**2ªEVSEGURIDAD LOCAL**

* **Usuarios y permisos en Linux (ejercicios)**

ls -l /home/asir1

(dir /s c:\users\asir1)

usuario grupo otros

rwx rwx rwx

r - lectura

w - escritura/modificación (crear o modificar archivos en una carpeta)

x - ejecución/acceso (si puedes o no acceder al escritorio)

*w en fichero puedes dejar vacío el fichero pero no borrar el fichero*

*para poder borrar el fichero tiene que estar por encima el directorio*

chmod - cambiar los permisos de un fichero/directorio

**-Opción 1: ugoa+-=rwx**

u -> usuario

g -> grupo

o -> otros usuarios

a -> todos

“+” -> añadir

“-” -> quitar

“=” -> establecer

EJ: rw-r--r-- fichero.txt

chmod ug+x fichero.txt => rwxr-xr--

chmod=wx fichero.txt => rwxr-x-wx

chmod a-x fichero.txt => rw-r---w-

**-Opción 2: octal**

dnd hay permiso = 1

dnd no hay permiso = 2

rwx rw r-- => 111 110 100 => 7 6 4

EJ: rw-r--r-- fichero.txt

chmod 755 fichero.txt => rwxr-xr-x

chmod 632 fichero.txt => rw--wx-w-

**OCTAL:**

4 significa «leer»,

2 significa «escribir»,

1 significa «ejecutar», y

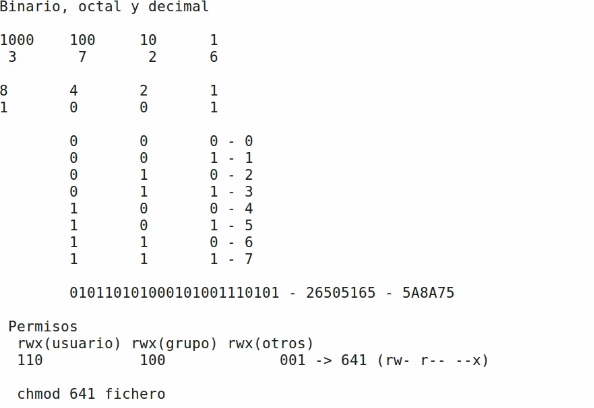
0 significa «sin permiso»

1.Crear usuario

2.Meterlo en grupo sudo

3.Logear en una terminal con ese usuario

4.Usar chmod



**COMANDOS IMPORTANTES:**

man (como el help de windows)

id (ej: administrador) dice que uid tiene ese usuario

uid=número de user

gid=número de grupo

etc

groups grupos a los que pertenence el usuario

whoami usuasrio con elq ue estamos conectados

su crear una shell dentro de otra

passwd->para cambiar la contraseña

sudo

adduser

usermod

deluserumask

addgroup

groupmod

delgroup

chown

chgrp

chmod

umask

**VER USUARIOS Y GRUPOS**

**grupos**: sudo cat /etc/group

**usuarios:** sudo cat /etc/passwd

1. usermod -aG sudo sammy

* **ALMACENAMIENTO SEGURO**
* Soportes:
  + Magnético: cintas, disquetes,discos duros
  + Magnético-óptico: super discos(IBM.zip,jazz) -> 120MB-1GB
  + Óptico: CD-ROM, dvd, blu-ray, hd-DVD -> 700MB-4.7GB-25GB-50GB
  + Eléctrico: tarjetas de memoria, pendrive
* Estructura Discos Duros:
  + particiones
    - primaria (0-4) máximo entre ambas = 4
    - extendida(0-1)
      * lógicas todas las que quiera

Formato sistemas de archivos (fat,fat16,fat32, fat32,ntfs,exfat,ext2,ext3,ext4)

* **Antivirus (torneo virus)**
* **Códigos redundantes (teoría)**
* **SEGURIDAD EN RED**

.... (muchas cosas)

* Seguridad local
* Configuración de red
  + Hardware, arquitectura, dispositivos
  + interfaz de red(ip ,mascara,puerta de enlace,dns)
  + comando de red

* Encriptado certificación, protocolos seguros (ssl-> secure socket layer
  + Ssh-> secure shell)
* Cortafuegos (firewall)==> reglas de acceso
  + Dmz -> zona desmilitarizada zona segura
* Monitorizacion y analisis de red
  + Ids-> detección de intrusos
  + Ips->prevención de intrusos
* Proxy VPN (red privada virtual)

COMANDOS DE RED WINDOWS

getmac /v (+info)

arp -a direcciones ip con dirección mac

ipconfig /all ver configuración de red

ipconfig /release liberar los valores que me han dado (abandonar esa ip que me han dado)

ipconfig /renew necesito una ip hay alguien que me la de?

