República Bolivariana de Venezuela

Universidad Centroccidental “Lisandro Alvarado”

Barquisimeto Edo Lara

Variaciones de NMAP

Práctica Evaluada

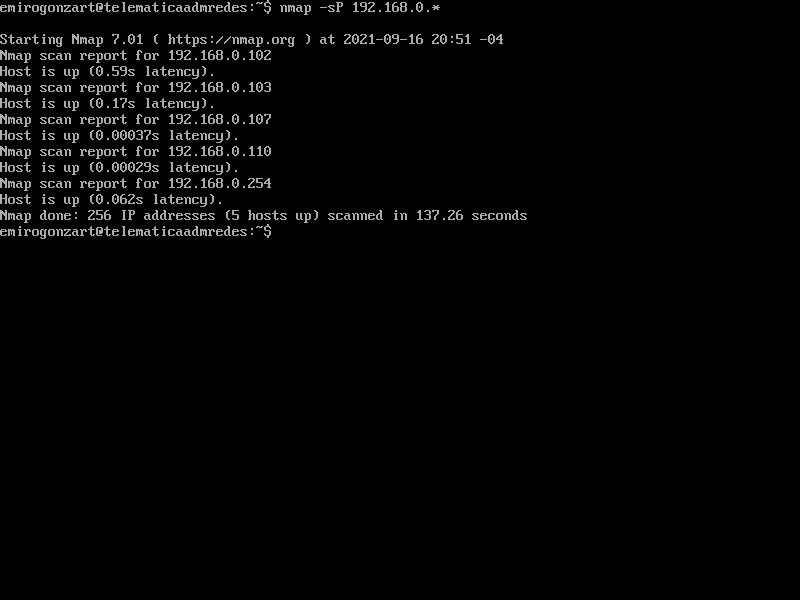
Nombre: Emiro González

C.I 24.567.641

Asignatura: Administración de Redes

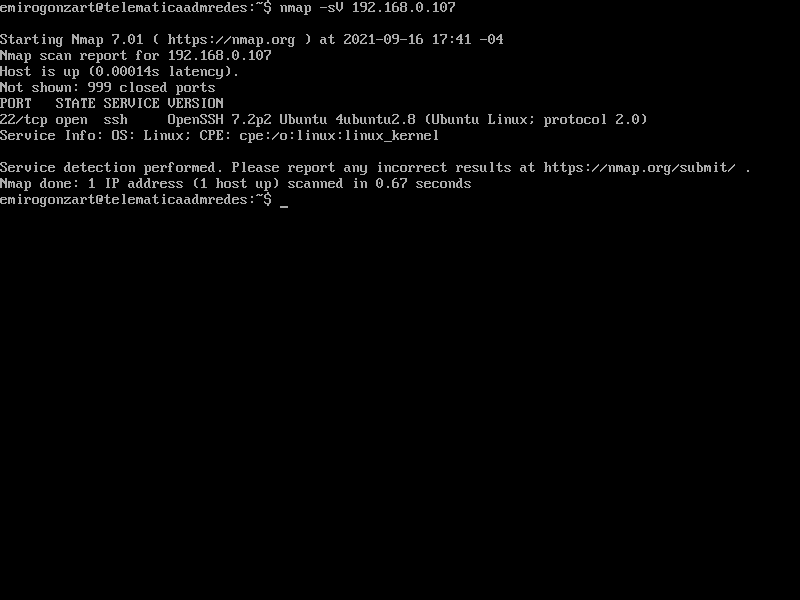
Lista de comandos empleados

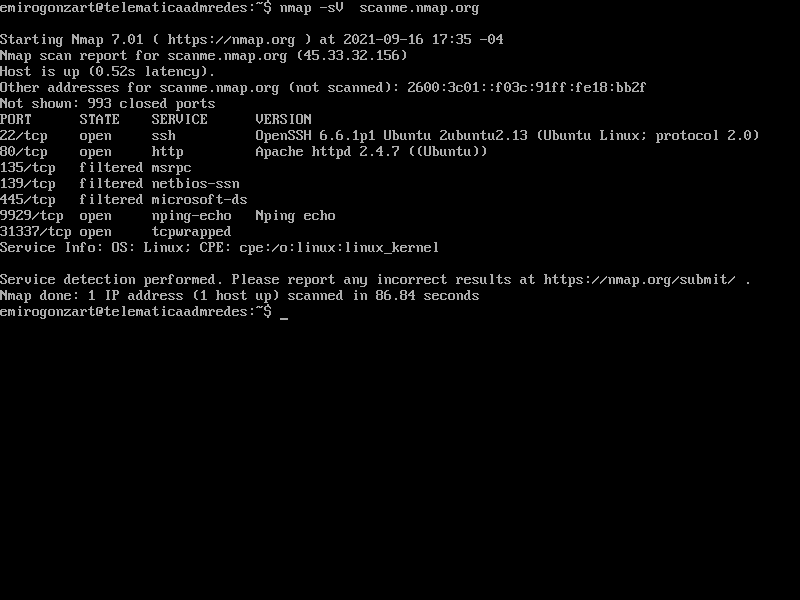
1 Comando para escanear toda la red local



