MF0952_2_Publicació de Págines Web

Profesor: Javier Perea de la Casa

Programación

- Profesor: Javi Perea
    - mail: javier.perea@stucom.com
- ¿Qué vamos a ver en Publicación de páginas web?
    - **Tema 1**: Características de seguridad en la publicación de páginas web.
    - **Tema 2**: Herramientas software de transferencia de ficheros
    - **Tema 3**: Publicación de páginas web.
    - **Tema 4**: Pruebas y verificación de páginas web

Programación

- Este módulo se estructura **por temas (no UFs).**
    - Habrá 4 actividades (que desarrollarán la parte práctica de todos los temas) principales que tendrán un peso evaluativo.
    - Al finalizar el módulo se realizará una **prueba objetiva** tipo test
    - Al finalizar cada tema, haremos una pequeña prueba **kahoot** tipo test para comprobar que los conocimientos se van asentando.
        - No tiene peso evaluativo pero su resolución nos servirá para prepararnos para la prueba objetiva tipo test.

Programación

- Ponderación
  - 70% examen final
    - 2 convocatorias, segunda convocatoria se accede si se suspende o no se presenta al examen.
  - 30% actividades prácticas
- Hay que asistir un **mínimo de un 75% de las 90 horas** del módulo para poder presentarse a las convocatorias de los exámenes.
- En el examen habrá que sacar un mínimo de un 4 para poder calcular la media, de lo contrario habrá que asistir a la segunda convocatoria.

Entregas y fechas de examen

- Actividades
  - A1: Creació d’ un Host Virtual, ús de sistema gestors de servidors web.
    - Horas de trabajo: 9
    - Fecha de entrega: **10/07/2022**
  - A2: Estructuració de la web. Assignació de permisos y distribució en directoris.
    - Horas de trabajo: 9
    - Fecha de entrega: **15/07/2022**
  - A3: Gestió i manteniment de client FTP. Protocol de transferencia d’arxius.
    - Horas de trabajo: 12
    - Fecha de entrega: **20/07/2022**
  - A4: Creació i manipulació de contingut web a través de CMS (Wordpress)
    - Horas de trabajo: 15
    - Fecha de entrega: **26/07/2022**
- Examen (Tipo Test)
  - Duración: 2 horas
    - 1a convocatoria: **21/07/2022**
    - 2a convocatoria: **27/07/2022**

Método de trabajo

- Cada clase intercalará
    - Explicación teórica
    - Trabajo práctico
- El seguimiento-observación del trabajo práctico durante la clase compensará positivamente en la puntuación de las actividades prácticas que se propongan a entregar.
- Y sobre todo, ¡¡preguntad lo que necesitéis y ayudaros entre vosotros!! :)
    - ***“Cuando las arañas tejen juntas, pueden atar a un león.”***

Tema 1 - Característiques de seguretat en la publicació de pàgines web

Profesor: Javier Perea de la Casa

1. Índice

Introducció

- Sistema Operativo: Conjunto de programas que se ejecutan cuando se arranca una máquina, permite 2 cosas
  - Gestionar el hardware de una máquina
  - Proporcionar servicios de software con los cuales interacciona el usuario.

Introducción

Cualquier desarrollador web y/o administrador de sistemas debe hacerse unas primeras preguntas antes de comenzar a publicar webs:

- ¿Datos sensibles a la LOPD?
- ¿El servidor dónde se publicará tiene medidas antimalware y antivirus?
- ¿Está protegido el servidor para impedir el acceso de otros usuarios del equipo de trabajo?

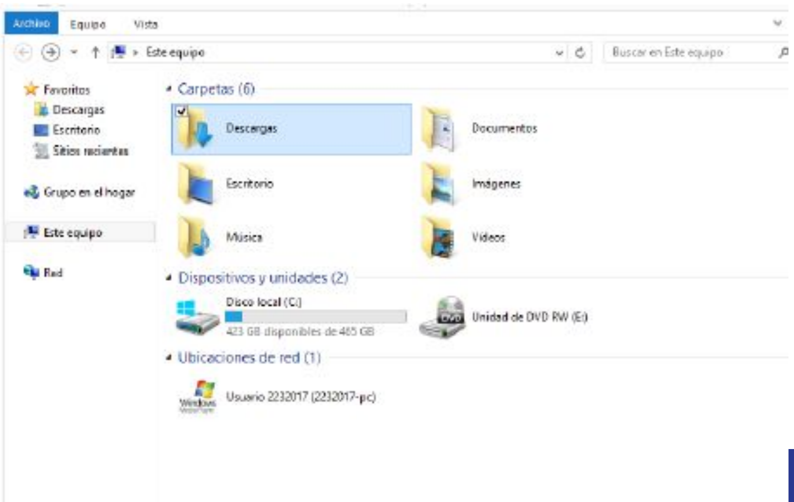
Introducció

- **Para dar respuesta a estas preguntas es interesante saber que:**
    - El desarrollador tiene que contemplar la seguridad en los equipos en los cuales se desarrolle el producto y el lugar donde, finalmente, vaya a instalarse el sitio web.
    - Debe haber una protección antimalware y antivirus así como un control de seguridad en el acceso de usuarios (con credenciales).
        - Se debe tener el software del servidor siempre actualizado para evitar posibles bugs y ataques.
    - Cuando **se despliega** un sitio web (hosting) este tiene que cumplir estas medidas de seguridad.
    - ¿Dónde podemos ver las pautas para proteger la información?
        - https://www.aepd.es/es/documento/reglamento-ue-2016-679-consolidado.pdf1.1.

LOPD

Seguretat en diferents sistemes d'arxius

- Sistema de archivos: Método y estructura de datos el cual un SO utiliza para organizar los diferentes archivos de un sistema de almacenamiento.
    - Tipos de organización de archivos: FAT, EXT4, NTFS, etc.



Seguretat en diferents sistemes d’arxius

El administrador del equipo es el que se encargará de gestionar los privilegios de todos y cada uno de los usuarios.

Imaginad que queréis compartir información, es siempre el usuario administrador el que indica quién puede acceder a esta información y con qué privilegios.

- ¿Y qué tipos de permisos podemos otorgar sobre carpetas o archivos?
    - Lectura
    - Escritura y/o Modificar

Seguretat en diferents sistemes d’ arxius

- **Todos los sistemas interconectados deben tener su propia arquitectura “segura”**
    - **Arquitectura de seguridad:** Implementación de mecanismos y servicios con funciones de seguridad que se apoyarán en muchos casos en servicios, mecanismos y funciones ya implementados en la propia arquitectura de comunicaciones.
    - Pensad que es mucho más fácil que se propague malware debido a que las redes son cada vez más complejas y el número de sistemas interconectados aumenta cada día de manera continua (Smartphones, IoT…)

Seguretat en diferents sistemes d’arxius

- ¿Qué entendemos por comunicación entre dos sistemas informáticos distintos?
    - Peticiones de un sistema//Respuestas del otro. P.ej: Servidor Web.
    - Transferencia de archivos de un lugar a otro, información.
- Y para que sea seguro… ¿Qué se debe garantizar en la comunicación entre dos sistemas?
    - Autenticación
    - Control de acceso
    - Confidencialidad
    - Integridad
    - No repudio

Seguretat en diferents sistemes d’arxius

- Vale… pero… ¿cómo hago un sistema **seguro?**
  - Si queremos un sistema de archivos seguro debemos implementar sistemas, métodos y procedimientos que así lo permitan.
    - Asignación de permisos de acceso discrecionales según perfiles de usuarios
    - Utilización de cortafuegos
    - Antivirus
    - Copias de seguridad
    - Cifrado de información y encriptación de archivos y carpetas.

