

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: AN TOÀN HỆ ĐIỀU HÀNH
MÃ HỌC PHẦN: INT1484**

**NHÓM LỚP: 01
TÊN BÀI:
KHÁM PHÁ NHẬT KÝ (LOG) UNIX TRÊN CENTOS**

Sinh viên thực hiện:
B22DCAT176 Nguyễn Thị Thùy Linh

Giảng viên: PGS.TS. Hoàng Xuân Dậu

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC	2
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	3
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	5
CHƯƠNG 3. KẾT QUẢ THỰC HÀNH	22
TÀI LIỆU THAM KHẢO	23

DANH MỤC HÌNH ẢNH

<i>Hình ảnh 1: Đăng nhập người dùng</i>	<i>5</i>
<i>Hình ảnh 2: Khám phá thư mục log.....</i>	<i>5</i>
<i>Hình ảnh 3: Xem quyền truy cập.....</i>	<i>6</i>
<i>Hình ảnh 4: Đọc log source</i>	<i>6</i>
<i>Hình ảnh 5: Đọc log secure</i>	<i>7</i>
<i>Hình ảnh 6: Đọc log secure</i>	<i>7</i>
<i>Hình ảnh 7: Đọc man last.....</i>	<i>8</i>
<i>Hình ảnh 8: Cấu hình thời gian</i>	<i>9</i>
<i>Hình ảnh 9: Bản ghi MARK</i>	<i>10</i>
<i>Hình ảnh 10: Man của logger.....</i>	<i>10</i>
<i>Hình ảnh 11: Cấu hình RULE.....</i>	<i>11</i>
<i>Hình ảnh 12: Kiểm tra log</i>	<i>12</i>
<i>Hình ảnh 13: Cấu hình debug.....</i>	<i>12</i>
<i>Hình ảnh 14: Kiểm tra log debug.....</i>	<i>13</i>
<i>Hình ảnh 15: Thay đổi quyền trên lệnh logger.....</i>	<i>13</i>
<i>Hình ảnh 16: Cấu hình RULE.....</i>	<i>14</i>
<i>Hình ảnh 17: Mở máy trạm.....</i>	<i>14</i>
<i>Hình ảnh 18: Địa chỉ IP máy trạm.....</i>	<i>15</i>
<i>Hình ảnh 19: Địa chỉ IP máy ghi log</i>	<i>15</i>
<i>Hình ảnh 20: Đọc log từ máy trạm</i>	<i>16</i>
<i>Hình ảnh 21: Cấu hình thông báo.....</i>	<i>16</i>
<i>Hình ảnh 22: Kiểm tra log thông báo</i>	<i>16</i>
<i>TÀI LIỆU THAM KHẢO.....</i>	<i>22</i>

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

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

1.2 Tìm hiểu lý thuyết

CentOS (Community ENTERprise Operating System) là một bản phân phối Linux miễn phí, được xây dựng từ mã nguồn của Red Hat Enterprise Linux (RHEL).

Syslog được hiểu là một giao thức client/server. Giao thức Syslog dùng để chuyển log và thông điệp đến máy nhận log. Hiện nay, máy nhận log thường được gọi là syslogd, syslog daemon hoặc syslog server và có thể gửi qua UDP hoặc TCP.

Các dữ liệu Syslog được gửi dạng cleartext. Syslog dùng port 514.

Định dạng tin nhắn Syslog sẽ bao gồm 3 phần đó là:

- **PRI** (giá trị ưu tiên được tính toán)
- **HEADER** (với thông tin nhận dạng)
- **MSG** (thông báo chính)

Vai trò của Syslog rất quan trọng. Giao thức này được sử dụng như một tiêu chuẩn, chuyển tiếp và thu thập log được sử dụng trên một phiên bản Linux.

Syslog cũng sẽ xác định mức độ nghiêm trọng (severity levels) cũng như mức độ cơ sở (facility levels) giúp người dùng hiểu rõ hơn về nhật ký được sinh ra

Trên CentOS, log thường được lưu trong thư mục:

/var/log /var/log/messages: Thông báo hệ thống, lỗi chung

/var/log/secure: Xác thực, ssh, sudo...

/var/log/maillog: Mail server trên máy tính.

Các file cấu hình lưu ở :

/etc/rsyslog.conf – cấu hình toàn cục

/etc/rsyslog.d/ – các file cấu hình mở rộng

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

- Khởi động lab:

labtainer centos-log2

Đăng nhập vào CentOS với tên người dùng Joe và mật khẩu "password4joe".

```
logger login: Joe
Password:
Login timed out after 60 seconds.
logger login: Joe
Password:
Last failed login: Mon Apr 21 15:07:07 UTC 2025 on pts/1
There was 1 failed login attempt since the last successful login.
[Joe@logger ~]$
```

Hình ảnh 1: Đăng nhập người dùng

Nhiệm vụ 1: Xem các tệp cấu hình

1. Trong terminal, nhập lệnh *sudo su* nhưng nhập sai mật khẩu cho người dùng root.
2. Nhập lại lệnh *sudo su*, nhưng lần này nhập đúng mật khẩu cho root. Nếu làm đúng, dấu nhắc sẽ kết thúc bằng ký tự '#'.

3. Khám phá thư mục log

- Thay đổi thư mục làm việc hiện tại thành */var/log*.
- Liệt kê nội dung của */var/log*

```
Password:
Last failed login: Mon Apr 21 15:07:07 UTC 2025 on pts/1
There was 1 failed login attempt since the last successful login.
[Joe@logger ~]$ sudo su
[root@logger Joe]# cd /var/log
[root@logger log]# ls -l
total 752
drwxr-xr-x 2 root root 4096 Mar  2  2018 anaconda
-rw-r--r-- 1 root utmp 1920 Apr 21 15:07 btmp
-rw-r--r-- 1 root root 193 Mar  2  2018 grubby_prune_debug
-rw-r--r-- 1 root root 292292 Apr 21 15:08 lastlog
-rw-r--r-- 1 root root 0 Mar  8  2018 maillog
-rw-r--r-- 1 root root 346458 Apr 21 15:10 messages
-rw-r--r-- 1 root root 77527 Apr 21 15:06 mydebug
drwxr-xr-x 2 root root 4096 Mar  2  2018 rhsm
-rw-r--r-- 1 root root 12719 Apr 21 15:08 secure
-rw-r--r-- 1 root root 0 Mar  8  2018 spooler
-rw-r--r-- 1 root root 0 Mar  2  2018 tallylog
-rw-rw-r-- 1 root utmp 1536 Apr 17 01:37 wtmp
-rw-r--r-- 1 root root 9660 Jan 24  2020 yum.log
[root@logger log]#
```

