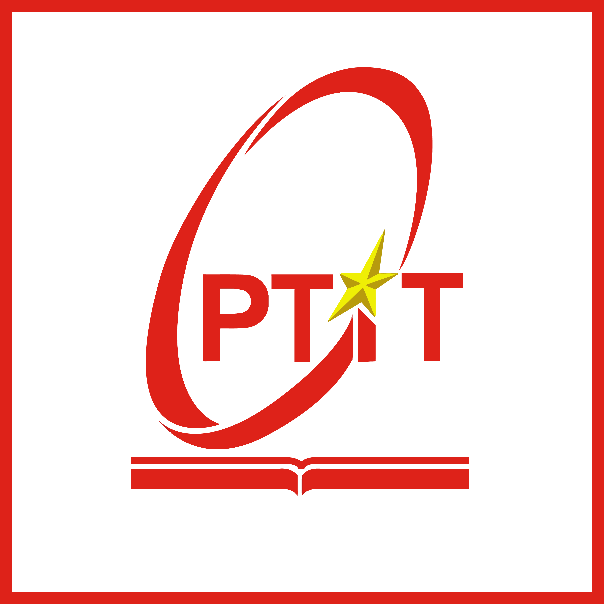
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA AN TOÀN THÔNG TIN**

**--------------**



**BÀI THỰC HÀNH 01**

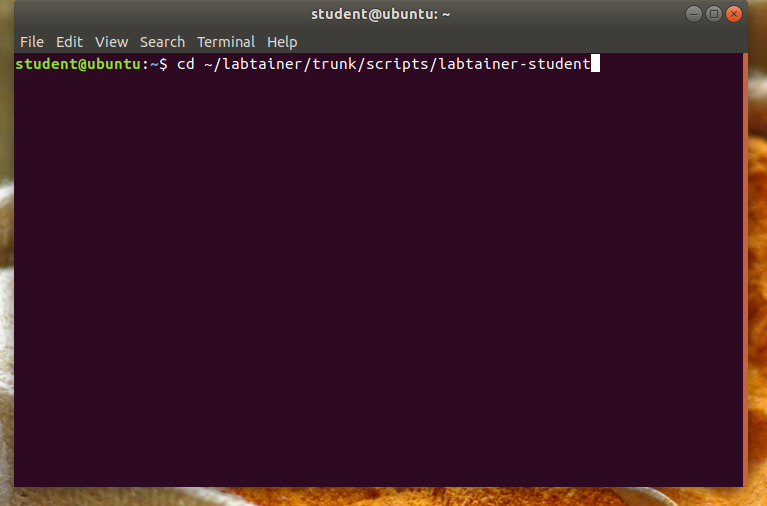
**MÔN HỌC: CƠ SỞ AN TOÀN THÔNG TIN**

|  |  |  |
| --- | --- | --- |
| **Giảng viên** | **:** | **Nguyễn Ngọc Điệp** |
| **Sinh viên** | **:** | **Lê Anh Tuấn** |
| **Lớp** | **:** | **D21CQAT01-B** |
| **Nhóm** | **:** | **03** |
| **Mã sinh viên** | **:** | **B21DCAT205** |
| **Số điện thoại** | **:** | **0369288612** |

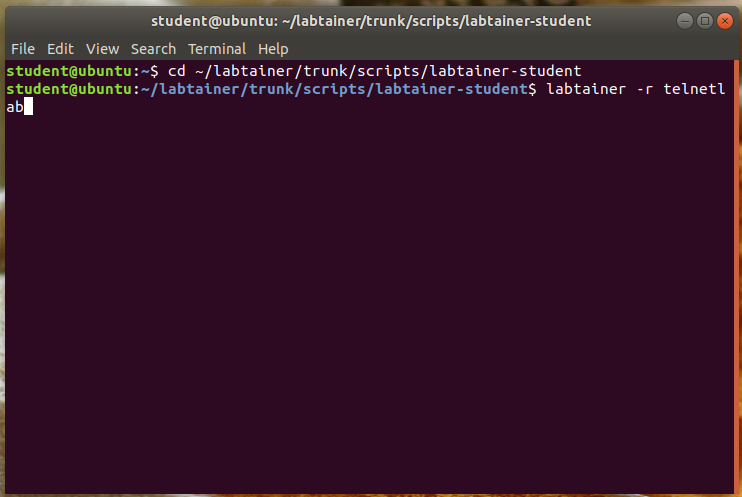
Tháng 9/2023

1. **Bài thực hành: sử dụng công cụ truy cập từ xa**

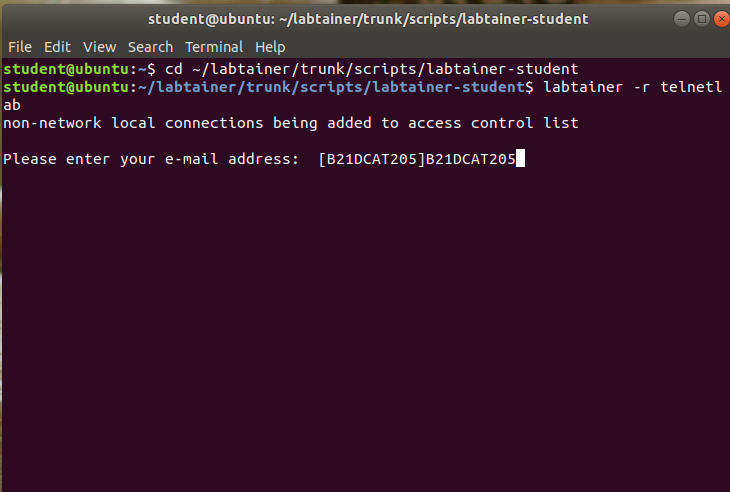
* Bật terminal và gõ dòng lệnh cd ~/labtainer/trunk/scripts/labtainer-student để chuyển vào thư mục labtainer-student



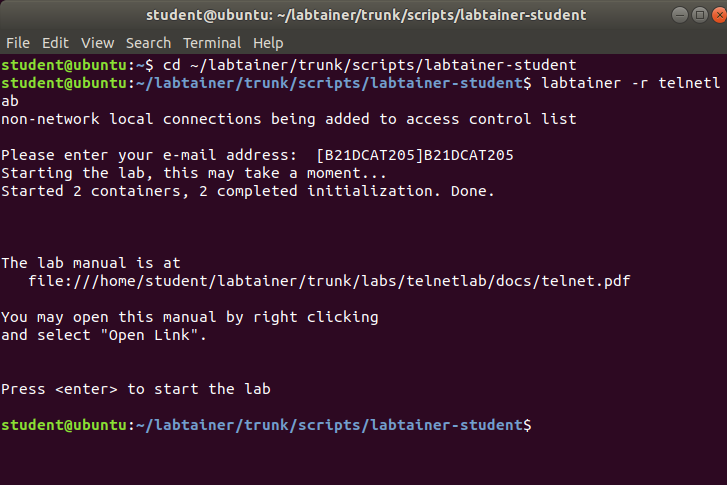
-Trong thư mục labtainer-student, ta tiếp tục gõ câu lệnh “labtainer -r telnetlab”



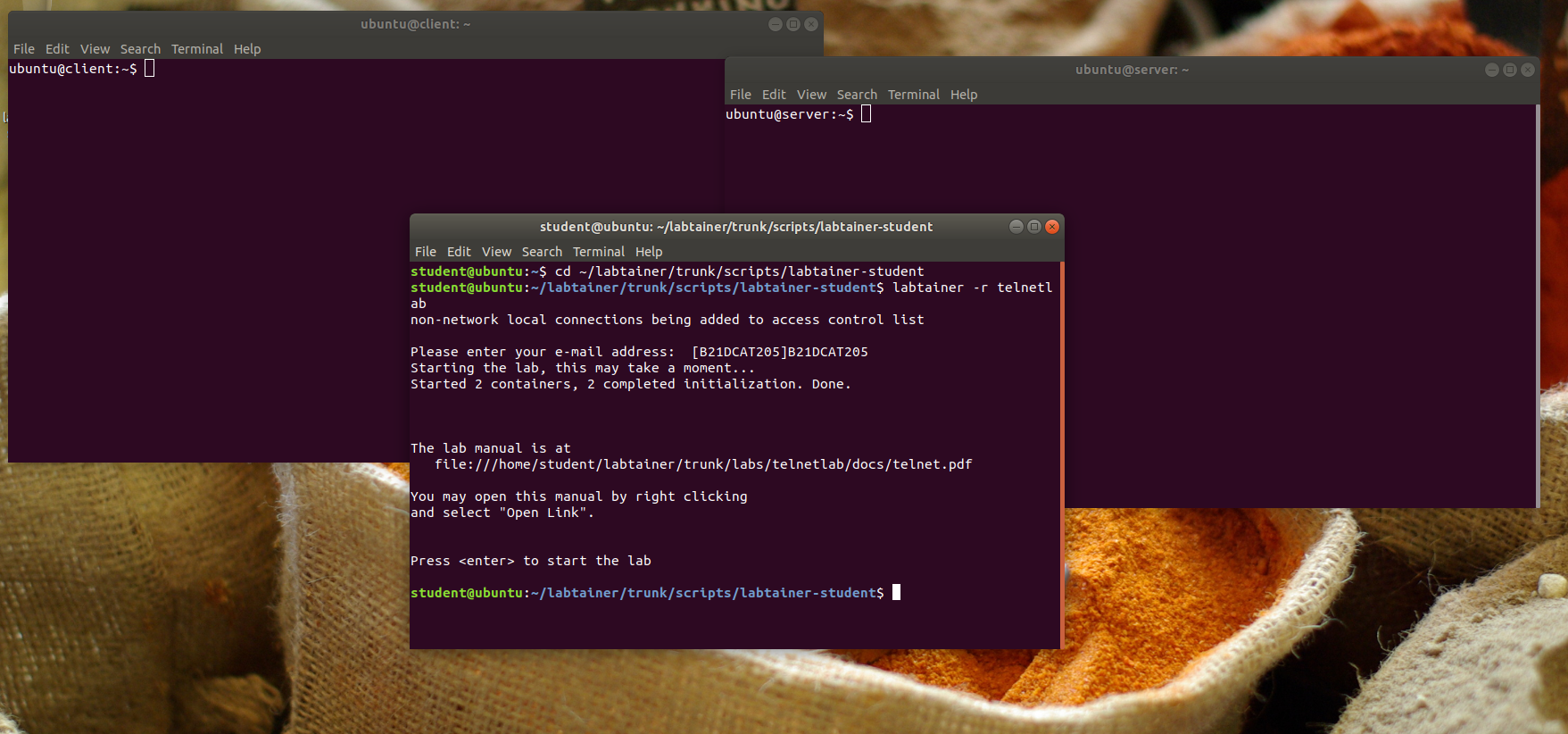
* Tiếp tục ta được yêu cầu nhập email, ta nhập mã sinh viên



