Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

5

Lab

Xây dựng hệ thống giám sát mạng với PfSense và Splunk

Thực hành môn An toàn mạng máy tính nâng cao

Tháng 3/2024

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Xây dựng một hệ thống giám sát an ninh mạng đơn giản sử dụng tường lửa PfSense kết hợp hệ thống quản lý log và sự kiện tập trung Splunk.

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Máy tính kết nối Internet
- Phần mềm tạo máy ảo: VMWare, Virtual Box, UTM
- Các máy ảo:
    - Tường lửa pfsense. Tải tại link: https://www.pfsense.org/download/(Lưu ý chọn phiên bản AMD64 ISO IPMI/Virtual Machines)
    - Client/user: máy ảo Window/Ubuntu
    - Splunk: máy ảo Ubuntu/Centos
  - Phần mềm:
    - Splunk Enterprise: Đăng ký và tải tại link https://www.splunk.com/en_us/products/splunk-enterprise.html

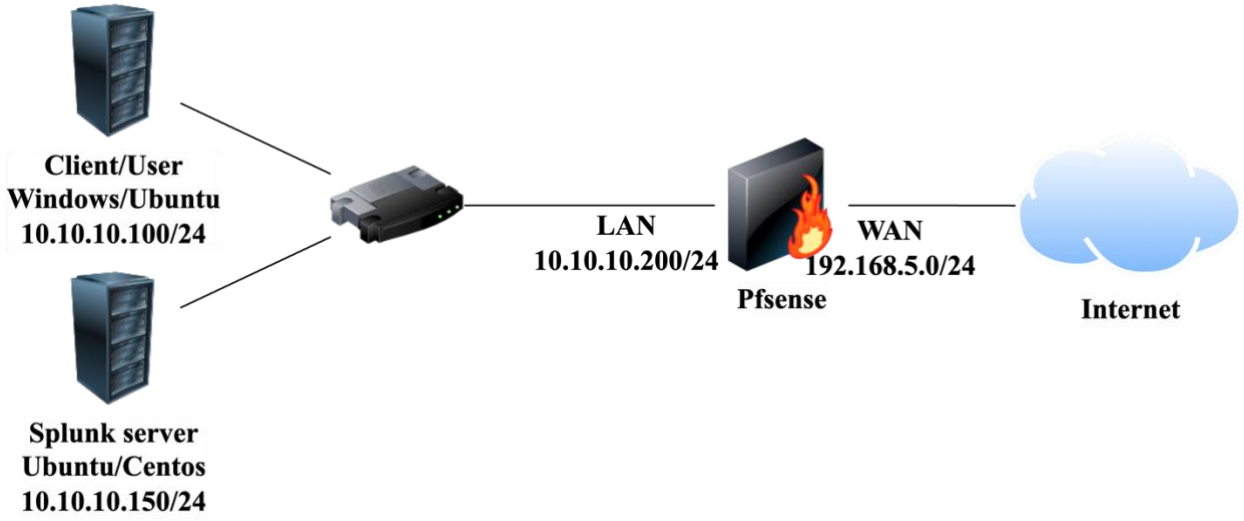
C. THỰC HÀNH

H ệ thống quản lý log và sự kiện tập trung (Security Information and Event Management - SIEM) là một giải pháp, công cụ để thu thập, phân tích và quản lý các thông tin và sự kiện liên quan đến bảo mật thông tin từ các nguồn khác nhau trong một mạng hoặc hệ thống. SIEM bao gồm:

- Thu thập dữ liệu: SIEM có khả năng thu thập dữ liệu từ nhiều nguồn khác nhau như log của hệ thống máy chủ, ứng dụng, thiết bị mạng, cảm biến bảo mật, và các nguồn dữ liệu khác.
- Phân tích sự kiện: Dữ liệu được thu thập sau đó được phân tích để phát hiện các mẫu hành vi bất thường hoặc các dấu hiệu của mối đe dọa bảo mật.
- Phát hiện và cảnh báo: Dựa trên kết quả của việc phân tích sự kiện, SIEM có thể phát hiện các mối đe dọa bảo mật và tạo ra các cảnh báo để cảnh báo về những sự cố tiềm ẩn.

- Quản lý sự cố: SIEM cung cấp các công cụ và giao diện để quản lý và phản ứng với các sự cố bảo mật, bao gồm việc điều tra, xác nhận, và giải quyết các sự cố này.
- Báo cáo và tuân thủ: SIEM cung cấp khả năng tạo ra các báo cáo chi tiết về các hoạt động và sự kiện bảo mật, giúp tổ chức duy trì tuân thủ các quy định bảo mật và tiêu chuẩn liên quan.

