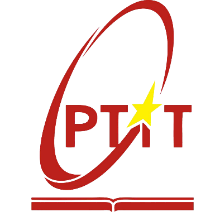
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

-------🙞🙜🕮🙞🙜-------



**Báo cáo xây dựng lab trên nền tảng labtainer**

**Chủ đề:** Nghiên cứu và xây dựng các bài thực hành dựa trên khung Mitre Att&ck trong kiểm thử xâm nhập

**Lab**: T1087 - Account Discovery I

Sinh viên thực hiện: Ngô Quang Dũng - B20DCAT029

Giảng viên hướng dẫn: TS. Nguyễn Ngọc Điệp

**Hà Nội - 2024**

**MỤC LỤC**

[MỤC LỤC 1](#_gjdgxs)

[DANH MỤC CÁC HÌNH VẼ 2](#_30j0zll)

[DANH MỤC CÁC BẢNG BIỂU 2](#_1fob9te)

[DANH MỤC CÁC TỪ VIẾT TẮT 3](#_3znysh7)

[1.1 Giới thiệu chung về bài thực hành 4](#_2et92p0)

[1.2 Nội dung và hướng dẫn bài thực hành 4](#_tyjcwt)

[**1.2.1** Mục đích 4](#_3dy6vkm)

[**1.2.2** Yêu cầu đối với sinh viên 4](#_1t3h5sf)

[**1.2.3** Nội dung thực hành 4](#_4d34og8)

[1.3 Phân tích yêu cầu bài thực hành 5](#_2s8eyo1)

[1.4 Thiết kế bài thực hành 5](#_17dp8vu)

[1.5 Cài đặt và cấu hình các máy ảo 8](https://docs.google.com/document/d/1hfn2yF06gobzwfBq4KR7ymxMCejHgIZDlf25SwvjSpI/edit#heading=h.1ksv4uv)

[1.6 Tích hợp và triển khai 10](#_1ci93xb)

[***1.6.1*** Docker Hub 10](#_3whwml4)

[***1.6.2*** Github 10](#_1pxezwc)

[1.7 Thử nghiệm và đánh giá 11](#_3o7alnk)

[TÀI LIỆU THAM KHẢO 13](#_vx1227)

**DANH MỤC CÁC HÌNH VẼ**

[Hình 1 Giao diện Labedit của bài lab](#_44sinio) 6

[Hình 2 Cài đặt phần Result](#_2jxsxqh) 7

[Hình 3 Dockerfiles của máy victim](https://docs.google.com/document/d/1hfn2yF06gobzwfBq4KR7ymxMCejHgIZDlf25SwvjSpI/edit#heading=h.z337ya) 7

[Hình 4 Dockerfiles của client](#_1y810tw) 8

[Hình 5 Add và commit bài lab](#_4i7ojhp) 8

[Hình 6 Đẩy các vùng chứa lên dockerhub](#_2xcytpi) 8

[Hình 7 Tạo imodule.tar chứa bài thực hành](#_2bn6wsx) 9

[Hình 8 Các vùng chứa được đẩy lên dockerhub](#_qsh70q) 9

[Hình 9 Tạo file Imodule.tar](#_3as4poj) 9

[Hình 10 File imodule.tar chứa bài thực hành](#_49x2ik5) 9

[Hình 11 Đẩy file imodule.tar lên github 1](#_2p2csry)0

[Hình 12 IP của máy server 1](#_147n2zr)0

[Hình 13 Client dò mật khẩu các tài khoản trên server 1](#_23ckvvd)1

[Hình 14 Trả lời task1 1](#_ihv636)1

[Hình 15 Client truy cập tài khoản user trên server qua SSH](#_32hioqz) 11

[Hình 16 Tạo file trên server 12](#_1hmsyys)

[Hình 17 Checkwork bài lab 13](#_2grqrue)

**DANH MỤC CÁC BẢNG BIỂU**

[Bảng 1. Bảng Result](https://docs.google.com/document/d/1hfn2yF06gobzwfBq4KR7ymxMCejHgIZDlf25SwvjSpI/edit#heading=h.3rdcrjn) 6

