

FUNDAMENTOS DE TIC Y CIBERSEGURIDAD



CARMEN XIA MARTÍNEZ Y ESPINOSA
PRÁCTICA II – ADMINISTRACIÓN WINDOWS Y LINUX EN VIRTUALBOX
1º GESTIÓN DE LA CIBERSEGURIDAD 2022-23

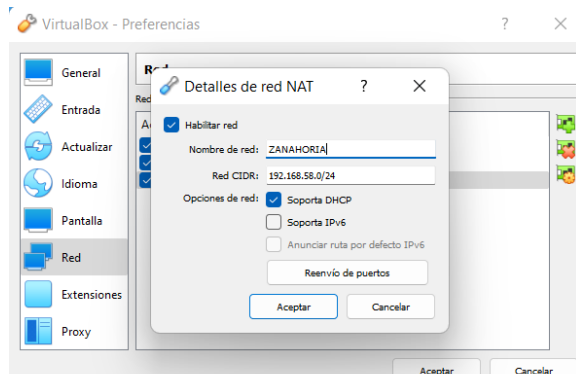
ÍNDICE

Contenido

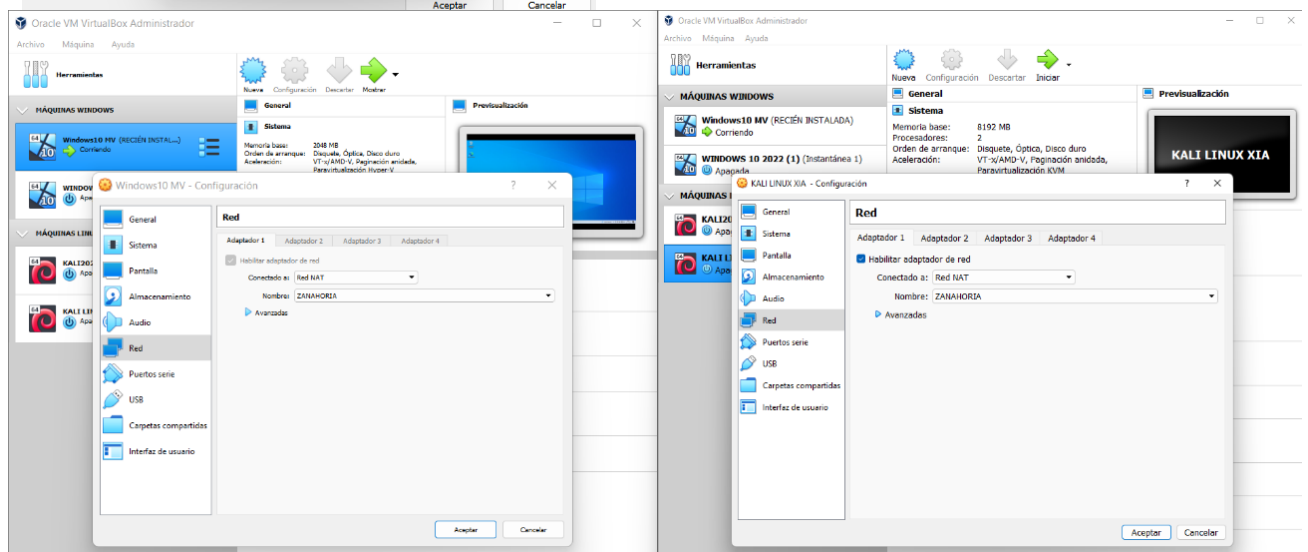
Pregunta 1.....	2
Pregunta 2.....	3
Pregunta 3.....	4
Pregunta 4.....	5
Pregunta 5.....	7
Pregunta 6.....	8
Pregunta 7.....	10
Pregunta 8.....	11
Pregunta 9.....	13
Pregunta 10.....	14

Pregunta 1. Configura una red entre ambas máquinas, en donde la red sea de clase C y el tercer octeto sea 58.

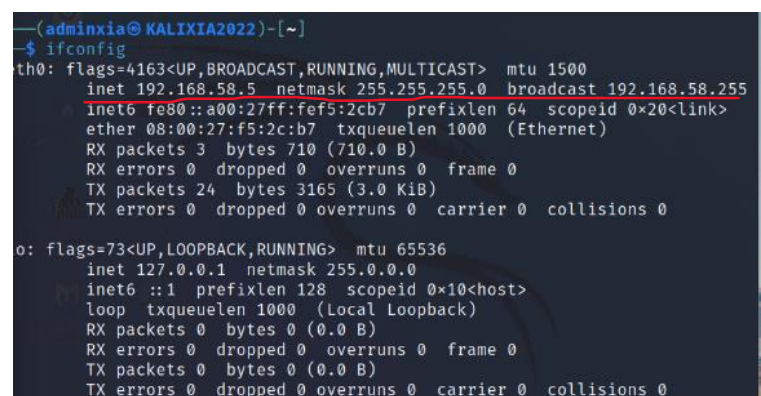
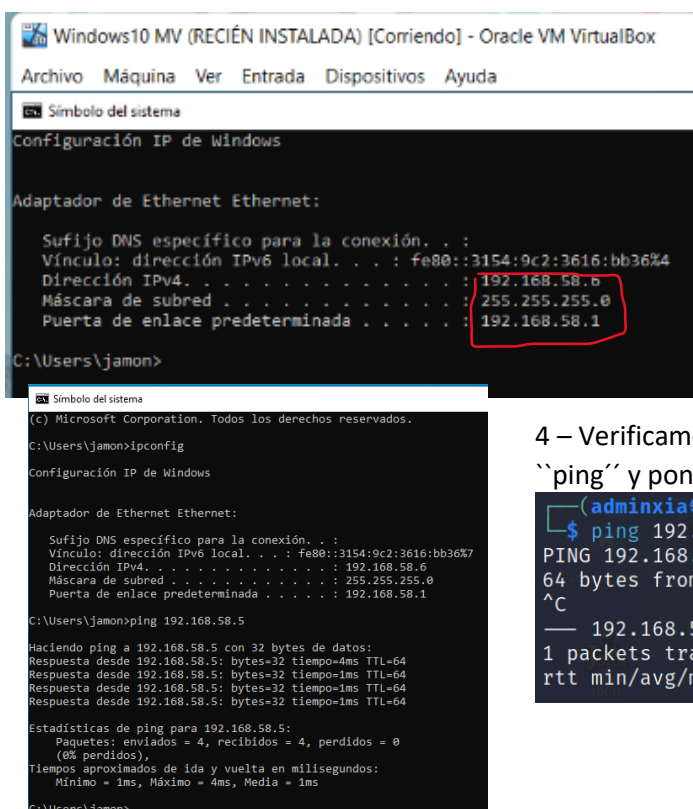
1 - Configuramos red tipo C en preferencias – red de VBOX



