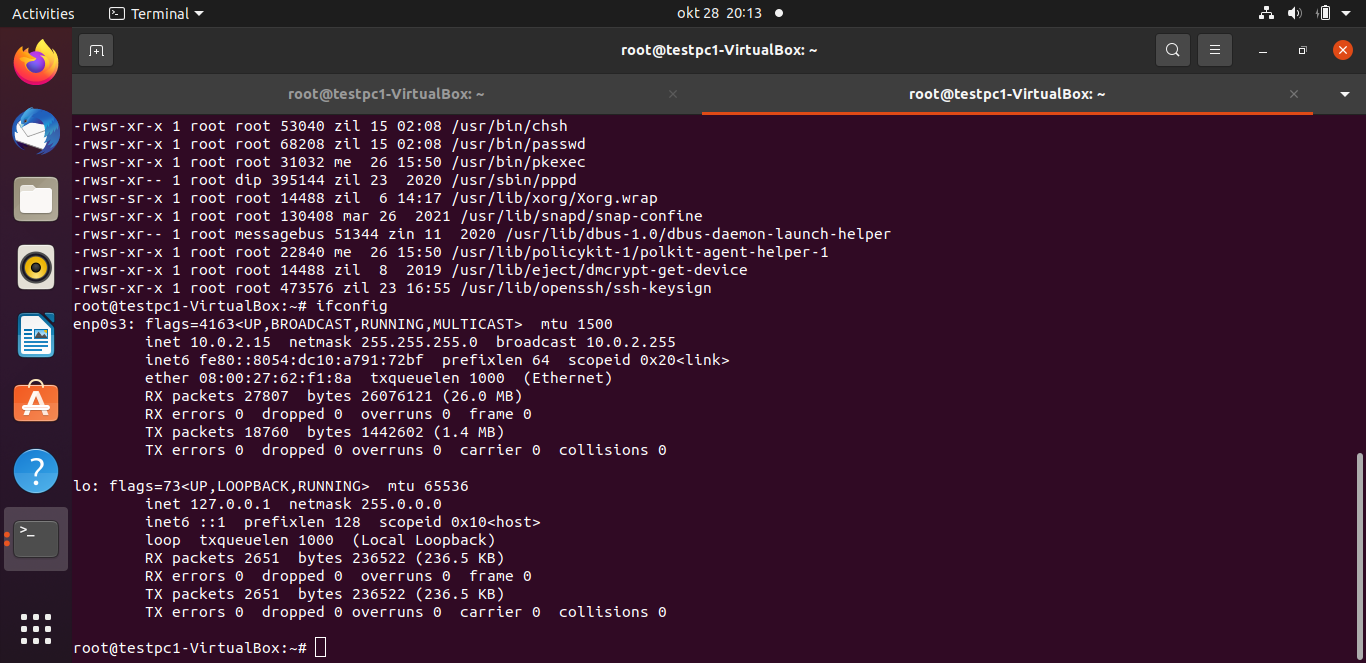
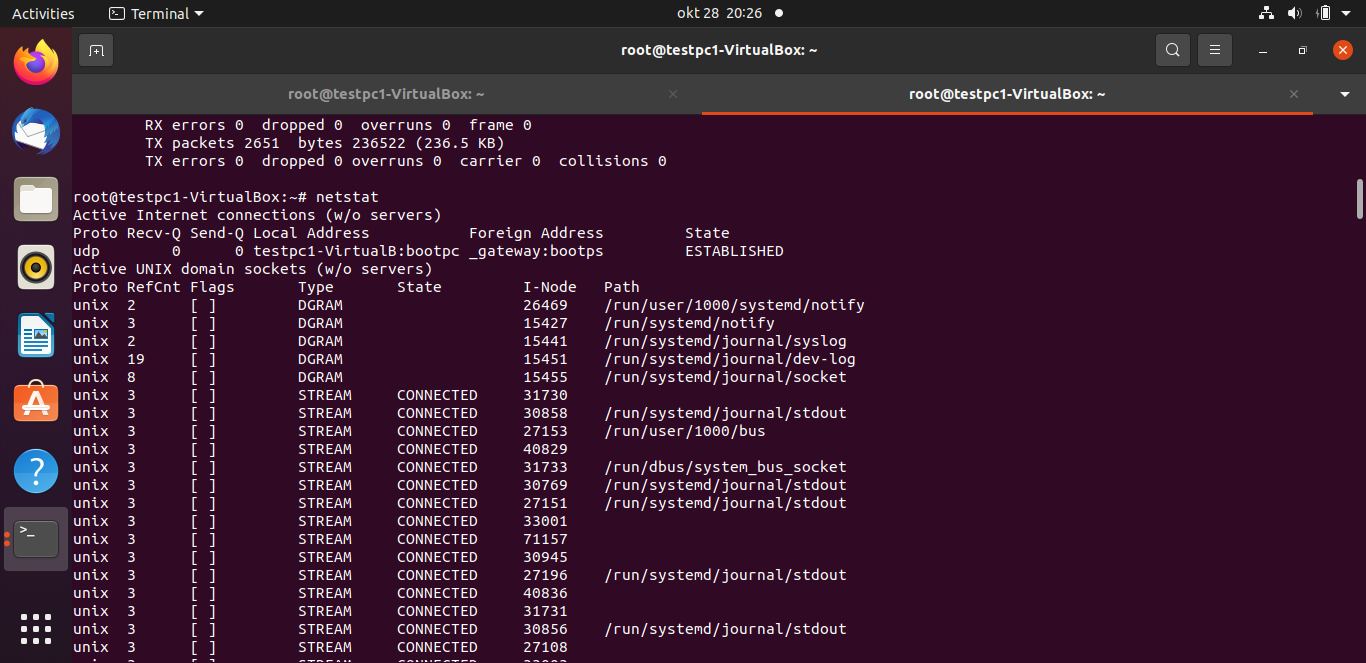
4530 LAB D

Ifconfig: Ifconfig is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary.If no arguments are given, ifconfig displays the status of the currently active interfaces.

