

# BÁO CÁO THỰC HÀNH

Môn học: An toàn mạng máy tính nâng cao

Lab 5: Xây dựng hệ thống giám sát mạng với PfSense và Splunk

GVHD: Đỗ Thị Phương Uyên

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT534.O21.ATTN

STT	Họ và tên	MSSV	Email
1	Hà Thị Thu Hiền	21522056	21522056@gm.uit.edu.vn
2	Phạm Ngọc Thơ	21522641	21522641@gm.uit.edu.vn
3	Nguyễn Ngọc Nhung	21521248	21521248@gm.uit.edu.vn
4	Đoàn Thị Ánh Dương	21521987	21521987@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

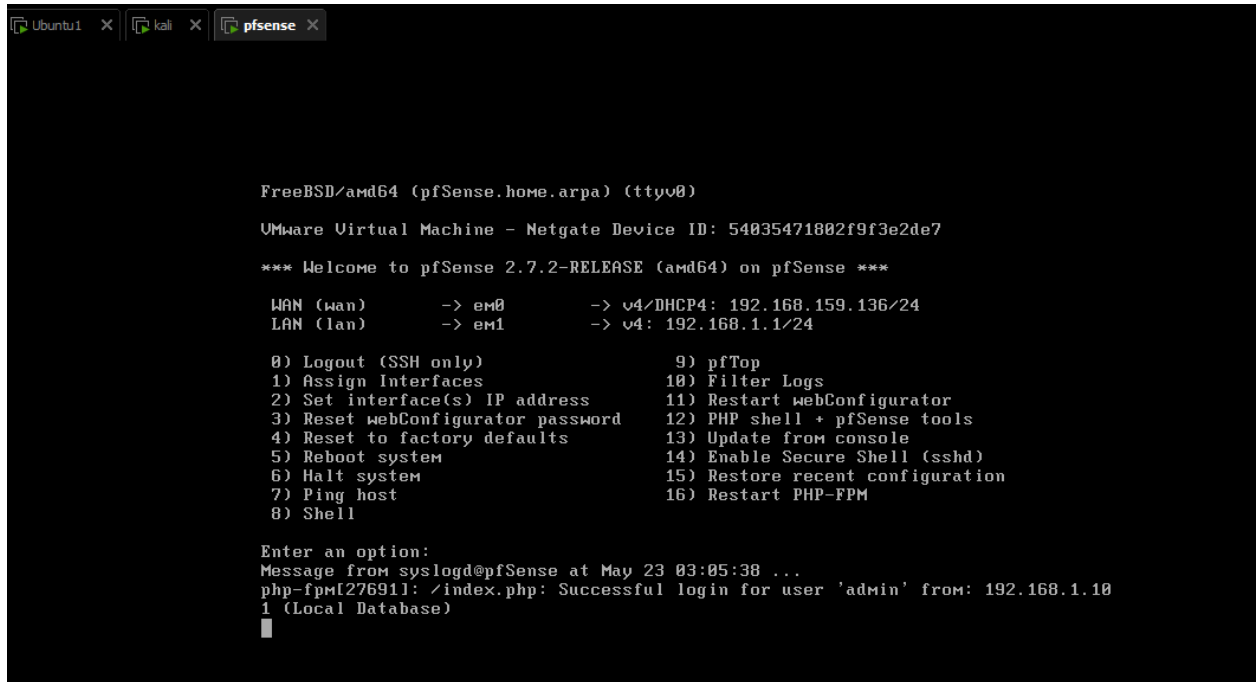
STT	Công việc	Kết quả tự đánh giá
1	Tất cả các bài tập	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

