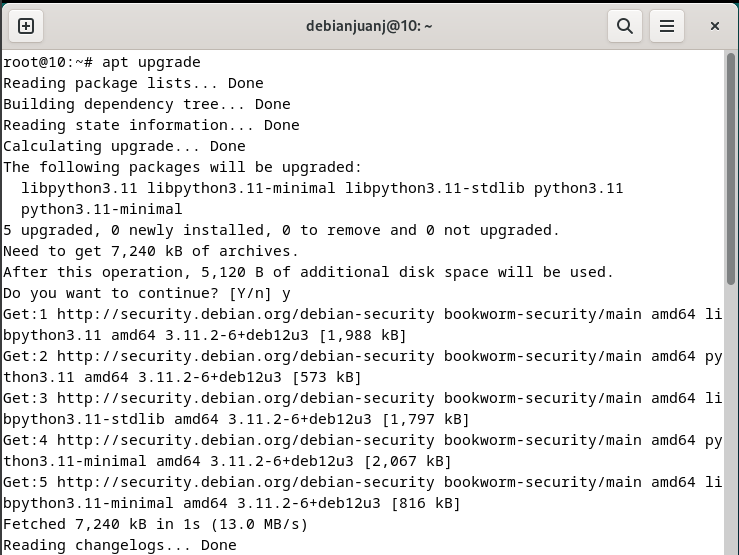
Laboratorio 2\_U3

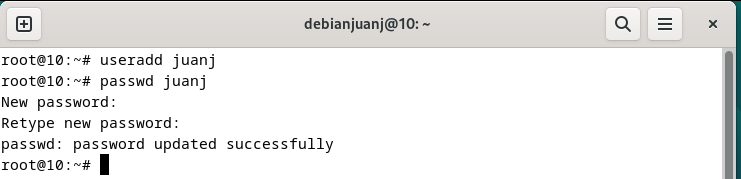
Nombre: Juan Jiménez Fecha: 27/08/2024

1. Emplear el comando de actualización del sistema y aplicaciones:



Para empezar la actividad se realizo la actualizacion de los repositorios de apt con los comandos “apt update” y “apt upgrade” estos 2 realizados mediante root.

1. Gestionar los usuarios:



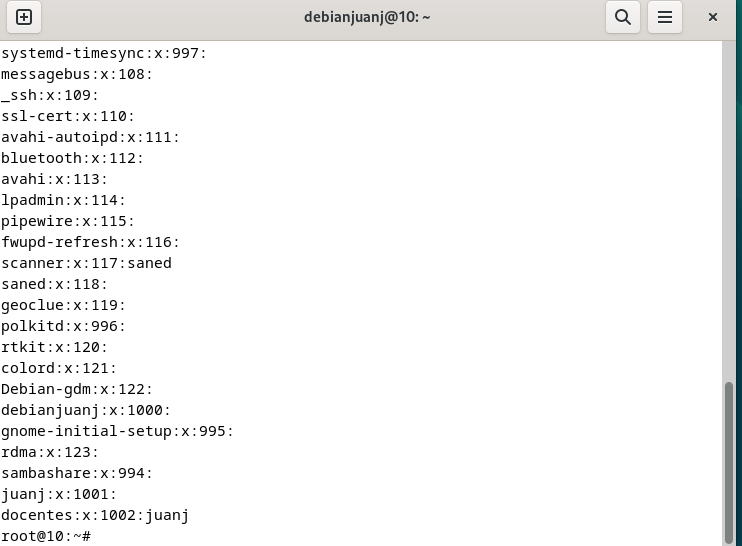
Se crea un usuario con el comando “useradd (nombreusuario)” y su respectiva contraseña con el comando “passwd (nombreusuario)” con este comando se coloca una contraseña a algún usuario que esté registrado.