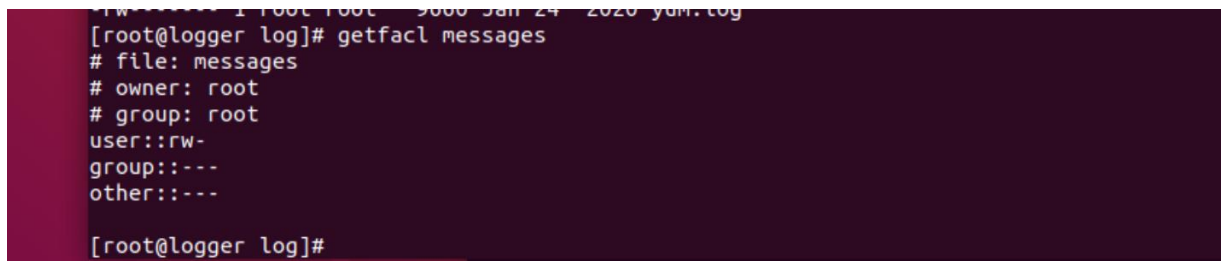
Hình ảnh 2: Khám phá thư mục log

Sinh viên sẽ thấy nhiều tệp và thư mục khác nhau. Lưu ý rằng tên màu xanh đề cập đến thư mục. Sinh viên có thể thấy một số "phần mở rộng" (extensions) khác nhau trên các tệp:

- + *.old*: Đây là bản sao "xoay vòng" (rotated) của nhật ký. Sinh viên sẽ thấy một tệp khác có cùng tiền tố, nhưng không có phần mở rộng ".old".

- + *-yyyymmdd*: Đây là một ví dụ khác về nhật ký "xoay vòng" (rotated) nhưng có một phần mở rộng hữu ích hơn: ngày mà nó đã được xoay vòng. Nếu sinh viên thấy phần mở rộng này, thì sinh viên cũng sẽ thấy một tệp khác có cùng tiền tố, nhưng không có phần mở rộng về ngày tháng.

- Xem quyền truy cập của messages log.



```
[root@logger log]# getfacl messages
# file: messages
# owner: root
# group: root
user::rw-
group::---
other::---
[root@logger log]#
```

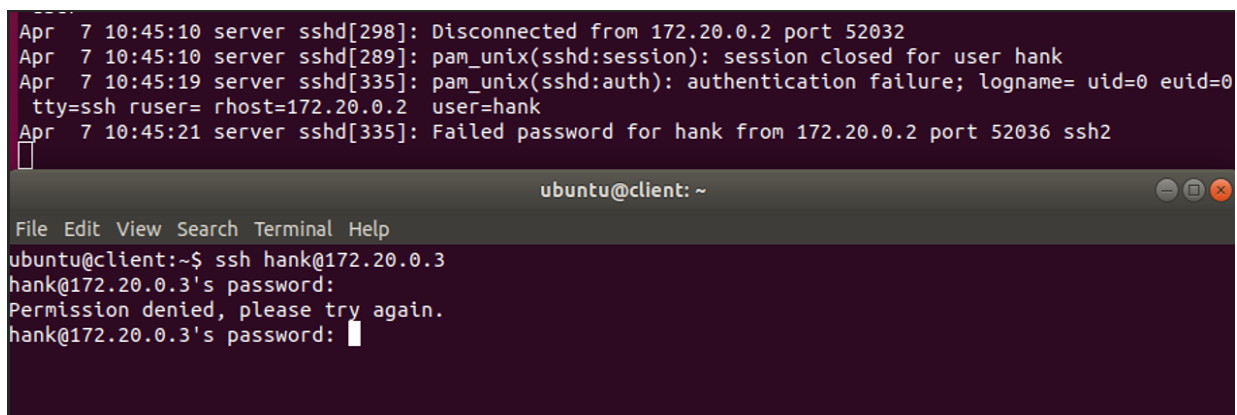
Hình ảnh 3: Xem quyền truy cập

- Ghi lại trong Mục số #1 của báo cáo quyền hạn mà người dùng thông thường có đối với tệp này.

- Đa số các tệp trong thư mục nhật ký là tệp văn bản, nhưng cũng có những ngoại lệ so với quy tắc thông thường của Unix. Nhiều tệp sẽ trống, hoặc là do tệp này vừa được xoay vòng, hoặc là do dịch vụ liên quan không hoạt động, hoặc chưa phát hiện được sự kiện có thể kiểm tra được liên quan đến dịch vụ đó.

4. Mật khẩu sai

- Các bản ghi liên quan đến đăng nhập được lưu trong tệp văn bản có tên là secure. Các bản ghi mới nhất được ghi vào cuối tệp



```
Apr  7 10:45:10 server sshd[298]: Disconnected from 172.20.0.2 port 52032
Apr  7 10:45:10 server sshd[289]: pam_unix(sshd:session): session closed for user hank
Apr  7 10:45:19 server sshd[335]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
  tty=ssh ruser= rhost=172.20.0.2 user=hank
Apr  7 10:45:21 server sshd[335]: Failed password for hank from 172.20.0.2 port 52036 ssh2
[
ubuntu@client: ~
File Edit View Search Terminal Help
ubuntu@client:~$ ssh hank@172.20.0.3
hank@172.20.0.3's password:
Permission denied, please try again.
hank@172.20.0.3's password: [
```

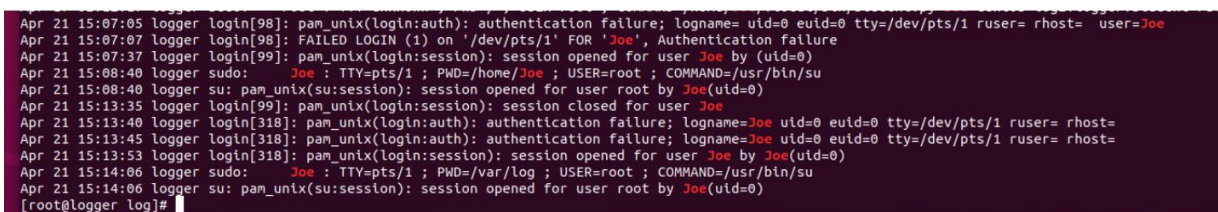
Hình ảnh 4: Đọc log source

- Mở tệp và tìm kiếm trạng thái failed khi cố gắng đăng nhập bằng tên người dùng Joe (không phải sự thất bại khi 'su' thành root).
- Trong Mục số #2 của báo cáo, ghi lại cụm từ được sử dụng để chỉ ra sự thất bại trong việc đăng nhập.
- Lưu ý rằng Mục số #3 cần trả lời các câu hỏi bổ sung. Trên máy chủ, chạy:

```
sudo less /etc/denyhosts.conf
```