**DANH MỤC CÁC TỪ VIẾT TẮT**

| **Từ  viết tắt** | **Thuật ngữ tiếng Anh/Giải thích** | **Thuật ngữ tiếng Việt/Giải thích** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. **Giới thiệu chung về bài thực hành**

Bài lab này giúp sinh viên tìm hiểu và thực hành kỹ thuật khám phá tài khoản trên hệ thống mục tiêu. Trong bài lab này, sinh viên sẽ học cách sử dụng công cụ để thực hiện tấn công nhằm tìm ra mật khẩu của các tài khoản trên máy chủ mục tiêu. Sau khi mật khẩu bị bẻ khóa, sinh viên sẽ sử dụng SSH để đăng nhập vào máy chủ và có thể thực hiện các hành động tiếp theo.

* 1. **Nội dung và hướng dẫn bài thực hành**
     1. ***Mục đích***

Bài lab này giúp sinh viên sử dụng công cụ để dò mật khẩu, qua đó nâng cao nhận thức về các phương pháp bảo vệ hệ thống, như sử dụng mật khẩu mạnh và cấu hình hệ thống an toàn để ngăn chặn các cuộc tấn công từ xa.

* + 1. ***Yêu cầu đối với sinh viên***

Hiểu cơ bản về cách sử dụng công cụ ví dụ như hydra.

* + 1. ***Nội dung thực hành***

Khởi động bài lab:

Vào terminal, gõ:

*startlab account-discovery1*

*(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công: ***client***, một cái là đại diện cho máy victim: ***server***.

Sử dụng Hydra để dò mật khẩu các tài khoản trên server

*hydra -l ubuntu -P list.txt ssh://172.21.0.20*

Sau khi lấy được tài khoản mật khẩu SSH vào tài khoản trên server

*ssh ubuntu@172.21.0.20*

Thực thi lệnh trên server:

*echo “client hello” > client.txt*

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

*stoplab account-discovery1*

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.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*startlab –r account-discovery1*

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

Bài thực hành gồm 2 máy tính nằm trong cùng mạng LAN. Trong đó 1 máy được gọi là attacker, máy còn lại là victim. Để hoàn thành bài thực hành sinh viên cần sử dụng script để tạo tên miền ngẫu nhiên, truy vấn các DNS từ client và server theo dõi được các truy vấn từ client .

* 1. **Thiết kế bài thực hành**

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker tạo ra 2 container: 1 container mang tên “client” đóng vai trò máy tấn công và 1 container mang tên “server” đóng vai trò máy nạn nhân.

Tạo mạng LAN có cấu hình: 172.21.0.0/24 và gateway: 172.21.0.1

Cấu hình docker gồm có:

Client: lưu cấu hình cho máy tấn công, trong đó gồm có:

Tên máy: client

Địa chỉ trong mạng LAN: 172.21.0.10

Gateway: 172.21.0.1

Server: lưu cấu hình cho máy chủ, trong đó gồm có:

Tên máy: Server

Địa chỉ trong mạng LAN: 172.21.0.20

Gateway: 172.21.0.1

config: lưu cấu hình hoạt động của hệ thống

dockerfiles: mô tả cấu hình của 2 container: client và server, trong đó:

Client: sử dụng các thư viện mặc định hệ thống và cài sẵn curl giúp thực hiện các lệnh và chức năng của tool này.

Server: sử dụng các thư viện mặc định hệ thống cùng với cấu hình tương tự máy attacker trong đó đã cài sẵn các dịch vụ apache.

