1. Documentar

La información es fundamental, por lo que tomar notas y tener organizada la información que se va obteniendo durante un *pentest* es muy importante. Se recomienda que se documente absolutamente todo, incluyendo la salida de la terminal y capturas de pantalla de aquello que se considere importante. Hay que tener claro que:

- toda esta información recopilada se analizará y servirá para la elaboración del informe final a entregar al cliente.
- documentar nuestras acciones y las salidas correspondientes permite interactuar con el objetivo no más de lo necesario, ayudando a ser sigilosos (*stealth*) durante la auditoría.
- tener información detallada y organizada sobre los objetivos, facilita enormemente el trabajo del auditor. Por ejemplo, en la fase de postexplotación se podrían ver relaciones existentes entre distintos sistemas de la organización objetivo.

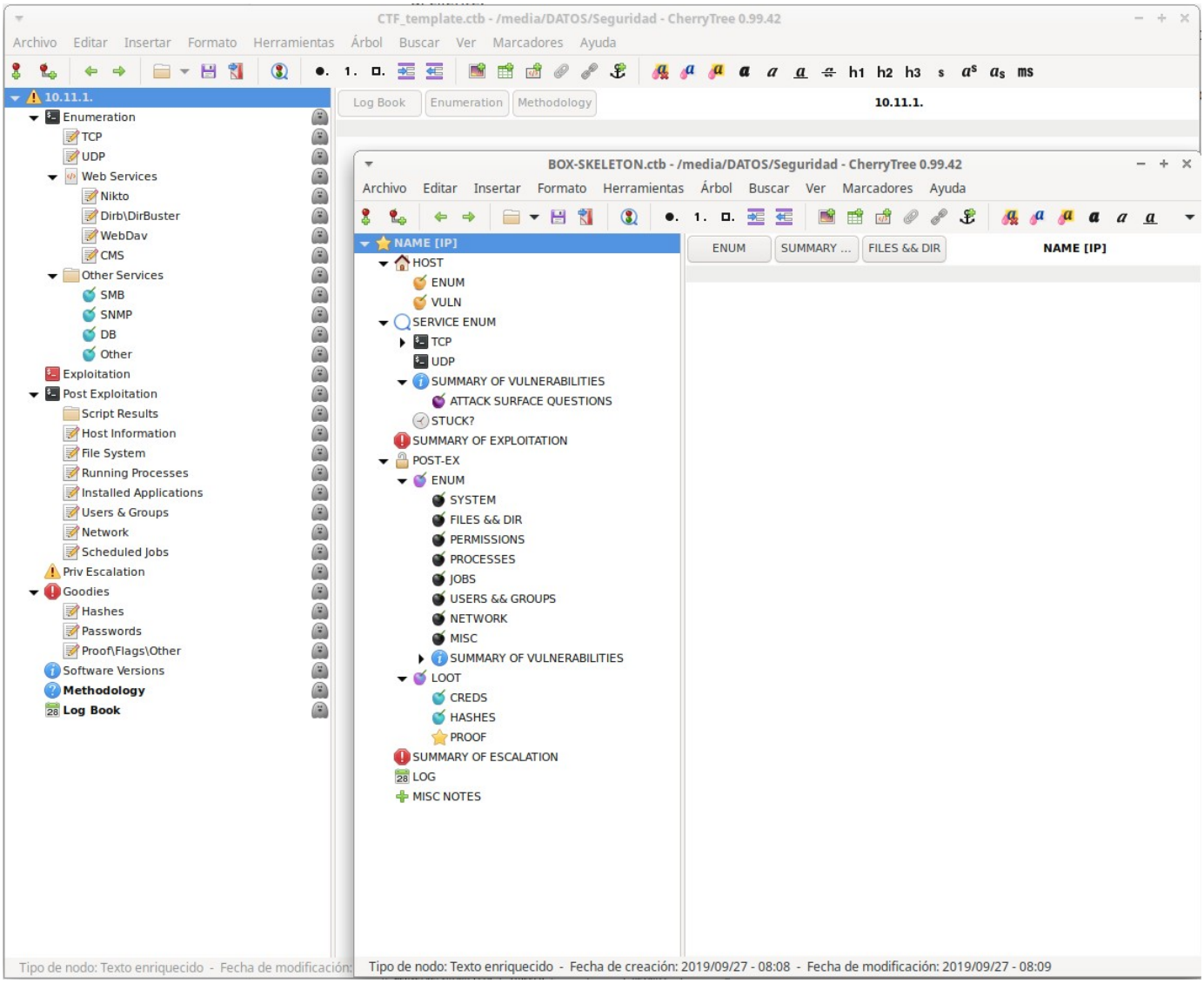
2. Herramientas para notas

Cherrytree

Cherrytree es una aplicación multiplataforma que permite tomar notar creando una estructura de árbol, existiendo plantillas especialmente diseñadas para pentesting:

- CTF_template.ctb
- BOX-Skeleton

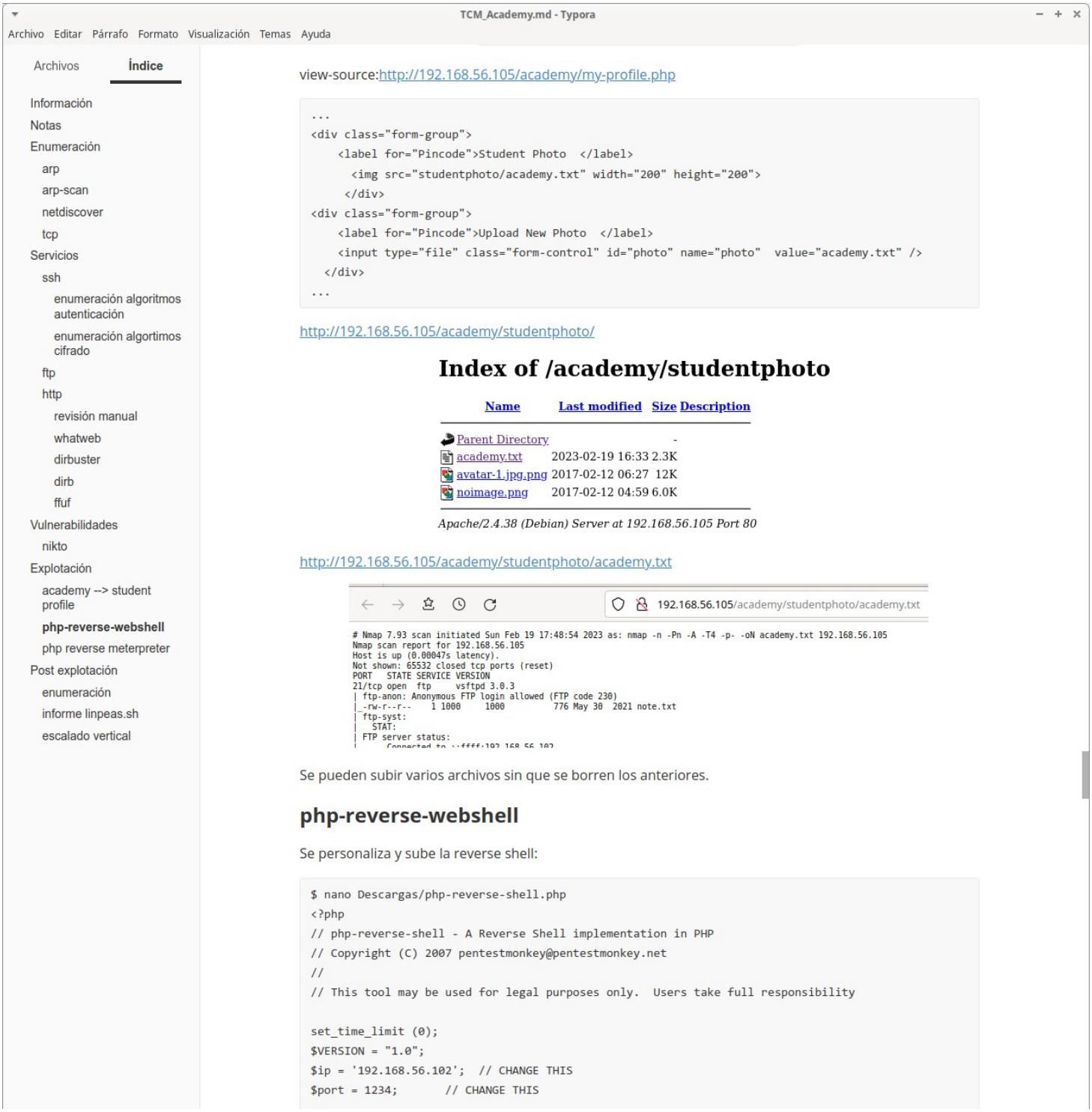
Permite guardar los archivos en formato xml o sqlite.



