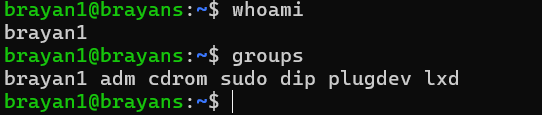
# PR\_01.3

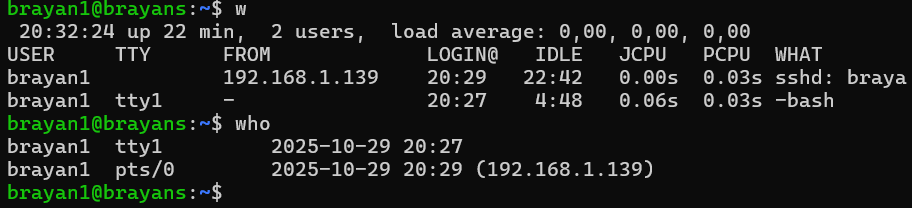
## Bloque 1: Comandos de Información y Preparación

1. Identidad del Usuario: Abre una terminal y ejecuta un comando para saber qué usuario eres y a qué grupos perteneces.

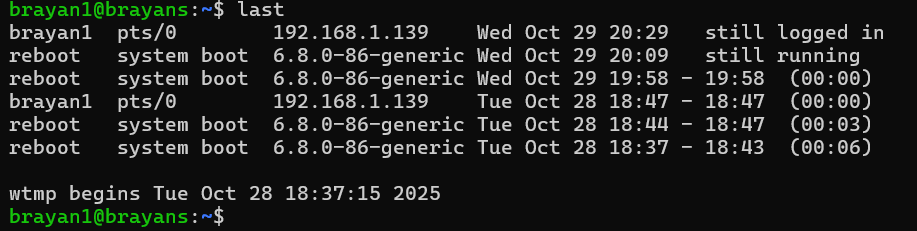


1. Usuarios Conectados: Muestra quién está conectado actualmente al sistema. Luego, ejecuta otro comando que te dé información más detallada, como el tiempo que llevan conectados y qué están ejecutando.

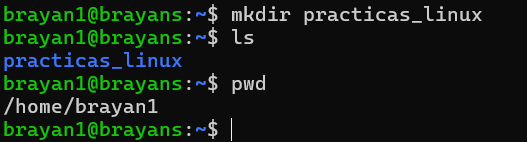
who o w



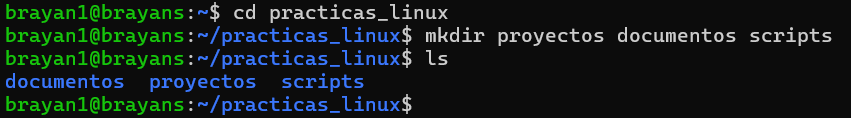
1. Historial de Conexiones: Lista los últimos inicios de sesión en el sistema.



1. Crear Entorno de Trabajo: En tu directorio personal ( /home/tu\_usuario ), crea una carpeta principal para todos los ejercicios llamada practicas\_linux.

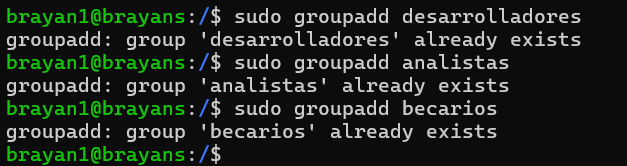


1. Estructura de Directorios: Dentro de practicas\_linux , crea la siguiente estructura de directorios: proyectos , documentos y scripts .

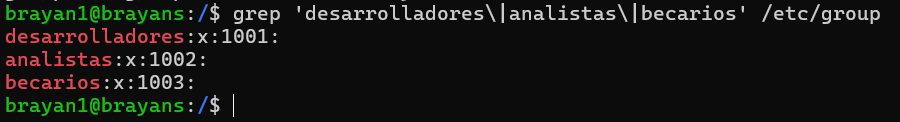


## Bloque 2: Gestión de Usuarios y Grupos

1. Crear Grupos: Crea tres nuevos grupos en el sistema: desarrolladores, analistas, y becarios.



1. Verificar Grupos: Confirma que los grupos se han creado correctamente buscando sus nombres en el archivo /etc/group .



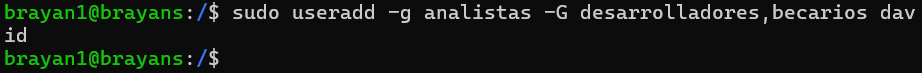
1. Crear un Usuario Básico: Crea un nuevo usuario llamado juan .