Các nhiệm vụ cần phải thực hiện để thực hành thành công:

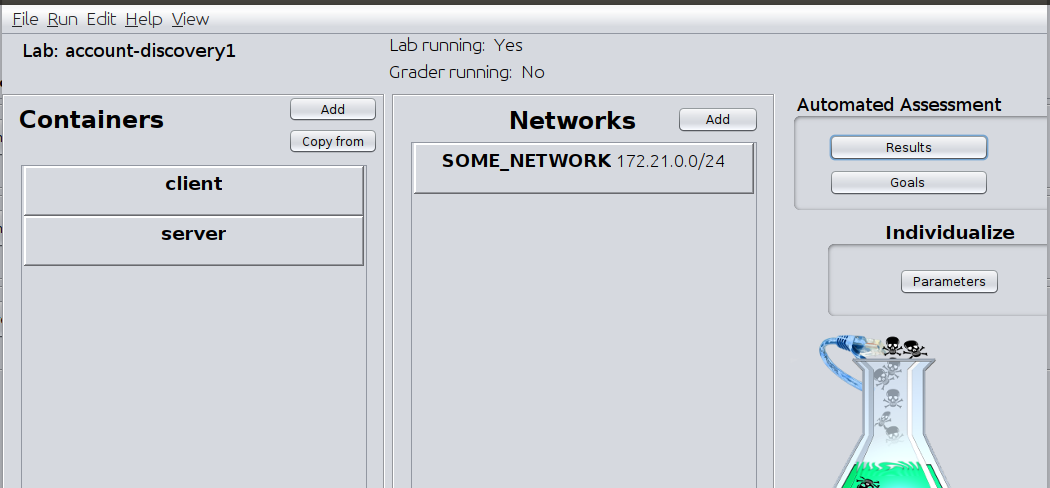
Task 1: Sinh viên cần điền kết quả mật khẩu đã dò được vào result.txt ở client.

Task 2: Sinh viên truy cập được vào tài khoản đã dò được bằng SSH.

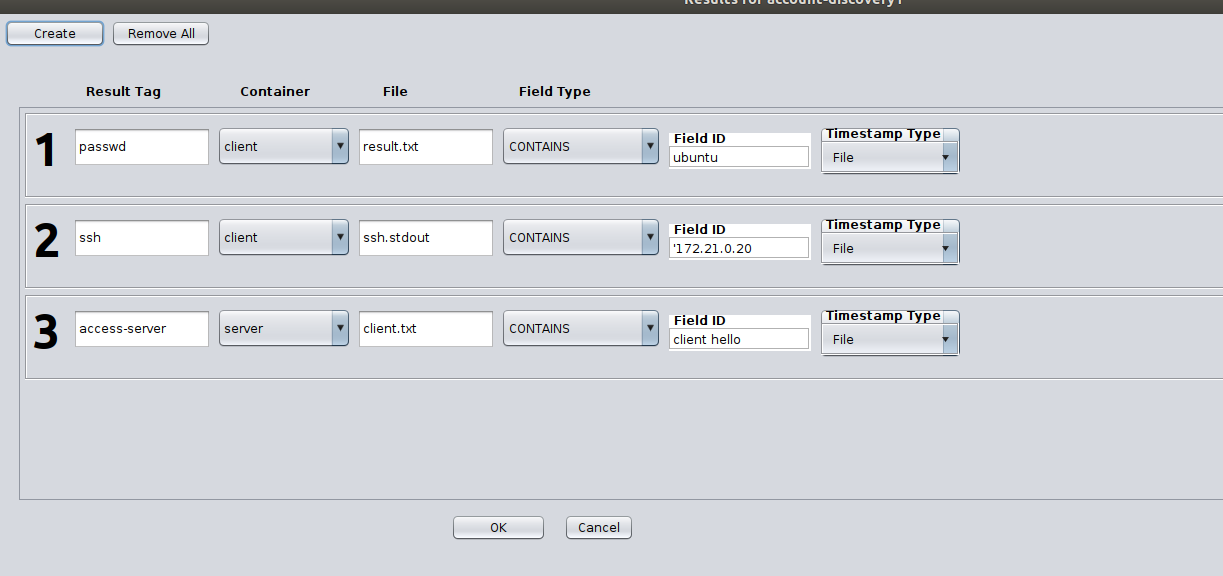
Task 3:Sinh viên thực thi được lệnh và tạo 1 file trên server.

Kết thúc bài lab và đóng gói kết quả.