* Ấn enter

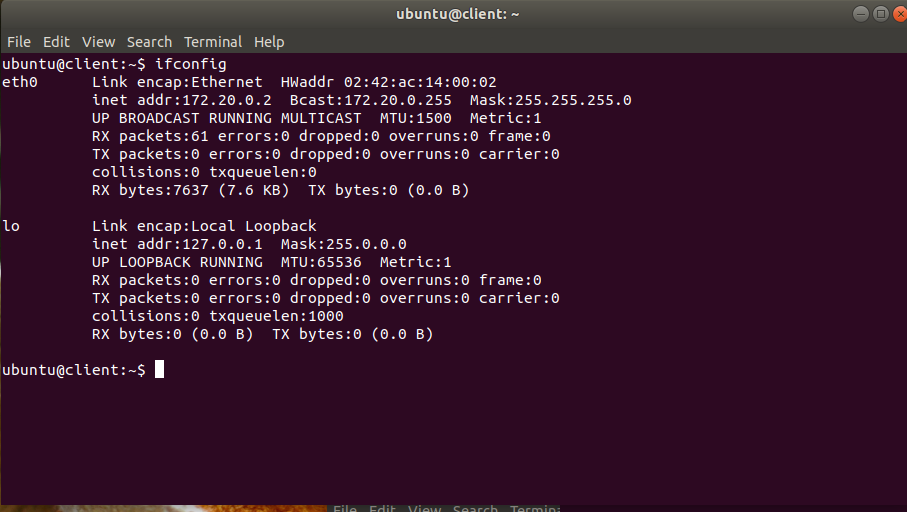


* Sau đó trên màn hình sẽ hiện ra 2 terminal, 1 terminal là của client (bên trái), 1 terminal của server (bên phải) như ở hình dưới đây:

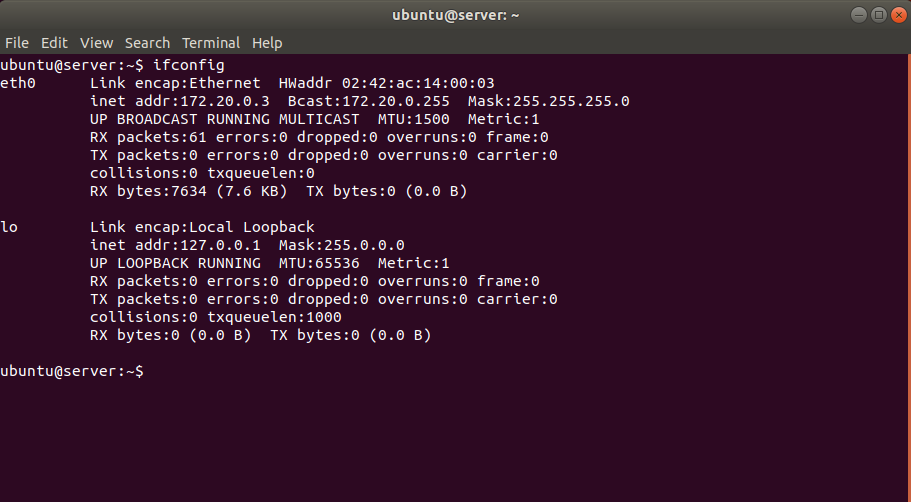


1. **Xác định IP của các máy**

* Trên terminal client và server sử dụng lệnh “ifconfig”, địa chỉ IP sẽ nằm sau “inet adddr:”
* Ta thấy rằng ở máy khách, địa chỉ ip sẽ là : 172.20.0.2.

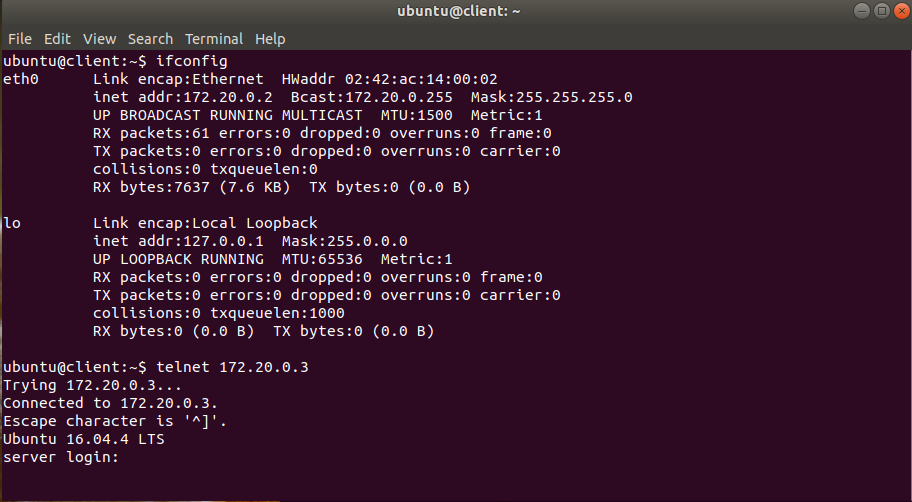


* Đối với máy chủ IP là 172.20.0.3

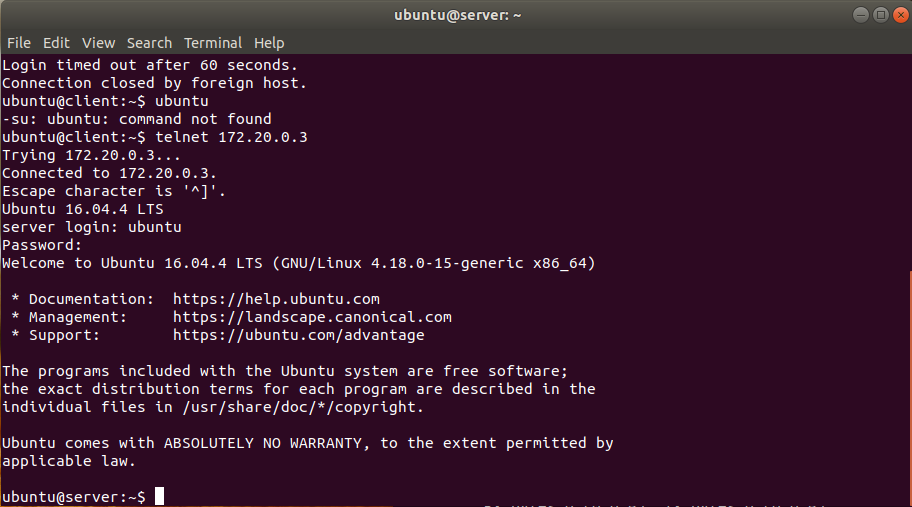


1. **Thực hiện telnet từ máy khách vào máy chủ và đọc dữ liệu trên máy chủ**

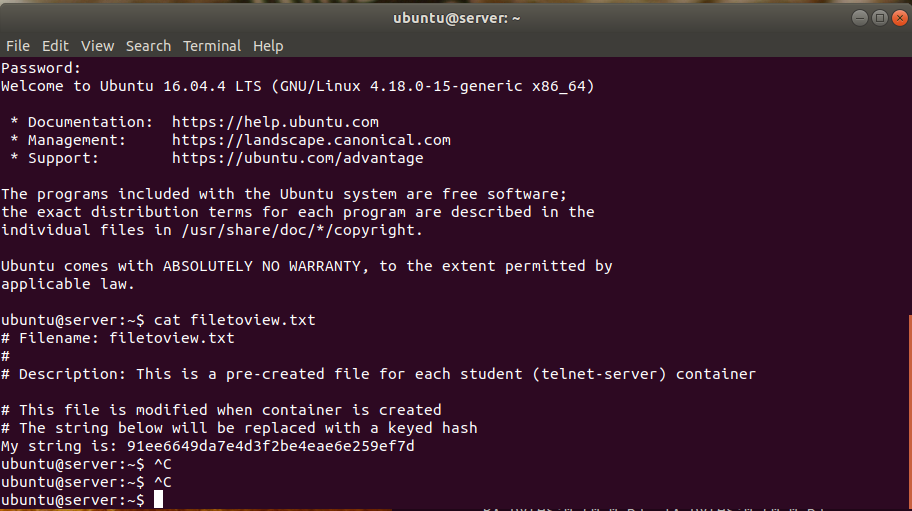
* Trên máy khách sử dụng telnet để kết nối với máy chủ thông qua địa chỉ IP: 172.20.0.3. Ta sử dụng lệnh: “telnet 172.20.0.3”.
* Sau đó, hiện yêu cầu đăng nhập đến server, ta nhập username và mật khẩu là “ubuntu”, đối với mật khẩu sẽ không nhìn thấy.



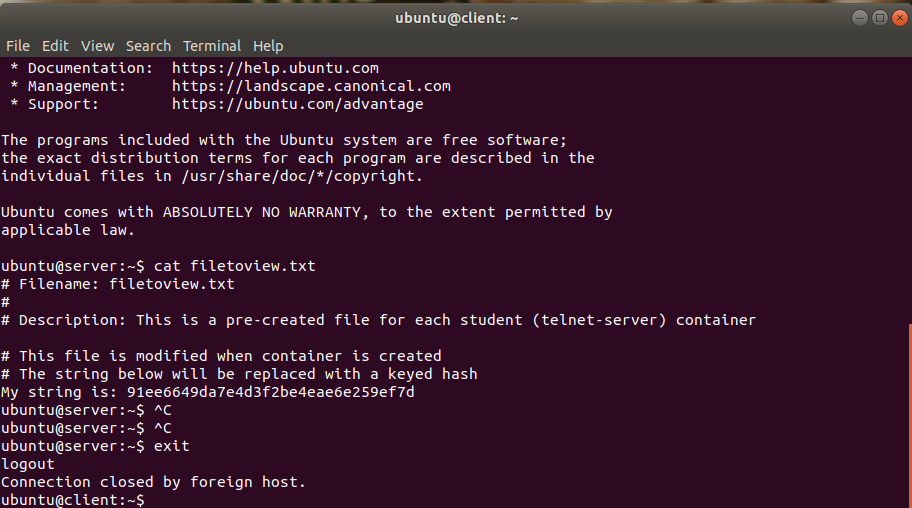
* Đăng nhập thành công đến máy chủ, ta có thể thấy tên terminal chuyển từ “ubuntu@client: ~” thành “ubuntu@server: ~”



* Sau khi đăng nhập vào máy chủ, thực hiện việc đọc tệp có sẵn chứa đoạn mật mã của sinh viên, sử dụng câu lệnh: “cat filetoview.txt”



* Thoát khỏi phiên telnet trên máy khách thông qua lệnh “exit”.