Bài thực hành này tập trung vào việc triển khai một giải pháp bảo mật mạng hiệu quả bằng cách sử dụng tường lửa PfSense và tích hợp với hệ thống SIEM Splunk để quản lý và phân tích log.



Mô hình thiết lập bao gồm:

- Tường lửa Pfsense kết nối với Internet, có thiết lập các rule để cho phép hoặc từ chối các lưu lượng kết nối, bảo vệ mạng nội bộ
- Client/user
- Splunk server: thu thập và phân tích log từ tường lửa Pfsense

1. Thiết lập tường lửa PFsense:

a. Cài đặt Pfsense:

Bước 1: Tải file ISO Pfsense cho máy ảo tại link: https://www.pfsense.org/download/ (Lưu ý chọn phiên bản AMD64 ISO IPMI/Virtual Machines)

Bước 2: Sử dụng VMWare tạo máy ảo Pfsense:

- Tạo một máy ảo mới với file ISO đã tải xuống ở bước 1. Chọn hệ điều hành FreeBSD 64-bit
- Thêm Network Adapter để có 2 Network Adapter là Host Only và Bridge

Tiến hành cài đặt Pfsense. Trong quá trình cài đặt, Pfsene có yêu cầu cấu hình các network interface và IP address

b. Cấu hình Pfsense:

Bước 1: Thiết lập network interface

- Tại giao diện Pfsene, chọn **1) Assign Interfaces**
- Chọn các network interface tương ứng với WAN và LAN dựa trên địa chỉ MAC
- Chọn không thiết lập VLANs

```
em0     00:0c:29:36:6f:35   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1     00:0c:29:36:6f:3f   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em0 a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> em1

Do you want to proceed [y|n]?
```

Bước 2: Cấu hình địa chỉ IP:

- Tại giao diện Pfsense, chọn **2) Set interface(s) IP address** để cấu hình IP
- Cấu hình IP cho card WAN và chọn cho phép quản trị tường lửa thông qua giao diện web
- Cấu hình IP cho card LAN

```
The IPv4 LAN address has been set to 10.10.10.200/24


The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: afbfe406dbf346e81198

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em1        -> v4/DHCP4: 192.168.5.58/24
 LAN (lan)       -> em0        -> v4: 10.10.10.200/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

c. Cấu hình máy Client/User:

Bước 1: Cài đặt và cấu hình địa chỉ IP cho Client

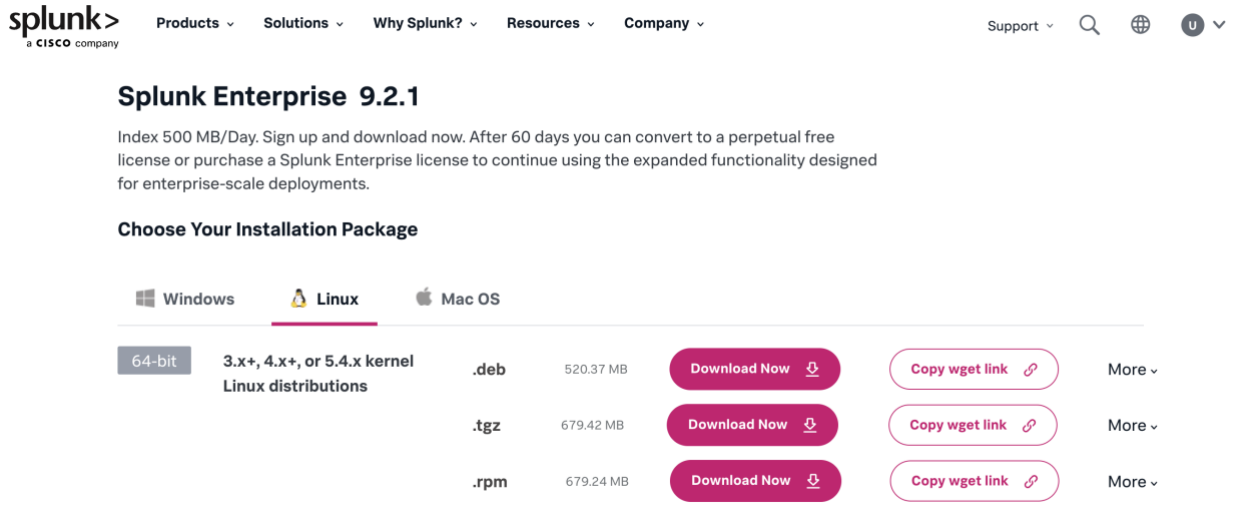
Bước 2: Kiểm tra kết nối tới tường lửa Pfsense và tới Internet bằng lệnh ping.

Bước 3: Truy cập giao diện quản trị của Pfsense theo địa chỉ IP

2. Cài đặt Splunk:

Bước 1: Cấu hình IP cho máy Splunk. Sau khi cấu hình, kiểm tra kết nối tới tường lửa Pfsense và tới Internet bằng lệnh ping.

Bước 2: Sử dụng wget tải Splunk Enterprise https://www.splunk.com/en_us/download/splunk-enterprise.html



