**General Instructions:**

* **Follow the instructions given in each section.**
* **Make sure that you attempt the questions in order.**

**SECTION-A (10\*1 mark=10 marks)**

***(All questions are compulsory)***

Q1 Which of the following commands is used to summarize the disk usage?

a) chkdsk

**b) du**

c) fdisk

d) disk

Q2 Which of the following commands is used to count just the number of lines contained in a file?

**a) wc – 1**

b) wc - w

c) wc - c

d) wc – r

Q3 Command used to determine the path of an executable file is

**a) which**

b) where

c) wexec

d) what

Q4 The command that can be used to restrict incoming messages to a user is

**a) mesg**

b) halt

c) grep

d) sleep

Q5 In "bash", "if" constructs are ended with

**a) Fi**

b) Endif

c) End

d) None of the above

Q6 What can he used to set up a firewall on a Linux system?

a) netstat

b) route

c) trace

**d) ipchain**

Q7 What will be printed for the command below?

$ grep –c “^echo” abc

a) The count of lines that do not contain the pattern echo in file abc

**b) The count of lines which begin with the pattern echo in file abc**

c) The count of lines that ends with the pattern echo in file abc

d) None of the above

Q8 What command is used to save the standard output in a file, as well as display it on the

terminal?

**a) tee**

b) grep

c) cat

d) more

Q9 Which tar command option is used to list the files in a tape archive format?

a) cvf

**b) tvf**

c) xvf

d) ovf

Q10 The command that can be used to restrict incoming messages to a user is

**a) mesg**

b) halt

c) grep

d) sleep

**SECTION-B (5\*2 mark=10 marks)**

***(All questions are compulsory)***

Q11 A user executes the following command successfully:

$ chmod +x file1.txt

Which of the following is true of the output of this command?

a) The command results in adding execute permission to the user who ran this command

b) The command results in adding execute permission for the owner of the file

c) The command results in an error since the file is not an executable file

**d) The command results in adding execute permission for all users (i.e., user,group & others)**

Q12 After running this program, as you press ‘s’, what will be the output of the program?

#!/bin/bash

echo "press 's' to print Sanfoundry"

read var

if $var=s

then

echo "Sanfoundry"

else

echo "You did not press s"

fi

exit 0

a) Sanfoudry

b) You did not press s

**c) program will generate an error message**

d) none of the mentioned

Q13 What will be output of following command:

$ echo "The process id is" $$$$

a) The process id is $$

b) The process id is $<pid>$<pid>

**c) The process id is <pid><pid>**

d) The process id is $$$$

Q14 What would be the current working directory at the end of the following command sequence?

$ pwd

/home/user1/proj

$ cd src

$ cd generic

$ cd .

$ pwd

a) /home/user1/proj

b) /home/user1/proj/src

c) /home/user1

**d) /home/user1/proj/src/generic \*\*\*\*\*\*\*\***

Q15 What is the output of the following program?

x = 3; y = 5; z = 10;

if [( $x -eq 3 ) -a ( $y -eq 5 -o $z -eq 10 )]

then

echo $x

else

echo $y

fi

a) 1

**b) 3**

c) 5

d) Error

**SECTION-C() (4x5 marks=20 marks)**

Q 16 How can you enhance the security of the password file in Linux?

Ans-

It is in the test file named ‘/etc/passwd’ that Linux usually keeps its user account details, including the one-way encrypted passwords. However, this file can be accessed with the help of different tools, which might throw security issues.

To minimize this risk, we will make use of the shadow password format that saves the account details in a regular file /etc/passwd as in the traditional method but with the password stored as a single ‘x’ character, i.e., it is not the original password that is actually stored in this file. Meanwhile, a second file /etc/shadow will have the encrypted password, along with the other relevant information, such as the account/password expiration date, etc. Most importantly, the latter file is readable only by the root account, and thus it minimizes the security risk.

Q 17 How can you determine the total memory used by LINUX?

Ans-

It is always required to keep a check on the memory usage in order to find out whether the user is able to access the server or the resources adequately. There are roughly 5 methods that determine the total memory used by Linux.

This is explained as below:

Free command: This is the most simple command to check memory usage. For Example, ‘$ free –m’, the option ‘m’ displays all the data in MBs.

/proc/meminfo: The next way to determine memory usage is to read /proc/meminfo file. For Example, ‘$ cat /proc/meminfo’

Vmstat: This command basically lays out the memory usage statistics. For Example, ‘$ vmstat –s’

Top command: This command determines the total memory usage as well as also monitors the RAM usage.

Htop: This command also displays memory usage along with other details.

Q 18 How to check which ports are listening in my Linux Server?

Ans-

We have two commands to check which ports are in listening in Linux Server. Following are the two commands

# netstat --listen

# netstat -l

Q 19 How to declare and delete variables in bash?

Ans-

The variable can be declared in bash by data type or without data type. If any bash variable is declared without declare command, then the variable will be treated as a string. Bash variable is declared with declare command to define the data type of the variable at the time declaration.

–r, -i, -a, -A, -l, -u, -t and –x options can be used with declare command to declare a variable with different data types.

Example:

#!/bin/bash

#Declare variable without any type

num=10

#Values will be combined but not added

result=$num+20

echo $result

#Declare variable with integer type

declare -i num=10

#Values will be added

declare -i result=num+20

echo $result

unset command is used to remove any bash variable. The variable will be inaccessible or undefined after using unset command.

Example:

#!/bin/bash

str="Linux Hint"

echo $str

unset $str

echo $str