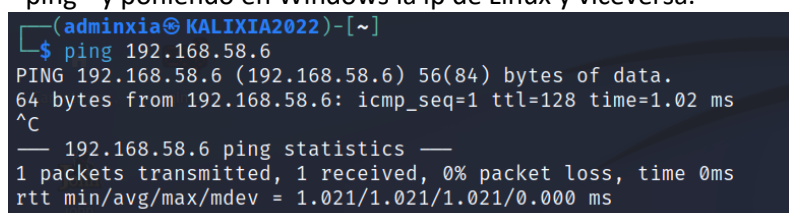
2 – Conectamos las dos máquinas (Windows y Kali a la red ``Zanahoria``)



3 – Iniciamos en Windows el comando ``ipconfig`` y en Linux ``ifconfig``

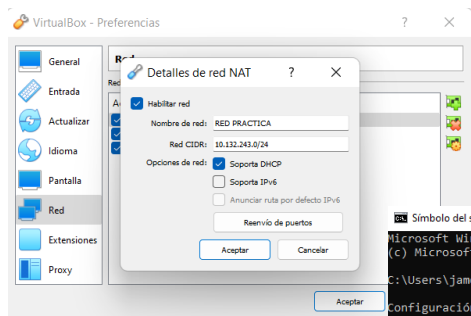


4 – Verificamos la conexión entre ambas haciendo el comando ``ping`` y poniendo en Windows la ip de Linux y viceversa.



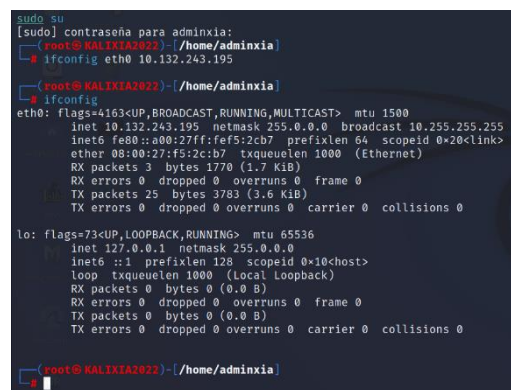
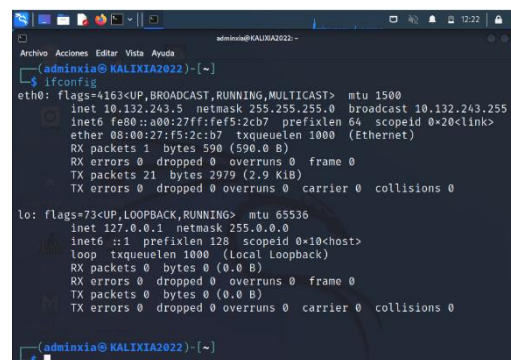
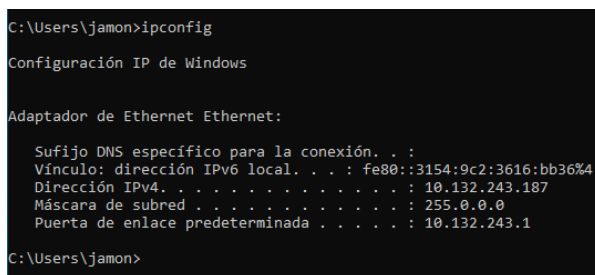
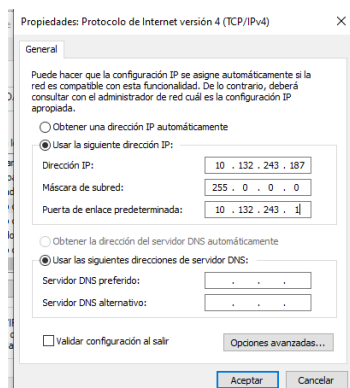
Pregunta 2. Ahora, configura una red tipo A, donde el segundo octeto sea el número 10000100 y el tercer octeto sea el número F3.

- Establece la ip de forma manual en ambas máquinas virtuales, para que tengas una máquina con el cuarto octeto con 10111011 y la otra con 11000011.
- Comprueba que hay conectividad entre ambas de manera bidireccional de nuevo.



1 – Configuramos la red tipo C, donde el segundo octeto es 132 y el tercero es 243 (metemos en la calculadora)

Verificamos en ambas máquinas que están conectadas a la red "Practica"



2 – Configuramos nuestra IP manual en Windows y luego verificamos con el comando ipconfig

Hacemos lo mismo en Linux iniciando como root, y con ifconfig añadimos eth0 y la ip que queramos

Pregunta 3.

