# Escaneo de red

¿Cuál es la dirección IP de tu Metasploitable2?

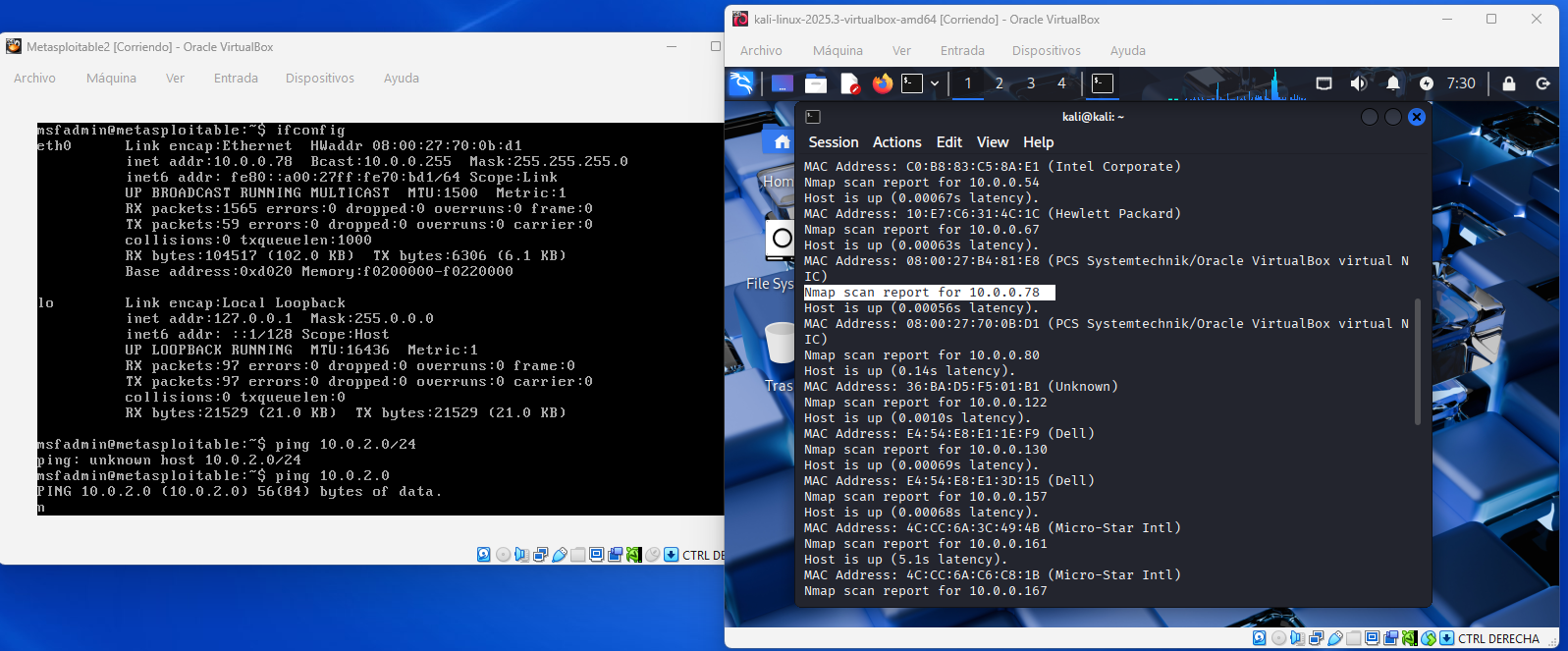
10.0.0.78

¿Te aparece al hacer escaneo con nmap?

Si

¿Qué significa el parámetro -sn en Nmap?