1.1.1. Sistema Operativo Linux

- Linux es un sistema operativo **libre** que no significa lo mismo que gratuito. ¿Sabríais la diferencia entre Freeware (gratuito) y Open Source (Software libre)?
    - Open Source quiere decir que cualquiera lo puede usar, distribuir y modificar.
- El SO Linux tiene diversas distribuciones, algunas de ellas de pago y otras no.
    - Pago
        - Red Hat
        - Suse
        - Mandriva
    - Sin pago
        - Ubuntu
        - Manjaro
        - OpenSuse
        - KaliLinux
        - Etc

1.1.1. Sistema Operativo Linux

- Linux puede implementar diversas soluciones de sistemas de archivos como EXT3, EXT4, ReiserFS, XFS.
  - Todos ellos con un sistema de **logs o journaling** consistentes en llevar a cabo un registro de diario en el que se almacena la información necesaria.
    - Con este sistema se consigue restablecer los datos afectados por la transacción en caso de que esta falle. Por ejemplo, cuando el sistema se cae por falta de corriente eléctrica.

1.1.1. Sistema Operativo Linux

- ¿Por qué Linux es un sistema con tantos seguidores actualmente?
  - Tenemos distribuciones gratis pudiendo emplear tantas licencias como se desee.
  - Desarrollado por miles de voluntarios en el mundo. Cualquier puede participar y pertenecer a la comunidad.
  - Código fuente abierto a todos.
  - Alta estabilidad, por lo que es difícil que se quede colgado.
  - Extremadamente seguro ya que tiene varios sistemas de protección. Su cortafuegos está incrustado en el propio núcleo del sistema.
  - Facilidad de uso en muchas tareas.
  - Lee y escribe en sistemas de archivos de Windows y Macintosh.
  - Se comunica con cualquier otro sistema de red.
  - Las distribuciones tienen diversos escritorios como Unity, Gnome, KDE, XFCE, LXDE.
  - Necesita bajos requerimientos Hardware para poder ejecutarse.
  - Ocupa poca memoria debido a la sencillez de UNIX

1.1.1. Sistema Operativo Linux

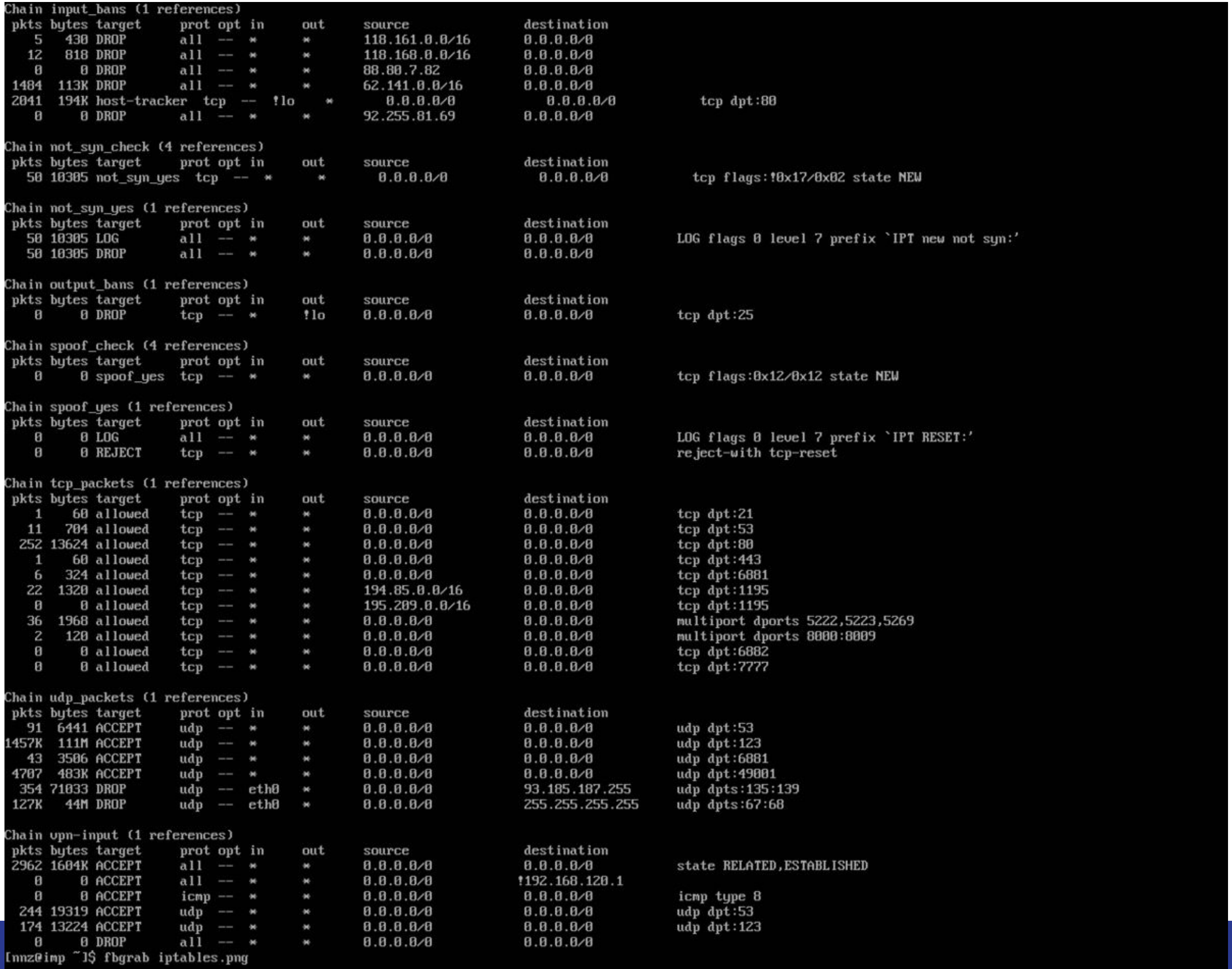
- Administración en Linux
  - En Linux suele haber un usuario que crearemos cuando instalemos el SO y tendrá acceso restringido al sistema. Para poder realizar tareas habituales se puede emplear este usuario.
  - Sin embargo, este usuario tiene acceso restringido a diversas operaciones de administración del sistema, para poder realizar este tipo de tareas nos autenticaremos como el usuario
    - **root:** este usuario actúa de administrador del sistema y podrá llevar tareas y manipular funciones internas del sistema. Por ejemplo: root será el encargado de permitir que se instalen los programas o paquetes en el SO…
  - **Seguridad:** a pesar de ser un sistema de alta seguridad no está libre de accesos indeseados, virus, spyware, etc. Por lo cual **es más que recomendable establecer mecanismos de defensa activa en estos SSOO.**

1.1.1. Sistema Operativo Linux

- Cortafuegos
  - Sistema de seguridad para **bloquear accesos no autorizados al ordenador** mientras sigue permitiendo la comunicación de nuestro ordenador con otros servicios.
- Cortafuegos en Linux
  - Este es parte integrante del núcleo (kernel) de Linux.
  - Cabe señalar las líneas **DROP**, con este parámetro conseguimos que las peticiones procedentes de las máquinas cuyas IPs coinciden con las marcadas no reciban respuesta. Es decir, de cara a ellas nuestro ordenador está apagado y fuera de cobertura.
  - El valor **ALL** indica que las comunicaciones por cualquier puerto están negadas.