Typora

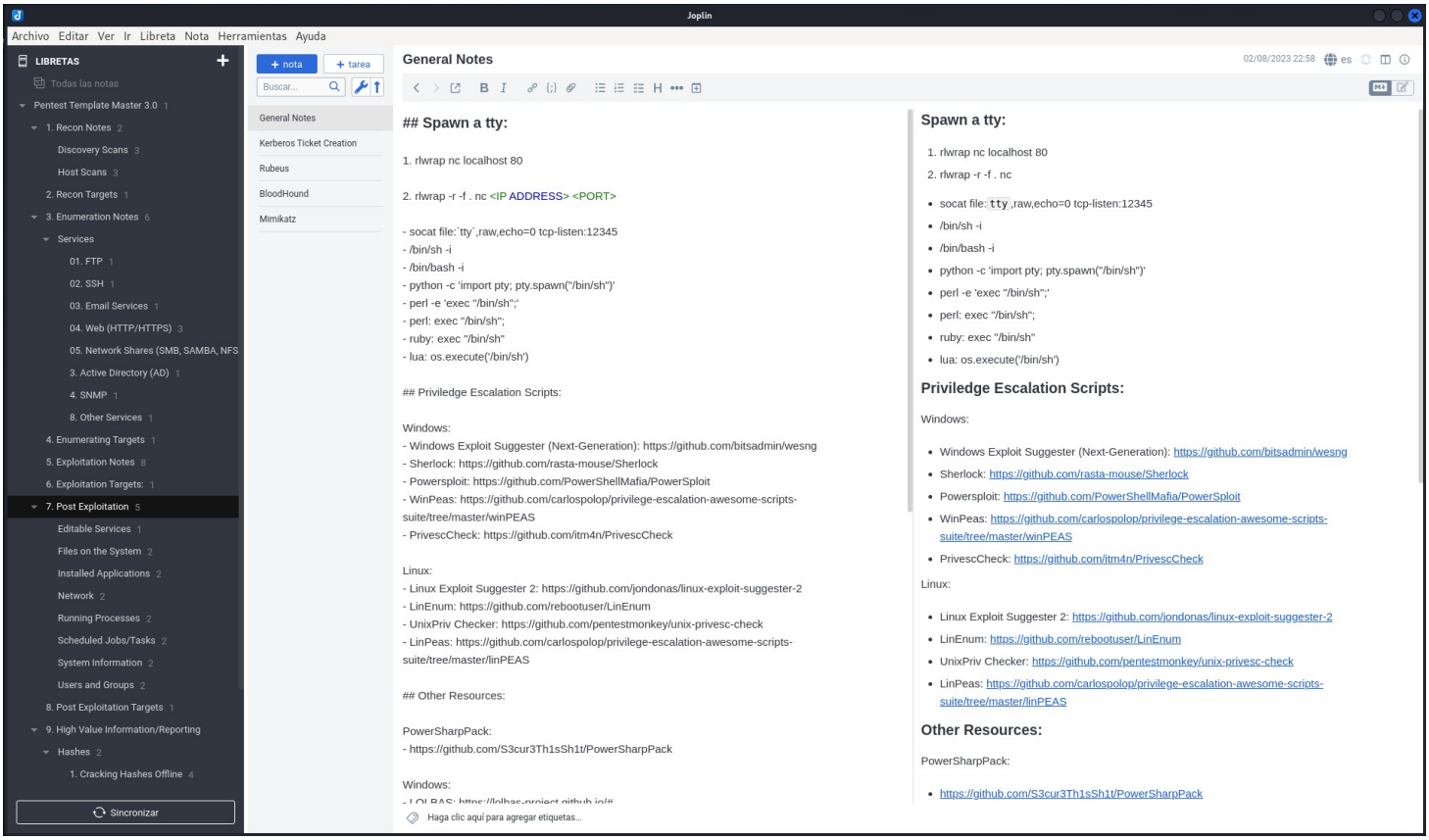
Markdown es un lenguaje de marcado ligero que permite aplicar formato a un texto empleando una serie de caracteres especiales. Aunque originalmente fue pensado para elaborar textos en la web de una forma más rápida y sencilla que con HTML, a día de hoy se emplea para documentar cualquier tipo de texto.