- a. Crea un usuario estándar sin privilegios en la máquina Kali y en la máquina Windows. El usuario debe contener tu nombre y tu primer apellido. **Ejemplo. Eduardodiaz.**

```
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>net user Carmenxiamartinez /add
Se ha completado el comando correctamente.
```

```
useradd Carmenxiamartinez

(root@KALIXIA2022)-[/home/adminxia]
# useradd Carmenxiamartinez
useradd: el usuario «Carmenxiamartinez» ya existe
```

- b. Crea un usuario administrador con privilegios en la máquina Kali y en la máquina Windows. El usuario debe contener tu nombre y tu primer apellido.

Ejemplo. Admin.eduardodiaz

```
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>net user adminxia /add
Se ha completado el comando correctamente.
```

```
root@KALIXIA2022: /home/adminxia
Archivo Acciones Editar Vista Ayuda
useradd adminxia2
```

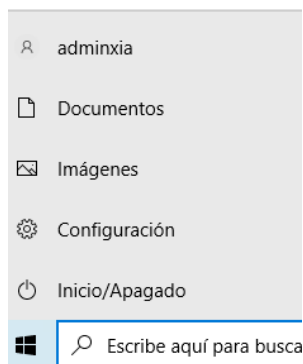
```
# User privilege specification
root    ALL=(ALL:ALL) ALL
adminxia ALL=(ALL:ALL) ALL
adminxia2 ALL=(ALL:ALL) ALL
```

Comando Linux → (root) nano /etc/sudoers

Cuentas de usuario

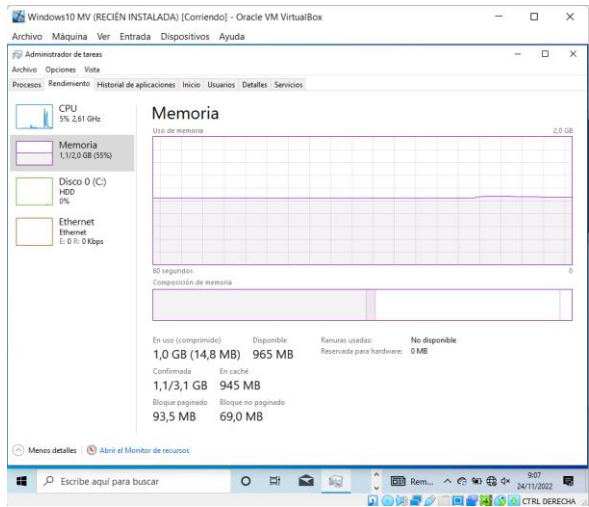
Usuarios	
Opciones avanzadas	
Use la siguiente lista para conceder o denegar acceso de usuario a su equipo, así como para cambiar contraseñas y otras configuraciones.	
Usuarios de este equipo:	
Nombre de usuario	Grupo
adminxia	Administradores
Carmenxiamartinez	Usuarios
jamonserran04@outlook.es	Administradores

- c. Inicia sesión en cada máquina con el usuario administrador que hayas creado.



Pregunta 4 Muestra para cada una de las máquinas virtuales (Windows y Kali) las siguientes características del sistema operativo:

a. Memoria RAM total del equipo y en uso actualmente.



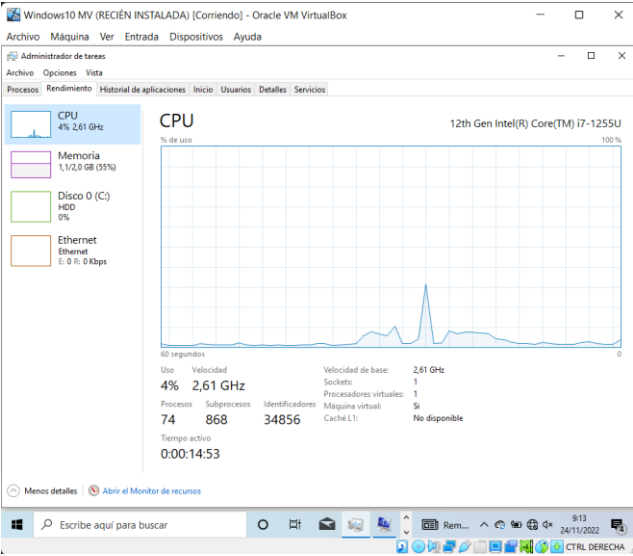
cat/proc/meminfo



```
processor       : 1
vendor_id      : GenuineIntel
cpu family     : 6
model          : 154
model name     : 12th Gen Intel(R) Core(TM) i7-1255U
stepping       : 4
microcode     : 0xffffffff
cpu MHz        : 2611.198
cache size     : 12288 KB
physical id    : 0
siblings       : 2
core id        : 1
cpu cores      : 2
apicid         : 1
initial apicid: 1
fpu            : yes
fpu_exception  : yes
cpuid level    : 22
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca c
mov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc
rep_good nopl xtopology nonstop_tsc cpuid tsc_known_freq pni ssse3 cx16 pci
d sse4_1 sse4_2 hypervisor lahf_lm invpcid_single ibrs_enhanced fsgsbase inv
pcid md_clear flush_l1d arch_capabilities
bugs           : spectre_v1 spectre_v2 spec_store_bypass swapgs
bogomips       : 5222.39
clflush size   : 64
cache alignment: 64
address sizes  : 39 bits physical, 48 bits virtual
power management:

(adminxia@KALIXIA2022)-[~]
$
```

