

# Fundamentos de las TICs y la Ciberseguridad



Eduardo Díaz-Mayordomo

Francisco De Santos

Facultad de CC. Jurídicas y Empresariales

Universidad Francisco de Vitoria

Grado en Gestión de la Ciberseguridad.

## CLASE PRÁCTICA ADMINISTRACIÓN LINUX

Nombre Alumno: Xia Martínez Espinosa

1. Actualizar la máquina virtual con todos los parches habilitados en el repositorio de Kali Linux.

```
Archivo Acciones Editar Vista Ayuda
zsh: corrupt history file /home/adminxia/.zsh_history
(adminxia@KALIXIA2022)-[~]
$ sudo apt-get update
[sudo] contraseña para adminxia:
Des:1 http://packages.microsoft.com/repos/code stable InRelease [10,4 kB]
Des:2 http://packages.microsoft.com/repos/code stable/main armhf Packages [118 kB]
Des:3 http://packages.microsoft.com/repos/code stable/main arm64 Packages [116 kB]
Des:4 http://packages.microsoft.com/repos/code stable/main amd64 Packages [116 kB]
Des:5 http://packages.microsoft.com/repos/code stable/main arm64 Contents (deb) [55,5 kB]
Des:6 http://packages.microsoft.com/repos/code stable/main armhf Contents (deb) [55,5 kB]
Des:7 http://packages.microsoft.com/repos/code stable/main amd64 Contents (deb) [55,5 kB]
Des:8 http://kali.download/kali kali-rolling InRelease [30,6 kB]
Des:9 http://kali.download/kali kali-rolling/main amd64 Packages [18,7 MB]
Des:10 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [43,3 MB]
Des:11 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Des:12 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [161 kB]
Des:13 http://kali.download/kali kali-rolling/non-free amd64 Packages [234 kB]
Des:14 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [897 kB]
Descargados 44,7 MB en 28s (1,628 kB/s)
Leyendo lista de paquetes... Hecho
(adminxia@KALIXIA2022)-[~]
```

2. Localiza si existe un usuario que se llame ufv

```
(adminxia@KALIXIA2022)-[~]
$ cd ufv
cd: no existe el fichero o el directorio: ufv
(adminxia@KALIXIA2022)-[~]
$
```

3. Crear un usuario sin privilegios con el siguiente nombre de usuario:

- Nombre + "." + Primer Apellido del alumno.

```
useradd: Permission denied.
useradd: no se pudo bloquear /etc/passwd, inténtelo de nuevo.
(adminxia@KALIXIA2022)-[~]
$ sudo useradd Xia_Martinez
(adminxia@KALIXIA2022)-[~]
$ cd Xia_Martinez
cd: no existe el fichero o el directorio: Xia_Martinez
(adminxia@KALIXIA2022)-[~]
$ sudo useradd Xia_Martinez
useradd: el usuario «Xia_Martinez» ya existe
(adminxia@KALIXIA2022)-[~]
$ whoami
adminxia
```

# Fundamentos de las TICs y la Ciberseguridad

Eduardo Díaz Mayordomo

Francisco De Santos

Facultad de CC. Jurídicas y Empresariales

Universidad Francisco de Vitoria

Grado en Gestión de la Ciberseguridad.

4. Incluir al nuevo usuario dentro del fichero sudoers y comprobar que podemos elevar privilegios.

```
(adminxia@KALIXIA2022)-[~]
$ sudo cat /etc/sudoers

This file MUST be edited with the 'visudo' command as root.
Please consider adding local content in /etc/sudoers.d/ instead of
directly modifying this file.
See the man page for details on how to write a sudoers file.

Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
Defaults    use_pty

# This preserves proxy settings from user environments of root
# equivalent users (group sudo)
Defaults:%sudo env_keep += "http_proxy https_proxy ftp_proxy all_proxy no_proxy"

# This allows running arbitrary commands, but so does ALL, and it means
# different sudoers have their choice of editor respected.
Defaults:%sudo env_keep += "EDITOR"

# Completely harmless preservation of a user preference.
Defaults:%sudo env_keep += "GREP_COLOR"

# While you shouldn't normally run git as root, you need to with etckeeper
Defaults:%sudo env_keep += "GIT_AUTHOR_* GIT_COMMITTER_*"

# Per-user preferences; root won't have sensible values for them.
Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
Defaults:%sudo env_keep += "GPG_AGENT_INFO"

Host alias specification

User alias specification

Cmd alias specification

User privilege specification
root    ALL=(ALL:ALL) ALL
EPE     ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
```

5. Modifica la contraseña de tu usuario.

```
(adminxia@KALIXIA2022)-[~]
$ sudo passwd root
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
```

6. Crea una carpeta en el directorio /home/usuario llamada "UFVKALI" y otra llamada "UFVUSER" utilizando sólo un comando.

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

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

(adminxia@KALIXIA2022)-[~/Escritorio]
$ pwd
/home/adminxia/Escritorio

(adminxia@KALIXIA2022)-[~/Escritorio]
$ ls
UFVKALI  UFVUSER
```



# Fundamentos de las TICs y la Ciberseguridad

7. Y 8. Muestra el contenido del directorio anterior sin cambiar el directorio actual.

```
(adminxia@KALIXIA2022)-[~/Escritorio]
$ ls Escritorio
ls: no se puede acceder a 'Escritorio': No existe el directorio

(adminxia@KALIXIA2022)-[~/Escritorio]
$ cat file1
cat: file1: No existe el fichero o el directorio

(adminxia@KALIXIA2022)-[~/Escritorio]
$ cat Escritorio
cat: Escritorio: No existe el fichero o el directorio

(adminxia@KALIXIA2022)-[~/Escritorio]
$ ls
UFVKALI  UFVUSER

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

De Santos  
resariales  
de Vitoria  
seguridad.