Bước 3: Cài đặt Splunk theo hệ điều hành tương ứng dựa trên hướng dẫn ở link sau: https://docs.splunk.com/Documentation/Splunk/9.2.1/SearchTutorial/InstallSplunk

Bước 4: Sau khi cài đặt, truy cập vào thư mục cài đặt Splunk (tại ở hệ điều hành Ubuntu là /opt/splunk/bin). Cấu hình để Splunk khởi động cùng hệ thống bằng câu lệnh ./splunk enable bootstart

Bước 5: Sau splunk được cài đặt và khởi động thành công, một đường link truy cập splunk sẽ tự động được mở (http://10.10.10.150:8080)

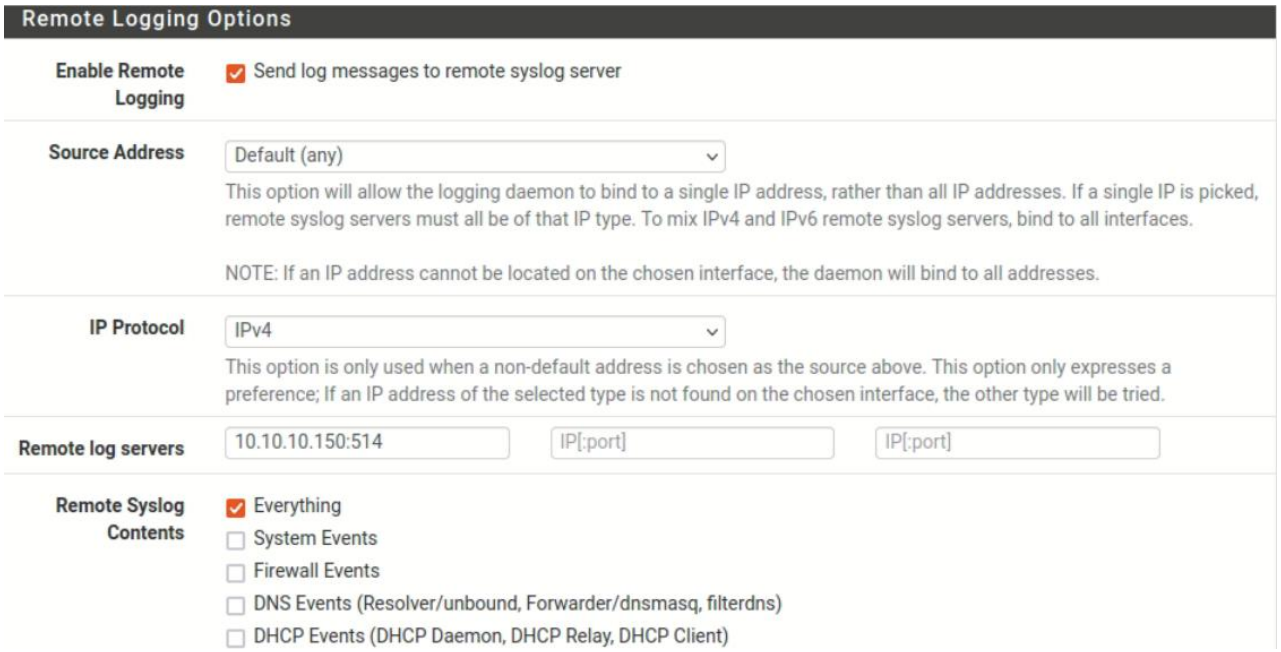
3. Cấu hình đẩy log từ Pfsense về Splunk

a. Tại firewall Pfsense:

Bước 1: Truy cập vào giao diện quản trị của Pfsense từ máy Client

Bước 2: Vào Status=>System Logs. Chọn tab Settings

Bước 3: Tích vào ô: Send log message to remote syslog server. Ip máy chủ nhận log là 10.10.10.150 (máy Splunk). Chọn các log muốn gửi qua Splunk và lưu lại.

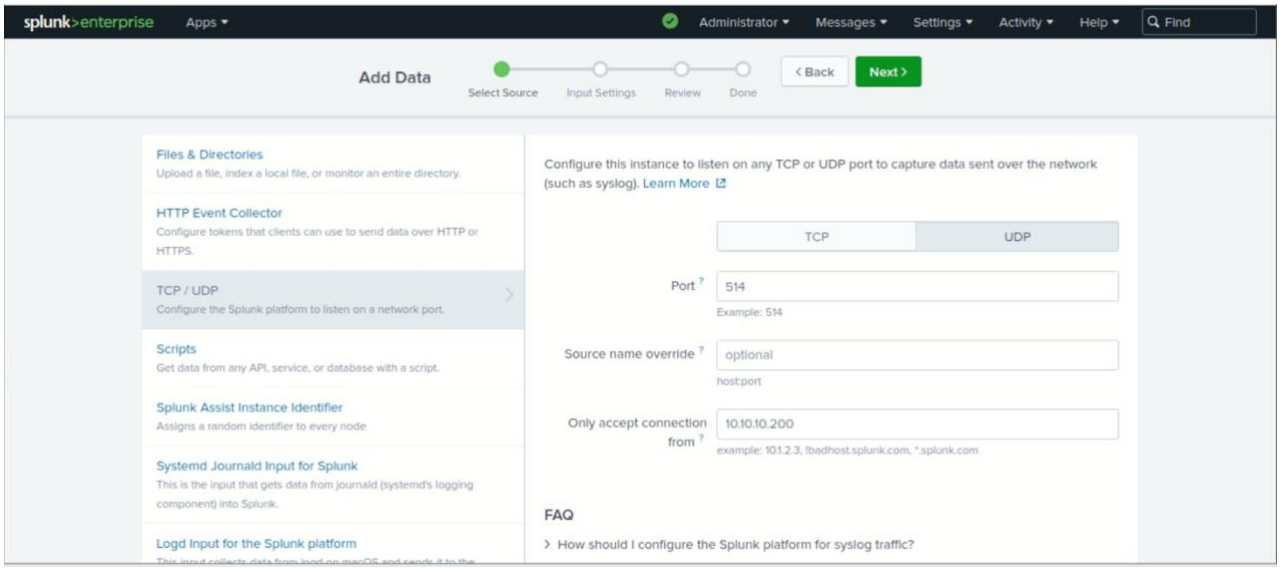


b. Tại server Splunk:

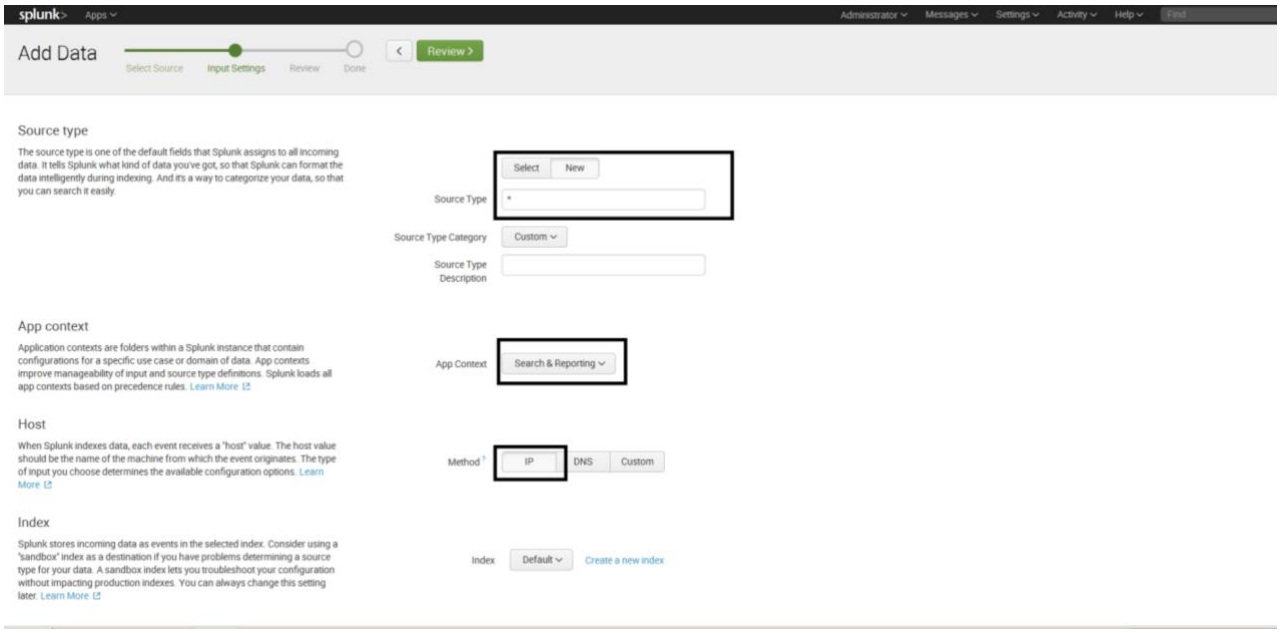
