**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

```
student@ubuntu:~/labtainer/labtainer-student$ labtainer -r sys-log
latest: Pulling from labtainers/sys-log.sys-log.student
4d325c66d6f5: Pull complete
9f984f2360ec: Pull complete
99e0ede1b3a8: Pull complete
f1efae37da38: Pull complete
92f5a1e1a2c2: Pull complete
2e59c9dbd276: Pull complete
205b134e2c30: Pull complete
e81d211f3553: Pull complete
117f74a56f21: Pull complete
Digest: sha256:f33994d3b3f4e6e208e222dc7b7701ec6c5c6c9bbb61592230d0ed8e019a575a
Status: Downloaded newer image for labtainers/sys-log.sys-log.student:latest

Please enter your e-mail address:  [B21DCAT205]
Started 1 containers, 1 completed initialization. Done.



The lab manual is at
   file:///home/student/labtainer/trunk/labs/sys-log/docs/sys-log.pdf
The report template at
   file:///home/student/labtainer/trunk/labs/sys-log/docs/sys-log-Template.docx

You may open those files by right clicking
and select "Open Link".
```

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

```
sys-log login: student
Password:

Login incorrect
sys-log login: student
Password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@sys-log:~$
```

**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 '#'.

```
student@sys-log:~$ sudo su
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
Sorry, try again.
[sudo] password for student:
sudo: 3 incorrect password attempts
student@sys-log:~$ sudo su
[sudo] password for student:
root@sys-log:/home/student#
```

- 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.

```
root@sys-log:/home/student# cd /var/log
root@sys-log:/var/log# ll
total 736
drwxrwxr-x 1 root   syslog   4096 Nov 18 14:15 ./
drwxr-xr-x 1 root   root     4096 Nov 18 14:15 ../
-rw-r--r-- 1 root   root    13031 Jul  6  2018 alternatives.log
drwxr-xr-x 1 root   root     4096 May  1  2018 apt/
-rw-r----- 1 syslog adm     10760 Nov 18 14:28 auth.log
-rw-r--r-- 1 root   root    42621 Apr 17  2018 bootstrap.log
-rw------- 1 root   utmp     4224 Nov 18 14:26 btmp
-rw-r----- 1 root   adm        31 Apr 17  2018 dmesg
-rw-r--r-- 1 root   root   297538 Jul  6  2018 dpkg.log
-rw-r--r-- 1 root   root    32032 Jul  7  2018 faillog
-rw-r--r-- 1 root   root      510 Jul  6  2018 fontconfig.log
drwxr-xr-x 2 root   root     4096 Apr 17  2018 fsck/
-rw-rw-r-- 1 root   utmp   292292 Nov 18 14:26 lastlog
-rw-r----- 1 syslog adm      4316 Nov 18 14:28 syslog
-rw-rw-r-- 1 root   utmp      384 Nov 18 14:26 wtmp
root@sys-log:/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.

```
Nov 18 14:27:46 sys-log sudo: pam_unix(sudo:auth): authentication failure; logname=student uid=10
00 euid=0 tty=/dev/pts/1 ruser=student rhost=  user=student
Nov 18 14:28:05 sys-log sudo:  student : 3 incorrect password attempts ; TTY=pts/1 ; PWD=/home/st
udent ; USER=root ; COMMAND=/bin/su
```

- 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.

```
Nov 18 14:42:43 sys-log login[455]: pam_unix(login:auth): check pass; user unknown
```

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

```
Nov 18 14:25:38 sys-log login[206]: FAILED LOGIN (2) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
```

- 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.

