Implementación de zonas DMZ en entornos GNU/Linux para el fortalecimiento de la seguridad perimetral-Etapa 7 Implementando Seguridad en GNU/Linux

Juan David Sierra Llanos
e-mail:jdsierrall@unadvirtual.edu.co

RESUMEN: *El presente trabajo muestra el proceso de instalación y configuración para habilitar servicios en una zona DMZ dentro de una red, utilizando el sistema operativo Ubuntu Server como plataforma para la implementación de dichos servicios.*

PALABRAS CLAVE: Ubuntu, zona, DMZ, sistema operativo,linux

1 INTRODUCCIÓN

En el presente trabajo se aborda la administración y seguridad de redes mediante el diseño e implementación de una zona desmilitarizada (DMZ), cuyo propósito es aislar servicios críticos como servidores web y de transferencia de archivos con el fin de reducir el riesgo de que un ataque comprometa la red interna. Asimismo, se analiza la configuración de reglas de filtrado de tráfico en un servidor Ubuntu Server, orientadas a permitir únicamente las comunicaciones estrictamente necesarias y a fortalecer de manera integral la postura de seguridad del entorno de red.

2 MARCO TEORICO

2.1 Zona DMZ

Una DMZ o zona desmilitarizada es una red perimetral que protege y agrega una capa adicional de seguridad a la red de área local interna de una organización del tráfico no confiable.

El objetivo final de una red de zona desmilitarizada es permitir que una organización acceda a redes no confiables, como Internet, mientras garantiza que su red privada o LAN permanezca segura. Por lo general, las organizaciones almacenan servicios y recursos externos, así como servidores para el Sistema de nombres de dominio (DNS), el Protocolo de transferencia de archivos (FTP), correo, proxy, el Protocolo de voz sobre Internet (VoIP) y los servidores web, en la DMZ. (fortinet, 2025)

Teniendo en cuenta la implementación de servicios **HTTP que nos permite que el navegador se comunique al servidor web mientras que el FTP nos ayuda en la transferencia de archivos entre el cliente y el servidor estos dos** protocolos son utilizados en servicios dmz.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 Temática 3: Permitir servicios de la Zona DMZ para la red. Producto esperado:

1. Permitir los servicios HTTP (Puerto 80) y FTP (Puerto 21) desde el servidor Web bajo Ubuntu Server.
2. Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red. Verificar en el tráfico de salida, la creación de las reglas.

Esta temática fue desarrollada por el estudiante Juan David Sierra Llanos

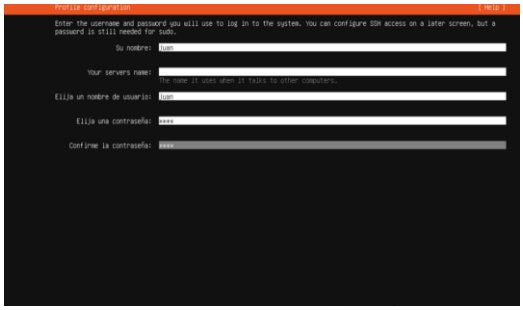
Fig.1 Grub de arranque de ubuntu.

Fuente: Autoria Propia

Fig.2 Selecion de idioma.

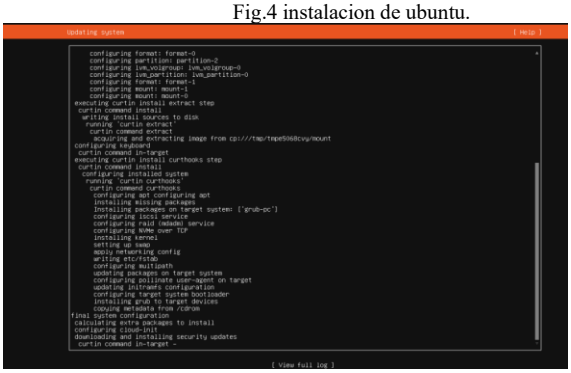
Fuente: Autoria Propia

Fig.3 selección de host.



