**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

**BÁO CÁO BÀI THỰC HÀNH**

Khám phá Nhật ký (Log) Unix

Họ và tên sinh viên: Lê Anh Tuấn

Mã số sinh viên: B21DCAT205

Họ và tên giảng viên: TS. Đinh Trường Duy

Hà Nội 11 năm 2023

**1. GIỚI THIỆU BÀI THỰC HÀNH**

**1.1 Mục đích**

- Mục tiêu của bài tập này là để cung cấp cho sinh viên một trải nghiệm thực tế với cấu hình và kiểm thử syslog.

**1.2 Yêu cầu**

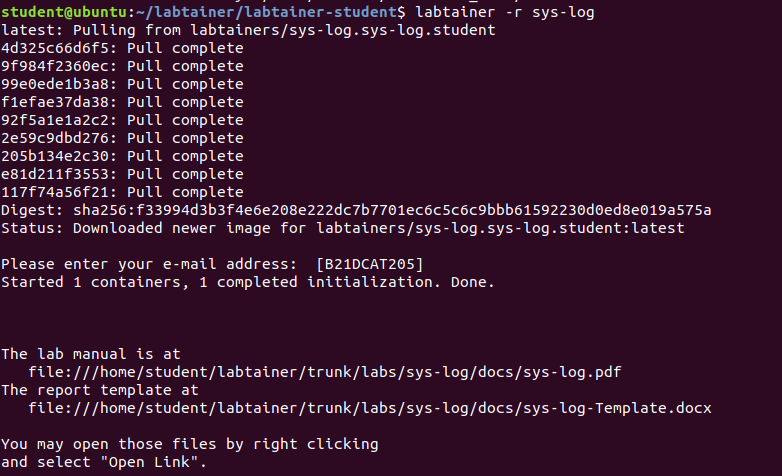
- Nắm được kiến thức về syslog và Linux.

**2 NỘI DUNG THỰC HÀNH**

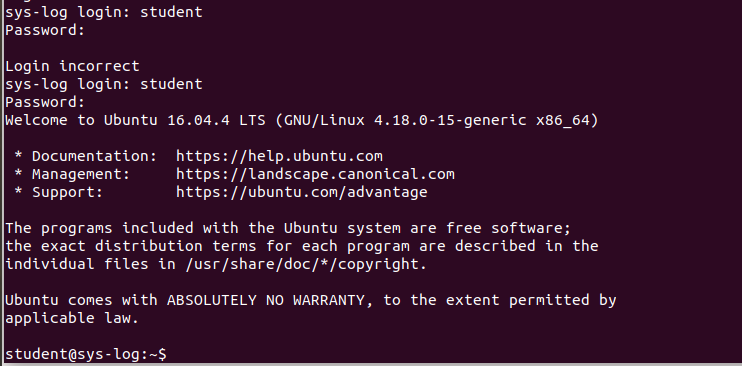
**Chuẩn bị lab**

                 Khởi động lab:

labtainer –r sys-log

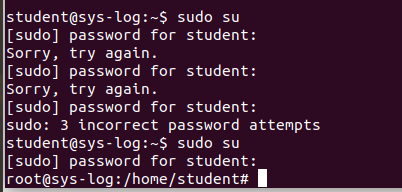
****

Đăng nhập sinh viên tài khoản: **student** và mật khẩu **password123**

****

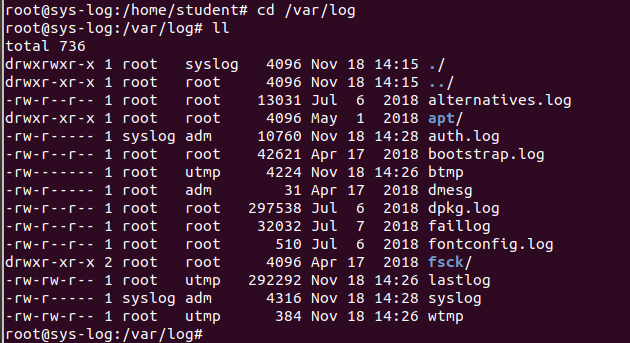
**Nhiệm vụ 1:** Khám phá

* Trong terminal, nhập lệnh sudo su nhưng nhập sai mật khẩu cho người dùng student.
* Sau đó nhập lại lệnh sudo su, nhưng lần này nhập đúng mật khẩu cho sinh viên, đó là password123. Nếu làm đúng, dấu nhắc sẽ kết thúc sinh viêng ký tự '#'.