Este comando permite el escanear todos los dispositivos conectados dentro de nuestra red local.

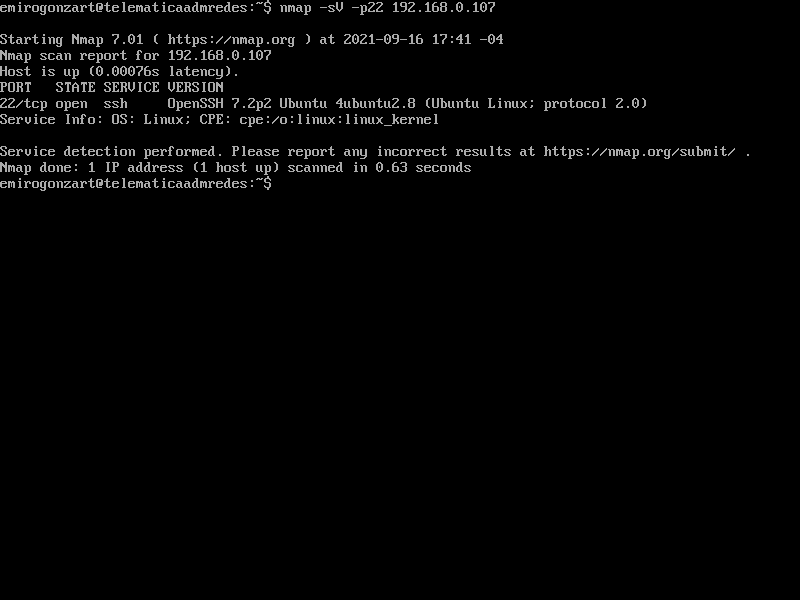
2 Comando -sV





Permite el detectar las versiones

3Verificar estado único de puerto

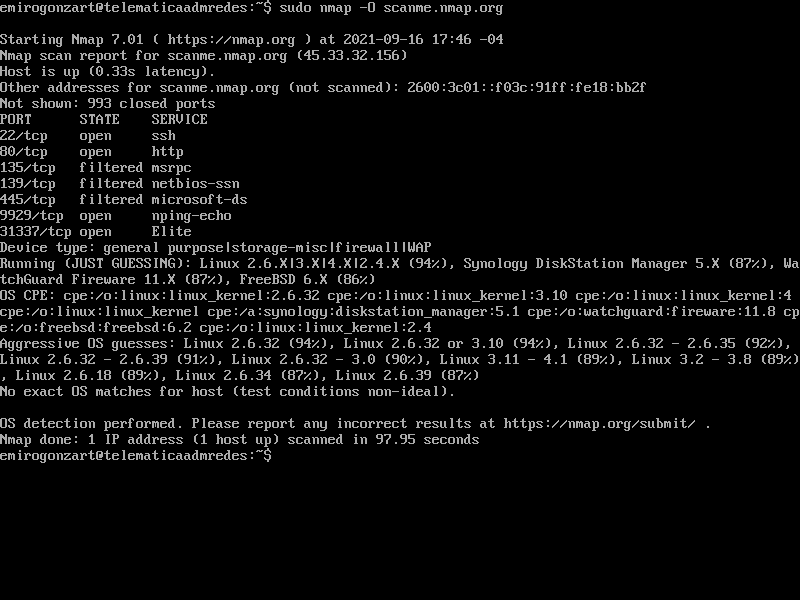




Este comando permite el verificar el estatus y la versión de un puerto en específico (-p22 = Puerto 22). De forma general, si se deseara escanear todos los puertos, solo basta con colocar el parámetro -p y los sondeará todos.

