TEC | Tecnológico de Costa Rica

Instituto Tecnológico de Costa Rica
Área Académica de Ingeniería en Computadores
CE 4303 — Principios de Sistemas Operativos

# Laboratorio 4
## Administración y Seguridad de la información

| | | | |
|---|---|---|---|
| Fecha de asignación: | 23 de Mayo, 2025 | Fecha de entrega: | 6 de Junio, 2025 |
| Grupos: | Individual | Profesor: | Jason Leitón, Leonardo Araya |

## 1. Objetivos

- Comprender los conceptos relacionados con la administración de la información de una manera práctia, bajo un ambiente de Linux.
- Analizar los conceptos de seguridad de una manera práctica utilizando un Sistema Operativo de Linux.

## 2. Indicaciones

1. Para el siguiente laboratorio deberá ejecutar los pasos que se detallan en cada uno de los apartados, comprobando su ejecución con capturas de pantalla en el resultado del mismo. Esta información deberá estar en un documento PDF para cargarlo en Tecdigital según corresponda.
2. Se debe de realizar la guía de preguntas y adjuntar las soluciones junto con enunciados en el mismo documento del punto anterior.
3. La fecha de entrega será la indicada en este documento y debe ser de manera individual.
4. En caso de que el laboratorio necesite código fuente, este también debe de incorporarse como parte de la solución del mismo, ya que será evaluado.
5. El laboratorio debe ser revisado por el profesor antes de la fecha de cargar los archivos, por lo que el estudiante será el encargado de mostrar su trabajo, en caso de que no lo haga la nota será cero.

## 3. Preguntas guía

1. Investigue para que se utiliza los comandos: useradd, userdel, passwd, así como los diferentes ID de usuarios.
2. ¿Qué son grupos primarios y grupos secundarios en Linux?

3. Realice un cuadro comparativo entre Inode y ACL.

4. Investigue el comando para cambiar permisos a un archivo. Coloque los métodos por medio de letras y de números.

5. ¿Qué es la tabla de particiones NTFS y EXT32? ¿Cuál es su funcionamiento?

# 4. Creación de Usuarios

Para la siguiente sección se debe tomar captura de cada paso que se ejecuta.

1. Cree una máquina virtual nueva con el sistema operativo Centos. Los comandos pueden variar de una versión a otra, sin embargo, puede modificarlos en caso de que sea necesario. Observe que los comandos que inician con # es porque debe hacerlo con usuario privilegiado (sudo).

2. Conéctese por medio de ssh a la máquina recien creada.

3. Agregue tres diferentes usuarios con contraseñas diferentes. Utilice el comando *# useradd < name >* y *# echo < password1 > — passwd –stdin < username1 >* .

4. Confirme que cada usuarios se creó realizando los siguientes comandos. Note las diferencias en las salidas de datos.

   - *# id < username >*
   - *# yum install finger -y*
   - *# finger < username >*
   - *# cat /etc/passwd — grep < username >*

5. Cree los grupos y usuarios que se muestran en la siguiente tabla. Utilice los comandos: *# groupadd < groupname >* y *# usermod -aG < groupname >< username >*

| Grupo | Nombre de Grupo | Lista de usuario |
|---|---|---|
| Profesores | Professors | Jason, Luis, Diego |
| Asistentes | Assistents | Josué, Viviana, Steven |
| Estudiantes | Students | Pedro, Juan, Harold |

6. Valide que se hayan creado los grupos de usuario y sus respectivas listas. Además verifique la ruta */etc/groupfile*. Ejecute los siguientes comandos: *# id < username >* y *# cat /etc/group — grep < username >*

# 5. Permisos

En esta sección se presentarán algunos comandos para establecer, verificar y cambiar los permisos de un archivo y directorio. De igual manera que el anterior debe aportar el screenshot para cada paso.

## 5.1. Archivos

1. Ejecute los comandos: *$ touch /tmp/test* y *$ ls -l /tmp/test*. Explique la función de cada uno de ellos, así como el resultado de de la ejecución. Muestre un screenshot. Debe explicar cada parte del resultado.

2. Ejecute, y explique el resultado de los siguientes comandos.

   - *$ chmod o+w /tmp/test*.
   - *$ chmod 666 /tmp/test*.
   - *$ chmod a-rwx /tmp/test*.
   - *$ cat /tmp/test* .
   - *$ chmod u+rw /tmp/test*.