****

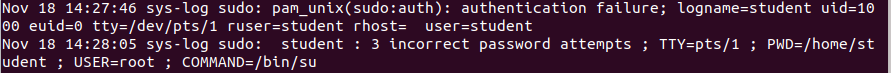
* Khám phá thư mục log

- Thay đổi thư mục làm việc hiện tại thành /var/log sau đó liệt kê nội dung của /var/log.

****

* Mật khẩu sai

- Sử dụng *cat /var/log/auth.log.* Mở tệp và tìm kiếm sự thất bại khi sinh viên cố gắng đăng nhập sinh viên tên người dùng student.

****

* Mật khẩu là tên người dùng

 - Với tệp nhật ký auth.log vẫn mở, tìm dòng ghi chú cho biết sinh viên đã nhập "password" làm tên người dùng.



- Cụm từ được sử dụng khi sinh viên nhập một tên người dùng không hợp lệ.

****

* Tệp wtmp

- Đọc phần DESCRIPTION trong trang man để tìm hiểu chức năng của lệnh.

- Chức năng được cung cấp bởi tùy chọn -t của lệnh last: Cho biết trạng thái của những đăng nhập với thời gian cụ thể.

****

**Nhiệm vụ 2:**Cấu hình lại rsyslog cho MARK

* Mở tệp cấu hình rsyslog.

Sử dụng câu lệnh *leafpad /etc/rsyslog.conf*

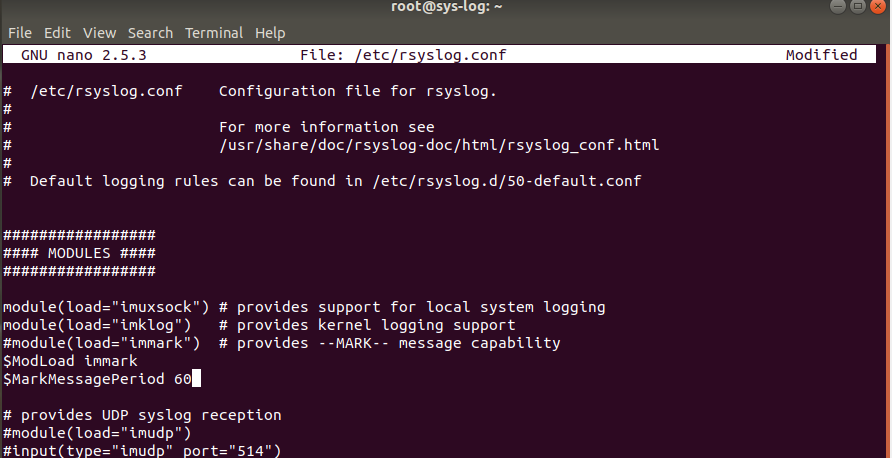
* Bật tính năng Mark.

- Trong phần "### MODULES ###", tìm dòng có "#module(load="imark")", và sau dòng đó, thêm hai dòng sau:

*$ModLoad immark*

*$MarkMessagePeriod 60*

- Lưu thay đổi và thoát khỏi trình soạn thảo sử dụng crtl+o -> enter, để thoát crtl+x.

****

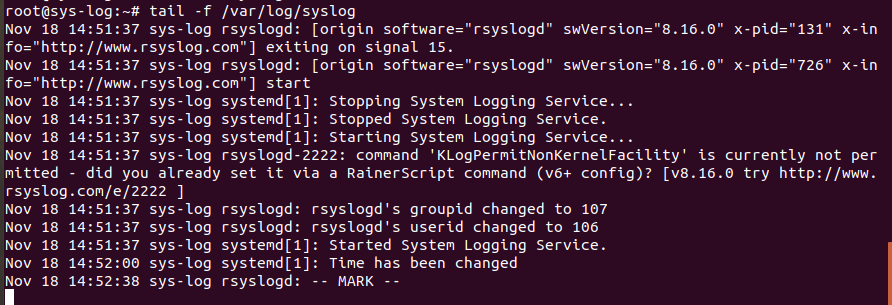
* Khởi động lại tiến trình rsyslog.

