HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

Bài báo cáo thực hành số 2

Môn học: Phân tích mã độc

Khám phá Nhật ký (Log) Unix trên CentOS

Tên sinh viên: Ninh Chí Hướng

Mã sinh viên: B20DCAT094

Nhóm lớp : 02

Giảng viên hướng dẫn: PGS.TS Đỗ Xuân Chợ

HÀ NỘI, THÁNG 10/2023

Bài thực hành: Khám phá Nhật ký (Log) Unix trên CentOS

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.

2. **Yêu cầu đối với sinh viên:**

Nắm được kiến thức về CentOS và syslog.

3. **Nội dung thực hành**

Chuẩn bị lab

- Khởi động lab:

```
labtainer centos-log2
```

(chú ý: sinh viên sử dụng tên tài khoản của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu trong terminal, để sử dụng khi chấm điểm. Thông thường tên tài khoản của sinh viên chính là Mã sinh viên)

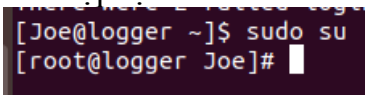
Các nhiệm vụ

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

#1 Quyền hạn của người dùng thông thường có đối với tệp messages

1. Trong terminal, nhập lệnh sudo su nhưng nhập sai mật khẩu cho người dùng root.

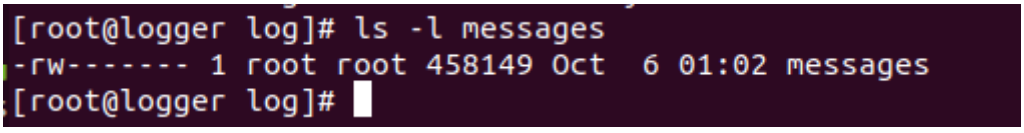
2. Nhập lệnh sudo su. Nếu làm đúng, dấu nhắc sẽ kết thúc bằng ký tự '#'.

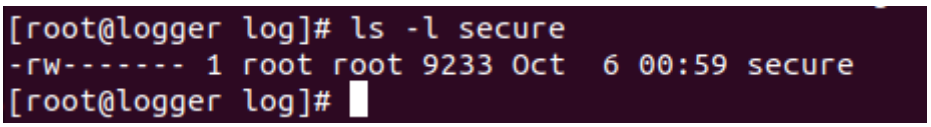


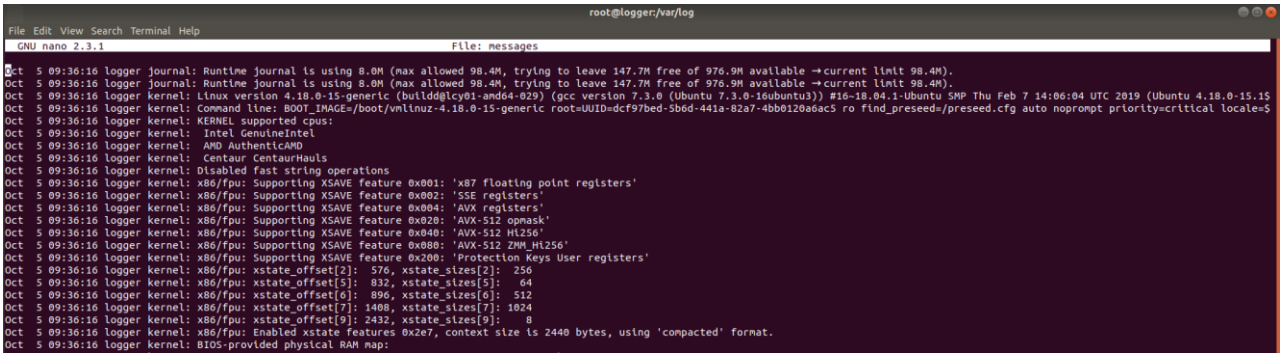
3. Khám phá thư mục log

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

Xem quyền truy cập của messages log.







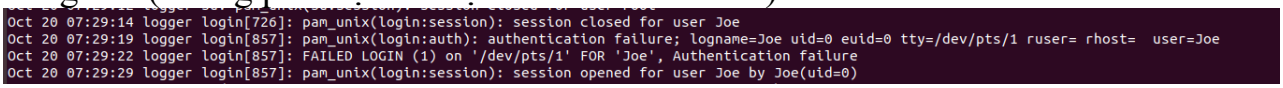
o rw chỉ ra rằng tệp messages là 1 tệp văn bản và người dùng có nguyền đọc và ghi ở đây là người dùng gốc(root)

o Phần còn lại "-------" đại diện cho quyền hạn cho nhóm người dùng khác trong hệ thống nhưng trong trường hợp này tất cả các quyền đều bị tắt

4. Mật khẩu sai

o 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.

o 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).



