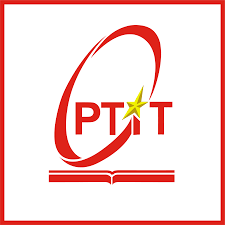
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

KHOA AN TOÀN THÔNG TIN



MÔN HỌC: PHÂN TÍCH MÃ ĐỘC

**BÁO CÁO THỰC HÀNH BÀI 6**

Giảng viên: PGS.TS. Đỗ Xuân Chợ

Sinh viên: Hoàng Trung Kiên – B20DCAT098

Hà Nội – 5/2023

Mục lục

[I. Lý thuyết. 3](#_Toc149038503)

[1. Mục đích. 3](#_Toc149038504)

[2. Thực hành. 3](#_Toc149038505)

[**2.1. Khám phá.** 3](#_Toc149038506)

[2.2 Sử dụng strace. 4](#_Toc149038507)

[2.3 Kiểm tra cổng bằng sendudp.py. 4](#_Toc149038508)

[2.4 Phân tích động. 6](#_Toc149038509)

[II. Checkwork. 6](#_Toc149038510)

# I. Lý thuyết.

## 1. Mục đích.

Bài tập này giới thiệu việc sử dụng tiện ích strace trong Unix để ghi lại các lời gọi của hệ thống (system call) được thực hiện bởi một chương trình đang chạy.

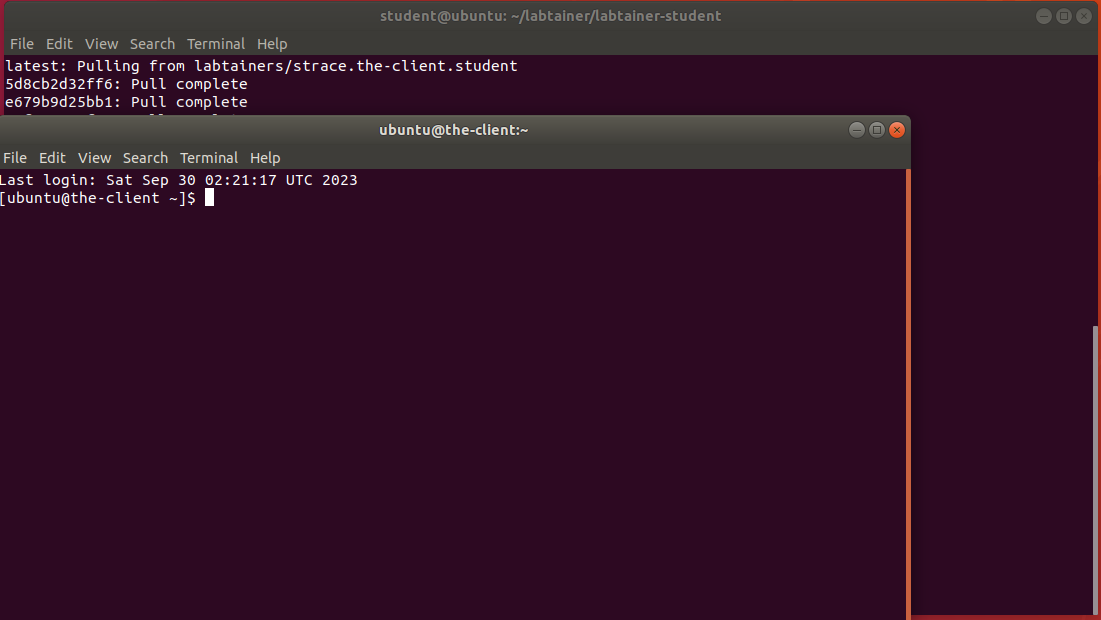
Giúp sinh viên hiểu cách sử dụng strace.

Hiểu cách đầu ra của strace tương ứng với các system call.

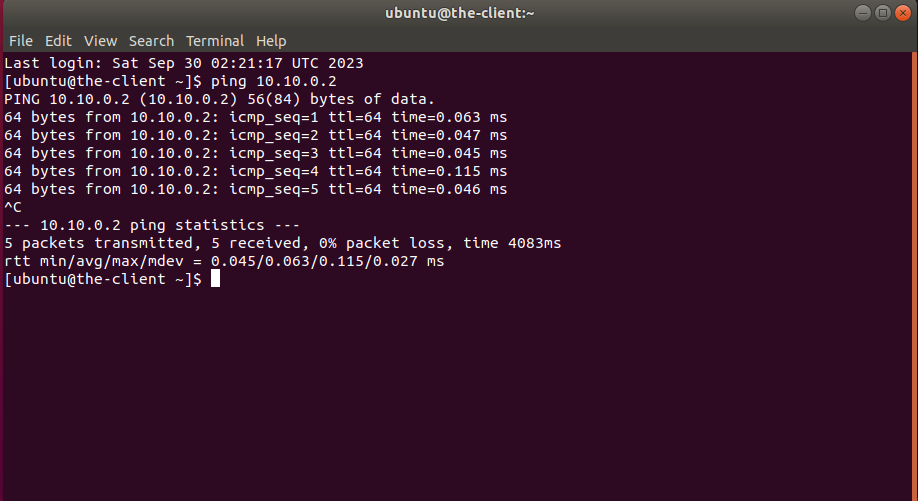
Sử dụng strace để phân tích động phần mềm.