+info:
https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona

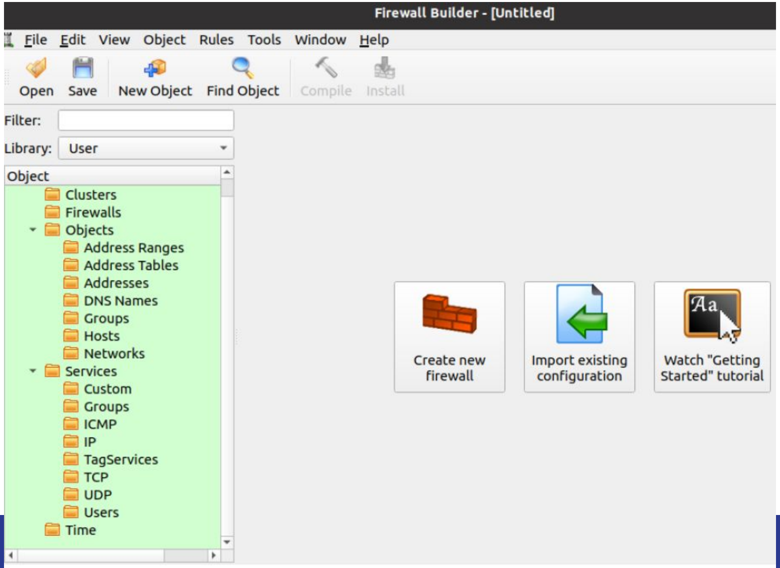
Ejemplo cortafuegos IPTABLES



```
Chain input_bans (1 references)
 pkts bytes target     prot opt in     out     source               destination
    5   430 DROP       all  --  *      *       118.161.0.0/16       0.0.0.0/0
   12   818 DROP       all  --  *      *       118.168.0.0/16       0.0.0.0/0
    0     0 DROP       all  --  *      *       88.80.7.82           0.0.0.0/0
 1484  113K DROP       all  --  *      *       62.141.0.0/16        0.0.0.0/0
 2041  194K host-tracker  tcp  --  !lo    *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    0     0 DROP       all  --  *      *       92.255.81.69         0.0.0.0/0

Chain not_syn_check (4 references)
 pkts bytes target     prot opt in     out     source               destination
   50 10305 not_syn_yes  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:!0x17/0x02 state NEW

Chain not_syn_yes (1 references)
 pkts bytes target     prot opt in     out     source               destination
   50 10305 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 7 prefix `IPT new not syn:'
   50 10305 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain output_bans (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      !lo     0.0.0.0/0            0.0.0.0/0           tcp dpt:25

Chain spoof_check (4 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 spoof_yes  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp flags:0x12/0x12 state NEW

Chain spoof_yes (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 7 prefix `IPT RESET:'
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with tcp-reset

Chain tcp_packets (1 references)
 pkts bytes target     prot opt in     out     source               destination
    1    60 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:21
   11   704 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:53
  252 13624 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:80
    1    60 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:443
    6   324 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:6881
   22  1320 allowed    tcp  --  *      *       194.85.0.0/16        0.0.0.0/0           tcp dpt:1195
    0     0 allowed    tcp  --  *      *       195.209.0.0/16       0.0.0.0/0           tcp dpt:1195
   36  1968 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 5222,5223,5269
    2   120 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           multiport dports 8000:8009
    0     0 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:6882
    0     0 allowed    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp dpt:7777

Chain udp_packets (1 references)
 pkts bytes target     prot opt in     out     source               destination
   91  6441 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
1457K  111M ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:123
   43  3506 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:6881
 4707  483K ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:49001
  354 71033 DROP       udp  --  eth0   *       0.0.0.0/0            93.185.187.255      udp dpts:135:139
 127K   44M DROP       udp  --  eth0   *       0.0.0.0/0            255.255.255.255     udp dpts:67:68

Chain vpn-input (1 references)
 pkts bytes target     prot opt in     out     source               destination
 2962 1604K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0           !192.168.120.1
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 8
  244 19319 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:53
  174 13224 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0           udp dpt:123
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
[nnz@imp ~]$ fbgrab iptables.png
```

1.1.1. Sistema Operativo Linux

- También podemos implementar soluciones más sencillas en lo que respecta al Firewall de Linux, sin necesidad de usar la terminal.
  - Una herramienta muy útil es **FWBuilder**
    - **Aplicación gráfica que facilita la gestión del cortafuegos.**



1.1.1. Sistema Operativo Linux

Más herramientas que permiten proteger nuestros ordenadores con SO Linux

FAIL2BAN

- **FAIL2BAN**: Nos permite indicar qué software debe ser protegido contra ataques por "fuerza bruta"
  - Dispone de un fichero de configuración para esto
    - Ubicado en /etc/fail2ban/jail.conf

1.1.1. Sistema Operativo Linux

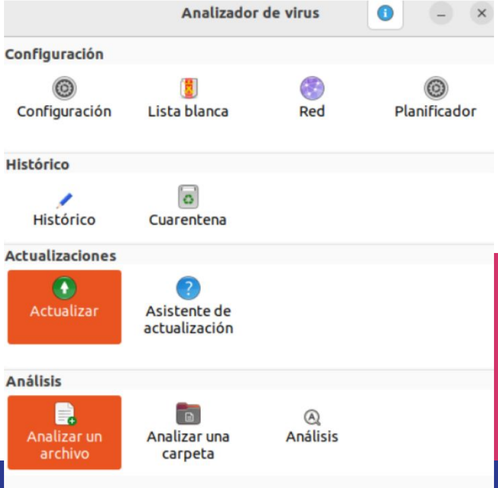
- Imaginad que tenemos un servidor SSH (explicaremos más tarde) el cual queremos proteger de un **acceso remoto por el puerto 23.**
    - El fichero de configuración /etc/fail2ban/jail.conf debería quedar así.

```
[ssh]

enabled=true

port = ssh

filter = sshd

action = iptables[name=SSH, port=23, protocol=tcp]

logpath=/var/log/auth.log

maxretry=6
```

FAIL2BAN

1.1.1. Sistema Operativo Linux

- Antivirus
    - Los sistemas Linux son poco propensos a ser infectados de malware debido a que internamente a nivel de núcleo del sistema implementan ya **mecanismos de seguridad de alto nivel**.
        - **Sin embargo, no hay garantías de que un sistema Linux no llegue a infectarse.**
    - CLAMAV
        - Libre y gratuito
    - Dispone de aplicación gráfica llamada "ClamTK".

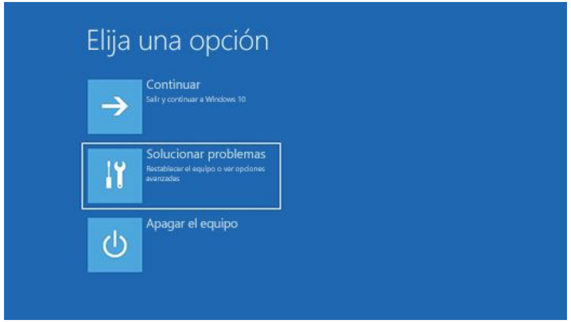


Empezamos a desarrollar la primera parte de la actividad…

- Descarga VirtualBox e instala el SO Ubuntu Desktop como máquina virtual.
    - Asignarle un espacio de 4GB-6GB de RAM
    - Reserva dinámica del espacio de almacenamiento.
- Documenta en un word el proceso (pantallas de instalación de la VM y explicación del proceso)
    - La entrega se realizará con el resto de actividades de la práctica.
- Y recordad… ¡Preguntad toda duda que tengáis!

1.1.2. Sistema Operativo Windows

- ¿Cómo nos protegemos de un ataque en un sistema Windows?
  - Si estamos bajo ataque, Windows nos permite **arrancar** el sistema "**a prueba de errores**", acceder como administrador y poder realizar las tareas de mantenimiento oportunas.
  - A diferencia de Linux en Windows podemos manipular el nivel de los usuarios a través del **UAC**.
    - Consiste en indicarle el nivel de aviso de cambios en el sistema por parte de una aplicación o servicio.

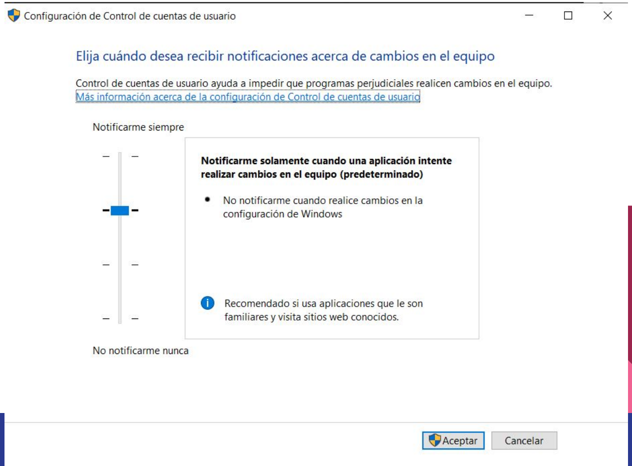


Elija una opción

Continuar
Salir y continuar a Windows 10

Solucionar problemas
Restablecer el equipo o ver opciones avanzadas

Apagar el equipo



Configuración de Control de cuentas de usuario

Elija cuándo desea recibir notificaciones acerca de cambios en el equipo

Control de cuentas de usuario ayuda a impedir que programas perjudiciales realicen cambios en el equipo.
Más información acerca de la configuración de Control de cuentas de usuario