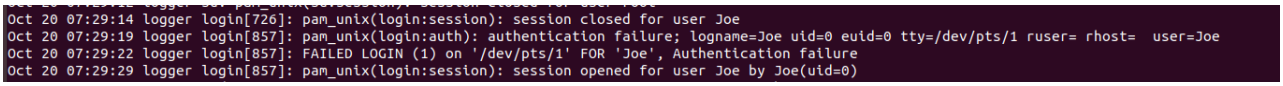
#2: Cụm từ được sử dụng để chỉ ra sự thất bại trong việc đăng nhập.

o Cụm từ được sử dụng để chỉ ra sự thất bại trong việc đăng nhập ở đây là: "Authentication failure". Thông báo này thông báo rằng "Joe" không cung cấp thông tin xác thực hợp lệ (ví dụ: tên người dùng không chính xác, mật khẩu sai, v.v.), dẫn đến việc đăng nhập không thành công.

#3: Câu trả lời bổ sung

5. Mật khẩu là tên người dùng

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

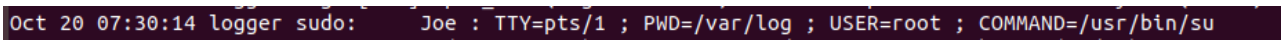


#4: Cụm từ được sử dụng khi bạn nhập một tên người dùng không hợp lệ.

- Cụm từ được sử dụng khi bạn nhập một tên người dùng không hợp lệ ở đây là: "FOR 'UNKNOWN'". Thông báo này thường xuất hiện khi cố gắng đăng nhập với một tên người dùng không tồn tại trong hệ thống hoặc tên người dùng đã bị nhập sai. Nó cho thấy rằng hệ thống không thể xác định người dùng cụ thể nào đang cố gắng đăng nhập và quá trình xác thực đã thất bại.

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.



#5: Thông tin được ghi lại về việc sử dụng su

- Thông báo này cho thấy rằng người dùng "Joe" đã sử dụng lệnh "su" để chuyển đổi sang người dùng khác hoặc quyền hạn cao hơn.

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

```
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 host-
 Manual page last(1) line 30 (press h for help or q to quit)
```

#6: Lựa chọn -t của lệnh last

- Hiển thị trạng thái đăng nhập theo thời gian được chỉ định

```
[root@logger log]# last -t 20230801000000 wtmp

wtmp begins Thu Oct  5 09:36:18 2023
```

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

a. 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

b. Bật tính năng Mark:

- 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.

```
#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
$ModLoad immark  # provides --MARK-- message capability
$MarkMessagePeriod 60
```

c. 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***

```
[root@logger log]# service rsyslog restart
Redirecting to /bin/systemctl restart rsyslog.service
[root@logger log]#
```

d. Xem thay đổi này đã được thực hiện trong các nhật ký vằng 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.

```
[root@logger log]# tail -f /var/log/messages
Oct 20 07:30:14 logger su: (to root) Joe on pts/1
Oct 20 07:34:55 logger systemd: Started Session 10 of user Joe.
Oct 20 07:34:55 logger systemd-logind: New session 10 of user Joe.
Oct 20 07:34:55 logger systemd: Starting Session 10 of user Joe.
Oct 20 07:35:16 logger su: (to root) Joe on pts/1
Oct 20 07:50:18 logger systemd: Stopping System Logging Service...
Oct 20 07:50:18 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="39" x-info="http://www.rsyslog.com"] exiting on signal 15.
Oct 20 07:50:18 logger systemd: Starting System Logging Service...
Oct 20 07:50:18 logger rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="1249" x-info="http://www.rsyslog.com"] start
Oct 20 07:50:18 logger systemd: Started System Logging Service.
Oct 20 07:51:18 logger rsyslogd: -- MARK --
Oct 20 07:52:18 logger rsyslogd: -- MARK --
Oct 20 07:53:18 logger rsyslogd: -- MARK --
```

3. 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.