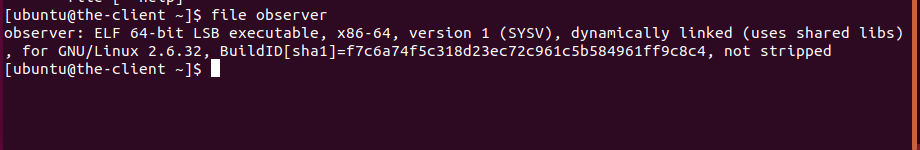
## 2. Thực hành.

### **2.1. Khám phá.**

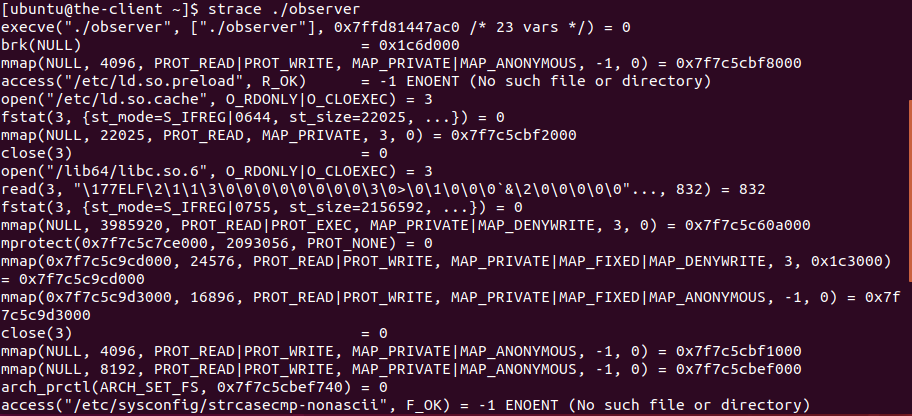


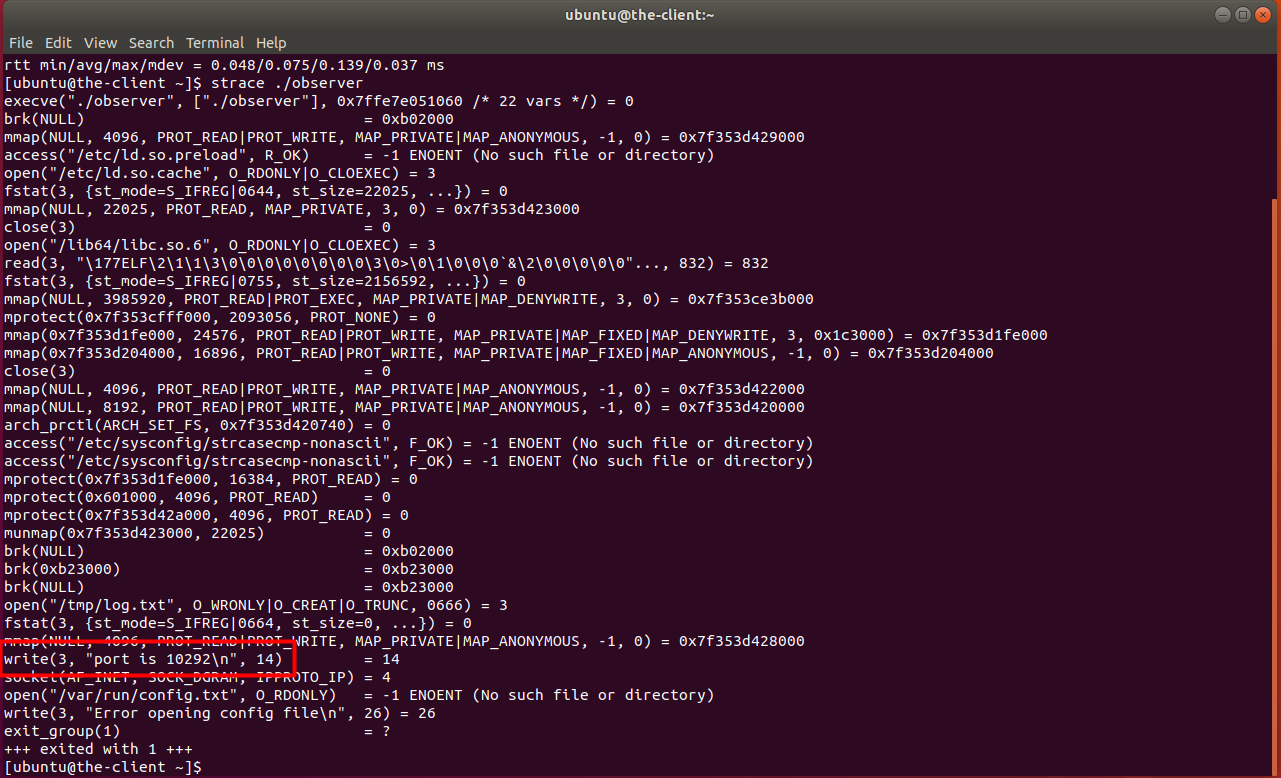
Từ client ping đến server





### 2.2 Sử dụng strace.

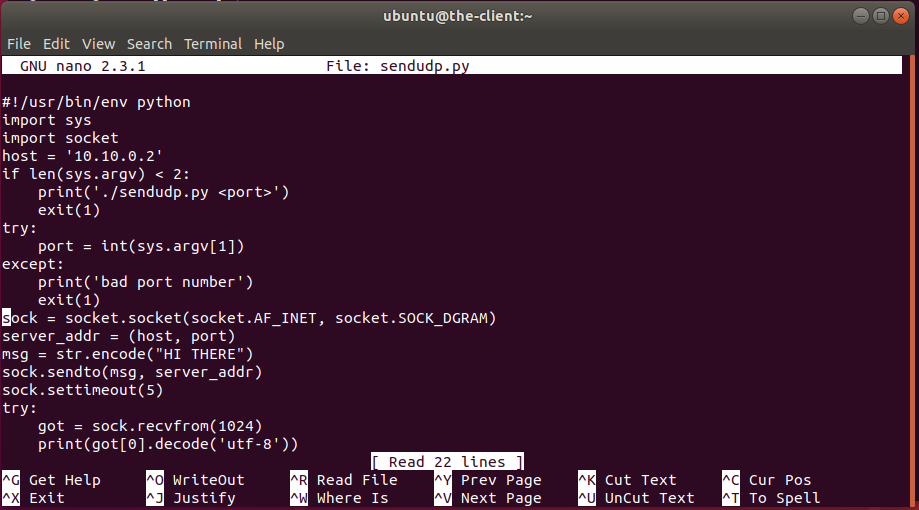




Ta tìm ra cổng đang mở là 10292

### 2.3 Kiểm tra cổng bằng sendudp.py.

Đoạn code này trong file sendudp.py có nhiệm vụ là gửi 1 thông điệp udp tới 1 máy chủ và nhận phản hồi từ máy chủ đó



Nội dung của đoạn code trong file sendudp.py

**#!/usr/bin/env python**

import sys

import socket

host = '10.10.0.2' **# Địa chỉ IP của máy chủ**

if len(sys.argv) < 2:

print('./sendudp.py <port>')

exit(1)

try:

port = int(sys.argv[1]) **# Cổng được truyền vào dưới dạng đối số**