8. Muestra el directorio actual en el que estás trabajando.

(Respondida en la 7)

9. Comprueba con qué usuario estás trabajando.

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

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

10. Muestra la versión de kernel.

```
(adminxia@KALIXIA2022)-[~/Escritorio]
$ uname -r
5.18.0-kali5-amd64
```



# Fundamentos de las TICs y la Ciberseguridad

Eduardo Díaz-Mayordomo

11. Muestra la fecha y hora actuales.

```
(adminxia@KALIXIA2022)-[~/Escritorio]
$ date
vie 28 oct 2022 08:52:24 CEST
```

12. Muestra todos los archivos del directorio /bin que empiecen por c. Hazlo desde el directorio en el que te encuentras.

13. Crea el fichero "usuario.txt" en el directorio /UFVUSER, y quítale todos los permisos de lectura.

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

(adminxia@KALIXIA2022)-[~/Escritorio/UFVUSER]
$ touch usuario.txt

(adminxia@KALIXIA2022)-[~/Escritorio/UFVUSER]
$ ls
usuario.txt
```

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVUSER]
$ chmod usuario.txt -r
```

14. Borra la carpeta "UFVUSER".

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVUSER]
$ ..

(adminxia@KALIXIA2022)-[~/Escritorio]
$ rm -R UFVUSER

(adminxia@KALIXIA2022)-[~/Escritorio]
$ ls
UFVKALI

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



# Fundamentos de las TICs y la Ciberseguridad

15. Crear un fichero llamado "documento.txt" en el directorio /UFVKALI. Eduardo Díaz-Mayordomo

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ touch documento.txt

(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ ls
documento.txt

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

16. Edita el fichero e incluye cinco frases cuales quieras.

```
GNU nano 6.3
Hola buenos días
Que tal
PATATAS con Huevos
HOLA caracola
Jamón serrano, que rico
```

17. Muestra el contenido del archivo sin abrirlo.

18. Busca si hay alguna frase que contenga la palabra "que" dentro de documento.txt

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ find / -name documento.txt que
find: paths must precede expression: `que'
```

19. Muestra los permisos del fichero y el propietario del mismo.

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ ls -l documento.txt
-rw-r--r-- 1 adminxia adminxia 0 oct 28 09:12 documento.txt
```

20. Establece los siguientes permisos al fichero "documento.txt"

- Lectura, escritura y ejecución a nivel de usuario.
- Lectura a nivel de grupo
- Lectura y ejecución para permisos especiales

# Fundamentos de las TICs y la Ciberseguridad

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ chmod -r documento.txt

(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ chmod -w documento.txt
chmod: no se puede acceder a 'documento.txt': No existe el fichero o el directorio

(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ ls
documento.txt  documento.txt.save

(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ chmod -w documento.txt

(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ chmod -x documento.txt
```

21. Cambiar el propietario del fichero a otro usuario de la máquina.

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ chown Xia_Martinez documento.txt
chown: cambiando el propietario de 'documento.txt': Operación no permitida

(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ sudo chown Xia_Martinez documento.txt
[sudo] contraseña para adminxia:
```

22. Comprime el fichero “documento.txt” en formato Gunzip y TAR.

23. Mueve el fichero tar creado a la carpeta “/HOME/nombre.apellido”.

24. Borra el fichero “documento.txt”.

25. Descomprime el fichero en formato Gunzip o TAR.

26. Muestra información detallada del comando df.

27. Qué opciones, combinaciones, tenemos con el comando df.



# Fundamentos de las TICs y la Ciberseguridad

Eduardo Díaz-Mayordomo

Francisco De Santos

28. Muestra las particiones montadas.

```
(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ df -h
S.ficheros          Tamaño Usados  Disp Uso% Montado en
udev                3,9G      0    3,9G  0% /dev
tmpfs               796M    984K   795M  1% /run
/dev/mapper/KALIXIA2022--vg-root 38G    13G    24G 36% /
tmpfs               3,9G      0    3,9G  0% /dev/shm
tmpfs               5,0M      0    5,0M  0% /run/lock
/dev/sda1           455M    84M   347M 20% /boot
tmpfs               796M    80K   796M  1% /run/user/1000

(adminxia@KALIXIA2022)-[~/Escritorio/UFVKALI]
$ df -i
S.ficheros          Nodos-i NUsados NLibres NUsa% Montado en
udev              1008967   412 1008555   1% /dev
tmpfs             1018305   690 1017615   1% /run
/dev/mapper/KALIXIA2022--vg-root 2550912 368168 2182744 15% /
tmpfs             1018305     1 1018304   1% /dev/shm
tmpfs             1018305     3 1018302   1% /run/lock
tmpfs             124440    361 124079   1% /boot
/dev/sda1         203661     91 203570   1% /run/user/1000
```

29. Muestra las conexiones de red y servicios activos en el sistema.

30. Obtener la siguiente información de la máquina:

- Las tareas con máximo consumo de CPU.
- Las tareas en forma de árbol.
- La memoria que está consumiendo y la memoria libre que tiene el sistema.
- Información del procesador y la memoria ram.

31. Cómo cambiarías la dirección MAC del adaptador de red de la máquina virtual.

32. Cómo cambiarías la ip de tu máquina virtual

# Fundamentos de las TICs y la Ciberseguridad

33. Como reiniciarías y apagarías tu equipo por comando

Eduardo Díaz-Mayordomo

Francisco De Santos

Facultad de CC. Jurídicas y Empresariales



```
(adminxia@KALIXIA2022)-[~]  
$ shutdown -h now  
  
(adminxia@KALIXIA2022)-[~]  
$ shutdown -r now
```

El primer comando lo apaga, el segundo comando lo reinicia