5. Mật khẩu là tên người dùng

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



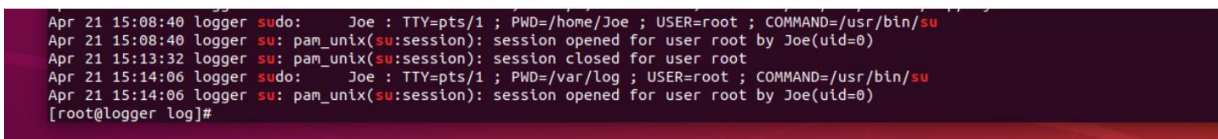
```
Apr 21 15:07:05 logger login[98]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0 tty=/dev/pts/1 ruser= rhost= user=Joe
Apr 21 15:07:07 logger login[98]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'Joe', Authentication failure
Apr 21 15:07:37 logger login[99]: pam_unix(login:session): session opened for user Joe by (uid=0)
Apr 21 15:08:40 logger sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/su
Apr 21 15:08:40 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Apr 21 15:13:35 logger login[99]: pam_unix(login:session): session closed for user Joe
Apr 21 15:13:40 logger login[318]: pam_unix(login:auth): authentication failure; logname=Joe uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 21 15:13:45 logger login[318]: pam_unix(login:auth): authentication failure; logname=Joe uid=0 euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 21 15:13:53 logger login[318]: pam_unix(login:session): session opened for user Joe by Joe(uid=0)
Apr 21 15:14:06 logger sudo: Joe : TTY=pts/1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/su
Apr 21 15:14:06 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
[root@logger log]#
```

Hình ảnh 5: Đọc log secure

- Trong Mục số #4 của báo cáo, ghi lại cụm từ được sử dụng khi bạn nhập một tên người dùng không hợp lệ.

6. Sử dụng su

- Với tệp nhật ký secure vẫn mở, tìm mục ở cuối tệp liên quan đến hành động su thành root trước đó. Xem thông tin được lưu trữ về sử dụng su.



```
Apr 21 15:08:40 logger sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/bin/su
Apr 21 15:08:40 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Apr 21 15:13:32 logger su: pam_unix(su:session): session closed for user root
Apr 21 15:14:06 logger sudo: Joe : TTY=pts/1 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/su
Apr 21 15:14:06 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
[root@logger log]#
```

Hình ảnh 6: Đọc log secure

- Trong Mục số #5 của báo cáo, ghi lại thông tin đã được ghi lại về sử dụng su
- Thoát khỏi trình soạn thảo khi sinh viên đã hoàn thành.

7. Tệp wtmp

- Một trong số các tệp nhị phân trong thư mục nhật ký là tệp wtmp phổ biến, yêu cầu sử dụng các công cụ khác để trích xuất thông tin từ nó, chẳng hạn như lệnh last.
- Mở trang hỗ trợ “man” cho lệnh last bằng cách thực hiện các bước sau:

```
man last
```


- Đọc phần DESCRIPTION để tìm hiểu chức năng của lệnh.
- Điều hướng đến phần OPTIONS.

```

root@logger:/var/log
File Edit View Search Terminal Help

DESCRIPTION
last searches back through the file /var/log/wtmp (or the file designated by the -f flag) and displays a list of all users logged in (and out) since that file was created. Names of users and tty's can be given, in which case last will show only those entries matching the arguments. Names of ttys can be abbreviated, thus last 0 is the same as last tty0.

When last catches a SIGINT signal (generated by the interrupt key, usually control-C) or a SIGQUIT signal (generated by the quit key, usually control-), last will show how far it has searched through the file; in the case of the SIGINT signal last will then terminate.

The pseudo user reboot logs in each time the system is rebooted. Thus last reboot will show a log of all reboots since the log file was created.

Lastb is the same as last, except that by default it shows a log of the file /var/log/btmp, which contains all the bad login attempts.

OPTIONS
-f file
    Tells last to use a specific file instead of /var/log/wtmp.

-num
    This is a count telling last how many lines to show.

-n num
    The same.

-t YYYYMMDDHHMMSS
    Display the state of logins as of the specified time. This is useful, e.g., to determine easily who was logged in at a particular time -- specify that time with -t and look for "still logged in".

-f file
    Specifies a file to search other than /var/log/wtmp.

-R
    Suppresses the display of the hostname field.

-a
    Display the hostname in the last column. Useful in combination with the next flag.

-d
    For non-local logins, Linux stores not only the host name of the remote host but its IP number as well. This option translates the IP number back into a hostname.

-F
    Print full login and logout times and dates.

-i
    This option is like -d in that it displays the IP number of the remote host, but it displays the IP number in numbers-and-dots notation.

Manual page last(1) line 11 (press h for help or q to quit)

```

Hình ảnh 7: Đọc man last

- Trong Mục số #6 của báo cáo tự mô tả và giải thích lựa chọn -t của lệnh last.

Nhiệm vụ 2: Cấu hình lại rsyslog cho MARK

Trong phần này, sinh viên sẽ bật tính năng MARK và khởi động lại syslog để chấp nhận thay đổi.

1. Mở tệp cấu hình rsyslog.

Trong khi vẫn chạy với đặc quyền root trong terminal, khởi chạy một trình soạn thảo từ dòng lệnh (như leafpad) để mở tệp /etc/rsyslog.conf

Lưu ý: khi tiến trình rsyslog đọc tệp này trong quá trình khởi tạo, bất cứ điều gì sau ký tự '#' (từ đó đến cuối dòng) được xem như một chú thích.