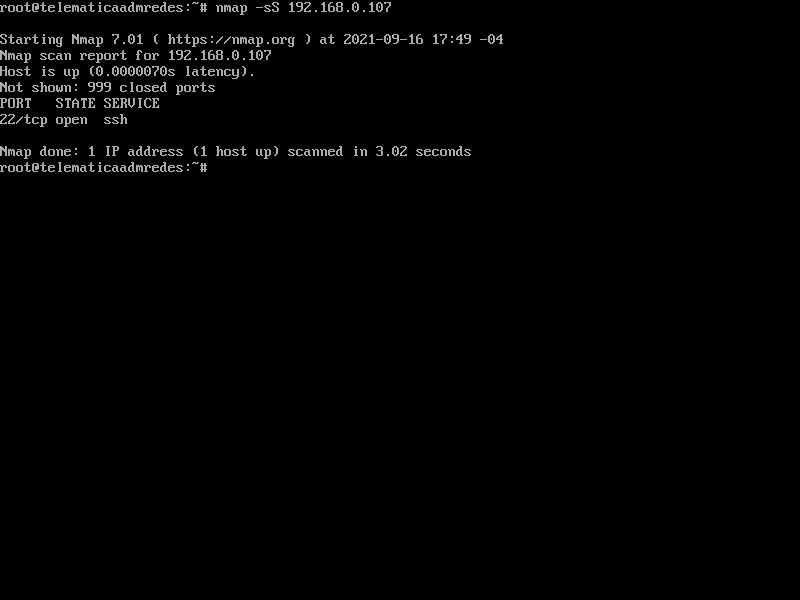
4 Comando -O

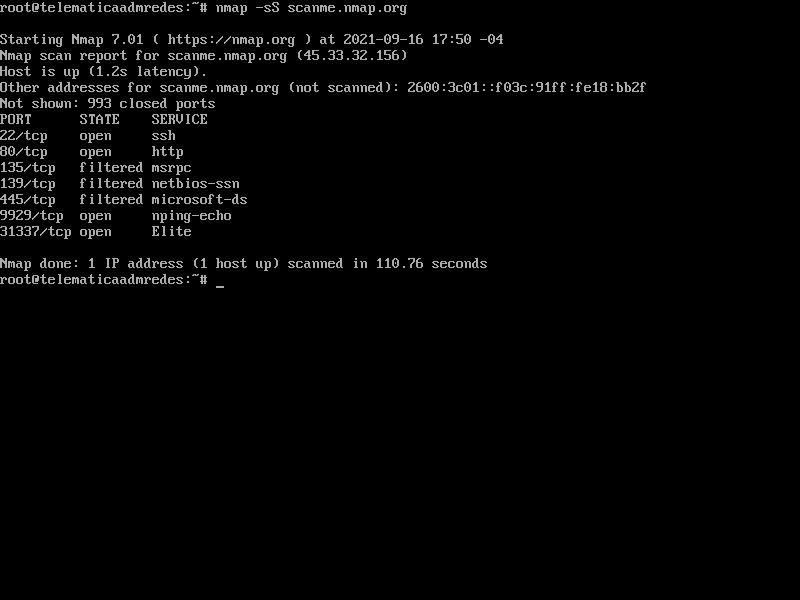




Permite el visualizar la información proveniente del sistema operativo acerca de donde se está realizando el escaneo. En la imagen, el SO detectado corresponde a Linux