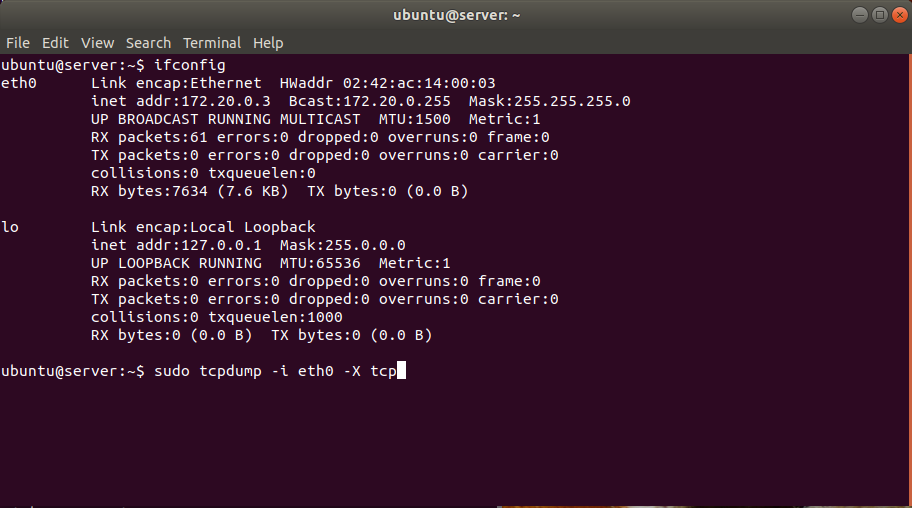


1. **Xem mật khẩu không được mã hóa**

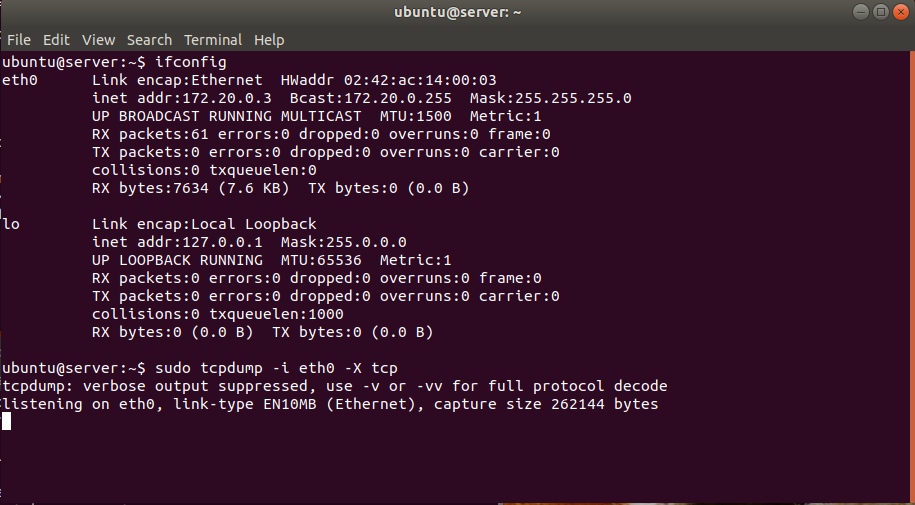
* Trên server, chạy tcpdump để hiển thị lưu lượng mạng TCP với câu lệnh:

sudo tcpdump -i eth0 -X tcp

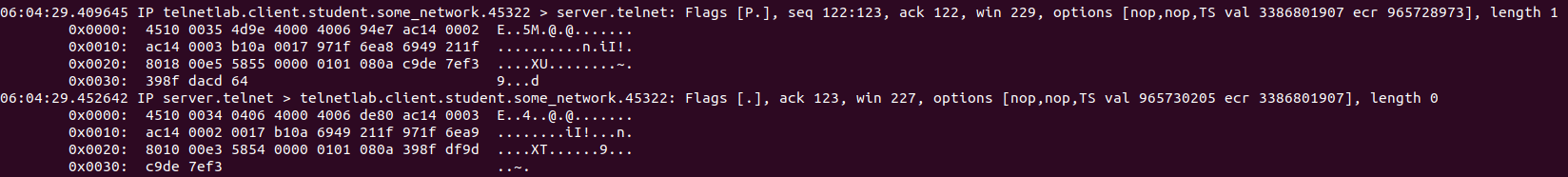
* Tcpdump là câu lệnh thực hiện bắt gói mạng và hiển thị gói mạng. Trong đó:
* -i là trường/giao diện mạng muốn theo dõi, ở đây là eth0 thường là bắt gói tin từ Client đến Server
* -X để hiển thị gói mạng dưới dạng hex và ASCII
* tcp là bộ lọc chỉ lấy gói tin giao tiếp bằng giao thức tcp.



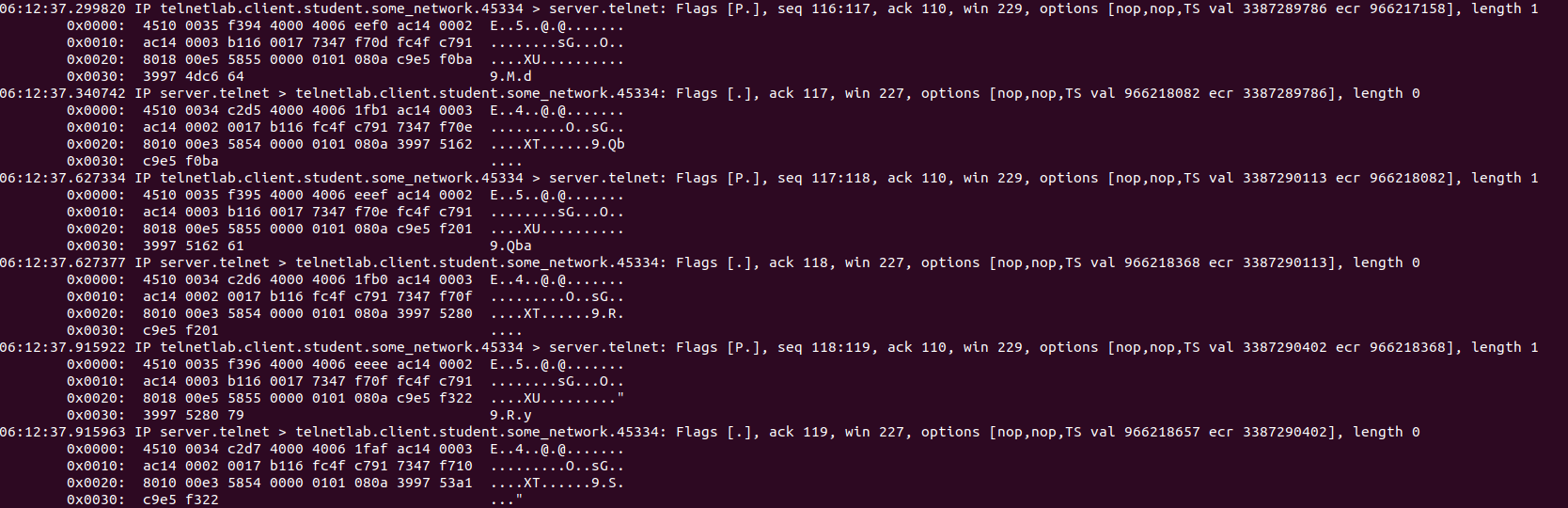
* Ta thấy lưu lượng mạng là 262144 bytes



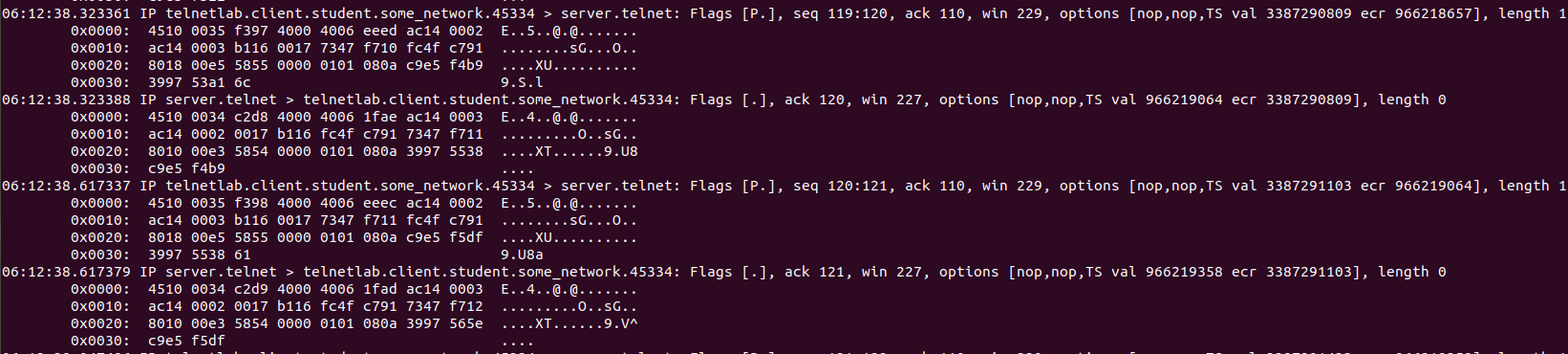
* Tiếp tục trên máy khách bắt đầu phiên telnet với câu lệnh “telnet 172.20.0.3”, khi có yêu cầu login, nhập tài khoản là “ubuntu”, đối với mật khẩu hãy nhập “daylamatkhau”, gõ từng kĩ tự và quan sát terminal của máy chủ.
* Ta biết rằng mật khẩu sai, nhưng trên terminal máy chủ hiện rõ mật khẩu sai mà ta vừa gõ.
* Đây là 2 gói ack sau khi ta nhấn chữ d trong “daylamatkhau”