2. Bật tính năng Mark.

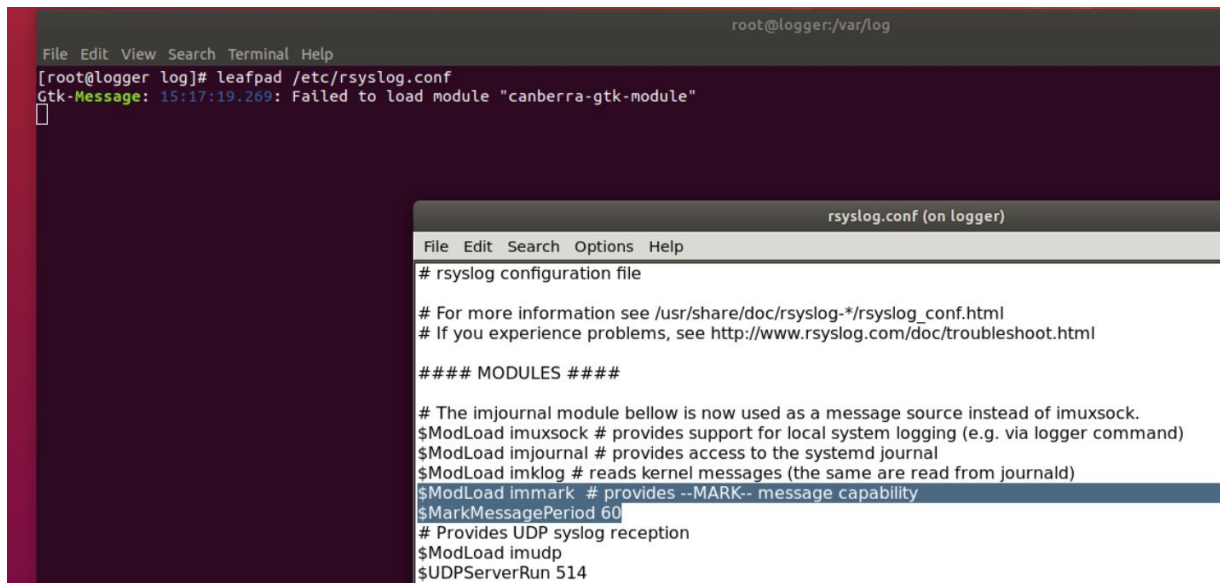
Mặc định, việc chèn thời gian vào một tần suất đã chỉ định được vô hiệu hóa.

- Trong phần "#### MODULES ####", tìm dòng có \$ModLoad immark, và xóa '#' để kích hoạt tính năng này.
- Thiết lập tần suất của timestamps với việc thêm dòng tiếp theo dòng bên trên vừa mới thêm vào:

\$MarkMessagePeriod 60

“60” là số giây giữa các timestamps (giá trị mặc định thường là 20 phút)

- Lưu thay đổi và thoát khỏi trình soạn thảo.



Hình ảnh 8: Cấu hình thời gian

3. Khởi động lại tiến trình rsyslog.

Khởi động lại tiến trình rsyslog sẽ khiến nó khởi tạo lại và đọc lại tệp cấu hình (đồng nghĩa với việc thay đổi được áp dụng). Thực hiện các bước sau để khởi động lại:

```
service rsyslog restart
```

4. Xem thay đổi này đã được thực hiện trong các nhật ký bằng cách sử dụng lệnh tail như sau:

```
tail -f /var/log/messages
```

Lệnh tail hiển thị một số dòng cuối cùng của tệp (khác với lệnh head, hiển thị một số dòng đầu tiên của tệp). Tùy chọn "-f" cho biết để chờ đợi “mãi mãi” và hiển thị thêm dòng khi chúng được thêm vào cuối tệp.

Sinh viên sẽ thấy một dòng ghi lại việc dừng rsyslogd, và sau đó là một dòng ghi lại rằng rsyslogd đã được khởi động.

Tiếp tục chờ đợi cho đến khi thấy một bản ghi MARK xuất hiện trong nhật ký. Sau khi sinh viên đã thấy nó (hoặc sau hơn một phút), nhấn Ctrl-C để thoát khỏi tail

```
root@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# leafpad /etc/rsyslog.conf
Gtk-Message: 15:17:19.269: Failed to load module "canberra-gtk-module"
[root@logger log]# service rsyslog restart
Redirecting to /bin/systemctl restart rsyslog.service
[root@logger log]# tail -f /var/log/messages
Apr 21 15:16:00 logger kernel: audit: type=1400 audit(1745248560.532:35): apparmor="DENIED" operation="open" info="Failed name lookup - disconnected path
3 profile="/usr/bin/man" name="/var/lib/docker/overlay2/3366aa2f63f47b49b56b8bb9fb2d1e8efa4a58658a5aa94f5ac654aee418b1fc/diff/usr/share/man" pld=4437 con
uested mask="r" denied mask="r" fsuid=0 ouid=0
Apr 21 15:16:00 logger kernel: audit: type=1400 audit(1745248560.532:36): apparmor="DENIED" operation="open" info="Failed name lookup - disconnected path
3 profile="/usr/bin/man" name="/var/lib/docker/overlay2/3366aa2f63f47b49b56b8bb9fb2d1e8efa4a58658a5aa94f5ac654aee418b1fc/diff/usr/share/man" pld=4437 con
uested mask="r" denied mask="r" fsuid=0 ouid=0
Apr 21 15:16:24 logger rsyslogd: -- MARK --
Apr 21 15:17:24 logger rsyslogd: -- MARK --
Apr 21 15:18:24 logger rsyslogd: -- MARK --
Apr 21 15:19:03 logger systemd: Stopping System Logging Service...
Apr 21 15:19:03 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="42" x-info="http://www.rsyslog.com"] exiting on signal 15.
Apr 21 15:19:03 logger systemd: Starting System Logging Service...
Apr 21 15:19:03 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="622" x-info="http://www.rsyslog.com"] start
Apr 21 15:19:03 logger systemd: Started System Logging Service.
Apr 21 15:20:03 logger rsyslogd: -- MARK --
```

Hình ảnh 9: Bản ghi MARK

Nhiệm vụ 3: Cấu hình lại và Kiểm tra rsyslog

Trong phần này, sinh viên sẽ làm quen với tiện ích logger để tạo thủ công các mục syslog. Một quản trị viên hệ thống có thể sử dụng lệnh này để ghi lại các thay đổi mà họ thực hiện trên hệ thống, và nó có thể được sử dụng để kiểm tra các thay đổi trong cấu hình syslog. Sinh viên sẽ thực hiện một số thay đổi trong các quy tắc syslog, sau đó sử dụng logger để kiểm tra các thay đổi đó.

