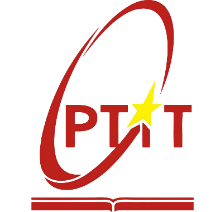
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

-------🙞🙜🕮🙞🙜-------



**Báo cáo bài thực hành**

**Tìm hiểu về công cụ Nftables**

Sinh viên thực hiện:

B20DCAT59 Nguyễn Cảnh HIếu

Giảng viên hướng dẫn: TS.Phạm Hoàng Duy

MỤC LỤC

[MỤC LỤC 1](#_Toc186672271)

[DANH MỤC CÁC HÌNH VẼ 2](#_Toc186672272)

[DANH MỤC CÁC BẢNG BIỂU 2](#_Toc186672273)

[1.1 Giới thiệu chung về bài thực hành 3](#_Toc186672274)

[1.2 Nội dung và hướng dẫn bài thực hành 3](#_Toc186672275)

[1.2.1 Mục đích 3](#_Toc186672276)

[1.2.2 Yêu cầu đối với sinh viên 3](#_Toc186672277)

[1.2.3 Nội dung thực hành 3](#_Toc186672278)

[1.3 Phân tích yêu cầu bài thực hành 4](#_Toc186672279)

[1.4 Thiết kế bài thực hành 4](#_Toc186672280)

[1.5 Cài đặt và cấu hình các máy ảo 6](#_Toc186672281)

[1.6 Tích hợp và triển khai 8](#_Toc186672282)

[***1.6.1 Docker Hub*** 8](#_Toc186672283)

[***1.6.2 Github*** 9](#_Toc186672284)

[1.7 Thử nghiệm và đánh giá 9](#_Toc186672285)

[TÀI LIỆU THAM KHẢO 14](#_Toc186672286)

DANH MỤC CÁC HÌNH VẼ

[Hình 1 Giao diện Labedit của bài lab 7](#_Toc186672290)

[Hình 2 Cài đặt phần Result 7](#_Toc186672291)

[Hình 3 Dockerfiles của máy nftable 7](#_Toc186672292)

[Hình 4 Dockerfiles của client 8](#_Toc186672293)

[Hình 5 Treataslocal của nftable 8](#_Toc186672294)

[Hình 6 Treataslocalcủa client 8](#_Toc186672295)

[Hình 7 Đẩy các vùng chứa lên dockerhub 9](#_Toc186672296)

[Hình 8 Đã đẩy lên docker 9](#_Toc186672297)

[Hình 9 IP của máy nftable 9](#_Toc186672298)

[Hình 10 IP máy client 10](#_Toc186672299)

[Hình 11 Kiểm tra phiên bản nftables 10](#_Toc186672300)

[Hình 12 Kiểm tra nftables.conf 11](#_Toc186672301)

[Hình 13 Checkwork nhiệm vụ 1 11](#_Toc186672302)

[Hình 14 Cấu hình chặn gói tin 11](#_Toc186672303)

[Hình 15 Kiểm tra list ruleset 12](#_Toc186672304)

[Hình 16 Checkwork nhiệm vụ 2 12](#_Toc186672305)

[Hình 17 Chặn kết nối ssh 12](#_Toc186672306)

[Hình 18 Checkwork nhiệm vụ 3 13](#_Toc186672307)

[Hình 19 Chặn ssh 13](#_Toc186672308)

[Hình 20 Checkwork nhiệm vụ 4 13](#_Toc186672309)

[Hình 21 Thử nghiệm ping từ client đến nftable 13](#_Toc186672310)

[Hình 22 Thử nghiệm ssh từ client đến nftable 14](#_Toc186672311)

[Hình 23 Checkwork nhiệm vụ 5 14](#_Toc186672312)

DANH MỤC CÁC BẢNG BIỂU

[Bảng 1. Bảng Result 6](#_Toc186672313)

* 1. Giới thiệu chung về bài thực hành

Bài thực hành "Tìm hiểu về công cụ Nftables" được thiết kế nhằm giúp sinh viên hiểu rõ hơn về khái niệm cơ bản của quản lý các quy tắc lọc gói (packet filtering) và quản lý lưu lượng mạng bàng cách khai thác chúng thông qua việc sử dụng Nftables – một công cụ mạng mạnh mẽ và linh hoạt. Đây là một bước khởi đầu quan trọng để sinh viên làm quen với các kỹ thuật liên quan đến an ninh mạng. Trong bài thực hành này, sinh viên sẽ tìm hiểu cách sử dụng Nftables để thực hiện chặn, lọc và ghi lại log các gói tin input và output, từ đó hiểu rõ hơn về cách các gói tin được gửi và nhận qua mạng. Đây là một kỹ năng cơ bản nhưng vô cùng quan trọng đối với sinh viên nắm được vai trò của tường lửa trong việc bảo vệ mạng, như chặn các kết nối không mong muốn, lọc gói dữ liệu, và kiểm soát lưu lượng. Thông qua bài thực hành, sinh viên không chỉ hiểu cách Nftables hoạt động mà còn nhận thức được những rủi ro bảo mật tiềm ẩn trong các hệ thống mạng nếu không được bảo vệ đúng cách. Điều này sẽ giúp sinh viên nâng cao kiến thức và kỹ năng về bảo mật thông tin.

