HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484

CA THỰC HÀNH: 01
NHÓM LỚP: 01
TÊN BÀI:
HẠN CHẾ TRUY CẬP SSH BẰNG CÔNG CỤ DENYHOST

Sinh viên thực hiện:

Nguyễn Văn Hùng B22DCAT136

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC 1
DANH MỤC CÁC HÌNH VẼ 2
DANH MỤC CÁC TỪ VIẾT TẮT 3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 4
1.1 Mục đích 4
1.2 Tìm hiểu lý thuyết 4
1.2.1 Giới thiệu 4
1.2.2 Cơ chế hoạt động của Denyhosts 4
1.2.3 Các file quan trọng 4
1.2.3.1 /var/log/auth.log 4
1.2.3.2 /etc/denyhosts.conf 5
1.2.3.3 /etc/hosts.deny 5
1.2.3.4 /etc/hosts.allow 5
1.2.4 Ứng dụng thực tế của DenyHosts 5
CHƯƠNG 2. NỘI DUNG THỰC HÀNH 6
2.1 Chuẩn bị môi trường 6
2.2 Các bước thực hiện 6
2.2.1 Khởi động bài Lab 6
2.2.2 Nhiệm vụ 1: Xem các tệp cấu hình 7
2.2.2.1 Tệp auth.log 7
2.2.2.2 Tệp denyhosts.conf 7
2.2.2.3 Tệp hosts.deny 8
2.2.3 Nhiệm vụ 2: Khóa user hợp lệ bằng bot 8
2.2.4 Nhiệm vụ 3: Khôi phục đăng nhập 9
2.2.5 Nhiệm vụ 4: Khóa user không hợp lệ 10
CHƯƠNG 3. KẾT QUẢ THỰC HÀNH 12
TÀI LIỆU THAM KHẢO 13

DANH MỤC CÁC HÌNH VẼ

Hình 1 . Khởi động bài Lab 6
Hình 2 . Các terminal hiển thị 7
Hình 3 . SSH từ máy khách và xem log từ máy chủ 7
Hình 4 . Xem tệp denyhosts.conf 8
Hình 5 . Xem tệp hosts.deny 8
Hình 6 . Chạy bot tấn công 9
Hình 7 . Thử SSH sau khi bị chặn 9
Hình 8 . Thêm IP máy khách vào whitelist 10
Hình 9 . Thử SSH lại và thành công 10
Hình 10 . Thử SSH với tài khoản người dùng lạ 11
Hình 11 . Kết quả bài thực hành 12

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ tiếng Anh/Giải thích	Thuật ngữ tiếng Việt/Giải thích
SSH	Secure Shell	Giao thức bảo mật để thiết lập kết nối từ xa

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

Khám phá việc sử dụng tiện ích denyhosts trên một máy chủ SSH để giới hạn số lần đăng nhập SSH từ một địa chỉ IP.

1.2 Tìm hiểu lý thuyết

1.2.1 Giới thiệu

SSH, hay Secure Shell, là một giao thức mạng cho phép một máy tính kết nối an toàn với một máy tính khác qua mạng không bảo mật như internet, bằng việc có một thỏa thuận chung về cách thức liên lạc. SSH là một giao thức application layer, là layer thứ 7 của mô hình OSI.

SSH thường được thực hiện bằng mô hình client-server. Một máy tính được gọi là SSH client và một máy khác hoạt động như SSH server hoặc host.

DenyHosts là một phần mềm bảo mật mã nguồn mở dùng để bảo vệ máy chủ SSH khỏi các cuộc tấn công brute-force. Nó giám sát file log của hệ thống để phát hiện các nỗ lực đăng nhập SSH không thành công (sai tên người dùng hoặc mật khẩu), sau đó tự động chặn địa chỉ IP đáng ngờ để ngăn chặn các cuộc tấn công tiếp theo.