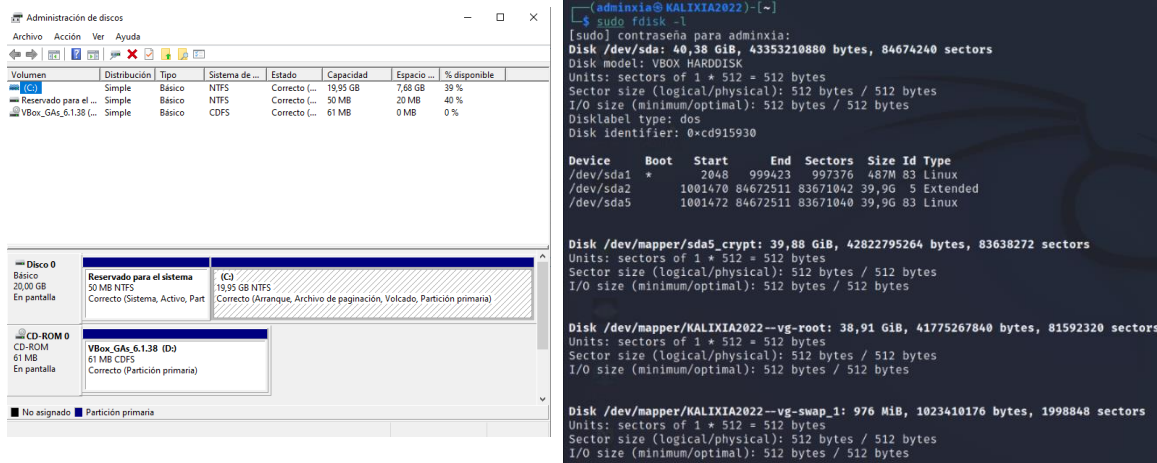
b. Procesador. Tipo de procesador y uso actualmente.



```
(adminxia@KALIXIA2022)-[~]
$ cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 154
model name     : 12th Gen Intel(R) Core(TM) i7-1255U
stepping       : 4
microcode     : 0xffffffff
cpu MHz        : 2611.198
cache size     : 12288 KB
physical id    : 0
siblings       : 2
core id        : 0
cpu cores      : 2
apicid         : 0
initial apicid: 0
fpu            : yes
fpu_exception  : yes
cpuid level    : 22
wp             : yes
flags          : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca c
mov pat pse36 clflush mmx fxsr sse sse2 ht syscall nx rdtscp lm constant_tsc
rep_good nopl xtopology nonstop_tsc cpuid tsc_known_freq pni ssse3 cx16 pci
d sse4_1 sse4_2 hypervisor lahf_lm invpcid_single ibrs_enhanced fsgsbase inv
pcid md_clear flush_l1d arch_capabilities
bugs           : spectre_v1 spectre_v2 spec_store_bypass swapgs
bogomips       : 5222.39
clflush size   : 64
cache alignment: 64
address sizes  : 39 bits physical, 48 bits virtual
power management:

processor       : 1
```

c. Espacio en disco y particiones. Mostrar la velocidad de lectura y escritura de este.



The image shows two screenshots. The left screenshot is a Windows Disk Management window titled 'Administración de discos'. It displays a list of volumes with columns for Volume, Distribution, Type, File System, Status, Capacity, Space, and % Free. The right screenshot is a terminal window showing the output of the 'fdisk -l' command. It lists disk information for /dev/sda, /dev/sda1, /dev/sda2, /dev/sda5, /dev/mapper/sda5_crypt, /dev/mapper/KALIXIA2022--vg-root, and /dev/mapper/KALIXIA2022--vg-swap_1.

Volume	Distribución	Tipo	Sistema de...	Estado	Capacidad	Espacio	% disponible
(C:)	Simple	Básico	NTFS	Correcto (...)	19.95 GB	7.68 GB	39 %
Reservado para el ...	Simple	Básico	NTFS	Correcto (...)	50 MB	20 MB	40 %
VBox_GAs_6.1.38 (...)	Simple	Básico	CDFS	Correcto (...)	61 MB	0 MB	0 %

```

[admin@KALIXIA2022:~]$ sudo fdisk -l
[sudo] contraseña para admin:
Disk /dev/sda: 40,38 GiB, 4353210880 bytes, 84674240 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xcd915930

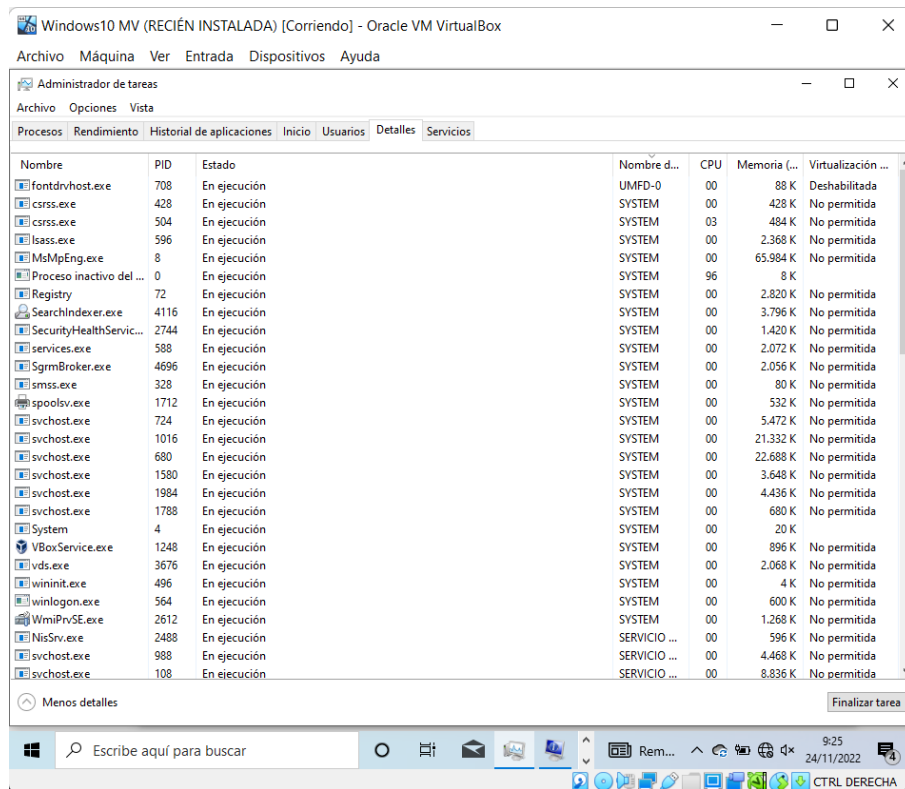
Device Boot      Start         End      Sectors  Size Id Type
/dev/sda1 *        2048     999423     997376    487M 83 Linux
/dev/sda2          1001470 84672511 83671042   39,9G  5 Extended
/dev/sda5          1001472 84672511 83671040   39,9G 83 Linux

Disk /dev/mapper/sda5_crypt: 39,88 GiB, 42822795264 bytes, 83638272 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/KALIXIA2022--vg-root: 38,91 GiB, 41775267840 bytes, 81592320 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/KALIXIA2022--vg-swap_1: 976 MiB, 1023410176 bytes, 1998848 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
  