1. Đọc phần DESCRIPTION trong trang man của tiện ích logger:

man logger

```
root@logger:/var/log
File Edit View Search Terminal Help
LOGGER(1) User Commands
NAME
    logger - a shell command interface to the syslog(3) system log module
SYNOPSIS
    logger [options] [message]
DESCRIPTION
    logger makes entries in the system log. It provides a shell command interface to the syslog(3) system log module.
OPTIONS
    -n, --server server
        Write to the specified remote syslog server instead of to the builtin syslog routines. Unless --udp or --tcp is specified the logger will first try to use UDP, but if it fails a TCP connection is attempted.
    -d, --udp
        Use datagram (UDP) only. By default the connection is tried to syslog port defined in /etc/services, which is often 514.
    -T, --tcp
        Use stream (TCP) only. By default the connection is tried to syslog-conn port defined in /etc/services, which is often 601.
    -P, --port port
        Use the specified port. When this option is not specified, the port defaults to syslog for udp and to syslog-conn for tcp connections.
    -i, --id
        Log the process ID of the logger process with each line.
    -f, --file file
        Log the contents of the specified file. This option cannot be combined with a command-line message.
    -h, --help
        Display a help text and exit.
    -p, --priority priority
        Enter the message into the log with the specified priority. The priority may be specified numerically or as a facility.level pair. For example, -p local3.info logs the message as informational in the local3 facility. The default is user.notice.
    -S, --size size
Manual page logger(1) line 1 (press h for help or q to quit)
```

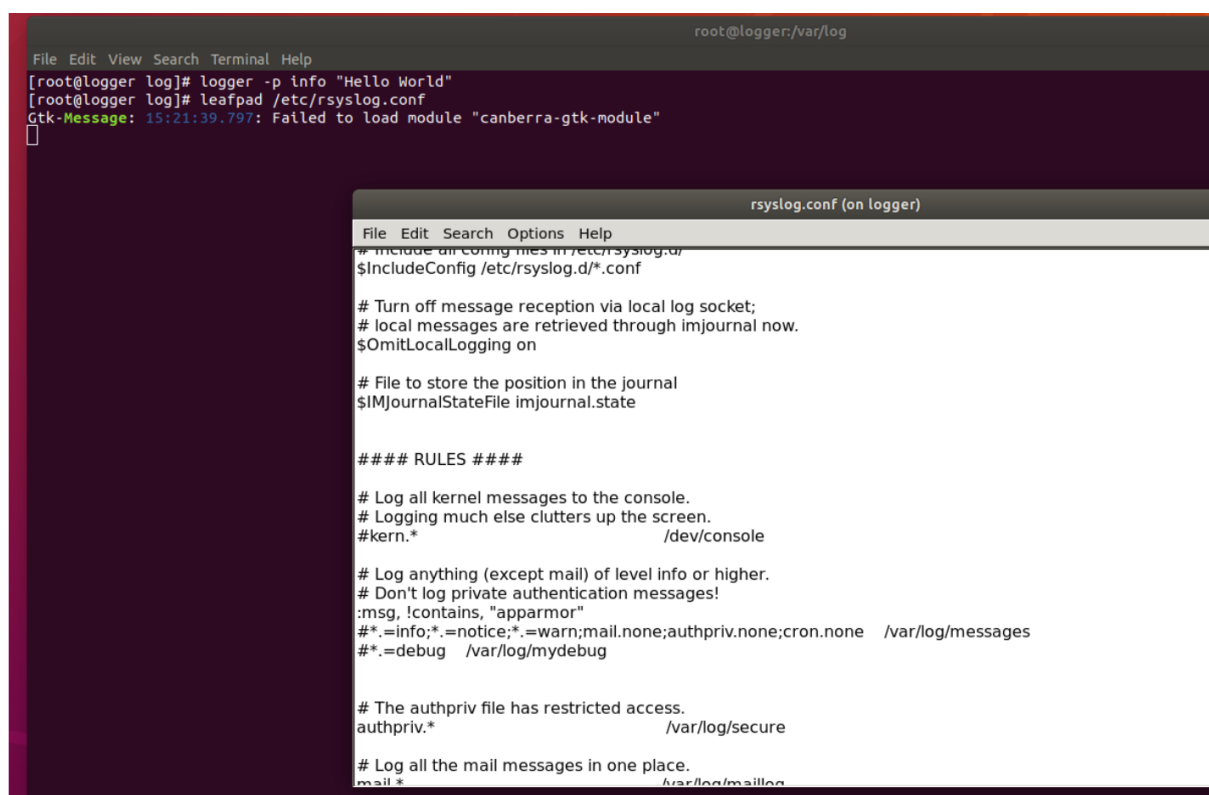
Hình ảnh 10: Man của logger

2. Tạo một mục trong /var/log/messages với mức ưu tiên "info" bằng 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.

3. Mở lại tệp cấu hình rsyslog tại /etc/rsyslog.conf và cuộn xuống phần “##### RULES #####”.



```
File Edit View Search Terminal Help
[root@logger log]# logger -p info "Hello World"
[root@logger log]# leafpad /etc/rsyslog.conf
Gtk-Message: 15:21:39.797: Failed to load module "canberra-gtk-module"

rsyslog.conf (on logger)
File Edit Search Options Help
# include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

# Turn off message reception via local log socket;
# local messages are retrieved through imjournal now.
$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state

##### RULES #####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
:msg, !contains, "apparmor"
#*.=info;*.=notice;*.=warn;mail.none;authpriv.none;cron.none /var/log/messages
#*.=debug /var/log/mydebug

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* /var/log/maillog
```

Hình ảnh 11: Cấu hình RULE

Trong Mục số #7 của báo cáo sinh viên hãy viết quy tắc syslog chỉ định điều gì sẽ xảy ra với mục mà sinh viên đã gửi đến syslog trong bước #2 ở trên.

4. Thoát khỏi trình soạn thảo.

5. Sử dụng grep (hoặc chọn công cụ khác) để xác minh rằng mục nhật ký đã được lưu trong tệp mà sinh viên nghĩ rằng nó sẽ được lưu (theo quy tắc sinh viên ghi lại trong mục số #7 của báo cáo). [Nếu không có trong đó, thì sinh viên đã làm sai. Trong trường hợp đó, hãy xem xét lại quy tắc sinh viên chọn cho đến khi sinh viên đạt được đúng.]

```
root@logger:
File Edit View Search Terminal Help
[root@logger log]# logger -p info "Hello World"
[root@logger log]# leafpad /etc/rsyslog.conf
Gtk-Message: 15:21:39.797: Failed to load module "canberra-gtk-module"
[root@logger log]# grep "Hello World" /var/log/messages
Apr 17 01:57:03 logger Joe: Hello World
Apr 17 01:57:43 logger Joe: Hello World
Apr 21 15:20:53 logger Joe: Hello World
[root@logger log]#
```

Hình ảnh 12: Kiểm tra log

6. Mở lại tệp cấu hình syslog và cuộn xuống phần RULES.

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.

```
#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
:msg, !contains, "apparmor"
*.=info;*.=notice;*.=warn;mail.none;authpriv.none;cron.none /var/log/messages
*.=debug /var/log/mydebug
```

Hình ảnh 13: Cấu hình debug

Trong Mục số #8 của báo cáo, sinh viên hãy viết quy tắc đã sử dụng để đáp ứng yêu cầu trên.