1.2.2 Cơ chế hoạt động của Denyhosts

DenyHosts hoạt động theo các bước sau:

- Giám sát log: Theo dõi file log đăng nhập hệ thống để phát hiện các lần đăng nhập thất bại, thường là:
    - /var/log/auth.log (trên Ubuntu/Debian)
    - /var/log/secure (trên CenOS/RHEL)
- Phân tích và đếm: Đếm số lần đăng nhập thất bại từ mỗi địa chỉ IP:
    - User hợp lệ (valid user): DENY_THRESHOLD_VALID
    - User không hợp lệ (invalid user): DENY_THRESHOLD_INVALID
- Áp dụng quy tắc: Khi số lần đăng nhập thất bại vượt quá ngưỡng cấu hình:
- Thêm IP vào /etc/hosts.deny
- Có thể cập nhật iptables để chặn IP
- Khi một địa chỉ IP bị chặn, mọi kết nối SSH tiếp theo từ IP đó sẽ bị từ chối tự động.

1.2.3 Các file quan trọng

1.2.3.1 /var/log/auth.log

- File log ghi lại tất cả các sự kiện liên quan đến xác thực
- Chứa thông tin về:
    - Đăng nhập thành công/thất bại

- User/IP thực hiện đăng nhập
- Thời gian đăng nhập

1.2.3.2 /etc/denyhosts.conf

- File cấu hình chính của DenyHosts với các tham số quan trọng:
  - DENY_THRESHOLD_INVALID: Số lần đăng nhập sai tối đa cho user không tồn tại (mặc định thường là 5)
  - DENY_THRESHOLD_VALID: Số lần đăng nhập sai tối đa cho user hợp lệ (mặc định thường là 10)
  - DENY_THRESHOLD_ROOT: Số lần đăng nhập sai tối đa cho root
  - DAEMON_SLEEP: Thời gian (giây) giữa các lần kiểm tra log

1.2.3.3 /etc/hosts.deny

- File cấu hình của TCP Wrappers
- Chứa danh sách các host/IP bị từ chối truy cập
- Định dạng: sshd: IP bị chặn

1.2.3.4 /etc/hosts.allow

- File cấu hình xác định các host/IP được phép truy cập dịch vụ với độ ưu tiên cao hơn hosts.deny

1.2.4 Ứng dụng thực tế của DenyHosts

Được sử dụng trong các máy chủ Linux cung cấp dịch vụ SSH để:

- Ngăn chặn các công cụ brute-force như Hydra, Medusa, bot SSH.
- Giảm nguy cơ chiếm quyền root do đoán mật khẩu.
- Tăng cường bảo mật cho máy chủ công khai trên Internet.

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

2.1 Chuẩn bị môi trường

- Phần mềm ảo hóa, chẳng hạn: VMWare Workstation.
- Máy ảo Labtainer.