*service rsyslog restart*



* Xem hiệu quả của thay đổi này trong các nhật ký sinh viêng cách sử dụng lệnh tail như sau:

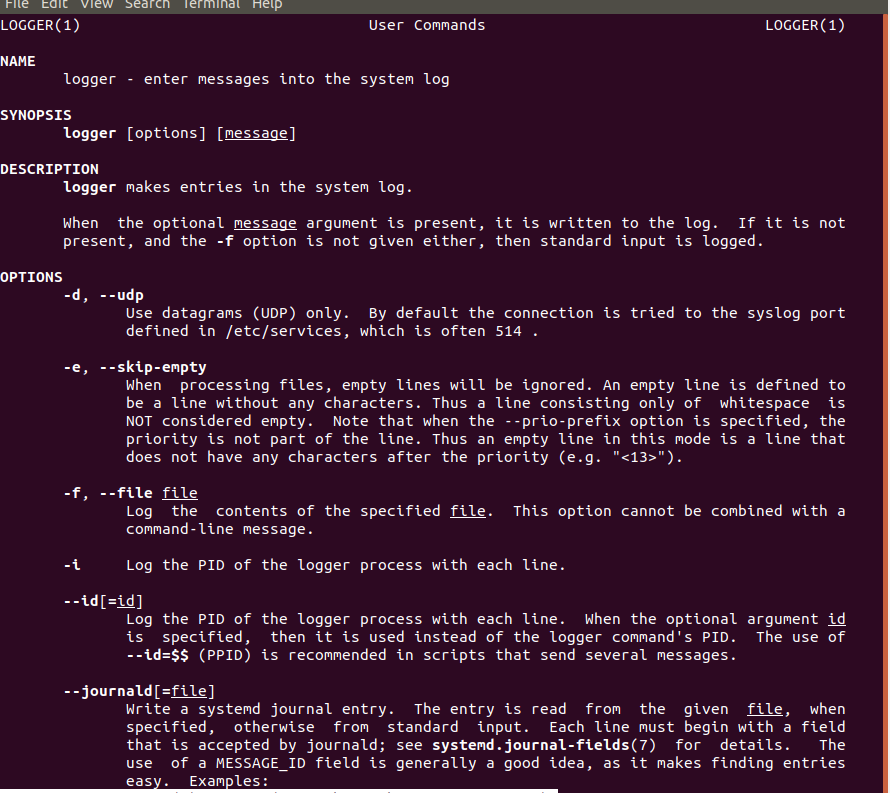
*tail -f /var/log/syslog*



**Nhiệm vụ 3:**Cấu hình lại và kiểm tra rsyslog

* Đọc phần DESCRIPTION trong trang man của tiện ích logger:

*man logger*



* Tạo một mục trong /var/log/syslog với mức ưu tiên "info" sinh viên cách thực hiện các bước sau:

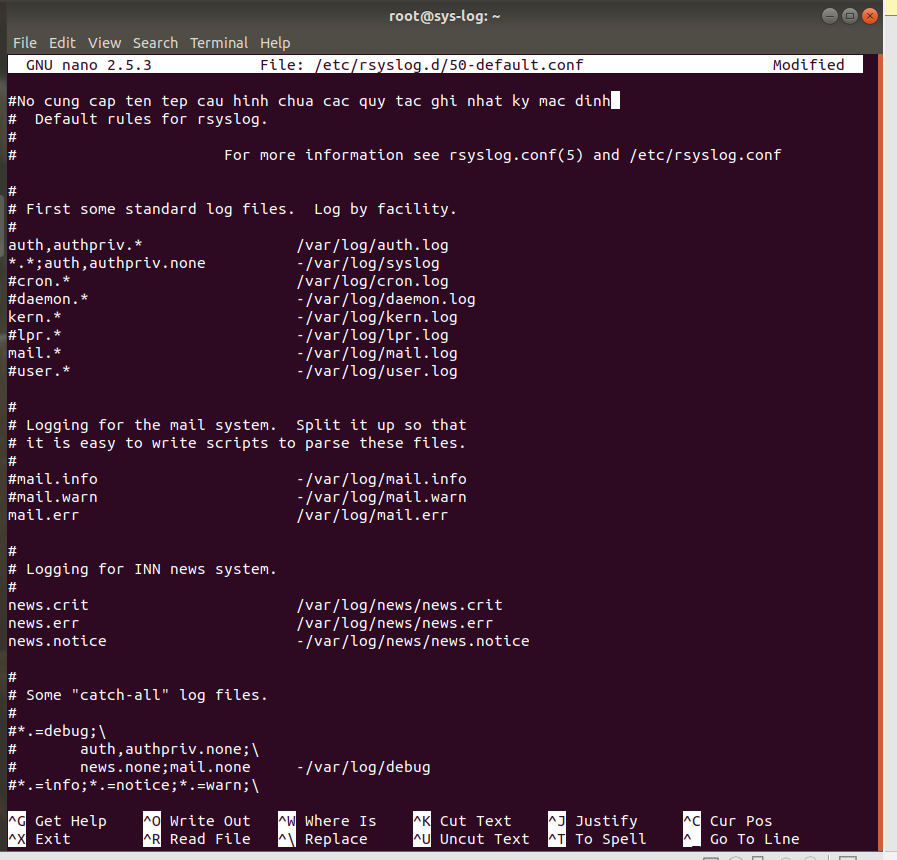
*logger -p info "Hello World"*

Khi không chỉ định cơ sở dữ liệu, như trong trường hợp của lệnh trên, cơ sở dữ liệu "user" được sử dụng mặc định.



* Mở lại tệp cấu hình rsyslog tại */etc/rsyslog.d/50-default.conf* và ghi lại trong phần đầu của nó rằng nó cung cấp tên tệp cấu hình chứa các quy tắc ghi nhật ký mặc định. Mở tệp đó.

*nano /etc/rsyslog.d/50-default.conf*



* Quy tắc syslog chỉ định điều gì sẽ xảy ra với mục sinh viên gửi đến syslog trong bước #2 ở trên.

*Quy tắc được đưa vào:*

***if $syslogseverity-text == 'info' then /var/log/messages***

*Trong quy tắc này:*

* ***if $syslogseverity-text == 'info'*** *kiểm tra xem mức ưu tiên của thông điệp là "info".*
* ***then /var/log/messages*** *cho biết rằng thông điệp có mức ưu tiên "info" sẽ được ghi vào tệp* ***/var/log/messages***
* Thoát khỏi trình soạn thảo.
* Sử dụng grep để xác minh rằng mục nhật ký của ta đã được lưu trong tệp *syslog.*

****

* Mở lại tệp cấu hình */etc/rsyslog.d/50-default.conf.*

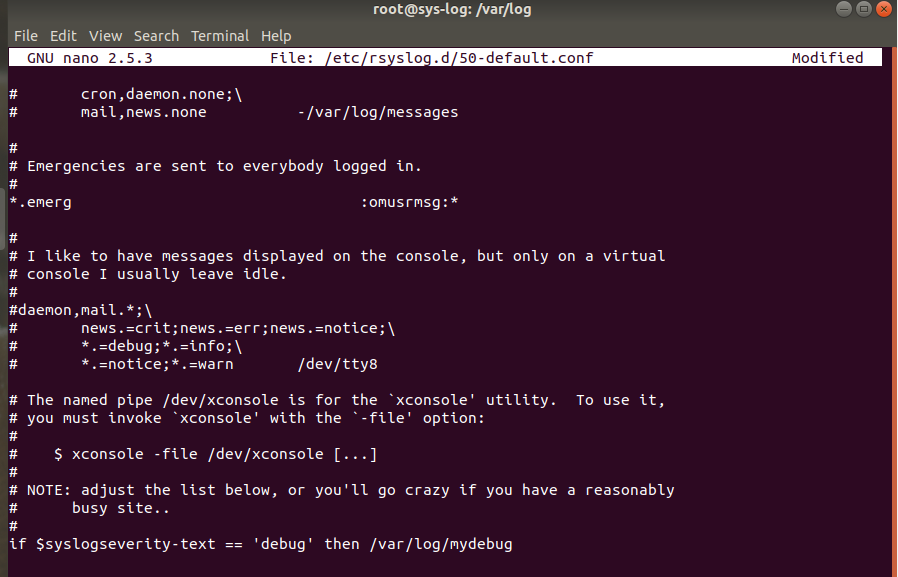
Thêm một quy tắc syslog mới để đưa tất cả các thông báo với mức ưu tiên "debug" vào một tệp có tên là /var/log/mydebug. Tệp này chỉ nên chứa các thông báo debug.

