Práctica 1 – Prepara **tres** máquinas virtuales: una con el sistema operativo Windows 10, otra con el sistema operativo Ubuntu Desktop y otra con el sistema operativo Windows Server 2022.

Seguridad en Windows

Práctica 2 – Desde tu ordenador (host), haz PING a la IP de una de las máquinas virtuales. ¿Qué sucede?

```
CMD → ping IP_MÁQUINA_VIRTUAL
```

a) Si no hay respuesta, configura el firewall de la máquina virtual para que permita la respuesta de PING.
b) Si hay respuesta, configura el firewall de la máquina virtual para que no permita la respuesta de PING.
c) Sobre la regla que permite el PING, abre las propiedades de la misma y mira todas las opciones de configuración para la misma.

Práctica 3 – Agrega una nueva regla que permita:

a) La entrada de conexiones UDP en el puerto 2048, aplicada solo en perfiles de red privados.
b) Las conexiones del programa mspaint.exe deben ser bloqueadas en todos los perfiles de red.
c) Las conexiones del Escritorio remoto deben ser bloqueadas en todos los perfiles de red.
d) El servicio de Hora de Windows no debe usarse con el protocolo IPv6 y en ninguna dirección remota

Práctica 4 – Desactiva el firewall, pero solo en el perfil privado de una de las máquinas virtuales.

Práctica 5 – Comprueba los certificados que tengas instalados en tu equipo Windows.

Práctica 6 – Realiza una copia de seguridad en Windows, guardándola en un medio externo. Simulemos que el sistema ha fallado y que no arranca. Restaura el sistema desde la copia de seguridad.

Práctica 7 – Crea una nueva carpeta (C:\Nuevo).

a) Mira los permisos por defecto.
b) Crea dos usuarios: usu1 y usu2. Crea el grupo grupo1. Mete a los dos usuarios en el grupo1. Agrega al grupo1 los permisos de la carpeta creada anteriormente. Comprueba los permisos que se le han asignado a grupo1.
c) Cambia los permisos de grupo1 para que puedan escribir dentro de la carpeta. Abre una sesión con el usuario usu1 y crea un fichero dentro de la carpeta C:\Nuevo.

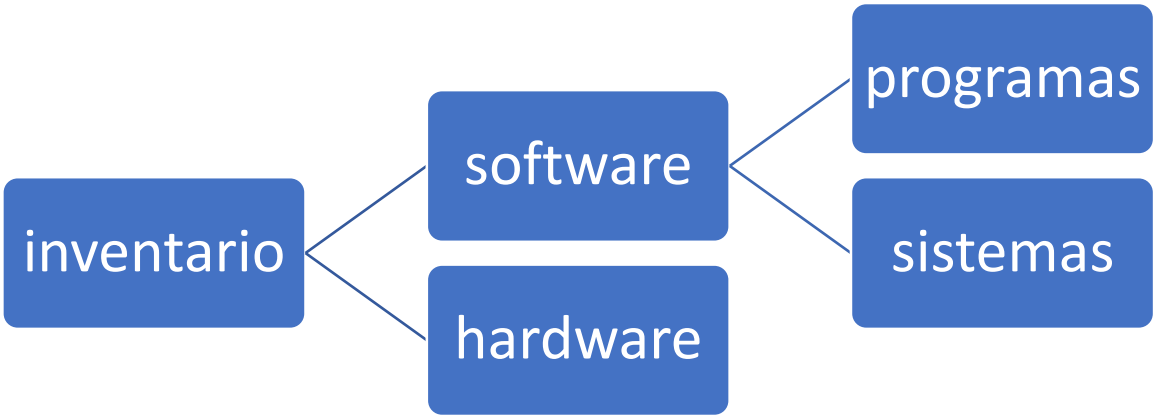
Cierra la sesión y abre otra con el usuario usu2. Borra el fichero creado por el usuario usu1.

d) Con la sesión abierta del usuario usu2 crea un fichero dentro de la carpeta C:\Nuevo. Agrega al grupo grupo1 y al grupo de todos los usuarios los permisos de lectura.
e) Asigna permisos de control total al usuario usu1. Cambia a la sesión del usuario usu1 y quita al grupo1 de los permisos de lectura.
f) Abre una sesión con el administrador y copia el programa notepad.exe a la carpeta C:\Nuevo. Cierra la sesión y abre otra con el usuario usu1. Intenta ejecutar el programa que está dentro de C:\Nuevo. Comprueba los permisos que tiene el usuario usu1 sobre notepad.exe. Intenta ejecutar notepad.exe como administrador.
g) Comprueba los usuarios que tienes dados de alta en el sistema. Comprueba si el usuario invitado está habilitado; si es así, deshabilítalo.
h) Crea un usuario usu3 cuya contraseña no caduque nunca, pero que tenga que cambiarla la primera vez que inicie el sistema. Comprueba si sucede así.