## BÁO CÁO CHI TIẾT

1. 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



```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 54035471802f9f3e2de7
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.159.136/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

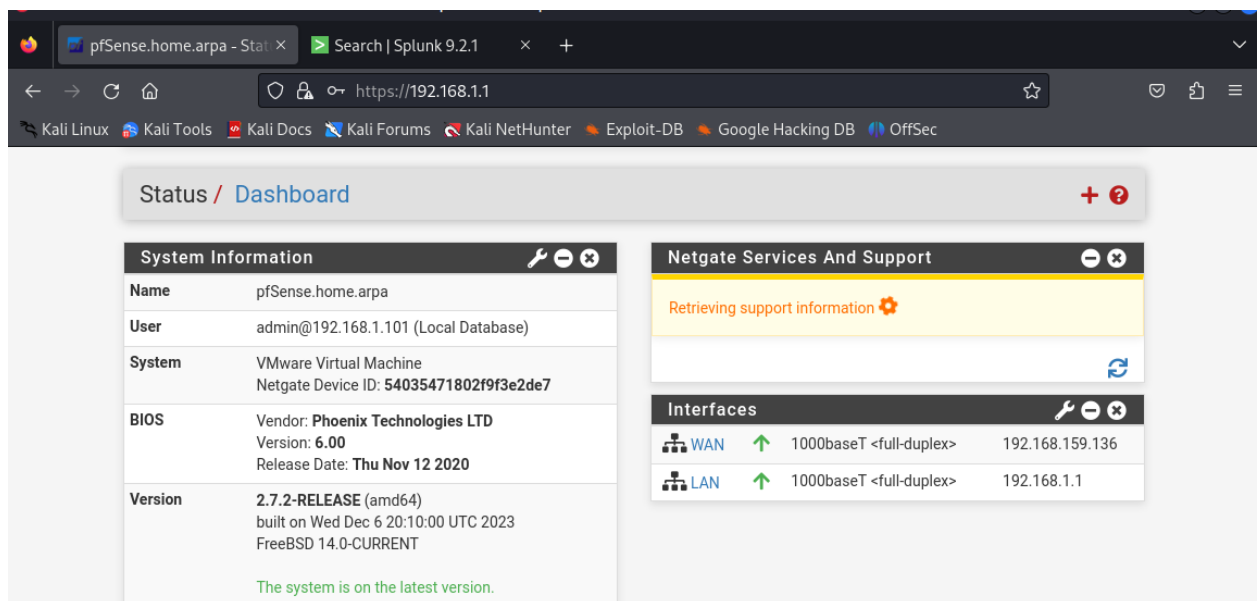
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

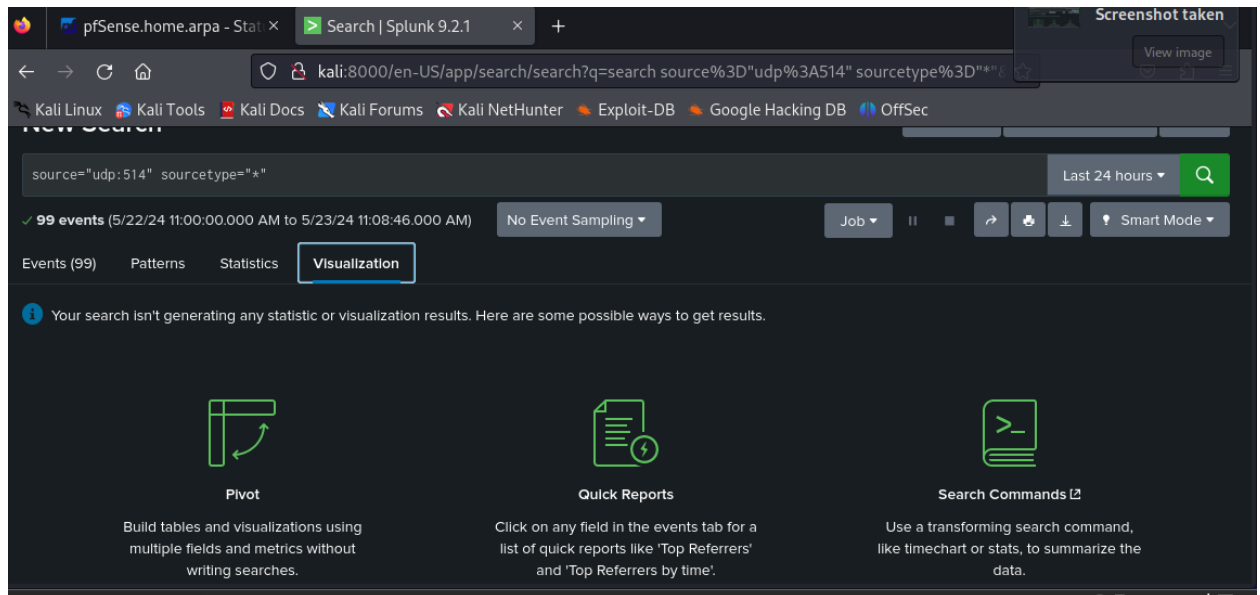
Enter an option:
Message from syslogd@pfSense at May 23 03:05:38 ...
php-fpm[276911]: /index.php: Successful login for user 'admin' from: 192.168.1.10
1 (Local Database)
```

```
(hahien@kali)-[/opt/splunk/bin]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::20c:29ff:fe1d:2ffb prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:1d:2f:fb txqueuelen 1000 (Ethernet)
    RX packets 13141 bytes 18218038 (17.3 MiB)
    RX errors 35 dropped 0 overruns 0 frame 0
    TX packets 6457 bytes 445490 (435.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 15472 bytes 26587162 (25.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15472 bytes 26587162 (25.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(hahien@kali)-[/opt/splunk/bin]
$
```