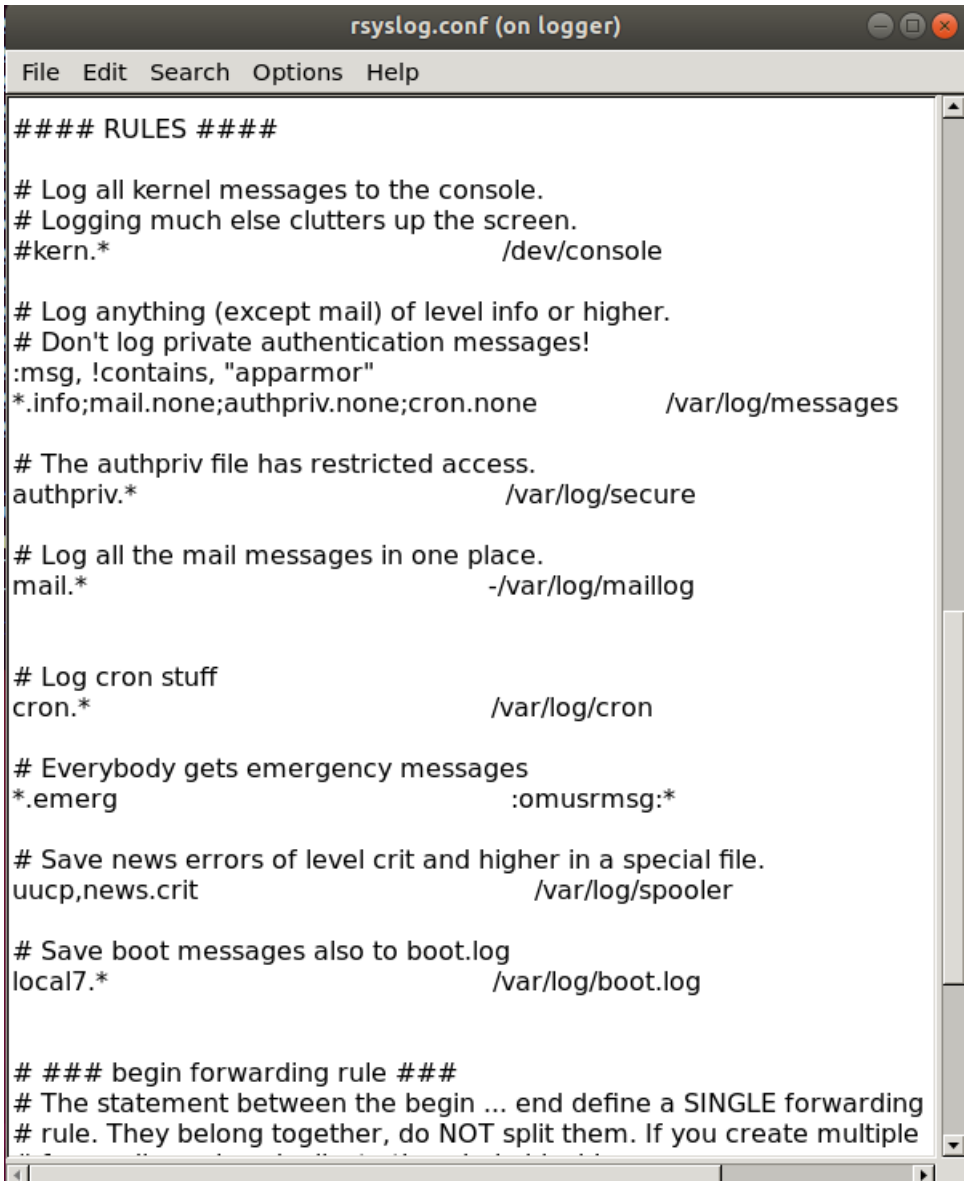
1. Đọc phần DESCRIPTION trong trang man của tiện ích logger: man logger

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.

```
[root@logger log]# man logger
[root@logger log]# logger -p info "Hello World"
[root@logger log]#
```

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



o #7: Quy tắc syslog chỉ định điều gì sẽ xảy ra với mục mà sinh viên đã gửi đến syslog trong bước tạo thư mục trong /var/long/messagess *.info;mail.none;authpriv.none;cron.none /var/log/messages

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 log]# grep "Hello World" /var/log/messages
Oct 20 07:56:35 logger Joe: Hello World
Oct 20 08:15:48 logger Joe: Hello World
```

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.