Práctica 8 – Crea una nueva carpeta en la partición de datos. Utiliza los permisos especiales NTFS para que el usuario usu1 tenga control total sobre ella, pero no pueda crear directorios, aunque sí ficheros. Compruébalo.

Práctica 9 – Crea los usuarios prog1 y prog2 que pertenezcan a un grupo llamado programadores. Para el siguiente árbol de directorios:

a) el grupo programadores debe tener como permiso el control total sobre las carpetas por herencia desde inventario.
b) Muestra los permisos en sistemas.
c) Deshabilita la herencia de permisos en la carpeta hardware y haz que sólo prog1 tenga permisos de control total sobre la carpeta hardware y que prog2 tenga sólo permisos de lectura, ejecución y mostrar el contenido de la carpeta.
d) Muestra los permisos de la carpeta hardware.



Seguridad en Linux

Práctica 10 – Lee sobre el comando ufw (***u**ncomplicated **f**ire**w**all*) y, utilizándolo, realiza las siguientes acciones en tu máquina virtual:

a) No permita la conexión por SSH (puerto 22) a tu máquina virtual.
b) Permita la conexión por SSH para la máquina virtual de tu compañero, pero que no la permita para el resto.

c) Muestra el estado del cortafuegos.
d) Deshabilita el firewall.

Práctica 11 – Comprueba los certificados que tengas instalados en tu equipo Linux.

Práctica 12 – Crea un usuario llamado usunuevo y que pertenezca al grupo nuevos. Crea una carpeta en tu directorio personal llamada accesonuevos. Haz que esa carpeta sólo tenga permisos para el propietario:

a) Utiliza las ACL para añadir permisos de lectura, acceso y escritura a los usuarios que pertenezcan al grupo nuevos.
b) Comprueba que puedes acceder a ese directorio como usunuevo y crea un fichero dentro de él.
c) Vuelve a ser tu usuario y elimina la lista de control de acceso creada.

Práctica 13 – Utilizando el comando scp (*secure copy*), copia un archivo que se encuentre en tu máquina virtual a la máquina virtual de un compañero. Previamente, tu compañero te habrá creado un usuario para ti en su máquina virtual

Práctica 14 – Descarga una foto en tu carpeta personal. Ábrela y después elimínala.

a) Descarga SystemRescue y, utilizando la herramienta PhotoRec, trata de recuperar la foto.
b) Pero para esto no necesitamos la ISO de SystemRescue, podemos descargar PhotoRec y ejecutarlo en el sistema Ubuntu

Práctica 15 – Utilizando el software Backups, realiza las siguientes acciones:

a) Realiza una copia del directorio de usuario.
b) Programa una copia del directorio de usuario cada dia.
c) Restaura la copia del directorio

Práctica 16 – Observa los mensajes que ha lanzado el sistema y, de las últimas 10 entradas, identifica a qué se refieren.

Práctica 17 – Cierra la sesión de usuario y trata de iniciarla otra vez, pero equivocándote en la contraseña. Después introduce la contraseña correctamente y busca el log donde ha quedado registrado el evento del intento de acceso.

Cifrado y Hash

Práctica 18 – Crea un fichero de texto con el contenido que tú quieras. Tras realizar los siguientes Hash, cambia el contenido del fichero de texto y vuelve a realizar el Hash. Comprueba el resultado de antes y después en ambos casos:

a) MD5, utilizando el comando md5.
b) SHA-256, utilizando el comando shasum.

Para poder utilizar esos comandos, será necesario instalar previamente el paquete coreutils.

Práctica 19 – Con Wireshark, captura tráfico de:

a) Navegación web a varias páginas utilizando HTTPS.
b) Una conexión SSH entre un ordenador y la VM Linux.
c) Navegación web HTTP.

Después, para la captura de tráfico y filtra los distintos tráficos (según protocolo, direcciones IP, etc.). Comprueba si puedes observar el contenido de los paquetes.

Bonus Track – Crea tu propio *firewall* (y más)

Práctica 20 – Utilizando la distribución pfSense, comprueba lo que puedes hacer con ella, especialmente con:

a) *Firewall*.
b) VPN.
c) Portal cautivo.
d) *Proxy* (usando el *software open source* Squid).

NOTA: Datos de configuración de la red:

a) Interfaz de la máquina virtual: adaptador puente.
b) Dirección IP: DHCP; servidor de DNS: DHCP.

NOTA PARA CUANDO HAYA QUE USAR EL WINDONWS SERVER: configuración de red:

- 10.0.X.Y/24, siendo X tu número de la lista e Y la máquina virtual.
- Adaptador de VirtualBox: internal network.