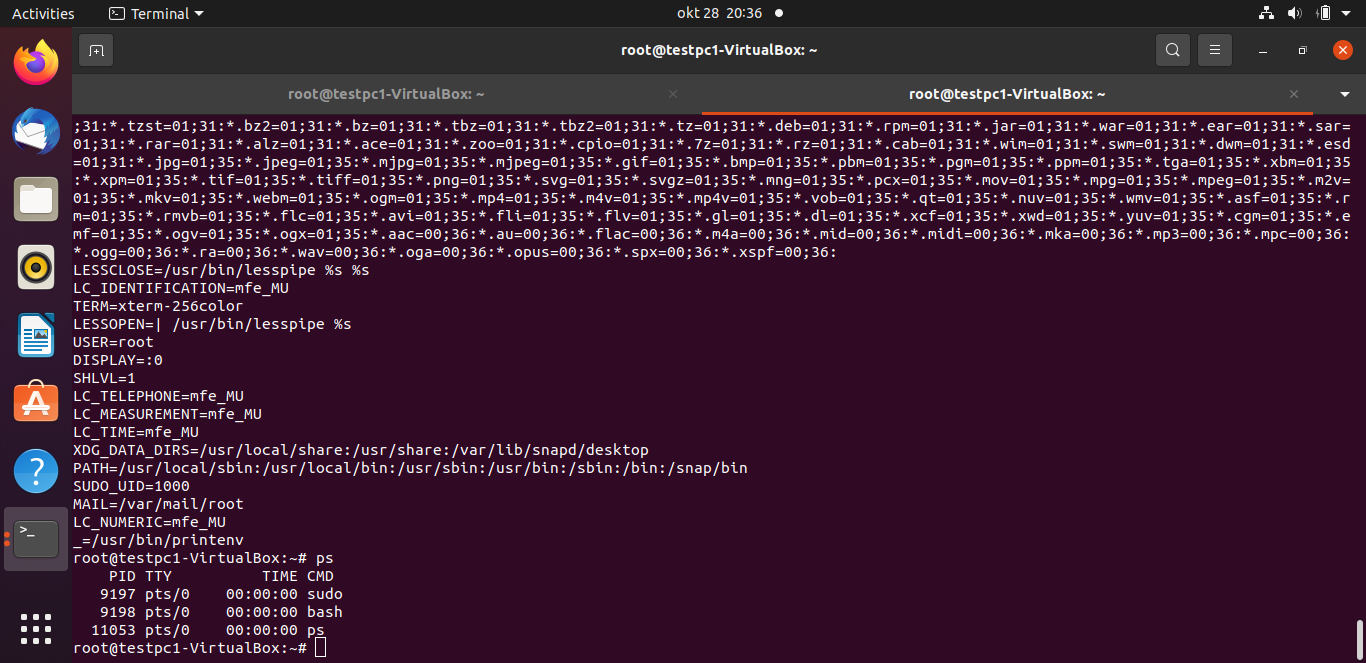


Netstat: The network statistics command is a networking tool used for troubleshooting and configuration, that also serves as a monitoring tool for both incoming and outgoing connections over the network.



Printenv: This command prints all or the specified environment variables. It can also set or unset shell variables. When used without an argument it will print a list of all variables including environment and shell variables, and shell functions.

Ps: Process Status, this command is used to list the currently running processes and their PIDs along with some other information depending on the accompanying option used.



Top: It provides a dynamic real-time view of the running system. Usually, this command shows in summary, information of the system and the list of processes or threads which are currently managed by the kernel.

Su: super user; Allows login as root user.

Sudo: super user do; allows a current user account to be elevated to have root privileges temporarily.

Useradd:  used for adding or creating user accounts in Linux.

Usermod: used to change the properties of a user in Linux via the terminal eg passwords or login directory.

Userdel:used to delete a user account and related files.

Groupadd:creates a new group account using the values specified on the command line and the default values from the system.

Chgrp:used to change the group ownership of a file or directory

Chmod: change mode; is used to manage file system access permissions on Unix and Unix-like systems. There are three basic file system permissions, or modes, to files and directories: read (r) write (w) and (x) execute.

Umask: used to assign the default file permission sets for newly created folders and files

Chown: change owner, is used to change the owner of file system files, directories in Linux

Chroot:  is used to change the root directory in Linux

Find: The find command is used to search and locate the list of files and directories based on conditions the specified for files that match the arguments.

Q 3. Can you read the content of the file /etc/shadow when you are not root? Why?

The content of file /etc/shadow cannot be read when not root because it belongs to an administrative group owned by the user root. Which means it can only be accessed with root privileges.

Check the content of the file /etc/shadow when you are root, and explain the file.