7. Lưu các thay đổi của bạn vào tệp cấu hình và sau đó thoát khỏi trình soạn thảo.

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

systemctl restart rsyslog

Nếu thay đổi trong rsyslog.conf có lỗi cú pháp, nó sẽ được báo cáo ở cuối tệp /var/log/messages.

9. Bây giờ sinh viên đã biết cách sử dụng logger, hãy sử dụng nó để kiểm tra quy tắc mà sinh viên đã thêm vào rsyslog.conf ở bước #6 ở trên.

```
[root@logger log]# cat /etc/rsyslog.conf
Gtk-Message: 15:22:40.678: Failed to load module
[root@logger log]# systemctl restart rsyslog
[root@logger log]# logger -p debug "Debug Test"
[root@logger log]# cat /var/log/mydebug
Apr 17 01:59:06 logger systemd: Stopping System
Apr 21 15:23:23 logger systemd: Starting System Logging Service...
Apr 21 15:23:25 logger rsyslogd: [origin software="rsyslogd" swVer:
Apr 21 15:23:25 logger systemd: Started System Logging Service.
Apr 21 15:23:32 logger Joe: Debug Test
Apr 21 15:23:32 logger Joe: Debug Test
[root@logger log]#
```

Hình ảnh 14: Kiểm tra log debug

Trong Mục số #9 của báo cáo, mô tả cách sinh viên đã sử dụng logger (và các lệnh khác) để kiểm tra quy tắc sinh viên đã thêm trong bước #6.

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

ll/bin/logger

Không nên cho phép người dùng thông thường thực thi lệnh logger. Thay đổi quyền sao cho chỉ người dùng root và nhóm root mới có thể thực thi nó.

Trong Mục số #10 của báo cáo, viết lệnh (hoặc các lệnh) sinh viên đã sử dụng để thay đổi quyền trên lệnh logger.

```
[root@logger log]#
[root@logger log]# ls -l /bin/logger
-rwxr-x--- 1 root root 29224 Dec  1 2017 /bin/logger
[root@logger log]# chmod 750 /bin/logger
[root@logger log]# chown root:root /bin/logger
[root@logger log]#
```

Hình ảnh 15: Thay đổi quyền trên lệnh logger

Nhiệm vụ 4: Ghi log tập trung

Giả sử sinh viên có một số hệ thống Linux cần quản lý. Thay vì cấu hình và xem xét việc ghi log trên từng hệ thống, sinh viên có thể xác định một hệ thống ghi log tập trung và sau đó chuyển tiếp các thông báo log từ mỗi hệ thống đến hệ thống ghi log tập trung đó. Ở phần này, sinh viên sẽ cấu hình hệ thống "logger" hiện có để chấp nhận các thông báo log từ các máy tính từ xa, và sinh viên sẽ cấu hình một máy tính trạm để chuyển tiếp các log của nó đến hệ thống ghi log.

Mở lại tệp cấu hình */etc/rsyslog.conf* trên máy tính ghi log.

Tìm các mục sau trong tệp cấu hình và bỏ chú thích chúng (xóa dấu "#") để cho phép chấp nhận thông báo syslog trên cổng 514 qua TCP hoặc UDP:

```
$ModLoad imudp
```

```
$UDPServerRun 514
```

```
$ModLoad imtcp
```

```
$InputTCPServerRun 514
```

Khởi động lại rsyslog

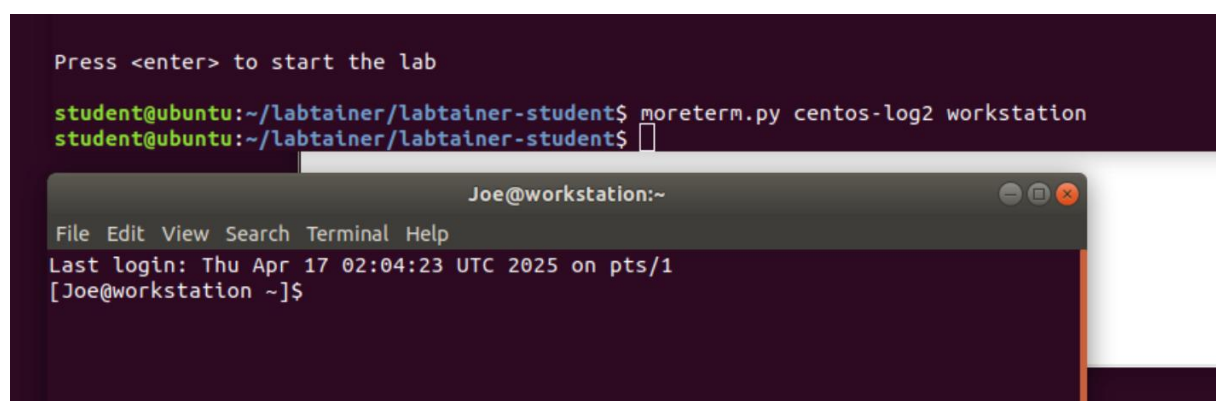
```
systemctl restart rsyslog
```



Hình ảnh 16: Cấu hình RULE

Trên terminal chính của hệ thống lab sử dụng lệnh:

```
moreterm.py centos-log2 workstation
```



Hình ảnh 17: Mở máy trạm

Một terminal ảo mới được mở và kết nối với máy tính trạm. Máy tính này chia sẻ mạng với máy tính ghi log của sinh viên. Sử dụng "ifconfig" trên mỗi máy tính để xem địa chỉ IP của mỗi máy tính.

```
[root@workstation Joe]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.25.0.3 netmask 255.255.255.0 broadcast 172.25.0.255
    ether 02:42:ac:19:00:03 txqueuelen 0 (Ethernet)
    RX packets 78 bytes 8961 (8.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1727 bytes 234994 (229.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@workstation Joe]#
```