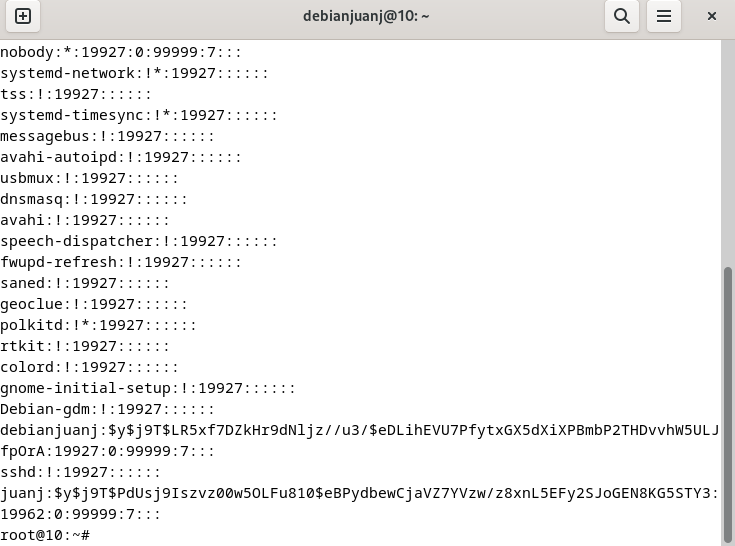


Con el comando “groupadd (nombregrupo)” se agrega un grupo a la listas de grupos del equipo y con el comando “gpasswd -a (nombreusuario) (nombregrupo)” con este comando se agrega un usuario a un grupo.

1. Verificar en los archivos /etc/passwd, /etc/group y /etc/shadow , la creación de los usuarios, la definición de los grupos y las contraseñas encriptadas:

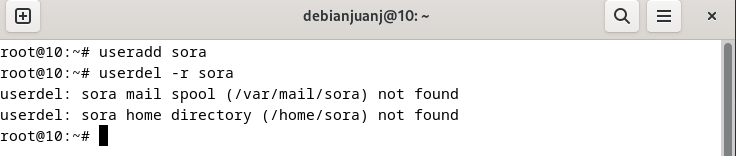






Con los comandos “cat /etc/passwd” se verifica los datos de las contraseñas de los diferentes usuarios que se encuentran en el equipo, con el comando “cat /etc/group” se verifican los grupos que se encuentran en el equipo y con el comando “cat /etc/shadow” este se mira las conexiones entre los usuarios y los grupos.

1. Eliminar un usuario:

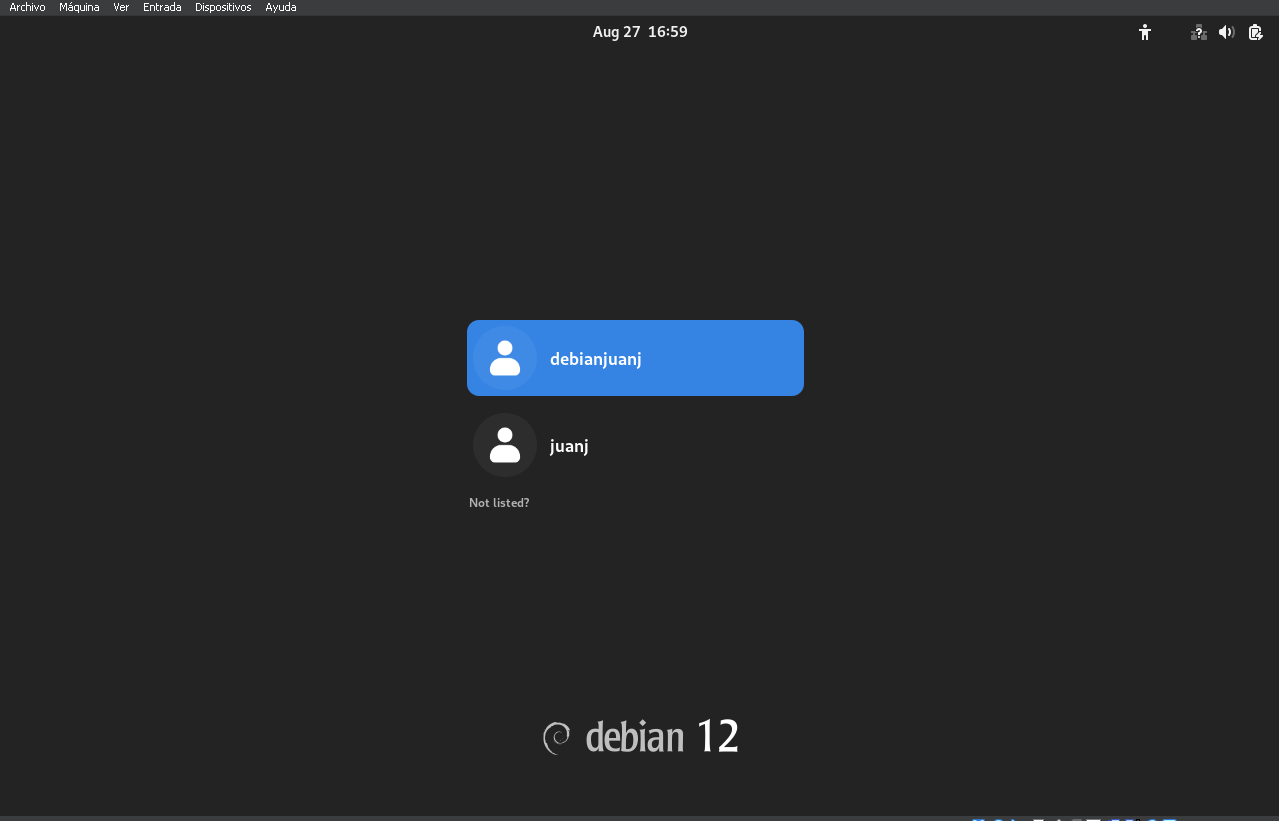
Con el comando “userdel -r (nombreusuario)” se eliminan usuarios del grupo de usuarios del equipo.