The file represents an individual user account and contains the following nine fields separated by colons (**:**)

* Username: connects the /etc/shadow file with /etc/passwd file.it represents login name and stores the same information in both files.
* Encrypted password: this field stores the user password that is encrypted using the SHA512 algorithm. This algorithm uses a random salt mixed with the original password before encryption. However, if two users use the same passwords, the resultant encrypted passwords will be different because of this encryption feature.
* Controlled Login: because Linux does not support blank passwords in its login process, any user or service that does not have a valid password or a blank password is not allowed to login.
* Date of last password change: this field keeps track of the number of days since user password was changed, in order to update the user on when next to change the password.
* Minimum required days between password change: this field records the last password change date and sets a minimum required number of days that must elapse until the next password change date. Similarly, if this field is s et to blank, a user can use a password for as long as possible.
* Number of days in advance to display password expiry notification. If the number of left to change password are equal to or less than the the days specified if this field, the user will get a warning notification to change password. This message will only be displayed when using command line.
* Number of days after password expiration: This is the number of days that can pass after the user's password has reached its maximum expiration date before the system disables the account. The user still has a second chance to change their password, even though it is technically expired.
* Account expiration date:This date is the end of the number of days after password expiration when the system will automatically disable the user's account. Once disabled, the user will be unable to login until an administrator enables it.
* Reserve: This field is ignored as it currently serves no purpose and is reserved for potential future use.

Check the content of the file /etc/login.defs, and explain the file.

This file contains configuration control definitions for the login package, three items must be clearly defined here and they include MAIL\_DIR, ENV\_SUPATH and ENV\_PATH.if unspecified, some arbitrary and sometimes correct value will be assumed. The others may be left unspecified. The MAIL\_DIR and MAIL\_FILE variables are used by useradd, usermod, and userdel to create, move, or delete the user's mail spool. ENV\_SUPATH which is of string datatype If set, will be used to define the PATH environment variable when the superuser logs in. The value is a colon separated list of paths (for example/sbin:/bin:/usr/sbin:/usr/bin) and can be preceded by PATH=. The default value is PATH=/sbin:/bin:/usr/sbin:/usr/bin…….

ENV\_PATH (string)If set, it will be used to define the PATH environment variable when a regular user login. The value is a colon separated list of paths (for example /bin:/usr/bin) and can be preceded by PATH=. The default value is PATH=/bin:/usr/bin……

Some other functions include:Password aging controls:

#

# PASS\_MAX\_DAYS Maximum number of days a password may be used.

# PASS\_MIN\_DAYS Minimum number of days allowed between password changes.

# PASS\_MIN\_LEN Minimum acceptable password length.

# PASS\_WARN\_AGE Number of days warning given before a password expires.

#

PASS\_MAX\_DAYS 99999

PASS\_MINDAYS 0

PASS\_WARN\_AGE 7

# Min/max values for automatic uid selection in useradd

#

UID\_MIN 1000

UID\_MAX 60000

# System accounts

SYS\_UID\_MIN 100

SYS\_UID\_MAX 999

#

# Min/max values for automatic gid selection in groupadd

#

GID\_MIN 1000

GID\_MAX 60000

# System accounts

SYS\_GID\_MIN 100

SYS\_GID\_MAX 999

LOGIN\_RETRIES 5

LOGIN\_TIMEOUT 60

CHFN\_RESTRICT rwh

DEFAULT\_HOME yess

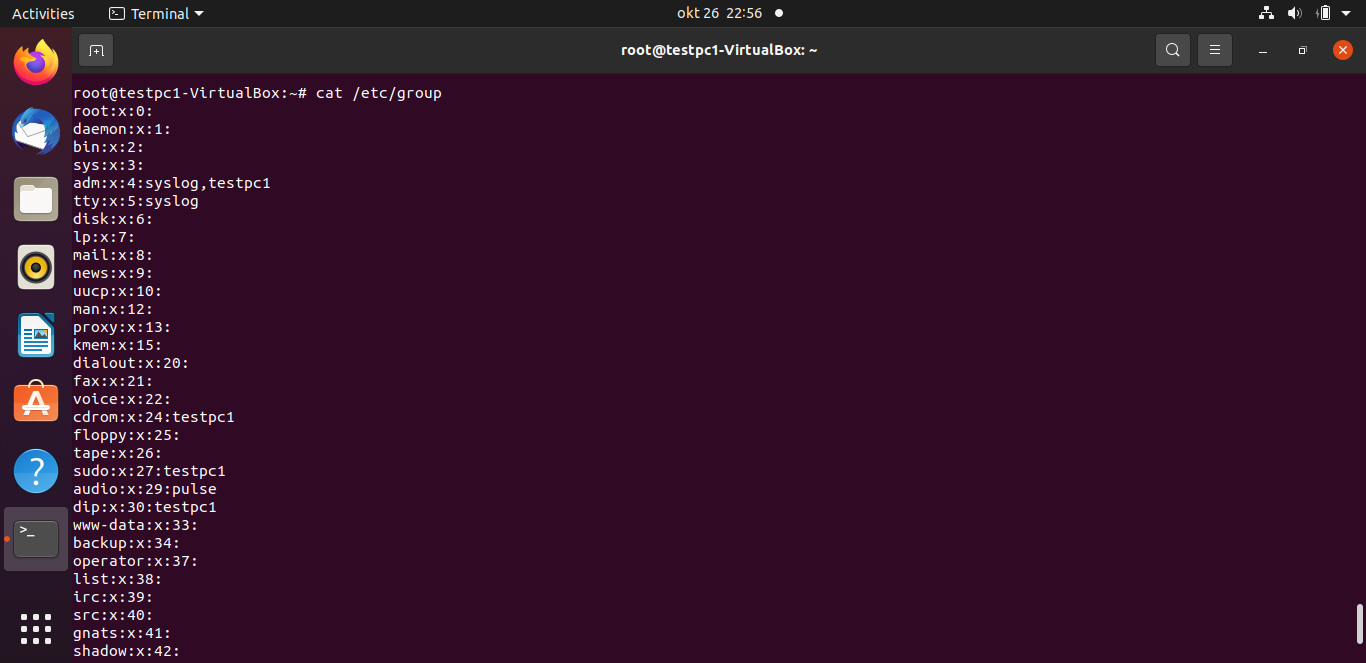
USERGROUP\_ENABLE yes

ENCRYPT\_METHOD SHA512.

Check the content of the file /etc/group, and explain the file, what do each line and

each field in a line mean?

The /etc/group is a text file which defines the default system group entries for system groups to which users belong to in the Linux and UNIX operating system. Each record appears on a single line and is a new group. Attributes of the group are separated by colon as seen below;

  
some groups include:

adm: used to monitor functions such as performance, cron and accounting.

Bin: used for system internal grouping

Uucp: this group manager the UUCP system

Mail: this group allows users to access the mail command.

Lp: allows users to access the lp command

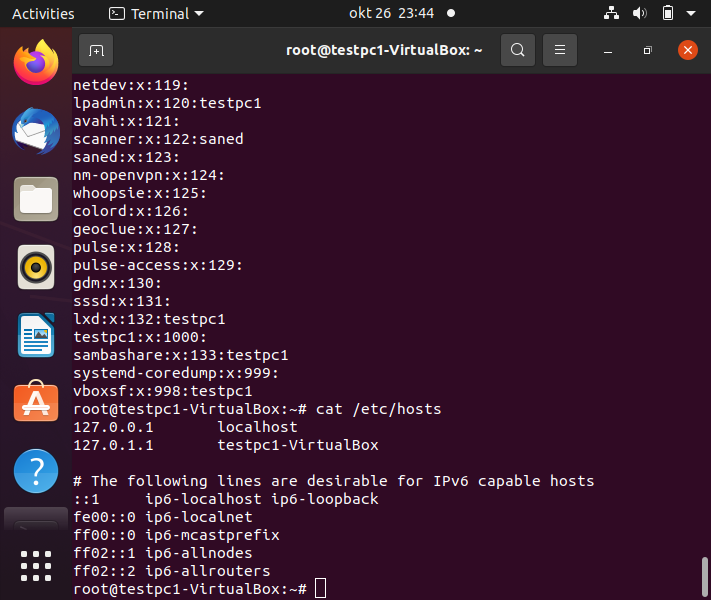
Tty: allows users access to serial and USB devices

Root: this group allows users access to all system functions.

Check the content of the file /etc/hosts, and explain the file, what do each line and

each field in a line mean?

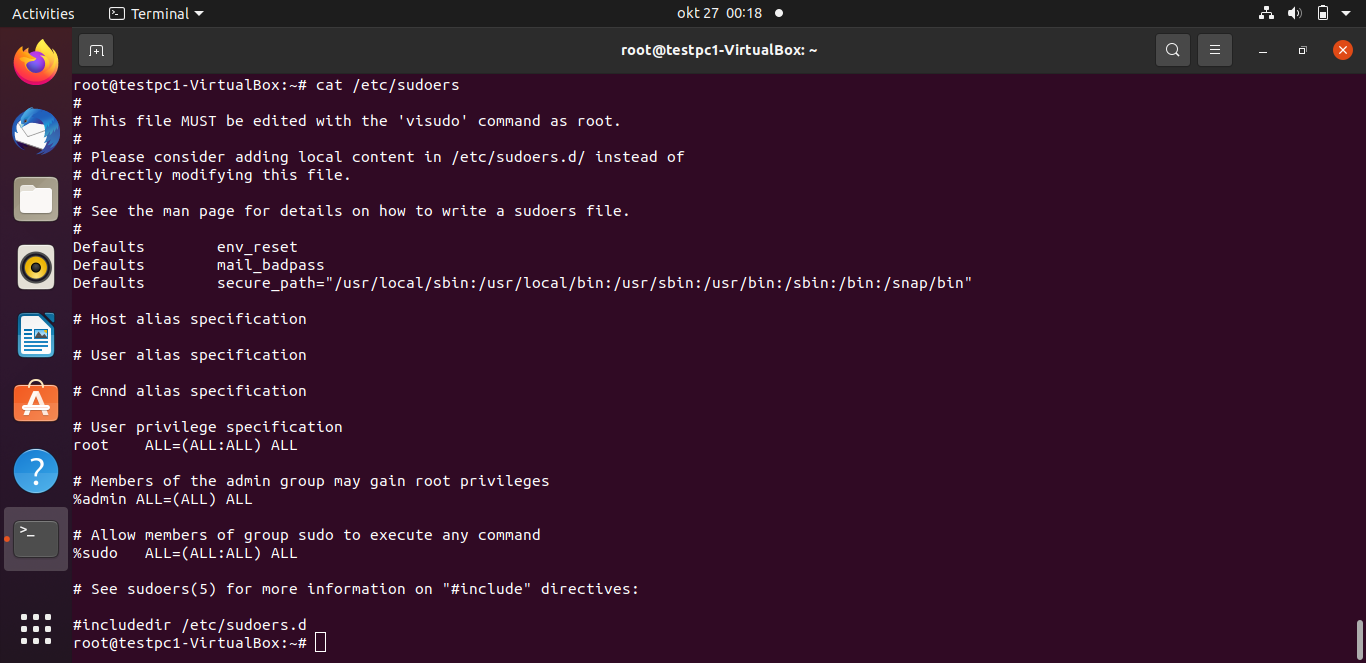
This is a simple text file that contains IP addresses to hostname mappings. Each line consists of an IP address, followed by one or more hostnames.