```

c. Muestra los procesos que están corriendo en el sistema Windows, cuyo usuario propietario es SYSTEM.



The image shows a screenshot of the Windows Task Manager window titled 'Windows 10 MV (RECÍEN INSTALADA) [Corriendo] - Oracle VM VirtualBox'. The 'Procesos' tab is selected, showing a list of running processes with columns for Name, PID, Estado, Nombre de usuario, CPU, Memoria, and Virtualización. The processes are sorted by CPU usage.

Nombre	PID	Estado	Nombre de usuario	CPU	Memoria	Virtualización
fontdrvhost.exe	708	En ejecución	SYSTEM	00	88 K	Deshabilitada
csrss.exe	428	En ejecución	SYSTEM	00	428 K	No permitida
csrss.exe	504	En ejecución	SYSTEM	03	484 K	No permitida
lsass.exe	596	En ejecución	SYSTEM	00	2.368 K	No permitida
MsMpEng.exe	8	En ejecución	SYSTEM	00	65.984 K	No permitida
Proceso inactivo del ...	0	En ejecución	SYSTEM	96	8 K	No permitida
Registry	72	En ejecución	SYSTEM	00	2.820 K	No permitida
SearchIndexer.exe	4116	En ejecución	SYSTEM	00	3.796 K	No permitida
SecurityHealthService...	2744	En ejecución	SYSTEM	00	1.420 K	No permitida
services.exe	588	En ejecución	SYSTEM	00	2.072 K	No permitida
SgrmBroker.exe	4696	En ejecución	SYSTEM	00	2.056 K	No permitida
smss.exe	328	En ejecución	SYSTEM	00	80 K	No permitida
spoolsv.exe	1712	En ejecución	SYSTEM	00	532 K	No permitida
svchost.exe	724	En ejecución	SYSTEM	00	5.472 K	No permitida
svchost.exe	1016	En ejecución	SYSTEM	00	21.332 K	No permitida
svchost.exe	680	En ejecución	SYSTEM	00	22.688 K	No permitida
svchost.exe	1580	En ejecución	SYSTEM	00	3.648 K	No permitida
svchost.exe	1984	En ejecución	SYSTEM	00	4.436 K	No permitida
svchost.exe	1788	En ejecución	SYSTEM	00	680 K	No permitida
System	4	En ejecución	SYSTEM	00	20 K	No permitida
VBoxService.exe	1248	En ejecución	SYSTEM	00	896 K	No permitida
vds.exe	3676	En ejecución	SYSTEM	00	2.068 K	No permitida
wininit.exe	496	En ejecución	SYSTEM	00	4 K	No permitida
winlogon.exe	564	En ejecución	SYSTEM	00	600 K	No permitida
WmiPrvSE.exe	2612	En ejecución	SYSTEM	00	1.268 K	No permitida
NisSrv.exe	2488	En ejecución	SERVICIO ...	00	596 K	No permitida
svchost.exe	988	En ejecución	SERVICIO ...	00	4.468 K	No permitida
svchost.exe	108	En ejecución	SERVICIO ...	00	8.836 K	No permitida

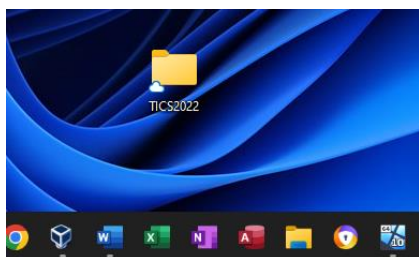
Pregunta 5.

a. Crea una partición de 4 Gb en la máquina Windows con el sistema de archivos NTFS.

b. Crea una partición de 4 Gb en la máquina Kali con el sistema de archivos EXT4.

Pregunta 6.