2.2 Các bước thực hiện

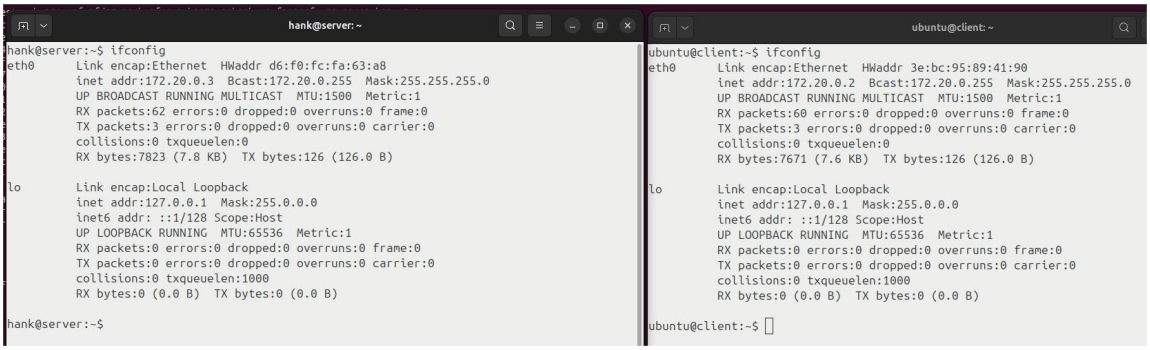
2.2.1 Khởi động bài Lab

- Khởi động lab: *labtainer -r denyhost*
- Nhập e-mail (Mã sinh viên): *B22DCAT136*

```
    labtainer <labname> -r
student@LabtainerVMware:~/labtainer/labtainer-student$ labtainer -r denyhost
latest: Pulling from labtainers/denyhost.server.student
396fe0bedbac: Pull complete
703b42cd31c2: Pull complete
d72bda0db177: Pull complete
3f3a593b92bd: Pull complete
d8895c255db6: Pull complete
cc70cb1d6275: Pull complete
a5c29abff389: Pull complete
Digest: sha256:10fa3fd87a384bc8f16e2cb9972c90b82be18ef91066fae55e32412eb92ea7c9
Status: Downloaded newer image for labtainers/denyhost.server.student:latest
latest: Pulling from labtainers/denyhost.client.student
aee4dc4db6a5: Pull complete
aa1f0710a518: Pull complete
c6f7346496c7: Pull complete
0d40ca3fd0ba: Pull complete
d8b17e46e375: Pull complete
e3823fa93e24: Pull complete
14feac39a88d: Pull complete
c263aed0df3e: Pull complete
Digest: sha256:bb14eaebf600ddb17011d237aaf71f5e583ae10af71de6f945c73281baae903a
Status: Downloaded newer image for labtainers/denyhost.client.student:latest
non-network local connections being added to access control list

Please enter your e-mail address:  [B22DCAT136]
Starting the lab, this may take a moment...
Started 2 containers, 2 completed initialization. Done.



The lab manual is at
   file:///home/student/labtainer/trunk/labs/denyhost/docs/denyhosts.pdf


You may open that manual by right clicking
and select "Open Link".


Press <enter> to start the lab

student@LabtainerVMware:~/labtainer/labtainer-student$
```

Hình 1. Khởi động bài Lab

- Các terminal hiển thị: một terminal kết nối với một máy khách và một terminal kết nối với một máy chủ SSH.

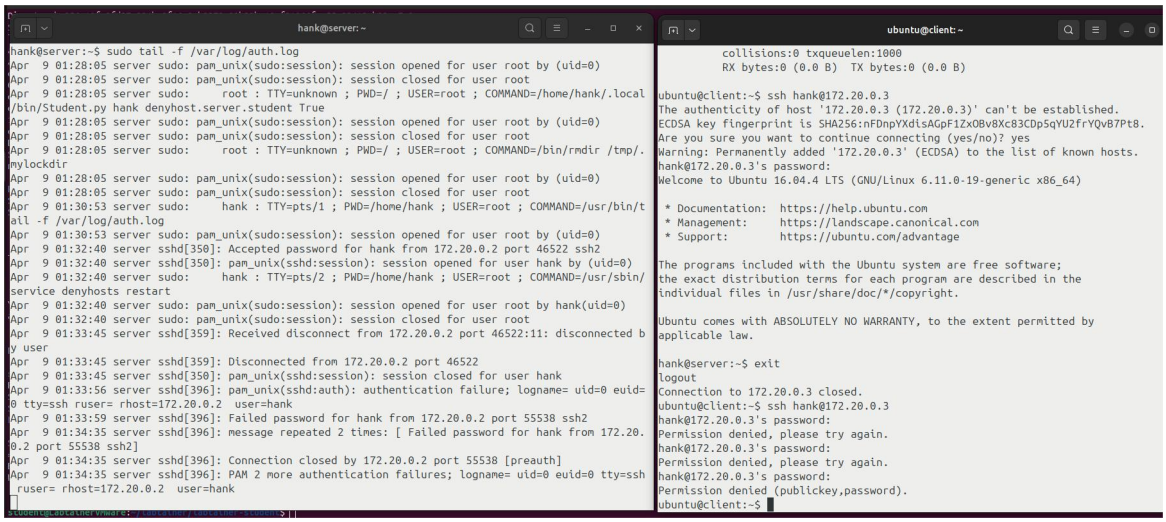


Hình 2. Các terminal hiển thị

2.2.2 Nhiệm vụ 1: Xem các tệp cấu hình

2.2.2.1 Tệp auth.log

- Trên máy chủ SSH, gõ lệnh: *sudo tail -f /var/log/auth.log*
- Trên máy khách, thực hiện:
    - SSH vào máy chủ với mật khẩu đúng:
        - *ssh hank@172.20.0.3*
        - Mật khẩu: *hank21*
    - Quan sát log ta thấy có hiển thị đăng nhập thành công.
- Thoát ra trên máy khách: exit
    - SSH lại với mật khẩu sai: *ssh hank@172.20.0.3*
    - Quan sát log ta thấy có hiển thị đăng nhập thất bại.

