

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 Chợt

Sinh viên: Hoàng Trung Kiên – B20DCAT098

Hà Nội – 5/2023

Mục lục

I. Lý thuyết.	3
1. Mục đích.	3
2. Thực hành.	3
2.1. Khám phá.	3
2.2 Sử dụng strace.	4
2.3 Kiểm tra cổng bằng sendudp.py.....	4
2.4 Phân tích động.....	6
II. Checkwork.	6

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.

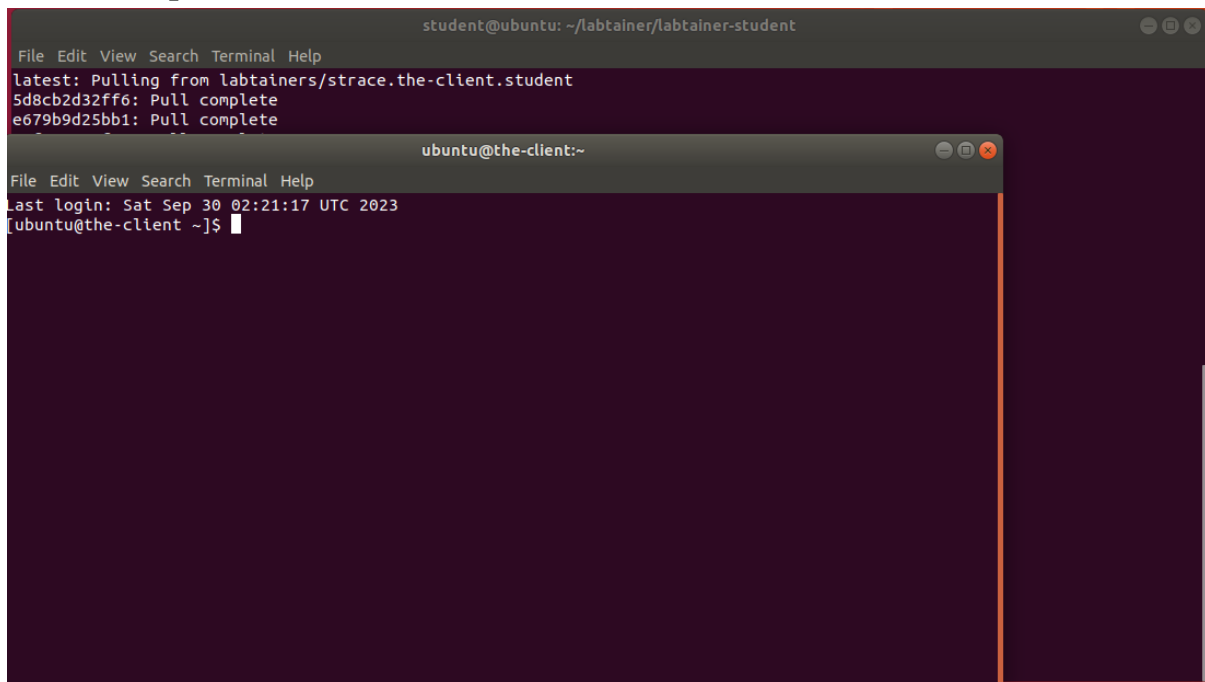
Giúp sinh viên hiểu cách sử dụng strace.

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

Sử dụng strace để phân tích động phần mềm.