Escaneo de host sin puerto, es decir que Nmap verificara si los host están activos en la red sin escanear los puertos de esos hosts

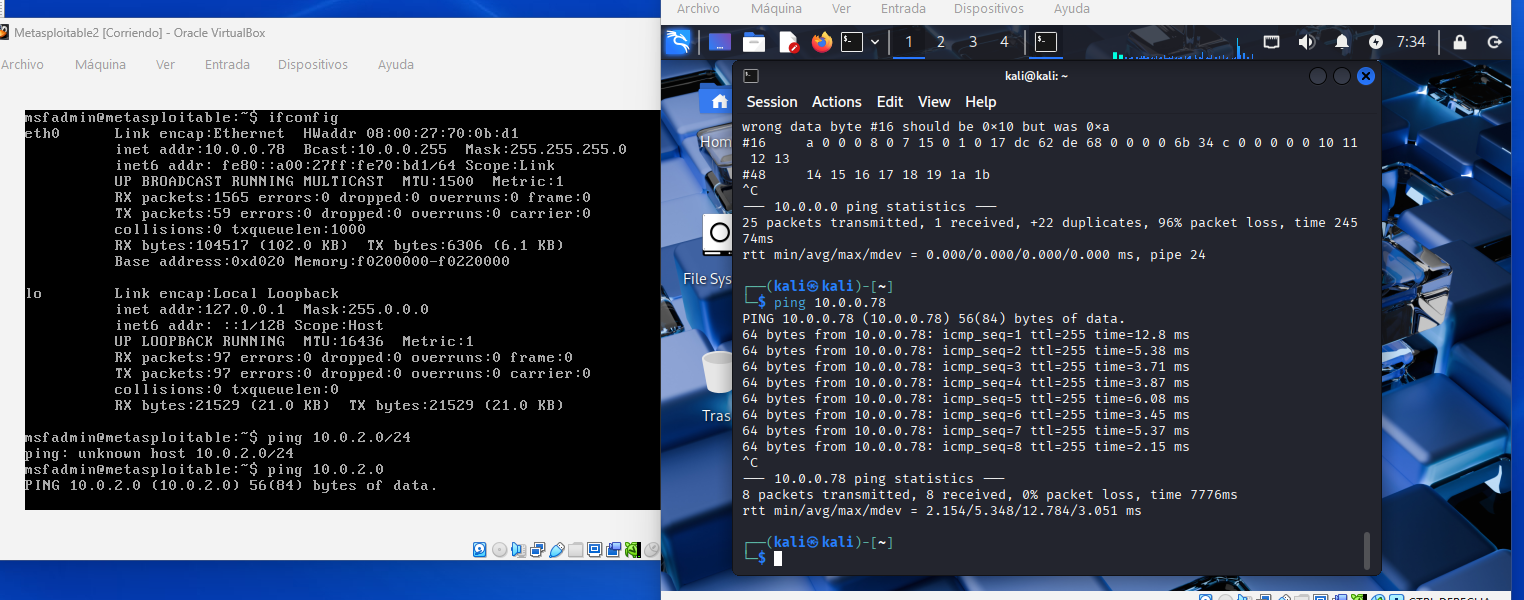




**¿Qué indican los tiempos de respuesta obtenidos?**

Indica los paquetes de datos de 64 bytes fue recibido del servidor como respuesta a la petición con su número de secuencia y los bytes que contiene