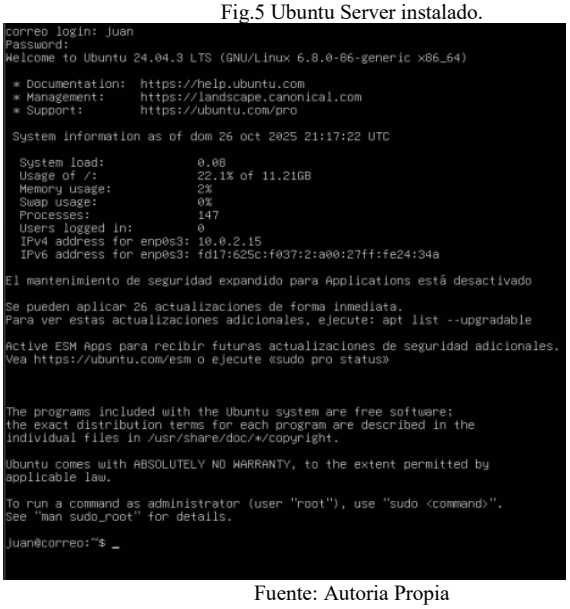
Fuente: Autoria Propia

Fig.4 instalacion de ubuntu.



Fuente: Autoria Propia

Fig.5 Ubuntu Server instalado.



Fuente: Autoria Propia

Fig.6 clonación de máquinas.

Fuente: autoría Propia.

Fig.7 Configuracion de red.

Fuente: Autoria Propia

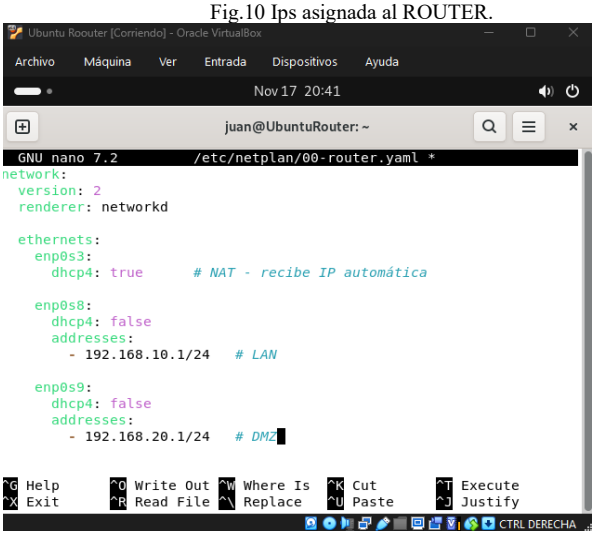
Fig.8 Configuracion de red adaptador 2.

Fuente: Autoria Propia.

Fig.9 Configuracion de red adaptador 3.

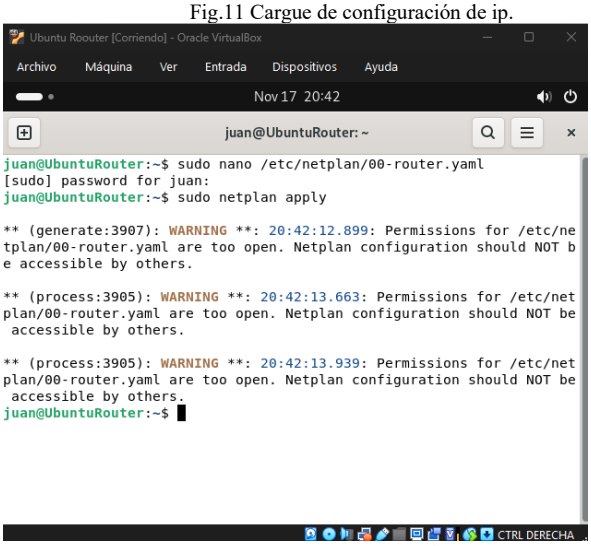
Fuente: Autoria Propia.