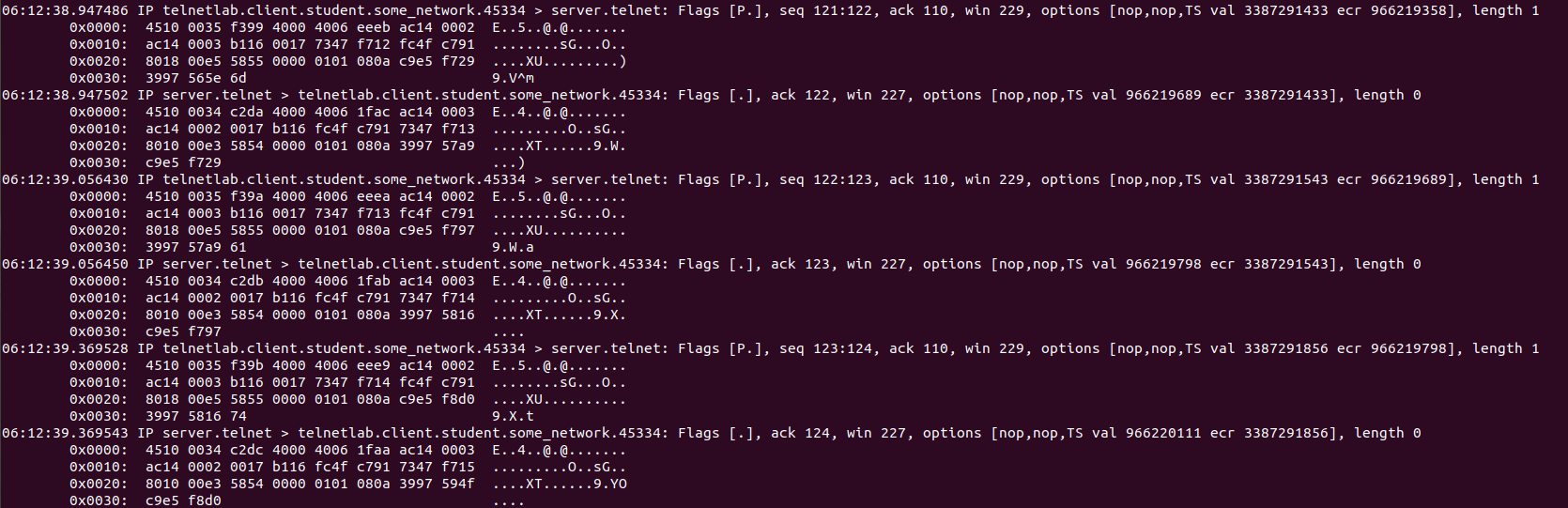
* Tương tự vậy ta có :

“day”

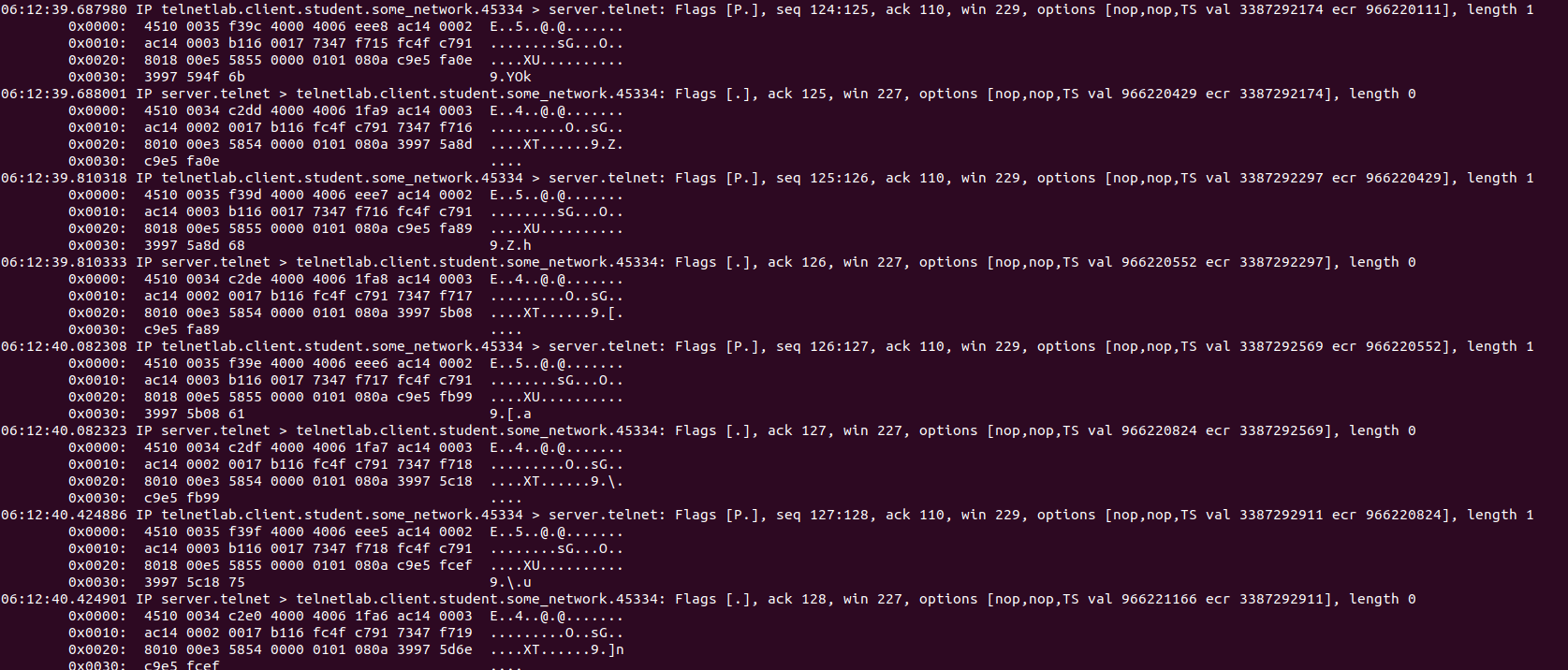
“la”



“mat”



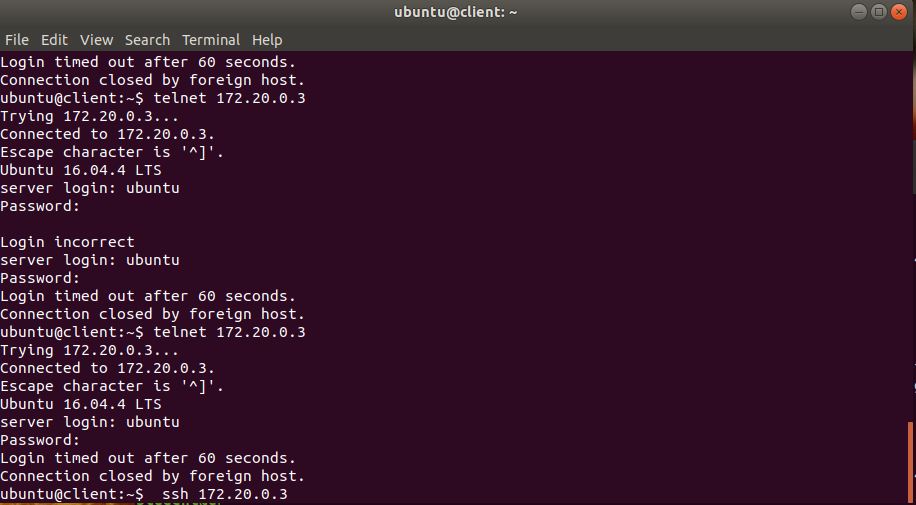
“khau”



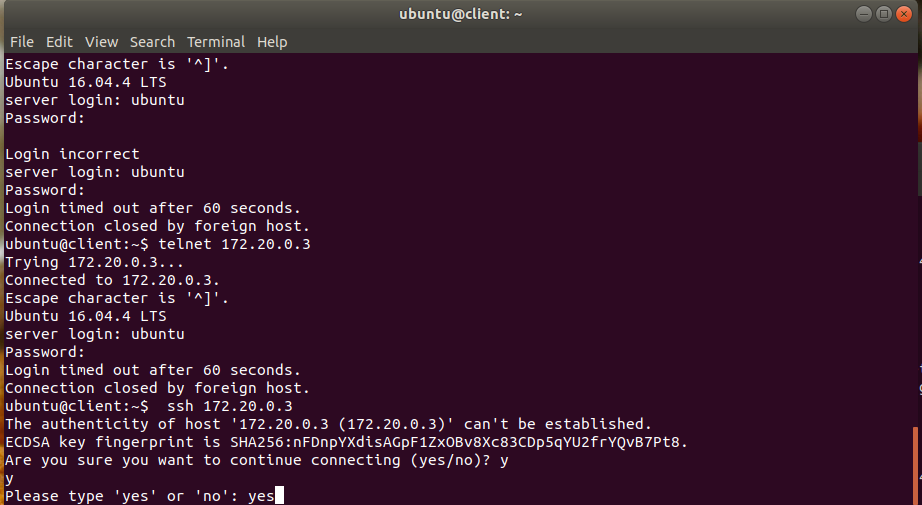
- Mật khẩu bị lộ trên lưu lượng mạng. Mạng telnet đã xuất hiện sự tương tác giữa Client với Server, từng bước nhập dữ liệu đều bị hiển thị trên lưu lượng mạng

1. **Thực hiện ssh từ máy khách vào máy chủ và đọc dữ liệu trên máy chủ**

* Trên máy khách sử dụng ssh để kết nối với máy chủ thông qua địa chỉ IP: 172.20.0.3. Gõ câu lệnh “ssh 172.20.0.3”.