**¿Qué información puedes deducir sobre la conectividad entre tu máquina y Metasploitable?**

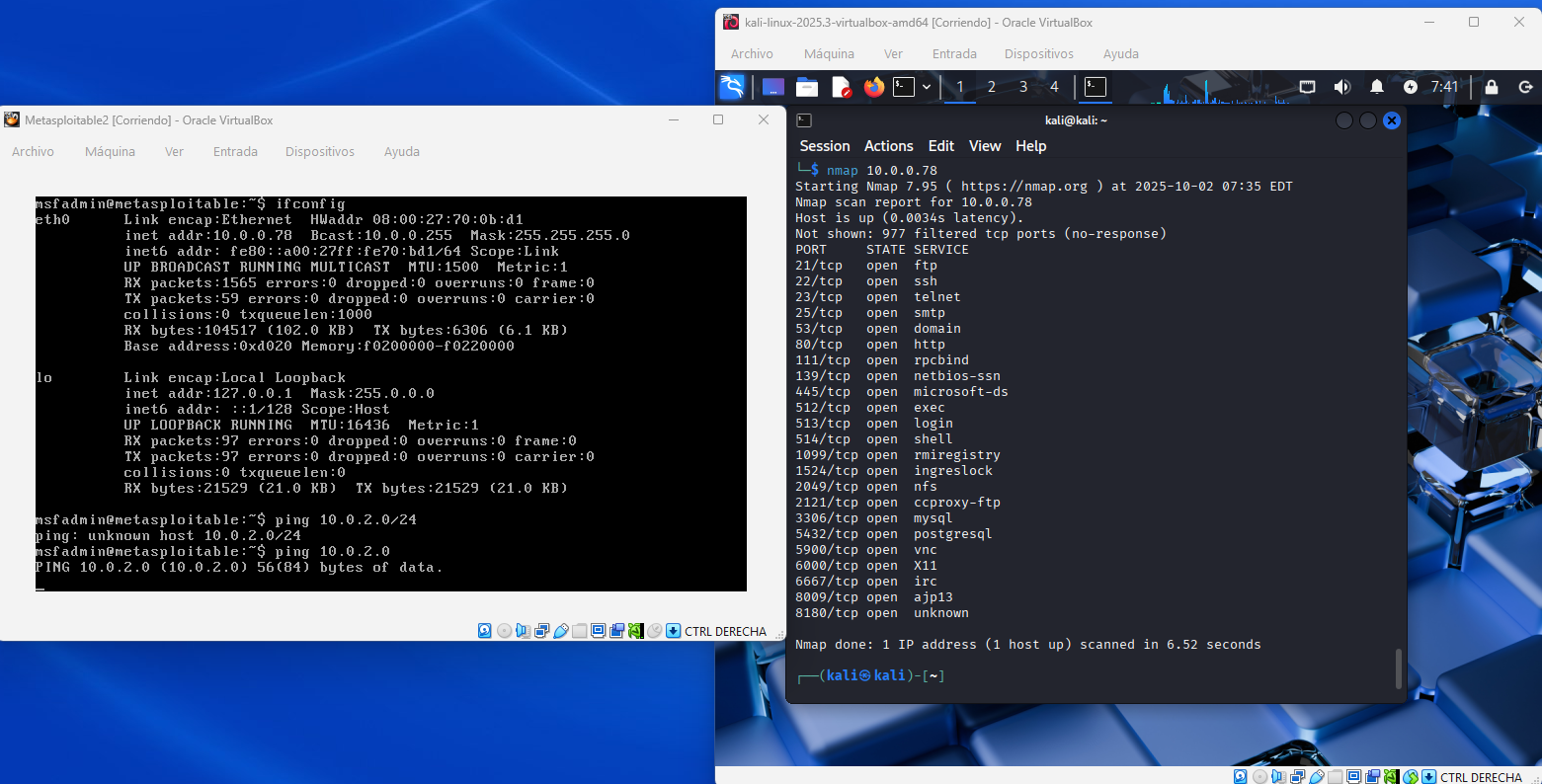
Que ambas se detectan y se puede recibir y enviar paquetes