Notificarme siempre

Notificarme solamente cuando una aplicación intente realizar cambios en el equipo (predeterminado)

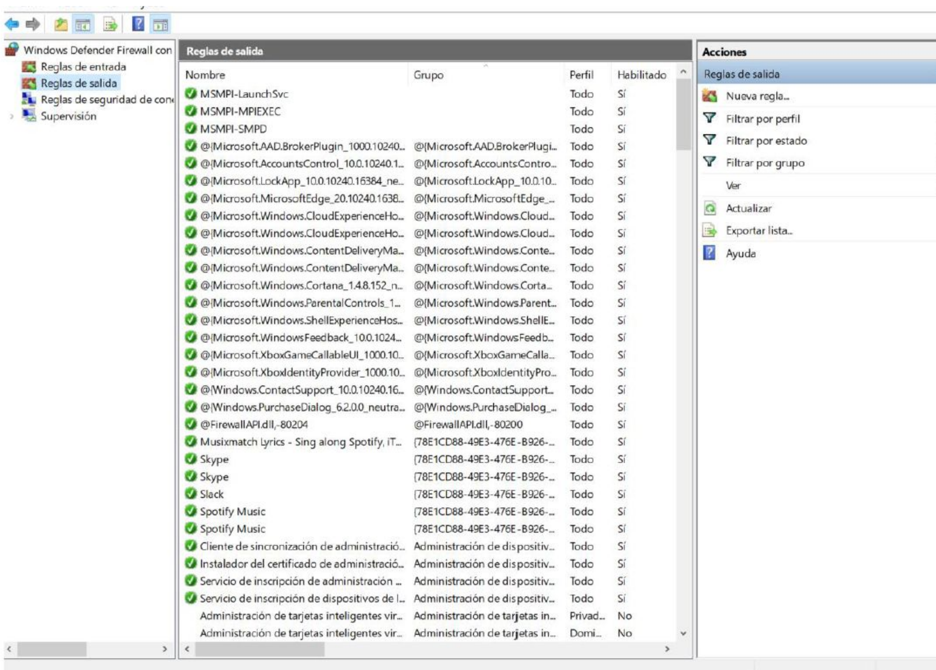
- No notificarme cuando realice cambios en la configuración de Windows

Recomendado si usa aplicaciones que le son familiares y visita sitios web conocidos.

No notificarme nunca

1.1.2. Sistema Operativo Windows

- ¿Cómo nos protegemos de un ataque en un sistema Windows?
    - Windows Defender Firewall
        - Cortafuegos de Windows
            - No incluido en el núcleo de Windows (lo que lo hace más inseguro que Linux)
    - Microsoft Security Essentials
        - No muy recomendable, vulnerabilidades básicas de seguridad
        - Mejor usar software de terceros
            - Avast, Kaspersky, Pandas…



Reglas de salida

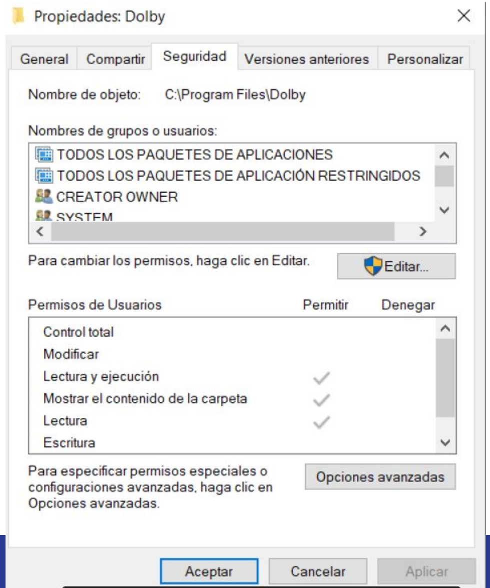
Nombre	Grupo	Perfil	Habilitado
MSMPI-LaunchSvc		Todo	Sí
MSMPI-MPIEXEC		Todo	Sí
MSMPI-SMPD		Todo	Sí
@{Microsoft.AAD.BrokerPlugin_1000.10240...	@{Microsoft.AAD.BrokerPlugi...	Todo	Sí
@{Microsoft.AccountsControl_10.0.10240.1...	@{Microsoft.AccountsContro...	Todo	Sí
@{Microsoft.LockApp_10.0.10240.16384_ne...	@{Microsoft.LockApp_10.0.10...	Todo	Sí
@{Microsoft.MicrosoftEdge_20.10240.1638...	@{Microsoft.MicrosoftEdge_...	Todo	Sí
@{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Todo	Sí
@{Microsoft.Windows.CloudExperienceHo...	@{Microsoft.Windows.Cloud...	Todo	Sí
@{Microsoft.Windows.ContentDeliveryMa...	@{Microsoft.Windows.Conte...	Todo	Sí
@{Microsoft.Windows.ContentDeliveryMa...	@{Microsoft.Windows.Conte...	Todo	Sí
@{Microsoft.Windows.Cortana_1.4.8.152_n...	@{Microsoft.Windows.Corta...	Todo	Sí
@{Microsoft.Windows.ParentalControls_1...	@{Microsoft.Windows.Parent...	Todo	Sí
@{Microsoft.Windows.ShellExperienceHos...	@{Microsoft.Windows.ShellE...	Todo	Sí
@{Microsoft.WindowsFeedback_10.0.1024...	@{Microsoft.WindowsFeedb...	Todo	Sí
@{Microsoft.XboxGameCallableUI_1000.10...	@{Microsoft.XboxGameCalla...	Todo	Sí
@{Microsoft.XboxIdentityProvider_1000.10...	@{Microsoft.XboxIdentityPro...	Todo	Sí
@{Windows.ContactSupport_10.0.10240.16...	@{Windows.ContactSupport...	Todo	Sí
@{Windows.PurchaseDialog_6.2.0.0_neutra...	@{Windows.PurchaseDialog_...	Todo	Sí
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	Todo	Sí
Musixmatch Lyrics - Sing along Spotify, iT...	{78E1CD88-49E3-476E-B926-...	Todo	Sí
Skype	{78E1CD88-49E3-476E-B926-...	Todo	Sí
Skype	{78E1CD88-49E3-476E-B926-...	Todo	Sí
Slack	{78E1CD88-49E3-476E-B926-...	Todo	Sí
Spotify Music	{78E1CD88-49E3-476E-B926-...	Todo	Sí
Spotify Music	{78E1CD88-49E3-476E-B926-...	Todo	Sí
Cliente de sincronización de administració...	Administración de dispositiv...	Todo	Sí
Instalador del certificado de administració...	Administración de dispositiv...	Todo	Sí
Servicio de inscripción de administración ...	Administración de dispositiv...	Todo	Sí
Servicio de inscripción de dispositivos de l...	Administración de dispositiv...	Todo	Sí
Administración de tarjetas inteligentes vir...	Administración de tarjetas in...	Privad...	No
Administración de tarjetas inteligentes vir...	Administración de tarjetas in...	Domi...	No

Permisos de acceso

- Los permisos de acceso nos permiten conocer qué usuarios o grupos de usuarios pueden acceder, manipular y ejecutar programas, archivos… dentro del sistema operativo.
- Tipos de permisos
  - **Control de acceso obligatorio**: Se trata de una herramienta de control de acceso multinivel. Se define una jerarquía de niveles de seguridad según los permisos que tenga el usuario. Es decir, una política de roles que garantice la seguridad en el acceso de la información.
  - **Control de acceso discrecional**: Aquí todos los objetos tienen un propietario.
  - **Control de acceso basado en roles**

Permisos de acceso

- Sistemas Windows
  - Definen 13 permisos para ficheros o directorios para el usuario o grupo.
    - Dando “permiso” o “denegando”.
  - Veamos un ejemplo de la sección seguridad del directorio Dolby.