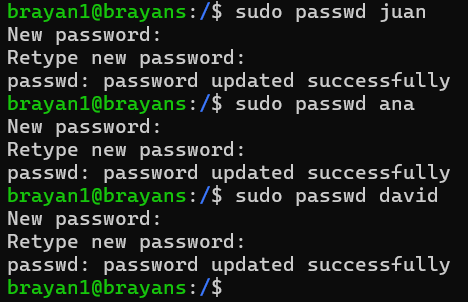
1. Crear Usuario con Grupo Primario: Crea una usuaria llamada ana y asígnala directamente al grupo primario desarrolladores.



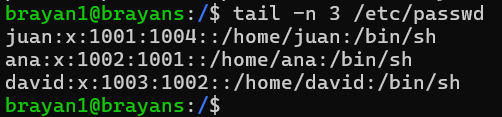
1. Crear Usuario Completo: Crea un usuario david asignándolo al grupo primario analistas y, a la vez, como miembro de los grupos secundarios desarrolladores y becarios .



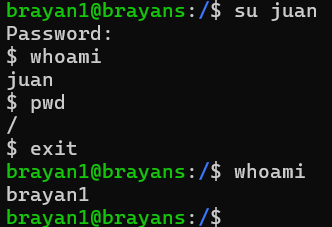
1. Establecer Contraseñas: Asigna una contraseña a los usuarios juan , ana y david .



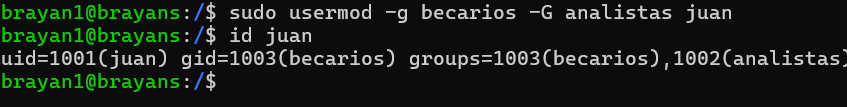
1. Verificar Usuarios: Comprueba que los tres nuevos usuarios existen en el sistema, inspeccionando el final del archivo /etc/passwd .



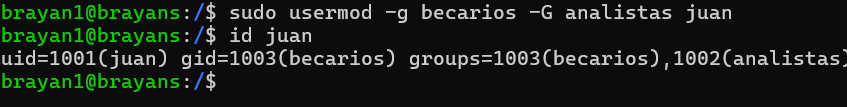
1. Cambiar de Usuario: Conviértete en el usuario juan usando el comando su . Una vez dentro de su sesión, comprueba quién eres y en qué directorio te encuentras. Vuelve a tu sesión de usuario original.



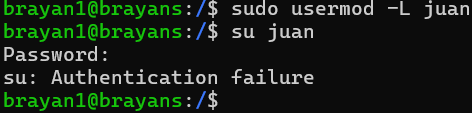
1. Modificar Grupos de un Usuario: Modifica al usuario juan para que su grupo primario sea becarios y añádelo también al grupo secundario analistas .



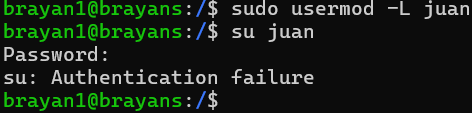
1. Verificar Modificación: Comprueba que los cambios del usuario juan se han aplicado correctamente.



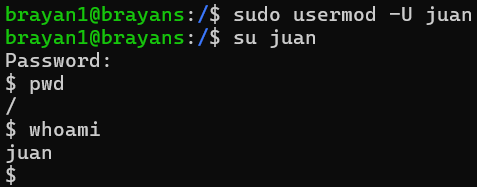
1. Bloquear una Cuenta: Bloquea la cuenta del usuario juan para que no pueda iniciar sesión.



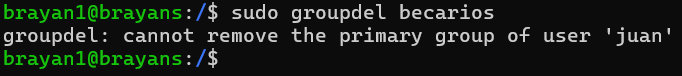
1. Intentar Cambiar a Usuario Bloqueado: Intenta convertirte en el usuario juan de nuevo. Debería fallar.



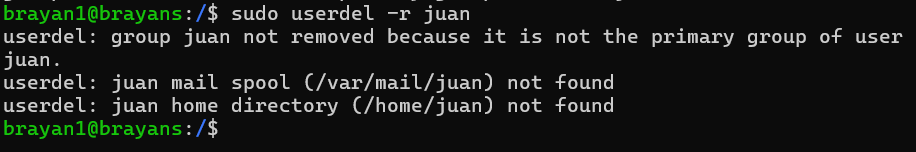
1. Desbloquear una Cuenta: Desbloquea la cuenta del usuario



1. Eliminar un Grupo: Elimina el grupo juan . becarios . ¿Qué ocurre? Nota: Fallará si algún usuario lo tiene como grupo primario).