1. **¿Cuántos puertos están abiertos en el escaneo básico?**

23 puertos

**¿Qué servicios identifica Nmap automáticamente?**

ftp, ssh, telnet, smtp, domain, etc…



1. **¿Cuál de los tres comandos ejecutó más rápido? ¿Por qué crees que es así?**

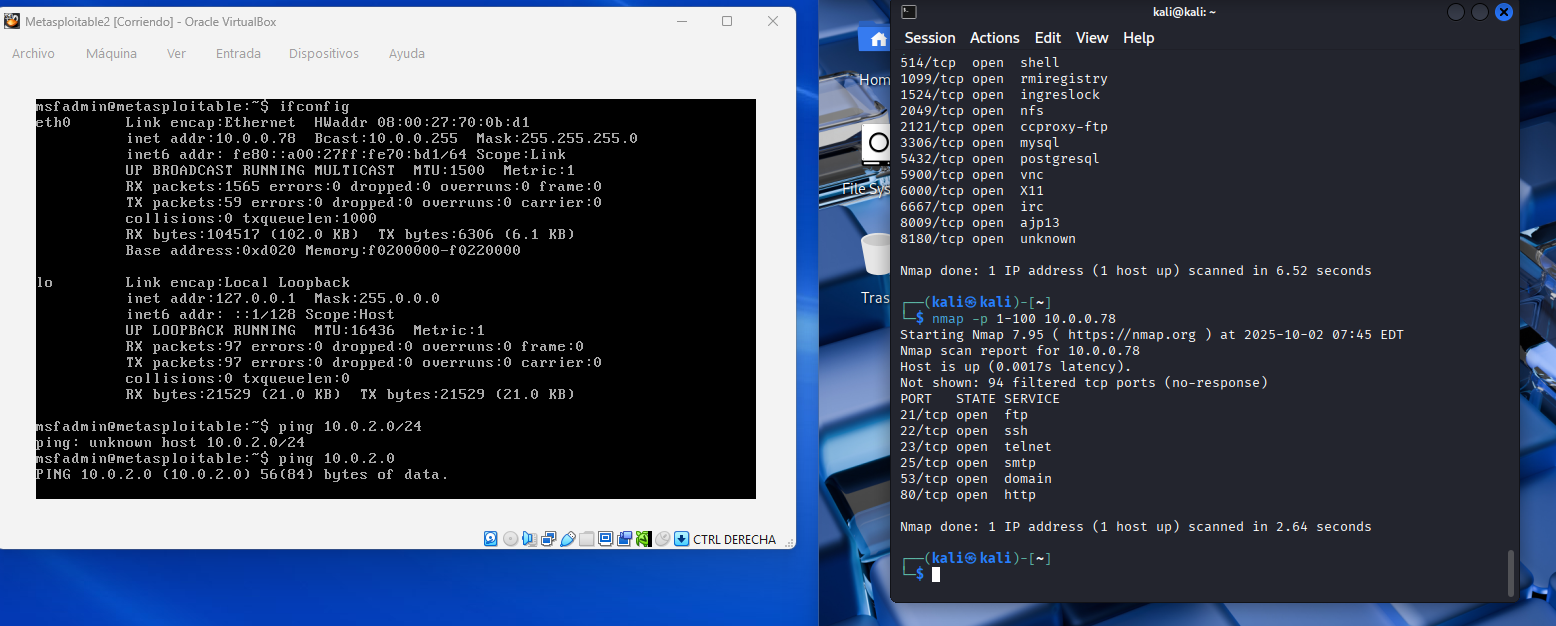
El nmap -p 80,443,8080,8443 ya que va directamente a los indicados, ahorrando tiempo

**En el escaneo de puertos 1-100, ¿cuántos puertos abiertos encontraste comparado con el escaneo completo del ejercicio 3?**