Su sencillez y flexibilidad hace que a día de hoy muchos *pentesters* se estén decantando por su uso. Aunque un fichero markdown (.md) no deja de ser un fichero de texto plano que puede crearse con cualquier editor, Typora es un editor que permite trabajar directamente con markdown o en modo WYSIWYG, además de permitir la exportación a otros formatos como pdf, html,docx, odt, …



Joplin

Joplin es otro editor de markdown que permite organizar la información en notas dentro de libros, que se pueden exportar e ficheros md. También existen plantillas para pentest como TJ-Pentest-Template.



3. Captura de la terminal

Gran parte del trabajo del *pentester* se va a desarrollar en la línea de comandos, siendo necesario documentar tanto el comando ejecutado como la salida del mismo. Hay comandos que ya tienen opciones para guardar su salida en ficheros pero en otras ocasiones habrá que recurrir a distintos métodos:

Redirección salida

Mediante `>` o `tee` se puede redirigir la salida de un comando hacia un fichero.

```
kali@kali:~$ cat /proc/version | tee kernel.txt
Linux version 6.5.0-kali3-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-4) 13.2.0, GNU ld (GNU Binutils for Debian) 2.41) #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09)

kali@kali:~$ cat kernel.txt
Linux version 6.5.0-kali3-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0-4) 13.2.0, GNU ld (GNU Binutils for Debian) 2.41) #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09)
```

script

Permite grabar las acciones de la terminal:

```
kali@kali:~$ script salida_script.txt
Script started, output log file is 'salida_script.txt'.
kali@kali:~$ whoami
kali
kali@kali:~$  ls -lhF /usr/share/windows-resources/binaries
total 1,9M
drwxr-xr-x 2 root root 4,0K sep  8 05:34 enumplus/
-rwxr-xr-x 1 root root  52K jul 17  2019 exe2bat.exe*
drwxr-xr-x 2 root root 4,0K sep  8 05:34 fgdump/
drwxr-xr-x 2 root root 4,0K sep  8 05:34 fport/
-rwxr-xr-x 1 root root  23K jul 17  2019 klogger.exe*
drwxr-xr-x 2 root root 4,0K sep  8 05:34 mbenum/
drwxr-xr-x 4 root root 4,0K sep  8 05:34 nbtenum/
-rwxr-xr-x 1 root root  58K jul 17  2019 nc.exe*
-rwxr-xr-x 1 root root 304K jul 17  2019 plink.exe*
-rwxr-xr-x 1 root root 688K jul 17  2019 radmin.exe*
-rwxr-xr-x 1 root root 356K jul 17  2019 vncviewer.exe*
```

```
-rwxr-xr-x 1 root root 302K jul 17  2019 wget.exe*
-rwxr-xr-x 1 root root  65K jul 17  2019 whoami.exe*
kali@kali:~$ exit
Script done.
kali@kali:~$
```

