SEGURIDAD LOGICA

ASIR V2

MODULO SAD

Alberto Resa Pérez

**INDICE**

[1. Objetivos. 2](#_Toc500435145)

[2. Desarrollo. 3](#_Toc500435146)

[Ejercicios 2 3](#_Toc500435147)

[Ejercicio 8 5](#_Toc500435148)

[3. Bibliografía. 7](#_Toc500435149)

# Objetivos.

Para esta práctica tenemos 2 objetivos.

El primero objetivo es descifrar la contraseña de 2 usuarios que se nos proporcionan. Después investigaremos sobre el código encriptado que se nos da y el significado de las diferentes partes.

El siguiente objetivo será ver las diferencias entre el comando chmod y el setfacl, para ello realizaremos las pruebas con los 2 comandos para ver claramente su funcionamiento.

# Desarrollo.

## Ejercicios 2

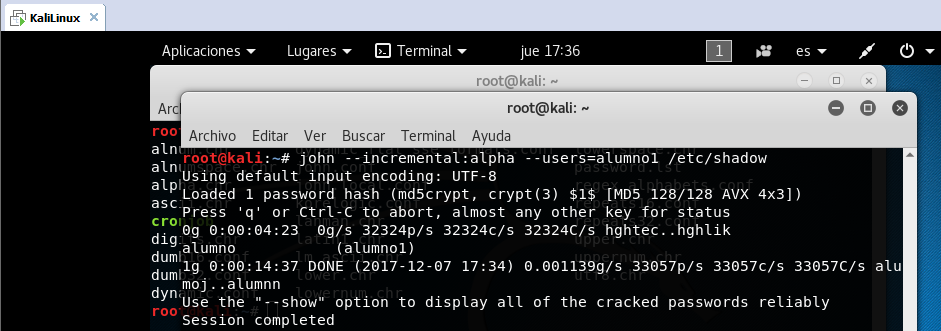
alumno1:$1$zmDCo$pP/Rrln2jTy3OeTvjL8Mg0:14544:0:99999:7:::

root:$1$bM36INXG$nlckzvSVJy.z42Atf5p6n.:11585:0:99999:7:::

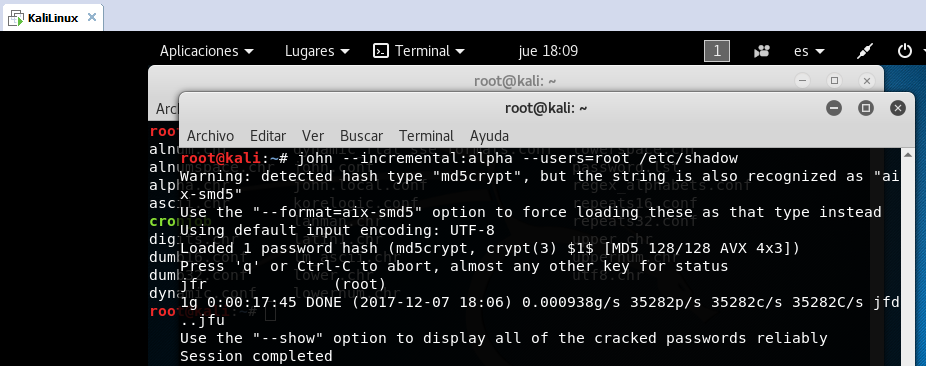
¿Qué contraseña poseen los usuarios: root y alumno1?

¿En qué tiempo has sido capaz de descifrar las contraseñas?

Para el usuario alumno1 hemos descifrado la contraseña que es alumno utilizando la fuerza bruta pero usando solo letras minúsculas. El tiempo necesario para descubrir la contraseña ha sido de 5 minutos.



El mismo proceso hemos utilizado para descifrar al root cuya contraseña es de jfr. El proceso de descifrado ha sido de 17 minutos.



¿Qué algoritmo de cifrado poseen sus contraseñas?

El algoritmo de cifrado es MD5 el cual nos identifica nada más iniciar el proceso de des encriptación.

¿Qué significado poseen cada uno de los campos que componen cada línea del archivo?

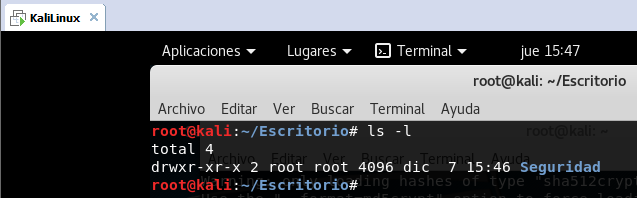
* $1$. Tipo de encriptación MD5.
* 11585. Número de días que lleva la contraseña sin cambiar.
* 0. Número de días que debe pasar antes de cambiar la contraseña.
* 99999. Número de días que pasaran antes de que caduque la contraseña.
* 7. Número de días de antelación con los que avisara antes de que caduque la contraseña.