Encontré únicamente 6 en comparación con los 23 del ejercicio 3

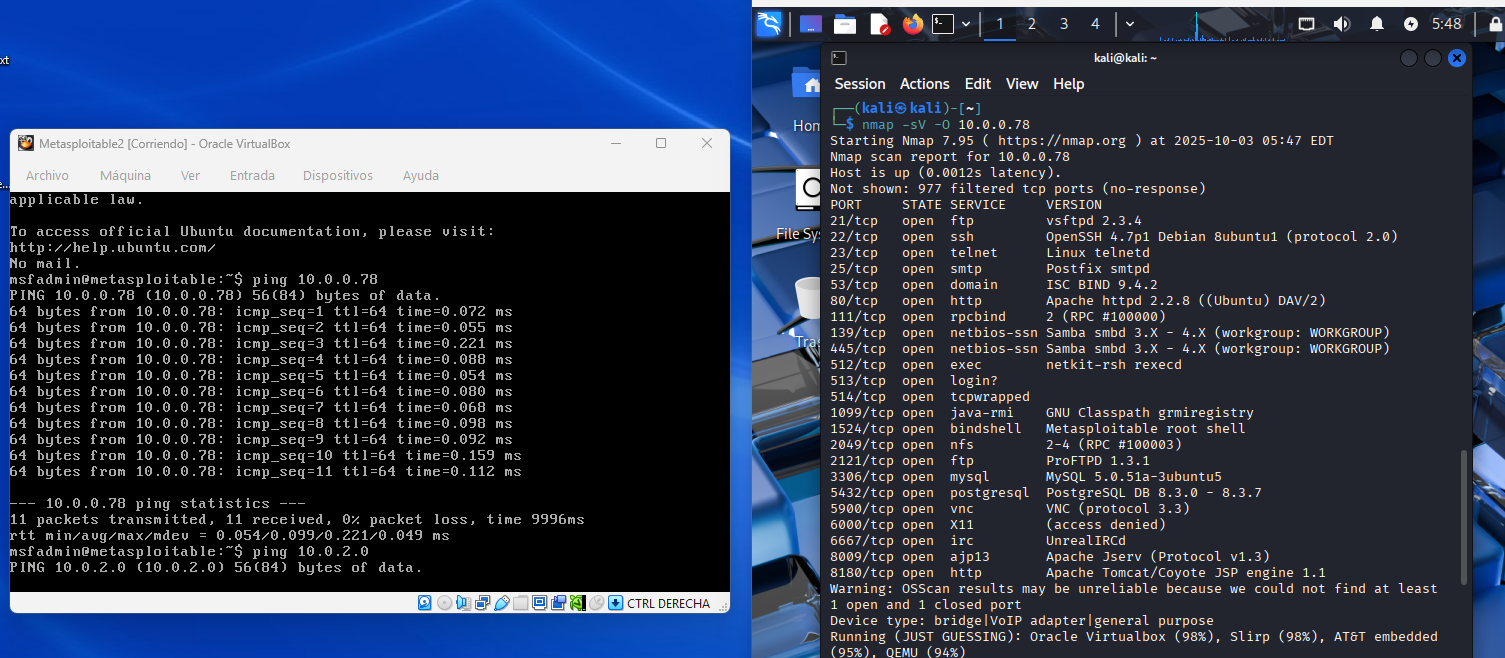
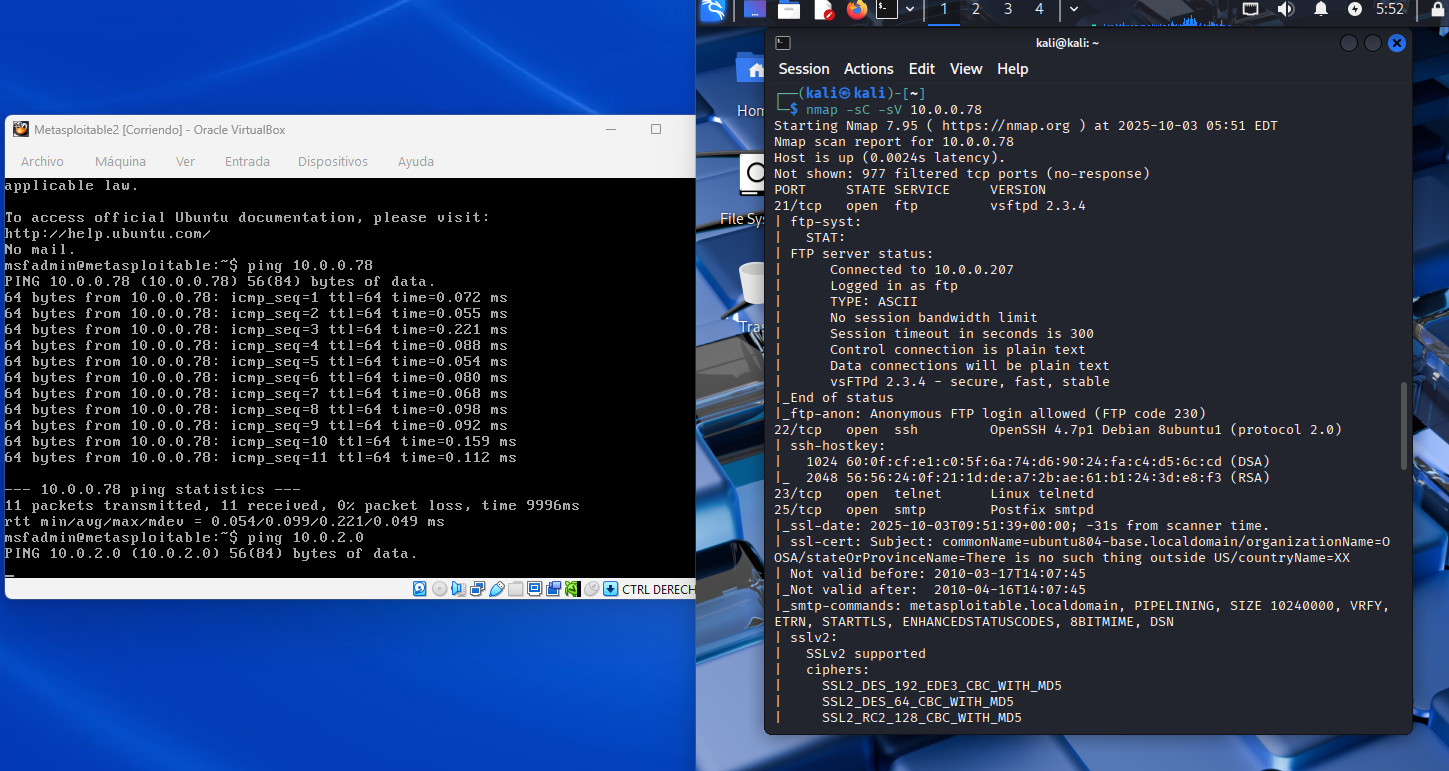
**¿Por qué crees que es útil poder escanear rangos específicos de puertos?**