ipconfig /displaydns muestra los dns que sabe esta máquina

ipconfig /flushdns borra esa tabla

ping x defecto 4 veces

ping [www.google.com](http://www.google.com) -n 2 y lo hace ese número de veces las peticiones

ping 10.16.5.1 -1 500 -l la cantidad que queremos con -l

ping 10.16.5.1 -1 1024 -t es de forma infinita

tracert [www.google.es](http://www.google.es) como el ping pero nos muestra los saltos que va tomando

nslookup [www.google.es](http://www.google.es) preguntar a un nombre que ip tiene

netstat ver las conexiones abiertas

netstat -n lo mismo pero de forma numérica

netstat -a aparecen todas las conexiones internas

netstat -b el programa asociado a cada conexión

netstat -r tabla de enrutamiento

COMANDOS DE RED LINUX

ifconfig (todas las tarjetas de red)

ifconfig eth0

ifdown eth0

ifup eth0

ping x defecto infinito

ping -c 4 y te lo hace 4 veces

mtr igual que el tracert de windows

nslookup

dig [www.google.es](http://www.google.es) @8.8.8.8 (nslookup pero le puedes indicar a que servidor le preguntas)

netstat (=windows nos muestra las conexiones abiertas)

netstat -a nos muestra todas las conexiones (estando conectadas o sin conectar

netstat -p mostrar cual es el programa o aplicación que esta conectada

route

**Firewall**

Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

**TODO EN MODO SUDO**

sudo service iptables status

sudo service iptables start

sudo service iptables restart

sudo service iptables stop

sudo iptables -L → listar las reglas

sudo iptables -P INPUT DROP → passas de accept a drop

**sudo iptables -A INPUT -s 10.5.0.0/16 -j ACCEPT**

-A (añadir una regla)

-s (indicar la source: en este caso de red por eso lleva la máscara)

-j (acción)

**sudo iptables -A INPUT -s 10.5.0.1 -p tcp –d port 80 -d 10.16.0.5.1 -j ACCEPT**

-p (indicar el protocolo

-d (destino)

sudo iptables -nL INPUT

n: lista pero el puerto sale con un número

sudo iptables -L INPUT –line-numbers (listado numerado)

sudo iptables -I INPUT 1 -d 10.16.5.1 -j ACCEPT

-I añadir

sudo iptables -D INPUT 1 -d 10.16.5.1 -j ACCEPT

-D borrar

sudo iptables -F (me borra todas)

**Legislación (trabajo)**

**Gparted**

1.select keymap from arch

2.QWERTY

3.SPANISH

4.STANDART

5.STANDART

6.LENGUA 25

7.MODO PREFER: 0

*Abrimos app:*

1.CREAR TABLA PARTICIONES (dispositivo)

2.Añadir particiones con los formatos deseados

3.TICK VERDE: aplicar todas las operaciones realizadas

**Clonezilla**

1. keep mantener
2. Start clonezilla
3. **device-image** o device-device
4. local\_dev pq lo tenia en local
5. ctrl+c para continuar una vez haya leido todos los discos
6. sdb1 q es donde tengo la imagen
7. antes de montarlo quieres hacer comprobeision= NOO
8. lost-found
9. si lees o si escribes done
10. modo beginner
11. restore disk
12. seleccionas la imagen q quieras
13. nsq d sekearr la imagen
14. -p choose
15. intro y se chequea la imagencita

—---------------------------------------------------------------------------------------------

Nada mas inicias

1. Clonezilla live(primera opción)
2. Spanish|Español
3. Mantener distribucion teclado
4. Iniciar clonezilla
5. Aquí puedes realizar varias opciones(**device-image** o device-device o más opciones)
6. part\_to\_local\_part **(IMPORTANTE LOS DISCOS DUROS TIENE QUE SER DEL MISMO TAMAÑO O QUE LA PARTIDICIÓN DEL DISCO DE ORIGEN QUEPA EN EL DISCO DE DESTINO POR TAMAÑO)**
7. Eliges el disco de origen
8. Eliges el disco de destino
9. Omitir la comprobación
10. Choose
11. Intro
12. y
13. y
14. Enter

1. Muestra la información del usuario actual.



2. Muestra los grupos del usuario actual.



3. Crea el grupo marvel.



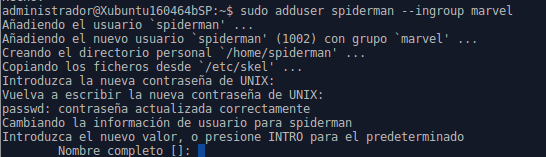
4. Crea el grupo dc.



5. Crea un usuario llamado spiderman en el grupo marvel y con contraseña spiderman.

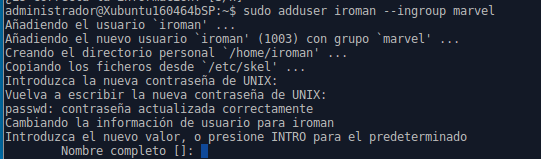
**Cuando creas el usuario abajo te pide que pongas la nueva contraseña.**

**Le das todo Enter cuando te pida nombre completo y luego a si para salir.**



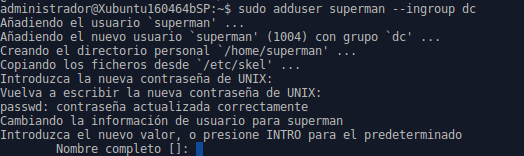
6. Crea un usuario llamado ironman en el grupo marvel y con

contraseña ironman.