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

Biết cách cấu hình tường lửa nftables từ cơ bản đến nâng cao. Hiểu cú pháp và cách sử dụng lệnh nft để quản lý bảng, chuỗi và quy tắc. Tự thiết lập được các kịch bản firewall thực tế để bảo vệ hệ thống mạng.

* + 1. Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ Nftables.

* + 1. Nội dung thực hành
* Khởi động bài lab:

Vào terminal, gõ:

*Labtainer oss\_ac\_nftables\_n3\_hieu\_2 -r*

*(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 cấu hình: **nftables**, một cái là đại diện cho máy thử nghiệm: **client**. Trên terminal **client**thực hiện kiểm tra ip để cấu hình tường lửa chặn trên terminal **nftables**

Trên terminal **nftbales**thực hiện cấu hình tường lửa để thực hiện chặn ip, dải ip, chặn ssh và ghi lại lịch sử

* Kết thúc bài lab:

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

*stoplab oss\_ac\_nftables\_n3\_hieu\_2 -r*

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 oss\_ac\_nftables\_n3\_hieu\_2 -r*

* 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 client, máy còn lại là nftables được xây dựng tích hợp công cụ Nftables. Để hoàn thành bài thực hành sinh viên cần sử dụng Nftables để thực hiện cấu hình tường lửa chặn một số ip, dải ip cụ thể, ssh vầ ghi lại log các gói tin bị chặn

* 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 “nftable” đóng vai trò cấu hinh tường lửa và 1 container mang tên “client” đóng vai trò máy thử nghiệm.

Tạo mạng LAN có cấu hình: 172.20.0.0/24 và gateway: 172.20.0.1

Cấu hình docker gồm có:

* nftable: lưu cấu hình cho máy, trong đó gồm có:
* Tên máy: nftable
* Địa chỉ trong mạng LAN: 172.20.0.10
* Gateway: 172.20.0.1
* client: lưu cấu hình cho máy, trong đó gồm có:
* Tên máy: client
* Địa chỉ trong mạng LAN: 172.20.0.20
* Gateway: 172.20.0.1
* Config: lưu cấu hình hoạt động của hệ thống
* Dockerfiles: mô tả cấu hình của 2 container: nftable và client, trong đó:
* nftable: sử dụng các thư viện mặc định hệ thống và tích hợp sẵn nftables giúp thực hiện các lệnh và chức năng của tool này.
* client: sử dụng các thư viện mặc định hệ thống cùng với cấu hình tương tự máy nftable
* Các nhiệm vụ cần phải thực hiện để thực hành thành công:
* Trên máy nftable thực hiện đọc và cấu hình nftables.conf bằng nano
* Cấu hình và áp dụng các quy tắc trong nftablles.conf gồm chặn ip, ssh từ máy client và ghi log các gói tin bị chặn
* Trên máy client thực hiện ping, ssh đến máy nftable để kiểm tra các quy tắc đã ap dụng thành công hay chưa

Kết thúc bài lab và đóng gói kết quả.

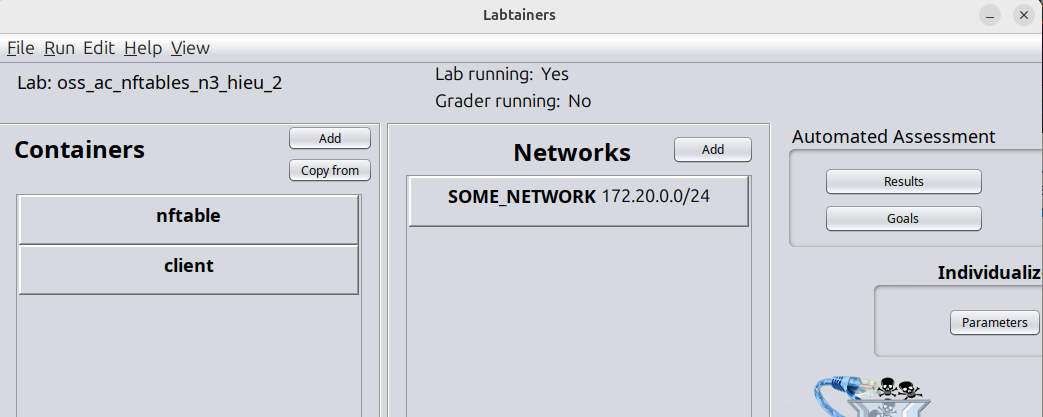
Thiết lập hệ thống mạng sao cho máy nftable và máy client cùng một mạng LAN.

