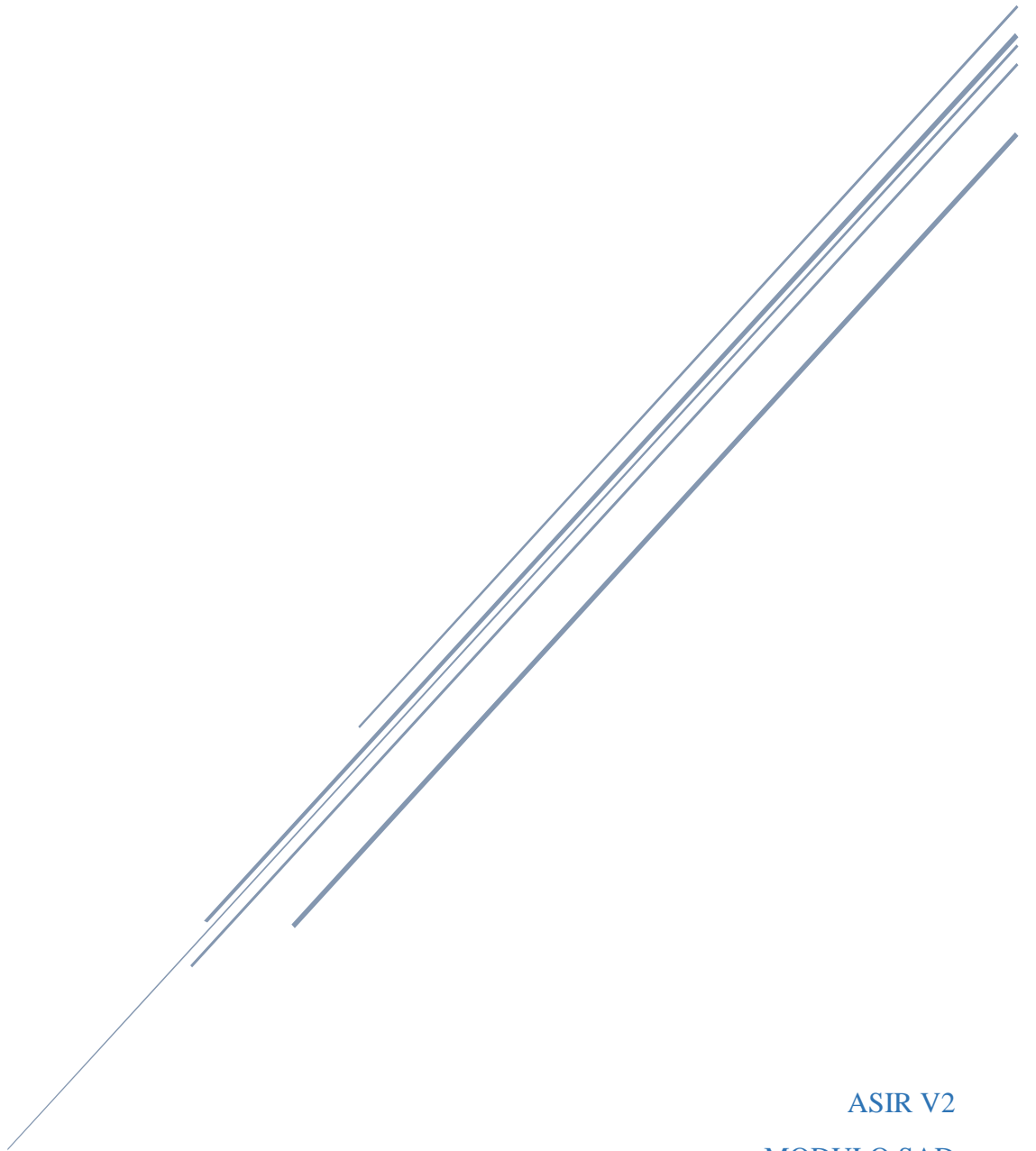


SEGURIDAD LOGICA



ASIR V2
MODULO SAD
Alberto Resa Pérez

INDICE

1. Objetivos.....	2
2. Desarrollo.....	3
Ejercicios 2.....	3
Ejercicio 8	5
3. Bibliografía.....	7

1. 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.