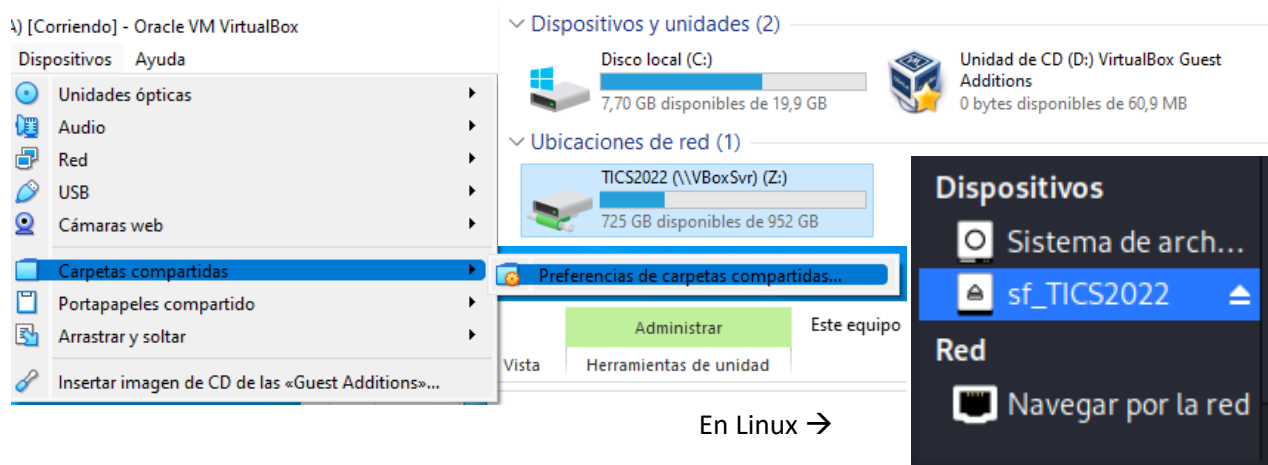
- a. Configura una carpeta compartida entre ambas máquinas y el host anfitrión. La carpeta compartida debe llamarse "TICS2022".



En nuestro ordenador físico creamos la carpeta. "TICS2022".

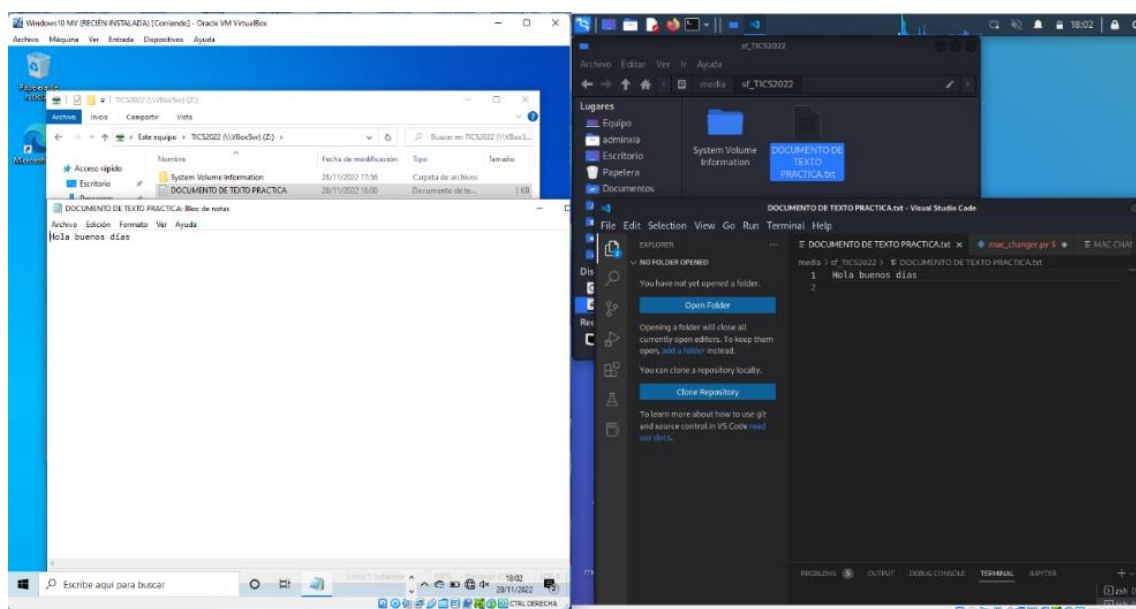
En VBOX, en la máquina WINDOWS, en dispositivos insertamos la imagen de las guest additions y instalamos la versión de 64 bits. Reiniciamos la máquina.

Añadimos nuestra carpeta compartida a la máquina virtual.



En Linux →

- b. Crea un archivo de texto en la máquina Windows y ábrelo desde la máquina Linux.



c) Crea un archivo de texto desde la máquina Linux, y ábrelo con la máquina anfitriona.

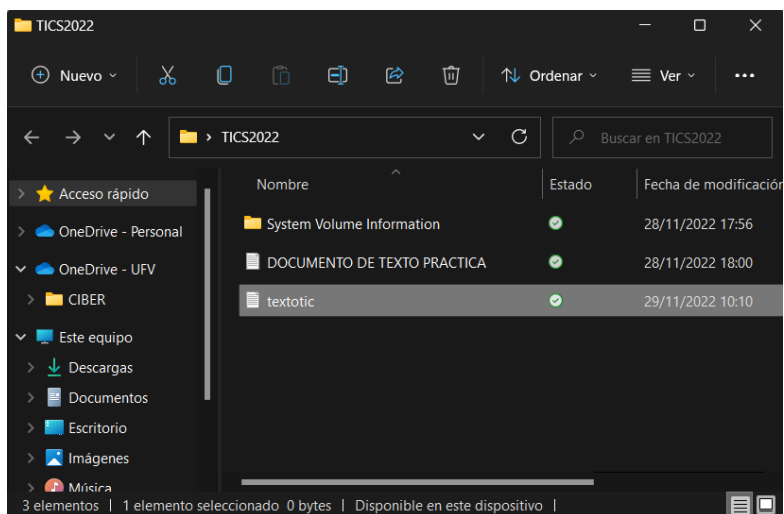
```
adminixia@KALIXIA2022: /media/sf_TICS2022
$ cd ..
$ ls
bin          home          libx32       proc         temp
boot        initrd.img    lost+found   root         usr
carpetcomidaescritorio lib          mnt          sbin         vmlinuz
dev          lib32         opt          srv           vmlinuz.old
etc          lib64         PATATA       sys

$ cd /media/sf_TICS2022/
$ ls
LS: command not found

$ ls
'DOCUMENTO DE TEXTO PRACTICA.txt' 'System Volume Information'

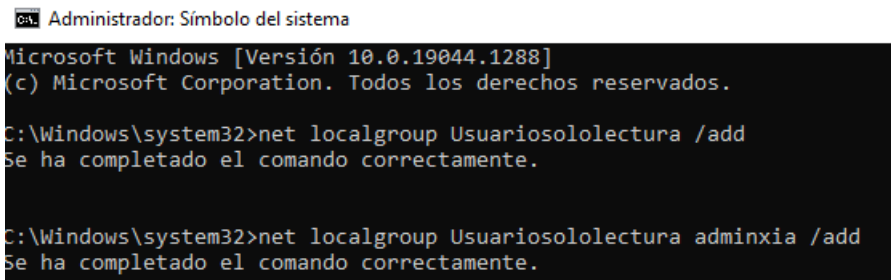
$ touch textotic.txt

$ ls
'DOCUMENTO DE TEXTO PRACTICA.txt' textotic.txt
'System Volume Information'
```