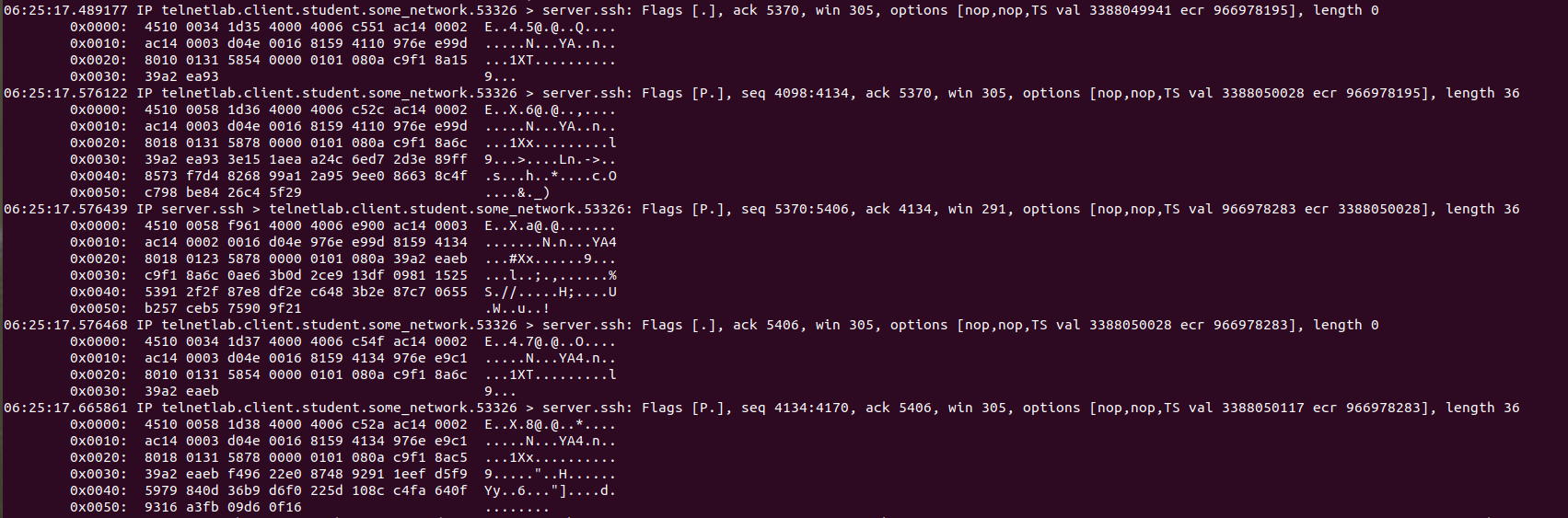
* Chọn yes và tiếp tục

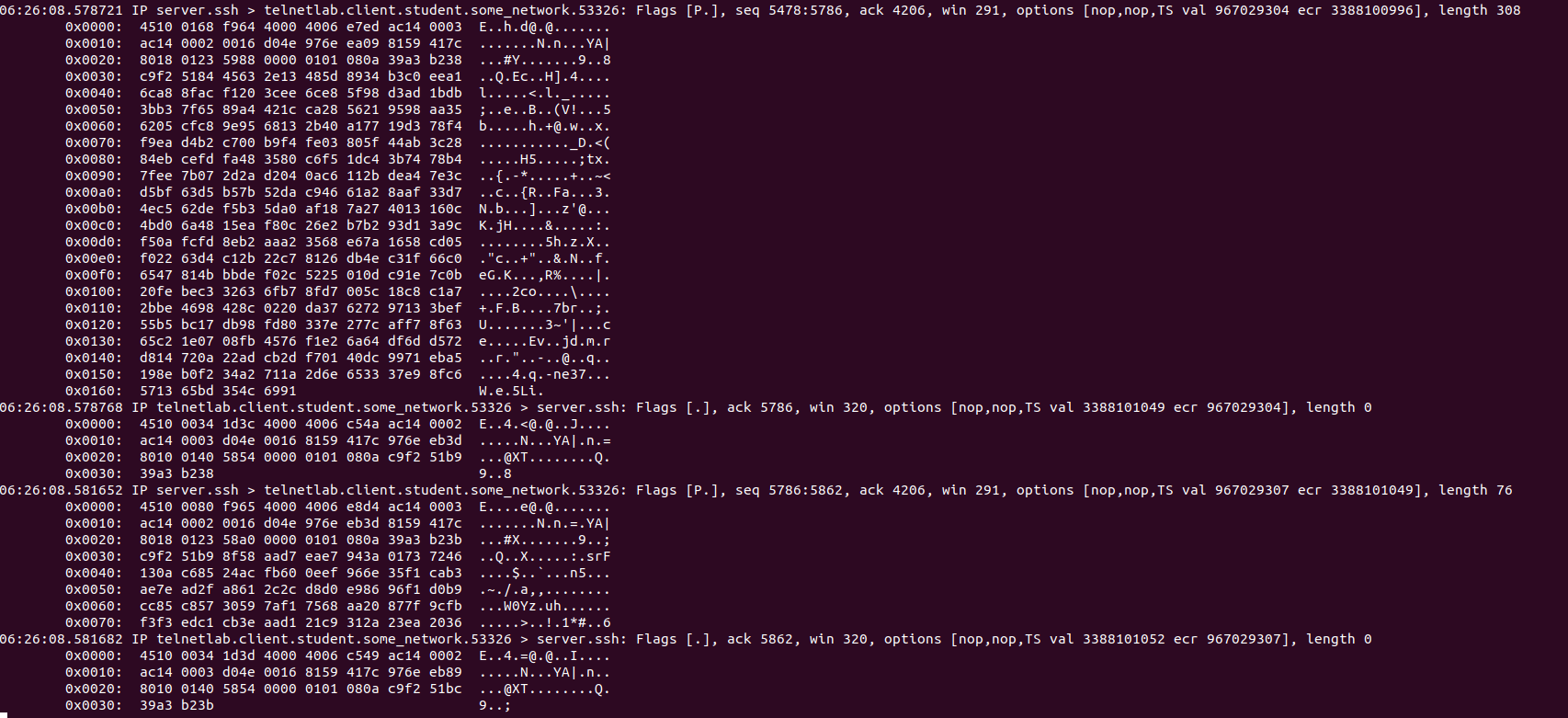


* Sau khi đăng nhập vào máy chủ, thực hiện việc đọc tệp có sẵn chứ đoạn mật mã của sinh viên, sử dụng câu lệnh “cat filetoview.txt”.
* Nhận thấy rằng khi sử dụng ssh đến Server, Server sẽ sử dụng một mã khóa tên ECDSA key để xác thực người dùng ssh đến. Khóa này sẽ mã hóa mật khẩu theo 1 key cho sẵn. Vậy nên khi kiểm tra lưu lượng mạng đường truyền, ta sẽ không thấy mật khẩu bị lộ.

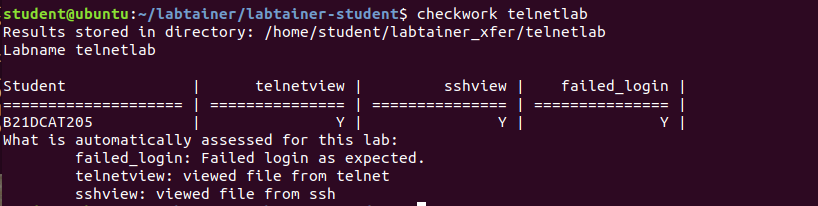


* Quan sát ta không thấy hiện mật khẩu



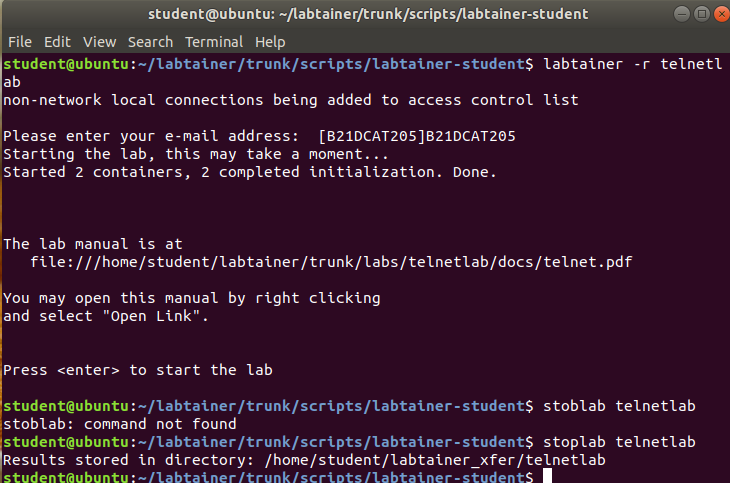


* Quan sát kết quả hiển thị của tcpdump và chú ý rằng không thấy mật khẩu xuất hiện trong đó.
* Chạy lệnh checkwork telnetlab để xem ta đã hoàn thành tất cả các yêu cầu đưa ra hay chưa.Ta thấy tất cả các yêu cầu đã được thực hiện

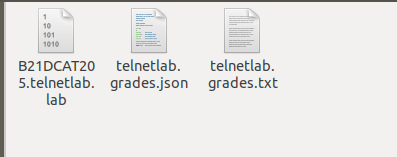


* Thoát khỏi phiên ssh trên máy khách thông qua lệnh “exit”.
* Kết thúc bài lab: trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab:

“stoplab telnetlab”.



* Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.



* Kết quả:

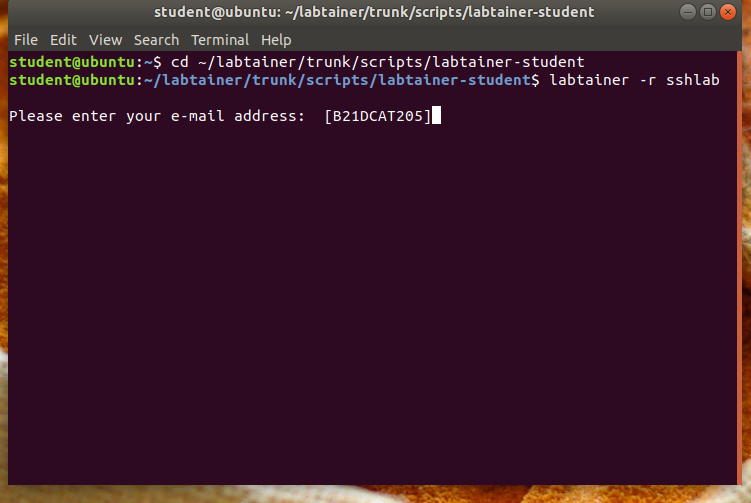


1. **Kết luận:**

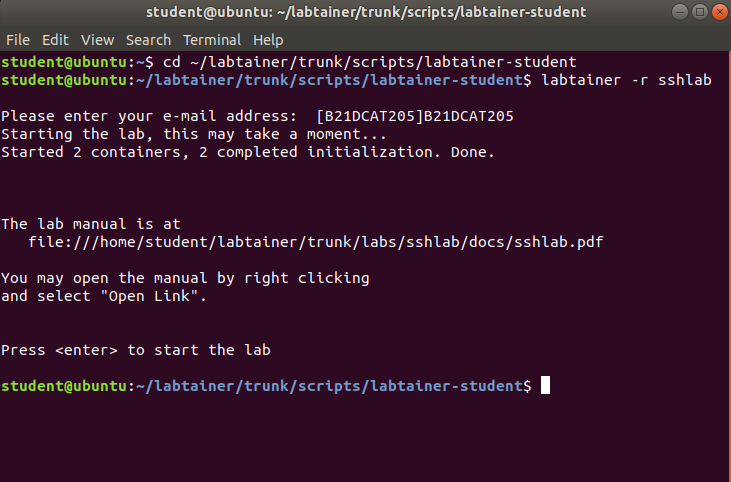
* Truy nhập từ xa từ máy khách đến máy chủ bằng telnet sẽ không an toàn do server không sử dụng key để xác thực người dùng , do đó mật khẩu sẽ bị lộ, thậm chị cả tài khoản.
* Ssh mã hóa đầu vào nên khi nhập, dữ liệu hiện trên đường truyền lưu lượng bị thay đổi (mã hóa).
* Đối với việc truy nhập từ xa từ máy khách đến máy chủ bằng ssh, Server sẽ sử dụng một mã khóa tên ECDSA key để xác thực người dùng ssh đến. Khóa này sẽ mã hóa mật khẩu theo 1 key cho sẵn. Vậy nên khi kiểm tra lưu lượng mạng đường truyền, ta sẽ không thấy mật khẩu bị lộ.

