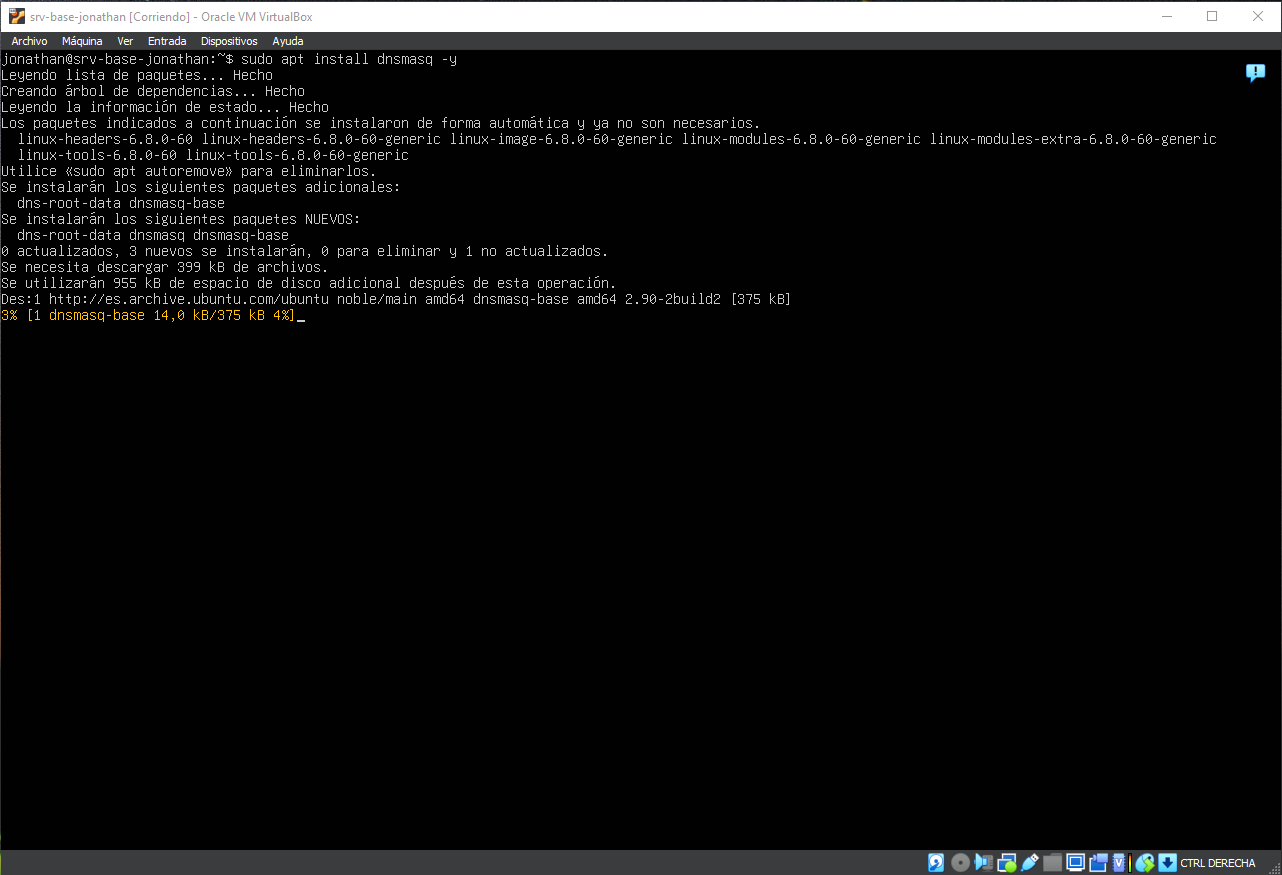
**Gestión de Red Inteligente con Servidor de Direccionamiento y Control de Acceso**