Để đánh giá được sinh viên đã hoàn thành bài thực hành hay chưa, cần chia bài thực hành thành các nhiệm vụ nhỏ, mỗi nhiệm vụ cần phải chỉ rõ kết quả để có thể dựa vào đó đánh giá, chấm điểm. Do vậy, trong bài thực hành này hệ thống cần ghi nhận các thao tác, sự kiện được mô tả và cấu hình như bảng 1:

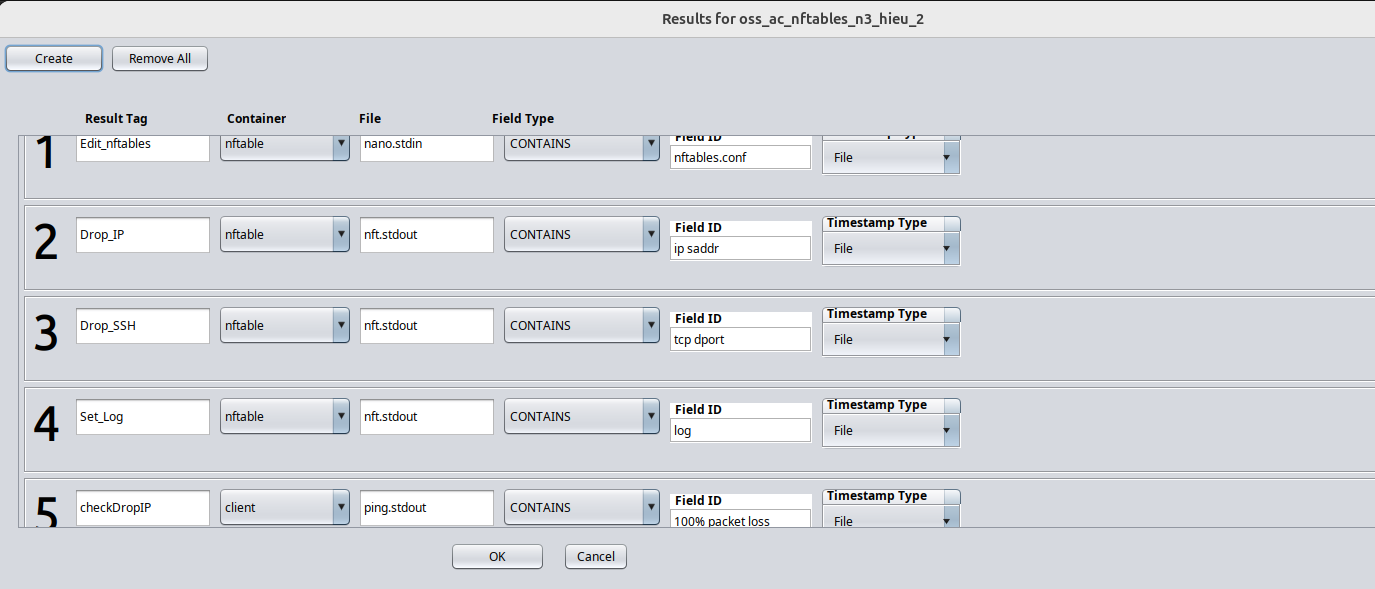
1. Bảng Result

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Result Tag | Container | File | Field Type | Field ID | Timestamp Type |
| Edit\_nftbales | nftable | nano.stdin | CONTAINS | /nftables.conf | File |
| Drop\_IP | nftable | nft.stdout | CONTAINS | saddr ip | File |
| Drop\_SSH | nftable | nft.stdout | CONTAINS | tcp dport | File |
| Set\_Log | nftable | nft.stdout | CONTAINS | log | File |
| CheckDropIP | client | ping.stdout | CONTAINS | 100% packet loss | File |