```
# Save boot messages also to boot.log
local7.*                                /var/log/boot.log
if $syslogseverity-text =='debug' then   /var/log/mydebug

# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
```

#8: Quy tắc đã sử dụng để đáp ứng yêu cầu debug if $syslogseverity-text ==’debug’ then /var/log/mydebug

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

```
[root@logger log]# systemctl restart rsyslog
[root@logger log]#
```

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

9. Kiểm tra quy tắc đã thêm vào rsyslog.conf

#9. Kiểm tra quy tắc debug

```
[root@logger log]# systemctl restart rsyslog
[root@logger log]# logger -p debug "ninh chi huong'
> ^C
[root@logger log]# logger -p debug "ninh chi huong"
[root@logger log]# grep "huong" /var/logmydebug
grep: /var/logmydebug: No such file or directory
[root@logger log]# grep "huong" /var/mydebug
grep: /var/mydebug: No such file or directory
[root@logger log]# grep "huong" /var/log/mydebug
Oct 20 08:03:57 logger Joe: ninh chi huong
```

```
[root@logger log]# ll /bin/logger
-rwxr-xr-x 1 root root 29224 Dec  1  2017 /bin/logger
```

10. Thực hiện các bước để hiện 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.

```
[root@logger log]# ll /bin/logger
-rwxr-xr-x 1 root root 29224 Dec  1  2017 /bin/logger
[root@logger log]# sudo chmod 750 /bin/logger
[root@logger log]# ll /bin/logger
-rwxr-x--- 1 root root 29224 Dec  1  2017 /bin/logger