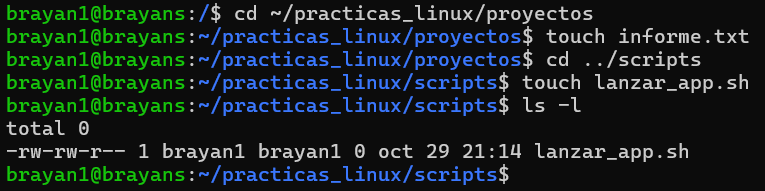
1. Eliminar Usuario y su Directorio: Elimina al usuario juan y asegúrate de que su directorio personal ( /home/juan ) también se borre.



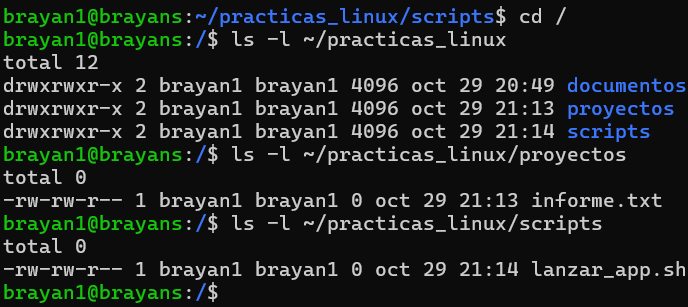
## Bloque 3: Permisos y Propiedad de Archivos

Realiza los siguientes ejercicios dentro de la carpeta practicas\_linux . de tu directorio home

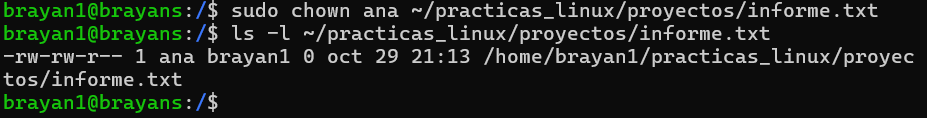
1. Crear Archivos de Prueba: Dentro de la carpeta vacío llamado informe.txt . Dentro de lanzar\_app.sh . proyectos , crea un archivo scripts , crea otro archivo vacío llamado



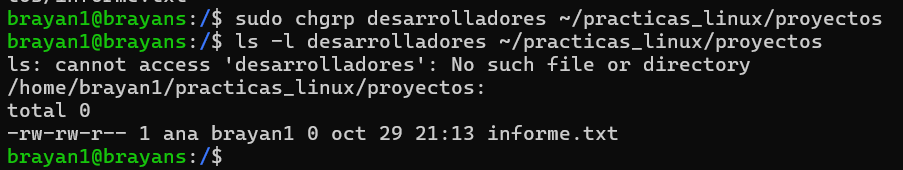
1. Ver Permisos: Muestra los permisos por defecto de los archivos y directorios que has creado. Anota quién es el propietario y el grupo.



1. Cambiar Propietario: Cambia el propietario del archivo pertenezca a la usuaria ana .



1. Cambiar Grupo: Cambia el grupo del directorio informe.txt para que proyectos para que pertenezca al grupo desarrolladores .

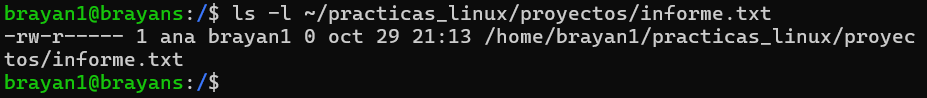


1. Cambiar Propietario y Grupo: Cambia el propietario y el grupo del archivo lanzar\_app.sh para que pertenezcan al usuario respectivamente, con un solo comando. david y al grupo analistas ,



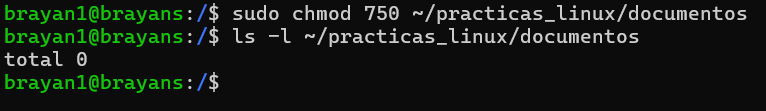
1. Permisos con Notación Octal Archivo): Usa la notación numérica (octal) para asignar los siguientes permisos a informe.txt : el propietario ( ana ) puede leer y escribir; el grupo ( desarrolladores ) solo puede leer; y los otros no tienen ningún permiso.



