

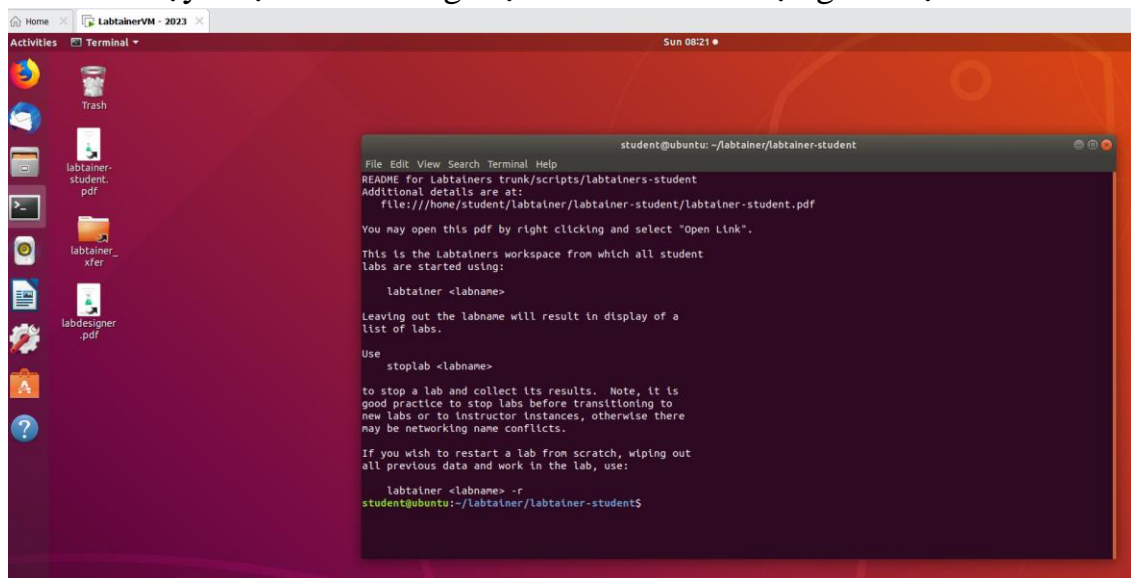
## Hướng dẫn thực hành môn Phân tích mã độc.

### 1. Yêu cầu:

- Sinh viên cần có máy tính hỗ trợ các phần mềm ảo hóa như VMware hoặc Virtual Box.
- Sinh viên tải file chứa môi trường thực hành theo đường dẫn sau:
  - o Sử dụng VMware: [https://ptitedu.vn-my.sharepoint.com/:u:/g/personal/duydt\\_ptit\\_edu\\_vn/Eek7nBQhdfdDi\\_SACdg5BjoBdm9WsO2Dsxt43l1lzPHwwA?e=QM3xIJ](https://ptitedu.vn-my.sharepoint.com/:u:/g/personal/duydt_ptit_edu_vn/Eek7nBQhdfdDi_SACdg5BjoBdm9WsO2Dsxt43l1lzPHwwA?e=QM3xIJ)
  - o Sử dụng Virtual Box: [https://ptitedu.vn-my.sharepoint.com/:u:/g/personal/duydt\\_ptit\\_edu\\_vn/EVLHPttcDFBIk8wMfs8mJFQBJZ8U0QuqWuA05O4Iy3ibBg?e=FEK7ik](https://ptitedu.vn-my.sharepoint.com/:u:/g/personal/duydt_ptit_edu_vn/EVLHPttcDFBIk8wMfs8mJFQBJZ8U0QuqWuA05O4Iy3ibBg?e=FEK7ik)
- Sau đó thì chạy file này trên môi trường máy ảo đã cài đặt.

### 2. Các bước thực hành

- Sau khi chạy được môi trường thực hành sẽ xuất hiện giao diện sau:



- Trên Terminal student@ubuntu (sau đây gọi là A): gõ lệnh để tải bài thực hành. Ví dụ cần thực hành bài “nmap-discovery” thì sử dụng lệnh sau:

*labtainer nmap-discovery*

Sau đó chờ môi trường tải bài thực hành về.

- Sau khi cài đặt được môi trường thực hành thì vào trang web [dsec.ptit.edu.vn](https://dsec.ptit.edu.vn) để xem đề bài thực hành. Để đăng nhập được cần nhập tên tài khoản là mã sinh viên, chú ý viết hoa (ví dụ B20DCCN001).
- Sau khi đăng nhập vào cần phải đổi mật khẩu
- Sau đó vào ca thực hành để nhận đề và làm theo hướng dẫn trên đề bài.

- Lưu ý để có thể chấm điểm trên hệ thống thì cần nhập đúng mã sinh viên (viết hoa) khi bắt đầu bài thực hành

Please enter your e-mail address: B20DCAT001

- Trong khi làm bài thực hành để kiểm tra xem đã làm đủ các yêu cầu chưa thì sử dụng lệnh *checkwork* để kiểm tra trên terminal A. nếu kết quả xuất hiện chữ Y tức là thành công

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/nmap-discovery
Labname nmap-discovery

Student          | nmap_count | did_ssh |
=====|-----|-----|
AT1008          | 7          | Y       |

What is automatically assessed for this lab:
  did_ssh: SSH'd to the proper port and viewed the target file
  nmap_count: count of use of nmap
```

- Sau khi thực hiện xong bài thực hành thì cần tìm file *.lab* trong folder *labtainer\_xfer* trên *desktop* của máy *Ubuntu*.
- Sau khi up file lên *dsec.ptit.edu.vn* nếu nhận được *AC* tức là đã hoàn thành.
- Lưu ý: sau khi đã hoàn thành bài TH (tức là sử dụng *stoplab*) thì vẫn có thể kiểm tra lại kết quả sử dụng

*Checkwork <tên\_bài>*

### 3. Báo cáo

- Để hoàn thành bài thực hành, sinh viên cần
  - o Nộp file *.lab* trên *dsec.ptit.edu.vn* và nhận kết quả *AC*
  - o Làm báo cáo thực hành file pdf và nộp báo cáo cùng file *.lab* (nén dưới dạng *.zip* hoặc *.rar*) gửi lên hệ thống LMS (<https://lmsattt.ptit.edu.vn/>); tài khoản sử dụng mã sinh viên (chữ viết thường) và mật khẩu; tìm đến môn Phân Tích Mã Độc và nộp bài trong phần bài thực hành. File thực hành cần có:
    - Trang bìa
    - Mục lục
    - Tìm hiểu lý thuyết: tìm hiểu về phần lý thuyết của bài thực hành
    - Nội dung thực hành: mô tả các bước làm bài thực hành (có hình ảnh minh chứng kết quả từng bước) đồng thời phân tích các bước thực hành này.
    - Lưu ý cần có ảnh chụp *checkwork* để kiểm tra kết quả
    - Kết luận bài thực hành