Nombre de objeto: C:\Program Files\Dolby

Nombres de grupos o usuarios:

- TODOS LOS PAQUETES DE APLICACIONES
- TODOS LOS PAQUETES DE APLICACIÓN RESTRINGIDOS
- CREATOR OWNER
- SYSTEM

Para cambiar los permisos, haga clic en Editar.

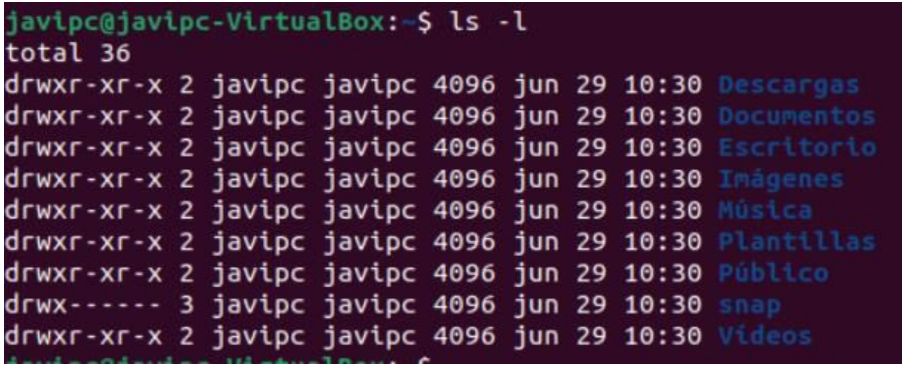
Permisos de Usuarios	Permitir	Denegar
Control total		
Modificar		
Lectura y ejecución	✓	
Mostrar el contenido de la carpeta	✓	
Lectura	✓	
Escritura		

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Permisos de acceso

- Sistemas Linux
  - 3 niveles de control de acceso
    - **Usuario (u):** Especifica al usuario, probablemente dueño del archivo o directorio.
    - **Grupo (g):** Especifica los usuarios que pertenecen al mismo grupo como el indicado en el archivo o directorio.
    - **Otros (o):** Representa al resto de usuarios.

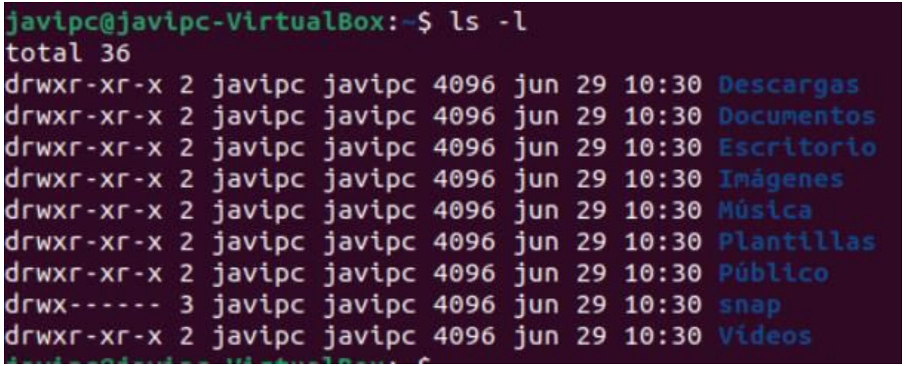
la d representará un fichero que realmente es un directorio



```
javipc@javipc-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Descargas
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Documentos
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Escritorio
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Imágenes
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Música
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Plantillas
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Público
drwx------ 3 javipc javipc 4096 jun 29 10:30 snap
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Vídeos
```

Nota: Solo cuando no coinciden el UID y el GID del usuario para el archivo correspondiente, se tendrá en cuenta el nivel de control de accesos (otros)

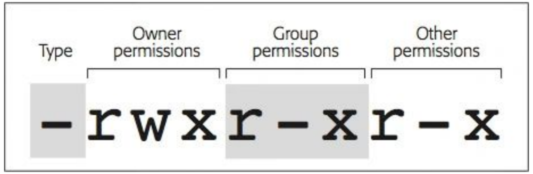
Permisos de acceso



```
javipc@javipc-VirtualBox:~$ ls -l
total 36
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Descargas
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Documentos
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Escritorio
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Imágenes
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Música
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Plantillas
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Público
drwx------ 3 javipc javipc 4096 jun 29 10:30 snap
drwxr-xr-x 2 javipc javipc 4096 jun 29 10:30 Vídeos
```

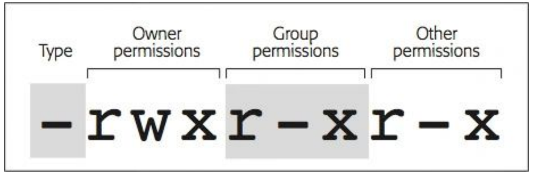
- Partes
  a. Permisos de contenido
  b. Número de enlaces al contenido
  c. Propietario del contenido
  d. Propietario del grupo del contenido
  e. Tamaño del contenido en bytes
  f. Fecha / hora de la última modificación del contenido
  g. Nombre de archivo o directorio

Permisos de acceso



- Sistemas Linux
  - 3 tipos de permisos: **Lectura (r), Escritura (w) y Ejecución (x).**
    - **Se comprueban en el siguiente orden**
      1. Si el UID (User Identifier del archivo es el mismo que el UID del proceso, solo se aplican permisos al propietario; los permisos de grupo y otros no se comprueban.
      2. Si los UID no coinciden, pero el GID (Group Identifier) del archivo coincide con uno de los GID del proceso (ya que un usuario puede pertenecer a varios grupos); el propietario y otros no se comprueban.
      3. Solo si el UID y GID del proceso no coinciden con los del archivo solo se comp

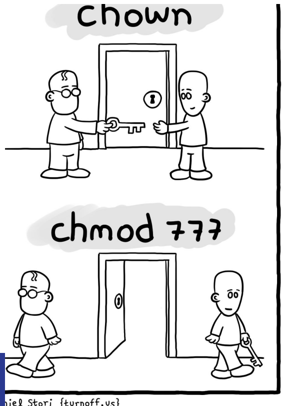
Permisos de acceso



- Linux
  - ¿Cómo damos permisos de acceso en Ubuntu?
    - Con la orden **chmod**
      - chmod ugo+rw ejemplo.txt
      - chmod 755 fichero o directorio.
    - Para entender cómo asignar permisos con números es necesario saber pasar a binario…
      - 7 es 111 -> activa r (read), w (write) y x (execution) del rol usuario
      - 5 es 101 -> activa r (read), y x (execution) del rol grupo
      - 5 es 101 -> activa r (read), y x (execution) del rol otros
    - Leer
      - https://www.ionos.es/digitalguide/servidores/know-how/asignacion-de-permisos-de-acceso-con-chmod/

Otro comando muy interesante y relacionado a chmod es **chown** (**ch**ange **own**er), que permite **cambiar el propietario del archivo.**

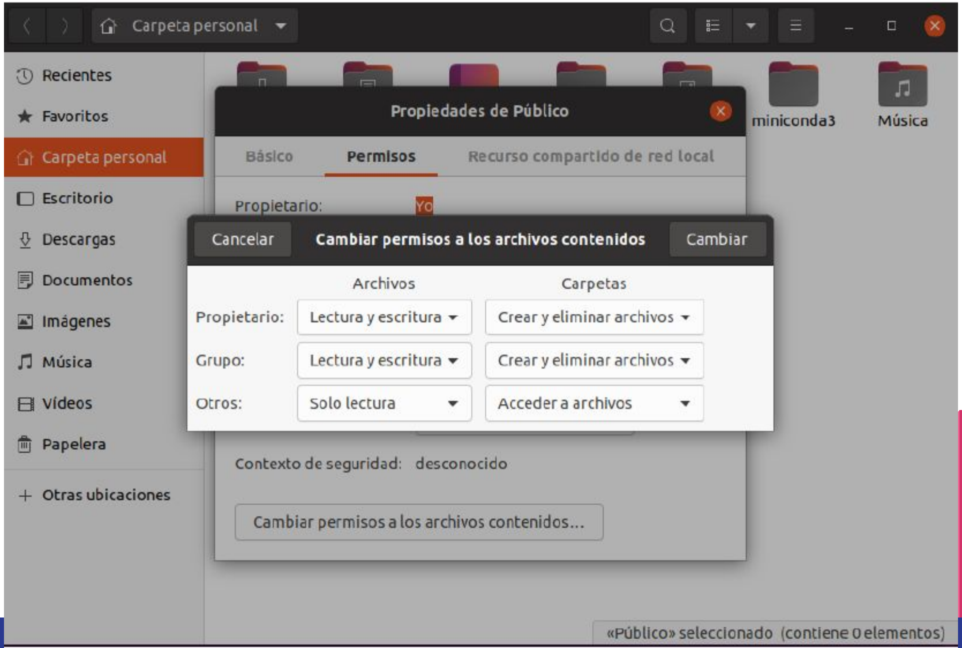
- https://www.ionos.es/digitalguide/servidores/know-how/asignacion-de-permisos-de-acceso-con-chmod/



iel Stori {turnoff.us}

Permisos de acceso

- Linux
  - También disponemos de herramienta gráfica para cambiar permisos a los archivos contenidos.