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.

Bước 1: Chọn Tab Dashboard. Chọn "Create New Dashboard" hoặc "New Dashboard".

Bước 2: Đặt tên cho Dashboard. Chọn không gian (app) mà bạn muốn lưu trữ dashboard. Đặt các tùy chọn bảo mật (Private, Shared in App, hoặc Global). Sau đó, nhấp vào "Create Dashboard".

Bước 3: Thêm Panels vào Dashboard.

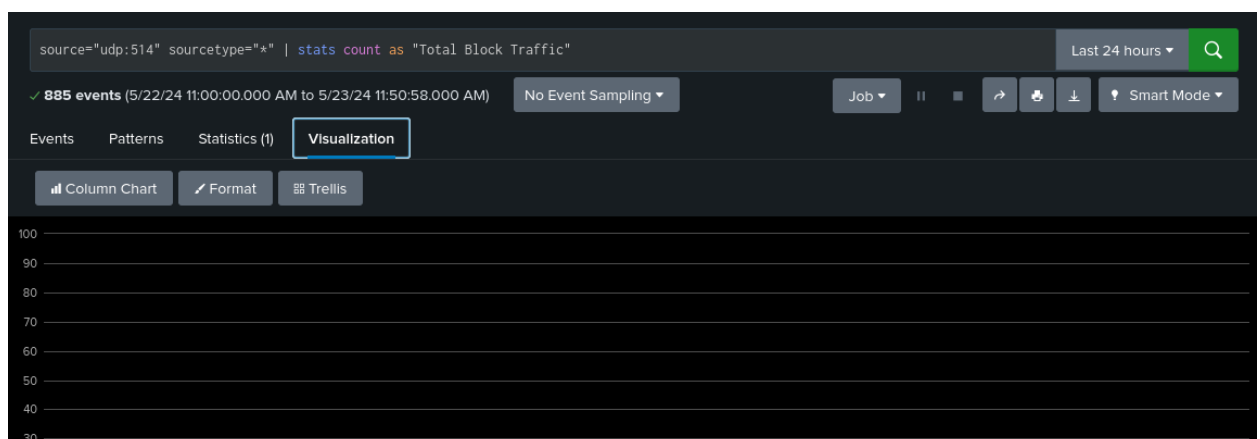
Sau khi tạo dashboard, chuyển đến giao diện chỉnh sửa dashboard. Nhấp vào "Add Panel". Chọn loại panel mà muốn thêm (ví dụ: search, pivot, prebuilt panel, hoặc panel từ một dashboard khác).

Ở đây, em chọn "New Search", sau đó nhập câu truy vấn Splunk muốn sử dụng.

Một số câu truy vấn:

- Tổng số lượng block traffic

`source="udp:514" sourcetype="*" | stats count as "Total Blocked Traffic"`



New data source

Data source name

TotalBlockedTraffic

☐ Access search results or metadata ?