```

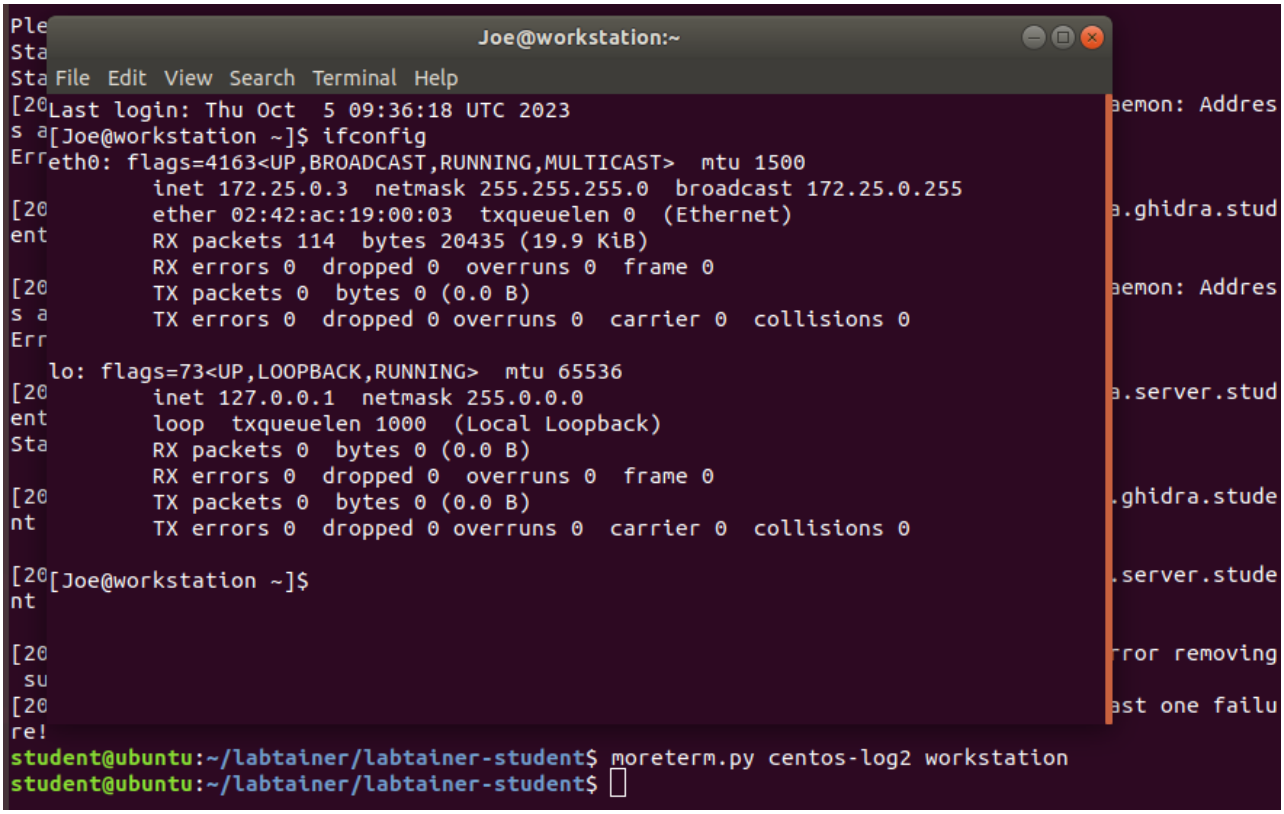
4. Nhiệm vụ 4: Ghi log tập trung:

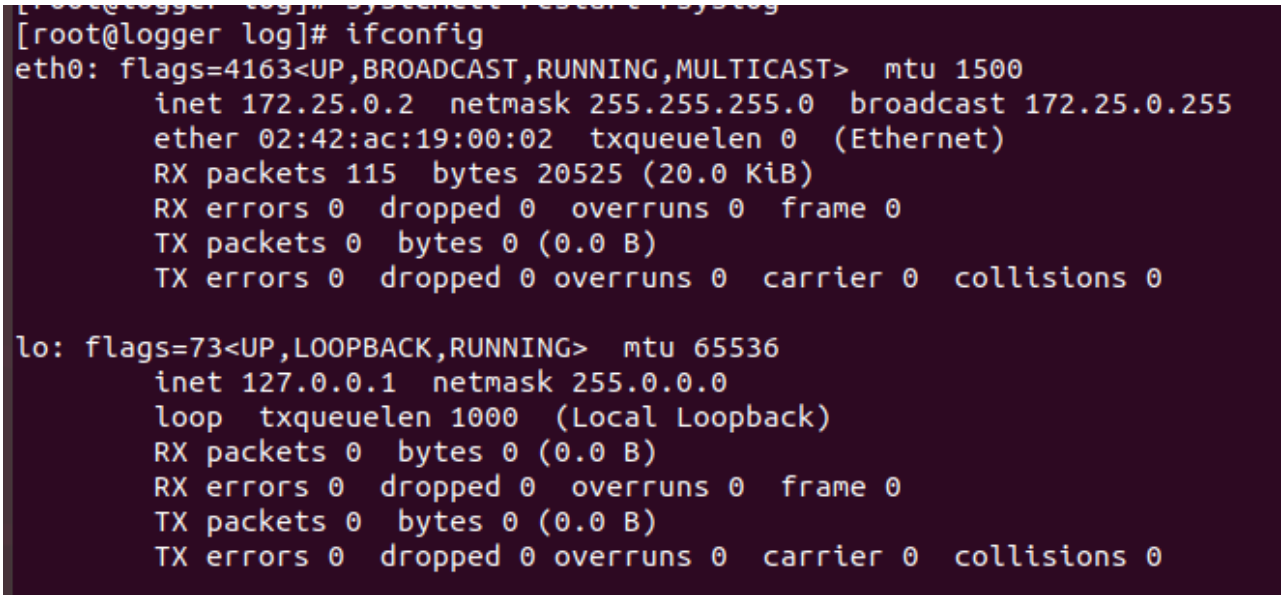
- Giả sử sinh viên có một số hệ thống Linux cần quản lý. Thay vì cấu hình và xem xét việc ghi log trên từng hệ thống, sinh viên có thể xác định một hệ thống ghi log tập trung và sau đó chuyển tiếp các thông báo log từ mỗi hệ thống đến hệ thống ghi log tập trung đó. Ở phần này, sinh viên sẽ cấu hình hệ 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.

1. Mở lại tệp cấu hình /etc/rsyslog.conf trên máy tính ghi log.
2. 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:

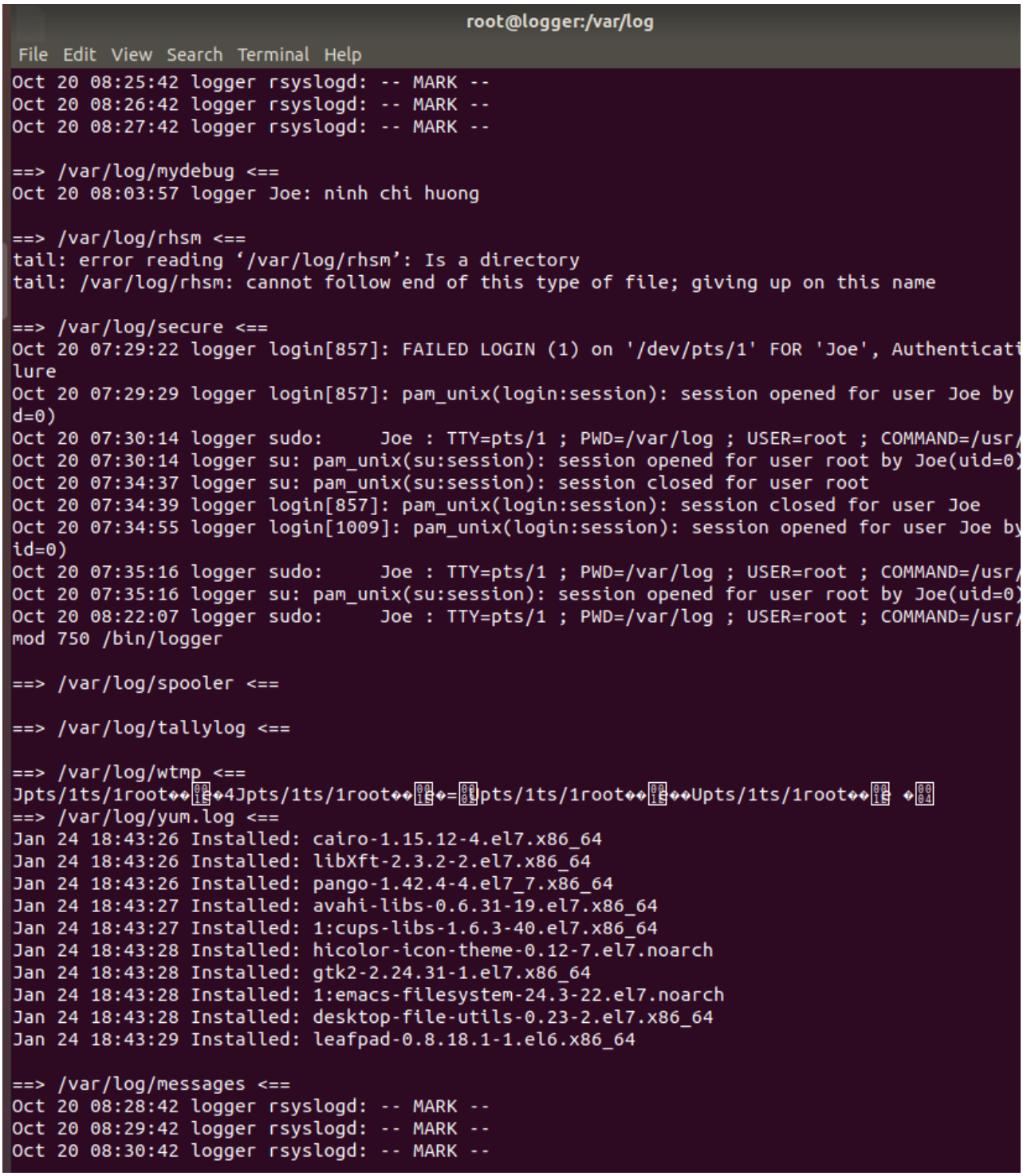
```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

