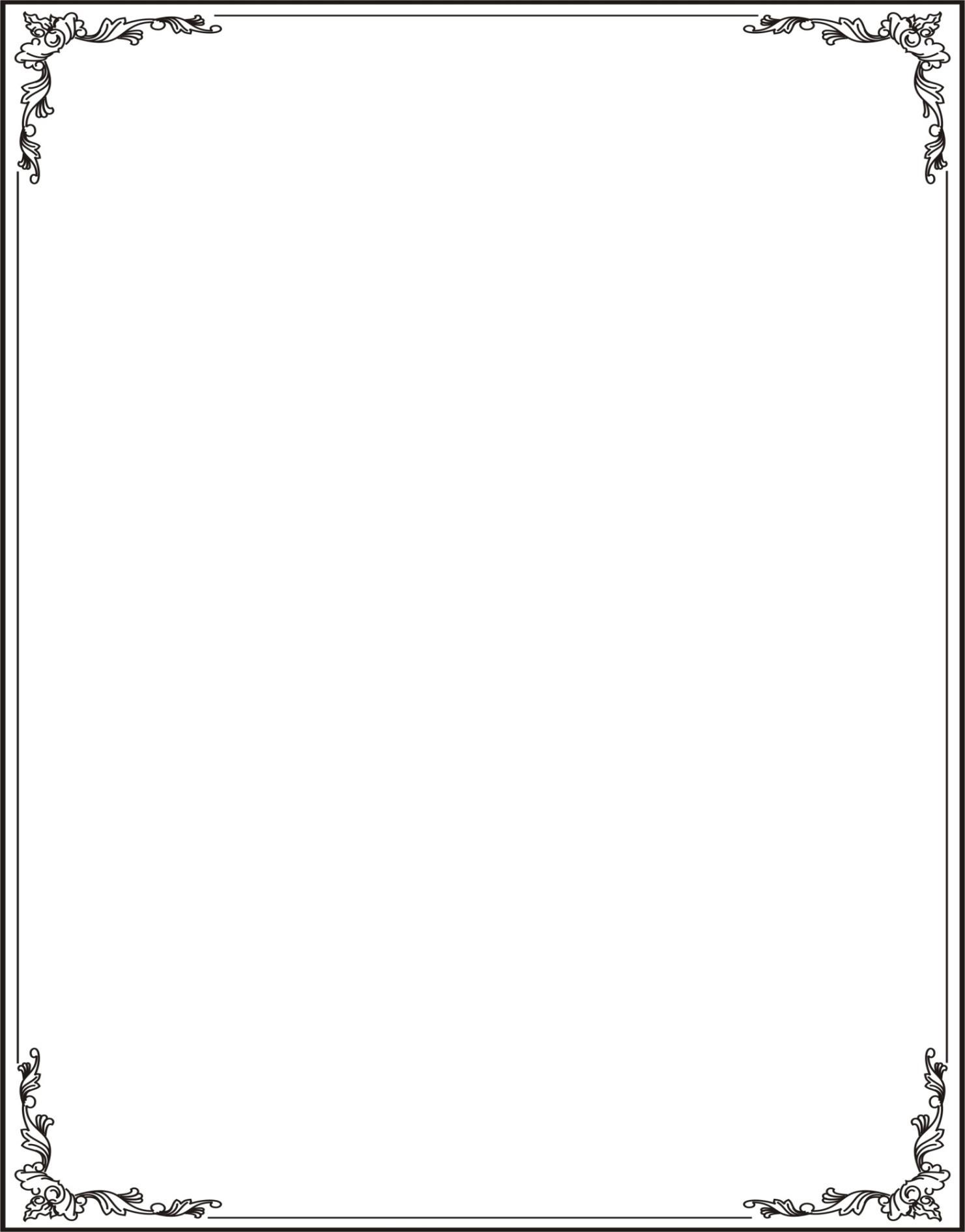
|  |
| --- |
| **HỌC VIỆN KỸ THUẬT MẬT MÃ** |
| **KHOA AN TOÀN THÔNG TIN** |





|  |
| --- |
| **BÁO CÁO MÔN HỌC** |
| **KỸ THUẬT LẬP TRÌNH** |

|  |
| --- |
| **ĐỀ TÀI** |
| **VẤN ĐỀ QUẢN LÝ LOGS TRONG HỆ THỐNG MẠNG** |

|  |  |
| --- | --- |
| Giáo viên hướng dẫn | **Bùi Việt Thắng** |
| Sinh viên thực hiện: | **Vũ Tiến Đạt**  **Đào Văn Trường**  **Đỗ Minh Nguyên**  **Nguyễn Mạnh Dương** |
| Nhóm | **6** |
| Lớp | **07** |

**MỤC LỤC**

[**DANH MỤC KÍ HIỆU VÀ VIẾT TẮT** 3](#_Toc129131775)

[**DANH MỤC HÌNH VẼ** 3](#_Toc129131776)

[**MỞ ĐẦU** 3](#_Toc129131777)

[**1. Lý do chọn đề tài** 3](#_Toc129131778)

[**2. Mục đích nghiên cứu** 3](#_Toc129131779)

[**3. Các nội dung chính đã thực hiện** 3](#_Toc129131780)

[**4. Kết cấu đề tài** 3](#_Toc129131781)

[**I.Tổng quan về quản lý Logs** 3](#_Toc129131782)

[**a. Giới thiệu quản lý Logs trong hệ thống mạng** 3](#_Toc129131783)

[**b. Các khái niệm và phân loại Logs** 3](#_Toc129131784)

[**b.1 Khái niệm** 3](#_Toc129131785)

[**b.2 Phân loại** 3](#_Toc129131786)

[**c. Tầm quan trọng của quản lý Logs trong mạng** 4](#_Toc129131787)

[**II. Phân tích yêu cầu quản lý Logs** 4](#_Toc129131788)

[**a.Định nghĩa yêu cầu của hệ thống quản lý Logs** 4](#_Toc129131789)

[**b. Xác định các mục tiêu quản lý Logs của hệ thống** 4](#_Toc129131790)

[**c. Phân tích các giải pháp quản lý Logs có sẵn** 4](#_Toc129131791)