2. Desarrollo.

Ejercicios 2

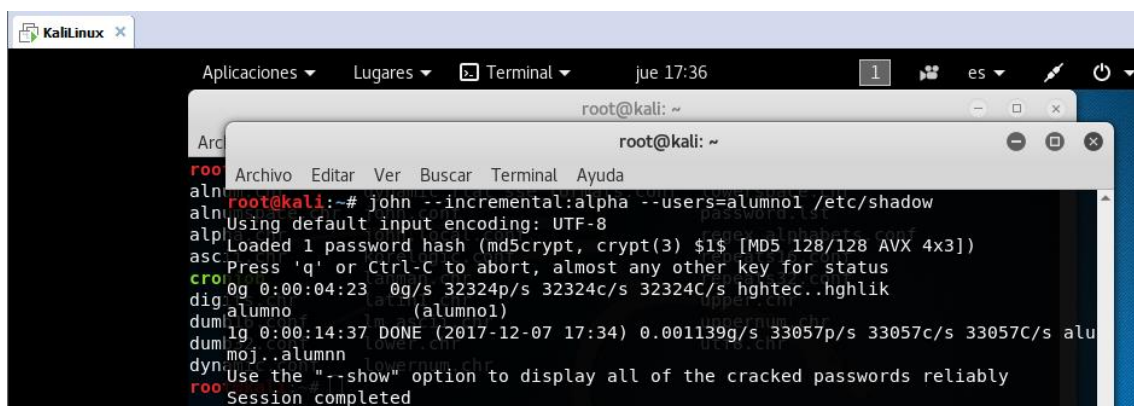
alumno1:\$1\$zmDCo\$pP/Rrln2jTy3OeTvjl8Mg0:14544:0:99999:7:::

root:\$1\$bM36lNXG\$nIckzvSVJy.z42Atf5p6n.:11585:0:99999:7:::

¿Qué contraseña poseen los usuarios: root y alumno1?

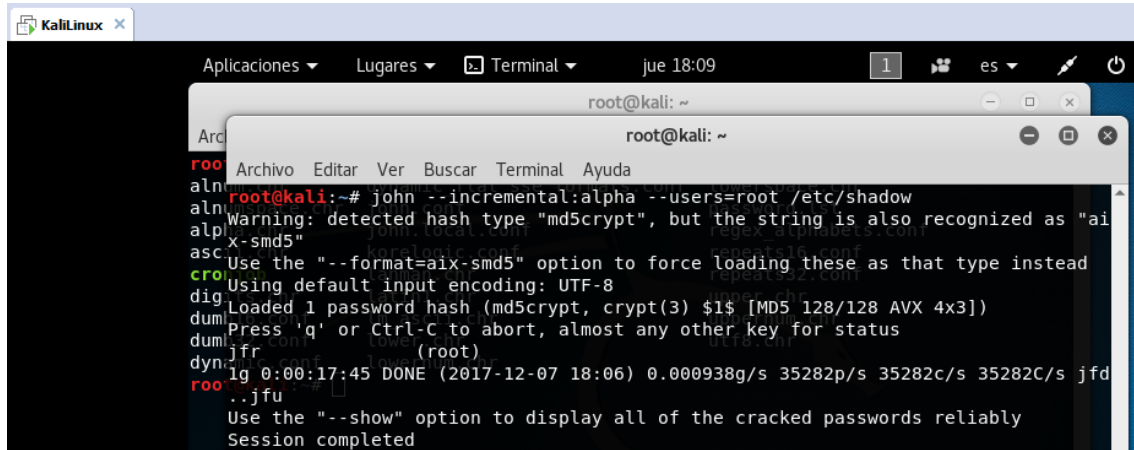
¿En qué tiempo has sido capaz de descifrar las contraseñas?

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.



```
root@kali: ~  
root@kali:~# john --incremental:alpha --users=alumno1 /etc/shadow  
Using default input encoding: UTF-8  
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
0g 0:00:04:23 0g/s 32324p/s 32324c/s 32324C/s hghtec..hghlik  
dig alumno (alumno1)  
dumlg 0:00:14:37 DONE (2017-12-07 17:34) 0.001139g/s 33057p/s 33057c/s 33057C/s alu  
dummoj..alumn  
dyn Use the "--show" option to display all of the cracked passwords reliably  
root Session completed
```

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



```
root@kali: ~  
root@kali:~# john --incremental:alpha --users=root /etc/shadow  
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-smd5"  
Use the "--format=aix-smd5" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 AVX 4x3])  
Press 'q' or Ctrl-C to abort, almost any other key for status  
jfr (root)  
lg 0:00:17:45 DONE (2017-12-07 18:06) 0.000938g/s 35282p/s 35282c/s 35282C/s jfr  
root@kali:~#  
..jfr  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed
```

¿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?

