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 |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **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.**

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**

A screenshot of a computer

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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"

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

- Block traffic theo thời gian

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

A screenshot of a computer

Description automatically generated

- 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:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

---

***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.

**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**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)