1. Bloquear un usuario:



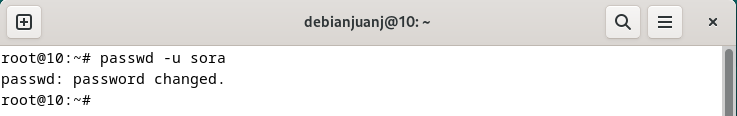
Con el comando “passwd -l (nombreusuario)” se bloquea la cuenta de un usuario que esté ingresado.

1. Verificar que el usuario está bloqueado cambiando de sesión:



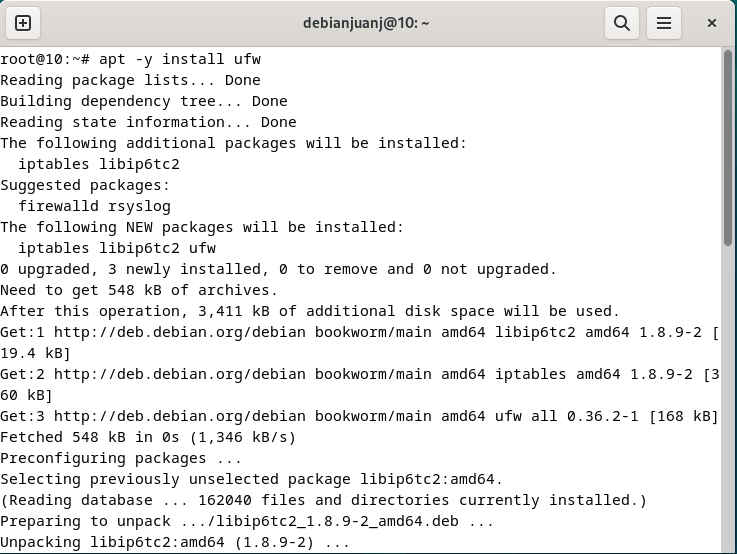
Se logra ver que el usuario “sora” desapareció de la lista de usuarios.

1. Desbloquear al usuario:



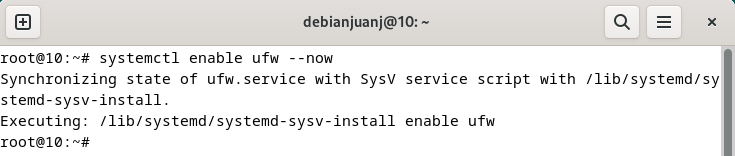
con el comando “passwd -y (nombreusuario)” con este comando se realiza la función de desbloquear un usuario especificado.

1. Instalar el firewall ufw en Linux:



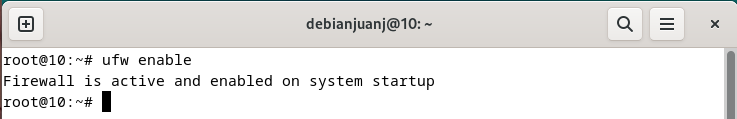
Se instala el firewall ufw con el comando “apt -y install ufw” y genera un montón de líneas de comandos que instalan el ufw.

