**EJERCICIO PRÁCTICO - FASE 1  
  
Identificación de la interfaz de red activa**

* Se usó el comando:

ip a

* Interfaz detectada: enp0s3
* IP dinámica inicial: 10.0.2.15

**Análisis de la red local real (desde Ubuntu host)**

* Dirección IP del host: 192.168.0.105
* Puerta de enlace: 192.168.0.1
* Decidimos configurar:  
  + IP estática: 192.168.0.150/24
  + Gateway: 192.168.0.1
  + DNS: 8.8.8.8 y 8.8.4.4

**Modificación del archivo de configuración de red**

* Ruta: /etc/netplan/00-installer-config.yaml
* Configuración aplicada:  
  network:
* version: 2
* ethernets:
* enp0s3:
* dhcp4: no
* addresses:
* - 192.168.0.150/24
* gateway4: 192.168.0.1
* nameservers:
* addresses:
* - 8.8.8.8
* - 8.8.4.4

**Corrección de errores detectados**

* Error: Permissions are too open
* Solución aplicada:

sudo chmod 600 /etc/netplan/00-installer-config.yaml

**Aplicación de cambios**

* Se ejecutó:

sudo netplan apply

**Verificación de conectividad**

* Se comprobó la red con:
* ping 192.168.0.1
* ping 8.8.8.8
* ping [google.com](http://google.com)

### **🎯 Resultado final**

✔️ El servidor Ubuntu tiene IP fija: 192.168.0.150  
 ✔️ Conectividad confirmada con gateway y servidores externos.  
 ✔️ Configuración documentada y funcional.

**EJERCICIO PRÁCTICO - FASE 2**

### **🧩 1. Configuración del Servidor DHCP**

**Instalación del paquete:  
  
sudo apt install isc-dhcp-server**

**Configuración del archivo /etc/dhcp/dhcpd.conf con subnet real de la red:  
  
subnet 192.168.0.0 netmask 255.255.255.0 {**

**range 192.168.0.100 192.168.0.120;**

**option routers 192.168.0.1;**

**option domain-name-servers 192.168.0.150;**

**default-lease-time 600;**

**max-lease-time 7200;**

**}**

**Interfaz especificada en /etc/default/isc-dhcp-server:  
  
INTERFACESv4="enp0s3"**

* **Corrección de errores al inicio (No subnet declaration, Not configured to listen) ajustando la red y permisos del archivo.**

**Verificación del estado:  
  
sudo systemctl status isc-dhcp-server**

### **🌐 2. Configuración del Servidor DNS Interno**

**Instalación de bind9:  
  
sudo apt install bind9**

**Creación de zona directa en /etc/bind/named.conf.local:  
  
  
zone "empresa.local" {**

**type master;**

**file "/etc/bind/db.empresa.local";**

**}**

**Configuración del archivo de zona /etc/bind/db.empresa.local:  
  
  
$TTL 604800**

**@ IN SOA empresa.local. root.empresa.local. (**

**2 ; Serial**

**604800 ; Refresh**

**86400 ; Retry**

**2419200 ; Expire**

**604800 ) ; Negative Cache TTL**

**@ IN NS empresa.local.**

**pc1 IN A 192.168.0.101**

### **🧪 3. Pruebas de funcionamiento**

**Comprobación de la resolución DNS:  
  
  
ping pc1.empresa.local**

**dig pc1.empresa.local**

* **Solución a errores de tipo "Destination Host Unreachable" o "Fallo temporal en la resolución" verificando:**
  + **Que la interfaz esté activa y con IP.**
  + **Que el servicio esté active (running).**
  + **Que el cliente tenga configurado el servidor DNS 192.168.0.150.**