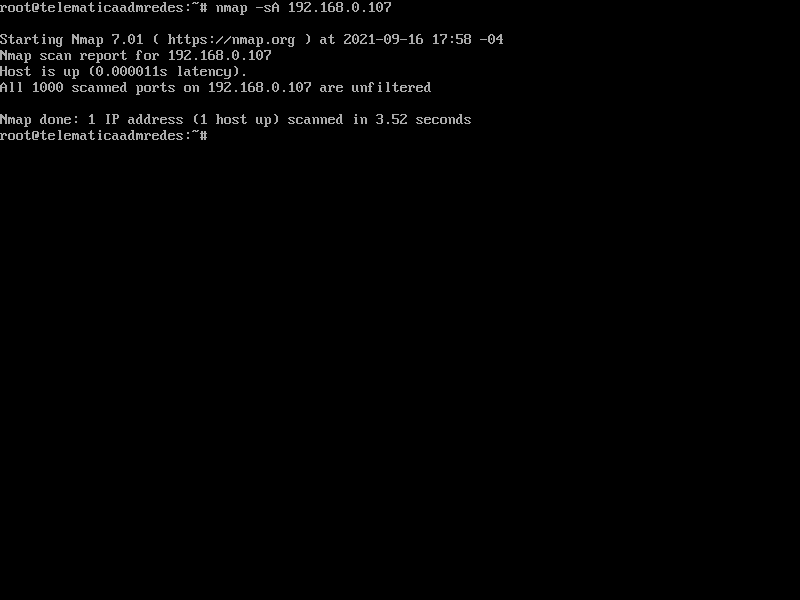
5 Variante nmap -sS

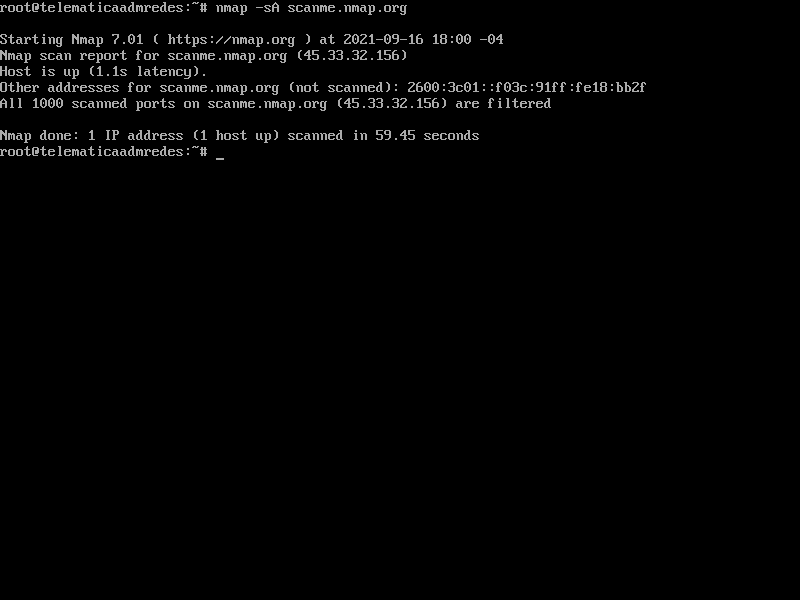




Este comando es una versión de escaneo avanzado que permite un escaneo de todos los puertos TCP.

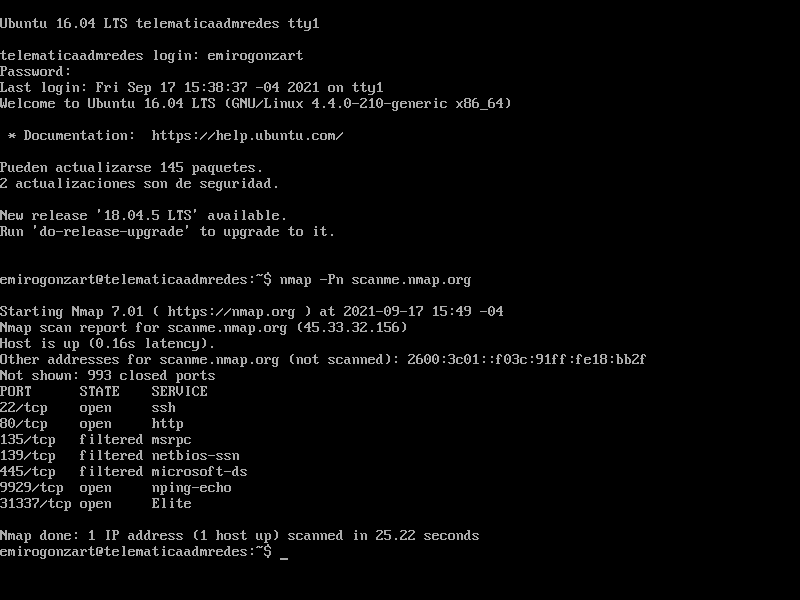
6 Variante nmap -sA





Este comando permite el escanear todos los servicios y puertos activos, mostrando la información de una manera resumida y sencilla.

7 Comando -Pn



El comando -Pn permite realizar todo el escaneo del sistema en todos sus puertos (aún si estos se encuentran apagados o “down”, puesto que permite el obviar estas interfaces y seguir ejecutando el escaneo). De igual forma, sirve para reducir el ruido existente durante el escaneo.

8 Comando -sT



El comando -sT permite el realizar un escaneo completo de todos los puertos disponibles.