1. Habilitar e instalar el servicio ufw:



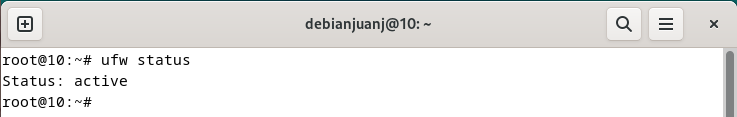
Con el comando “systemctl enable ufw –now” se habilita el servicio de ufw.

1. Habilitar el firewall:



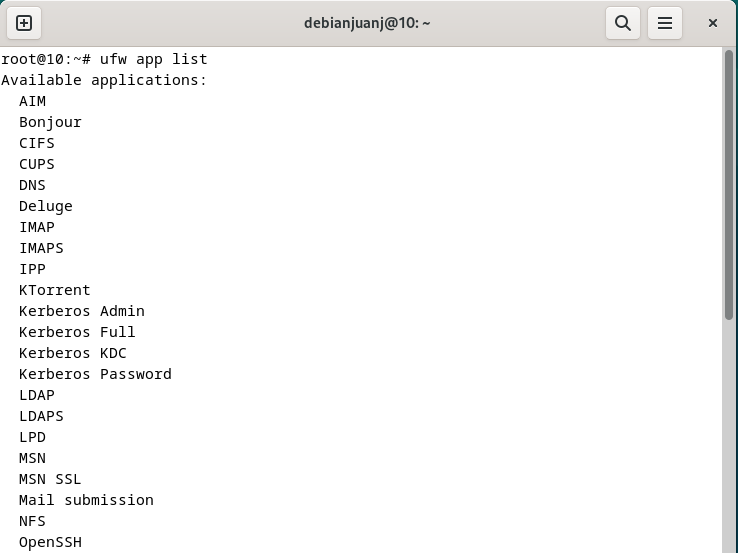
Con el comando “ufw enable” se habilita el funcionamiento del firewall de ufw.

1. Revisar las zonas activas y las reglas asociadas a cada una:



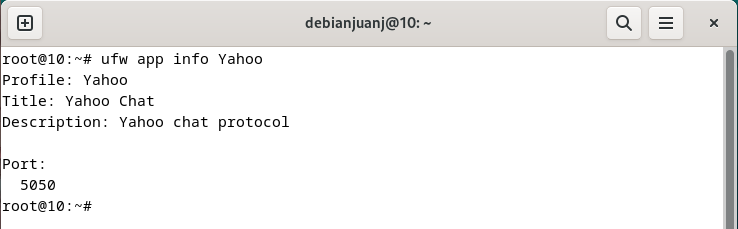
Con el comando “ufw status” se muestra el estado del servicio ufw, en este caso muestra que se encuentra operativo.

1. Observar las zonas del firewall:



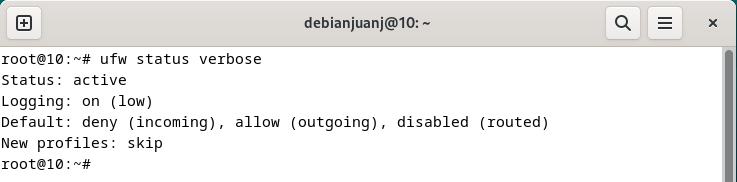
Con el comando “ufw app list” se muestra la lista de las aplicaciones en las que se encuentra habilitado el servicio de ufw.

1. Obtener información detallada sobre las reglas de una aplicación o servicio:



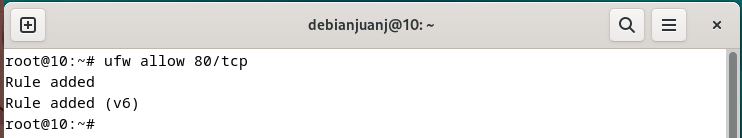
Con el comando “ufw app info (nombreAplicacion)” se muestra información sobre la aplicación que tenga compatibilidad con ufw.

1. Determinar de manera detallada el status de las zonas:



con el comando “ufw status verbose” te muestra el estado del ufw con algo de información extra.