SPL query [Open in search](#)

```
source="udp:514" sourcetype="*" | stats count as "Total Blocked Traffic"
```

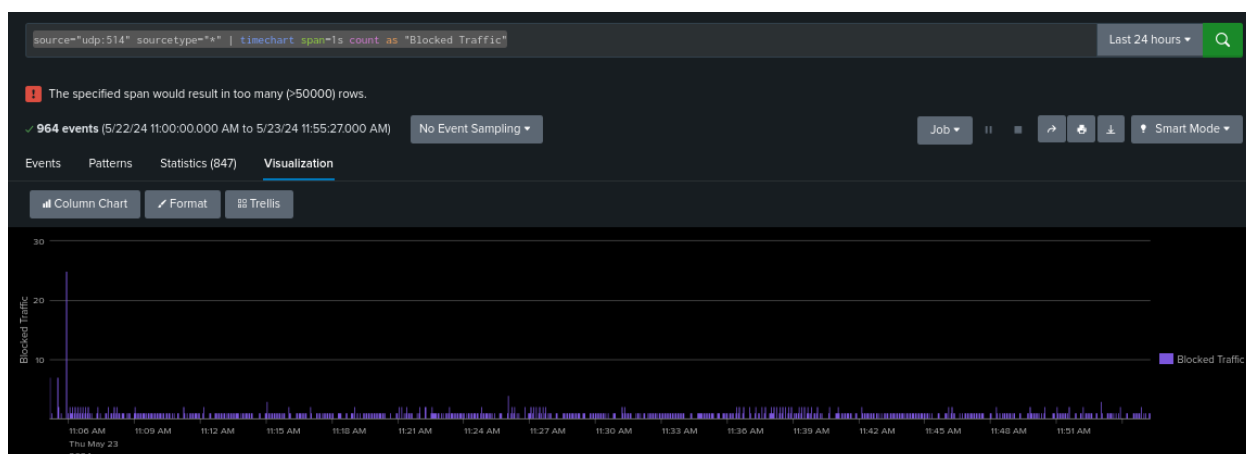
Time range

1 visualization will be updated

Cancel Apply and close

- Block traffic theo thời gian

source="udp:514" sourcetype="\*" | timechart span=1s count as "Blocked Traffic"