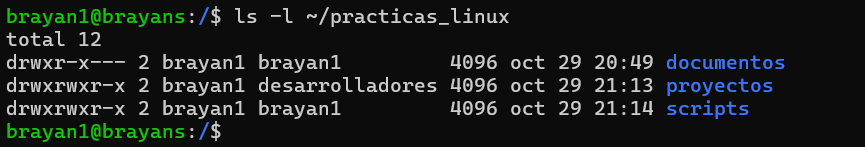


Propietario RW, grupo R, otros sin permisos

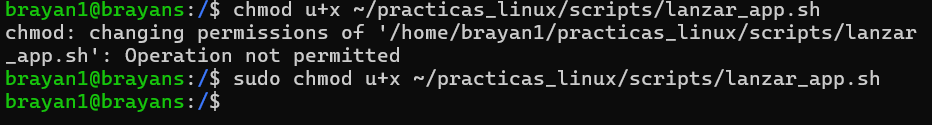
1. Permisos con Notación Octal Directorio): Asigna permisos de lectura, escritura y ejecución para el propietario y solo de lectura y ejecución para los miembros del grupo al directorio documentos .



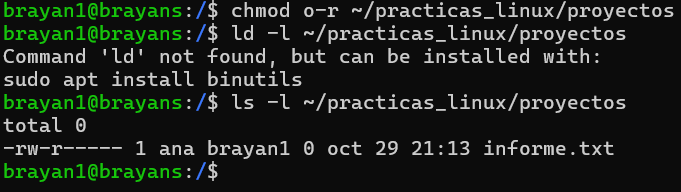
1. Verificar Permisos: Lista el contenido de practicas\_linux para verificar que todos los cambios de propietario y permisos se han aplicado correctamente.



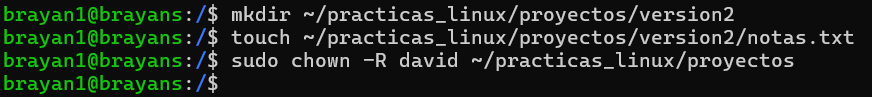
1. Permisos con Notación Simbólica (Añadir): Usa la notación simbólica para añadir el permiso de ejecución al propietario del script lanzar\_app.sh .



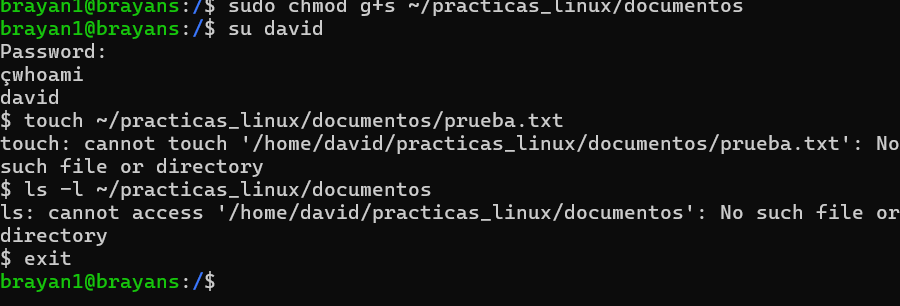
1. Permisos con Notación Simbólica (Quitar): Quita el permiso de lectura al “resto del mundoˮ (otros) en el directorio proyectos .



1. Permisos Recursivos: Dentro de proyectos , crea una nueva carpeta con un archivo version2 notas.txt dentro. Luego, cambia el propietario de la carpeta proyectos y todo su contenido para que pertenezca a david con un solo comando recursivo.



1. Permiso Especial SGID en Directorio: Establece el permiso especial SGID en el directorio documentos . Después, cambia a ser el usuario david ( su david ) y crea un nuevo archivo dentro de documentos . Verifica a qué grupo pertenece el nuevo archivo (debería heredar el del directorio documentos ). Vuelve a tu usuario.



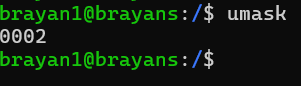
1. Permiso Especial SUID Establece el permiso SUID en el script lanzar\_app.sh .

Nota: Explica a tus alumnos qué implicaría esto si fuera un programa compilado).

