**DFCL Lab Assignment - LAB 1**

**Lab Questions:**

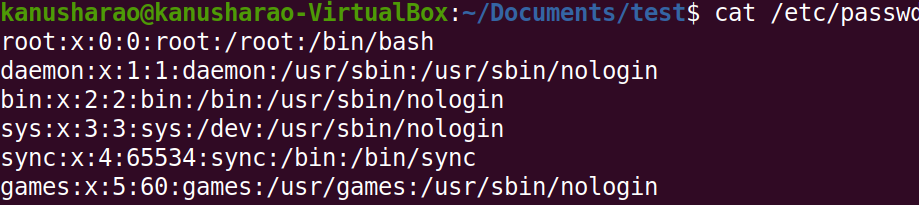
1. If we wanted to list all the .txt files in the current directory, what command would we want to use?

Ans: ls \*.txt



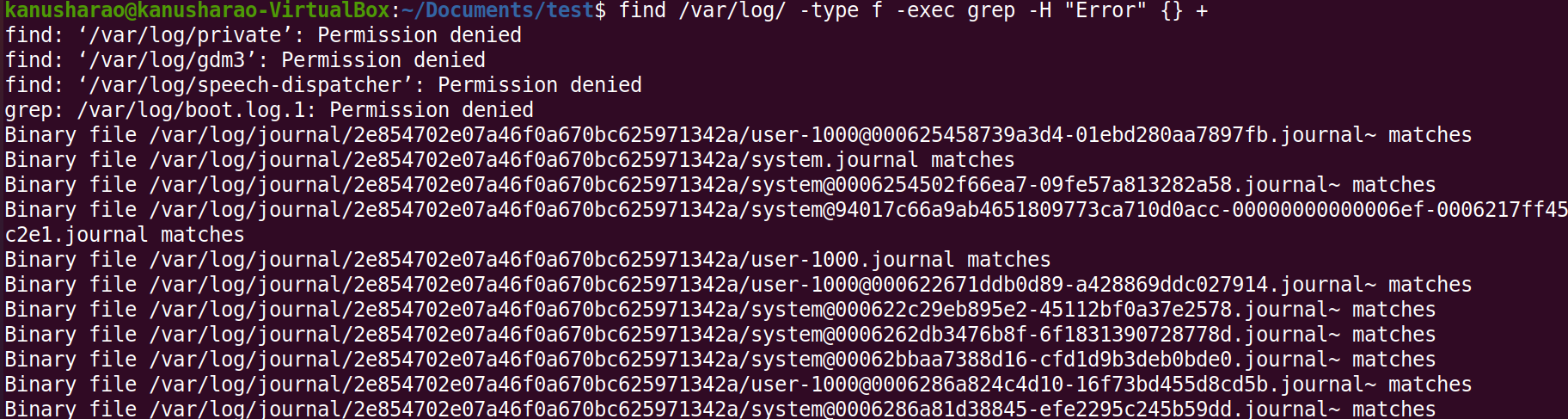
1. What command can we use to read the contents of the file /etc/passwd?

Ans: cat /etc/passwd



1. If we wanted to search for the string Error in all files in the /var/log directory, what would our command be?

Ans: find /var/log -type f -exec grep -H “Error” {} +

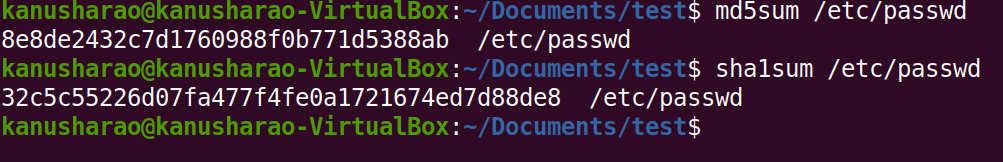


1. What would be the commands to calculate MD5 and SHA1 hashes of the file /etc/passwd?

Ans:

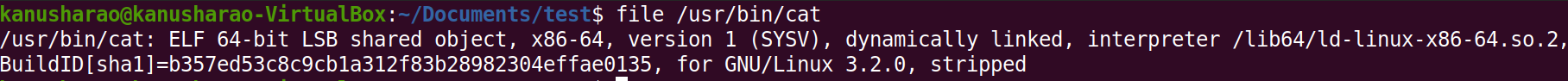
md5sum /etc/passwd

sha1sum /etc/passwd



1. Use the file command to determine the type of the file /usr/bin/cat and explain the output in 2-3 sentences.

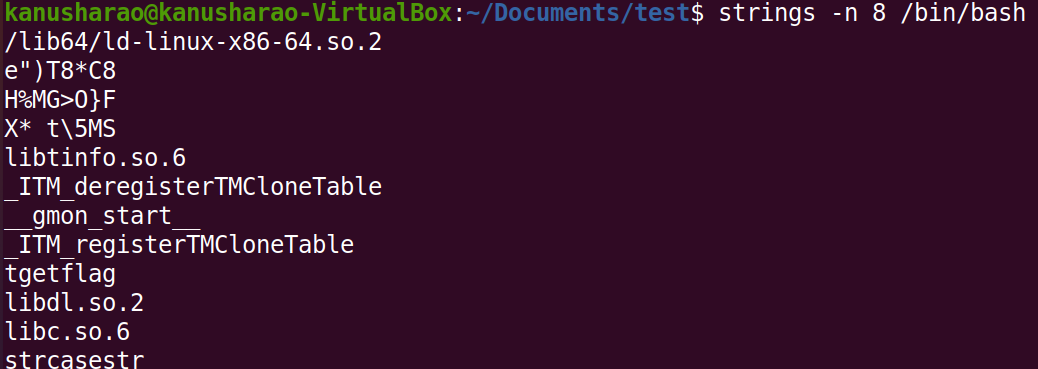
Ans: file /usr/bin/cat



* It is a 64-bit ELF binary for x86-64 architecture, dynamically linked with shared libraries and interpreted by /lib64/ld-linux-x86-64.so.2.
* It is compatible with GNU/Linux 3.2.0 and has been stripped of debugging symbols.

1. What command can we use to display all printable strings of length ≥ 8 in the file /bin/bash?

Ans: strings -n 8 /bin/bash



1. Given the following output of the file command, can you determine what’s wrong with this file?

$ file image.jpg

image.jpg: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=3ab23bf566f9a955769e5096dd98093eca750431, for GNU/Linux 3.2.0, not stripped

Ans: The image.jpg is not an image file but a ELF 64-bit LSB pie executable file. The file may have been named incorrectly or given a wrong extension for the executable.

1. If we wanted to look for files modified in the last 30 minutes in /home directory, what command would we want to use?

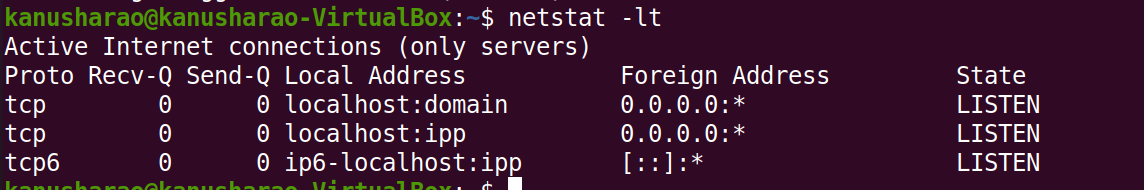
Hint: Explore how you can use find command to achieve this.

Ans: find /home -mmin -30



1. What command can we use to display information about all active TCP connections on the system?

Ans: netstat -lt



1. Given 3 corrupted image file, can you find a way to recover and view its contents?

Hint 1: A quick google search for “magic bytes” might help.

Hint 2: Explore how hexedit can help you here. The three corrupted files are named one, two and Three.

Used hexedit and modified the hex value to correct value for corresponding extention