except:

print('bad port number')

exit(1)

sock = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM) # Tạo socket UDP

server\_addr = (host, port) **# Địa chỉ máy chủ**

msg = str.encode("HI THERE") **# Chuỗi thông điệp được gửi**

sock.sendto(msg, server\_addr) **# Gửi thông điệp tới máy chủ**

sock.settimeout(5) **# Đặt thời gian chờ**

try:

got = sock.recvfrom(1024) **# Nhận phản hồi từ máy chủ**

print(got[0].decode('utf-8')) **# In ra nội dung phản hồi**

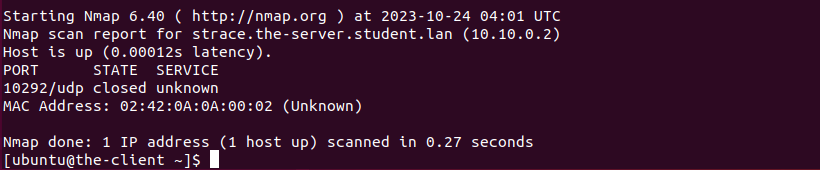
except socket.timeout:

print('No response from server') **# In ra thông báo nếu không nhận được phản hồi**

### 2.4 Phân tích động.

Chạy lệnh ./sendudp.py 10292 để kiểm tra





# II. Checkwork.

Checkwork để kiểm tra bài lab