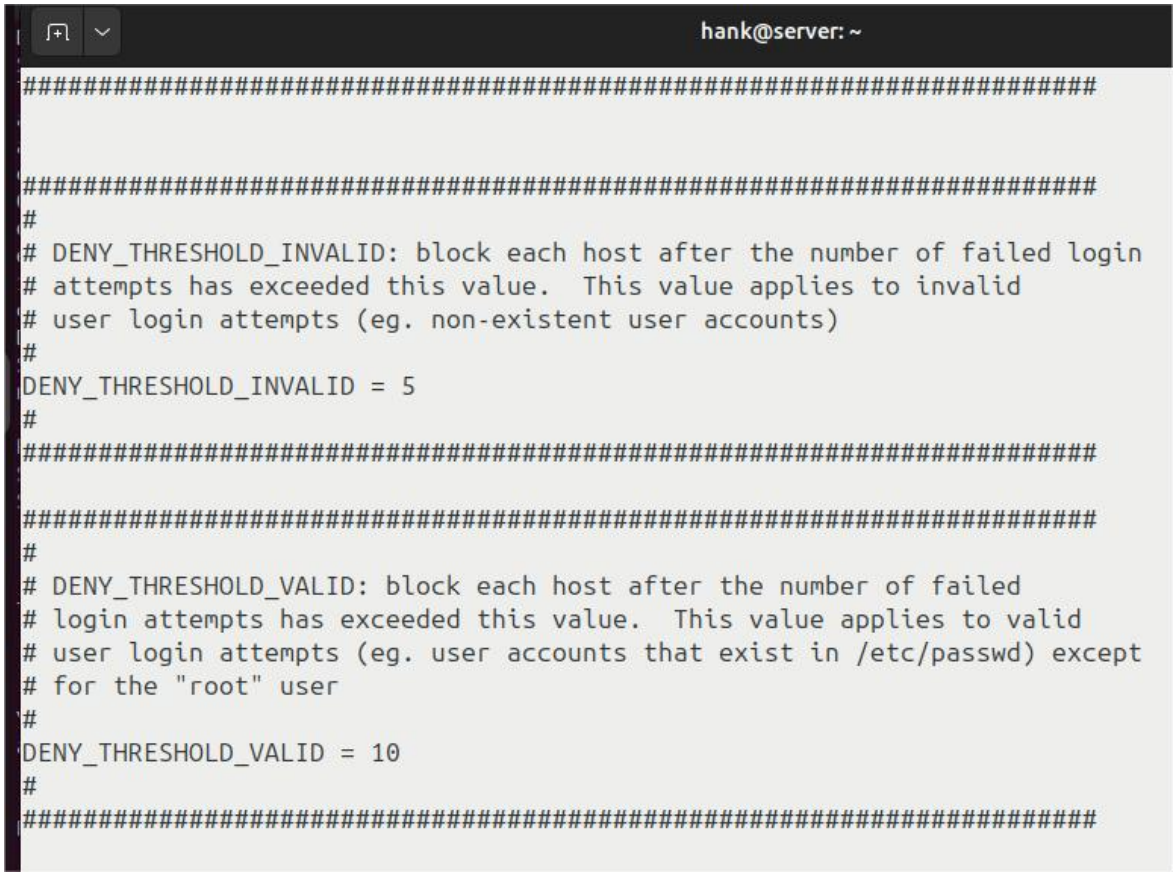


Hình 3. SSH từ máy khách và xem log từ máy chủ

2.2.2.2 Tệp denyhosts.conf

- Trên máy chủ, xem tệp denyhosts.conf bằng lệnh: *sudo less /etc/denyhosts.conf*
- Tìm hai thông số quan trọng:

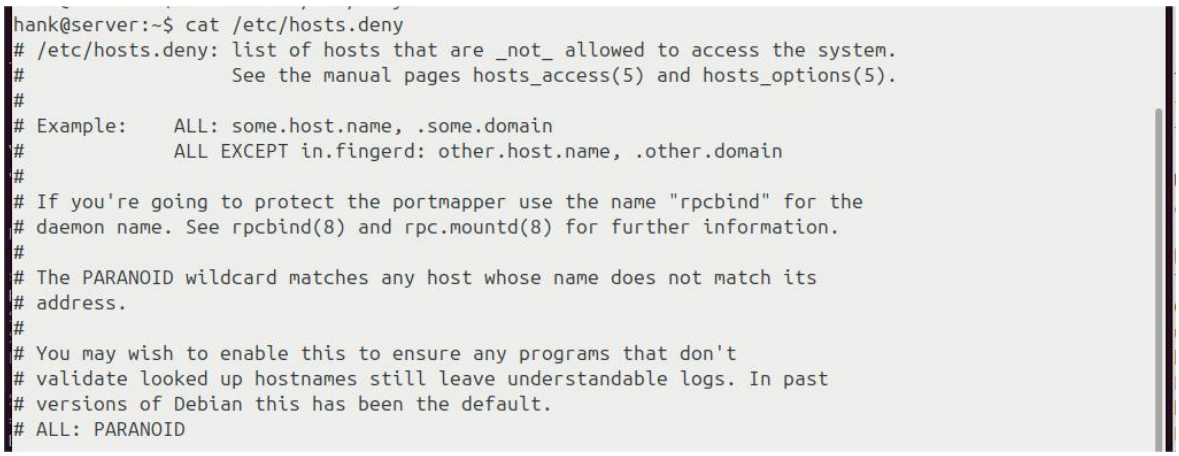
- DENY_THRESHOLD_INVALID (Số lần đăng nhập sai tối đa cho user không hợp lệ): 5
- DENY_THRESHOLD_VALID (Số lần đăng nhập sai tối đa cho user hợp lệ): 10