2. Thực hành.

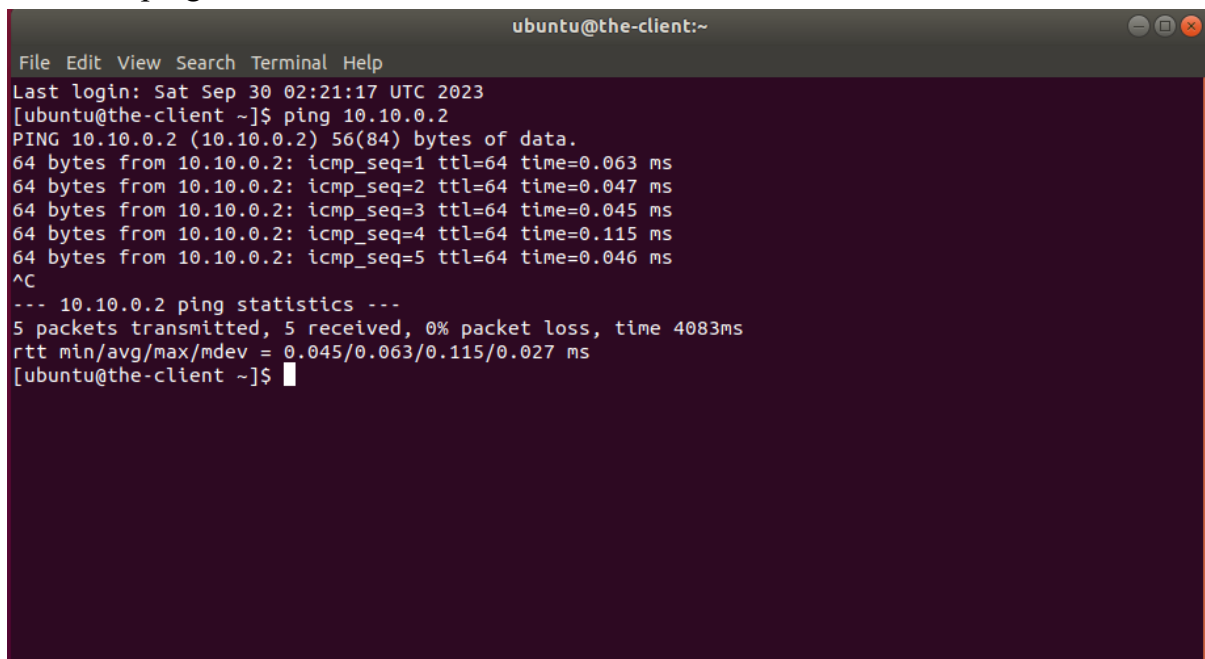
2.1. Khám phá.



```
student@ubuntu: ~/labtainer/labtainer-student
File Edit View Search Terminal Help
latest: Pulling from labtainers/strace.the-client.student
5d8cb2d32ff6: Pull complete
e679b9d25bb1: Pull complete

ubuntu@the-client:~
File Edit View Search Terminal Help
Last login: Sat Sep 30 02:21:17 UTC 2023
ubuntu@the-client ~]$
```

Từ client ping đến server



```
ubuntu@the-client:~
File Edit View Search Terminal Help
Last login: Sat Sep 30 02:21:17 UTC 2023
[ubuntu@the-client ~]$ ping 10.10.0.2
PING 10.10.0.2 (10.10.0.2) 56(84) bytes of data.
64 bytes from 10.10.0.2: icmp_seq=1 ttl=64 time=0.063 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 10.10.0.2: icmp_seq=3 ttl=64 time=0.045 ms
64 bytes from 10.10.0.2: icmp_seq=4 ttl=64 time=0.115 ms
64 bytes from 10.10.0.2: icmp_seq=5 ttl=64 time=0.046 ms
^C
--- 10.10.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4083ms
rtt min/avg/max/mdev = 0.045/0.063/0.115/0.027 ms
[ubuntu@the-client ~]$
```

```
[ubuntu@the-client ~]$ file observer
observer: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked (uses shared libs)
, for GNU/Linux 2.6.32, BuildID[sha1]=f7c6a74f5c318d23ec72c961c5b584961ff9c8c4, not stripped
[ubuntu@the-client ~]$
```