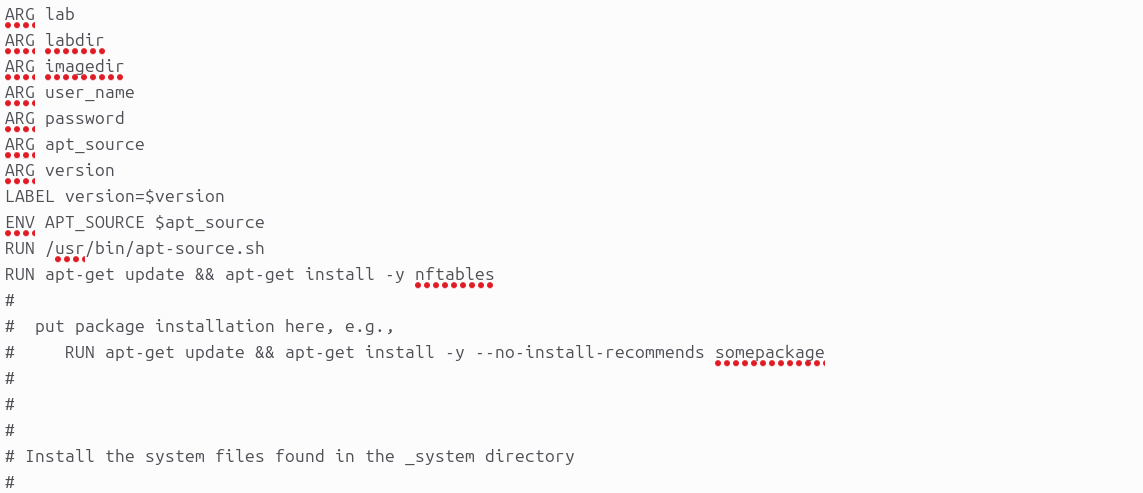
* Edit\_nftbales: hiển thị nội dung và chỉnh sửa file “nftables.conf” trên terminal máy nftable
* Drop\_IP: chặn các gói tin từ máy client.
* Drop\_SSH: chặn kết nối SSH từ máy client.
* Set\_Log: ghi lịch sử các gói tin trên máy nftable.
* CheckDropIP: kiểm tra các quy tác đã được ấp dụng chưa thử kết nối từ máy client sang máy nftable
  1. Cài đặt và cấu hình các máy ảo