The above image shows the typical default content of the /etc/ hosts file that contains entries for the loopback addresses.

Check the content of the file /etc/sudoers, and explain the file.

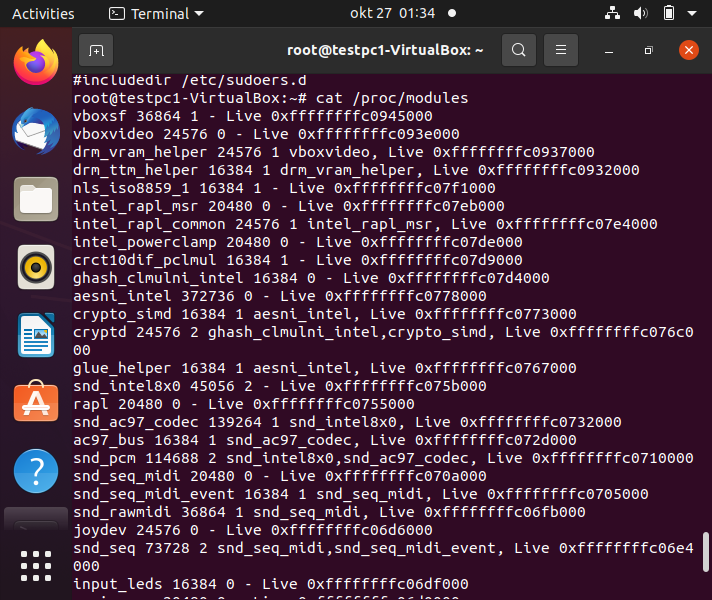
The**/etc/sudoers**file is what is used to determine if a user has permission to run commands that require elevated privileges.



The/etc/sudoers file should be edited only using the visudo command as root because improper editing of this file can remove the ability to run commands that require elevated privileges. Considerations should rather be on adding local content in /etc/sudoers.d/ instead of direct modification.

Check the content of the file /proc/modules, and explain the file.

This file displays a list of all modules loaded into the kernel.it consists of the module name, the memory size of the module, which is given in bytes, the number of instances of the module currently loaded onto the kernel, module dependencies if any, the load state the module is in which maybe live, loading or unloading and finally the current kernel memory offset.



Check the content of the file /etc/network/interfaces, and explain the file.

Check the content of the file /etc/securetty, and explain the file.

The /etc/securetty file allows you to specify which TTY devices the root user is allowed to login on. The /etc/securetty file is read by the login program usually /bin/login. Its format is a list of the tty devices names allowed, and for all others that are commented out or do not appear in this file, root login is disallowed. It is advisable to disable any tty not needed by commenting them out at the beginning of the line.

Check the content of the file /etc/security/time.conf, and explain the file.

The pam\_time module is used as an *account* module-type that does not accept arguments. It instead uses the /etc/securit*y/*time.conf file to get information related to login time and location restrictions. There are two important points concerning the */*etc/security*/*time.conf.

* If the */*etc/security file does not exist, there are no login restrictions related to login time or location.
* The limitations set by /etc/security apply to all users, including root.

Check the content of the file /etc/security/access.conf, and explain the file.