Pregunta 7.

- a. Crea un grupo de usuarios en la máquina Windows llamado “UsuariosSoloLectura” en el que incluyas al usuario estándar sin privilegios que generaste en la tercera pregunta.



```
ca. Administrador: Símbolo del sistema

Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>net localgroup Usuariosololectura /add
Se ha completado el comando correctamente.

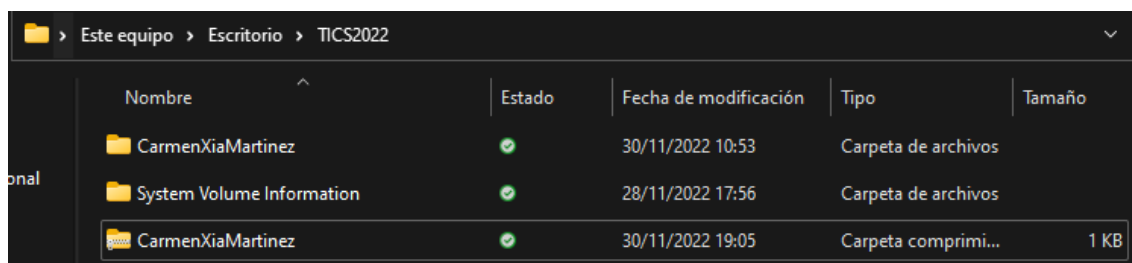
C:\Windows\system32>net localgroup Usuariosololectura adminxia /add
Se ha completado el comando correctamente.
```

- b. Crea una carpeta llamada “MisSecretos” en la nueva partición creada en la máquina Windows (4GB) y establece permisos y privilegios de solo lectura al grupo que has creado y crea un fichero dentro con extensión txt.

Pregunta 8. Desde la máquina Windows, en la carpeta compartida creada en la sexta pregunta de la presente práctica.

- Crea un directorio “NOMBRE+APELLIDOSALUMNO” con un archivo dentro y comprímelo en cualquiera de los formatos vistos durante el curso

Creación carpeta y comprimir haciendo clic derecho sobre ella (formato zip) →



- Descomprímelo en la máquina Kali Linux en una carpeta que crees en el escritorio del usuario que estás manejando.

Creación de carpeta en el escritorio

Descomprimir la carpeta.

```
(adminxia@KALIXIA2022)-[~]
$ cd Escritorio

(adminxia@KALIXIA2022)-[~/Escritorio]
$ ls
CARPETA2004          kali-nmap.desktop
'Documento texto tic' kali-sqlmap.desktop
kali-aircrack-ng.desktop org.wireshark.Wireshark.desktop
kali-hydra.desktop    'PRUEBAS LINUX '
kali-john.desktop      sf_TICS2022
kali-msfconsole.desktop

(adminxia@KALIXIA2022)-[~/Escritorio]
$ mkdir Carmenxiamartinezdescomprimida

(adminxia@KALIXIA2022)-[~/Escritorio]
$ ls
Carmenxiamartinezdescomprimida | kali-msfconsole.desktop
CARPETA2004                    kali-nmap.desktop
'Documento texto tic'         kali-sqlmap.desktop
kali-aircrack-ng.desktop      org.wireshark.Wireshark.desktop
kali-hydra.desktop            'PRUEBAS LINUX '
kali-john.desktop              sf_TICS2022
```

```
ls
CarmenXiaMartinez      'Nuevo documento de texto.txt'
CarmenXiaMartinez.zip  'System Volume Information'
'DOCUMENTO DE TEXTO PRACTICA.txt' textotit.txt

(adminxia@KALIXIA2022)-[~/Escritorio/sf_TICS2022]
$ unzip CarmenXiaMartinez.zip
Archive: CarmenXiaMartinez.zip
extracting: Carmen Xia Martinez/Textopregunta.txt

(adminxia@KALIXIA2022)-[~/Escritorio/sf_TICS2022]
$ ls
'Carmen Xia Martinez' 'DOCUMENTO DE TEXTO PRACTICA.txt' textotit.txt
CarmenXiaMartinez    'Nuevo documento de texto.txt'
CarmenXiaMartinez.zip 'System Volume Information'

(adminxia@KALIXIA2022)-[~/Escritorio/sf_TICS2022]
$ cd CarmenXiaMartinez

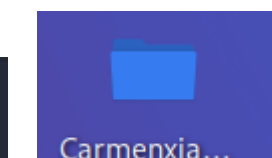
(adminxia@KALIXIA2022)-[~/Escritorio/sf_TICS2022/CarmenXiaMartinez]
$ ls
Textopregunta.txt
```