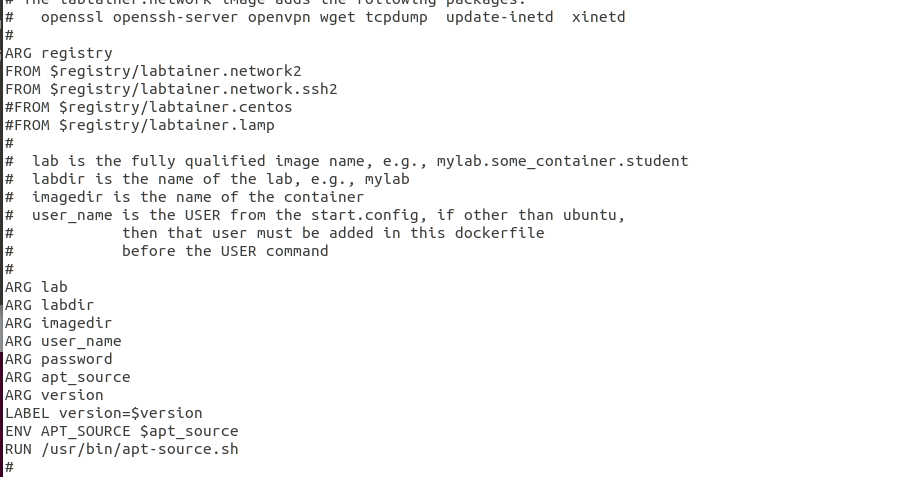
Thiết lập hệ thống mạng sao cho máy attacker và máy victim cùng một mạng LAN.



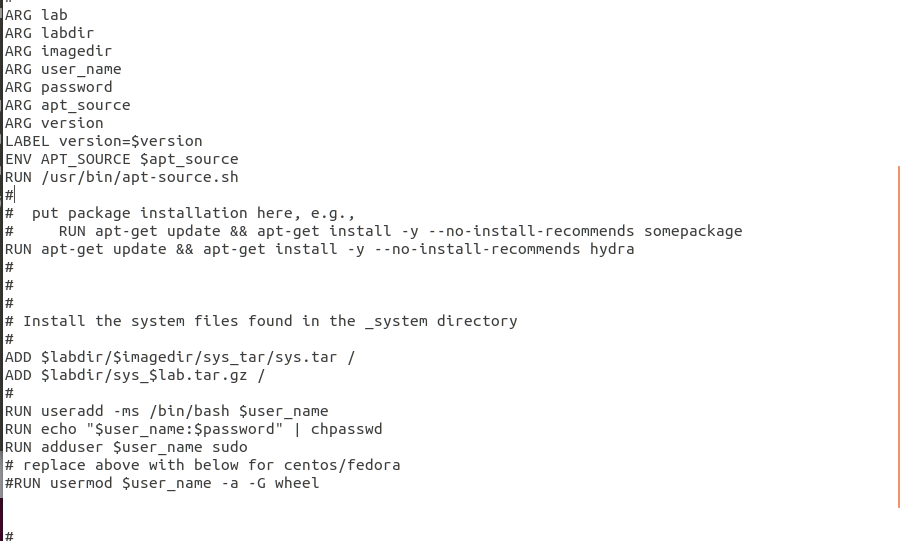
*Hình 1: Giao diện Labedit của bài lab*



*Hình 2: Cài đặt phần Result*



*Hình 3: Dockerfiles của máy victim*



*Hình 4: Dockerfiles của client*

* 1. **Tích hợp và triển khai**

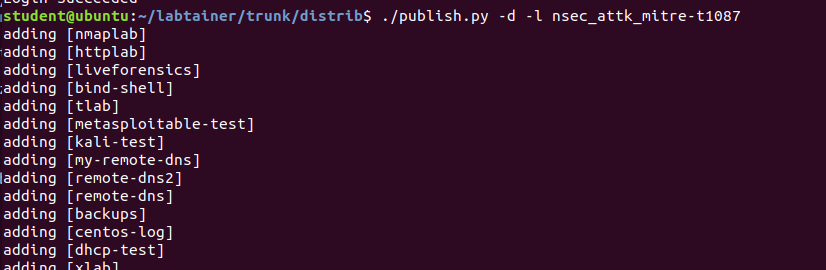
Bài thực hành đã được triển khai như sau:

* + 1. Docker Hub

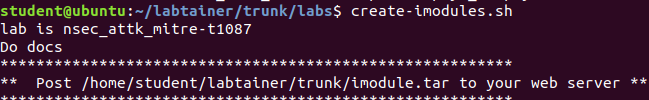
https://hub.docker.com/repositories/dung1604



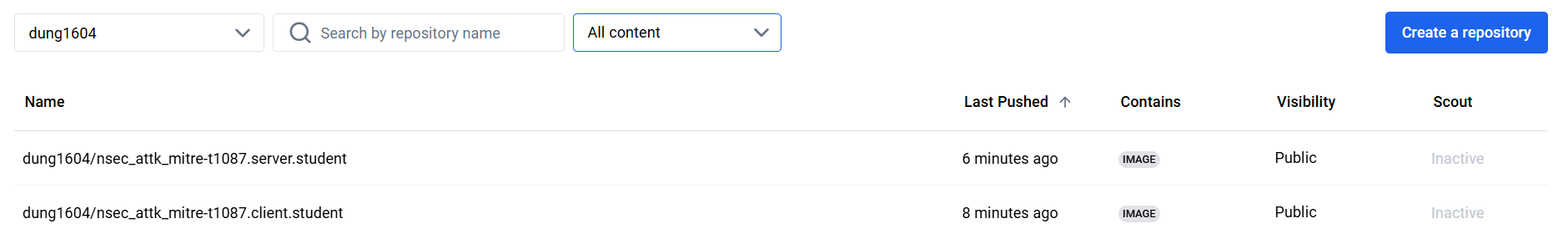
*Hình 5: Add và commit bài lab*



*Hình 6: Đẩy các vùng chứa lên dockerhub*



*Hình 7: Tạo imodule.tar chứa bài thực hành*

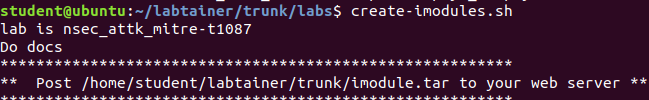


*Hình 8: Các vùng chứa được đẩy lên dockerhub*

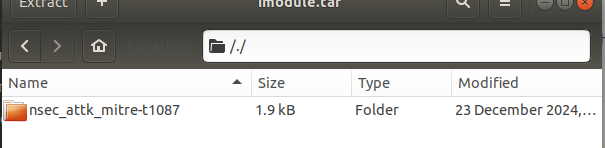
* + 1. Github

https://github.com/DUNG1604/nsec\_attk\_mitre-t1087

Nhập lệnh create-imodules.sh

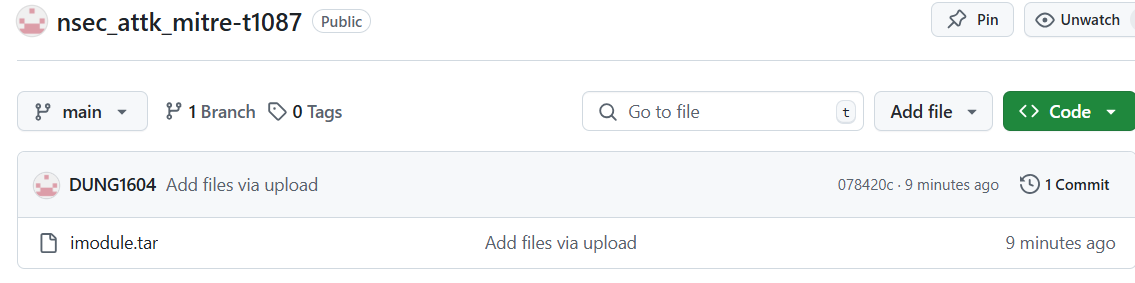


*Hình 9: Tạo file Imodule.tar*



*Hình 10: File imodule.tar chứa bài thực hành*

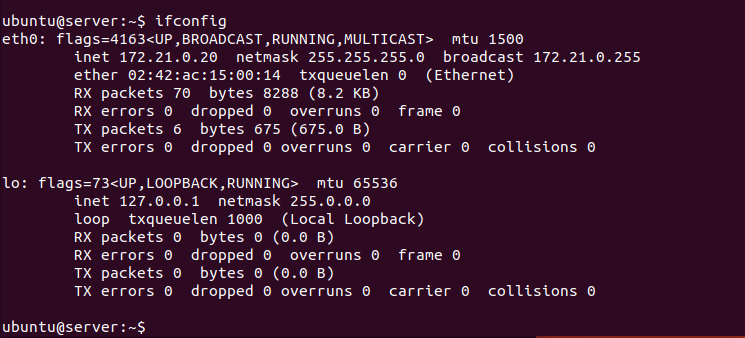
Tạo repo mới để đẩy imodule.tar lên và tạo phần release mới



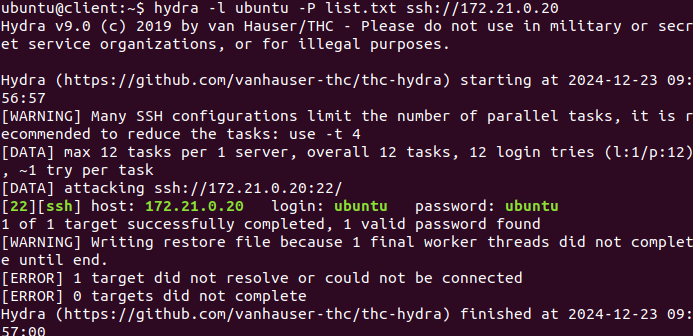