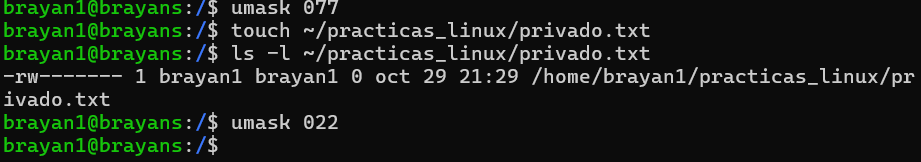


Si fuese un programa compliado se abriría

1. Comprobar umask : Muestra el valor umask actual de tu sesión.



1. Efecto de umask : Cambia temporalmente tu umask a archivo llamado 077 . Crea un nuevo archivo llamado privado.txt . Comprueba sus permisos por defecto. Luego, restaura el umask a su valor original.



## Bloque 4: Gestión de Servicios con systemctl

Nota: Para estos ejercicios, es seguro usar un servicio como cron / cups (impresión) o crond (tareas programadas). Evita usar servicios críticos como sshd si no estás seguro.

1. Estado Detallado de un Servicio: Comprueba el estado completo del

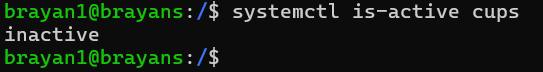
servicio cups . Analiza la salida: ¿está activo (active ), cargado ( loaded ) y habilitado ( enabled ? Anota las últimas líneas de su registro (log) que aparecen.



1. Comprobación Rápida: Utiliza un comando más directo para verificar si el

servicio cups está actualmente en ejecución (activo). La salida de este

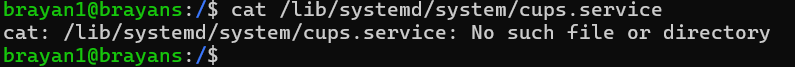
comando debería ser simplemente active o inactive .



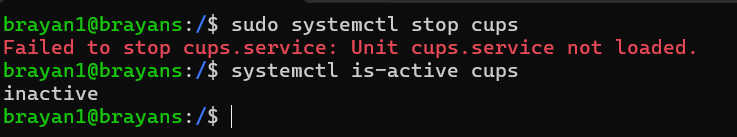
1. Ver Archivo de Unidad: Muestra el contenido del archivo de unidad del

servicio cups ( cups.service ). Esto te permitirá ver cómo está definido el

servicio.

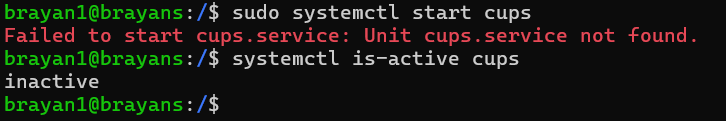


1. Detener un Servicio: Detén la ejecución del servicio estado de nuevo para confirmar que está cups . Comprueba su inactive (dead) .



1. Iniciar un Servicio: Vuelve a iniciar el servicio cups . Verifica una vez más

que ha vuelto al estado active (running) .

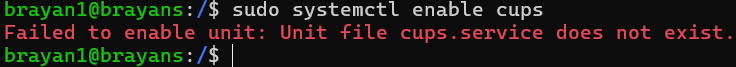


1. Reiniciar un Servicio: El comando restart es muy común tras un cambio de

configuración. Ejecútalo para el servicio cups .

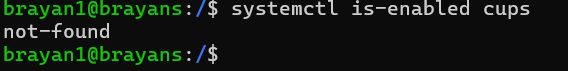


1. Habilitar para el Arranque: Asegúrate de que el servicio cups esté configurado para iniciarse automáticamente cada vez que el sistema arranque.

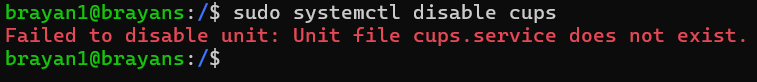


1. Verificar si está Habilitado: Usa un comando específico para preguntar si

cups está habilitado. La salida debería ser enabled o disabled .



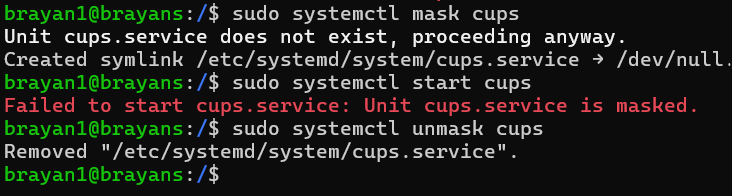
1. Deshabilitar para el Arranque: Ahora, desactiva el servicio no se inicie automáticamente. cups para que



1. Enmascarar un Servicio: El enmascaramiento es una forma más

contundente de deshabilitar, ya que impide cualquier tipo de inicio (manual

* + automático). Enmascara el servicio cups . Intenta iniciarlo después. Debería fallar. No olvides desenmascararlo ( unmask ) al terminar el ejercicio.