Fig.10 Ips asignada al ROUTER.



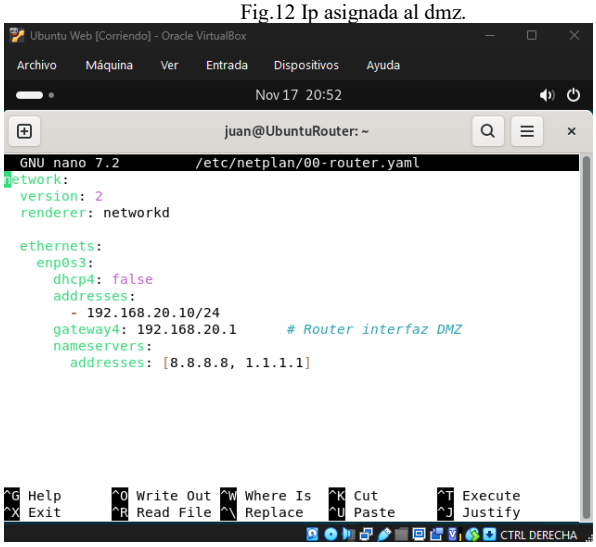
Fuente: Autoria Propia

Fig.11 Cargue de configuración de ip.



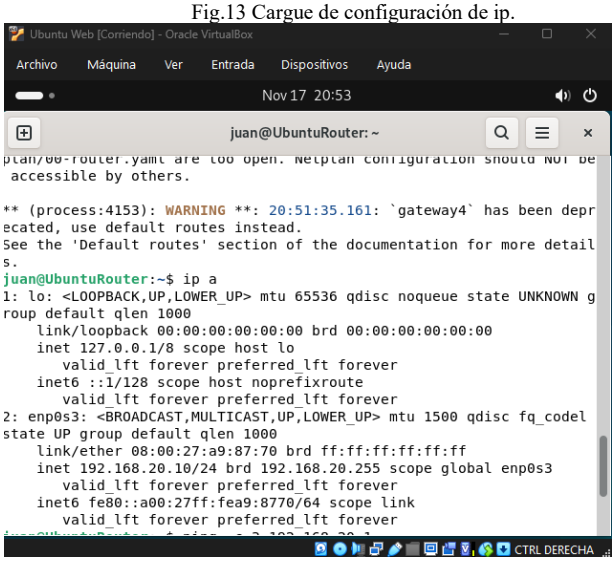
Fuente: autoría Propia

Fig.12 Ip asignada al dmz.



Fuente: autoría Propia

Fig.13 Cargue de configuración de ip.

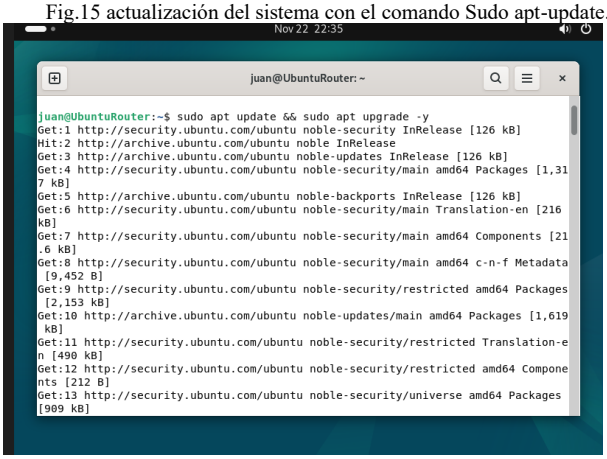


Fuente: autoría Propia

Fig.14 Ip asignada a lan.