**EJERCICIO PRÁCTICO - FASE 3  
  
Instalación y activación del firewall UFW  
 Se utilizó ufw como herramienta de gestión de firewall por su sencillez:  
  
sudo apt install ufw**

**sudo ufw enable**

**Permitir únicamente tráfico esencial**

**SSH (puerto 22) para administración remota:  
  
  
sudo ufw allow 22/tcp**

**HTTP (puerto 80) para el servidor web:  
  
sudo ufw allow 80/tcp**

**DNS (puerto 53) si el servidor actúa como DNS:  
  
  
sudo ufw allow 53**

**Restringir accesos desde IPs específicas**

**Solo se permitió el acceso SSH desde el equipo cliente:  
  
  
sudo ufw allow from 192.168.0.150 to any port 22**

**Aplicar reglas de seguridad avanzadas**

**Bloqueo por defecto de todo el tráfico entrante:  
  
sudo ufw default deny incoming**

**sudo ufw default allow outgoing**

**Protección contra ataques por fuerza bruta en SSH:  
  
sudo ufw limit ssh/tcp**

**Verificación del estado del firewall**

* **Comprobación de reglas activas:  
    
  sudo ufw status numbered**

**EJERCICIO EMPRESARIAL - FASE 1**

**👤 Usuarios creados**

| **Usuario** | **Rol** |
| --- | --- |
| **ana** | **Desarrolladora web** |
| **carlos** | **Técnico de infraestructura** |
| **elena** | **Responsable de documentación** |

### **👥 Grupos creados**

* **webdev → Para desarrolladores**
* **infra → Para infraestructura**
* **docs → Para documentación**

### **🔁 Asignación de usuarios a grupos**

| **Usuario** | **Grupo asignado** |
| --- | --- |
| **ana** | **webdev** |
| **carlos** | **infra** |
| **elena** | **docs** |

### **🔒 Seguridad**

* **Se establecieron contraseñas seguras para cada usuario.**
* **Se verificó correctamente la pertenencia a los grupos mediante el comando groups.**

**EJERCICIO EMPRESARIAL - FASE 2**

**🛠️ Pasos realizados:**

**Creación de las carpetas para cada grupo  
  
  
sudo mkdir -p /grupos/web /grupos/infra /grupos/docs**

**Asignación de propiedad de grupo  
  
  
sudo chown :webdev /grupos/web**

**sudo chown :infra /grupos/infra**

**sudo chown :docs /grupos/docs**

**Establecimiento de permisos (rwxrwx---)  
  
  
sudo chmod 770 /grupos/web**

**sudo chmod 770 /grupos/infra**

**sudo chmod 770 /grupos/docs**

**Activación de setgid para herencia de grupo  
  
  
sudo chmod g+s /grupos/web**

**sudo chmod g+s /grupos/infra**

**sudo chmod g+s /grupos/docs**

**EJERCICIO EMPRESARIAL - FASE 3**

### **🔨 Pasos realizados:**

1. **📄 Crear archivo plan.txt en /grupos/docs:**

**sudo touch /grupos/docs/plan.txt**

1. **👤 Otorgar propiedad del archivo a elena:**

**sudo chown elena:docs /grupos/docs/plan.txt**

1. **🔐 Establecer permisos base:**

* **Elena: lectura y escritura**
* **ana y carlos: solo lectura**

**sudo setfacl -m u:ana:r-- /grupos/docs/plan.txt**

**sudo setfacl -m u:carlos:r-- /grupos/docs/plan.txt**

1. **👥 Crear grupo lectura y añadir a los tres usuarios:**

**sudo groupadd lectura**

**sudo usermod -aG lectura ana**

**sudo usermod -aG lectura carlos**

**sudo usermod -aG lectura elena**

***Esto permite futura gestión más fácil, aunque no se usó directamente en los ACLs.***

1. **🔍 Verificar permisos aplicados:**

**getfacl /grupos/docs/plan.txt**

**EJERCICIO EMPRESARIAL - FASE 4**

🔐 **Política de caducidad de contraseñas** Se estableció una caducidad obligatoria de **60 días** para todos los usuarios del sistema usando el comando:  
  
sudo chage --maxdays 60 [usuario]

✔️ Asegura que las contraseñas se renueven periódicamente, reforzando la seguridad.

🚫 **Bloqueo de acceso SSH al usuario elena** Se denegó el acceso remoto por SSH al usuario elena editando el archivo de configuración:  
  
  
sudo nano /etc/ssh/sshd\_config

Se añadió:  
  
DenyUsers elena

Y se reinició el servicio:  
  
sudo systemctl restart ssh

💬 **Mensaje de bienvenida personalizado para nuevos usuarios** Se editó /etc/skel/.bashrc para que todos los nuevos usuarios vean un mensaje motivador al iniciar sesión.