Propietario: Yo

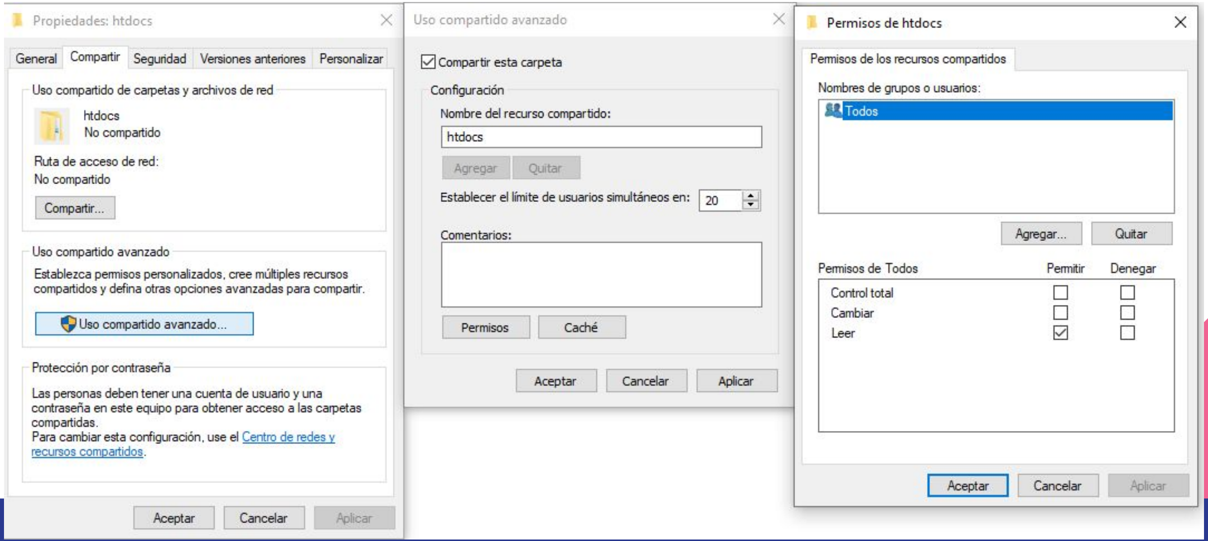
	Archivos	Carpetas
Propietario:	Lectura y escritura	Crear y eliminar archivos
Grupo:	Lectura y escritura	Crear y eliminar archivos
Otros:	Solo lectura	Acceder a archivos

Contexto de seguridad: desconocido

«Público» seleccionado (contiene 0 elementos)

Elección del tipo de acceso

- Casi todos los SSOO, permiten el uso del ordenador a varios usuarios.
- Entre mismos SSOO no necesitan comunicarse por medio de un servidor (Mac, Windows, Linux).
    - Cada sistema genera a cada usuario, una zona “privativa” en la que el usuario podrá compartir los derechos de lectura/escritura con otros usuarios.



Propiedades: htdocs

Uso compartido de carpetas y archivos de red

htdocs
No compartido

Ruta de acceso de red:
No compartido

Uso compartido avanzado

Establezca permisos personalizados, cree múltiples recursos compartidos y defina otras opciones avanzadas para compartir.

Protección por contraseña

Las personas deben tener una cuenta de usuario y una contraseña en este equipo para obtener acceso a las carpetas compartidas.
Para cambiar esta configuración, use el Centro de redes y recursos compartidos.

Uso compartido avanzado

☑ Compartir esta carpeta

Configuración

Nombre del recurso compartido: htdocs

Establecer el límite de usuarios simultáneos en: 20

Comentarios:

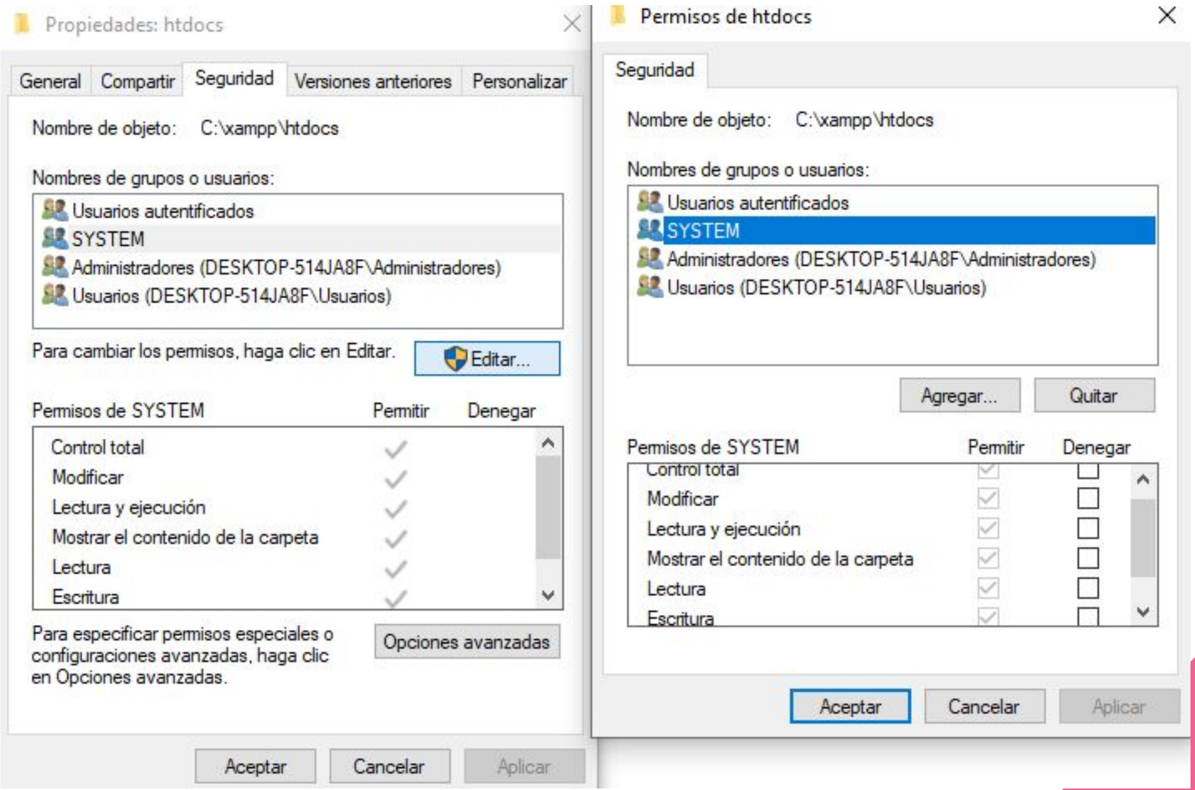
Permisos de htdocs

Permisos de los recursos compartidos

Nombres de grupos o usuarios:
Todos

Permisos de Todos	Permitir	Denegar
Control total	☐	☐
Cambiar	☐	☐
Leer	☑	☐

Implementación de accesos



Propiedades: htdocs

Nombre de objeto: C:\xampp\htdocs

Nombres de grupos o usuarios:

- Usuarios autentificados
- SYSTEM
- Administradores (DESKTOP-514JA8F\Administradores)
- Usuarios (DESKTOP-514JA8F\Usuarios)

Para cambiar los permisos, haga clic en Editar.