Visualización del archivo:

```
kali@kali:~$ cat salida_script.txt
Script started on 2021-10-27 08:54:59-04:00 [TERM="xterm-256color" TTY="/dev/pts/1" COLUMNS="155" LINES="54"]
kali@kali:~$  whoami
kali
kali@kali:~$ ls -lhF /usr/share/windows-resources/binaries
total 1,9M
drwxr-xr-x 2 root root 4,0K sep  8 05:34 enumplus/
-rwxr-xr-x 1 root root  52K jul 17  2019 exe2bat.exe*
drwxr-xr-x 2 root root 4,0K sep  8 05:34 fgdump/
drwxr-xr-x 2 root root 4,0K sep  8 05:34 fport/
-rwxr-xr-x 1 root root  23K jul 17  2019 klogger.exe*
drwxr-xr-x 2 root root 4,0K sep  8 05:34 mbenum/
drwxr-xr-x 4 root root 4,0K sep  8 05:34 nbtenum/
-rwxr-xr-x 1 root root  58K jul 17  2019 nc.exe*
-rwxr-xr-x 1 root root 304K jul 17  2019 plink.exe*
-rwxr-xr-x 1 root root 688K jul 17  2019 radmin.exe*
-rwxr-xr-x 1 root root 356K jul 17  2019 vncviewer.exe*
-rwxr-xr-x 1 root root 302K jul 17  2019 wget.exe*
-rwxr-xr-x 1 root root  65K jul 17  2019 whoami.exe*
kali@kali:~$  exit
```

Con opciones como `-a -t fichero_marcas_tiempo` y el comando `scriptreplay` se puede grabar y reproducir un vídeo de las acciones de la terminal.

asciinema

Asciinema es un programa que permite grabar y reproducir 'vídeos' de las acciones ejecutadas en la línea de comandos; así como compartilas en Internet, si lo deseamos. Los archivos de vídeo generados son muy ligeros y permiten durante su reproducción hacer copiar&pegar. No tienen sonido, pero proporcionan una forma muy sencilla de guardar y reproducir las acciones en la línea de comandos y con una calidad fantástica.

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install asciinema
kali@kali:~$ asciinema
usage: asciinema [-h] [--version] {rec,play,cat,upload,auth} ...

Record and share your terminal sessions, the right way.

positional arguments:
  {rec,play,cat,upload,auth}
    rec                 Record terminal session
    play                Replay terminal session
    cat                 Print full output of terminal session
    upload              Upload locally saved terminal session to asciinema.org
    auth                Manage recordings on asciinema.org account

optional arguments:
  -h, --help            show this help message and exit
  --version             show program's version number and exit

example usage:
  Record terminal and upload it to asciinema.org:
    asciinema rec
  Record terminal to local file:
    asciinema rec demo.cast
  Record terminal and upload it to asciinema.org, specifying title:
    asciinema rec -t "My git tutorial"
  Record terminal to local file, limiting idle time to max 2.5 sec:
    asciinema rec -i 2.5 demo.cast
```

```
  Replay terminal recording from local file:
    asciinema play demo.cast
  Replay terminal recording hosted on asciinema.org:
    asciinema play https://asciinema.org/a/difqlgx86ym6emrmd8u62yqu8
  Print full output of recorded session:
    asciinema cat demo.cast

For help on a specific command run:
  asciinema <command> -h
```

Grabando la línea de comandos en un vídeo en el ordenador

Para grabar la línea de comandos y guardar el vídeo en el ordenador simplemente ejecutamos: `asciinema rec -t "título" nombre_del_video.cast` y a continuación escribimos los comandos a grabar. Una opción interesante es `-i <tiempo_en_segundos>` que permite reducir el tiempo de inactividad en la línea de comandos al tiempo indicado. Por ejemplo:

```
kali@kali:~$ asciinema rec -i 2 -t "edición /etc/group" video1.cast
asciinema: recording asciicast to video1.cast
asciinema: press <ctrl-d> or type "exit" when you're done
kali@kali:~$ sudo nano /etc/group
[sudo] password for kali:
kali@kali:~$  exit
asciinema: recording finished
asciinema: asciicast saved to video1.cast
kali@kali:~$ ls -lhF
total 56K
....
-rw-r--r-- 1 kali kali  20K oct 27 06:53 video1.cast
....
```

Reproduciendo un vídeo en el ordenador

Para reproducir un vídeo hay que ejecutar el comando: `asciinema play nombre_video.cast`. Asciinema se encarga de reproducir el vídeo directamente en la línea de comandos, mostrando todos los comandos ejecutados y las salidas correspondientes. La opción `-i` también es de aplicación aquí.

