Tema 5

Despliegue de aplicaciones web

Francisco Alfonso Muñoz Sánchez

Indice

[Configuración del servicio de transferencia de archivos 2](#_Toc504999630)

[Instalando el servidor. 3](#_Toc504999631)

[Tipos de usuario y acceso al servicio. 4](#_Toc504999632)

[Configuración avanzada del chroot 10](#_Toc504999633)

# Configuración del servicio de transferencia de archivos

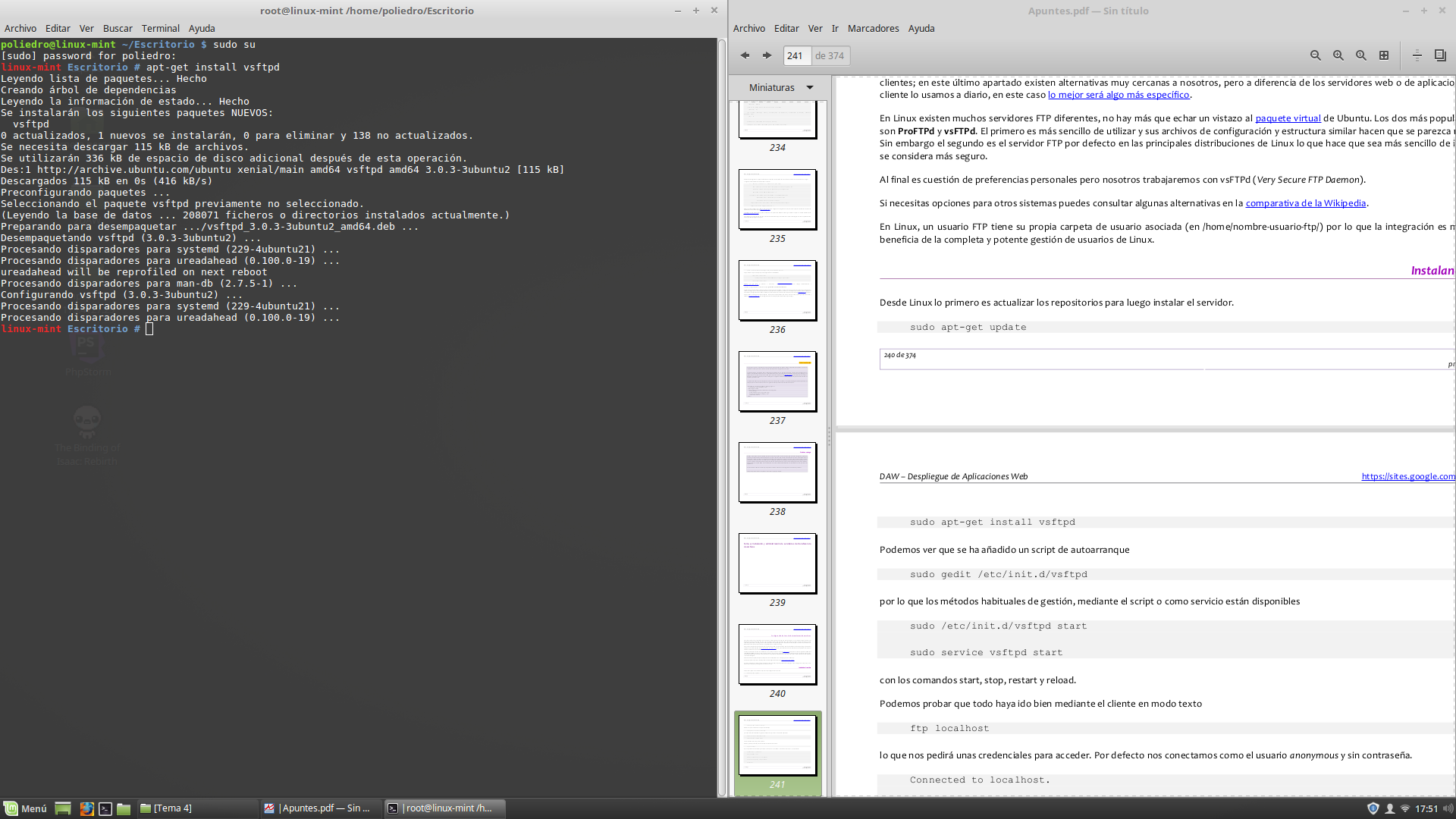
El protocolo clásico para la transferencia de archivos en Internet se demonina FTP (File Transfer Protocol). Con el estado actual de Internet y las múltiples opciones de trasferencia de archivos en la web puede parecer algo innecesario pero sigue siendo una opción sencilla y específica por lo que en ámbitos profesionales contínua gozando de buenísima salud. Por ejemplo sigue siendo el método más habitual para subir archivos, actualizaciones o midificaciones de contenido a un servidor web, especialmente en el modo de hosting.