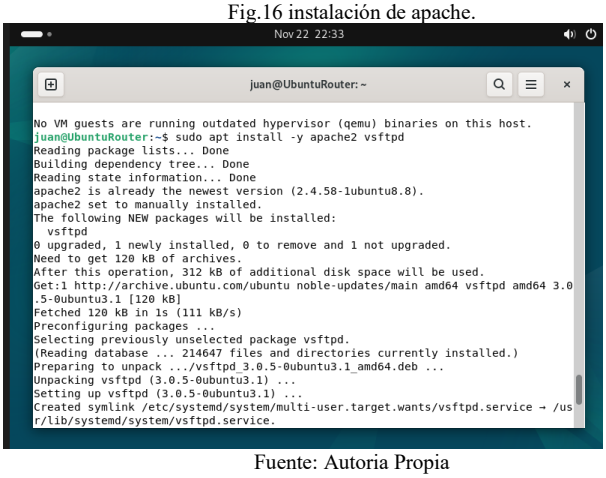
Fuente: Autoria Propia

Fig.15 actualización del sistema con el comando Sudo apt-update.



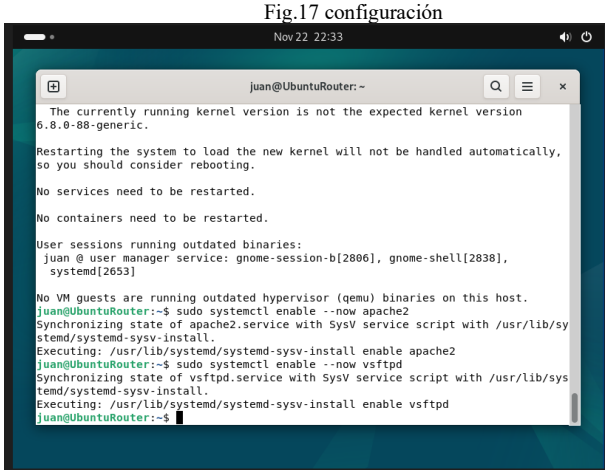
Fuente: autoría Propia

Fig.16 instalación de apache.