## 5.2. Directorios

1. Cree un directorio con el siguiente comando: *$ mkdir -p /tmp/mydirectory/mydir2*.

2. Ejecute los siguientes comandos: *$ ls -l /tmp/mydirectory* y *$ ls -ld /tmp/mydirectory*. Describa el resultado que se muestra en consola.

3. Si no permite que otros tengan permiso de ejecución en el directorio /tmp/mydirectory, no importa quién tenga acceso de lectura o escritura. Nadie puede acceder al directorio a menos que conozca el nombre exacto del archivo. Con el siguiente comando eliminas la ejecución de todos: *$ chmod a-x /tmp/mydirectory*.

4. ¿Qué ocurre si ejecuta el comando: *cd /tmp/mydirectory* ?

5. Restaure el acceso al directorio con el comando: *$ chmod ug+x /tmp/mydirectory*.

6. Verifique que otros no tengan permiso de acceso con el comando: *ls -ld /tmp/mydirectory*

7. Realice un archivo y un directorio, asigne, modifique y elimine permisos con representación numérica.

# 6. Lista de Control de Acceso

En esta sección se debe ejecutar los comandos y mostrar un screenshot de la consola con el resultado de los mismos.

1. Investigue el uso de los comandos: *getfacl* y *setfacl*. Muestre las diferentes sintaxis de uso.
2. Trate de editar el archivo */etc/motd*. Probablemente el un usuario no pueda editar y solo podrá leerlo. Ejecute el comando: *$ vim /etc/motd* (Note que el comando no se está ejecutando como root).
3. Utilice el comando *setfacl* (punto 1, por ejemplo setfacl -m d:u:rootadmin:rw /etc/motd) y agregue una ACL que garantice que un usuario que no sea root pueda leer y escribir el archivo */etc/motd*.
4. Ejecute el comando *getfacl /etc/motd*, verifique si la ACL que agregó en el punto anterior está correcta.
5. Como usuario no privilegiado (no root), ejecute el siguiente comando: *$ echo 'Welcome from rootadmin!' >> /etc/motd*.
6. Utilice otra terminal y conéctese por ssh a la máquina virtual, ¿Qué ocurre con respecto al inicio ordinario?
7. Como root, cree el directorio *mkdir /var/tmp/collab*.
8. Muestre las ACL. *getfacl /var/tmp/collab*
9. Cree una ACL que permita que un usuario no root pueda leer y escribir todos los archivos creados bajo el directorio de */var/tmp/collab*. Para esto ejecute el comando: *# setfacl -m d:u:rootadmin:rw /var/tmp/collab*.
10. Verifique la nueva ACL. *getfacl /var/tmp/collab*.
11. Ahora debe crear un archivo en el directorio creado llamado */var/tmp/collab/rootfile*. Ejecute el comando: *# echo rootfile contents > /var/tmp/collab/rootfile*.
12. Verifique el contenido con *cat /var/tmp/collab/rootfile*
13. Verifique la ACL del archivo. *getfacl /var/tmp/collab/rootfile*.
14. Ahora como usuario no root agregue una línea de texto en el archivo. Ejecute el comando *$ echo 'rootadmin was here' >> /var/tmp/collab/rootfile*
15. Verifique el contenido. *# cat /var/tmp/collab/rootfile*.

# 7. Práctica

Realice con líneas de comando la estructura de usuarios, ACL y archivos que muesta la figura 1.

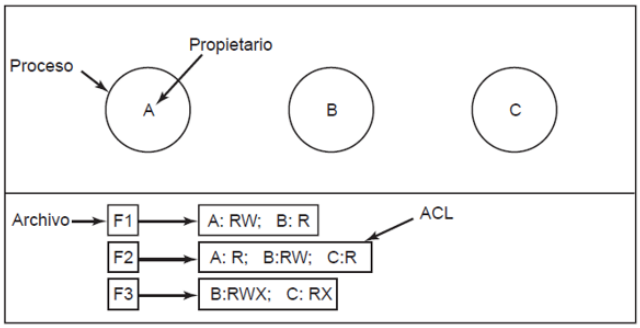


Figura 1: Estructura a realizar

# 8. Entregable

Documento con todas las capturas de pantallas que muestren la ejecución del taller.