1. **Bài thực hành: cách tạo khóa và sử dụng ssh**

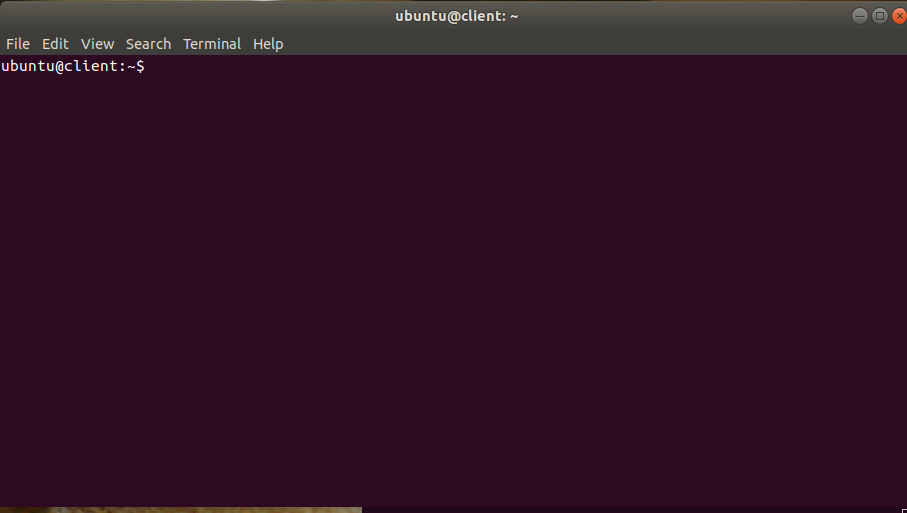
* Vào terminal, gõ: cd ~/labtainer/trunk/scripts/labtainer-student
* Sau đó gõ: labtainer -r sshlab để bắt đầu khởi động bài lab.
* Tiến hành nhập e-mail là mã sinh viên B21DCAT205



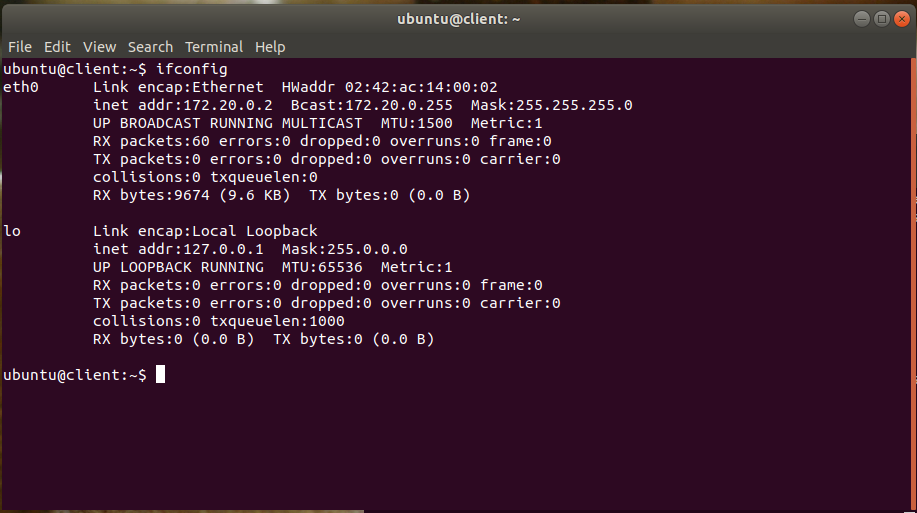
* Sau đó ấn enter



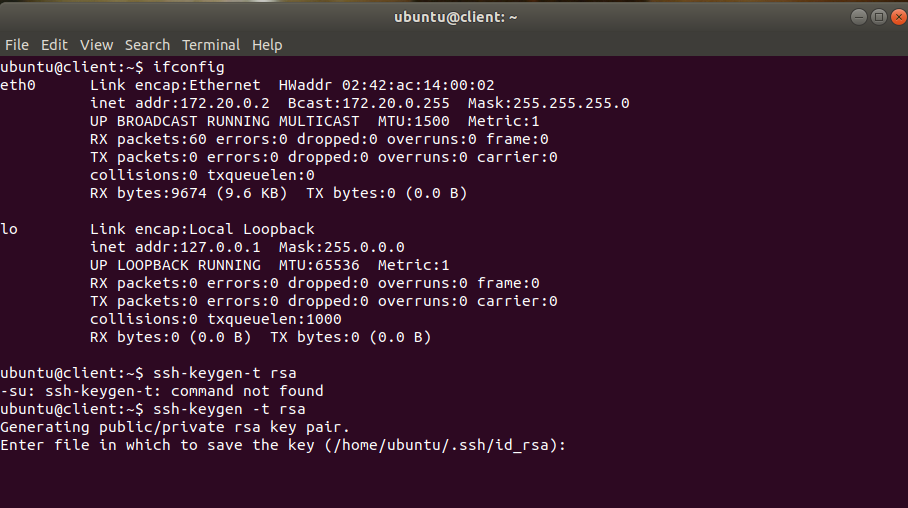
* Sau đó trên màn hình hiện thêm 1 terminal của máy khách



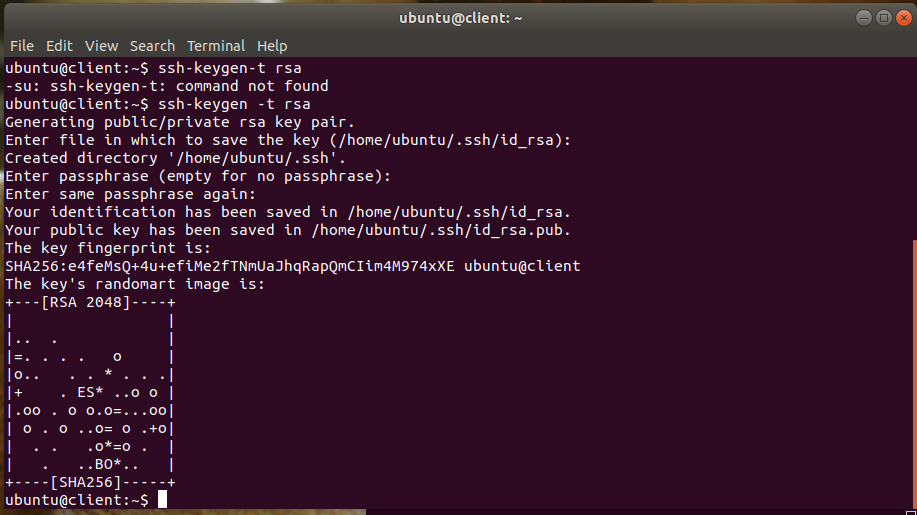
* Trên terminal máy khách client sử dụng lệnh ifconfig, địa chỉ IP sẽ nằm sau “inet adddr:”



* Trên máy khách client Sử dụng câu lệnh “ssh-keygen –t rsa” để tạo cặp khóa bất đối xứng sử dụng thuận toán RSA.



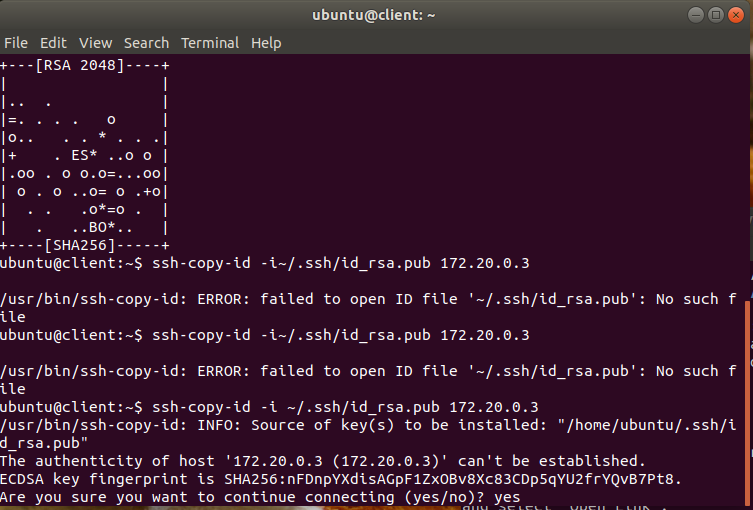
* Trong phần cài đặt ssh tiếp theo, sử dụng vị trí file mặc định và không điền gì cả để không sử dụng passphrase.
* Khóa riêng của client được lưu ở file “id\_rsa”, còn khóa công khai của client được lưu ở file “id\_rsa.pub”.



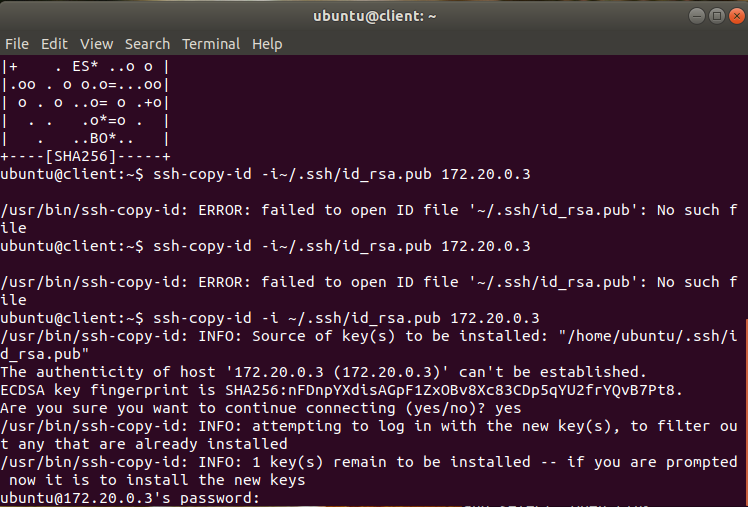
* Biết địa chỉ IP của server là 172.20.0.3, cần phải lưu khóa công khai lên server để server dùng nó mở tin nhắn mã hóa từ client. Trên terminal client đánh câu lệnh sau:

“ssh-copy-id -i ~/.ssh/id\_rsa.pub 172.20.0.3".

