# **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 1234”

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.

1. Run /scenariolabs/LogFiles/Q2

Attempt to log in as the user ‘sync’. (Change instructor in your connection string to sync)

Look at /var/log/messages. Can you see 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.

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!

1. Run the command sequence

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

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

The machine you are on has a webserver, which we need to enable.

Run the command ‘setenforce 0’. This switches off security enhanced linux. SELinux secure web facing services, providing an extra layer of security. We need to switch this off for the moment. Don’t worry, port 80 is not exposed to the internet.

Now start up the web service using the command

systemctl restart httpd

It should start without an error. We can test the service by running the command

wget -r <http://localhost>

# wget -r http://localhost

--2020-07-20 10:49:53-- http://localhost/

Resolving localhost (localhost)... ::1, 127.0.0.1

Connecting to localhost (localhost)|::1|:80... connected.

HTTP request sent, awaiting response... 200 OK

Length: 289 [text/html]

Saving to: ‘localhost/index.html’

100%[=====================================================================>] 289 --.-K/s in 0s

2020-07-20 10:49:53 (34.0 MB/s) - ‘localhost/index.html’ saved [289/289]

Loading robots.txt; please ignore errors.

--2020-07-20 10:49:53-- http://localhost/robots.txt

Reusing existing connection to [localhost]:80.

HTTP request sent, awaiting response... 404 Not Found

2020-07-20 10:49:53 ERROR 404: Not Found.

--2020-07-20 10:49:53-- http://localhost/images/sf01.jpg

Reusing existing connection to [localhost]:80.

HTTP request sent, awaiting response... 200 OK

Length: 124244 (121K) [image/jpeg]

Saving to: ‘localhost/images/sf01.jpg’

100%[=====================================================================>] 124,244 --.-K/s in 0s

2020-07-20 10:49:53 (381 MB/s) - ‘localhost/images/sf01.jpg’ saved [124244/124244]

--2020-07-20 10:49:53-- http://localhost/cgi-bin/myscript.sh

Reusing existing connection to [localhost]:80.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]

Saving to: ‘localhost/cgi-bin/myscript.sh’

[ <=> ] 101 --.-K/s in 0.001s

2020-07-20 10:49:53 (71.9 KB/s) - ‘localhost/cgi-bin/myscript.sh’ saved [101]

--2020-07-20 10:49:53-- http://localhost/images/sf03.jpg

Reusing existing connection to [localhost]:80.

HTTP request sent, awaiting response... 200 OK

Length: 129121 (126K) [image/jpeg]

Saving to: ‘localhost/images/sf03.jpg’

100%[=====================================================================>] 129,121 --.-K/s in 0s

2020-07-20 10:49:53 (425 MB/s) - ‘localhost/images/sf03.jpg’ saved [129121/129121]

FINISHED --2020-07-20 10:49:53--

Total wall clock time: 0.01s

Downloaded: 4 files, 248K in 0.002s (122 MB/s)

[root@ML-RefVm-198965 mywebpage]#

You will see messages about files downloading

Now run /scenariolabs/LogFiles/Q4. re-run the ‘wget’ command. This time there is an error.

Using your new found skills, first locate the error log. Find the error message and fix the problem. Good luck.

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.

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!