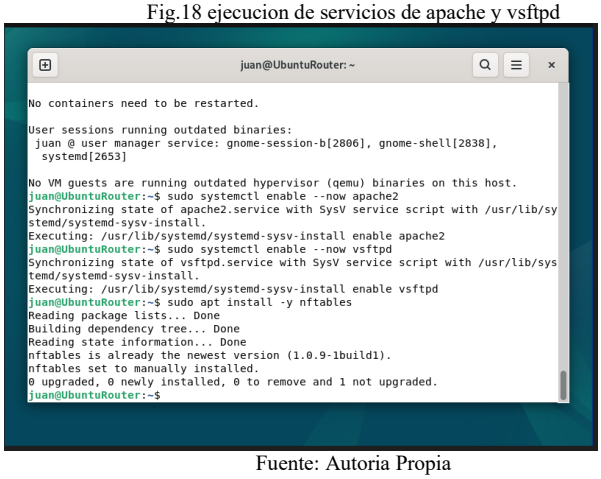
Fuente: Autoria Propia

Fig.17 configuración



Fuente: autoría Propia

Fig.18 ejecucion de servicios de apache y vsftpd

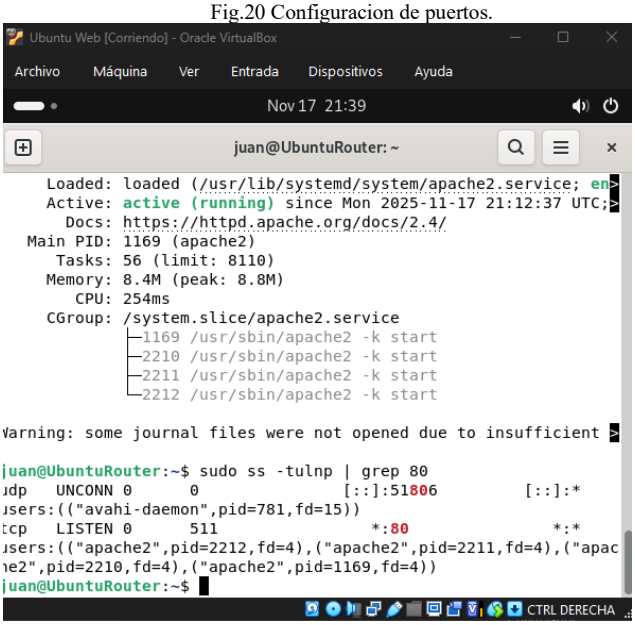


Fuente: Autoria Propia

Fig.19 Configurar firewall en el Router con nftables

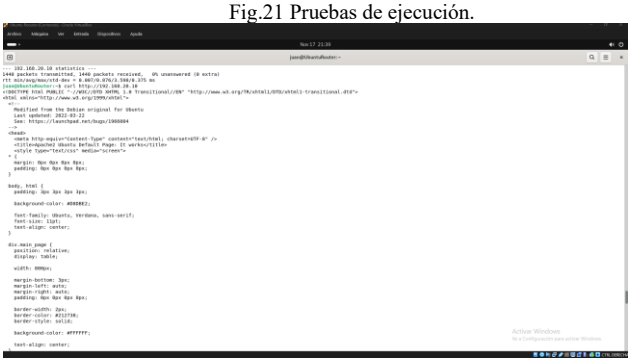
Fuente: Autoria Propia

Fig.20 Configuracion de puertos.



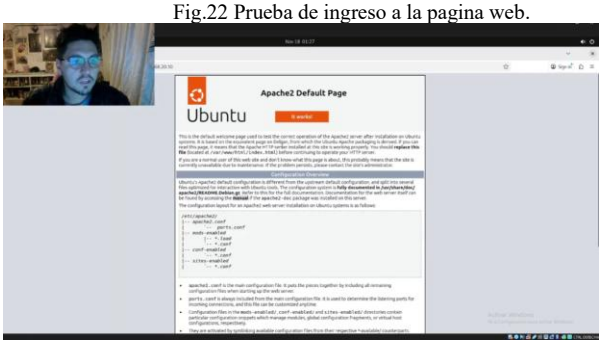
Fuente: Autoria Propia

Fig.21 Pruebas de ejecución.



Fuente: Autoria Propia

Fig.22 Prueba de ingreso a la pagina web.



Fuente: Autoria Propia

Fig.23 Prueba de bloqueo de puertos.

Fuente: Autoria Propia

4 CONCLUSIONES

La implementación de una zona DMZ en Ubuntu server me permitió establecer un sistema que ayuda a fortalecer la seguridad dentro de la infraestructura de la red, permitiendo controlar los servicios expuestos sin la necesidad de comprometer la integridad del sistema, por otro lado la habilitación de los servicios HTTP y FTP en los puertos 80 y 21 me garantiza la disponibilidad de los recursos web y de transferencia de datos, manteniendo al mismo tiempo una arquitectura segura y funcional.

5 REFERENCIAS

[1] Fortinet. (2025, 20 de Novembre). What is DMZ? https://www.fortinet.com/lat/resources/cyberglossary/what-is dmz

[2] LPI Learning. (2022). LPIC-1 Exam 101: Topic 102 – GNU and Unix commands. https://learning.lpi.org/es/learning-materials/101-500/102/

[3] Canonical Ltd. (2023). Ubuntu Desktop 20.04 LTS documentation. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[4] Debian Project. (2023). Debian administrator's handbook (Debian 12.5.0). https://www.debian.org/releases/stable/amd64/index.es.html

[5] Oracle. (2020). VirtualBox user manual. https://www.virtualbox.org/manual/

[6] Endian. (2016). Endian UTM 3.2 reference manual. http://docs.endian.com/3.2/utm/index.html

[7] LaCroix, J. (2020). Mastering Ubuntu Server: Gain expertise in the art of deploying, configuring, managing, and troubleshooting Ubuntu Server. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952