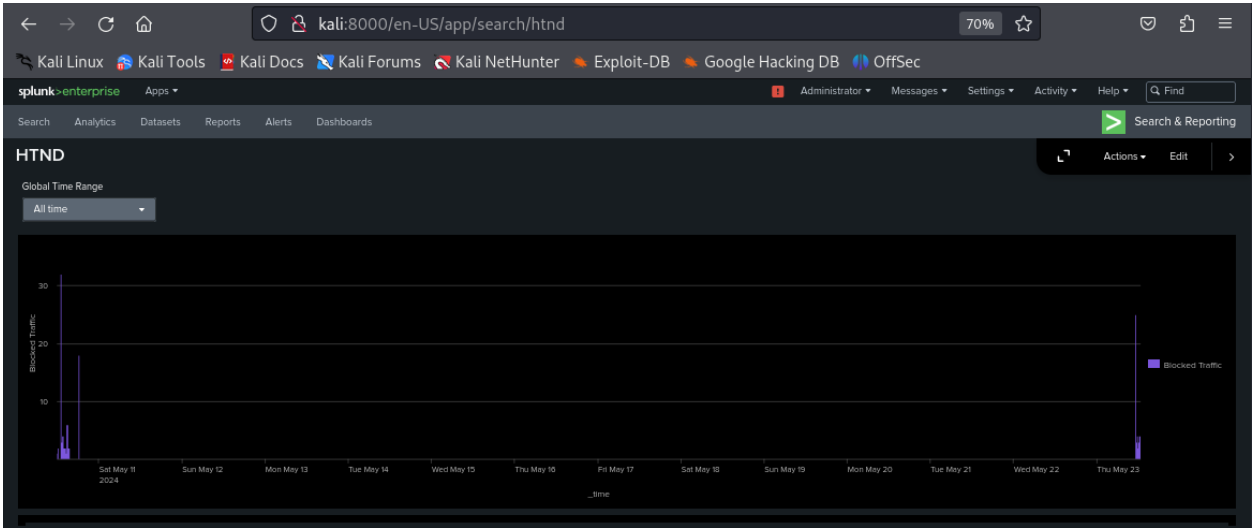
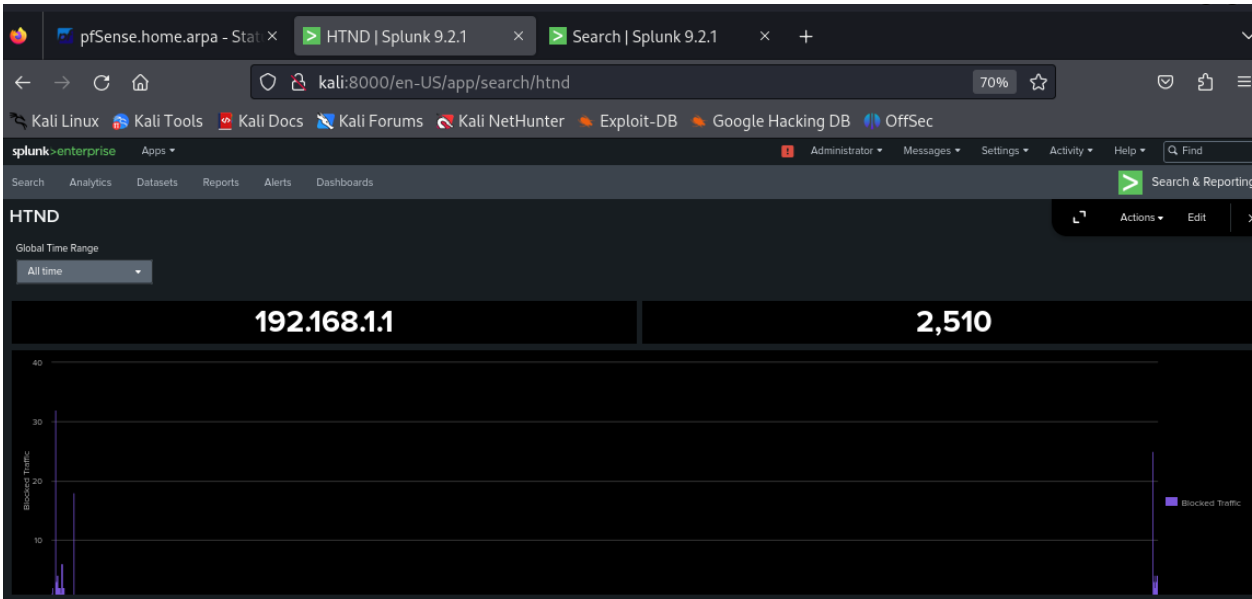
- Chi tiết các sự kiện block (Dynamic Panel):

source="udp:514" sourcetype="\*" | table \_time src\_ip dest\_ip protocol action

- Danh sách các host

source="udp:514" sourcetype="\*" | table host

Nhấn Save. Giao diện của dashboard như sau:



The screenshot shows the Splunk HTND dashboard with a table view of blocked traffic events. The table has columns for \_time, src\_ip, dest\_ip, protocol, and action. The data shows a series of blocked traffic events over time, with the most recent event occurring on May 23, 2024.

_time	src_ip	dest_ip	protocol	action
2024-05-23T11:48:24.000+08:00				
2024-05-23T11:48:23.000+08:00				
2024-05-23T11:48:22.000+08:00				
2024-05-23T11:48:17.000+08:00				
2024-05-23T11:48:16.000+08:00				
2024-05-23T11:48:14.000+08:00				
2024-05-23T11:48:14.000+08:00				
2024-05-23T11:47:59.000+08:00				
2024-05-23T11:47:58.000+08:00				
2024-05-23T11:47:57.000+08:00				



---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.DOCX và .PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).
- Ví dụ: [NT101.K11.ANTT]-Exe01\_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài nộp.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](https://courses.uit.edu.vn).

### Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

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

**HẾT**