Permisos de SYSTEM	Permitir	Denegar
Control total	✓	
Modificar	✓	
Lectura y ejecución	✓	
Mostrar el contenido de la carpeta	✓	
Lectura	✓	
Escritura	✓	

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Permisos de htdocs

Nombre de objeto: C:\xampp\htdocs

Nombres de grupos o usuarios:

- Usuarios autentificados
- SYSTEM
- Administradores (DESKTOP-514JA8F\Administradores)
- Usuarios (DESKTOP-514JA8F\Usuarios)

Permisos de SYSTEM	Permitir	Denegar
Control total	☑	☐
Modificar	☑	☐
Lectura y ejecución	☑	☐
Mostrar el contenido de la carpeta	☑	☐
Lectura	☑	☐
Escritura	☑	☐

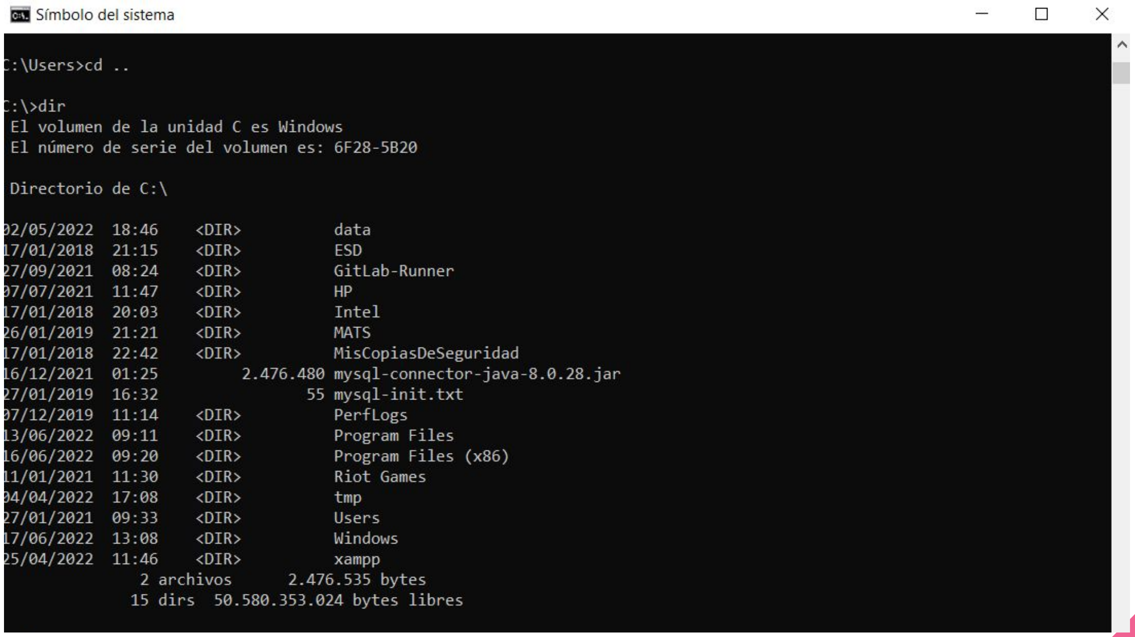
Permisos para el grupo SYSTEM (ADMIN) para la carpeta htdocs

Descripción de órdenes en distintos sistemas

- Es interesante conocer los comandos en modo consola que nos proporcionan los SSOO para tener la mayor flexibilidad operativa como **administradores de sistemas**.
- Windows
  - Para abrir la terminal vamos a inicio->buscar y escribimos **cmd**
  - Con la orden **dir** podremos listar el conjunto de archivos y directorios así como algunas propiedades de los mismos.

Descripción de órdenes en distintos sistemas

- Windows



```
:\Users>cd ..

:\>dir
 El volumen de la unidad C es Windows
 El número de serie del volumen es: 6F28-5B20

 Directorio de C:\

2/05/2022  18:46    <DIR>          data
7/01/2018  21:15    <DIR>          ESD
7/09/2021  08:24    <DIR>          GitLab-Runner
7/07/2021  11:47    <DIR>          HP
7/01/2018  20:03    <DIR>          Intel
6/01/2019  21:21    <DIR>          MATS
7/01/2018  22:42    <DIR>          MisCopiasDeSeguridad
6/12/2021  01:25         2.476.480 mysql-connector-java-8.0.28.jar
7/01/2019  16:32                55 mysql-init.txt
7/12/2019  11:14    <DIR>          PerfLogs
3/06/2022  09:11    <DIR>          Program Files
6/06/2022  09:20    <DIR>          Program Files (x86)
1/01/2021  11:30    <DIR>          Riot Games
4/04/2022  17:08    <DIR>          tmp
7/01/2021  09:33    <DIR>          Users
7/06/2022  13:08    <DIR>          Windows
5/04/2022  11:46    <DIR>          xampp
               2 archivos      2.476.535 bytes
              15 dirs  50.580.353.024 bytes libres
```

- Todos los comandos de Windows tienen su origen en
SO antiguo de Microsoft
  - ¿Sabríais decir cuál?

Descripción de órdenes en distintos sistemas

- Windows
  - dir
    - Obtenemos información de los archivos y directorios
  - cd
    - Son las siglas de ***c**hange* ***d**irectory*, permite cambiar de carpeta o directorio.
  - md
    - Crea un directorio en la ruta que se especifique.
  - rd
    - Borra un directorio en la ruta que se especifica
  - rename
    - Renombra un archivo
  - del
    - Elimina un archivo
  - move
    - Mueve un archivo

Descripción de órdenes en distintos sistemas

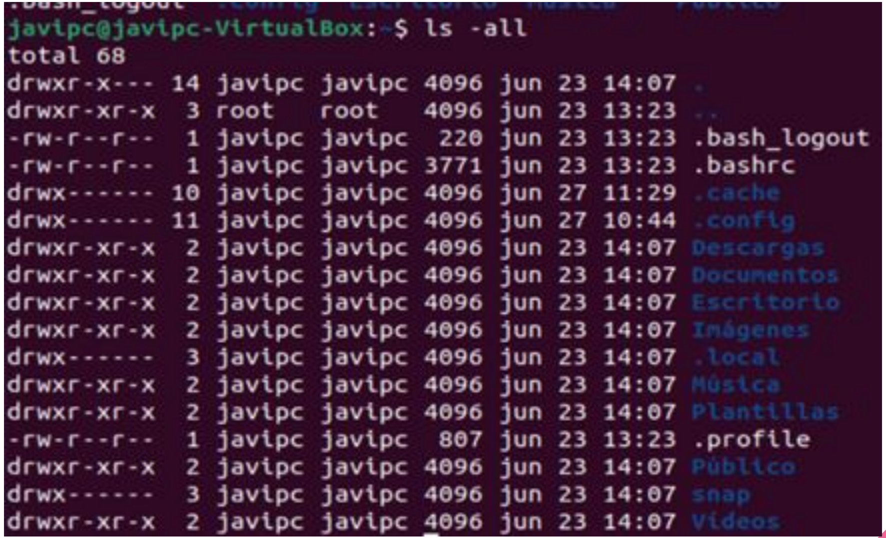
Mac OS X tiene la misma funcionalidad

- Linux
  - En el caso de GNU/Linux utilizaremos la orden “terminal” para acceder a la consola. Como el sistema operativo Linux es multiterminal podemos pasar del entorno gráfico a modo terminal pulsando simultáneamente CTRL-ALT-F2 y obtendremos acceso al terminal 2 (tty2).
    - Para pasar al terminal donde “corre” el entorno gráfico utilizaremos CTRL-ALT-F7.