2.2 Sử dụng strace.

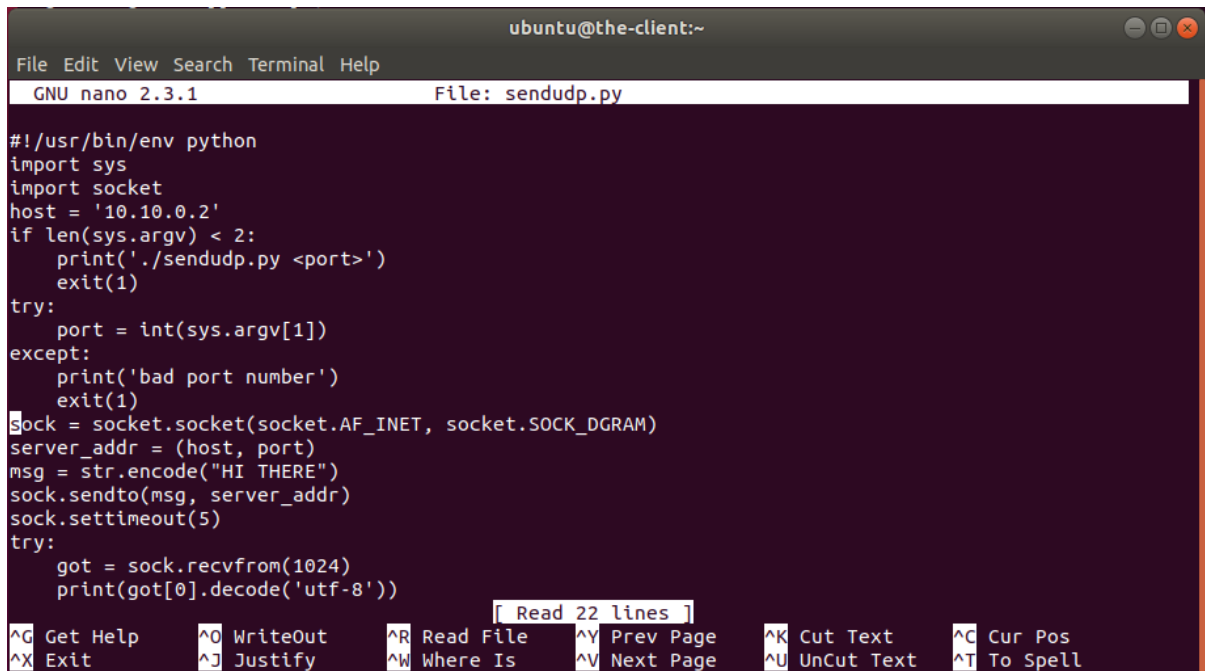
```
[ubuntu@the-client ~]$ strace ./observer
execve("./observer", ["/observer"], 0x7ffd81447ac0 /* 23 vars */) = 0
brk(NULL) = 0x1c6d000
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f7c5cbf8000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=22025, ...}) = 0
mmap(NULL, 22025, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f7c5cbf2000
close(3) = 0
```

```
File Edit View Search Terminal Help
rtt min/avg/max/ndev = 0.048/0.075/0.139/0.037 ms
[ubuntu@the-client ~]$ strace ./observer
execve("./observer", ["/observer"], 0x7ffe7e051060 /* 22 vars */) = 0
brk(NULL) = 0xb02000
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f353d429000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=22025, ...}) = 0
mmap(NULL, 22025, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f353d423000
close(3) = 0
open("/lib64/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
read(3, "\177ELF\2\1\1\3\0\0\0\0\0\0\0\3\0\0\0\1\0\0\0\0\2\0\0\0\0...", 832) = 832
fstat(3, {st_mode=S_IFREG|0755, st_size=2156592, ...}) = 0
mmap(NULL, 3985920, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7f353ce3b000
mprotect(0x7f353ce3b000, 2093056, PROT_NONE) = 0
mmap(0x7f353d1fe000, 24576, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x1c3000) = 0x7f353d1fe000
mmap(0x7f353d204000, 16896, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS, -1, 0) = 0x7f353d204000
close(3) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f353d422000
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f353d420000
arch_prctl(ARCH_SET_FS, 0x7f353d420740) = 0
access("/etc/sysconfig/strcasecmp-nonascii", F_OK) = -1 ENOENT (No such file or directory)
access("/etc/sysconfig/strcasecmp-nonascii", F_OK) = -1 ENOENT (No such file or directory)
mprotect(0x7f353d1fe000, 16384, PROT_READ) = 0
mprotect(0x601000, 4096, PROT_READ) = 0
mprotect(0x7f353d42a000, 4096, PROT_READ) = 0
munmap(0x7f353d423000, 22025) = 0
brk(NULL) = 0xb02000
brk(0xb23000) = 0xb23000
brk(NULL) = 0xb23000
open("/tmp/log.txt", O_WRONLY|O_CREAT|O_TRUNC, 0666) = 3
fstat(3, {st_mode=S_IFREG|0664, st_size=0, ...}) = 0
mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7f353d428000
write(3, "port is 10292\n", 14) = 14
socket(AF_INET, SOCK_DGRAM, IPPROTO_IP) = 4
open("/var/run/config.txt", O_RDONLY) = -1 ENOENT (No such file or directory)
write(3, "Error opening config file\n", 26) = 26
exit_group(1) = ?
+++ exited with 1 +++
[ubuntu@the-client ~]$
```

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



```
#!/usr/bin/env python
import sys
import socket
host = '10.10.0.2'
if len(sys.argv) < 2:
    print('./sendudp.py <port>')
    exit(1)
try:
    port = int(sys.argv[1])
except:
    print('bad port number')
    exit(1)
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
server_addr = (host, port)
msg = str.encode("HI THERE")
sock.sendto(msg, server_addr)
sock.settimeout(5)
try:
    got = sock.recvfrom(1024)
    print(got[0].decode('utf-8'))
```

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

```
[ubuntu@the-client ~]$ ./sendudp.py 10292
Yup, that is the port number!

Starting Nmap 6.40 ( http://nmap.org ) at 2023-10-24 04:01 UTC
Nmap scan report for strace.the-server.student.lan (10.10.0.2)
Host is up (0.00012s latency).
PORT      STATE SERVICE
10292/udp  closed unknown
MAC Address: 02:42:0A:0A:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
[ubuntu@the-client ~]$
```

II. Checkwork.

Checkwork để kiểm tra bài lab

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

Student          | strace_count | found_port |
=====|=====|=====|
B20DCAT098      | 1            | Y          |
What is automatically assessed for this lab:
```

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

Student          | strace_count | found_port |
=====|=====|=====|
B20DCAT098      | 2            | Y          |
What is automatically assessed for this lab:
```