## Ejercicio 8

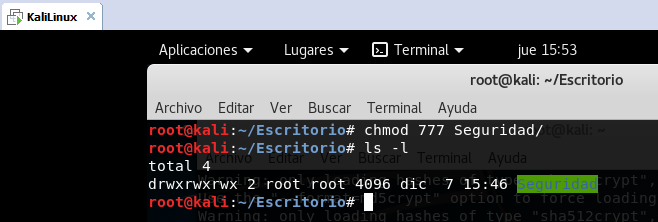
Explica las diferencias existentes en sistemas GNU/Linux entre el uso del comando chmod y setacl.

* Chmod. Este comando se utiliza para configurar los permisos de lectura, escritura y ejecución que tiene el usuario propietario, grupo propietario y el resto de usuarios sobre un archivo o directorio.

Como vemos en la imagen el directorio seguridad tiene como usuario y grupo propietario a root y para estos tiene los permisos rwx que corresponden a lectura, escritura y ejecución para el usuario root, después tiene los permisos r-x que corresponden a lectura y ejecución para los usuarios del grupo root y para otros usuarios.

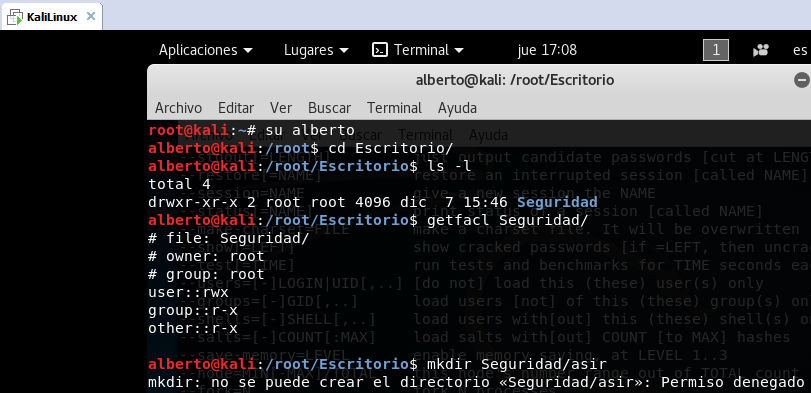


Como podemos ver hemos modificado los permisos y ahora son de lectura, escritura y ejecución para todos los usuarios, tanto para el propietario como para cualquier usuario.



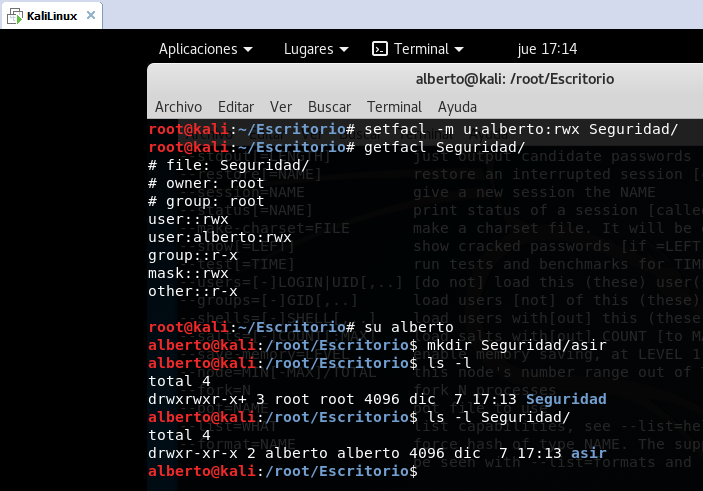
* Setfacl. Este comando da los permisos de escritura, lectura y ejecución sobre un archivo o directorio para unos usuarios o grupos específicos además del usuario y grupo propietario.

En este ejemplo podemos ver que el usuario Alberto no tiene permisos para escribir en el directorio de seguridad y por lo tanto no puede crear un nuevo directorio. Como también vemos en la imagen no está dentro de los permisos pro acl, realizamos la prueba de crear un nuevo directorio dentro de Seguridad y nos da error.



Ahora usamos el comando setfacl para para dar permisos de lectura, escritura y ejecución sobre el directorio Seguridad. Después volvemos a intentar a crear el directorio desde ese usuario y podemos ver como ahora si podemos crear el directorio.

Los directorios que tienen permisos por acl se pueden identificar por un + después de los permisos que se ven al realizar ls –l sobre un directorio.



# Bibliografía.

**Software.**

* 1. VMWare Workstation Pro 12.
  2. Máquina virtual con Kali Linux.
  3. John de Ripper Kali Linux.

**Documentación.**

* 1. Diferentes pdf entregados en clase.
  2. Diferentes webs.