1. ACLs de red con ufw permitir tráfico entrante HTTP en el puerto 80:



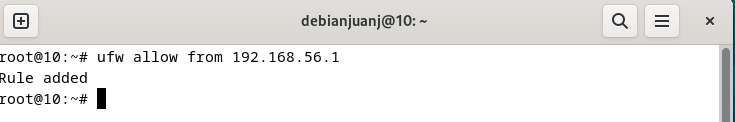
Con el comando “ufw allow 80/tcp” permite el trafico de los puertos 80 para servicios http.

1. Permitir tráfico entrante HTTPS en el puerto 443:



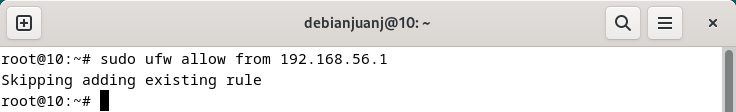
Con el comando “ufw allow 433/tcp” permite las conexiones https de los puertos 443

1. Permitir tráfico entrante SSH en el puerto 22 solo desde una dirección IP específica:



Con el comando “ufw allow from (ip deseada)” permite la conexion de algun puerto 22 para una ip en especifico.

1. Permitir tráfico entrante SSH en el puerto 22 solo desde una subred específica:



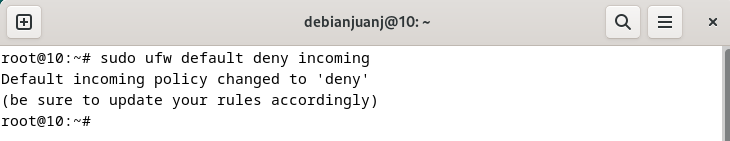
Con el comando “sudo ufw allow from (ip en específica)” permite la conexión de algún puerto de una subred.

1. Permitir tráfico saliente HTTPS:

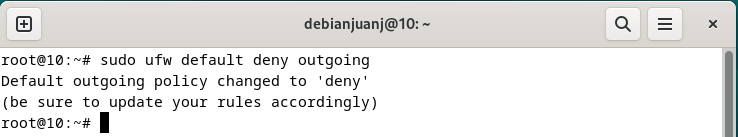


Con el comando “sudo ufw allow out 443/tcp” este permite el trafico saliente de los puertos https.

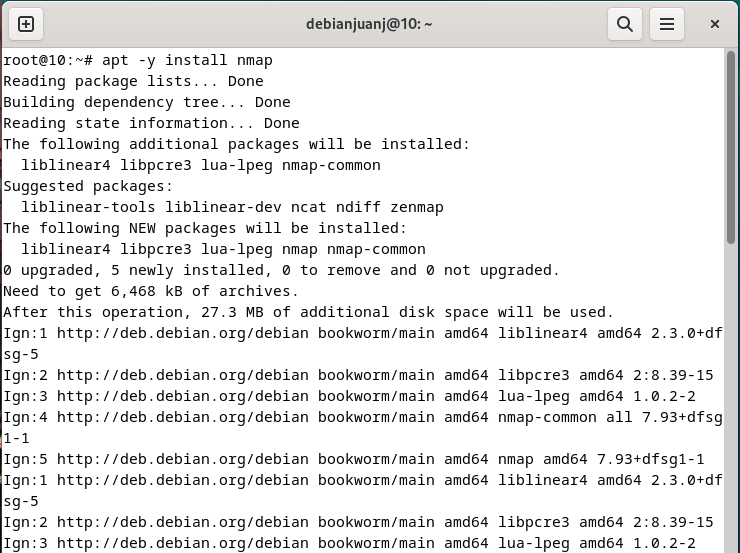
1. Denegar todo el tráfico entrante:

Con el comando “sudo ufw default deny incoming” deniega el tráfico entrante al equipo.