Hình 4. Xem tệp denyhosts.conf

2.2.2.3 Tệp hosts.deny

- Trên máy chủ, xem tệp hosts.deny bằng lệnh: *cat /etc/hosts.deny*

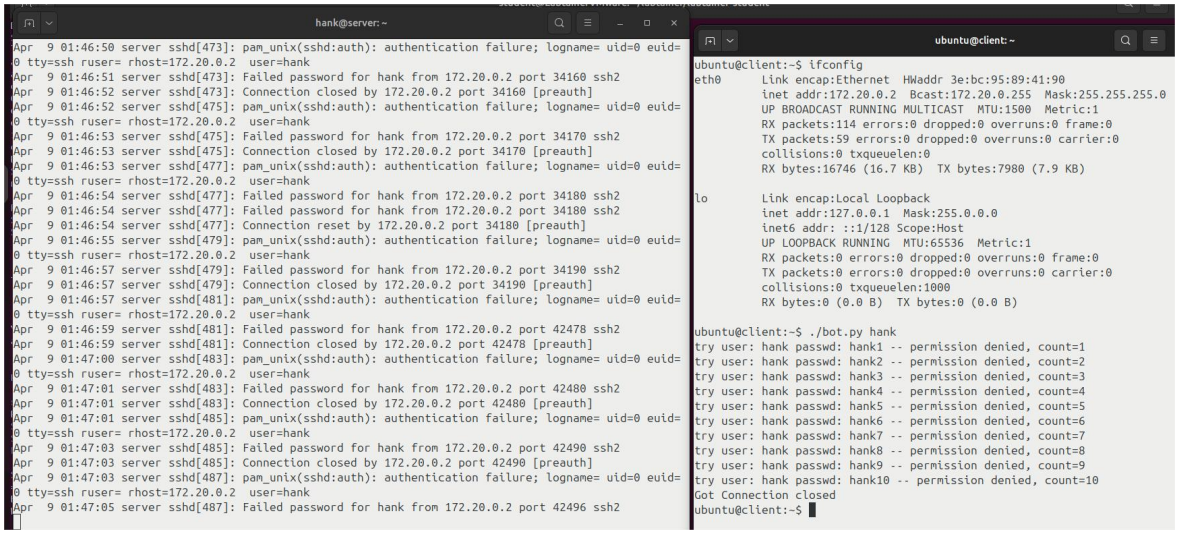


Hình 5. Xem tệp hosts.deny

2.2.3 Nhiệm vụ 2: Khóa user hợp lệ bằng bot

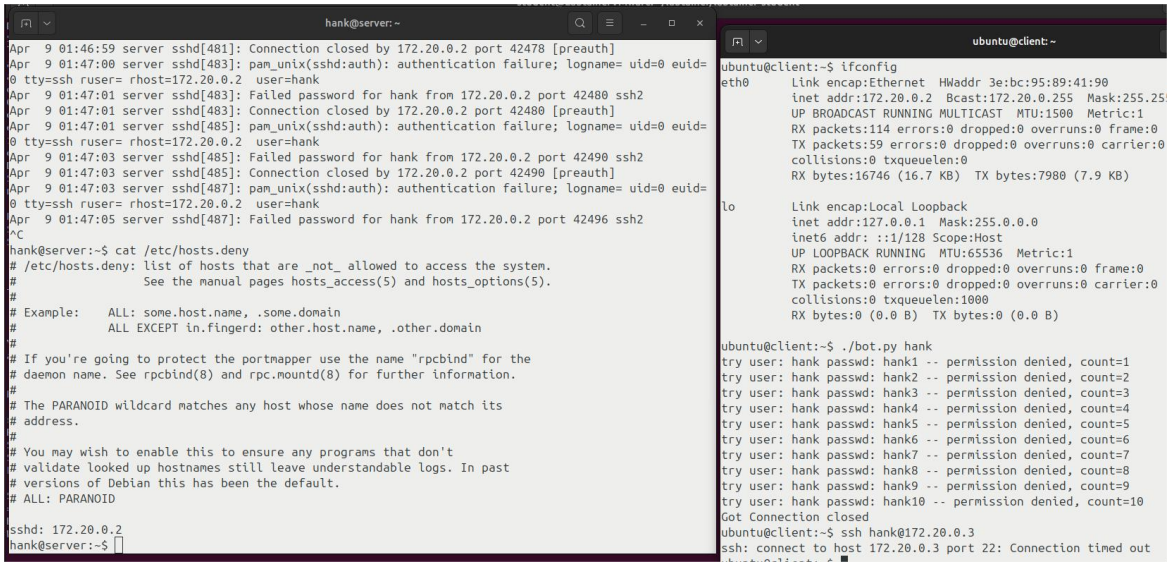
- Trên máy chủ, mở tệp auth.log: *sudo tail -f /var/log/auth.log*
- Kiểm tra IP của máy khách: *ifconfig*

- Chạy bot tấn công: *./bot.py hank*
- Bot sẽ thử các mật khẩu như hank1, hank2,... cho đến khi bị chặn.



Hình 6. Chạy bot tấn công

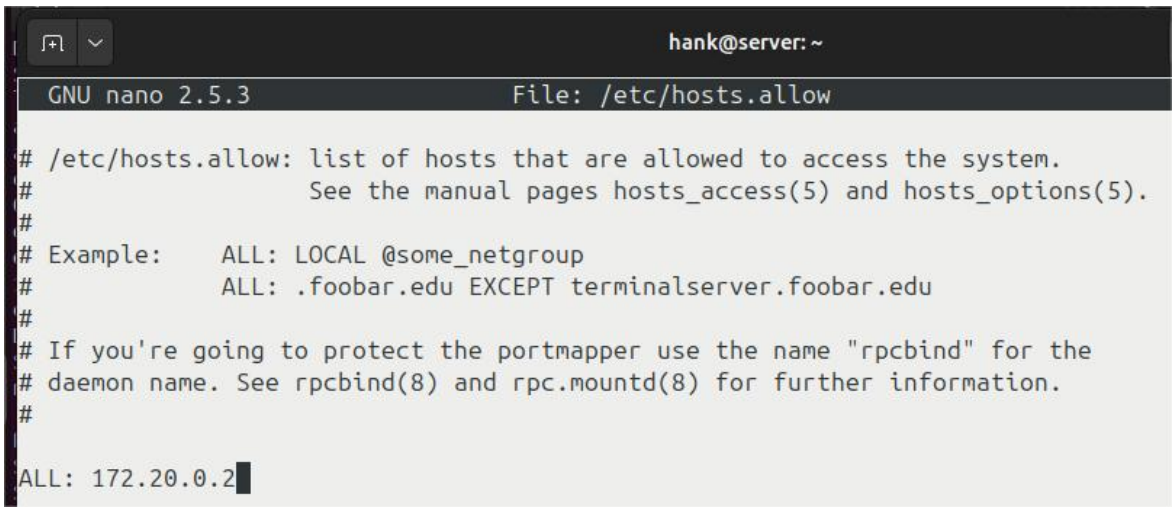
- Ta thấy được khi số lần đăng nhập sai vượt ngưỡng được cấu hình trong denyhosts.conf (DENY_THRESHOLD_VALID: 10), IP của bạn sẽ bị thêm vào /etc/hosts.deny: *sshd: 172.20.0.2*
- Thử SSH lại máy chủ từ máy khách: *ssh hank@172.20.0.3* → Không thể kết nối thành công.