3. Khởi động lại rsyslog
4. Trên terminal chính của hệ thống lab sử dụng lệnh: moreterm.py centos-log2 workstation
5. 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.

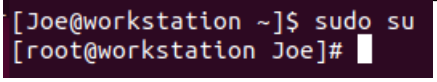

Joe@workstation:~
File Edit View Search Terminal Help
Last login: Thu Oct 5 09:36:18 UTC 2023
[Joe@workstation ~]$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.25.0.3 netmask 255.255.255.0 broadcast 172.25.0.255
ether 02:42:ac:19:00:03 txqueuelen 0 (Ethernet)
RX packets 114 bytes 20435 (19.9 KiB)
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
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
[Joe@workstation ~]$
student@ubuntu:~/labtainer/labtainer-student$ moreterm.py centos-log2 workstation
student@ubuntu:~/labtainer/labtainer-student$


[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 115 bytes 20525 (20.0 KiB)
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
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

6. Trên máy tính ghi log, sử dụng "tail" để xem các nhật ký: tail -f /var/log/*



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



8. Mở tệp /etc/rsyslog.conf trên máy tính trạm
   - 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

# 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 ###
```

9. Khởi động lại rsyslog trên máy tính trạm và quan sát các thông báo log trên máy tính ghi log.

```
==> /var/log/messages <==
Oct 20 08:28:42 logger rsyslogd: -- MARK --
Oct 20 08:29:42 logger rsyslogd: -- MARK --
Oct 20 08:30:42 logger rsyslogd: -- MARK --
Oct 20 08:31:43 logger rsyslogd: -- MARK --
Oct 20 08:32:43 logger rsyslogd: -- MARK --
Oct 20 08:33:43 logger rsyslogd: -- MARK --
Oct 20 08:34:31 workstation systemd: Stopping System Logging Service...
Oct 20 08:34:31 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="37" x
-info="http://www.rsyslog.com"] exiting on signal 15.
Oct 20 08:34:31 workstation systemd: Starting System Logging Service...
Oct 20 08:34:31 workstation rsyslogd: [origin software="rsyslogd" swVersion="8.24.0" x-pid="246"
x-info="http://www.rsyslog.com"] start
Oct 20 08:34:31 workstation systemd: Started System Logging Service.
Oct 20 08:34:43 logger rsyslogd: -- MARK --
```

10. 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.

```
==> /var/log/secure <==
Oct 20 08:36:37 workstation su: pam_unix(su:session): session closed for user root

==> /var/log/messages <==
Oct 20 08:36:42 workstation su: (to root) root on pts/1
Oct 20 08:36:43 logger rsyslogd: -- MARK --

==> /var/log/secure <==
Oct 20 08:36:42 workstation sudo:     Joe : TTY=pts/1 ; PWD=/home/Joe ; USER=root ; COMMAND=/usr/
bin/su
Oct 20 08:36:42 workstation su: pam_unix(su:session): session opened for user root by (uid=0)
Oct 20 08:37:24 workstation su: pam_unix(su:session): session closed for user root
```

checkwork

```
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 |
====================|=================|=================|=================|=================|=================|=================|=================|
B20DCAT094          |               8 |               2 |               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
```

1.Nhiệm vụ 5: Trả lời câu hỏi:

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

- Không có được quyền nào được cấp cho người dùng thông thường

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

- Failed" hoặc "Authentication 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.

```
Sep 25 14:16:05 logger login[251]: FAILED LOGIN (1) on '/dev/pts/2' FOR 'Joe', Authentication fa$
Sep 25 14:16:14 logger login[251]: FAILED LOGIN (2) on '/dev/pts/2' FOR 'Joe', Authentication fa$
```

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

"su:"

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

- Hiển thị trạng thái đăng nhập theo thời gian được chỉ định

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")?

- *.info;mail.none;authpriv.none;cron.none /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?

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

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

```
[root@logger log]# systemctl restart rsyslog
[root@logger log]# logger -p debug "ninh chi huong'
> ^C
[root@logger log]# logger -p debug "ninh chi huong"
[root@logger log]# grep "huong" /var/logmydebug
grep: /var/logmydebug: No such file or directory
[root@logger log]# grep "huong" /var/mydebug
grep: /var/mydebug: No such file or directory
[root@logger log]# grep "huong" /var/log/mydebug
Oct 20 08:03:57 logger Joe: ninh chi huong
```

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?

- Chomd 750 /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?

- Trong tệp cấu hình rsyslog.conf đã cung cấp, không có quy tắc cụ thể để xử lý các bản ghi từ kernel với mức ưu tiên là emerg

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
```

- Khi rsyslog nhận được một bản ghi từ facility mail với mức ưu tiên là notice, nó sẽ ghi bản ghi đó vào tệp log "/var/log/maillog".

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?
    - Trong tệp cấu hình rsyslog.conf đã cung cấp, không có quy tắc cụ thể để xử lý các bản ghi từ facility local6 với mức ưu tiên là err. Do đó, không có hành động cụ thể nào được xác định trong tệp cấu hình này để xử lý các bản ghi từ facility local6 với mức ưu tiên là err.
13. Mô tả bất kỳ thử nghiệm hoặc khám phá bổ sung nào sinh viên đã thực hiện.
    - Chưa có
14. Sinh viên đã học được điều gì từ bài thực hành này?
    - Các ghi log và thực hiện truy xuất log và phân quyền người dùng
15. Cần làm gì để cải thiện bài thực hành này?
    - Thực hiện nhiều thao tác truy nhập dữ liệu khác nhau trong từng /var/log hơn