1. Denegar todo el tráfico saliente:

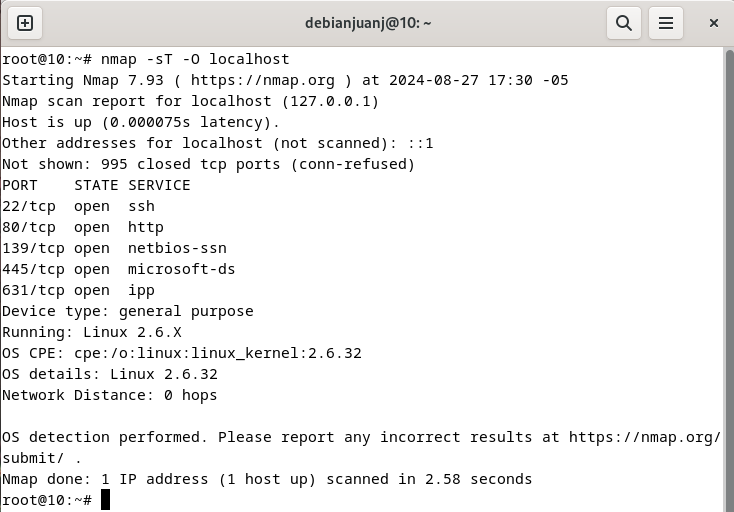
Con el comando “sudo ufw default deny outgoing” este se encarga de bloquear o denegar todo el tráfico saliente del equipo.

1. Monitoreo de puertos:



Con el comando “apt -y install nmap” se instala el servicio nmap para realizar la siguiente sección del laboratorio.

1. Revisar los puertos abiertos del sistema (localhost se puede reemplazar con una ip) :



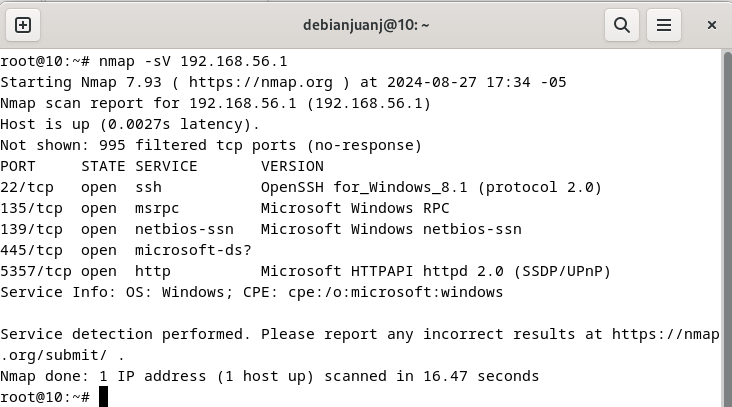
Con el comando “nmap -sT -O localhost” se revisa los puertos que estén abiertos del sistema.

1. Escaneo de puertos y detección de sistemas operativos:



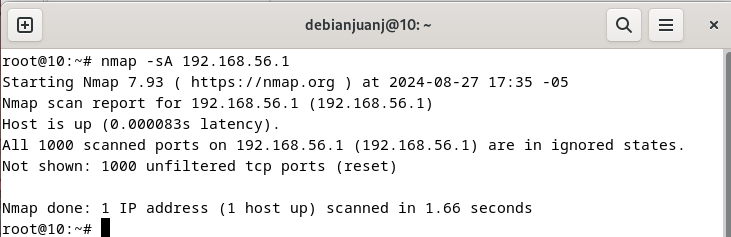
Con el comando “nmap -O <IP\_Adress>” con este comando verificamos el escaneo y la detección de los SO.

1. Escaneo de puertos y detección de versiones de servicios:



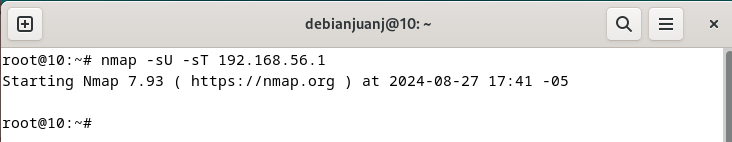
Con el comando “nmap -sV (ip deseada)” se escanea los puertos y la deteccion de las versiones de los servicios.

1. Escaneo de puertos con detección de firewall:



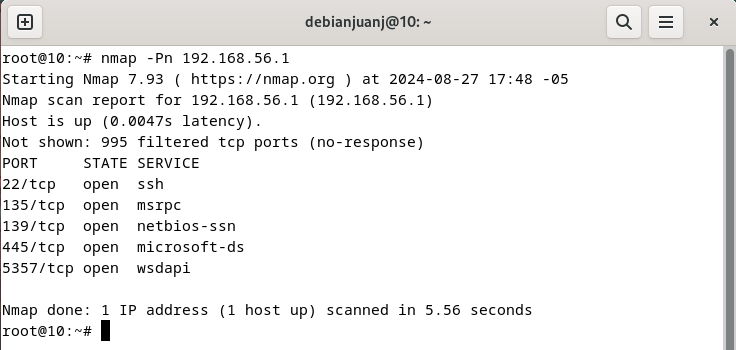
Con el comando “nmap –sA (ip deseada)” con este comando se realiza el escaneo de los puertos que tengan una detección de firewall.

