**NT534 – AN TOÀN MẠNG MÁY TÍNH NÂNG CAO**

**BÁO CÁO THỰC HÀNH LAB 4**

***Xây dựng hệ thống giám sát mạng với PfSense và Splunk***

**\*\*\***

THÔNG TIN CHUNG

# 1. Tên nhóm

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Dương Phạm Huy Thông | 22521431 | 22521431@gm.uit.edu.vn |

# 2. Nội dung thực hiện

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Nội dung** | **Tự đánh giá** | **Phụ trách** |
| 1 | Phần 1 | Done |  |
| 2 | Phần 2 | Done |  |

***Bên dưới đây là toàn bộ bài báo cáo chi tiết đã được nhóm thực hiện.***

*Mô hình sau được sử dụng trong cả bài thực hành:*

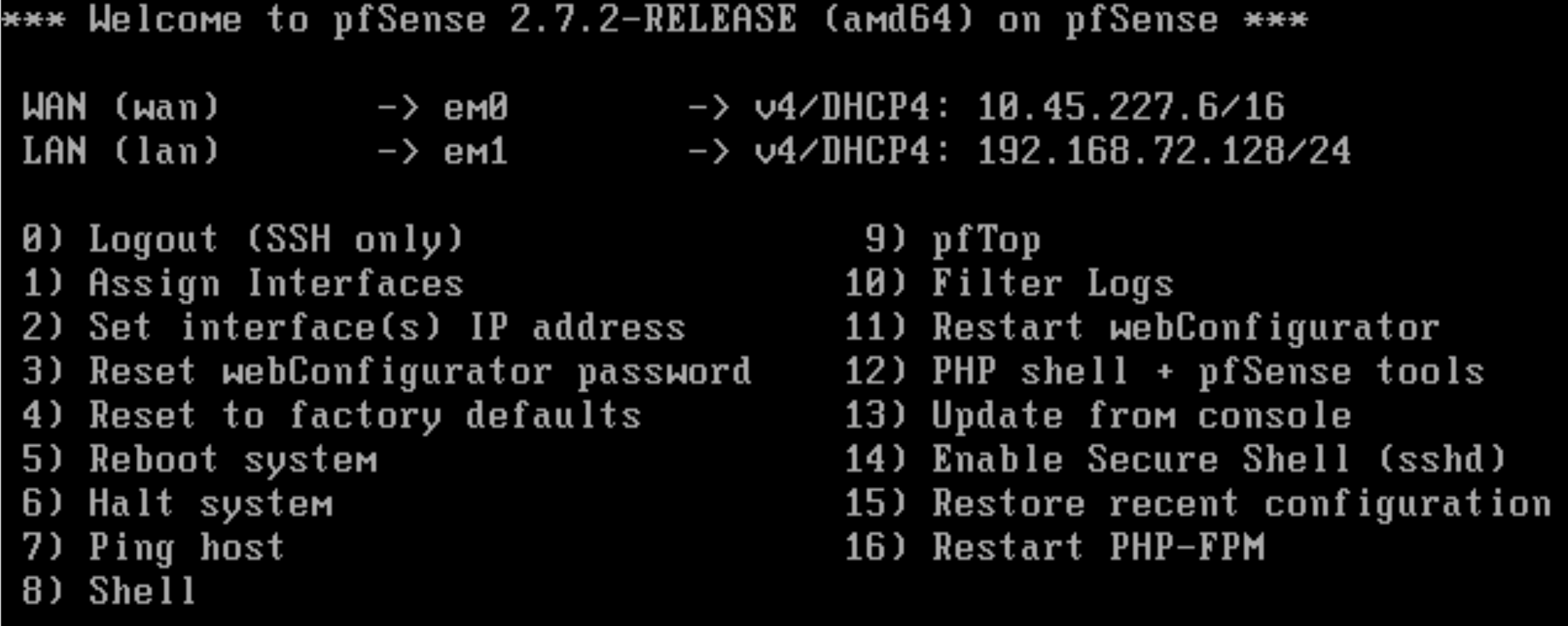
*A computer with a number of data

AI-generated content may be incorrect.*

BÀI LÀM

# I. YÊU CẦU 1. CẤU HÌNH CHUNG

- Thực hiện cấu hình pfSense theo hướng dẫn của bài lab



+ Trong đó nếu chưa có địa chỉ IP cho cả WAN và LAN thì phải thực hiện setting thông qua lựa chọn **2) Set interface(s) IP address.**

+ Nếu chưa cấu hình chọn interface cho WAN và LAN thực hiện chọn **1) Assign Interfaces.**

- Đảm bảo các máy **Client** và **Splunk** có cùng lớp mạng với địa chỉ **LAN.**

- Đối với các máy còn lại (**Client** và **Splunk**) thực hiện cấu hình thêm về địa chỉ IP của default gateway để có thể kết nối thông qua cổng LAN của pfSense.

- Thực hiện cấu hình thông qua file cấu hình **netplan** (/etc/netplan/01-network-manager-all.yaml)

+ Với máy Client:

A computer screen with a black background

AI-generated content may be incorrect.