```
-t, --until time
       Display the state of logins until the specified time.
```

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

- Mở tệp cấu hình rsyslog.
  Sử dụng câu lệnh *leafpad /etc/rsyslog.conf*

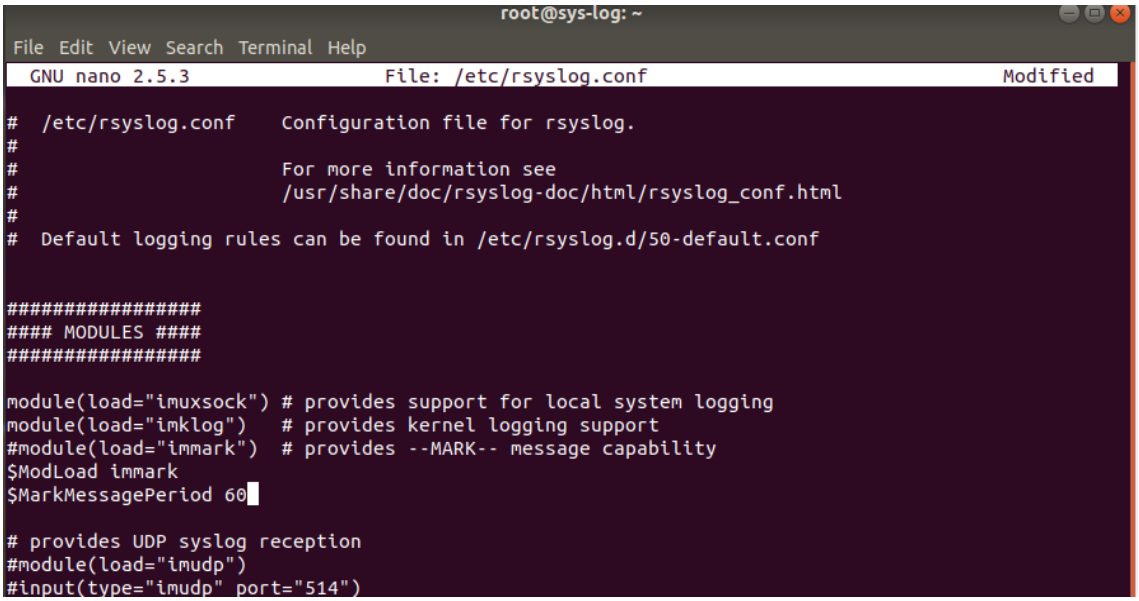
- Bật tính năng Mark.

  - 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*

```
root@sys-log:~# service rsyslog restart
root@sys-log:~#
```

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

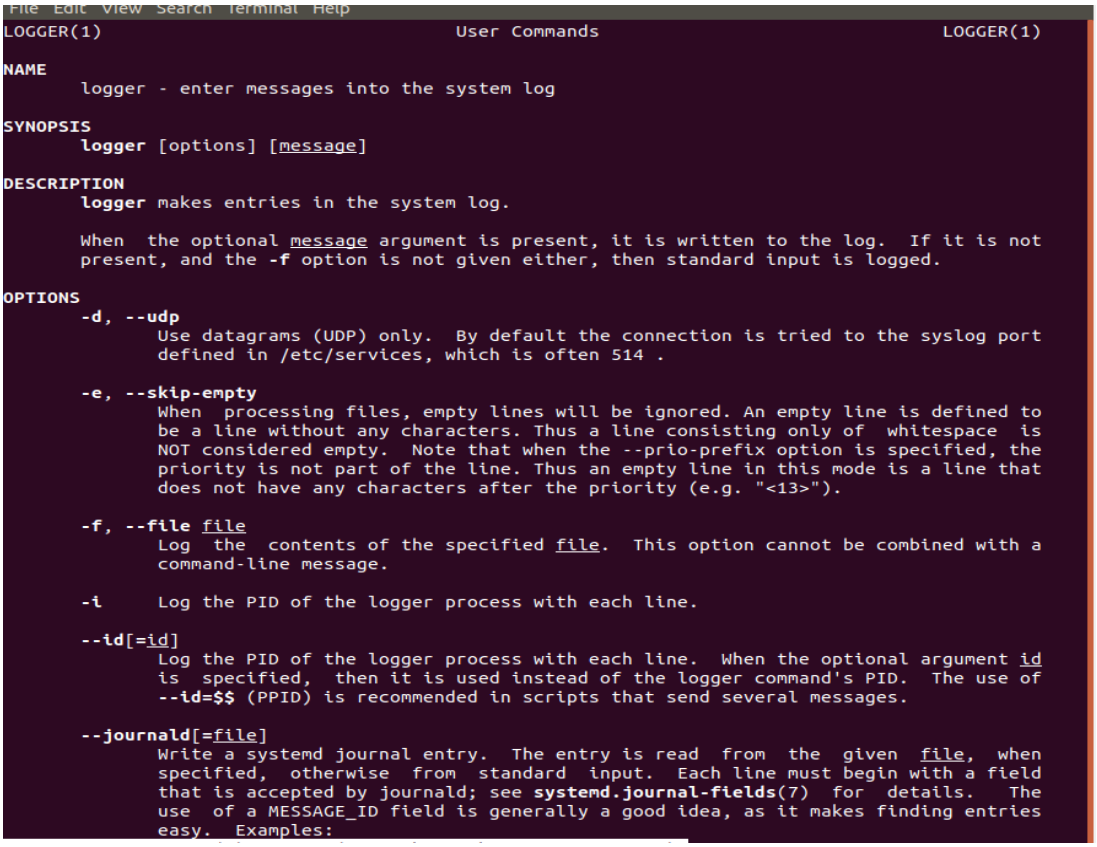
  *tail -f /var/log/syslog*