# **Fase 1: Instalación y configuración inicial de dnsmasq**

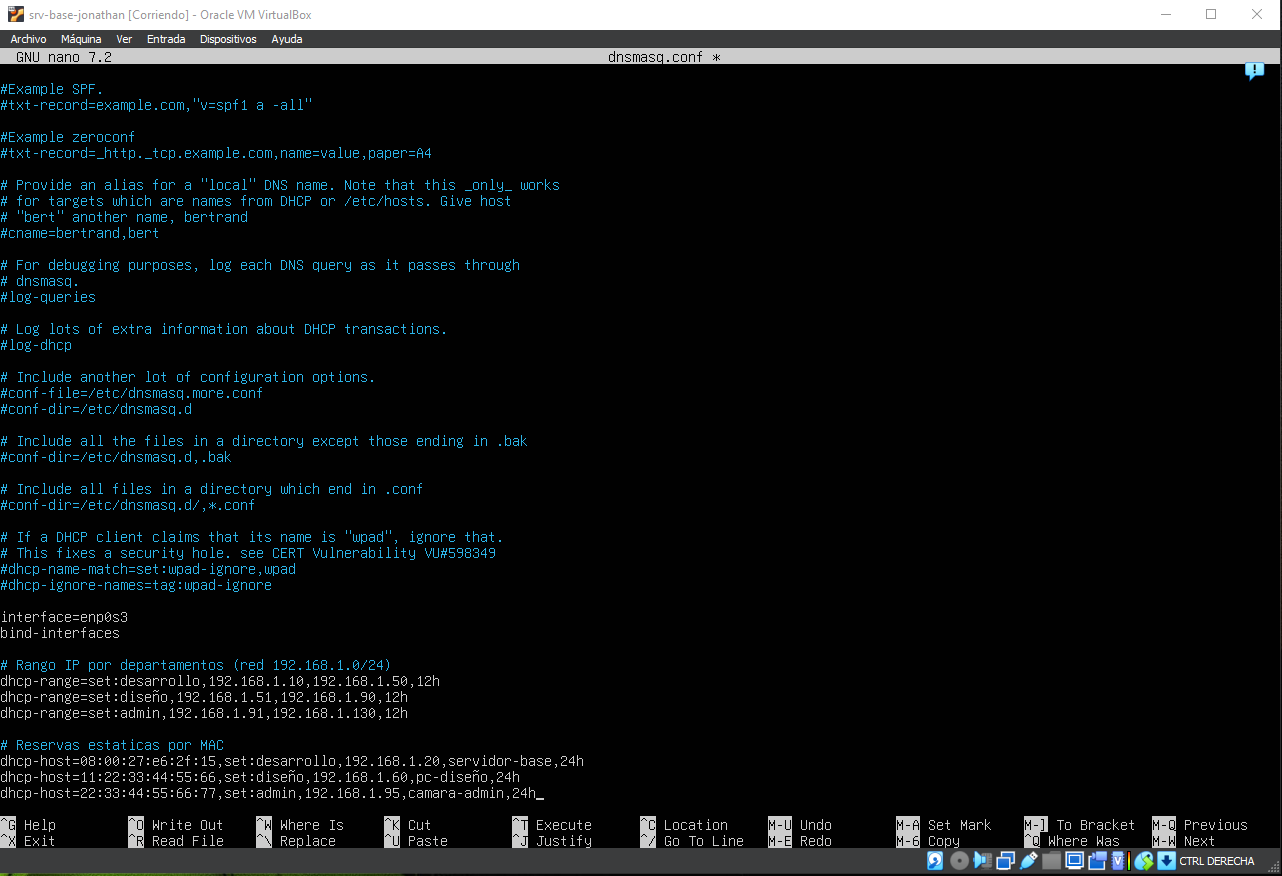
Instalamos el dnsmasq:

sudo apt install dnsmasq -y



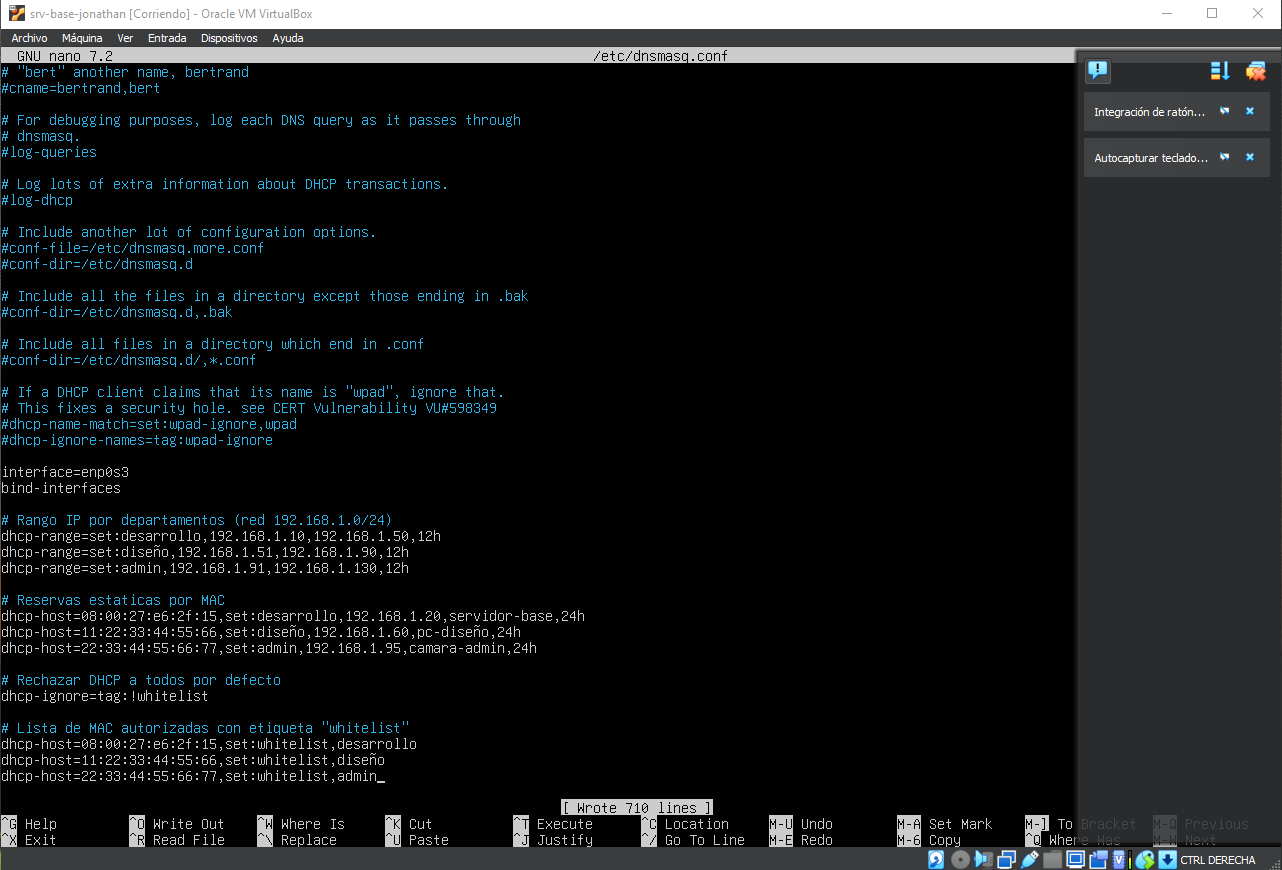
Nos iremos al archivo dsmasq.conf para configurar y definir la interfaz de rangos ip:

sudo nano /etc/dnsmasq.conf

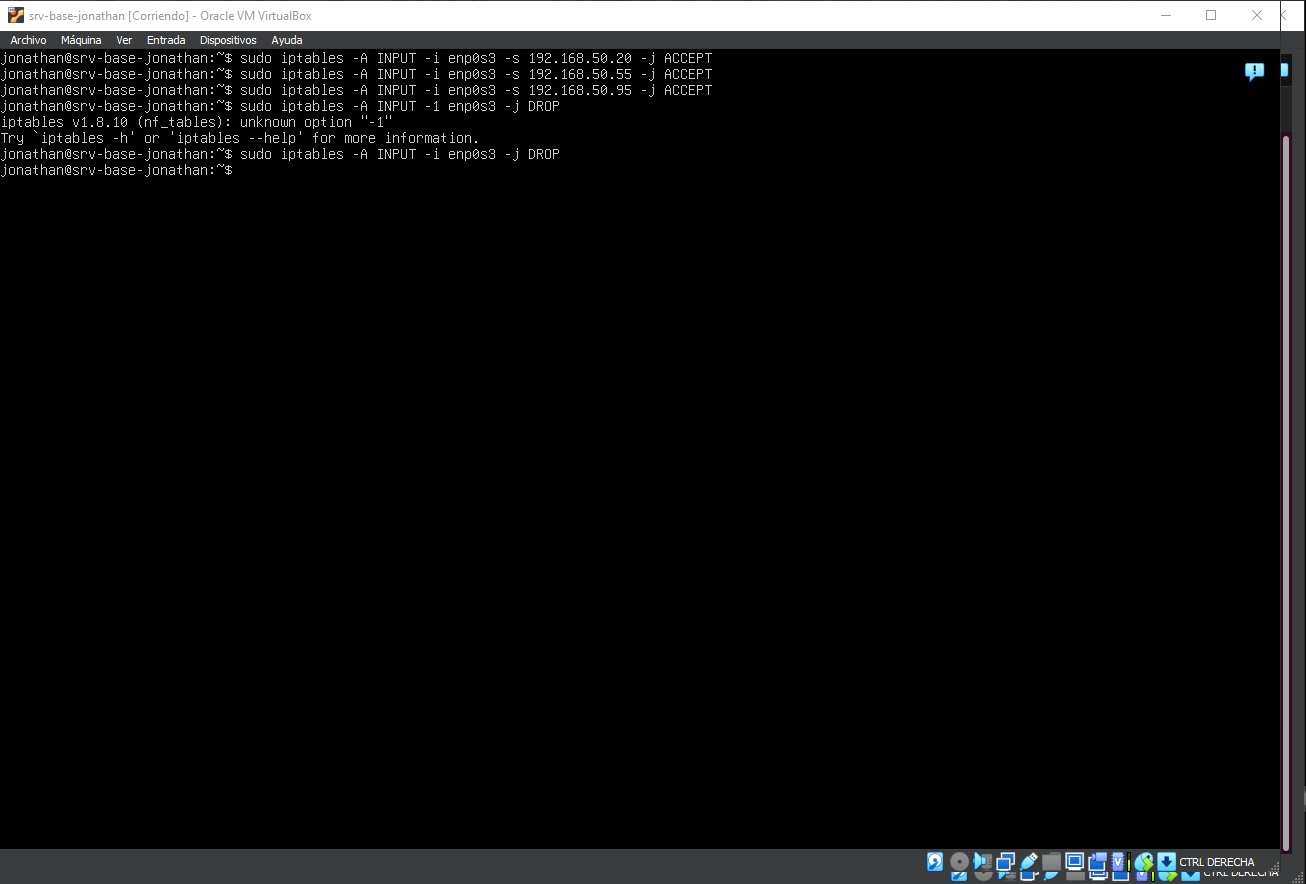


# Fase 2: Control de acceso básico

Añadimos una whitlist con rangos IP en /etc/dnsmasq.conf



Aplicamos reglas iptables para permitir sólo IPs autorizadas:



Instalamos la herramienta para guardar reglas y salvarlas:

sudo apt install iptables-persistent

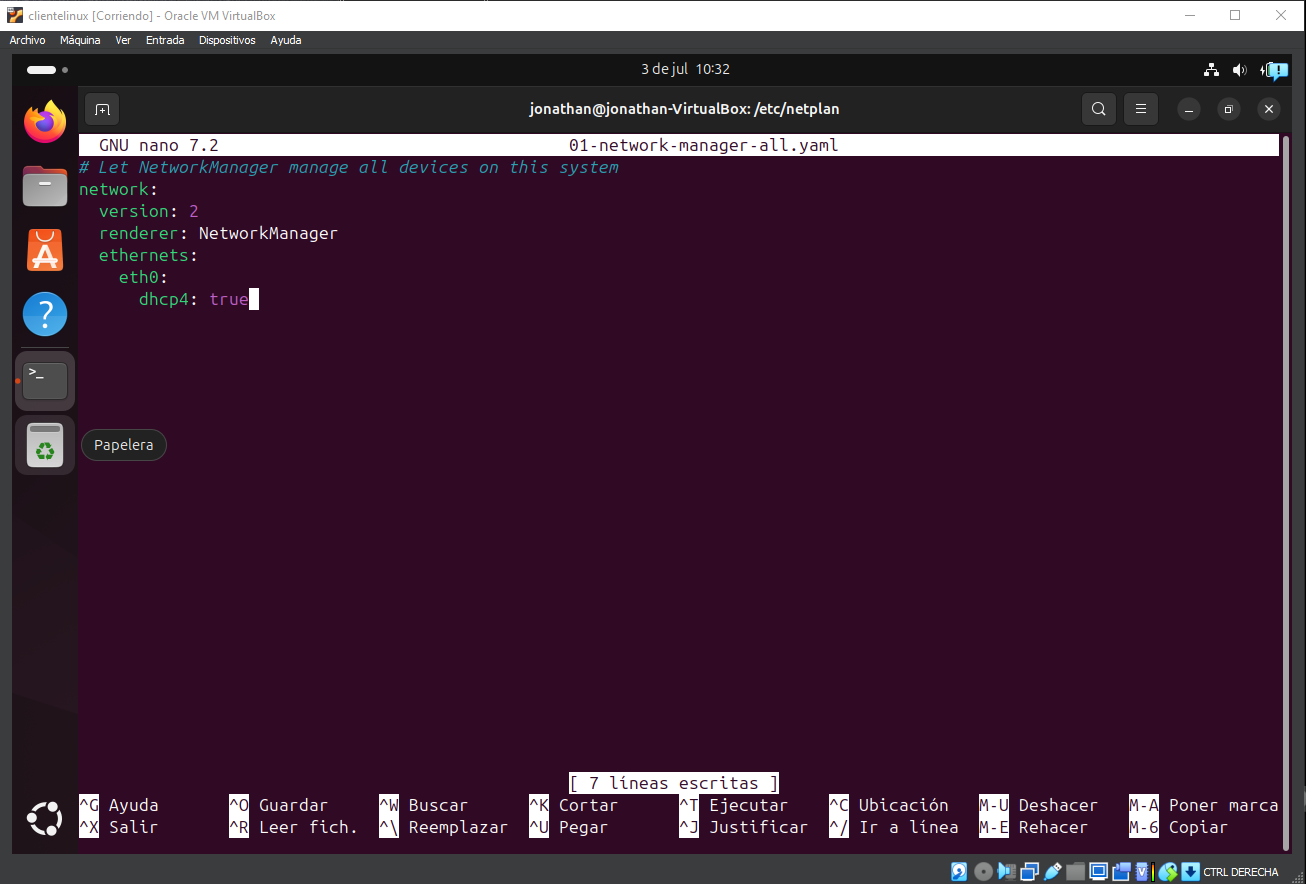
sudo netfilter-persistent save

# Fase 3: Integración con clientes y simulación de red

Configuramos el cliente para el uso de DHCP (archivo netplan):

sudo nano /etc/netplan/01-netcfg.yaml

sudo netplan apply

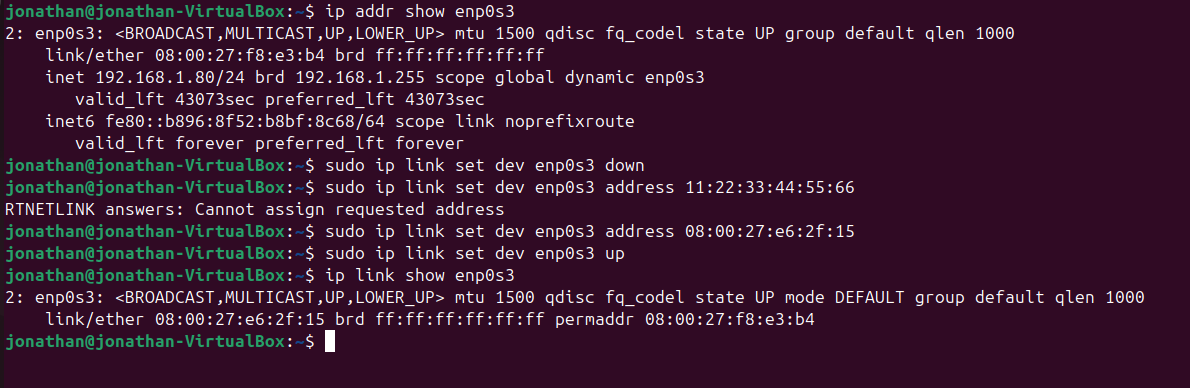


Cambiamos la MAC para simular diferentes dispositivos:

sudo ip link set dev enp0s3 down

sudo ip link set dev enp0s3 08:00:27:e6:2f:15

sudo ip link set dev enp0s3 up



Y podemos comprobar los cambios:

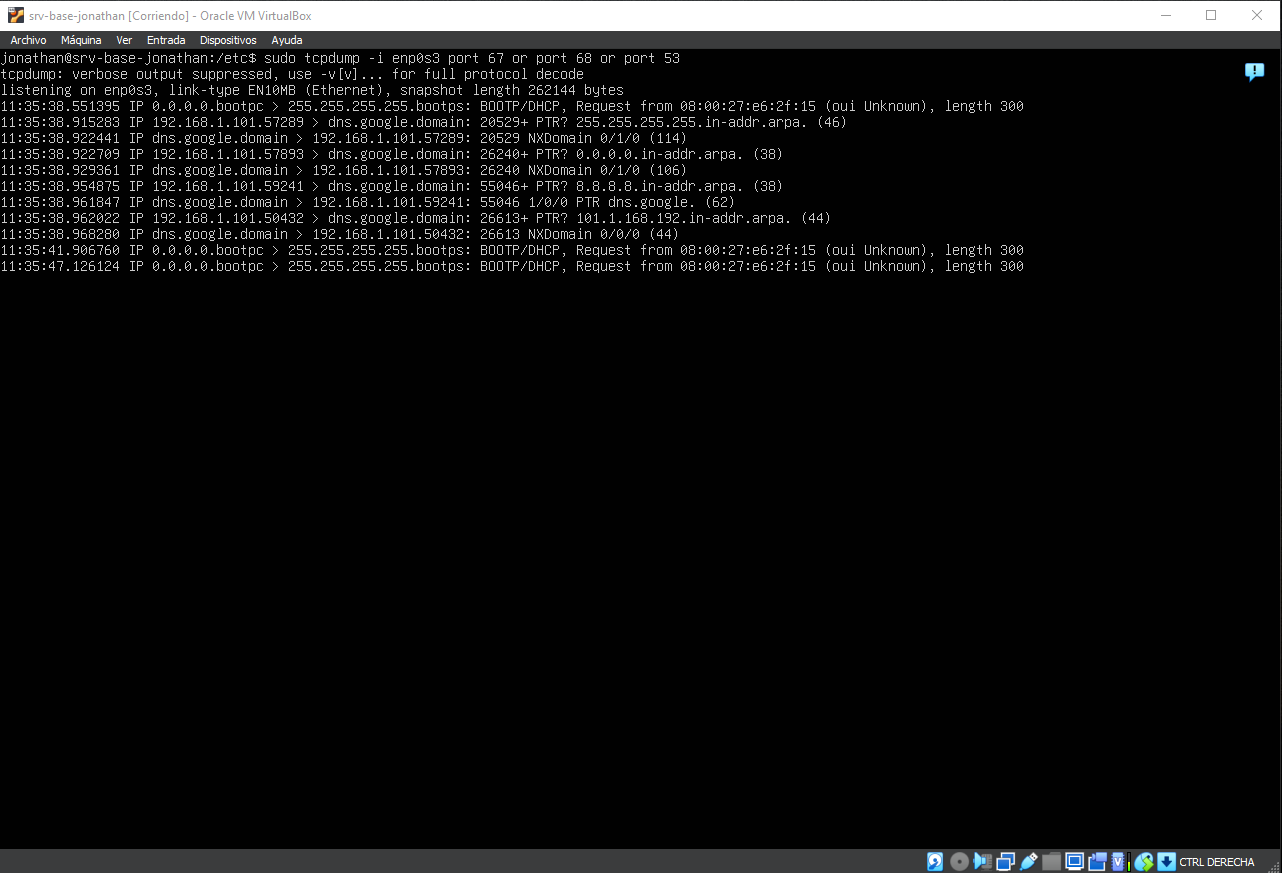
ip link show enp0s3

# Fase 4: Supervisión de tráfico e identificación

Instalamos y usamos tcpdump para capturar el tráfico DHCP y DNS:

sudo apt install tcpdump -y

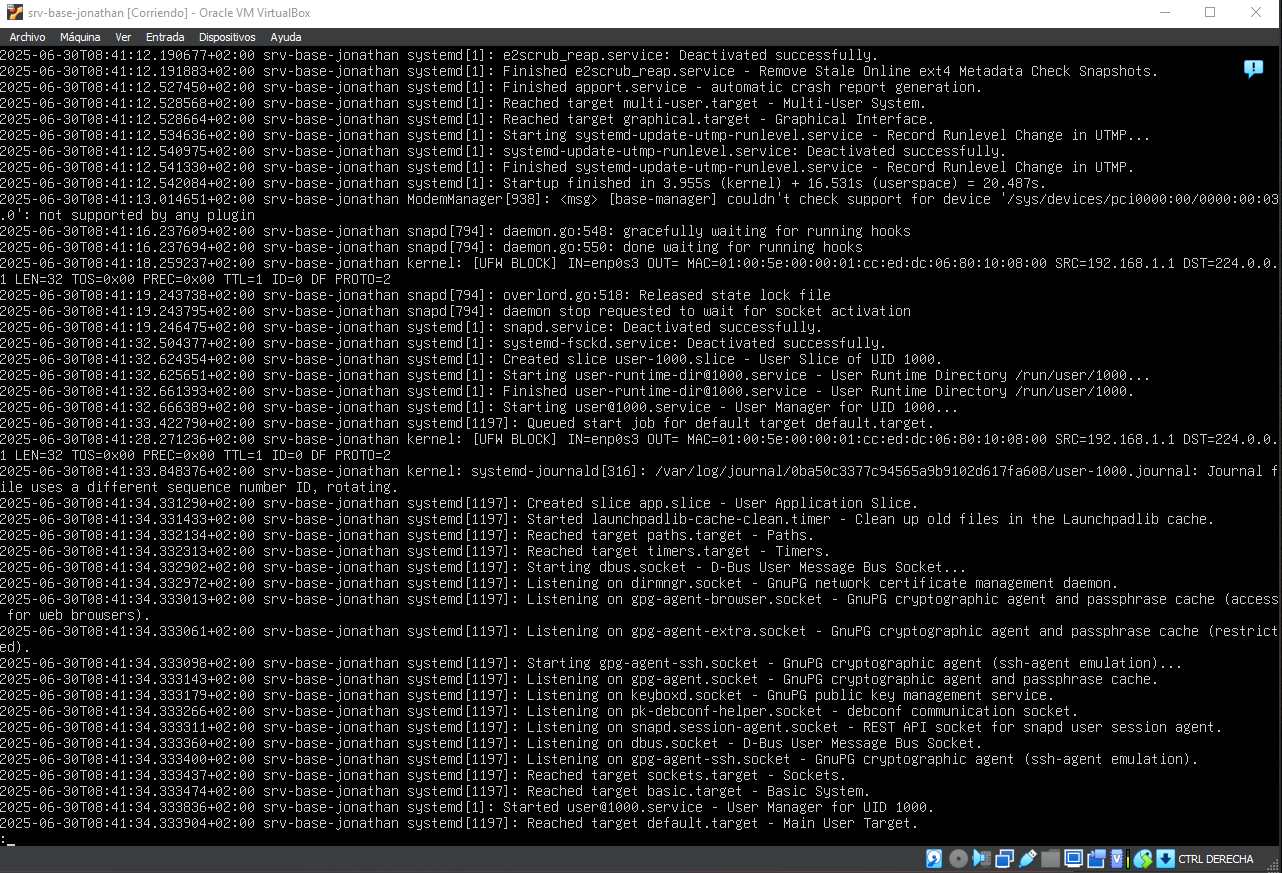
sudo tcpdump -i enp0s3 port 67 or port 68 or port 53



Podemos analizar los logs:

sudo grep dnsmasq /var/log/syslog

sudo tail -f /var/log/syslog | grep dnsmasq



Instalamos y usamos arp-scan para detectar dispositivos conectados:

sudo apt install arp-scan -y

sudo arp-scan --interface=enp0s3 --localnet