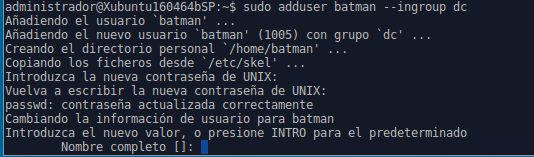
7. Crea un usuario llamado superman en el grupo dc y con contraseña

superman.



8. Crea un usuario llamado batman en el grupo dc y con contraseña

batman.



9. Haz login con spiderman el la terminal 2, con ironman en la terminal

3, con superman en la terminal 4 y con batman en la terminal 5.

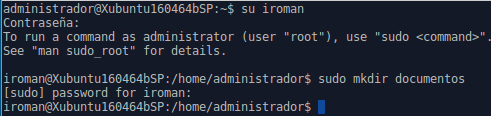
**Ctrl+Shift+T abres varias terminales en la misma pestaña.**



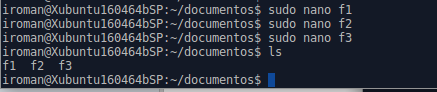
10.Con cada usuario crea la siguiente estructura en su carpeta personal: crea una carpeta llamada documentos con tres ficheros vacios f1 f2 y f3

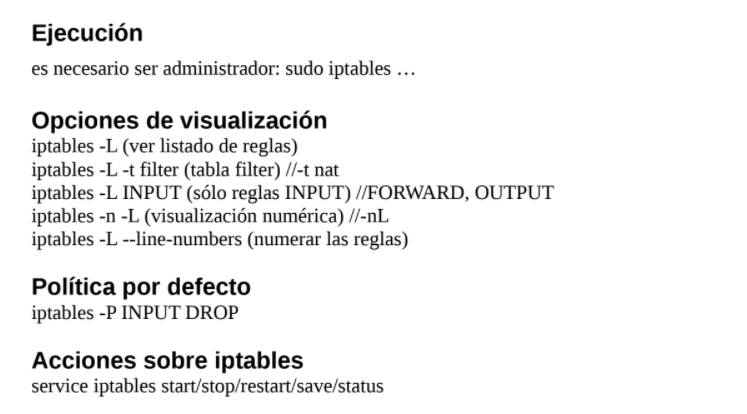
**Con el comando usermod hacemos que todos los usuarios que hemos creado tengan los privilegios de administrador y puedan crear cosas y hacer cosas.Cualquiera de las 2 opciones de abajo es válida para dar privilegios al usuario como sudoer.**

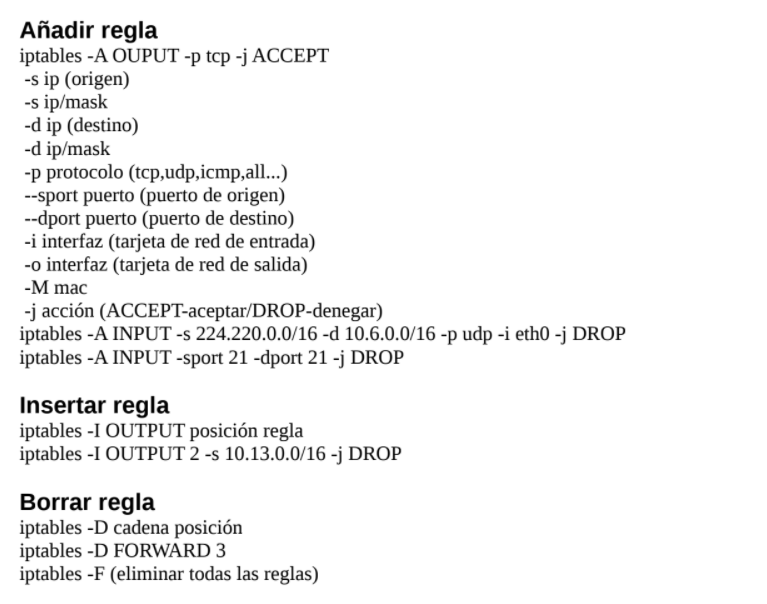




primero si tienes abierta otra terminal la cierras







3ªEV

Ingeniería social

1.Búsqueda de información<>No compartir información

2.Historia/Marco (roll) ->generar confianza<>ser críticos,no precipitarse

3.Limpieza<>denunciar, guardar pruebas

Ataques: phising, smishing, vishing, pretexting, baiting, tailgaiting, shouldersurfing, whaling, sim swapping, scareware, quid pro quo.

Ataque masivo y ataque selectivo.