```
kali@kali:~$ asciinema play video1.cast
```

Se puede pausar/reiniciar la reproducción pulsando la tecla `Espacio`. Si se pausa la reproducción y se pulsa la tecla . se reproduce carácter a carácter.

Subiendo vídeos a asciinema

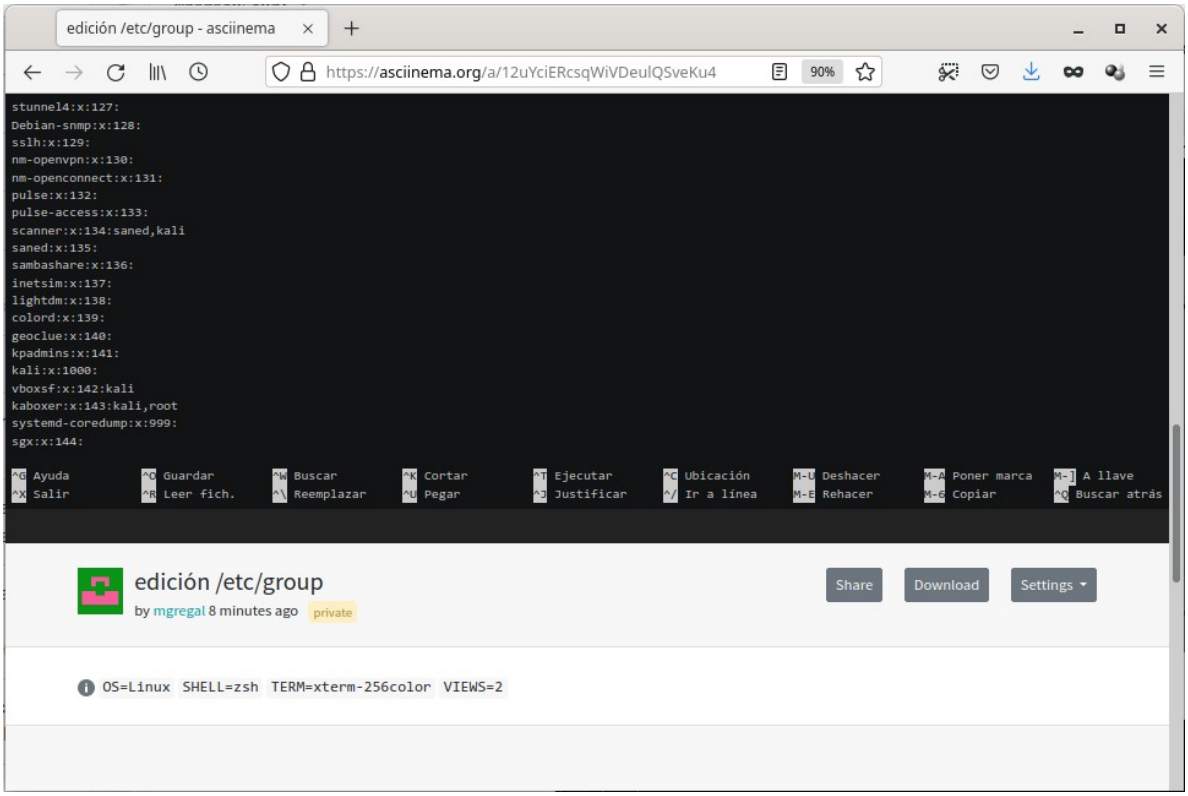
Para subir vídeos a la web de https://asciinema.org/ hay que crear una cuenta. Ejecutamos en el equipo:

```
kali@kali:~$ asciinema auth
Open the following URL in a web browser to link your install ID with your asciinema.org user account:

https://asciinema.org/connect/db87c640-9472-4998-af22-85f6b70396dd

This will associate all recordings uploaded from this machine (past and future ones) to your account, and allow you to
manage them (change title/theme, delete) at asciinema.org.
```

Se accede al enlace y se siguen las instrucciones relativas el email. Una vez creada la cuenta, usando el comando asciinema upload nombre_del_video.cast podemos subir el vídeo a la web:

```
kali@kali:~$ asciinema upload video1.cast
View the recording at:

   https://asciinema.org/a/12uYciERcsqWiVDeulQSveKu4
```

Accediendo a la URL indicada podremos reproducir el vídeo, editar ciertas características del mismo (título, descripción, hacerlo público o no), descargarlo y pulsando en *Share* ver el código html/javascript necesario para incrustarlo en un sitio web.

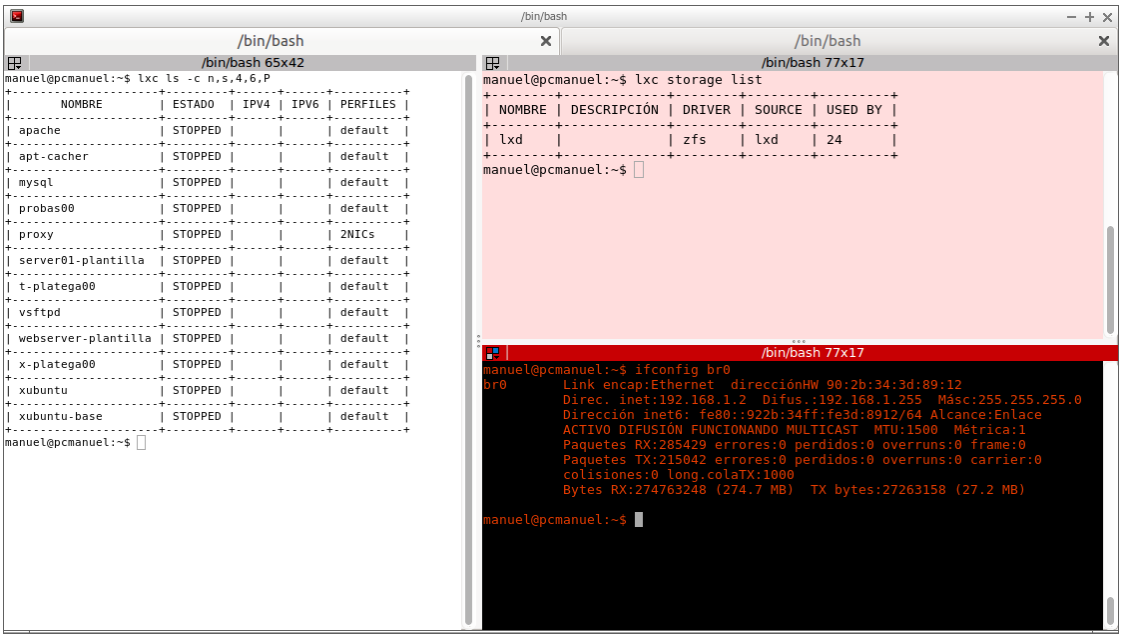


4. Captura de pantalla

terminator

Terminator es una terminal con algunas características especiales:

- Permite trabajar con pestañas.
- Permite trabajar con divisiones horizontales y verticales (*splits*).
- Permite definir perfles (*profiles*) con un tipo, tamaño y color de letra, color de fondo, ... Esta funcionalidad permite por ejemplo tener varios perfiles y asociarlos a equipos diferentes (p.e. estamos administrando varios servidores por ssh).