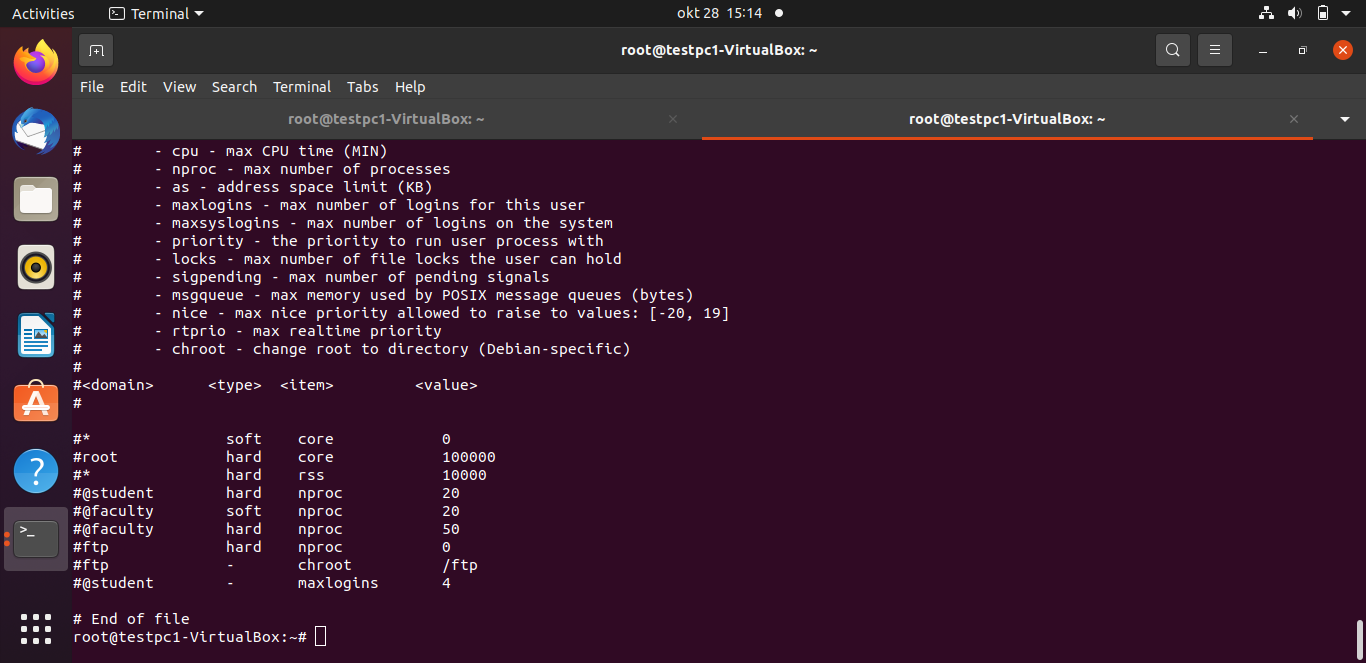
It is a login access configuration file that that is used to grant or deny access to users, groups, hosts, tty network etc. each line specifies a rule to allow or deny access. When someone logs in, the table is scanned for the first entry that matches the (user, host) combination, or, in case of non-networked logins, the first entry that matches the (user, tty) combination. The permissions field of that table entry determines whether the login will be accepted or refused.

Check the content of the file /etc/security/pam\_env.conf, and explain the file.

The /etc/security/pam\_env.conf file specifies the environment variables to be set, unset or modified by pam\_env. When someone logs in, this file is read and the environment variables are set accordingly. Each line starts with the variable name, there are then two possible options for each variable DEFAULT and OVERRIDE. DEFAULT allows and administrator to set the value of the variable to some default value, if none is supplied then the empty string is assumed. The OVERRIDE option tells pam\_env that it should enter in its value (overriding the default value) if there is one to use. OVERRIDE is not used, "" is assumed and no override will be done.

Check the content of the file /etc/security/limits.conf, and explain the file.

The /etc/security/limits.conf,file describes the  limit the amount of various system resources available to a user process. Each line describes a limit for a user in the form of domain, type, item and value. These limitations include how many files a process can have open, the size of a file the user can create, and how much memory can be used by the different components of the process such as the stack, data and text segments.

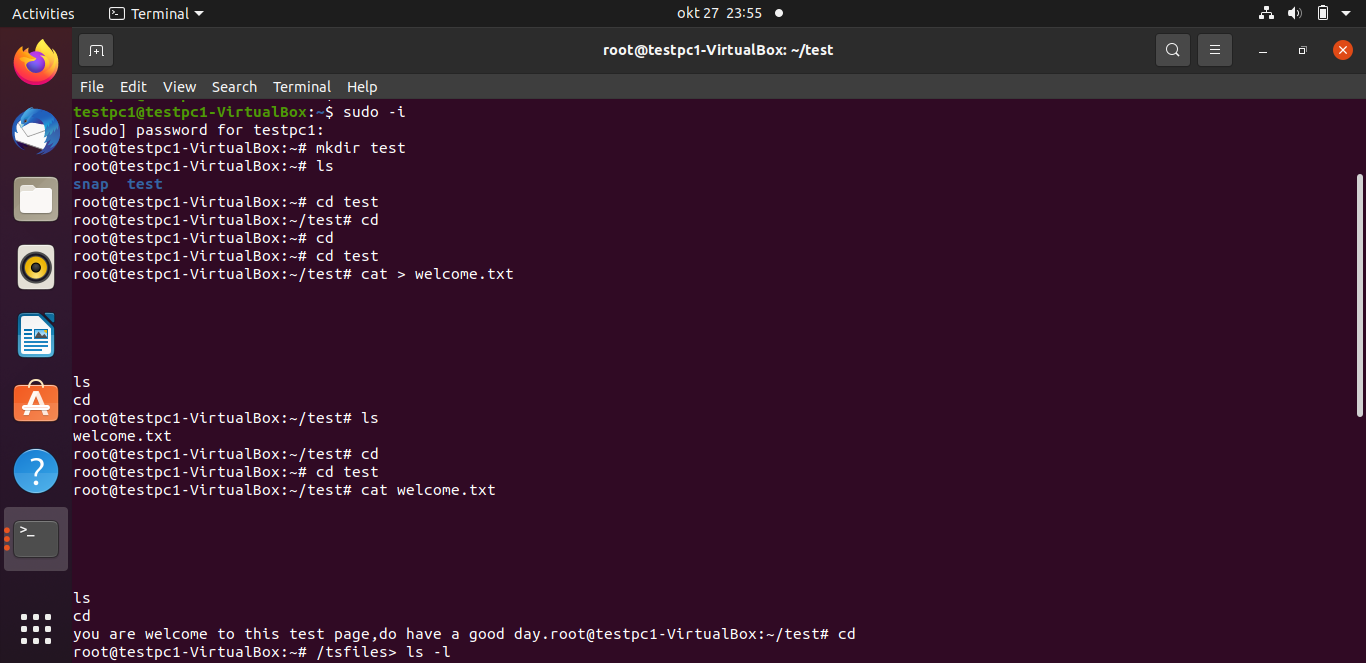


4. What is grub:  grub is a multiboot loading and managing program that manages the boot process. It is the most common bootloader for Linux distributions. A bootloader is the first software that runs when a computer starts. It loads the kernel of the operating system and then the kernel initializes the rest of the operating system: shell, display manager, desktop environment, etc. there is no need to specify the physical location of the Linux kernel for GRUB. It only required the hard disk number, the partition number and file name of the kernel and can boot almost any operation system using the direct and chain boot loading method.