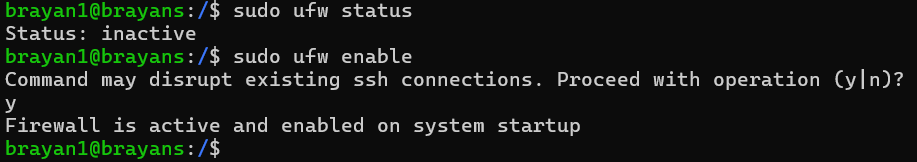
## Bloque 4: Gestión de ufw

1. Comprobar Estado y Activar UFW
   * Primero, ejecuta un comando para verificar el estado actual del firewall.

Probablemente estará inactivo.

* + A continuación, activa UFW. Presta atención al mensaje de advertencia,

especialmente si estás conectado por SSH.

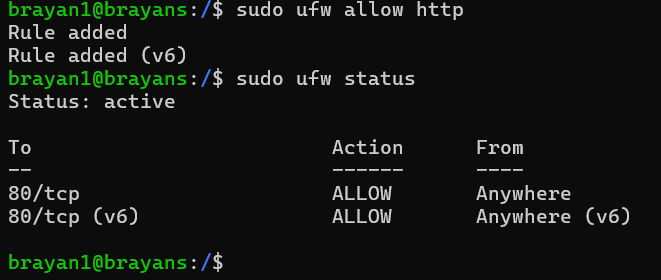


1. Permitir un Servicio We8b HTTP)

Imagina que tu servidor necesita alojar una página web. Añade una regla para permitir todas las conexiones entrantes para el servicio http .

* + Verifica el estado del firewall de nuevo para confirmar que la regla (y el

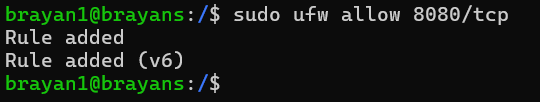
puerto 80 se ha añadido correctamente.



1. Abrir un Puerto Específico:
   * Imagina que estás ejecutando un servidor de aplicaciones web en el

puerto 8080. Añade una regla para permitir las conexiones entrantes TCP a

ese puerto.

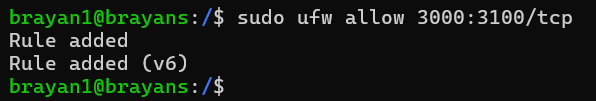


1. Permitir un Rango de Puertos:
   * Supón que una aplicación FTP necesita un rango de puertos pasivos.

Añade una regla para permitir las conexiones

desde el 3000 al 3100.

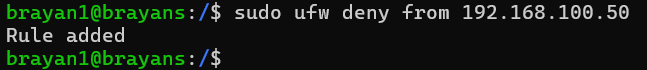
TCP en el rango de puertos



1. Bloquear una Dirección IP
   * Por seguridad, has detectado actividad sospechosa desde la IP

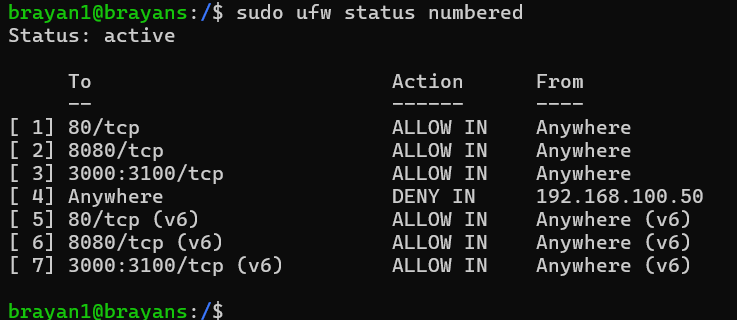
192.168.100.50 . Añade una regla para denegar todas las conexiones

provenientes de esa dirección IP.



1. Listar Reglas para Borrar:
   * Muestra todas las reglas activas del firewall, pero esta vez de forma

numerada, para prepararte para eliminar una de ellas.



1. Eliminar una Regla:
   * Basándote en la lista del ejercicio anterior, elimina la regla que creaste

para el puerto 8080 .

* + Vuelve a listar las reglas (de forma normal o numerada) para confirmar que la regla ha sido eliminada correctamente

