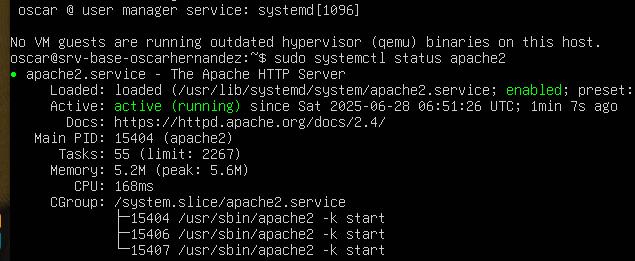
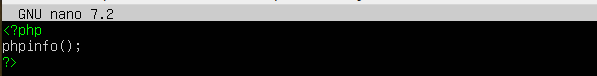
**fase 1, instalación y configuración de servidor web.**

instalación de apache2 y comprobamos su estado

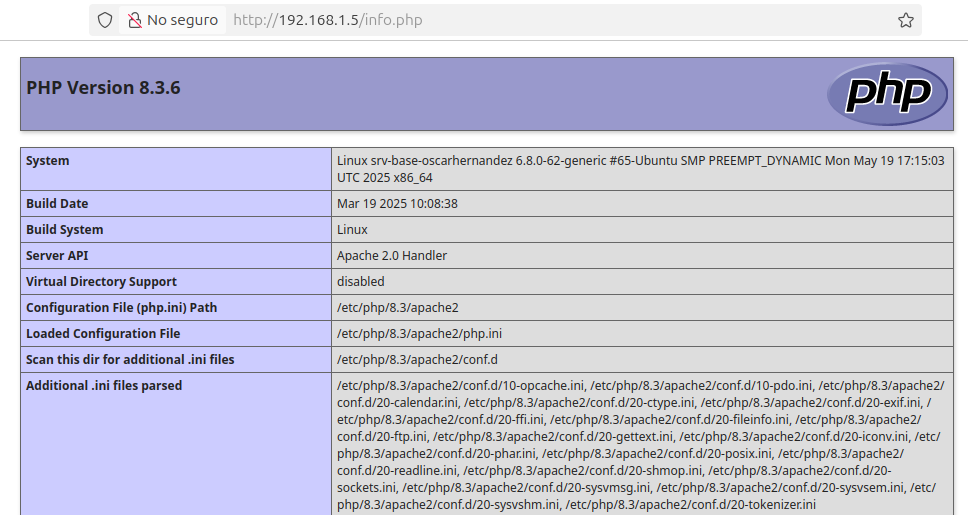


Crear una **página de prueba en HTML/PHP** que muestre información del servidor (phpinfo();). primero creamos el archivo





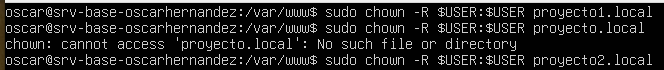
y hacemos la prueba desde un navegador



Configurar un **vhost** para alojar múltiples proyectos en el mismo servidor.



otorgar permisos necesarios



agregamos un archivo index.php para cada uno

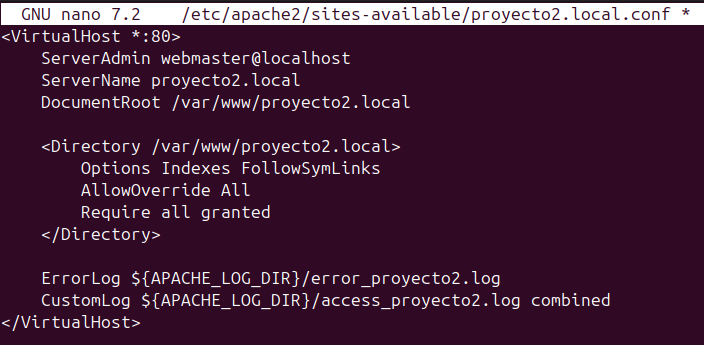




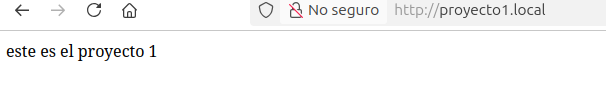
crear archivos de virtual hos copiando el archivo de configuracion y utilizandolo como plantilla

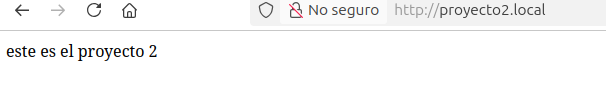


los editamos, desde la terminal de ubuntu he hecho una conexion ssh ya que no me deja hacer un copia y pega de lo que tengo que meter