Más práctico, más rápido y más eficiente



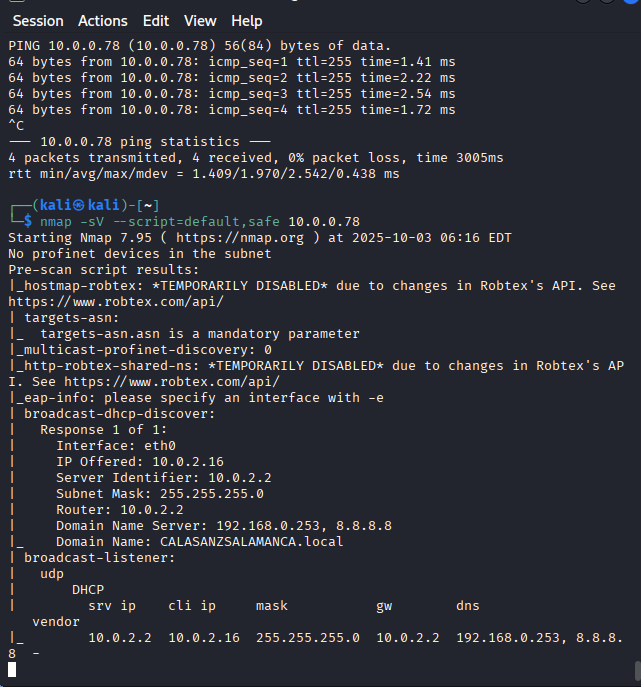
1. **¿Qué sistema operativo ejecuta Metasploitable2?**

Lista los 10 servicios principales con sus versiones exactas



1. ¿Qué servicios aparecen en ejecución en la máquina Metasploitable según la salida?

¿Qué versiones identifica nmap para al menos dos de esos servicios?

¿Hay algún servicio que muestre advertencias o mensajes de seguridad en la salida de los scripts? ¿Cuál y qué significa?

1. 