+ Với máy Splunk

A computer screen shot of a computer

AI-generated content may be incorrect. - Sau khi chỉnh sửa xong file cấu hình, thực hiện cấu quyền (***chmod 600***) file cấu hình. Thực hiện chạy lệnh **sudo netplan apply.**

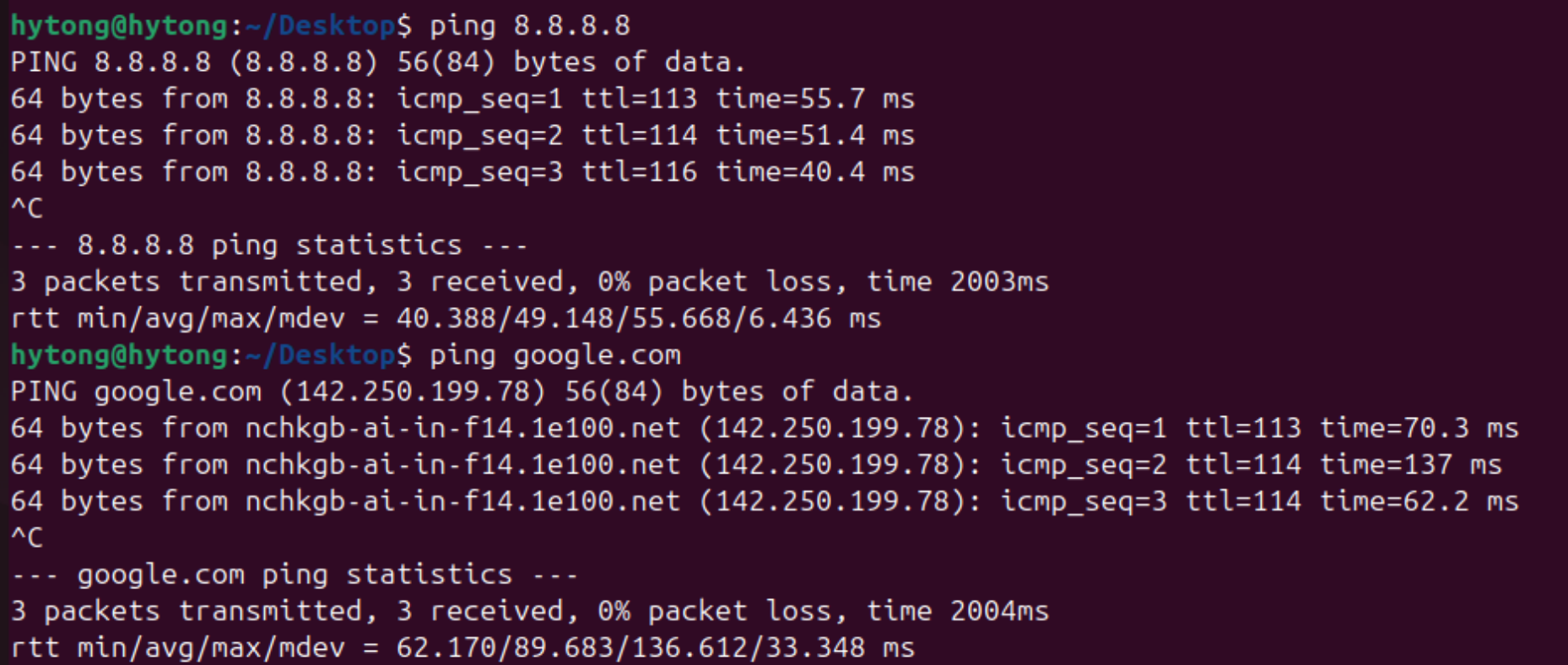
- Kiểm tra lại thông qua lệnh **ping** đến 8.8.8.8 và google.com

+ Trên máy Client:

A computer screen shot of a computer program

AI-generated content may be incorrect.

+ Trên máy Splunk:



- Sau khi thực hiện cấu hình như hướng dẫn để có thể đổ log từ pfSense về Splunk, ta thực hiện kiểm tra lại cấu hình:

A screenshot of a computer

AI-generated content may be incorrect.

# II. YÊU CẦU 2.

## a. Tạo Dashboard đơn giản

- Trong Splunk Dashboard, thực hiện chọn vào phần **Search and Report**, sau đó chọn vào tùy chọn **Dashboards**. Tại đây chọn **Create New Dashboard**

**A screenshot of a computer

AI-generated content may be incorrect.**

- Tiếp đó thực hiện điền tên mong muốn dành cho Dashboard, chọn **Classic Dashboard** (hoặc các lựa chọn khác tùy vào nhu cầu). Sau đó chọn **Create**.

A screenshot of a computer

AI-generated content may be incorrect.

- Tiếp theo, với mỗi một câu lệnh search, ta thực hiện chọn **Add Panel**, sẽ có một bảng lựa chọn để chọn hình thức hiển thị

A screenshot of a computer

AI-generated content may be incorrect.

