# **Scenario Based Questions**

**Login to the Linux system using the account you are given.**

**Run the command**

**sudo -i**

**This will enable you to run a series of administrative commands *as root*.**

***Please be patient, some of the commands take a minute or so to run.***

# Log File Management

1. Run /scenariolabs/LogFiles/Q1

Now run logger –p kern.error “Test Messages 1214”

Does this message appear in /var/log/messages at the end?

If not, then something is wrong with the system logging arrangement? Try to find out what.

Try: logger -p kern.error “Test Message 1214”

Try: systemctl restart rsyslog

Try: logger -p kern.error “Test Message 1214”

Try: tail /var/log/messages

Geoff’s version

logger -p kern.error “Test Message 1214”

tail /var/log/messages (NB: can’t see it – Q is the network down?)

ps ef | grep rsyslog (NB: notice there is no syslog deamon)

systemctl status rsyslog (NB: it is not running)

systemctl start rsyslog (NB: running)

logger -p kern.err “Test Message 1214”

tail /var/log/messages

1. Run /scenariolabs/LogFiles/Q2

Now use putty and attempt to log in as ‘apache’.

Look at /var/log/messages. can you see the messages relating to the bad login. They ought NOT to be there. (No messages about bad logins and the like should be in /var/log/messages as this file is sometimes shared with third parties. No account/user names should be visible.) Try to fix this.

Try see the last bad login: lastb | head

instruct ssh:notty static-84-9-5-23 Mon Jul 18 16:08 - 16:08 (00:00)

Try see bad login in messages: tail /var/log/messages

Jul 19 19:33:01 ml-refvm-422293 systemd: Created slice User Slice of root.

Jul 19 19:33:02 ml-refvm-422293 systemd: Started Session 37 of user root.

Jul 19 19:33:02 ml-refvm-422293 systemd: Removed slice User Slice of root.

Jul 19 19:34:01 ml-refvm-422293 systemd: Created slice User Slice of root.

Jul 19 19:34:01 ml-refvm-422293 systemd: Started Session 38 of user root.

Jul 19 19:34:01 ml-refvm-422293 systemd: Removed slice User Slice of root.

Jul 19 19:35:01 ml-refvm-422293 systemd: Created slice User Slice of root.

Jul 19 19:35:01 ml-refvm-422293 systemd: Started Session 39 of user root.

Jul 19 19:35:01 ml-refvm-422293 systemd: Started Session 40 of user root.

Jul 19 19:35:01 ml-refvm-422293 systemd: Removed slice User Slice of root.

Try to look at the rsylog file: cat /etc/rsyslog.conf (NB: looks fine)

Try: grep "Failed password" /var/log/messages | head -3 (NB: brought up failed logins from 2 hrs ago

nano /etc/rsyslog.conf (NB: change the line with authpriv.emerg to authpriv.none)

systemctl restart rsyslog

tail /var/log/messages | grep apache (NB: shows nothing as it should)

tail /var/log/secure | grep apache (NB: shows bad loggins)

Geoff’s version

grep apache /var/log/messages

tail /var/log/messages (NB: the bad loggins are here but they should not be they should be in secure

grep ‘var/log/messages’ /etc/rsyslog.conf

we can see “…authpriv.emeg…” it should be authpriv.none, so change it

nano /etc/rsyslog.conf

systemctl restart rsyslog

tail /var/log/messages | grep apache (NB: shows nothing)

tail /var/log/secure | grep apache (NB: shows bad logins)

1. Run /scenariolabs/LogFiles/Q3

Take a look at /var/log/cron. Can you see that a job runs every minute mentioning /tmp/hiLog?

Wait one minute and confirm this log entry has stopped. Look at the content of /tmp/hiLog to confirm that, in fact the cron job itself is still running. What of the log entries? Please fix!

cat /var/log/cron

cat /tmp/hiLog

cron -l

crontab -l (NB: cron is logging but log is not)

grep cron /etc/rsyslog

nano /etc/rsyslog.conf (NB: edit, cron.none to cron.info

grep ‘^cron’ /etc/rsyslog.conf (NB: use this to find the line starting with cron)

systemctl restart rsyslog

1. Run the command sequence

touch /etc/now ; find /var –type f –newer /etc/now

This move updates the modification time of the file /etc/now and then searches the whole of /var for files updated more recently than /etc/now. *Under these circumstances there should not be any*.

Now point the web browser on the windows machine at the IP address of the Linux machine. You should see a website. Now run /scenariolabs/LogFiles/Q4. Reload the webpage and you should now see an error.

Rerun find /var –type f –newer /etc/now

You should now see all a series of file names, not all of which are directly related to you recent activity but some will be. They should reveal the name of error log associated with httpd. Use the information in the relevant file to correct the problem.

Touch /etc/now ; find /var -type f -newer /etc/now

Wget -r <http://localhost> ; find /var -type f -newer /etc/now (NB: this shows me that the error log can be found in /var/log/httpd/error\_log

Tail /var/log/httpd/error\_log (NB: see “cannot serve directory /web/: No matching Directory Index (index.html)”)

ls / (NB: we see we have a web folder)

ls -l /web (NB: we can see a file index.htm, the file is not index.html

mv /web/index.htm /web/index.html

wget -r http://localhost

1. Run the command sequence

Run /scenariolabs/LogFiles/Q5

Now run ‘systemctl stop httpd’

then

‘systemctl start httpd’.

Read the error message, follow the instructions, read the error messages, fix the problem!

systemctl stop httpd

systemctl start httpd

systemctl status httpd.service (NB: says could not open configuration file /etc/httpd/conf/httpd.conf: No such file or directory)

look for the file

cd /etc/httpd/conf

ls -l (NB: shows “was-httpd.conf” which is an old version)

systemclt start httpd

wget -r http://localhost