Mover la carpeta al escritorio (debido a un error no me dejaba, he movido la carpeta del escritorio a la compartida y de ahí al escritorio de nuevo).

```
(adminxia@KALIXIA2022)-[/media/sf_TICS2022]
$ sudo su
[sudo] contraseña para adminxia:

(root@KALIXIA2022)-[/media/sf_TICS2022]
# mv CarmenXiaMartinez /Carmenxiamartinezdescomprimida

(root@KALIXIA2022)-[/media/sf_TICS2022]
# mv Carmenxiamartinezdescomprimida /Escritorio
```



```
(root@KALIXIA2022)-[/]
# cd Escritorio

(root@KALIXIA2022)-[/Escritorio]
# ls
Carmenxiamartinezdescomprimida Textopregunta.txt
```

- c. Revisa los permisos al archivo que hay dentro del directorio en la máquina Kali Linux y quítale todos los permisos de lectura. Comprueba que no se puede leer el contenido.

```
(adminxia@KALIXIA2022)-[~/Escritorio/Carmenxiamartinezdescomprimida/CarmenXiaMartinez]
$ ls -l Textopregunta.txt
--w-r--r-- 1 adminxia adminxia 0 nov 30 19:48 Textopregunta.txt

(adminxia@KALIXIA2022)-[~/Escritorio/Carmenxiamartinezdescomprimida/CarmenXiaMartinez]
$
```

- d. Ahora establece permisos al fichero para que solo el usuario pueda leer, escribir y ejecutar, y el resto de los grupos y usuarios solo puedan leerlo.

```
chmod 744 Textopregunta.txt

(adminxia@KALIXIA2022)-[~/Escritorio/Carmenxiamartinezdescomprimida/CarmenXiaMartinez]
$ ls -l
total 0
-rwxr--r-- 1 adminxia adminxia 0 nov 30 19:48 Textopregunta.txt

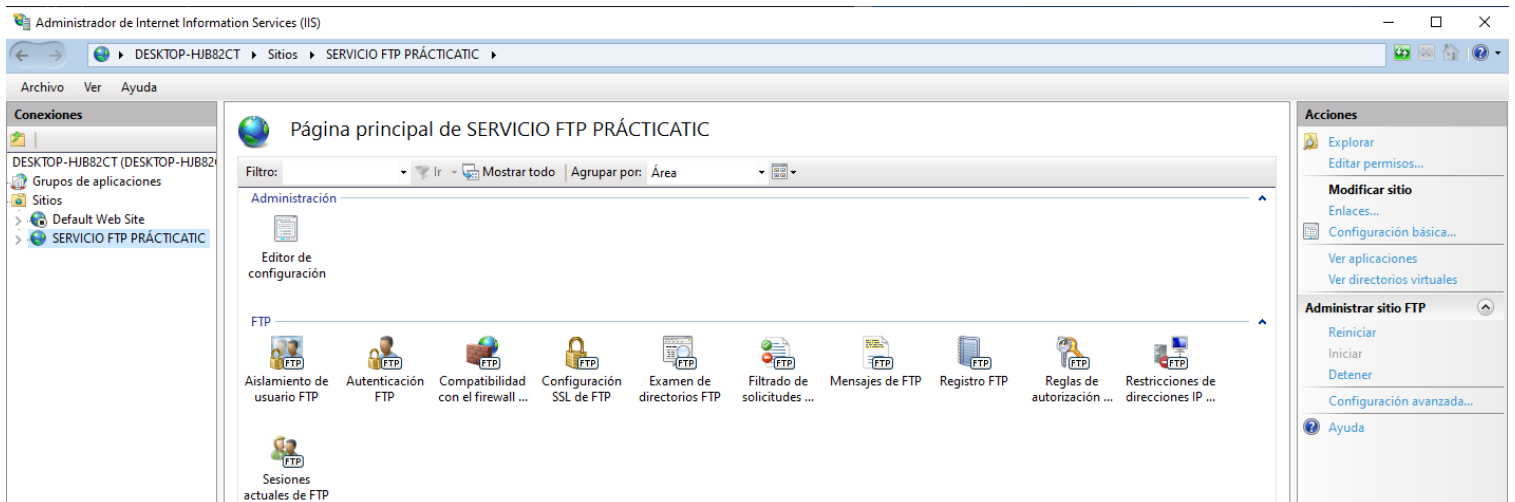
(adminxia@KALIXIA2022)-[~/Escritorio/Carmenxiamartinezdescomprimida/CarmenXiaMartinez]
$ ls -l Textopregunta.txt
-rwxr--r-- 1 adminxia adminxia 0 nov 30 19:48 Textopregunta.txt
```

Pregunta 9. Crea un servidor ftp (Pista: Recomendable instalar la aplicación Filezilla Server) en la máquina Windows.

- a. Configura el servicio con un usuario y una carpeta donde se alojen todos los ficheros a utilizar en el servidor ftp.

```
C:\Users\jamon>ftp 10.0.2.15
Conectado a 10.0.2.15.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
Usuario (10.0.2.15:(none)): jamonserran04@outlook.es
331 Password required
```

- b. Deshabilita el Firewall de Windows y conéctate desde la máquina Kali Linux al servicio FTP montado y copia un fichero a tu elección.



- c. Habilita el Firewall de Windows de nuevo y configura los accesos para que siga funcionando el servicio.

- d. ¿Qué puerto de conexión utiliza el protocolo FTP?

Pregunta 10. Crea un servidor ftp en la máquina Kali Linux.

- a. Conéctate desde la máquina Windows desde un cliente ftp.
- b. Conéctate desde la máquina Windows desde un navegador web (no válido Internet Explorer ni Microsoft Edge).