Bước 1: Truy cập vào giao diện quản trị của Splunk từ máy Client

Bước 2: Thêm Data inputs:

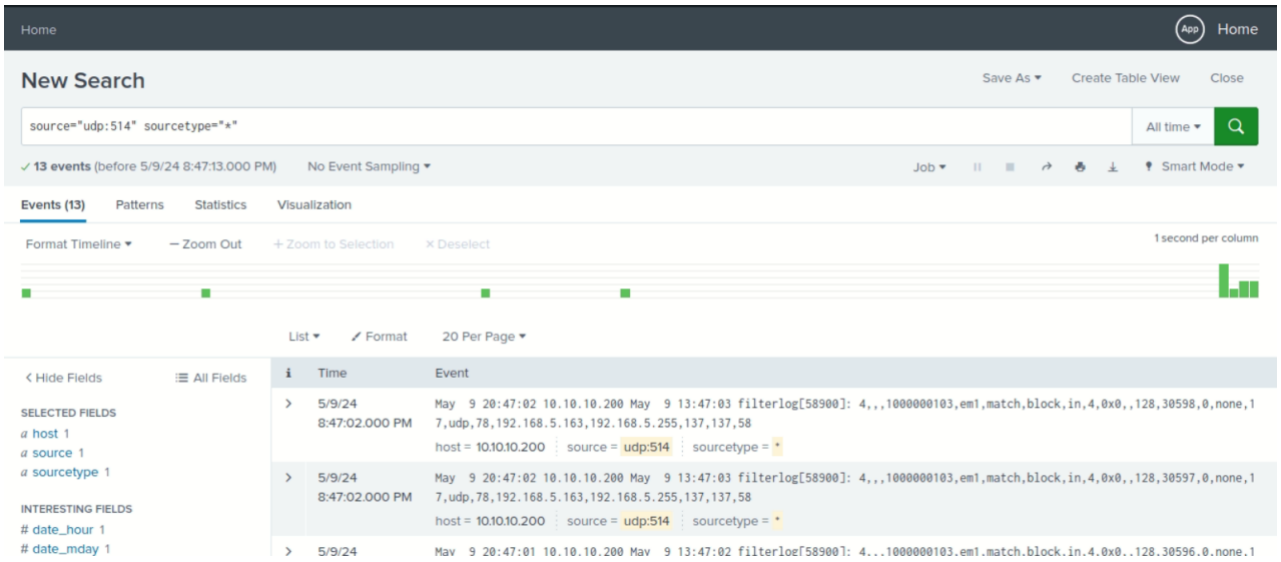
- Chọn Setting =>Data inputs
- Chọn Addnew trong phần UDP.
- Cấu hình port 514 và địa chỉ ip gửi log về là địa chỉ của tường lửa PfSense: 10.10.10.200. Sau đó chọn Next.



- Đặt các thông số theo hình và lưu kết quả



Bước 3: Kiểm tra log nhận được.



Như vậy, chúng ta đã cấu hình thành công đẩy log từ tường lửa PfSense sang Splunk. Splunk cung cấp cho chúng ta nhiều công cụ khác nhau để tìm kiếm, lọc, tạo các visulazation, dashboard, hỗ trợ cho việc phân tích, biểu diễn log.

Task: Dùng công cụ Search của Splunk, lọc ra những log block traffic của PfSense, từ đó đề xuất và xây dựng một Dashboard đơn giản biểu diễn log traffic của PfSense

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:

- File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
- Ví dụ: [NT534.K11.ANTN.1]-Lab1_1852xxxx_1852yyyy.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!