Hình 7. Thử SSH sau khi bị chặn

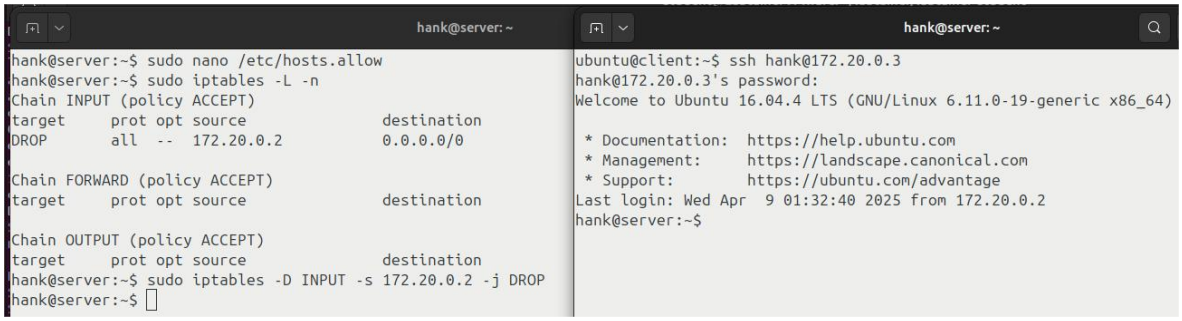
2.2.4 Nhiệm vụ 3: Khôi phục đăng nhập

- Trên máy chủ, thêm IP máy khách vào whiltelist:
  - Mở tệp hosts.allow: *sudo nano /etc/hosts.allow*
  - Thêm IP: *ALL: 172.20.0.2*



Hình 8. Thêm IP máy khách vào whitelist

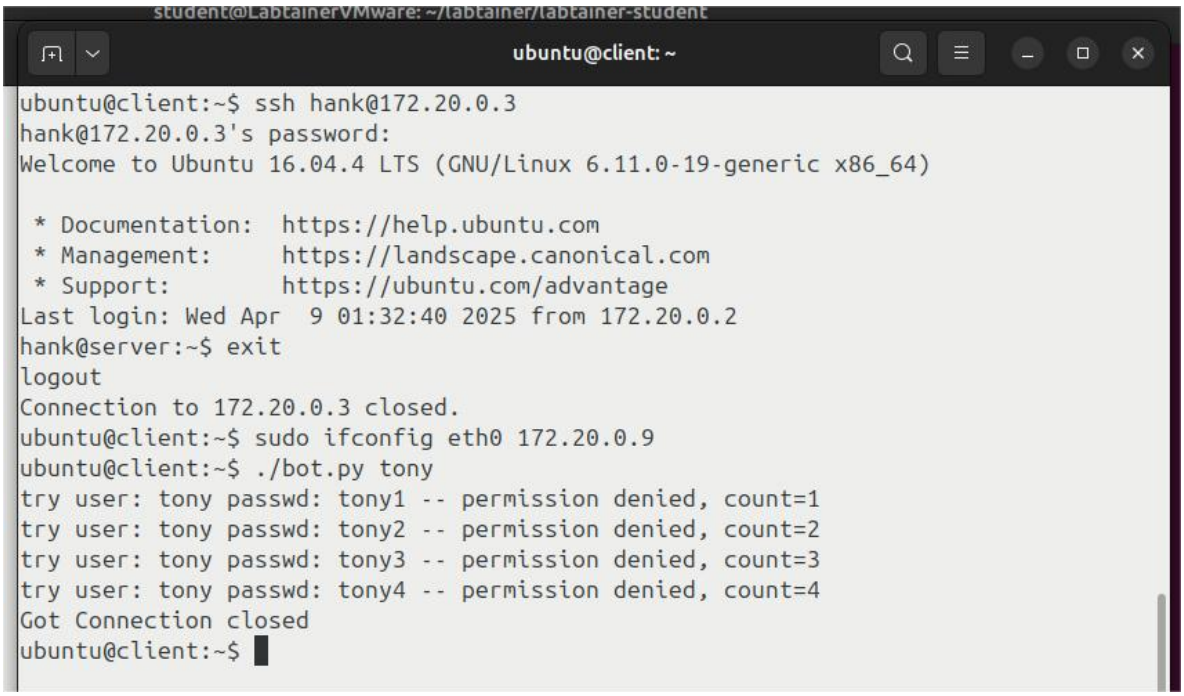
- Ngoài ra, địa chỉ IP bị cấm cũng có thể bị chặn bằng cách sử dụng "iptables", ta có thể kiểm tra bằng lệnh: *sudo iptables -L -n*
- Nếu thấy IP của bạn trong danh sách chặn: *DROP all -- 172.20.0.2*
    - Gỡ bỏ lệnh chặn: *sudo iptables -D INPUT -s 172.20.0.2 -j DROP*
- Thử SSH lại từ máy khách để kiểm tra:



Hình 9. Thử SSH lại và thành công

2.2.5 Nhiệm vụ 4: Khóa user không hợp lệ

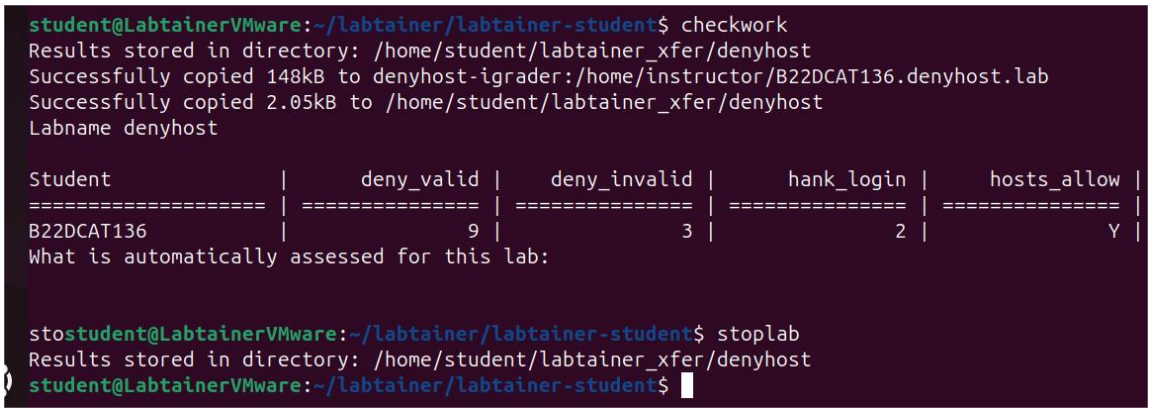
- Trên máy khách, thay đổi địa chỉ IP của máy khách để máy khách của chúng ta không còn trong danh sách cho phép whitelist: *ifconfig eth0 172.20.0.9*
- Sau đó, thử lại bot.py, nhưng lần này cung cấp một người dùng khác: *./bot.py tony*
- Khi vượt ngưỡng DENY_THRESHOLD_INVALID, IP sẽ bị chặn.



Hình 10. Thử SSH với tài khoản người dùng lạ

CHƯƠNG 3. KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:



Hình 11. Kết quả bài thực hành

- Trên terminal đầu tiên sử dụng câu lênh sau để kết thúc bài lab: *stoplab*
- Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới lệnh stoplab.

TÀI LIỆU THAM KHẢO

[1] hatcai, VIBLO MOBILE APP, Tổng quan về SSH và cách connect SSH đến Server, 2022

[2] Vivek Gite, How to install denyhosts on Ubuntu Linux 18.04 LTS (intrusion prevention security tool), 2022