Hình ảnh 18: Địa chỉ IP máy trạm

```
root@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.25.0.2 netmask 255.255.255.0 broadcast 172.25.0.255
    ether 02:42:ac:19:00:02 txqueuelen 0 (Ethernet)
    RX packets 1800 bytes 243793 (238.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6 bytes 252 (252.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@logger log]#
```

Hình ảnh 19: Địa chỉ IP máy ghi log

Trên máy tính ghi log, sử dụng "tail" để xem các nhật ký:

*tail -f /var/log/**

Sử dụng "sudo su" để nâng cao đặc quyền trên máy tính trạm.


```
==> /var/log/messages <==
Apr 21 15:27:23 workstation su: (to root) root on pts/1

==> /var/log/mydebug <==
Apr 21 15:27:23 workstation sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr
/bin/su
Apr 21 15:27:23 workstation su: (to root) root on pts/1
Apr 21 15:27:23 workstation su: pam_unix(su:session): session opened for user root by (uid=0)

==> /var/log/secure <==
Apr 21 15:27:23 workstation sudo: Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr
/bin/su
Apr 21 15:27:23 workstation su: pam_unix(su:session): session opened for user root by (uid=0)

==> /var/log/messages <==
Apr 21 15:27:25 logger rsyslogd: -- MARK --

==> /var/log/mydebug <==
Apr 21 15:27:25 logger rsyslogd: -- MARK --
```

Hình ảnh 20: Đọc log từ máy trạm

Mở tệp `/etc/rsyslog.conf` trên máy tính trạm và tìm phần "RULES". Ở cuối phần đó, thêm dòng sau để chuyển hướng tất cả các thông báo đến máy tính ghi log:

`*.* @172.25.0.2`

```
*rsyslog.conf (on workstation)
File Edit Search Options Help

# Log all the mail messages in one place.
mail.*                                -/var/log/maillog

# Log cron stuff
cron.*                                /var/log/cron

# Everybody gets emergency messages
*.emerg                               :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit                        /var/log/spooler

# Save boot messages also to boot.log
local7.*                              /var/log/boot.log

*.* @172.25.0.2

### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
```

Hình ảnh 21: Cấu hình thông báo

Bây giờ hãy khởi động lại rsyslog trên máy tính trạm và quan sát các thông báo log trên máy tính ghi log.

Thử nghiệm với các sự kiện liên quan đến bảo mật khác nhau như giảm đặc quyền và nâng cao đặc quyền trên máy tính trạm và thực hiện các lệnh logger từ máy tính trạm.

```
Jan 24 18:43:29 installed: tearpad-0.0.10-1.1.el6.x86_64

==> /var/log/messages <==
Apr 21 15:30:00 workstation logger: Log from workstation

==> /var/log/mydebug <==
Apr 21 15:30:00 workstation logger: Log from workstation

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@workstation Joe]# logger -p info "Log from workstation"
[root@workstation Joe]#
```

Hình ảnh 22: Kiểm tra log thông báo

Nhiệm vụ 5: Các câu hỏi khác

Mở lại `/etc/rsyslog.conf`.

Tham khảo `/etc/rsyslog.conf`, trả lời các câu hỏi trong các mục #11 đến #13 của báo cáo.

2. Mô tả hành động và kết quả trong Mục số #14 của báo cáo.

3. Trong Mục #15 của báo cáo hãy mô tả những điều sinh viên đã học từ bài thực hành này.

14. Trong Mục #16 của báo cáo hãy mô tả bất kỳ đề xuất nào có để cải thiện bài thực hành này.

Câu hỏi :

1. Đối với tệp log có tên `/var/log/messages`, quyền nào được cấp cho người dùng thông thường?

```
root@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# ls -l /var/log/messages
-rw----- 1 root root 370018 Apr 21 15:33 /var/log/messages
[root@logger log]#
```

Người dùng thông thường không được cấp bất cứ quyền nào

2. Trong `/var/log/secure`, từ ngữ nào được sử dụng để chỉ một nỗ lực đăng nhập không thành công?

```
[root@logger log]# cat secure | grep "fail"
Apr 17 01:43:03 logger login[264]: pam_unix(login:auth): authentication failure; logname= uid=0
euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 17 01:43:05 logger login[264]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
Apr 17 01:43:15 logger login[264]: FAILED LOGIN (2) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
Apr 17 01:43:39 logger login[265]: pam_unix(login:auth): authentication failure; logname= uid=0
euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 17 01:43:41 logger login[265]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
Apr 17 01:52:42 logger login[564]: pam_unix(login:auth): authentication failure; logname=Joe uid=0
euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 17 01:52:44 logger login[564]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
Apr 21 15:07:05 logger login[98]: pam_unix(login:auth): authentication failure; logname= uid=0 euid=0
tty=/dev/pts/1 ruser= rhost= user=Joe
Apr 21 15:07:07 logger login[98]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'Joe', Authentication failure
Apr 21 15:13:40 logger login[318]: pam_unix(login:auth): authentication failure; logname=Joe uid=0
euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 21 15:13:42 logger login[318]: FAILED LOGIN (1) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
Apr 21 15:13:45 logger login[318]: pam_unix(login:auth): authentication failure; logname=Joe uid=0
euid=0 tty=/dev/pts/1 ruser= rhost=
Apr 21 15:13:47 logger login[318]: FAILED LOGIN (2) on '/dev/pts/1' FOR 'UNKNOWN', Authentication failure
[root@logger log]#
```

Từ “failure”

3. Liên quan đến Mục #2 ở trên, hãy mô tả một tình huống thực tế mà thông tin này có thể hữu ích.

Quản trị viên phát hiện nhiều lần đăng nhập thất bại từ cùng một địa chỉ IP trong log. Đây có thể là dấu hiệu của brute-force attack (tấn công dò mật khẩu).