[**III. Thiết kế hệ thống quản lý Logs** 4](#_Toc129131792)

[**a. Thiết kế kiến trúc của hệ thống quản lý Logs** 4](#_Toc129131793)

[**b. Thiết kế các thành phần trong hệ thống quản lý Logs** 4](#_Toc129131794)

[**c. Thiết kế giao diện và cơ chế báo động** 4](#_Toc129131795)

# **DANH MỤC KÍ HIỆU VÀ VIẾT TẮT**

# **DANH MỤC HÌNH VẼ**

# **MỞ ĐẦU**

## **1. Lý do chọn đề tài**

## **2. Mục đích nghiên cứu**

Nghiên cứu các vần đề trong quản lý Logs trong hệ thống mạng

## **3. Các nội dung chính đã thực hiện**

## **4. Kết cấu đề tài**

# **I.Tổng quan về quản lý Logs**

## **a. Giới thiệu quản lý Logs trong hệ thống mạng**

## **b. Các khái niệm và phân loại Logs**

### **b.1 Khái niệm**

- Log ghi lại liên tục các thông báo về hoạt động của cả hệ thống hoặc của các dịch vụ được triển khai trên hệ thống và file tương ứng. Log file thường là các file văn bản thông thường dưới dạng “clear text” tức là bạn có thể dễ dàng đọc được nó, vì thế có thể sử dụng các trình soạn thảo văn bản (vi, vim, nano…) hoặc các trình xem văn bản thông thường (cat, tailf, head…) là có thể xem được file log.

- Các file log có thể nói cho bạn bất cứ thứ gì bạn cần biết, để giải quyết các rắc rối mà bạn gặp phải miễn là bạn biết ứng dụng nào. Mỗi ứng dụng được cài đặt trên hệ thống có cơ chế tạo log file riêng của mình để bất cứ khi nào bạn cần thông tin cụ thể thì các log file là nơi tốt nhất để tìm.