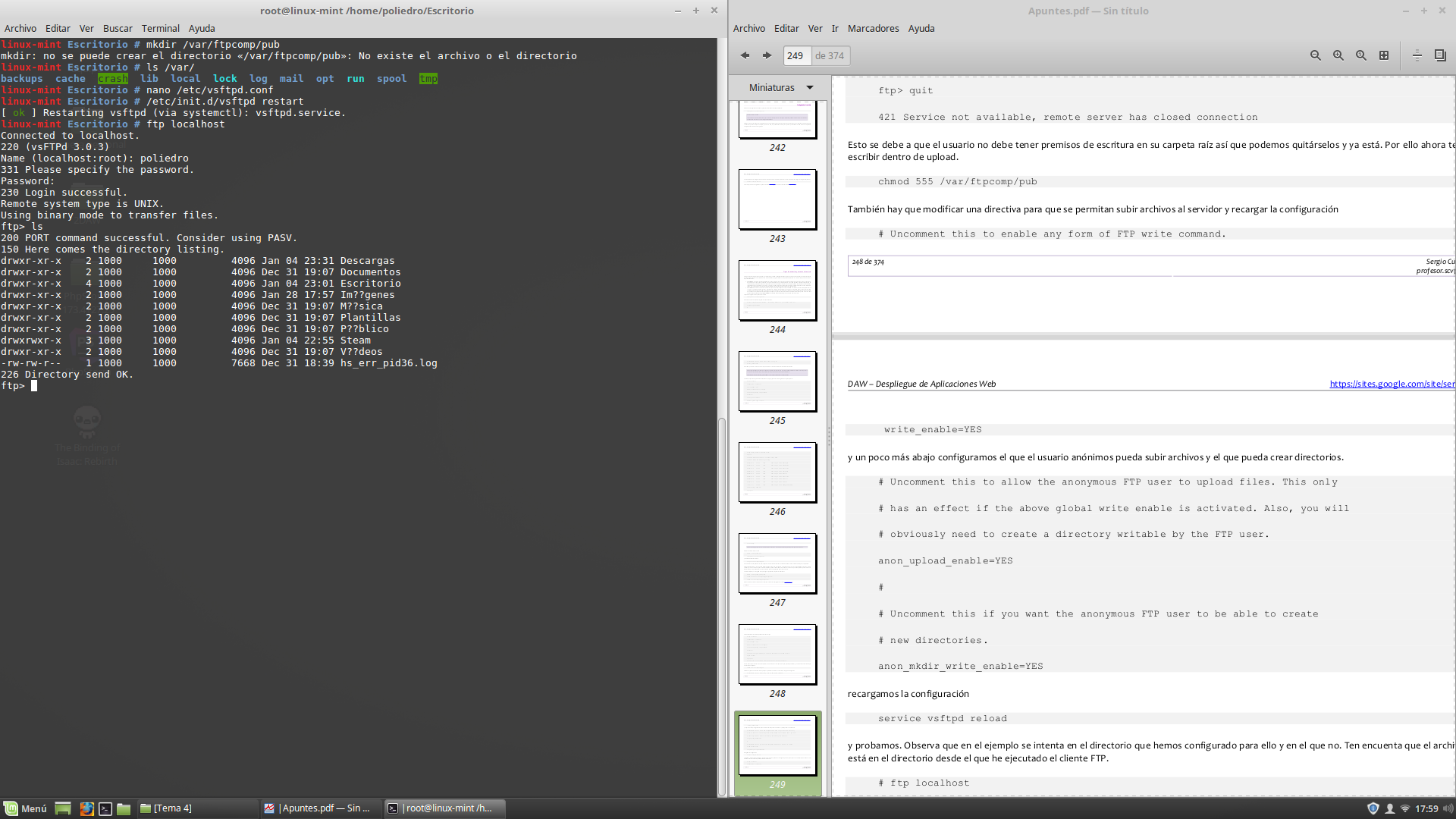
FTP se ajusta a una arquitectura cliente/servidor como todo lo que hemos visto hasta ahora. Primero instalaremos el servidor, para luego ver diferentes clientes; en este último apartado existen alternativas muy cercanas a nosotros, pero a diferencia de los servidores web o de aplicaciones en los que el cliente lo usamos a diario, en este caso lo mejor será algo más específico.