```
root@sys-log:~# tail -f /var/log/syslog
Nov 18 14:51:37 sys-log rsyslogd: [origin software="rsyslogd" swVersion="8.16.0" x-pid="131" x-in
fo="http://www.rsyslog.com"] exiting on signal 15.
Nov 18 14:51:37 sys-log rsyslogd: [origin software="rsyslogd" swVersion="8.16.0" x-pid="726" x-in
fo="http://www.rsyslog.com"] start
Nov 18 14:51:37 sys-log systemd[1]: Stopping System Logging Service...
Nov 18 14:51:37 sys-log systemd[1]: Stopped System Logging Service.
Nov 18 14:51:37 sys-log systemd[1]: Starting System Logging Service...
Nov 18 14:51:37 sys-log rsyslogd-2222: command 'KLogPermitNonKernelFacility' is currently not per
mitted - did you already set it via a RainerScript command (v6+ config)? [v8.16.0 try http://www.
rsyslog.com/e/2222 ]
Nov 18 14:51:37 sys-log rsyslogd: rsyslogd's groupid changed to 107
Nov 18 14:51:37 sys-log rsyslogd: rsyslogd's userid changed to 106
Nov 18 14:51:37 sys-log systemd[1]: Started System Logging Service.
Nov 18 14:52:00 sys-log systemd[1]: Time has been changed
Nov 18 14:52:38 sys-log rsyslogd: -- MARK --
```

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

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

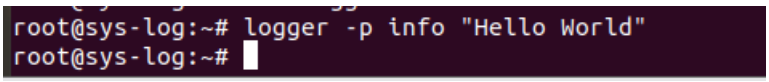
  *man logger*




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

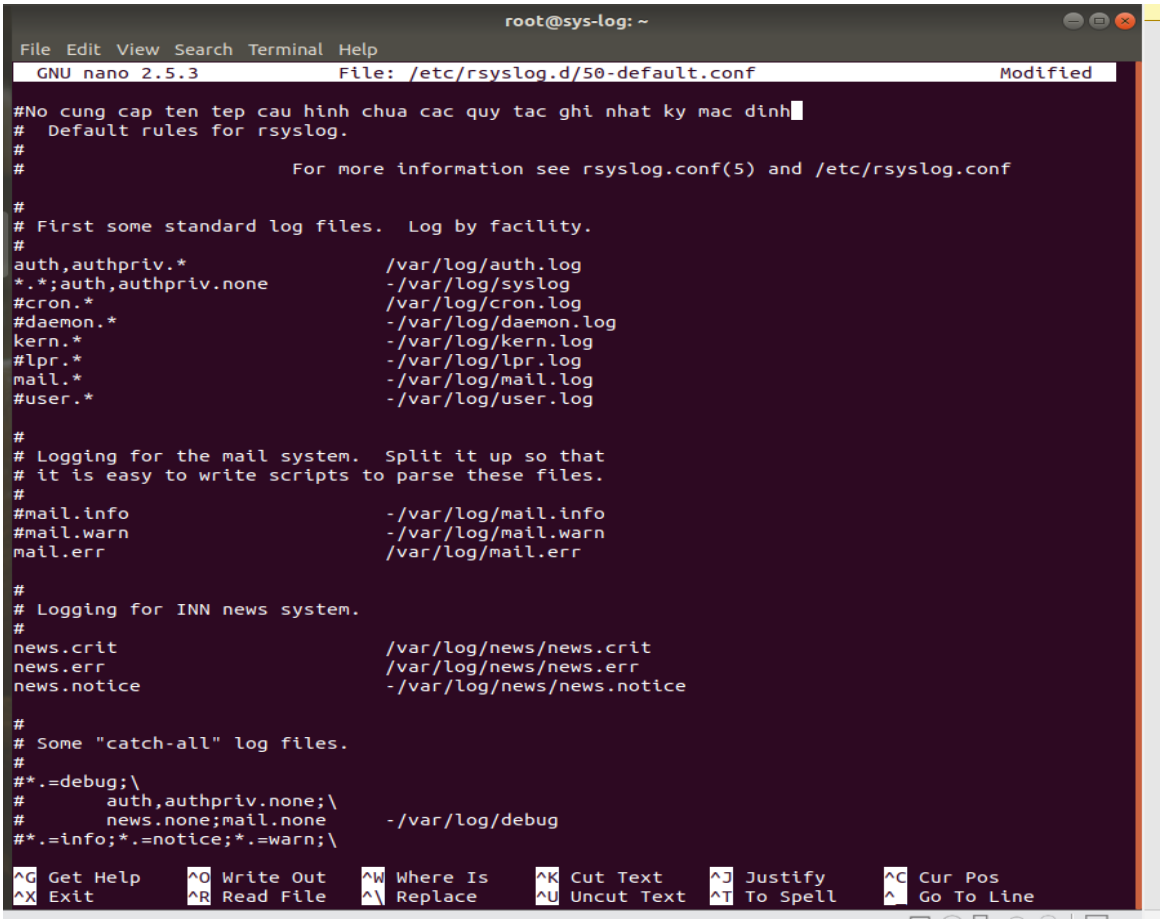
  *logger -p info "Hello World"*

  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.*