1. Giao diện Labedit của bài lab

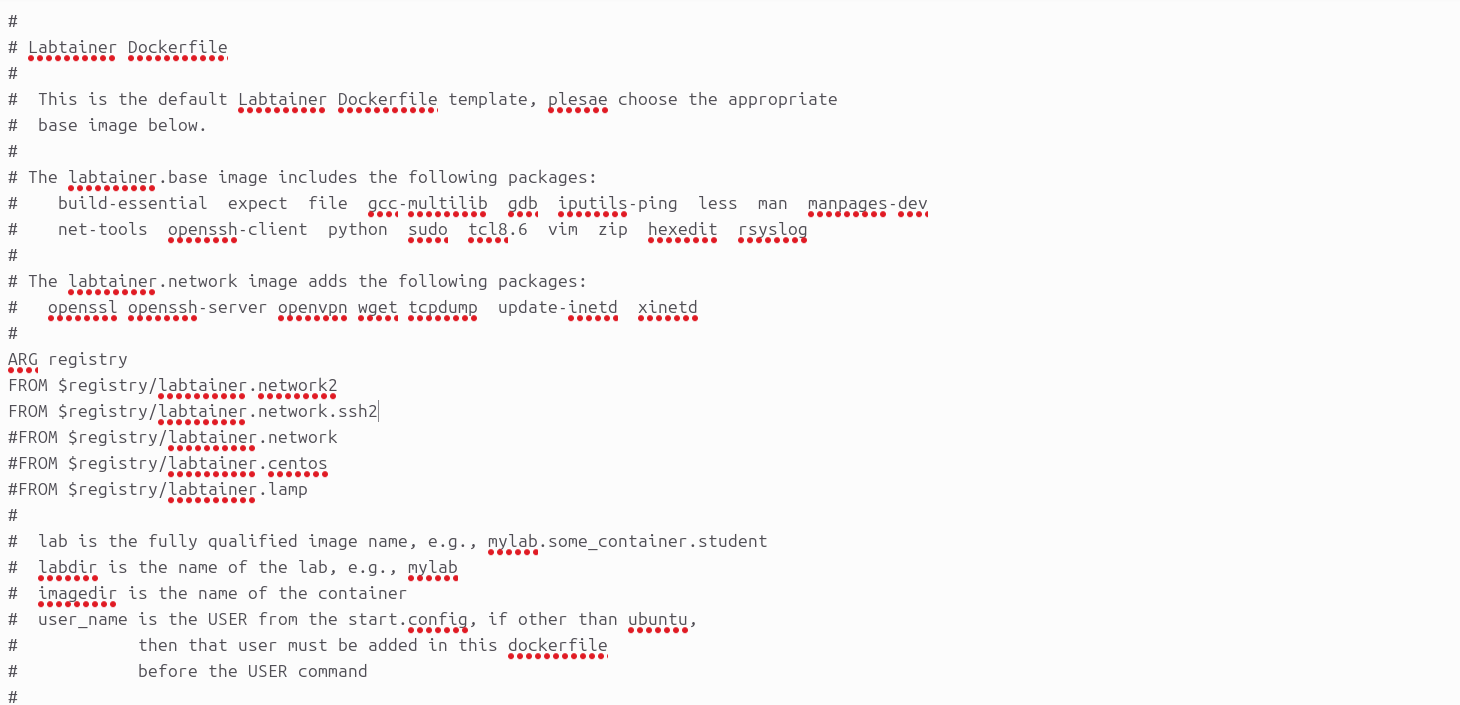


1. Cài đặt phần Result



1. Dockerfiles của máy nftable

* Cài đặt thêm package: Câu lệnh dưới đây được sử dụng trong một tệp Dockerfile để cài đặt và cấu hình một ứng dụng:
* RUN apt-get update && apt-get install -y nftables: Cập nhật danh sách các gói phần mềm có sẵn, sau đó sử dụng “apt-get install -y nftables” để cài đặt nftbales. Tùy chọn -y tự động chấp nhận các điều khoản và điều kiện, cho phép quá trình cài đặt diễn ra mà không cần sự cho phép của người dùng.



1. Dockerfiles của client



1. Treataslocal của nftable



1. Treataslocalcủa client
   1. Tích hợp và triển khai

Bài thực hành đã được triển khai như sau:

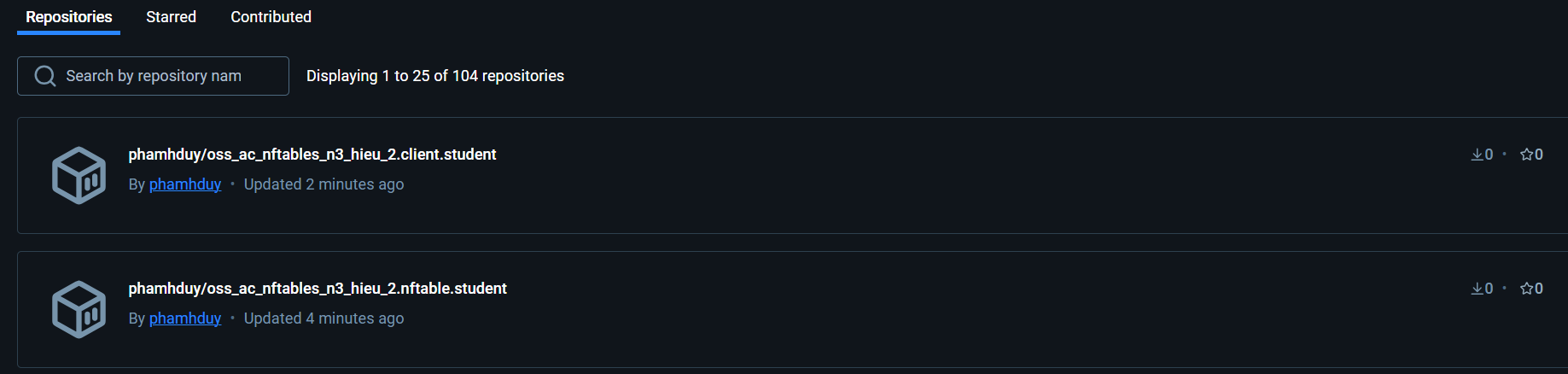
***Docker Hub***

https://hub.docker.com/r/phamhduy/oss\_ac\_nftables\_n3\_hieu\_2.nftable.student

https://hub.docker.com/r/phamhduy/oss\_ac\_nftables\_n3\_hieu\_2.client.student



1. Đẩy các vùng chứa lên dockerhub

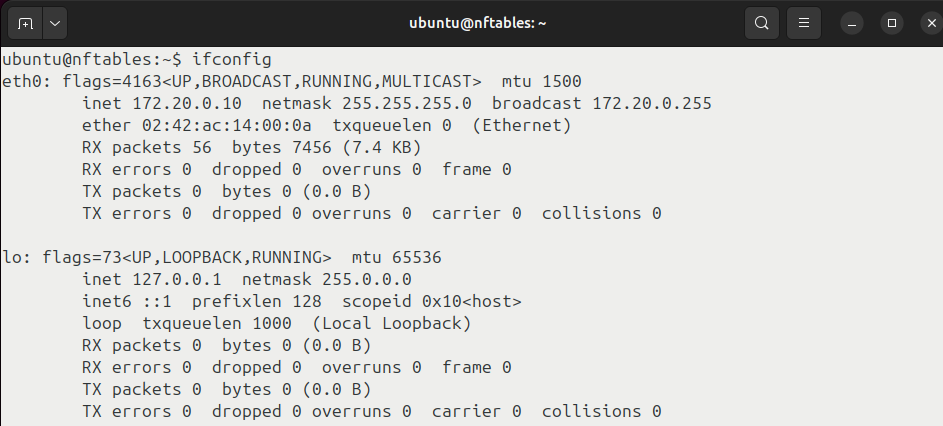


1. Đã đẩy lên docker

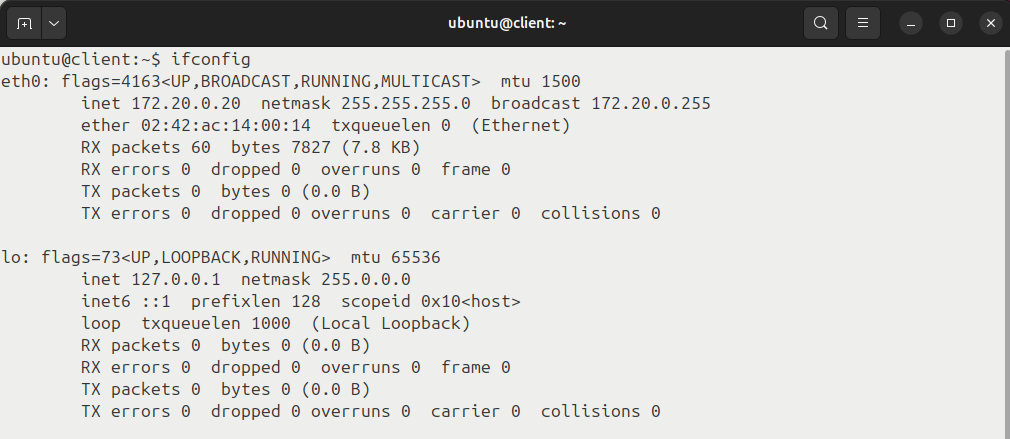
***Github***

* 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:

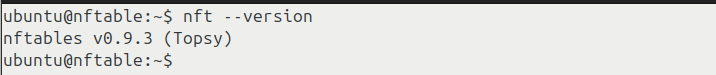


1. IP của máy nftable



1. IP máy client

Kiểm tra nftables đã được cài đặt thành công trên máy nftable chưa:



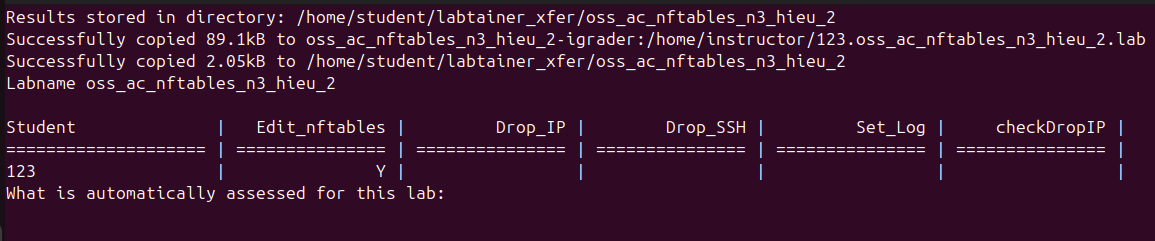
1. Kiểm tra phiên bản nftables

Nếu chưa có, thì có thể cài đặt bằng lệnh:

* *sudo apt update*
* *sudo apt install nftables*
* ***Nhiệm vụ 1:*** Tìm hiểu cấu trúc cơ bản nftbale 🡺 Mở và cấu hình tường lửa ở nftbales.conf



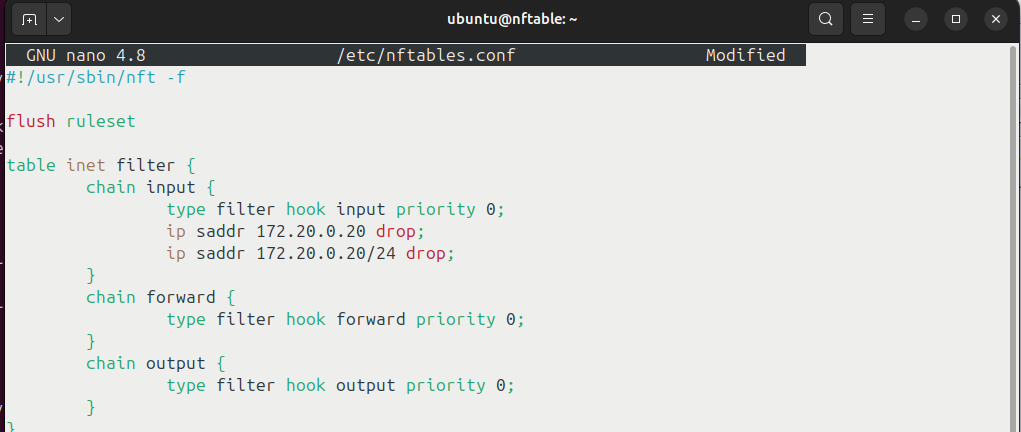
1. Kiểm tra nftables.conf



1. Checkwork nhiệm vụ 1

* ***Nhiệm vụ 2:*** Cấu hình chặn gói tin đến từ máy client.