INSTRUCCIÓN	¿QUÉ HACE?
cd [directorio]	Cambia el directorio por el especificado como parámetro.
mkdir directorio	Crea un nuevo directorio.
rmdir directorio	Borra un directorio vacío
mv fichero [fichero2… ficheroN] destino	Mueve o renombra ficheros o directorios
rm fichero1 [fichero2…ficheroN] destino	Borra ficheros y directorios con el parámetro -R (recursivo)
cp fichero1 [fichero2… ficheroN] destino	Copia ficheros y directorios en el directorio indicado.
pwd	Muestra en pantalla la ruta completa del directorio actual o activo

Descripción de órdenes en distintos sistemas

- Linux
  - Para poder visualizar en la terminal los archivos con sus correspondientes permisos se usa.
    - ls -l



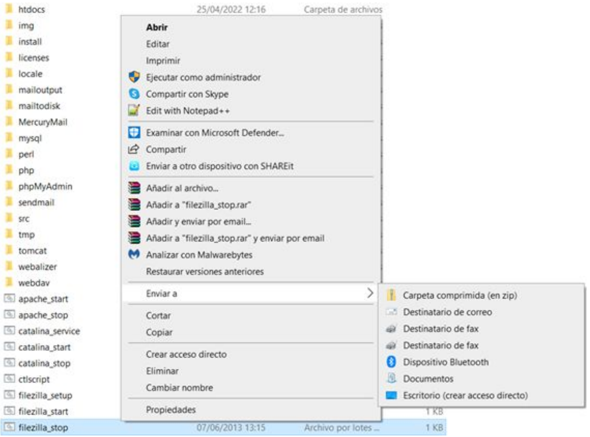
```
javipc@javipc-VirtualBox:~$ ls -all
total 68
drwxr-x--- 14 javipc javipc 4096 jun 23 14:07 .
drwxr-xr-x  3 root   root   4096 jun 23 13:23 ..
-rw-r--r--  1 javipc javipc  220 jun 23 13:23 .bash_logout
-rw-r--r--  1 javipc javipc 3771 jun 23 13:23 .bashrc
drwx------ 10 javipc javipc 4096 jun 27 11:29 .cache
drwx------ 11 javipc javipc 4096 jun 27 10:44 .config
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Descargas
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Documentos
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Escritorio
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Imágenes
drwx------  3 javipc javipc 4096 jun 23 14:07 .local
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Música
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Plantillas
-rw-r--r--  1 javipc javipc  807 jun 23 13:23 .profile
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Público
drwx------  3 javipc javipc 4096 jun 23 14:07 snap
drwxr-xr-x  2 javipc javipc 4096 jun 23 14:07 Vídeos
```

Implementación y comprobación de las distintas órdenes

- Una manera de comprobar si las acciones realizadas utilizan los comandos es mediante el **explorador de archivos**.
    - Nos facilita explorar de forma más amplia y global si cabe, la estructura de los directorios o carpetas y los archivos que lo contienen.
- Aunque la realización de tareas es **más rápida con comandos de consola** resulta siempre más cómodo de cara al usuario común acceder y manipular la información desde el explorador de archivos.

Implementación y comprobación de las distintas órdenes

- Independientemente de las opciones que se encuentran en la barra de tareas, también disponemos de un menú contextual que nos permite realizar más operaciones sobre un archivo o directorio como podemos observar en la imagen.



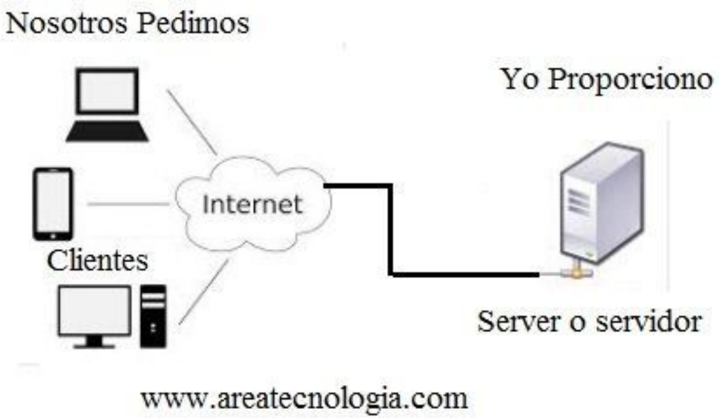
Implementación y comprobación de las distintas órdenes

- Algunos paquetes de ofimática como Office o herramientas como DreamWeaber o Notepad++, disponen de opciones
  - Permiten la **creación y modificación de los documentos** de la zona del sistema de archivos al que tengamos acceso y privilegios para hacerlo.
- Para llevar a cabo operaciones de manera más rápida se suelen usar los denominados atajos de teclado.
  - CTRL+X (Cortar), CTRL+C (Copiar), CTRL+V (Pegar), CTRL+Z(Deshacer)
  - ALT+TAB (Cambiar ventana de aplicación), CTRL+TAB (Cambiar página navegador).
  - +Atajos interesantes: https://openwebinars.net/blog/15-atajos-de-teclado-imprescindibles-para-linux/

Servidores y servicios

- Servidor
  - Es un ordenador y sus programas, estando este al servicio de otros ordenadores.
  - Atiende y responde a las peticiones que les hacen otros ordenadores.
  - Servidor hosting
    - Contratas el servicio de alojamiento, correo electrónico y servicios de Bases de Datos, entre otros
    - Limitados al uso de una aplicación. (En este caso a la aplicación web y alojamiento de email)
    - Generalmente se contrata un servicio en la "nube" que cuente únicamente con alojamiento web. Puede que el servicio de correo no lo tengo el servidor de hosting
  - Servidor dedicado
    - Servidor propio, puedes alojar servicios, página web, correo…
    - La administración de estos servicios es costosa.
    - Es conveniente descentralizar (tener los servicios en distintos servidores para evitar fallos graves)
- Servicio.
  - Generalmente es un proceso dentro del servidor que da respuesta a la petición que recibe.
  - El servicio de correo electrónico (en un servidor de correo) será el encargado de enviar el correo a la persona destino.
  - Ejemplos: Dropbox, correo electrónico, web hosting

Servidores y servicios



Servidores y servicios

- Tipos de servidores
    - Servidores de email
        - Funcionan como una oficina de correos para almacenar, recibir, enviar correos.
        - Son programados para responder efectivamente ante requisitos de los clientes en cuanto al tipo de correo que reciben o envían.
    - **Servidores web**
        - Se encargan de guardar la información en formato HTML (con sus correspondientes procesos PHP, JS, estilos -CSS-...) de los sitios web que se encuentran en internet
        - Ejemplos: **Apache, Nginx**
    - **Servidor de bases de datos**
    - **Servidor FTP**
        - Permite la posibilidad de transferir archivos y datos entre otros ordenadores y servidores.

Instalación de servicios

- Un servidor web es un software que forma parte del servidor y tiene como misión principal devolver información (páginas) cuando recibe peticiones por parte de los usuarios.
- En otras palabras, es el software que permite que los usuarios que quieren ver una página web en su navegador puedan hacerlo.
- Nosotros veremos la gestión e instalación del servidor web (Apache) en Ubuntu.
  - El servidor HTTP Apache es el más usado del mundo.
- Todos los servicios de hosting web que existen nos dan ya el servidor web para hacer públicas (en la web) todas nuestras páginas web.

Empezamos a desarrollar la segunda parte de la actividad…

1. Instala el servidor web Apache en la máquina virtual de Ubuntu.
2. Configúralo para un dominio. Montando un host virtual.
3. Documentad todo el proceso con capturas de pantalla en el Word que se está desarrollando.

Usad de referencia la siguiente página: https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04-es

Empezamos a desarrollar la tercera parte de la actividad…

1. Instala el servidor web SSH en Ubuntu

   Usad de referencia la siguiente página:
   https://www.internetlan.us/2013/02/instalar-y-configurar-ssh-en-ubuntu/

Empezamos a desarrollar la tercera parte de la actividad…

1. Crea un usuario al cual le corresponda actuar de administrador del sitio web
2. Desarrollar dos páginas web sencillas en HTML
   - Subirlas al servidor Apache a la carpeta seleccionada
3. Realizar una petición de las páginas web (con el servidor web Apache activo) desde fuera de la máquina virtual. Es decir, desde un sistema Windows o Mac.

Usad de referencia la siguiente página:
https://www.internetlan.us/2013/02/instalar-y-configurar-ssh-en-ubuntu/

Kahoot final del temario