```
root@sys-log:/var/log# grep "Hello World" syslog
Nov 18 14:58:30 sys-log student: Hello World
```

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

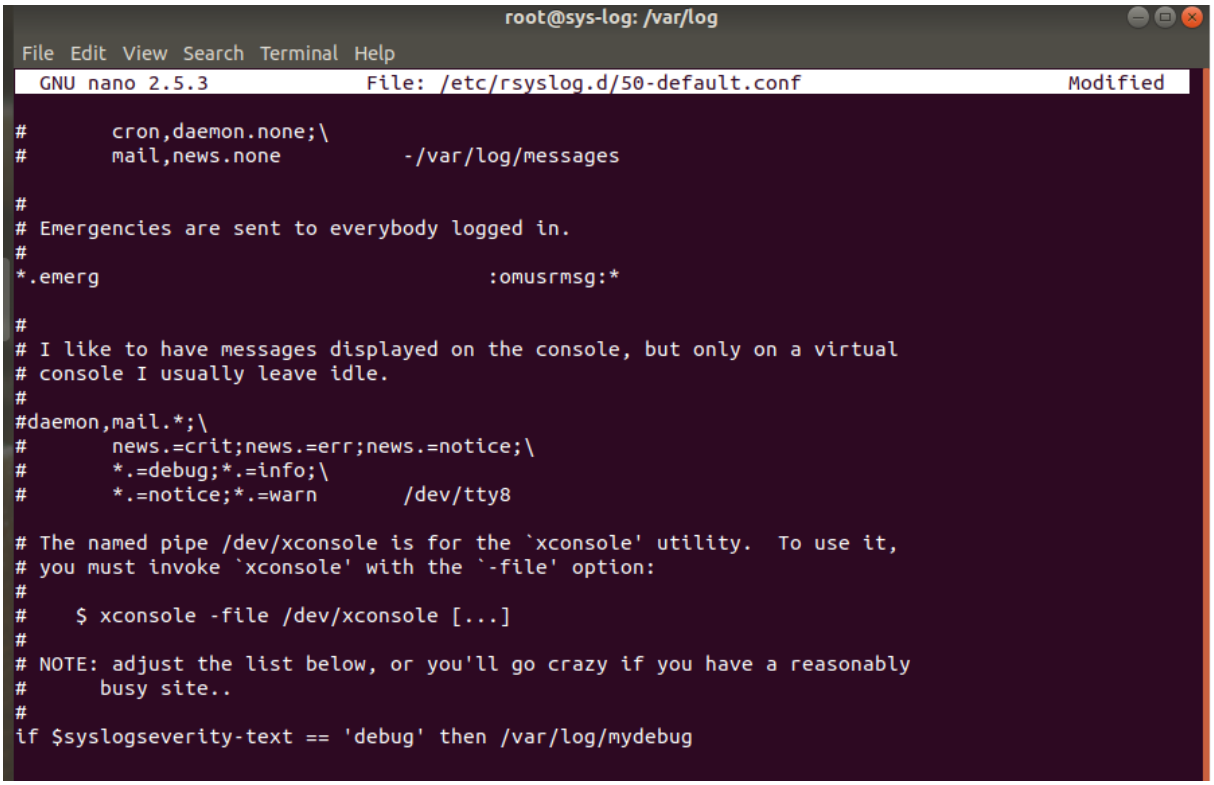
  Thêm một quy tắc syslog mới để đưa tất cả các thông báo với mức ưu tiên "debug" vào một tệp có tên là /var/log/mydebug. Tệp này chỉ nên chứa các thông báo debug.

- 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):