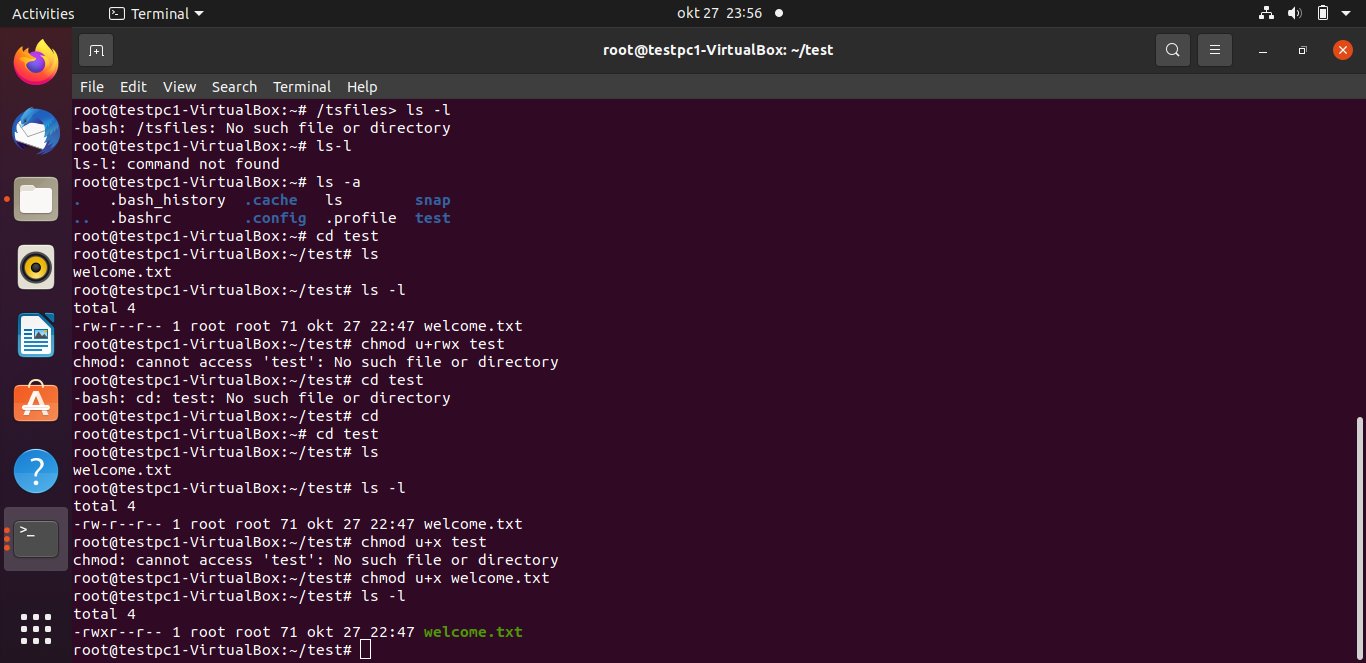
How to change the boot order of different operating systems on the same machine, in a few steps

* Open a Terminal window
* Fine the entry number of other operating system type cat /boot/grub/grub.cfg| grep menuentry
* Edit the default grub file /etc/default/grub type sudo vi/etc/default/grub(change the GRUB\_DEFAULT from 0 to the number of the intended operating system )
* Update the changes in the boot loader Type: sudo update-grub.