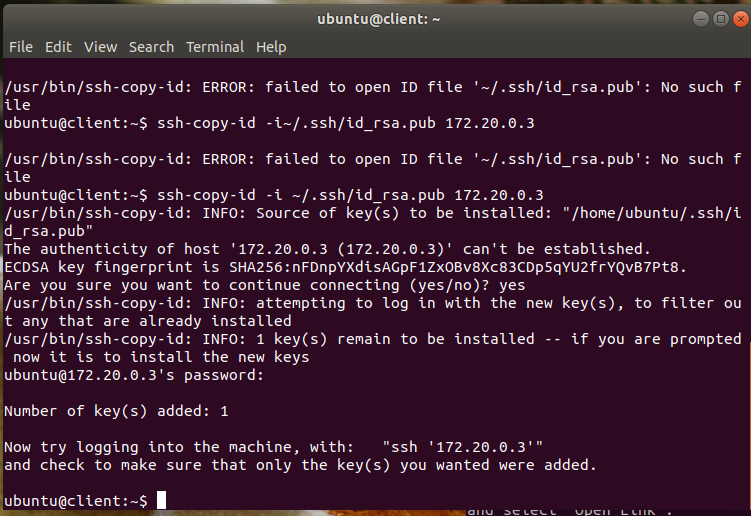
* Câu lệnh trên sử dụng để lưu khóa công khai của Client lên Server
* Khi ta chạy câu lệnh ssh-copy-id -i ~/.ssh/id\_rsa.pub 172.20.0.3” nó sẽ thực hiện các công việc kết nối SSH đến máy chủ 172.20.0.3 với tên người dùng Client và xác thực bằng mật khẩu ban đầu (nếu có). Tạo thư mục .ssh trên máy chủ nếu nó chưa tồn tại. Sao chép nội dung của id\_rsa.pub và thêm vào tệp .ssh/authorized\_keys trên Server. Điều này cho phép bạn xác thực vào Server bằng cách sử dụng khóa công khai từ Client mà không cần mật khẩu.



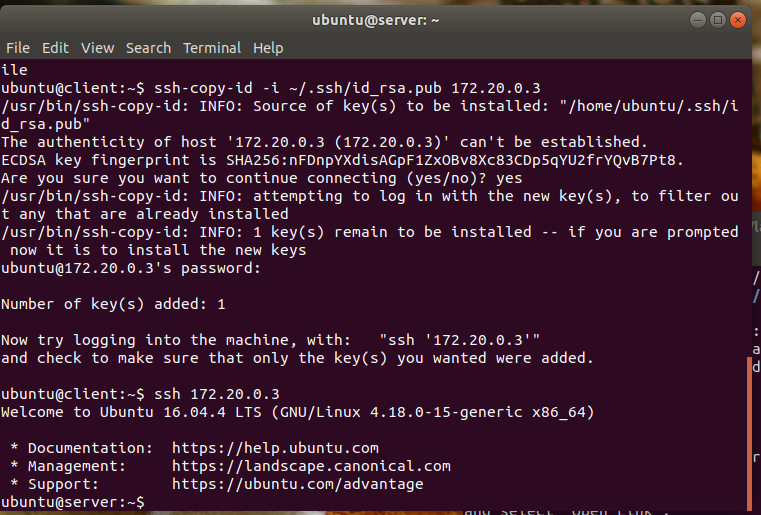
* Tiếp tục ấn yes -> enter



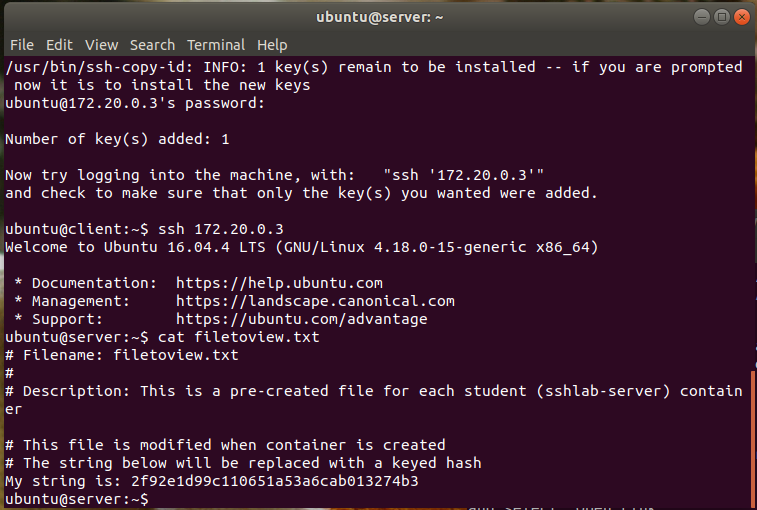
* Nhập mật khẩu của máy chủ server là: “ubuntu”



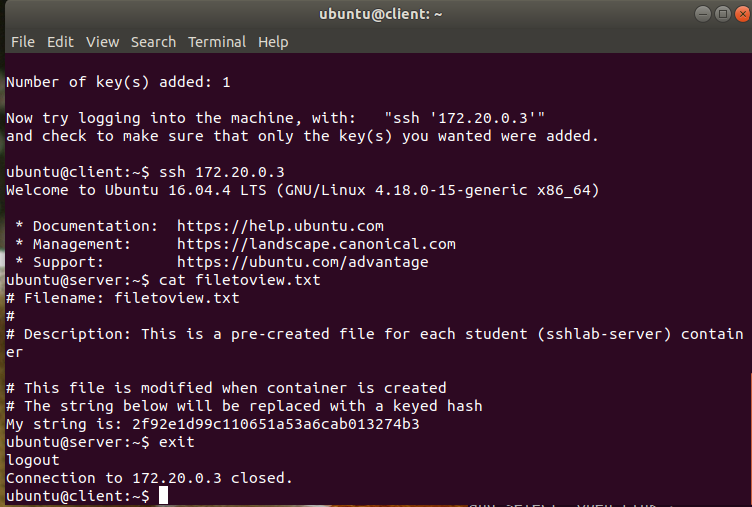
* Thực hiện ssh đến máy chủ server:



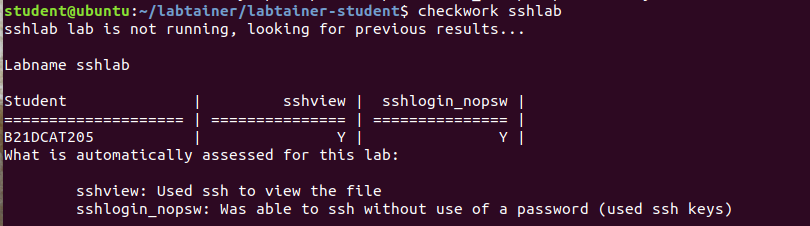
* Tìm và đọc tệp , sử dụng câu lệnh “cat filetoview.txt”



* Thoát khỏi server: exit

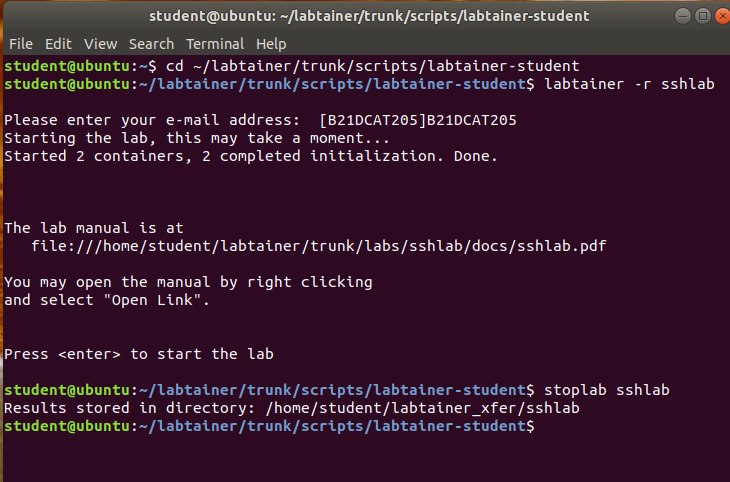


* Checkwork để xem mình làm đủ hết các yêu cầu chưa.

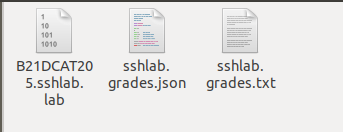


* Kết thúc bài lab: trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab:

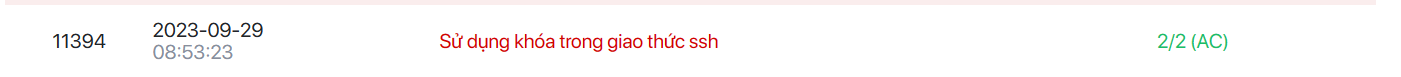
stoplab sshlab



* File kết quả:



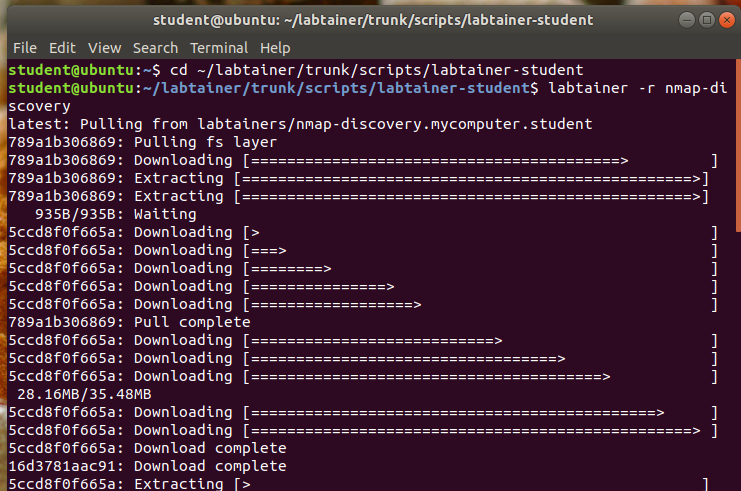
* Kết quả:



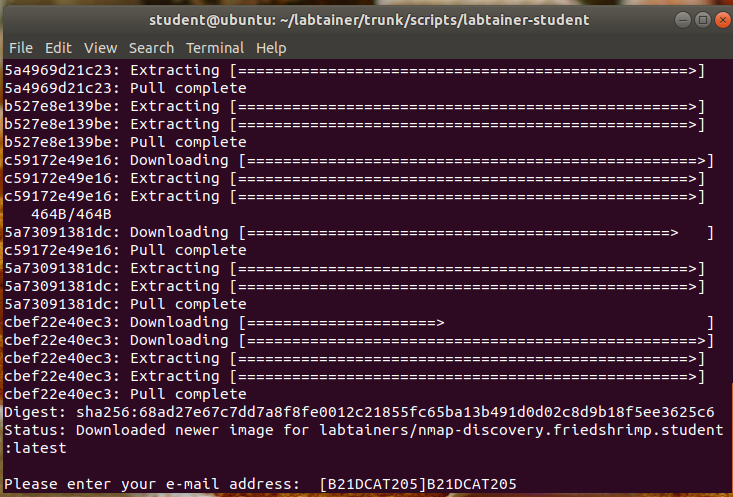
* Kết luận: Khi ta tạo ra cặp khóa tạo cặp khóa bất đối xứng sử dụng thuận toán RSA, điều này cho phép ta xác thực vào Server bằng cách sử dụng khóa công khai từ Client mà không cần mật khẩu.