En Linux existen muchos servidores FTP diferentes, no hay más que echar un vistazo al paquete virtual de Ubuntu. Los dos más populares actualmente son ProFTPd y vsFTPd. El primero es más sencillo de utilizar y sus archivos de configuración y estructura similar hacen que se parezca mucho a Apache. Sin embargo el segundo es el servidor FTP por defecto en las principales distribuciones de Linux lo que hace que sea más sencillo de instalar y además se considera más seguro.

En Linux, un usuario FTP tiene su propia carpeta de usuario asociada (en /home/nombre-usuario-ftp/) por lo que la integración es muy alta y FTP se beneficia de la completa y potente gestión de usuarios de Linux.

## Instalando el servidor.

Primero instalamos vsftpd

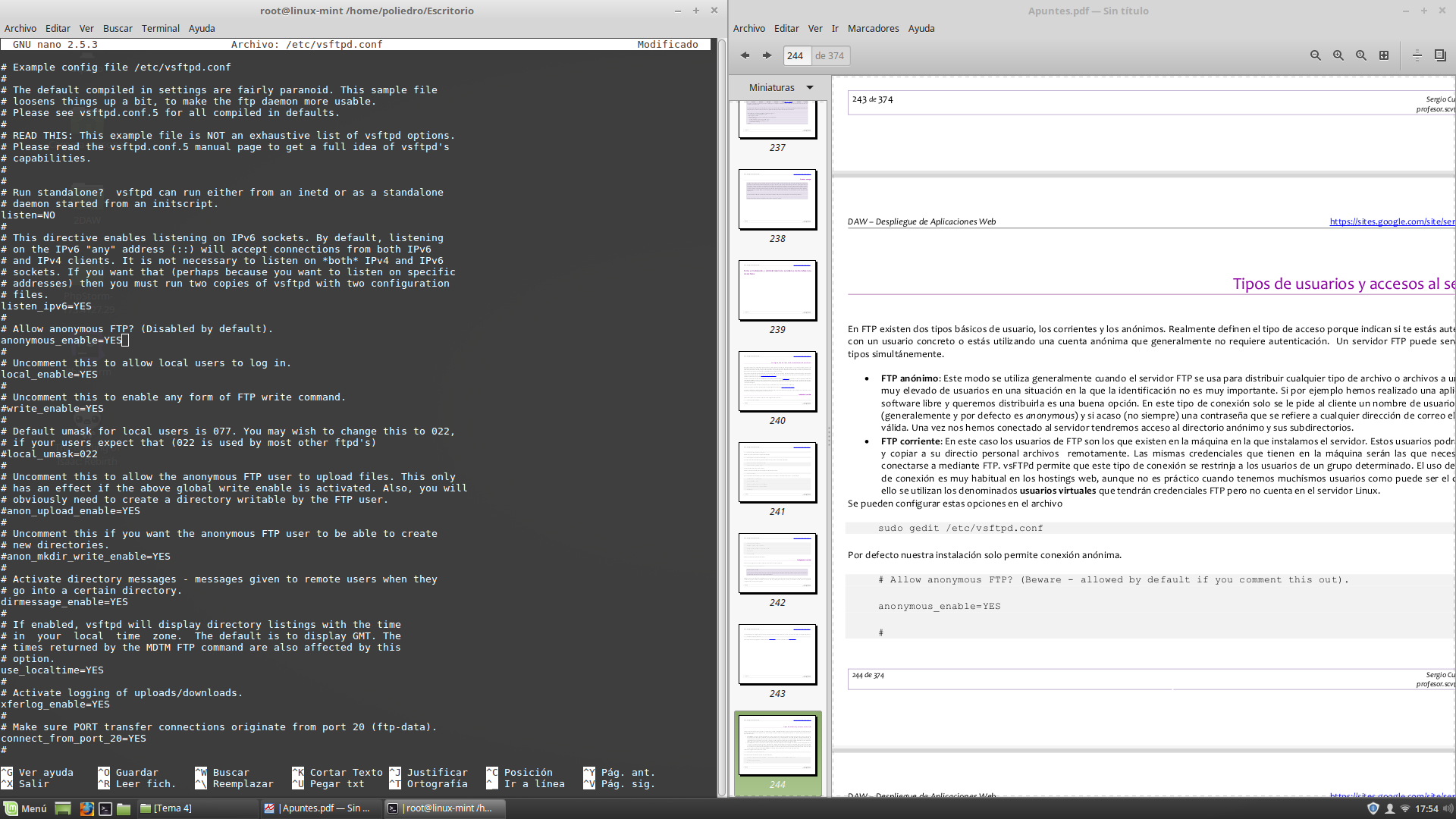
Vemos que funciona

# Tipos de usuario y acceso al servicio.

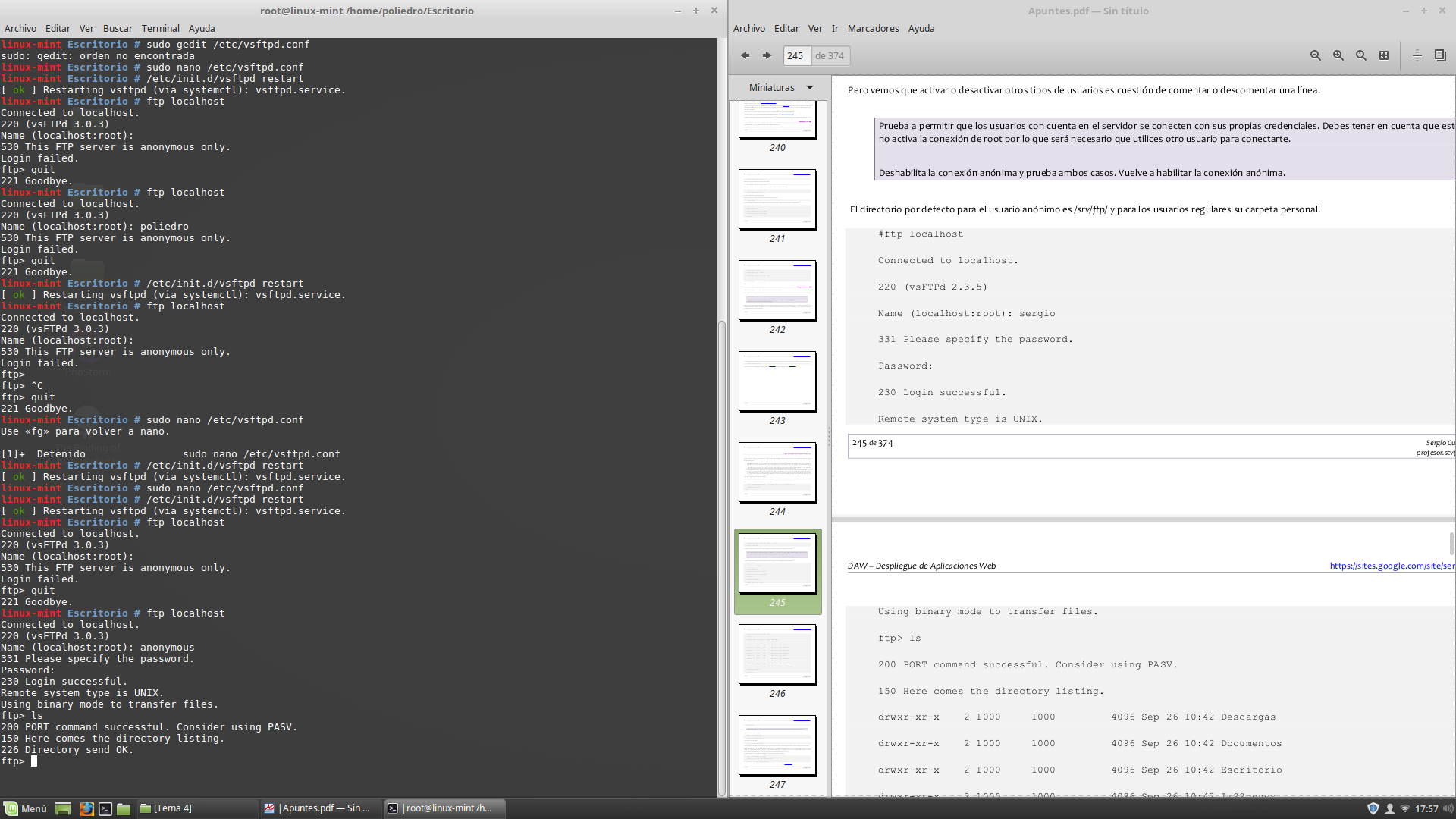
En FTP existen dos tipos básicos de usuario, los corrientes y los anónimos. Realmente definen el tipo de acceso porque indican si te estás autenticando con un usuario concreto o estás utilizando una cuenta anónima que generalmente no requiere autenticación. Un servidor FTP puede servir ambos tipos simultánemente.