* Quy tắc sinh viên đã sử dụng để đáp ứng yêu cầu trên.

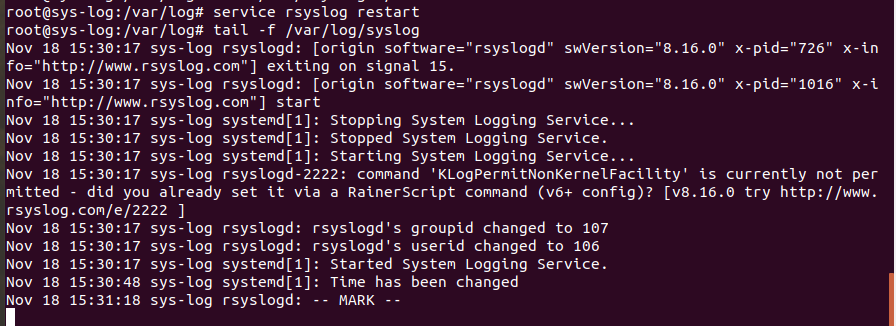
*Quy tắc được thêm vào file rsyslog.conf :*

***if $syslogseverity-text == 'debug' then /var/log/mydebug***

* ***if $syslogseverity-text == 'debug'****: Điều này là điều kiện để kiểm tra thông điệp log. Nó kiểm tra mức độ ưu tiên của thông điệp log. Cụ thể, nó kiểm tra xem mức độ ưu tiên của thông điệp log có phải là "debug" hay không. Nếu mức độ ưu tiên của thông điệp log là "debug," điều kiện này trở thành đúng.*
* ***then /var/log/mydebug****: Nếu điều kiện trên là đúng (mức độ ưu tiên là "debug"), quy tắc này chỉ định nơi thông điệp log sẽ được ghi. Trong trường hợp này, thông điệp log với mức độ ưu tiên "debug" sẽ được ghi vào tệp log* ***/var/log/mydebug****.*



* Khởi động lại rsyslog (để quy tắc mới có hiệu lực):



* Bây giờ ta đã biết cách sử dụng logger, hãy sử dụng nó để kiểm tra quy tắc ta đã thêm vào quy tắc mặc định ở bước #6 ở trên.



Mô tả cách ta đã sử dụng logger (và các lệnh khác) để kiểm tra quy tắc sinh viên đã thêm trong bước #6: Sử dụng câu lệnh logger -p debug <Message>, sau đó sử dụng lệnh cat mydebug để xem message vừa thêm

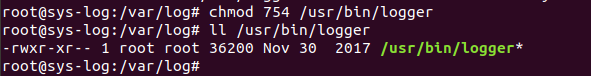
* Thực hiện các bước sau để hiển thị quyền liên quan đến lệnh logger:

*ll /usr/bin/logger*



Để chỉ cho phép người dùng root và nhóm root thực thi tệp logger, bạn cần gỡ bỏ quyền thực thi (x) cho người dùng. Bạn có thể sử dụng lệnh chmod như sau: sudo chmod 754 /bin/logger

Với quyền đọc (4), ghi (2) và thực thi (1).

