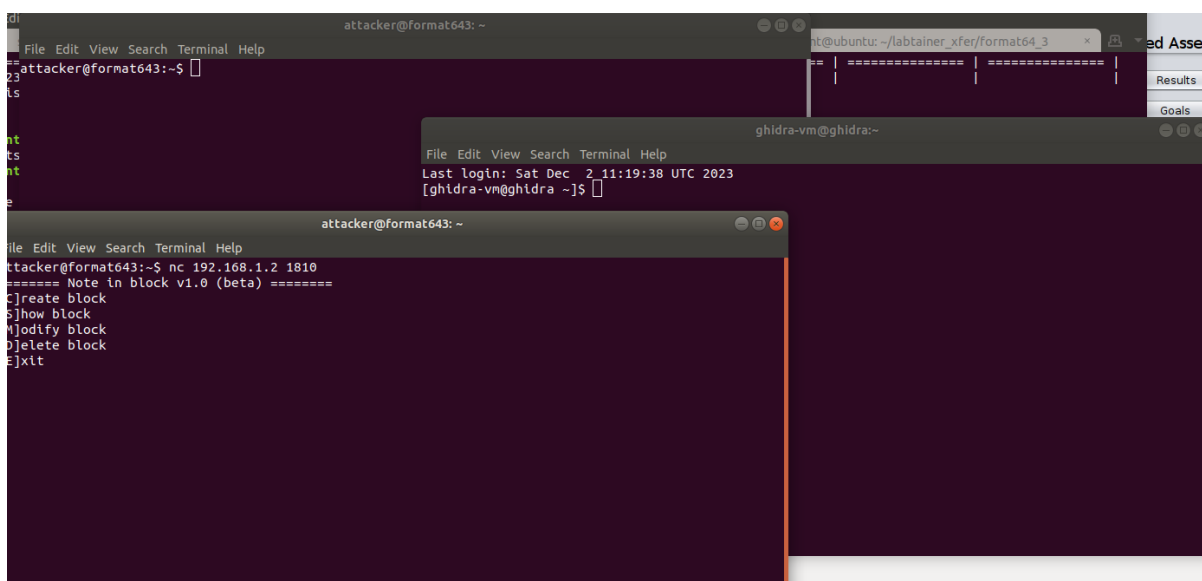
Hình 9. Chỉnh sửa file treataslocal trên máy attacker

- Cài đặt Results ở phần Automated Assesment:



Hình 10. Cài đặt chấm điểm tự động

- Tiến hành save lab, sau đó build và chạy thử lab



Hình 11. build lab và chạy bài lab

#### IV. Thử nghiệm lab và kết quả

```
Labname format64_3
Student      | trigger_bug | secret | vmmap | find_freehook | find_s stem | overwrite |
=====|=====|=====|=====|=====|=====|=====|
test123      |              |        |        |              |              |          |
What is automaticall assessed for this lab:
```

Hình 12. Run lab và thực hiện check work trước khi thực hiện bài lab

```
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/format64_3
Labname format64_3
Student      | trigger_bug | secret | vmmap | find_freehook | find_system | overwrite |
=====|=====|=====|=====|=====|=====|=====|
test123      |              |        |        |              |              |          |
What is automatically assessed for this lab:
student@ubuntu:~/labtainer/trunk/scripts/labtainer-student$
```

Hình 13. Thực hiện bài lab sau đó check work

#### V. Triển khai bài lab

- Chuyển tới thư mục chứa các bài thực hành: **labtainer/trunk/labs**
- Khởi tạo git: **git init** (chỉ khởi tạo một lần, không lặp lại với mỗi lần).
- Lấy tên của Docker Hub để đăng ký cho registry bài lab mới ở config/start.config (tại Labtainers GUI: Edit / Config (registry))
- Trong đường dẫn thư mục của bài lab, chạy cleanlab4svn.py để xóa những files tạm.
- Sau đó trong đường dẫn cha của bài lab:

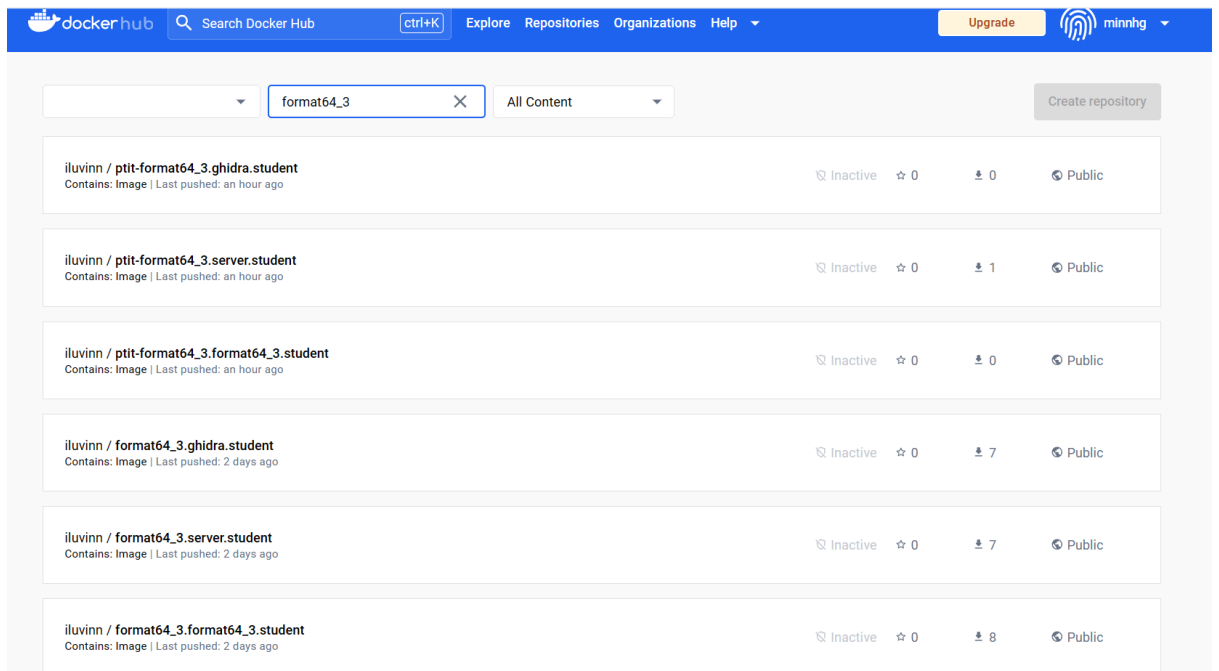
git add <tên bài lab> git commit <tên bài lab> -m

"Adding an IModule"

```
File Edit View Search Terminal Help
student@ubuntu:~/labtainer/trunk/labs$ rm -fr .git
student@ubuntu:~/labtainer/trunk/labs$ clear
student@ubuntu:~/labtainer/trunk/labs$ git init
Initialized empty Git repository in /home/student/labtainer/trunk/labs/.git/
student@ubuntu:~/labtainer/trunk/labs$ git add ptit-buf64_2
student@ubuntu:~/labtainer/trunk/labs$ git add ptit-buf64_3
student@ubuntu:~/labtainer/trunk/labs$ git add ptit-format64_2
student@ubuntu:~/labtainer/trunk/labs$ git add ptit-format64_3
student@ubuntu:~/labtainer/trunk/labs$ git add ptit-fastbin
student@ubuntu:~/labtainer/trunk/labs$ git commit -m "add n08 labs"
[master (root-commit) 198181d] add n08 labs
235 files changed, 7106 insertions(+)
```

Hình 14. Đẩy bài lab lên git

- Đẩy images của vùng chứa (container) lên DockerHub  
cd \$LABTAINER\_DIR/distrib  
./publish.py -d -l my-new-lab



Hình 15. Các images của vùng chứa được đẩy lên DockerHub

- Tạo file IModule tar chứa bài thực hành: create-imodules.sh

```
student@ubuntu: ~/labtainer/trunk/labs$ cd ../distrib/
student@ubuntu: ~/labtainer/trunk/distrib$ create-imodules.sh
lab is ptit-buf64_2
Do docs
lab is ptit-buf64_3
Do docs
lab is ptit-fastbin
Do docs
lab is ptit-format64_2
Do docs
lab is ptit-format64_3
Do docs
*****
** Post /home/student/labtainer/trunk/imodule.tar to your web server **
*****
student@ubuntu: ~/labtainer/trunk/distrib$
```

Hình 16. Tạo file Imodule tra chứa bài thực hành

- Sau đó, copy và lưu lại file imodule.tar. Đường dẫn URL vào link imodule:

<https://github.com/iluvinn/cdatpm-ptit.git>

## TÀI LIỆU THAM KHẢO

[Labtainer Lab Designer User Guide](#)