- Sau khi chọn hình thức biểu thị kết quả tìm kiếm, ta thực hiện điền câu truy vấn để tìm kiếm thông tin trên log. Để đảm bảo câu truy vấn thực hiện đúng theo yêu cầu, có thể lựa chọn **Run Search** để kiểm tra kết quả trả về trước khi tạo Panel.

A screenshot of a computer

AI-generated content may be incorrect.

## b. Đề xuất các yêu cầu để xây dựng Dashboard đơn giản

- **Panel 1:** Tổng số sự kiện block theo thời gian (sử dụng **line chart**)

|  |
| --- |
| ***source="udp:514" sourcetype="\*" "match, block"***  ***| timechart count by src\_ip*** |

A screenshot of a calendar

AI-generated content may be incorrect.

- **Panel 2:** Top địa chỉ IP nguồn bị block nhiều nhất (sử dụng **bar chart**)

|  |
| --- |
| ***source="udp:514" sourcetype="\*" "match, block"***  ***| stats count by src\_ip***  ***| sort -count***  ***| head 10*** |

A purple bar with white text

AI-generated content may be incorrect.

- **Panel 3:** Bảng chi tiết các log block (sử dụng **Statistics Table**)

|  |
| --- |
| ***source="udp:514" sourcetype="\*" "match, block"***  ***| rex field=\_raw "match, lock.\*?(\d+,\d+,\w+),.\*?(?<src\_ip>\d+\.\d+\.\d+\.\d+),(?<dst\_ip>\d+\.\d+\.\d+\.\d+),(?<proto>\d+),(?<src\_port>\d+),(?<dst\_port>\d+)"***  ***| table \_time src\_ip dst\_ip proto src\_port dst\_port*** |

A screenshot of a computer

AI-generated content may be incorrect.

- **Panel 4:** Top 10 Destination IP bị chặn nhiều nhất (sử dụng **Bar char**)

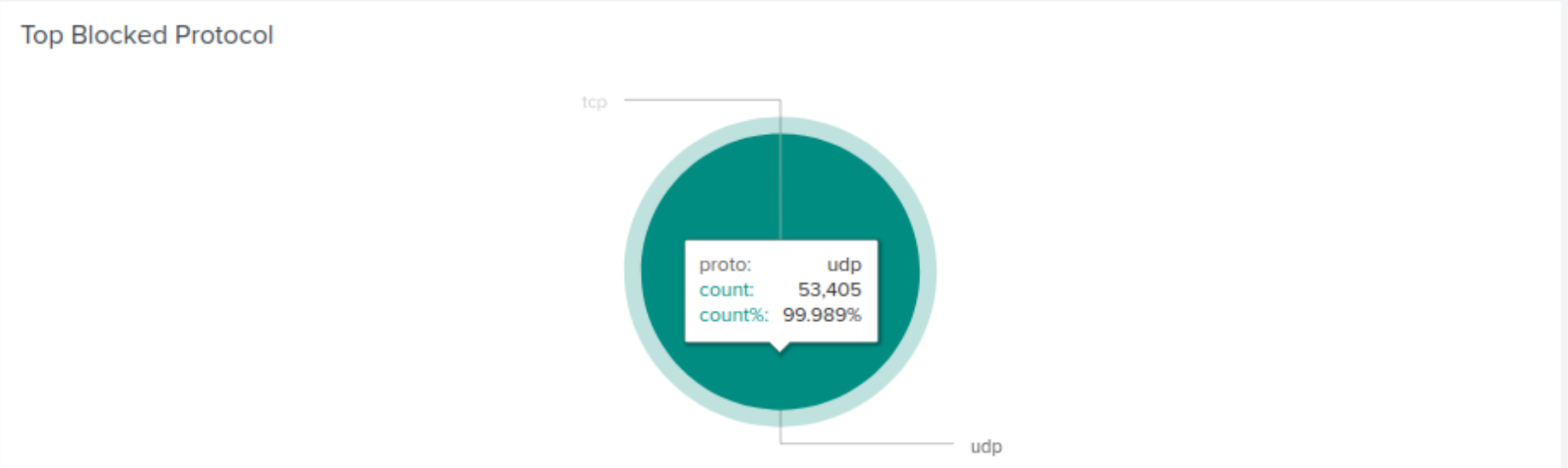
|  |
| --- |
| ***source="udp:514" sourcetype="\*" "match, block"***  ***| rex field=\_raw ".\*?match, block.\*?,udp,(?<src\_ip>\d+\.\d+\.\d+\.\d+),(?<dst\_ip>\d+\.\d+\.\d+\.\d+)"***  ***| stats count by dst\_ip***  ***| sort -count***  ***| head 10*** |

A graph with purple bars

AI-generated content may be incorrect.

- **Panel 5:** Thống kê loại giao thức bị chặn (sử dụng **Pie char**)

|  |
| --- |
| ***source="udp:514" sourcetype="\*" "match, block"***  ***| rex field=\_raw ".\*?match, block.\*?,(?<proto>tcp|udp|icmp)"***  ***| stats count by proto***  ***| sort -count*** |



- Tổng hợp báo cáo được in ra file PDF đính kèm.

**--Hết--**