4. Trong `/var/log/secure`, từ ngữ nào được sử dụng để chỉ rằng sinh viên đã tăng đặc quyền bằng lệnh `su`?

```
root@logger:/var/log
File Edit View Search Terminal Help
[root@logger log]# cat secure | grep "session"
Apr 17 01:37:23 logger su: pam_unix(su:session): session opened for user Joe by (uid=0)
Apr 17 01:37:23 logger su: pam_unix(su:session): session closed for user Joe
Apr 17 01:43:50 logger login[265]: pam_unix(login:session): session opened for user Joe by (uid=0)
Apr 17 01:44:05 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Apr 17 01:52:36 logger su: pam_unix(su:session): session closed for user root
Apr 17 01:52:38 logger login[265]: pam_unix(login:session): session closed for user Joe
Apr 17 01:52:52 logger login[564]: pam_unix(login:session): session opened for user Joe by Joe(uid=0)
Apr 17 01:52:59 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Apr 17 02:03:09 logger su: pam_unix(su:session): session opened for user Joe by Joe(uid=0)
Apr 17 02:03:13 logger su: pam_unix(su:session): session closed for user Joe
Apr 21 15:07:37 logger login[99]: pam_unix(login:session): session opened for user Joe by (uid=0)
Apr 21 15:08:40 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Apr 21 15:13:32 logger su: pam_unix(su:session): session closed for user root
Apr 21 15:13:35 logger login[99]: pam_unix(login:session): session closed for user Joe
Apr 21 15:13:53 logger login[318]: pam_unix(login:session): session opened for user Joe by Joe(uid=0)
Apr 21 15:14:06 logger su: pam_unix(su:session): session opened for user root by Joe(uid=0)
Apr 21 15:26:19 workstation su: pam_unix(su-l:session): session opened for user Joe by (uid=0)
Apr 21 15:27:23 workstation su: pam_unix(su:session): session opened for user root by (uid=0)
[root@logger log]#
```

Từ “`su:session`”

5. Hãy mô tả chức năng được cung cấp bởi tùy chọn `-t` của lệnh `last`.

```
[root@logger log]# last -t 20250421111111
root      pts/1                Thu Apr 17 01:37 - 01:37  (00:00)
root      pts/1                Thu Apr 17 01:37 - 01:37  (00:00)

wtmp begins Thu Apr 17 01:37:20 2025
[root@logger log]#
```

Tùy chọn `-t` dùng để chỉ định thời điểm kết thúc truy vết đăng nhập theo định dạng `YYYYMMDDHHMMSS` và một số tùy chọn khác

6. Quy tắc nào trong tệp cấu hình `syslog` sẽ phù hợp với bản ghi mà sinh viên đã gửi bằng lệnh `logger` (tức là một facility là “`user`” và một priority là “`info`”)?

Quy tắc : “*user.info /var/log/messages*”

7. Quy tắc nào sinh viên đã thêm để đưa các thông báo gỡ lỗi (và chỉ các thông báo gỡ lỗi) vào */var/log/mydebug*?

Quy tắc đã thêm “**.=debug /var/log/mydebug*”

8. Sinh viên đã kiểm tra quy tắc gỡ lỗi mới như thế nào?

Dùng lệnh logger để gửi bản ghi với mức debug: “*logger -p user.debug "This is a debug test"*”

Sau đó kiểm tra file : *cat /var/log/mydebug*

9. Sinh viên đã sử dụng lệnh nào để thay đổi quyền trên logger để chỉ người dùng root và nhóm root mới có thể thực thi nó?

chmod 750 /bin/logger chown root:root /bin/logger

10. Nhìn vào tất cả các quy tắc hoạt động trong *rsyslog.conf*, hành động nào sẽ *rsyslog* thực hiện nếu nhận được một bản ghi từ kernel với mức ưu tiên là *emerg*? Mặc định có dòng sau:

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                     /dev/console
```

```
# Everybody gets emergency messages
*.emerg                                     :omusrmsg:*
```

Ghi vào */var/log/kern.log*

Gửi tới tất cả user đang đăng nhập (do dấu sao *)

11. Nhìn vào tất cả các quy tắc hoạt động trong *rsyslog.conf*, hành động nào sẽ *rsyslog* thực hiện nếu nhận được một bản ghi từ facility mail với mức ưu tiên là *notice*?

```
# Log all the mail messages in one place.
mail.*                                     -/var/log/maillog
```

mail. /var/log/mail.log*

→ Vì *notice* ≥ *info* → phù hợp → log sẽ vào */var/log/mail.log*

12. Nhìn vào tất cả các quy tắc hoạt động trong rsyslog.conf, hành động nào sẽ rsyslog thực hiện nếu nhận được một bản ghi từ facility local6 với mức ưu tiên là err?

```
# Save boot messages also to boot.log
local6.* /var/log/boot.log
```

```
# Ghi log info trở lên (loại debug)
```

```
local6.* /var/log/local6.log
```

→ log err sẽ được ghi vào /var/log/local6.log Nếu không có dòng xử lý local6 → log bị bỏ qua

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

- Thử gửi log với nhiều mức khác nhau: info, warn, err
- Quan sát log chuyển đến đâu

14. Sinh viên đã học được điều gì từ bài thực hành này?

- Hiểu được cách hoạt động của hệ thống ghi log trong Linux
- Biết cấu trúc và nội dung file /var/log
- Biết cách tùy chỉnh syslog bằng rsyslog.conf
- Biết cách phân tích log để giám sát hệ thống
- Biết dùng logger để thử nghiệm

15. Cần làm gì để cải thiện bài thực hành này?

- Thêm phần hướng dẫn về logrotate
- Thêm ví dụ cụ thể về tấn công thực tế và log của nó
- Hướng dẫn trực quan với hình ảnh
- Cho phép sinh viên viết rule riêng và so sánh kết quả
- Thêm phần tổng hợp cuối lab để ôn lại keypoint

CHƯƠNG 3: KẾT QUẢ THỰC HÀNH

Màn hình checkwork bài thực hành:

```
student@ubuntu:~/labtainer/labtainer-student$ checkwork
Results stored in directory: /home/student/labtainer_xfer/centos-log2
Labname centos-log2

Student | logger_count | last_count | service_count | debug_log | exact_debug |
log_mark | centralized |
===== | ===== | ===== | ===== | ===== | ===== |
B22DCAT176 | 14 | 1 | 1 | Y | Y |
Y | Y |

What is automatically assessed for this lab:
log_mark: Altered rsyslog.conf, resulting in mark written to system log
logger_count, last_count, service_count: Counts of quantity of commands issued.
debug_log: Altered rsyslog.conf, resulting in debug messages going to
a custom log file (though it may not be limited to debug messages)
exact_debug: Altered rsyslog.conf, resulting in only debug messages going to
a custom log file
student@ubuntu:~/labtainer/labtainer-student$ stoplab
```

TÀI LIỆU THAM KHẢO

- [1] Đinh Trường Duy, Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2022.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.