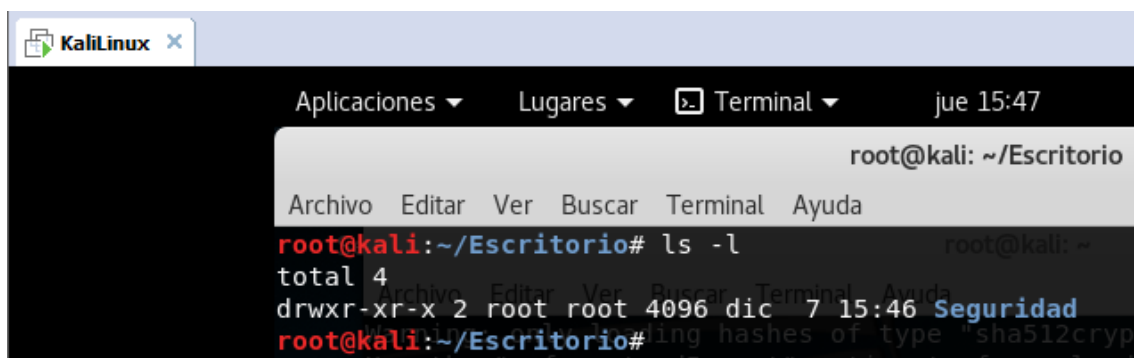
- \$1\$. Tipo de encriptación MD5.
- 11585. Número de días que lleva la contraseña sin cambiar.
- 0. Número de días que debe pasar antes de cambiar la contraseña.
- 99999. Número de días que pasaran antes de que caduque la contraseña.
- 7. Número de días de antelación con los que avisara antes de que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

Ejercicio 8

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

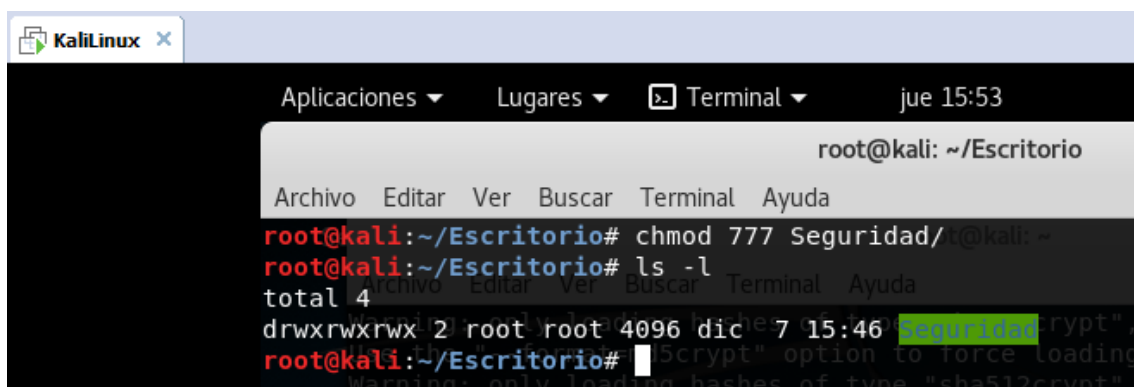
- `Chmod`. Este comando se utiliza para configurar los permisos de lectura, escritura y ejecución que tiene el usuario propietario, grupo propietario y el resto de usuarios sobre un archivo o directorio.

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.



```
KaliLinux x
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 15:47
root@kali: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~/Escritorio# ls -l
total 4
drwxr-xr-x 2 root root 4096 dic 7 15:46 Seguridad
root@kali:~/Escritorio#
```

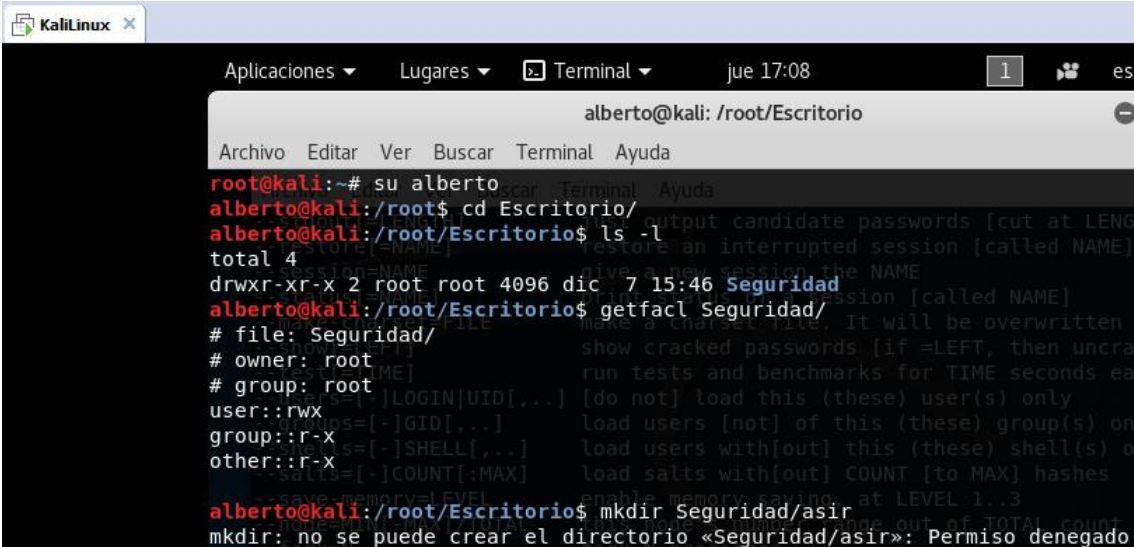
Como podemos ver hemos modificado los permisos y ahora son de lectura, escritura y ejecución para todos los usuarios, tanto para el propietario como para cualquier usuario.



```
KaliLinux x
Aplicaciones ▾ Lugares ▾ Terminal ▾ jue 15:53
root@kali: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~/Escritorio# chmod 777 Seguridad/
root@kali:~/Escritorio# ls -l
total 4
drwxrwxrwx 2 root root 4096 dic 7 15:46 Seguridad
root@kali:~/Escritorio#
```