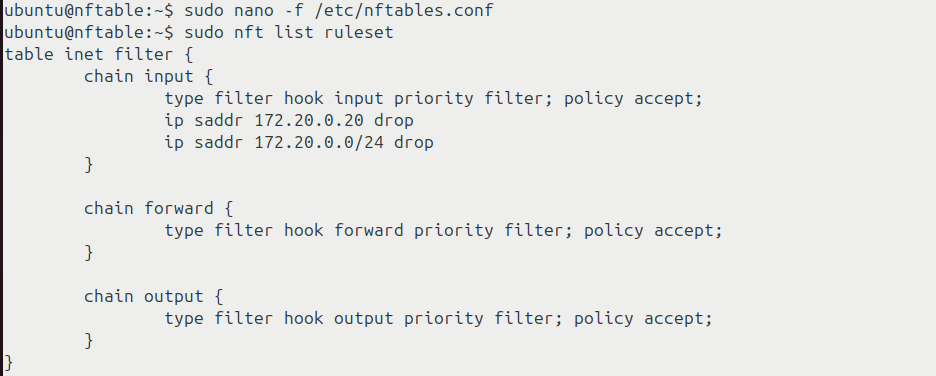
Kiểm tra ip của máy client “172.20.0.20”.



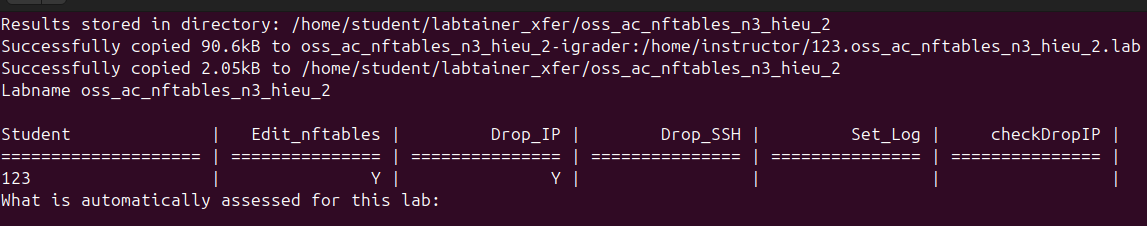
1. Cấu hình chặn gói tin

Lưu và áp dụng cấu hình:

* *sudo nft -f /etc/nftables.conf*
* *sudo nft list ruleset*

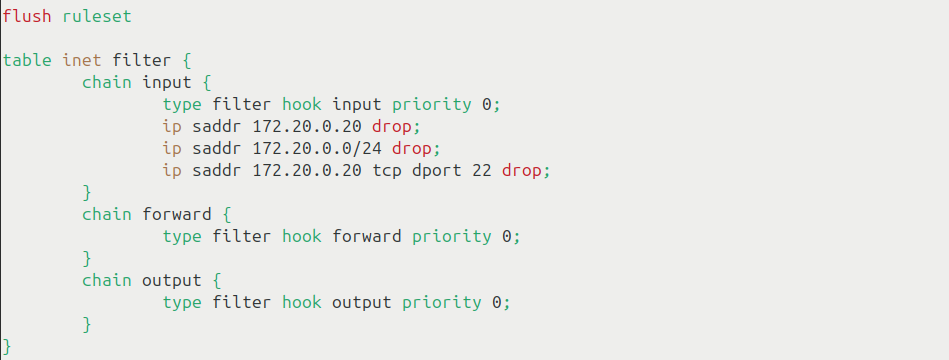


1. Kiểm tra list ruleset



1. Checkwork nhiệm vụ 2

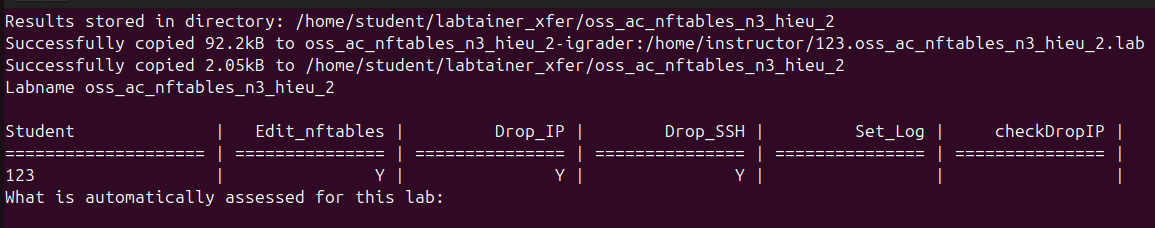
* ***Nhiệm vụ 3:*** chặn ssh từ máy client đến nftable