****

**Nhiệm vụ 4:**Các câu hỏi khác

* **Mô tả bất kỳ thử nghiệm hoặc khám phá bổ sung nào sinh viên đã thực hiện.**

- Tìm hiểu thêm về các mức ưu tiên (priority levels) trong hệ thống log, như "emerg", "alert", "crit", "err", "warning", "notice", "info", và "debug".

- Thử nghiệm thêm các tùy chọn của lệnh last

* **Sinh viên đã học được điều gì từ bài thực hành này**

- Từ bài thực hành này, sinh viên đã học được nhiều điều quan trọng liên quan đến hệ thống ghi log và quản lý log trên hệ thống Linux, bao gồm:

1. Hiểu về cơ bản về ghi log: Sinh viên đã học về ý nghĩa và quá trình ghi log trên hệ thống, bao gồm việc thu thập thông tin liên quan đến hoạt động của hệ thống, ứng dụng và người dùng.
2. Sử dụng rsyslog: Sinh viên đã học cách sử dụng rsyslog, một công cụ quan trọng trong việc quản lý log trên Linux, để cấu hình quy tắc ghi log và xử lý thông báo log.
3. Quản lý tệp log: Sinh viên đã học cách quản lý các tệp log trên hệ thống, bao gồm việc cấu hình nơi lưu trữ log, quản lý tệp log đã xoay vòng và xác định quyền truy cập cho các tệp log.
4. Sử dụng lệnh logger: Sinh viên đã hiểu cách sử dụng lệnh logger để tạo và ghi thông báo vào log, cũng như cách sử dụng các mức ưu tiên và các facility khác nhau.
5. Hiểu về quyền truy cập và quản lý tệp: Sinh viên đã học cách kiểm tra và thay đổi quyền truy cập cho các tệp log, đặc biệt là cách đảm bảo chỉ người dùng hoặc nhóm cụ thể có quyền truy cập vào tệp log.
6. Hiểu về cấu hình rsyslog: Sinh viên đã làm quen với cấu hình rsyslog thông qua tệp cấu hình rsyslog.conf, bao gồm việc thêm và chỉnh sửa quy tắc log.
7. Theo dõi và kiểm tra log: Sinh viên đã học cách theo dõi log và kiểm tra việc ghi log thông qua các lệnh như tail, cat và last.

* **Cần làm gì để cải thiện bài thực hành này?**

- Trong bài thực hành trên chỉ có một máy trạm, vì vậy nên ta có thể thử nghiệm với nhiều máy trạm gửi thông báo log tới máy chủ.

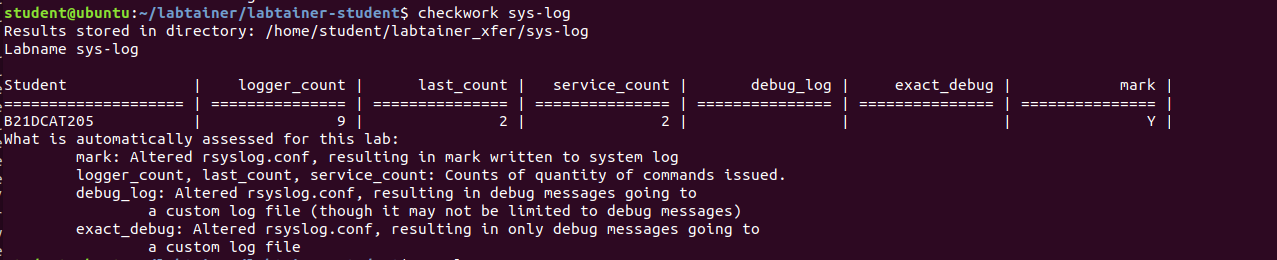
- Các máy trạm và máy chủ có thể cùng mạng LAN hoặc không cùng mạng LAN.

- Thử nghiệm thêm các tùy chọn của công cụ logger (-i , -t , -T, -P,…).

- Thử nghiệm tấn công đăng nhập từ xa bằng cách thử mật khẩu (ssh, telnet) và quan sát file nhật kí.

- Xác thực và mã hóa log trên rsyslog(cài đặt gói gnutls – một thư viện mã hóa).

**Checkwork sau khi hoàn thành**

****