- 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.

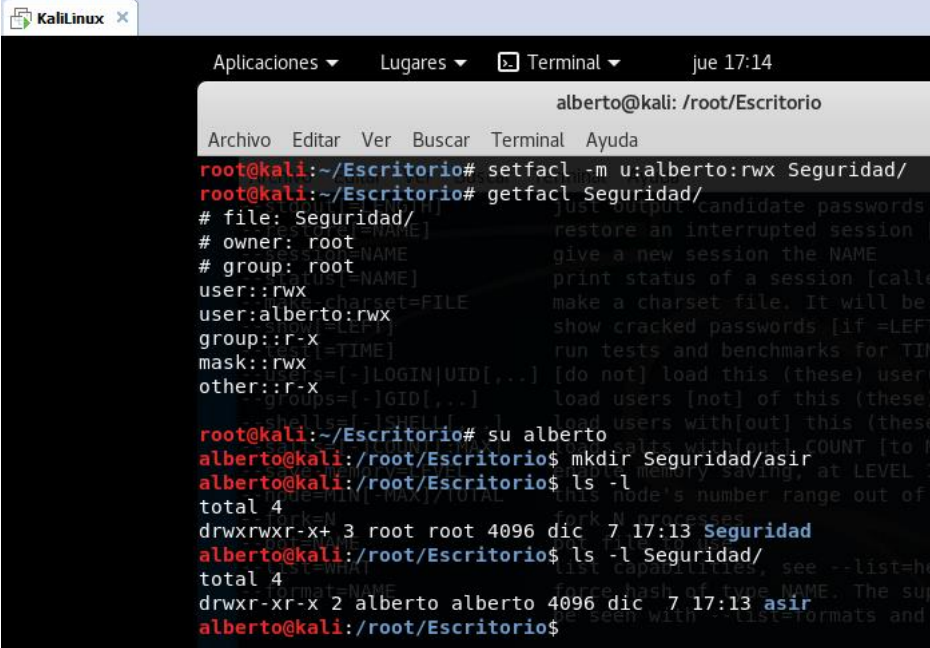
En este ejemplo podemos ver que el usuario Alberto no tiene permisos para escribir en el directorio de seguridad y por lo tanto no puede crear un nuevo directorio. Como también vemos en la imagen no está dentro de los permisos pro acl, realizamos la prueba de crear un nuevo directorio dentro de Seguridad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



```
alberto@kali: /root/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# su alberto
alberto@kali:/root$ cd Escritorio/
alberto@kali:/root/Escritorio$ ls -l
total 4
drwxr-xr-x 2 root root 4096 dic  7 15:46 Seguridad
alberto@kali:/root/Escritorio$ getfacl Seguridad/
# file: Seguridad/
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
alberto@kali:/root/Escritorio$ mkdir Seguridad/asir
mkdir: no se puede crear el directorio «Seguridad/asir»: Permiso denegado
```

Ahora usamos el comando `setfacl` 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.



```
KaliLinux x
Aplicaciones Lugares Terminal jue 17:14
alberto@kali: /root/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~/Escritorio# setfacl -m u:alberto:rwx Seguridad/
root@kali:~/Escritorio# getfacl Seguridad/
# file: Seguridad/
# owner: root
# group: root
user::rwx
user:alberto:rwx
group::r-x
mask::rwx
other::r-x
root@kali:~/Escritorio# su alberto
alberto@kali:/root/Escritorio$ mkdir Seguridad/asir
alberto@kali:/root/Escritorio$ ls -l
total 4
drwxrwxr-x+ 3 root root 4096 dic  7 17:13 Seguridad
alberto@kali:/root/Escritorio$ ls -l Seguridad/
total 4
drwxr-xr-x 2 alberto alberto 4096 dic  7 17:13 asir
alberto@kali:/root/Escritorio$
```

3. Bibliografía.

Software.

- VMWare Workstation Pro 12.
- Máquina virtual con Kali Linux.
- John de Ripper Kali Linux.

Documentación.

- Diferentes pdf entregados en clase.
- Diferentes webs.