1. Chặn kết nối ssh

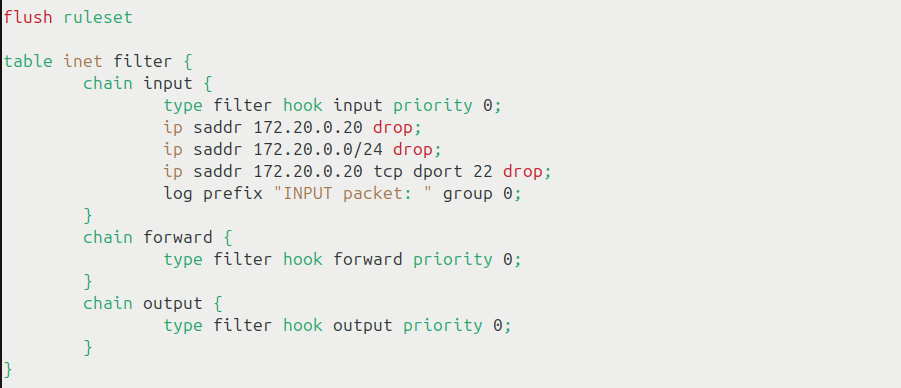
Lưu và áp dụng cấu hình:

* *sudo nft -f /etc/nftables.conf*
* *sudo nft list ruleset*

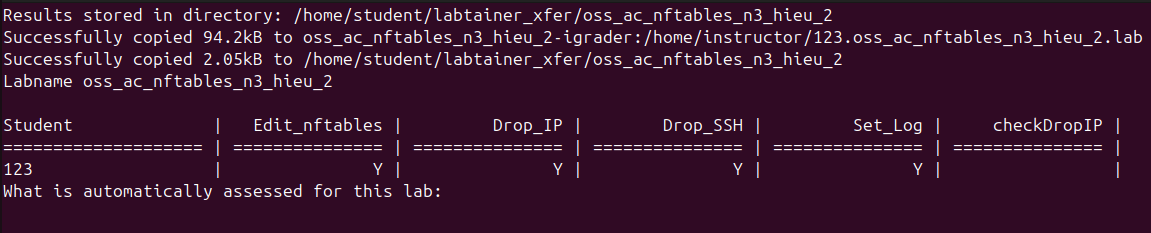


1. Checkwork nhiệm vụ 3

* ***Nhiệm vụ 4:*** Ghi lịch sử các gói tin

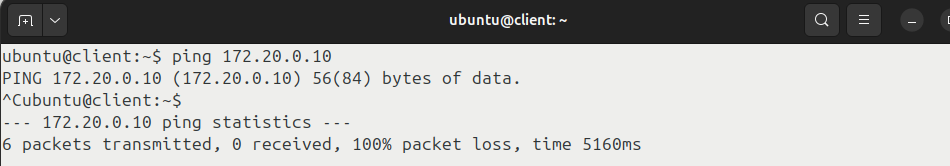
******

1. Chặn ssh

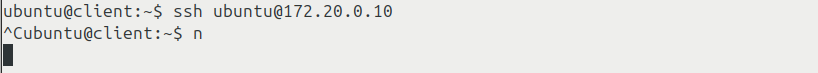


1. Checkwork nhiệm vụ 4

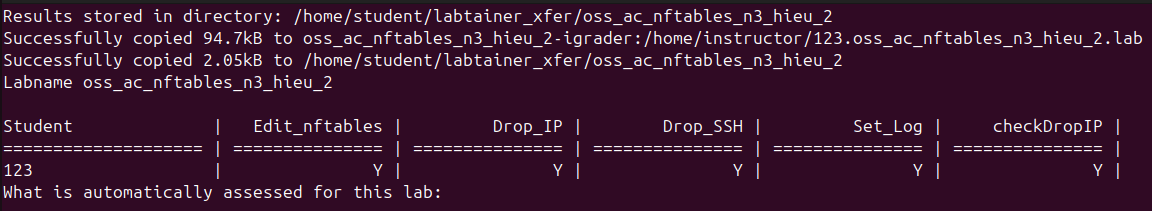
* ***Nhiệm vụ 5:*** thử nghiệm ping và ssh



1. Thử nghiệm ping từ client đến nftable



1. Thử nghiệm ssh từ client đến nftable



1. Checkwork nhiệm vụ 5

TÀI LIỆU THAM KHẢO