 FTP anónimo: Este modo se utiliza generalmente cuando el servidor FTP se usa para distribuir cualquier tipo de archivo o archivos a un número muy elevado de usuarios en una situación en la que la identificación no es muy importante. Si por ejemplo hemos realizado una aplicación de software libre y queremos distribuirla es una buena opción. En este tipo de conexión solo se le pide al cliente un nombre de usuario anónimo (generalemente y por defecto es anonymous) y si acaso (no siempre) una contraseña que se refiere a cualquier dirección de correo electrónico válida. Una vez nos hemos conectado al servidor tendremos acceso al directorio anónimo y sus subdirectorios.  FTP corriente: En este caso los usuarios de FTP son los que existen en la máquina en la que instalamos el servidor. Estos usuarios podrán leer de y copiar a su directio personal archivos remotamente. Las mismas credenciales que tienen en la máquina serán las que necesiten para conectarse a mediante FTP. vsFTPd permite que este tipo de conexión se restrinja a los usuarios de un grupo determinado. El uso de este tipo de conexión es muy habitual en los hostings web, aunque no es práctico cuando tenemos muchísmos usuarios como puede ser el caso. Para ello se utilizan los denominados usuarios virtuales que tendrán credenciales FTP pero no cuenta en el servidor Linux.

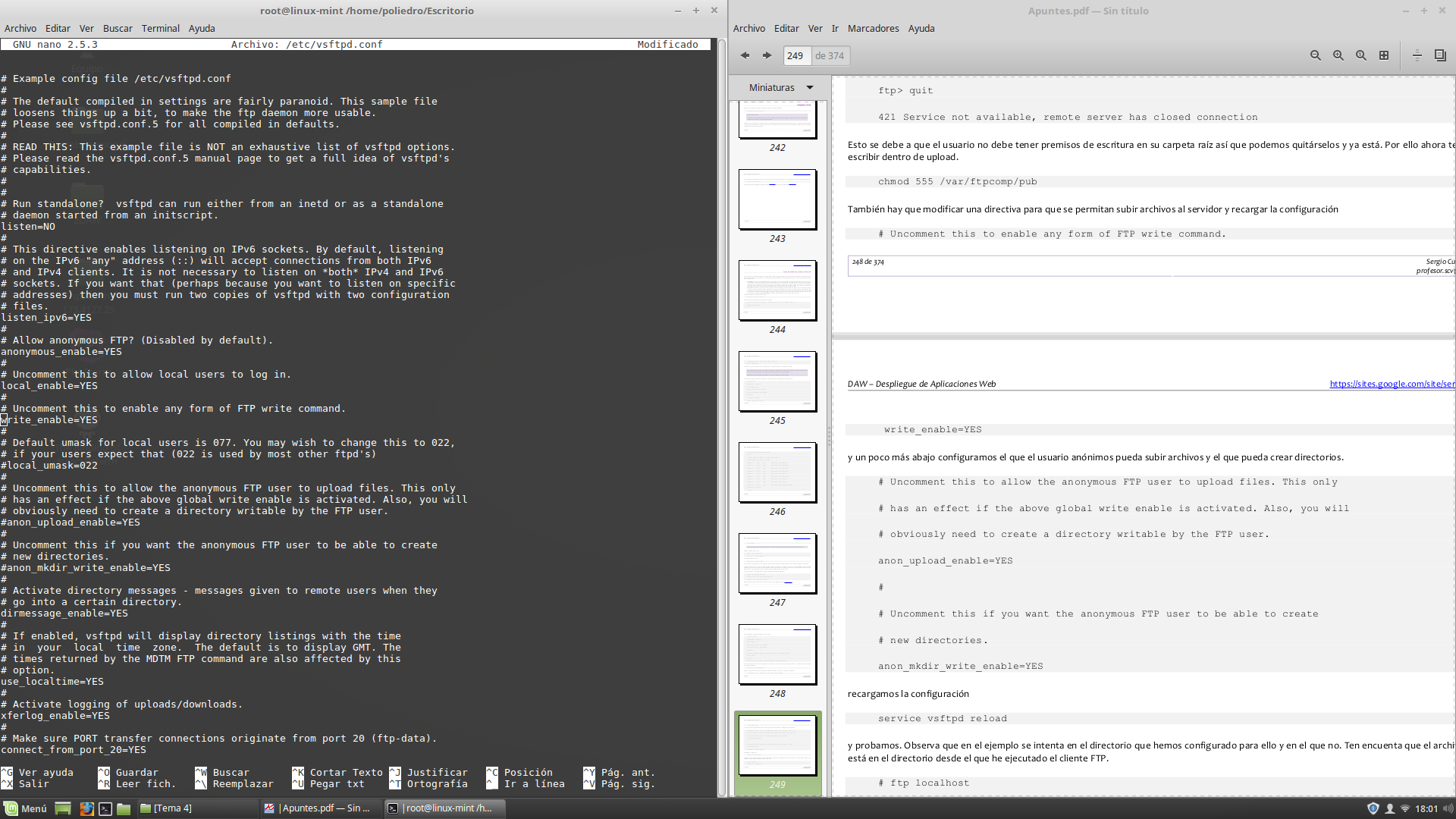
Descomentamos la línea de anonimo

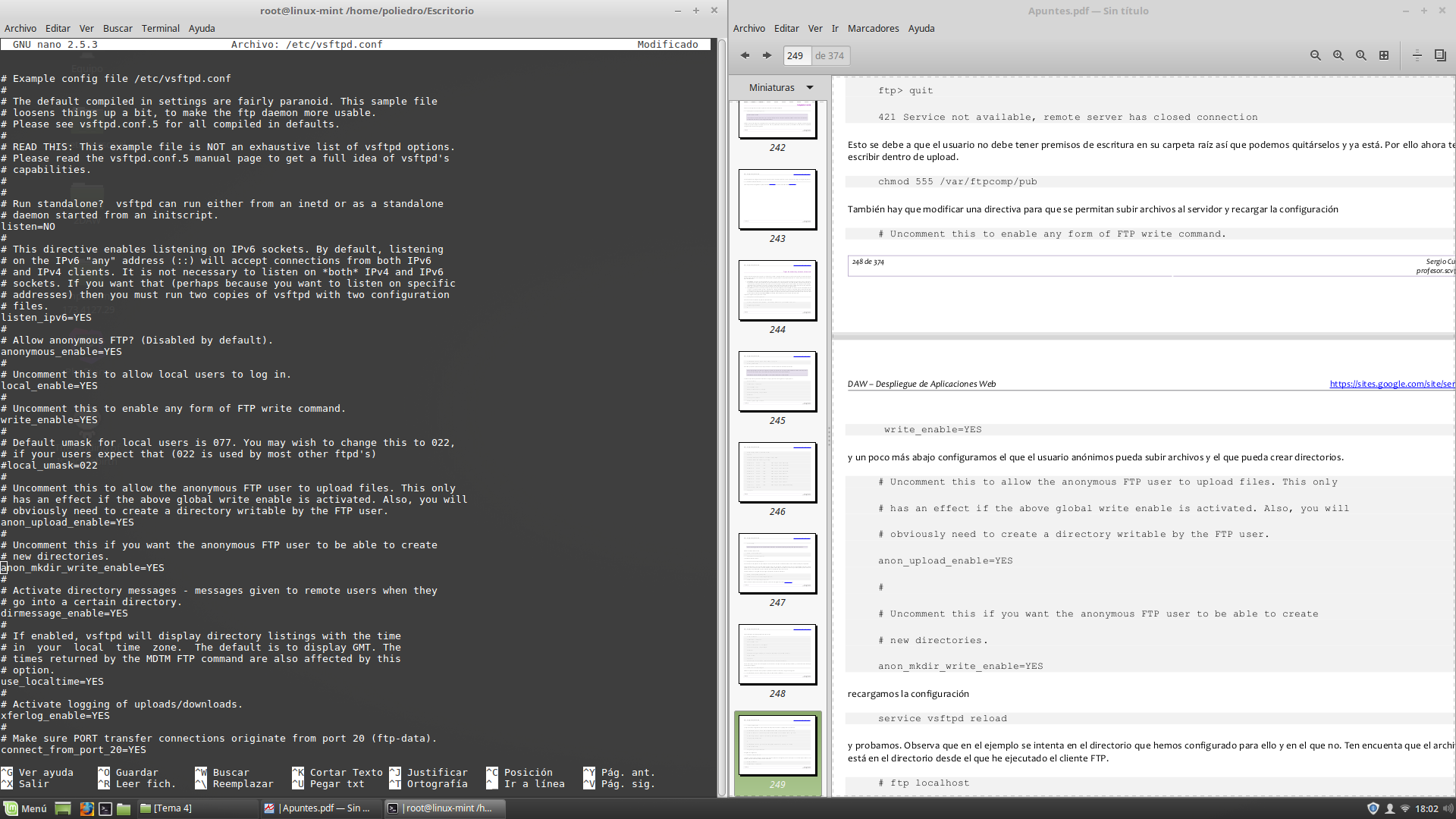
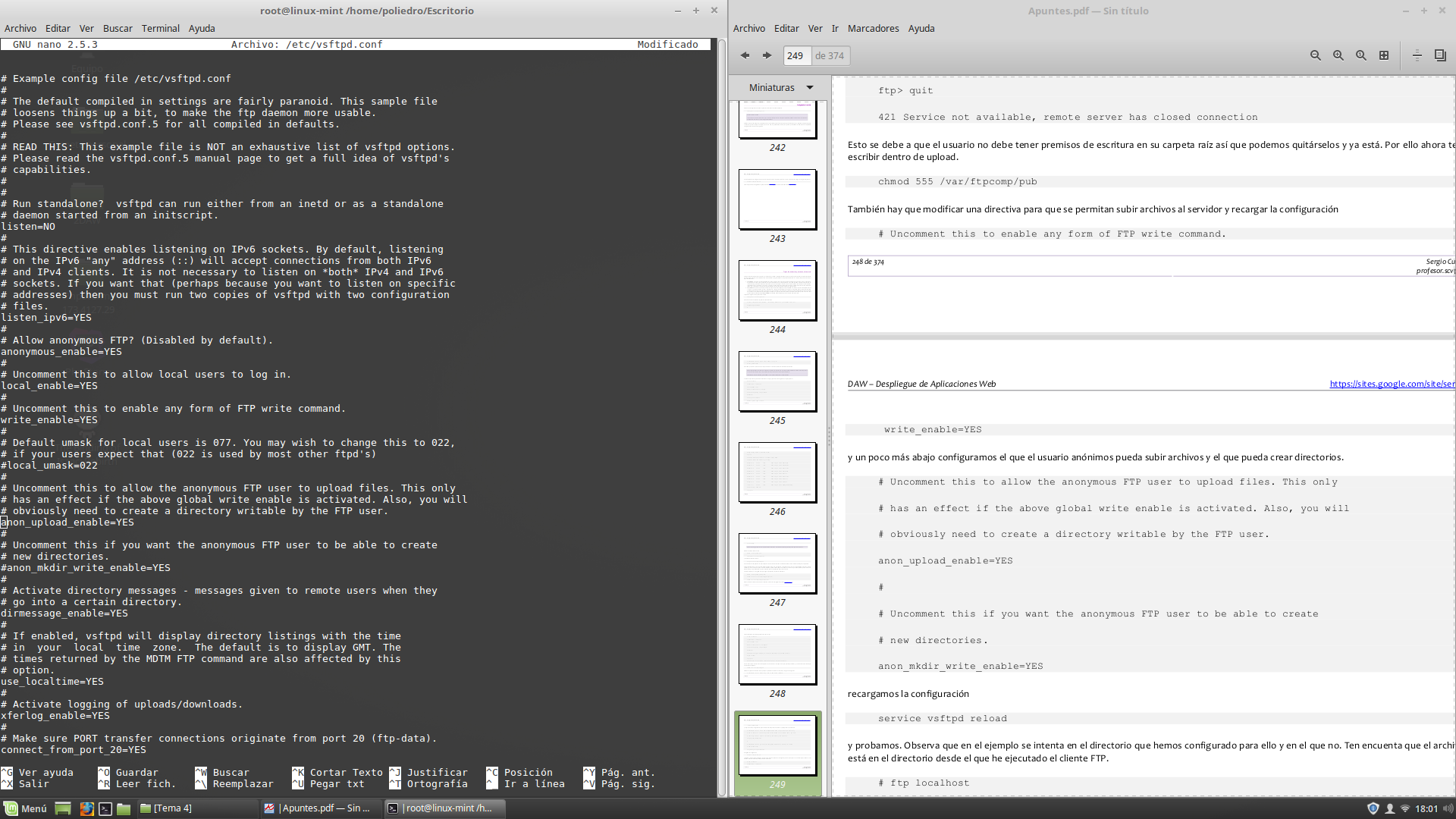


Y ya nos permite conectarnos en anónimo.



Configuramos que el anónimo pueda subir cosas.





## Configuración avanzada del chroot

Realmente la opción anterior tiene un pequeño agujero de seguridad como se indica en las FAQ de svFTPd

Q) Help! What are the security implications referred to in the "chroot\_local\_user" option?

A) Firstly note that other ftp daemons have the same implications. It is a generic problem. The problem isn't too severe, but it is this: Some people have FTP user accounts which are not trusted to have full shell access. If these accounts can also upload files, there is a small risk. A bad user now has control of the filesystem root, which is their home directory. The ftp daemon might cause some config file to be read - e.g. /etc/some\_file. With chroot(), this file is now under the control of the user. vsftpd is careful in this area. But, the system's libc might want to open locale config files or other settings...

Para evitar esto hay que cambiar las opciones de configuración.