1. Escaneo de puertos TCP y UDP:

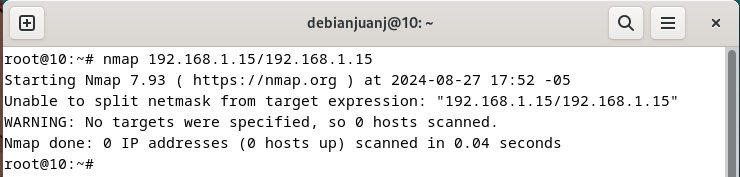


Con el comando “nmap -sU -sT (ip deseada)” se escanea los puertos tcp y udp.

1. Escaneo de puertos sin ping:

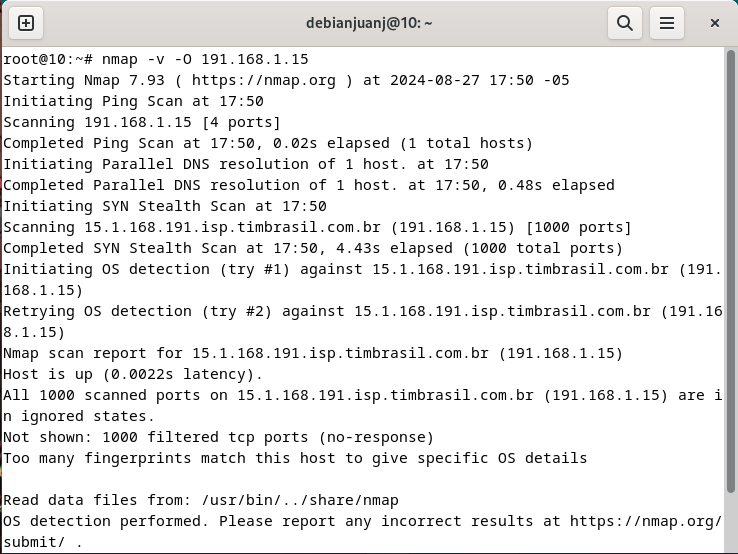
Con el comando “nmap -Pn (ip deseada)” se verifica los puertos que no tengan ping en la conexión.

1. Escaneo de puertos en una subred:



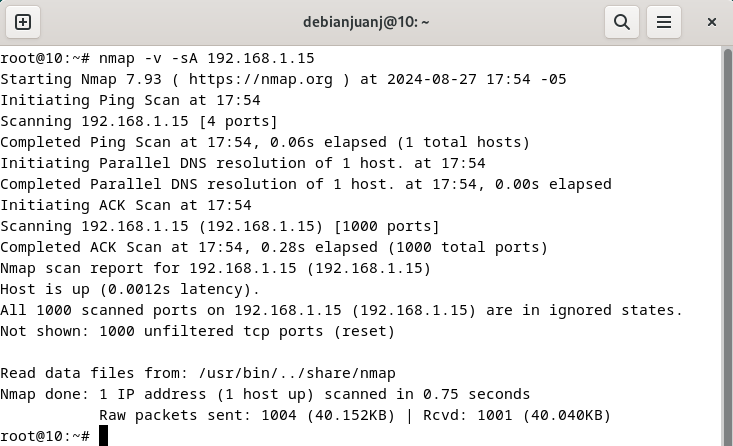
Con el comando “nmap (ip 1)/(ip 2)” para realizar un escaneo de los puertos en una subred.

1. Escaneo de puertos y detección de sistemas operativos con detalles detallados:



Con el comando “nmap -v -o (ip deseada)” con este comando se realiza el escaneo y la verificación entre las conexiones de los SO.

1. Escaneo de puertos con detección de firewall y detalles destacados:



Con el comando nmap -v -sA (ip deseada)” con este comando se escanea los puertos de detección firewall y detalles varios.

1. Determinar la información de un puerto (port = número de puerto):

Con el comando “cat /etc/services grep 661” se realiza el obtencion de informacion de un puerto que se designa por el usuario.