- Các tập tin log được đặt trong thư mục **/var/log**. Bất kỳ ứng dụng khác mà sau này bạn có thể cài đặt trên hệ thống của bạn có thể sẽ tạo tập tin log của chúng tại **/var/log**. Dùng lệnh **ls -l /var/log**để xem nội dung của thư mục này.

### **b.2 Phân loại**

#### **b.2.1 Syslog**

Syslog là một giao thức client/server là giao thức dùng để chuyển log và thông điệp đến máy nhận log. Máy nhận log thường được gọi là syslogd, syslog daemon hoặc syslog server. Syslog có thể gửi qua UDP hoặc TCP. Các dữ liệu được gửi dạng cleartext. Syslog dùng cổng 514.

Syslog ban đầu sử dụng UDP, điều này là không đảm bảo cho việc truyền tin. Tuy nhiên sau đó IETF đã ban hành RFC 3195 (Đảm bảo tin cậy cho syslog) và RFC 6587 (Truyền tải thông báo syslog qua TCP). Điều này có nghĩa là ngoài UDP thì giờ đây syslog cũng đã sử dụng TCP để đảm bảo an toàn cho quá trình truyền tin.

Trong chuẩn syslog, mỗi thông báo đều được dán nhãn và được gán các mức độ nghiêm trọng khác nhau. Các loại phần mềm sau có thể sinh ra thông báo: auth, authPriv, daemon, cron, ftp, dhcp, kern, mail, syslog, user,... Với các mức độ nghiêm trọng từ cao nhất trở xuống Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug.

#### **b.2.2 Rsyslog**

Rsyslog - "The rocket-fast system for log processing" được bắt đầu phát triển từ năm 2004 bởi Rainer Gerhards rsyslog là một phần mềm mã nguồn mở sử dụng trên Linux dùng để chuyển tiếp các log message đến một địa chỉ trên mạng (log receiver, log server) Nó thực hiện giao thức syslog cơ bản, đặc biệt là sử dụng TCP cho việc truyền tải log từ client tới server. Hiện nay rsyslog là phần mềm được cài đặt sẵn trên hầu hết hệ thống Unix và các bản phân phối của Linux như : Fedora, openSUSE, Debian, Ubuntu, Red Hat Enterprise Linux, FreeBSD…

**c. Tầm quan trọng của quản lý Logs trong mạng**  
Đây là những điều rất quan trọng bởi vì:

Bộ định tuyến của bạn có thể dễ dàng bị xâm phạm nếu không có cấu hình và hạn chế phù hợp.

Nếu tường lửa không được định cấu hình chính xác, tin tặc có thể dễ dàng phát hiện ra một cổng vô tình bị bỏ ngỏ và có thể truy cập vào mạng.

Các điểm truy cập giả mạo, phần mềm độc hại botnet và kỹ thuật xã hội có thể khiến mạng không dây của bạn trở thành một lỗ hổng trong mạng LAN của bạn.

Để vạch trần một cuộc tấn công hoặc xác định thiệt hại gây ra, bạn cần phân tích các sự kiện nhật ký trên mạng của mình theo thời gian thực. Bằng cách thu thập và phân tích nhật ký, bạn có thể hiểu những gì diễn ra trong mạng của mình. Mỗi tệp nhật ký chứa nhiều mẩu thông tin có thể là vô giá

# **II. Phân tích yêu cầu quản lý Logs**

## **a.Định nghĩa yêu cầu của hệ thống quản lý Logs**

## **b. Xác định các mục tiêu quản lý Logs của hệ thống**

## **c. Phân tích các giải pháp quản lý Logs có sẵn**

# **III. Thiết kế hệ thống quản lý Logs**

## **a. Thiết kế kiến trúc của hệ thống quản lý Logs**

## **b. Thiết kế các thành phần trong hệ thống quản lý Logs**

## **c. Thiết kế giao diện và cơ chế báo động**