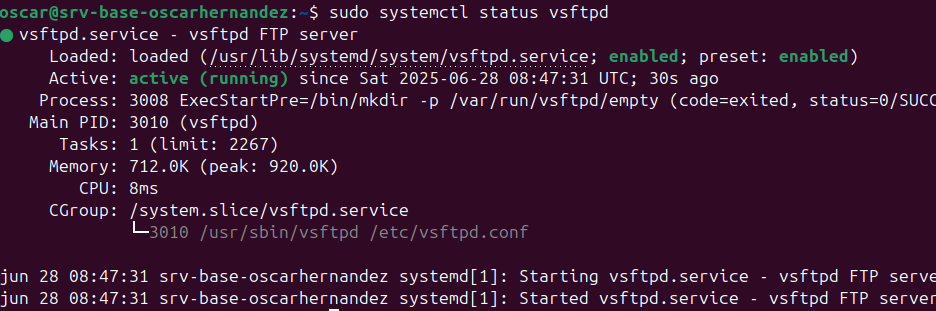
y hacemos la prueba desde el navegador



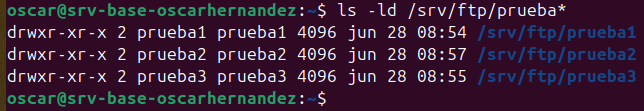


**fase 2, instalar y configurar ftp**

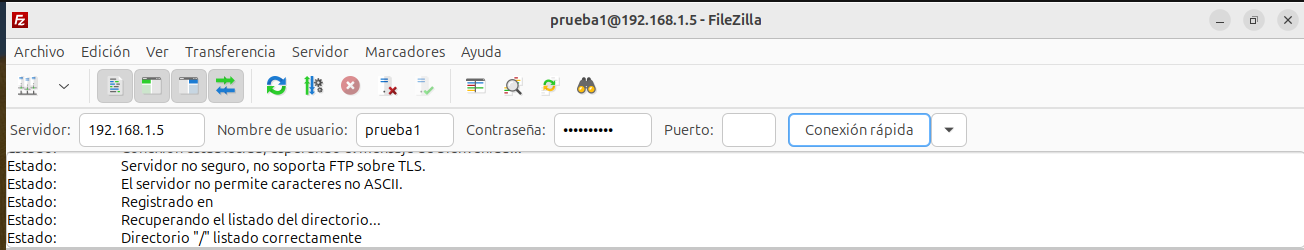
instalar vsftp



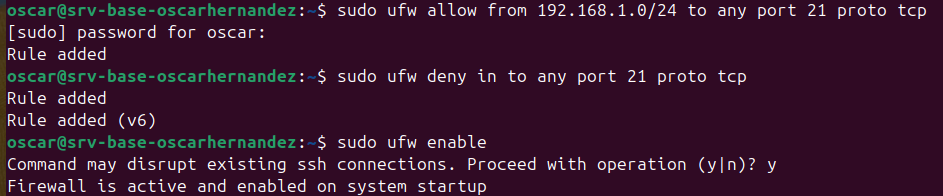
Crear **tres usuarios FTP** con acceso restringido a directorios específicos

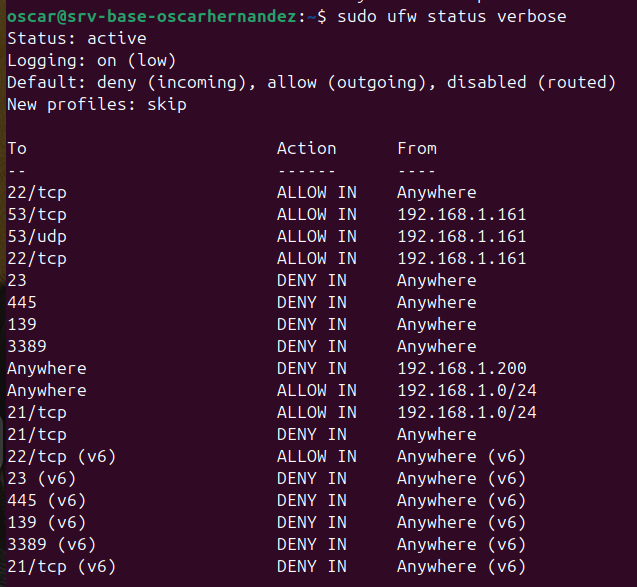


Probar la transferencia de archivos mediante un cliente FTP como **FileZilla**.



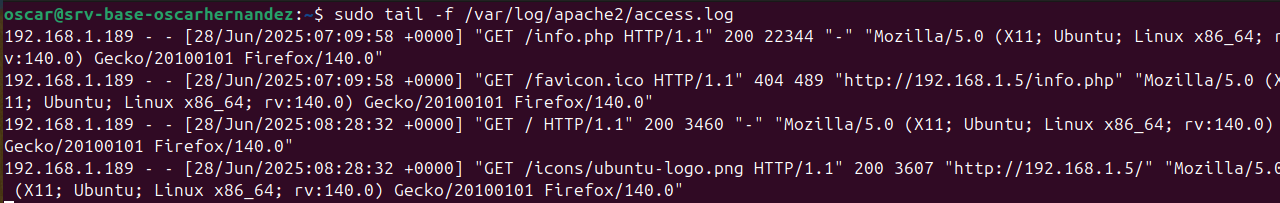
Configurar firewall (ufw o iptables) para permitir solo conexiones desde la red interna.



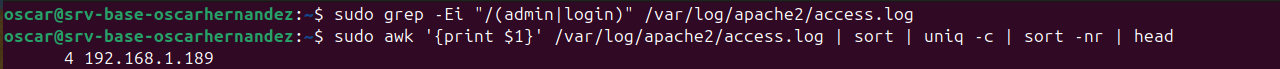


Implementar logs para detectar accesos sospechosos y revisar /var/log/apache2/access.log

verificamos que apache esta registrando los accesos



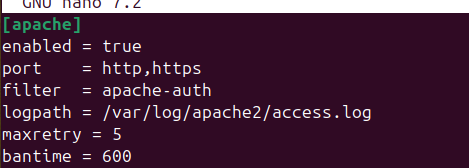
ver los ultimos intento y ver las ips con mas de 10 intentos



habilitar logs mas detallados



automatizar deteccion con herramientas utilizando fail2ban para bloquear ips con accesos maliciosos



por ultimo ver los logs a tiempo real