*Hình 11: Đẩy file imodule.tar lên github*

* 1. **Thử nghiệm và đánh giá**

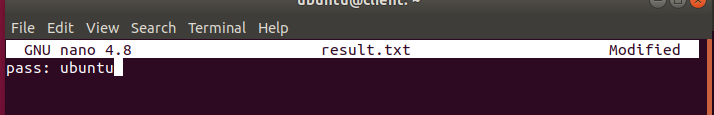
Bài thực hành đã được xây dựng thành công, dưới đây là hình ảnh minh họa về bài thực hành:



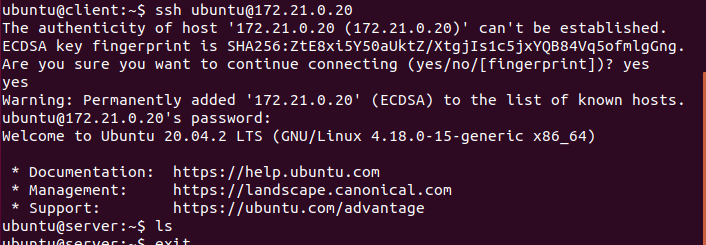
*Hình 12: IP của máy server*



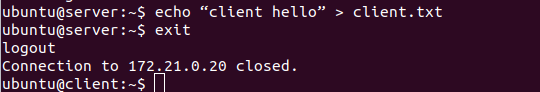
*Hình 13: Client dò mật khẩu các tài khoản trên server*



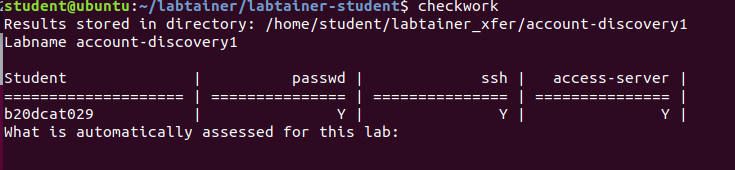
*Hình 14: Trả lời task1*



*Hình 15: Client truy cập tài khoản user trên server qua SSH*



*Hình 16: Tạo file trên server*



*Hình 17: Checkwork bài lab*

**TÀI LIỆU THAM KHẢO**

1. https://attack.mitre.org/techniques/T1087/
2. https://nps.edu/documents/107523844/117289221/labdesigner.pdf/9ab93fc3-7cfe-48f4-987b-2efda8d99346?t=1606868757623