- Permite extender sus funcionalidades mediante *plugins* como *TerminalShot* que permite sacar una imagen la terminal



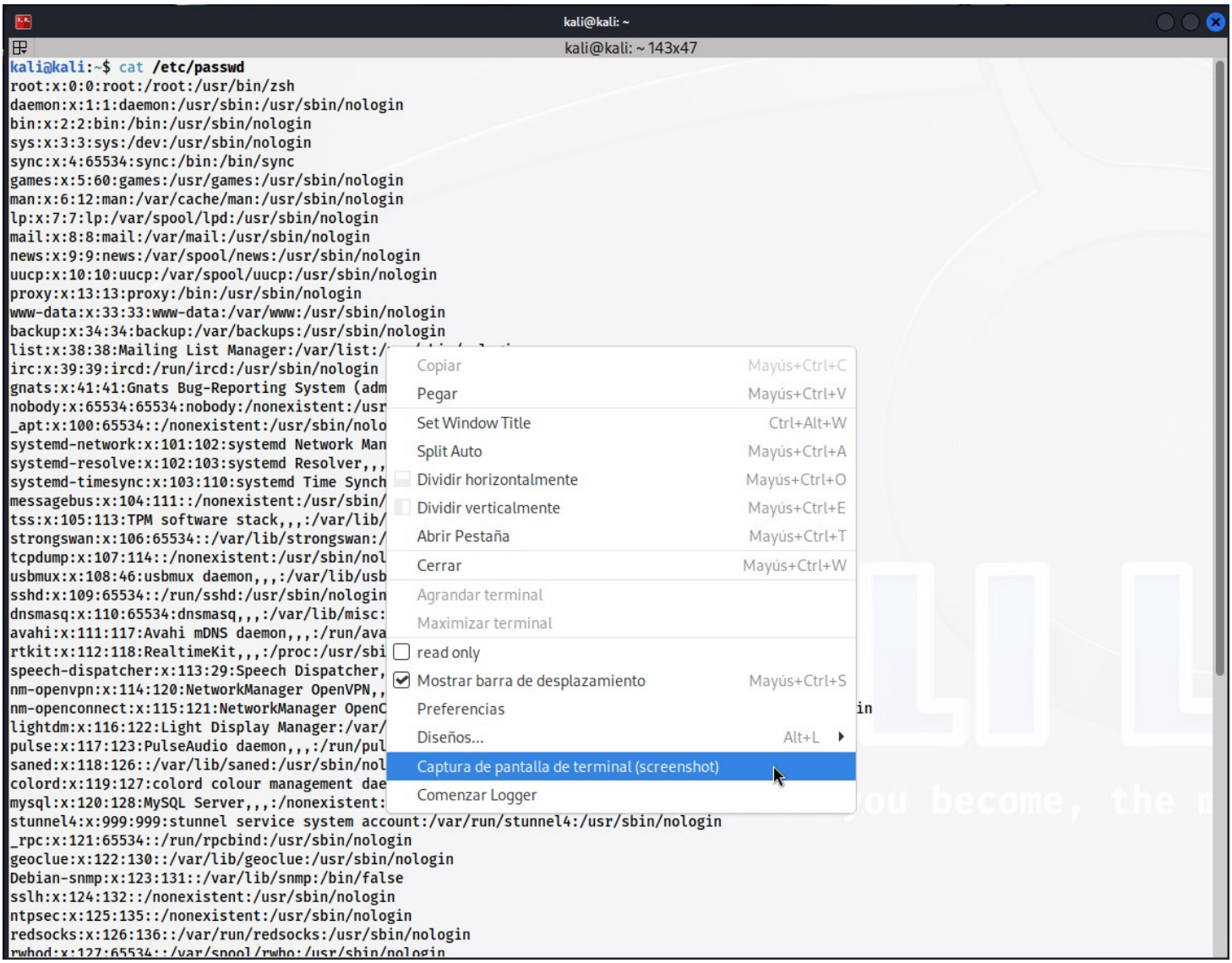
Para instalarlo:

```
kali@kali:~$  sudo apt update
kali@kali:~$ sudo apt-get install terminator
```

Una vez instalado podemos arrancarlo y pulsando el botón derecho del ratón podemos:

- Dividir el terminal horizontalmente.
- Dividir el terminal verticalmente.
- Abrir pestañas.
- Escoger la opción *Preferencias* para poder crear perfiles.

En *Preferencias* → *Plugins* se puede activar *TerminalShot* y a partir de ese momento se pueden sacar fotos de la terminal



shutter, flameshot

Tanto `shutter` como `flameshot` son capturadores de pantalla, que permiten sacar imágenes de todo el escritorio o de zonas del mismo, así como la posterior edición de la imagen. Para su instalación en Kali Linux:

```
kali@kali:~$ sudo apt-get install shutter
kali@kali:~$ sudo apt-get install flameshot
```