

Sistemas Informáticos

Unidad 05. Actividades no evaluables 03 - Soluciones



Autores: Sergi García, Alfredo Oltra

Actualizado Septiembre 2025



UNIDAD 05. ACTIVIDADES 03 - SOLUCIONES (ACTIVIDADES 04, 06 Y 07)

1. SOLUCIÓN EJERCICIO 04

1. Mostrar todas las líneas del fichero list.txt que contienen el texto lib.

```
grep "lib" list.txt
```

Explicación:

- grep busca cadenas de texto dentro de archivos.
- "lib" es el patrón que se busca.
- list.txt es el fichero donde se realiza la búsqueda.

➡ Muestra todas las líneas de list.txt que contienen la secuencia de caracteres lib (por ejemplo, library, glibc, etc.).

2. Mostrar cuántas líneas contienen mp3 en list.txt.

```
grep mp3 list.txt | wc -l
```

Explicación:

- grep mp3 list.txt encuentra todas las líneas que contienen la cadena mp3.
- La tubería (|) pasa la salida al siguiente comando.
- wc -l cuenta el número de líneas.

➡ Resultado: devuelve un número indicando cuántas líneas contienen mp3.

3. Mostrar ficheros dentro del directorio /etc/ que contienen la cadena host.

```
grep -r host /etc
```

Explicación:

- -r significa búsqueda recursiva: se buscan coincidencias en todos los ficheros dentro de /etc/.
- host es el patrón buscado.
- /etc es el directorio donde se busca.

➡ Muestra todas las líneas que contienen host dentro de los ficheros de /etc/. Incluye además el nombre del fichero al inicio de cada línea.

4. Mostrar todas las líneas del fichero list.txt que no contienen la letra a (mayúscula o minúscula).

👉 El comando que pusiste (grep -vi *a* list.txt) no es correcto. El correcto es:

```
grep -vi "a" list.txt
```


Explicación:

- -v invierte el resultado: muestra solo las líneas que no coinciden con el patrón.
- -i hace la búsqueda insensible a mayúsculas/minúsculas.
- "a" es el carácter a buscar.


➡ Resultado: todas las líneas que no contienen la letra a ni A.

5. Mostrar todas las líneas del fichero list.txt que no contienen a (mayúscula o minúscula) y contienen m (minúscula).

```
grep -vi "a" list.txt | grep "m"
```

 Explicación:

1. `grep -vi "a" list.txt` → selecciona solo las líneas que no contienen a ni A.
2. `| grep "m"` → de esas líneas, muestra solo las que contienen la letra m minúscula.

 Resultado: líneas de list.txt sin a (mayúscula o minúscula) y con m

2. SOLUCIÓN EJERCICIO 06

Contexto: suponiendo que temporalmente (por ejemplo 1 hora) tienes acceso como `root` en una máquina y en esa máquina existe permanentemente un usuario llamado `alumno` sin permisos en `sudoers`.

Pregunta 01: ¿Cómo podemos usar el bit SetUID para crear una puerta trasera (backdoor)? (Pista: el fichero `/bin/sh` puede ser útil).

Solución (como root):

```
cd $HOME
cp /bin/sh ./
chown root ./sh
chmod 4777 ./sh
```

Ahora hemos creado la puerta trasera.

Como usuario:

Ejecutar simplemente `./sh` en tu directorio home y serás `root` (puedes comprobarlo con `id`).

Pregunta 02: ¿Cómo detectar este tipo de puertas traseras en el sistema? ¿Qué medidas tomar para estar protegidos?

Solución: Usar:

```
find / -path /proc -prune -o -type f -perm +4000 -ls > listado.txt
```

Esto obtiene todos los ficheros con el bit SetUID activo. Si la lista cambia, puede haberse creado un nuevo archivo con SetUID. Además, se puede usar software de integridad del sistema como:

<http://www.ossec.net/>

3. SOLUCIÓN EJERCICIO 07

Los comandos que cambian usuarios/grupos o montan sistemas de ficheros requieren sudo. Ejecuta como usuario con privilegios o precede con sudo cuando haga falta.