```
root@sys-log:/var/log# service rsyslog restart
root@sys-log:/var/log# tail -f /var/log/syslog
Nov 18 15:30:17 sys-log rsyslogd: [origin software="rsyslogd" swVersion="8.16.0" x-pid="726" x-in
fo="http://www.rsyslog.com"] exiting on signal 15.
Nov 18 15:30:17 sys-log rsyslogd: [origin software="rsyslogd" swVersion="8.16.0" x-pid="1016" x-i
nfo="http://www.rsyslog.com"] start
Nov 18 15:30:17 sys-log systemd[1]: Stopping System Logging Service...
Nov 18 15:30:17 sys-log systemd[1]: Stopped System Logging Service.
Nov 18 15:30:17 sys-log systemd[1]: Starting System Logging Service...
Nov 18 15:30:17 sys-log rsyslogd-2222: command 'KLogPermitNonKernelFacility' is currently not per
mitted - did you already set it via a RainerScript command (v6+ config)? [v8.16.0 try http://www.
rsyslog.com/e/2222 ]
Nov 18 15:30:17 sys-log rsyslogd: rsyslogd's groupid changed to 107
Nov 18 15:30:17 sys-log rsyslogd: rsyslogd's userid changed to 106
Nov 18 15:30:17 sys-log systemd[1]: Started System Logging Service.
Nov 18 15:30:48 sys-log systemd[1]: Time has been changed
Nov 18 15:31:18 sys-log rsyslogd: -- MARK --
```

- 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.

```
root@sys-log:/var/log# logger -p debug "Le Anh Tuan - B21DCAT205"
root@sys-log:/var/log# cat mydebug
Nov 18 15:33:52 sys-log student: Le Anh Tuan - B21DCAT205
```

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*

```
root@sys-log:/var/log# ll /usr/bin/logger
-rwxr-xr-x 1 root root 36200 Nov 30  2017 /usr/bin/logger*
root@sys-log:/var/log#
```

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).

```
root@sys-log:/var/log# chmod 754 /usr/bin/logger
root@sys-log:/var/log# ll /usr/bin/logger
-rwxr-xr-- 1 root root 36200 Nov 30  2017 /usr/bin/logger*
root@sys-log:/var/log#
```

**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