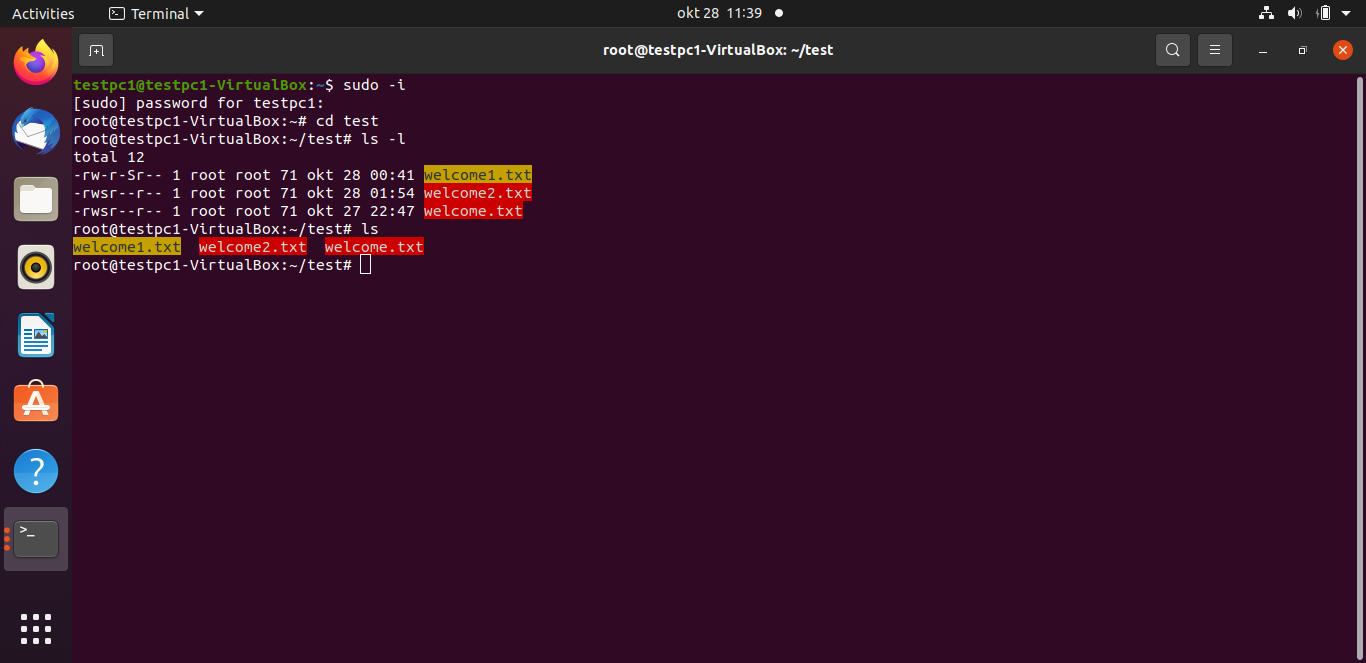
5. Create a subdirectory in your home directory and put a file welcome.txt with a short message in this subdirectory. Set the permission bits on the subdirectory so that the owner has ‘execute’ access



The test subdirectory has been created and welcome.txt file put in it.

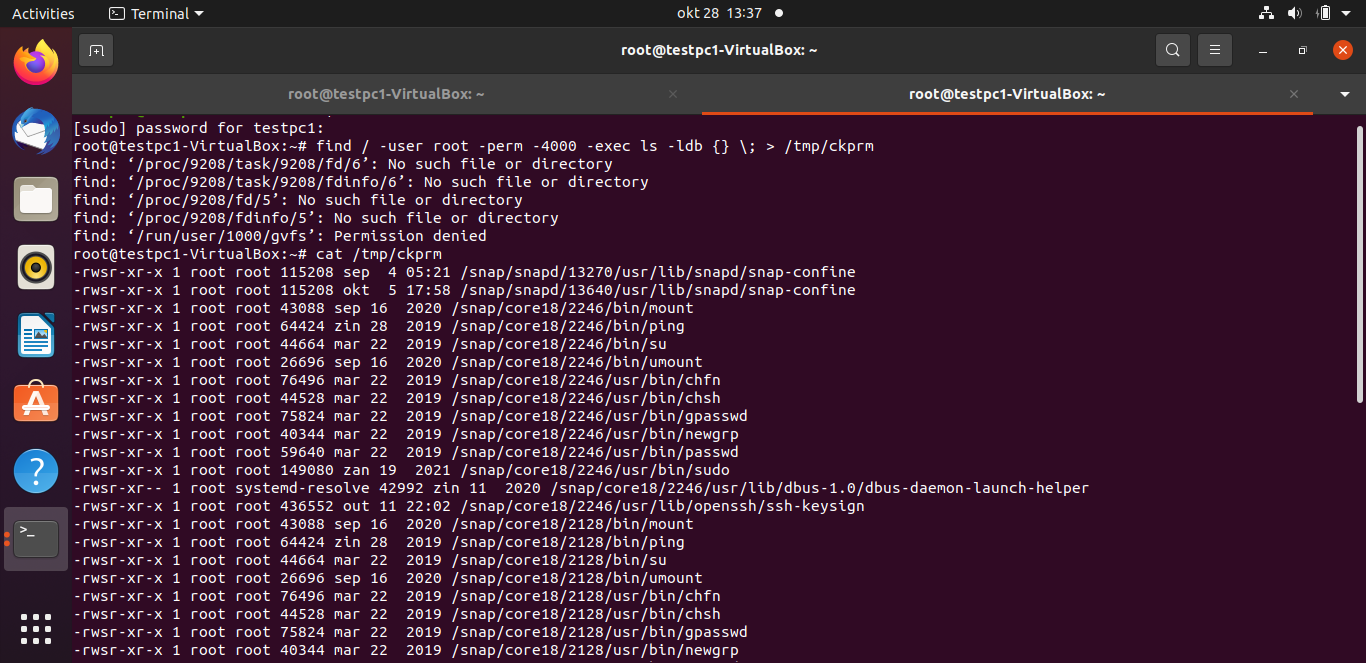


In the above image, “ test”subdirectory was created and a file welcome .txt put inside it. Its default permissions are rw for users, r for groups and r for others. These permissions re later changed to reflect rwx for users, r for groups and r for others.



Futher experiments with permissions as seen above shows that the user of welcome1.txt was assigned “write”permission and the group has setgid privilege.

The user of welcome 2.txt has read, write permission and setuid privileges. also, the user of welcome .txt has read, write permission and setuid privileges.

Display all files with suid permission set.

At the beginning of this lab we started by getting familiar with the linux system by trying out experimenting on the usage of some linux commands with which outcomes are recorded herein, we moved further into the use of terminal and commands to check , display and explain the features of some files and folders and certain functions that can be performed on them.