1. **Bài thực hành: phát hiện các lỗ hổng bảo mật sử dụng công cụ rà quét**

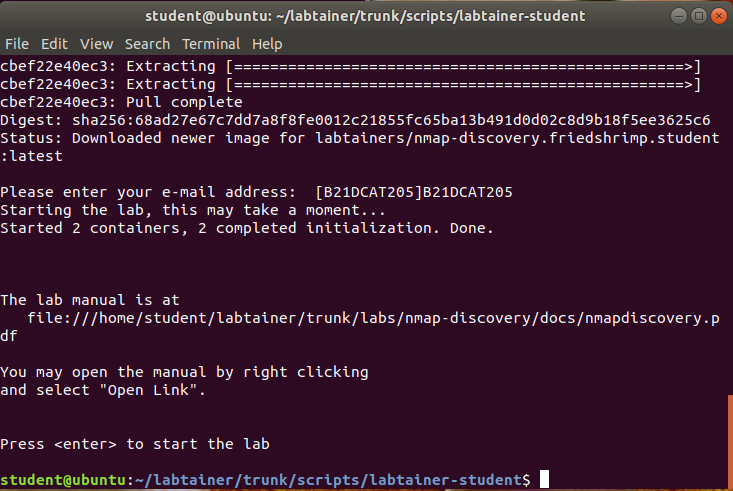
* Vào terminal, gõ: cd ~/labtainer/trunk/scripts/labtainer-student
* Sau đó gõ, labtainer -r nmap-discovery



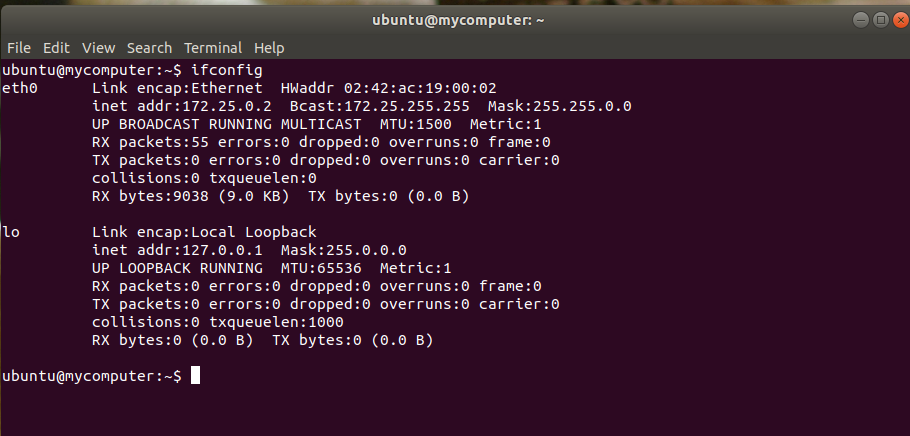
* Sau khi tải xong ta thực hiện nhập email là mã sinh viên B21DCAT205



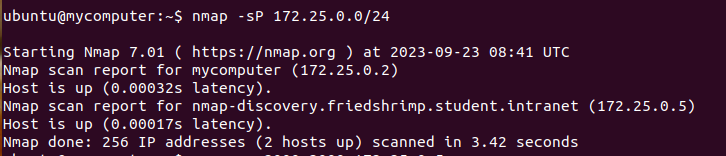
* Sau đó ấn enter



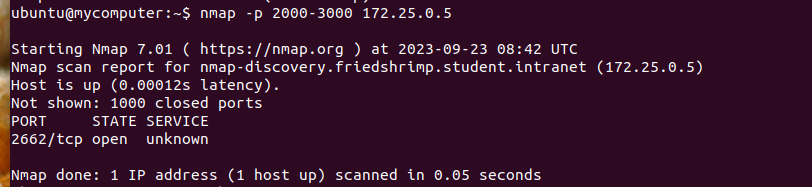
* Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy khách: mycomputer, một cái là đại diện cho máy chủ: friedshrimp.Biết rằng 2 máy nằm cùng mạng LAN
* Trên terminal mycomputer sử dụng lệnh “ifconfig”, xác định địa chỉ IP và địa chỉ mạng LAN: Ta xác định được đại chỉ IP là 172.25.0.2, đối với địa chỉ mạng Lan tương ứng sẽ là 172.25.0.0/24.
* Lý do cần sử dụng địa chỉ mạng LAN 172.25.0.0/24 trong lệnh nmap là vì nó xác định dải địa chỉ IP mà bạn muốn quét để tìm các máy hoạt động trong mạng LAN của bạn. Dải này bao gồm tất cả các địa chỉ IP từ 172.25.0.1 đến 172.25.0.254 (vì /24 cho biết rằng 24 bit đầu tiên của địa chỉ IP là mạng con), và ta muốn tìm các máy hoạt động trong dải này.



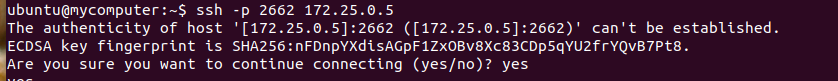
* Trên máy khách mycomputer sử dung nmap để tìm ra địa chỉ IP của máy friedshrimp vì chúng cùng nằm trong mạng LAN: nmap –sP <IP mạng LAN>. Với ip mạng LAN là 172.25.0.0/24.



* Ta xác đinh được ip của máy friedshrimp là 172.25.0.5
* Tiếp tục sử dụng nmap để tìm cổng dịch vụ đang mở trên máy friedshrimp biết rằng cổng (port) nằm từ 2000-3000.



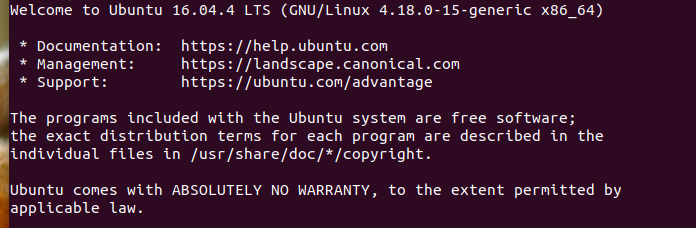
* Sau khi xác định được cổng ssh đang mở. Sử dụng ssh để truy cập vào máy chủ. Tên máy chủ và mật khẩu là: ubuntu.
* Sử dụng câu lệnh: ssh –p <port> <IP friedshrimp>
* Với port là 2662 và ip friedshrimp là 172.25.0.5
* Sau đó enter - > nhập yes -> enter



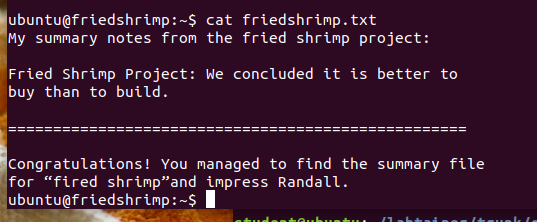
* Nhập mật khẩu ubuntu



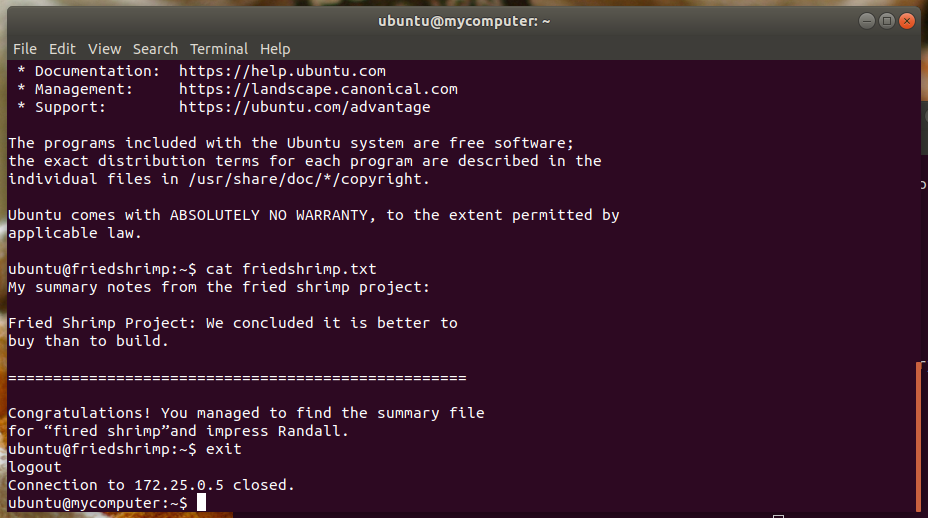
- Thành công đăng nhập vào máy Friendshrimp



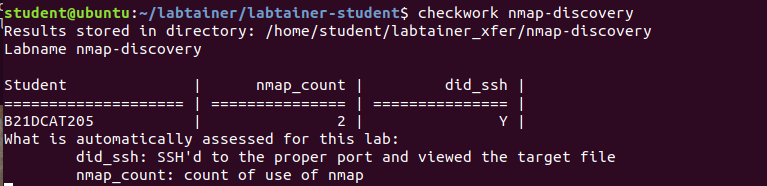
* Đọc file friedshrimp.txt sử dụng câu lệnh: cat friedshrimp.txt



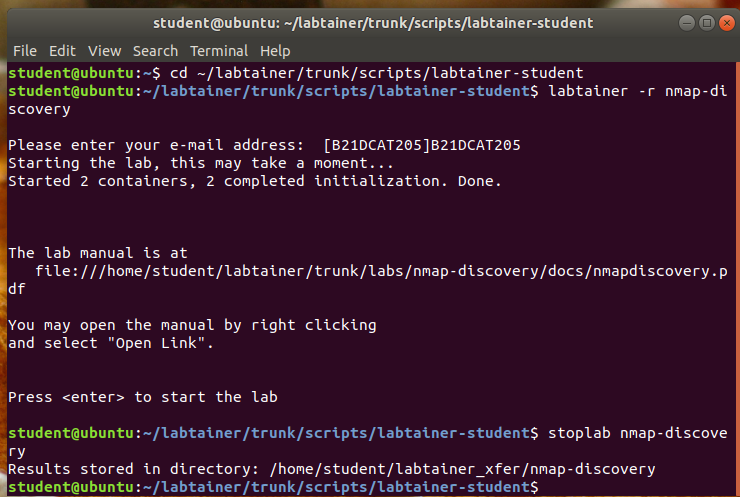
* Nhập “exit” để hủy kết nối.



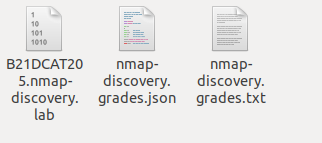
* Checkwork xem mình đã hoàn thành yêu cầu chưa



* Kết thúc bài lab: trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab: “stoplab nmap-discovery”.



* Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab. Sinh viên cần nộp file .lab để chấm điểm.



* Kết quả:



* Kết luận: Sử dụng công cụ nmap có thể giúp tìm địa chỉ IP của máy trong cùng mạng LAN, sau đó tìm cổng dịch vụ đang mở trên máy đó, rồi ta có thể truy nhập bằng ssh để rà quét lỗ hổng.