Tutorial Básico

1. Actualizar Linux: diferencias entre update y upgrade

```
sudo apt update
```

Actualiza la lista de paquetes disponibles desde los repositorios, sin instalar nada.

```
sudo apt upgrade
```

Instala las actualizaciones disponibles para los paquetes que ya están instalados.

2. Cambiar el nombre del equipo (hostname)

```
sudo hostname nuevo-nombre
```

Cambia el nombre del host de forma temporal (se pierde al reiniciar).

```
sudo nano /etc/hostname
```

Edita el archivo que contiene el nombre del host para un cambio permanente.

```
sudo nano /etc/hosts
```

Edita el archivo de resolución local de nombres para reflejar el nuevo hostname.

```
sudo reboot
```

Reinicia el sistema para aplicar los cambios de nombre.

3. Configurar red (manual y automática)

```
nmcli device status
```

Muestra el estado de los dispositivos de red.

```
nmcli device connect eth0
```

Conecta el dispositivo de red 'eth0' usando configuración automática (DHCP).

```
sudo systemctl restart NetworkManager
```

Reinicia el servicio de gestión de red para aplicar cambios.

```
sudo netplan apply
```

Aplica la configuración de red definida en los archivos YAML de Netplan.

4. ufw: Firewall en Linux

El firewall actúa como una barrera de seguridad entre tu sistema y la red. Su función principal es permitir o bloquear el tráfico de red entrante y saliente según reglas que definas. ufw (Uncomplicated Firewall) es una herramienta que simplifica la configuración de estas reglas para proteger tu sistema.

```
sudo ufw status verbose
```

Muestra el estado del firewall y las reglas actuales con detalles.

```
sudo ufw enable
```

Activa el firewall y aplica las reglas configuradas.

```
sudo ufw disable
```

Desactiva temporalmente el firewall.

```
sudo ufw allow 22
```

Permite el tráfico entrante al puerto 22 (SSH).

```
sudo ufw deny 80
```

Bloquea el tráfico entrante al puerto 80 (HTTP).

```
sudo ufw delete allow 22
```

Elimina la regla que permitía el tráfico por el puerto 22.

5. Habilitar servicio SSH

SSH permite conectarse de forma remota y segura a otro equipo a través de la red. Es fundamental para administrar servidores, ya que proporciona una terminal cifrada. Con SSH puedes ejecutar comandos, transferir archivos y gestionar el sistema sin estar físicamente presente.

```
sudo apt install openssh-server
```

Instala el servidor SSH para permitir conexiones remotas.

```
sudo systemctl enable ssh
```

Configura el servicio SSH para que se inicie automáticamente al arrancar el sistema.

```
sudo systemctl start ssh
```

Inicia inmediatamente el servicio SSH.

```
sudo systemctl status ssh
```

Muestra el estado actual del servicio SSH.

```
sudo ufw allow ssh
```

Permite el tráfico entrante al servicio SSH (puerto 22) en el firewall.