1) Crear directorio

```
mkdir ~/proyecto_acl  
cd ~/proyecto_acl
```

2) Crear usuarios y grupo (si no existen) y añadir al grupo

```
# crea el grupo  
sudo groupadd equipo
```

```
# crea usuarios (si ya existen, saltará error; en ese caso omitir)  
sudo useradd -m ana  
sudo useradd -m luis
```

```
# asigna contraseña (opcional para pruebas)  
sudo passwd ana  
sudo passwd luis
```

```
# añade usuarios al grupo 'equipo'  
sudo usermod -aG equipo ana  
sudo usermod -aG equipo luis
```

3) Crear el fichero informe.txt

```
echo "Informe inicial - prueba ACL" > informe.txt
```

4) Asignar ACLs solicitadas

Dar permisos a ana (lectura+escritura) sobre informe.txt:

```
setfacl -m u:ana:rw informe.txt
```

Dar permisos al grupo equipo (solo lectura) sobre informe.txt:

```
setfacl -m g:equipo:r-- informe.txt
```

Explicación: -m = modificar; u:ana:rw significa usuario ana con permisos read+write; g:equipo:r-- grupo equipo con lectura.

5) Ver las ACL aplicadas

```
getfacl informe.txt
```

Salida esperada (ejemplo):

```
# file: informe.txt
# owner: tuusuario
# group: tugrupo
user::rw-
user:ana:rw-
group::r--
group:equipo:r--
mask::rw-
other::r--
```

- user:: son permisos del propietario.
- user:ana: entrada ACL para ana.
- group:equipo: entrada ACL para el grupo equipo.
- mask limita los permisos efectivos para entradas no propias del propietario.

6) Configurar ACL por defecto en el directorio (herencia)

Para que nuevos ficheros en proyecto_acl hereden permisos, establece ACL por defecto en el directorio:

Dar permisos por defecto: propietario rwx, grupo equipo rw, otros ---:

permiso por defecto para el propietario

```
setfacl -m d:u::rwx ~/proyecto_acl
```

permiso por defecto para el grupo 'equipo'

```
setfacl -m d:g:equipo:rw ~/proyecto_acl
```

permiso por defecto para otros: ninguno

```
setfacl -m d:o:--- ~/proyecto_acl
```

También puedes hacerlo en una única línea:

```
setfacl -m d:u::rwx,d:g:equipo:rw,d:o:--- ~/proyecto_acl
```

d: indica que es default (por defecto / heredada).

7) Crear nuevo.txt y comprobar que hereda ACL

```
touch nuevo.txt
```

```
getfacl nuevo.txt
```

Salida esperada (ejemplo):

```
# file: nuevo.txt
# owner: tuusuario
# group: yourgroup
user::rwx
```

```
group::rw-  
group:equipo:rw-  
mask::rw-  
other::---
```

Verás que además de los permisos del propietario, aparece `group:equipo:rw-` heredado del `d:g:equipo:rw`.

8) Eliminar ACLs (limpiar)

- Eliminar la entrada ACL específica de ana:

```
setfacl -x u:ana informe.txt
```

- Eliminar todas las ACLs de un archivo (dejar solo permisos POSIX clásicos):

```
setfacl -b informe.txt
```

- Eliminar ACLs por defecto de un directorio:

```
setfacl -k ~/proyecto_acl # elimina entradas por defecto  
# o eliminar todo:  
setfacl -b ~/proyecto_acl
```

9) Comprobar eliminación

```
getfacl informe.txt  
getfacl nuevo.txt  
getfacl ~/proyecto_acl
```

Deberías ver que ya no aparecen las entradas `user:ana:` ni `group:equipo:` si las has eliminado.