Configuración de Servicios HTTP, FTP y Restricción del Protocolo ICMP en Ubuntu Server desde VirtualBox

Andres Valdes Felipe Valdes
afvaldesm@unadvirtual.edu.co

RESUMEN: *En la administración de sistemas operativos, una de las tareas más importantes es lograr que los servicios de red y los protocolos de comunicación funcionen de manera segura y estable, lo cual a desarrollar este ejercicio, busca poner en práctica la configuración de servicios básicos como HTTP y FTP en un servidor GNU/Linux, complementándolos con medidas de seguridad que impidan riesgos, como la restricción del protocolo ICMP para evitar escaneos o intentos de ping no deseados, entre otros y más allá de la parte técnica, la idea es aplicar lo aprendido sobre firewalls y control de tráfico de red en un escenario real, integrando buenas prácticas, que ayuden a mantener un balance entre accesibilidad y protección, que al hacerlo, no solo se garantiza que los servicios respondan de forma confiable, sino que también se refuerza la seguridad de la infraestructura frente a posibles vulnerabilidades, fortaleciendo competencias esenciales para la administración profesional de servidores GNU/Linux en entornos de trabajo reales.*

PALABRAS CLAVE: GNU/Linux, Ubuntu Server [1], servicios HTTP, bloqueo de ping.

1. INTRODUCCIÓN

En la administración de sistemas GNU/Linux, la habilitación y restricción de servicios y protocolos se vuelve fundamental; para garantizar tanto la funcionalidad como la seguridad de los entornos de red, enmarcando actividades prácticas de la configuración de servicios como HTTP y FTP, así como la restricción del protocolo ICMP para mejorar la protección contra escaneos y accesos no autorizados en la red, accediendo a herramientas administrativas y pruebas funcionales, en las cuales se evalúa el comportamiento del servidor bajo políticas definidas de acceso y denegación.

2. PROCEDIMIENTO

a. Configuración de la máquina virtual Ubuntu Server en VirtualBox:

   Se crea una instancia de Ubuntu Server asignando recursos mínimos (RAM, disco duro, red NAT o adaptador puente).

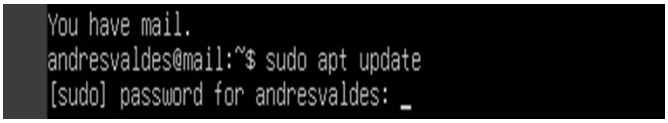
b. Se instalan los servicios necesarios: apache2 para HTTP y vsftpd para FTP.

   Estos servicios tienen unas funciones específicas para la aplicación de los servicios.

- Apache2 [2], que permite servir páginas web a través del protocolo HTTP (puerto 80).
- vsftpd (Very Secure FTP Daemon) [3], que permite la transferencia de archivos usando el protocolo FTP (puerto 21).

Figura 1

Actualización de recursos en el servidor.

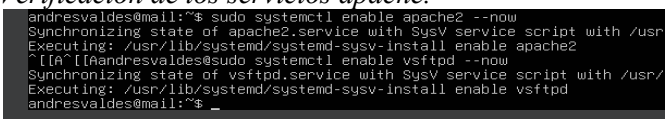


c. Abrir los puertos HTTP (80) y FTP (21) en el firewall (UFW), se bloquea por defecto el tráfico entrante lo cual permite explícitamente el tráfico por los puertos 80 (HTTP) y 21 (FTP) para que los servicios puedan ser accesibles desde otras máquinas.

- Usar UFW[4], para controlar el acceso a la red del servidor. Con comandos como sudo ufw allow, sudo ufw enable o sudo ufw status, puedes administrar qué servicios se permiten o bloquean.

Figura 2

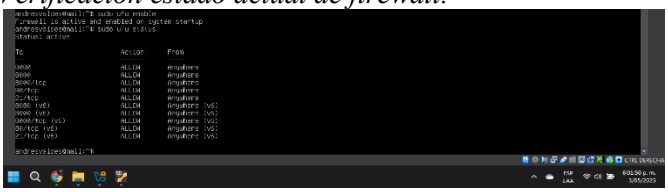
Verificación de los servicios apache.



- Sudo UFW STATUS, en este comando se muestra el estado actual del firewall, o sea si está activo o inactivo, qué puertos o servicios están permitidos o bloqueados, sirve para verificar si las reglas configuradas (como permitir el puerto 80 o 21) están aplicadas correctamente.

Figura 3

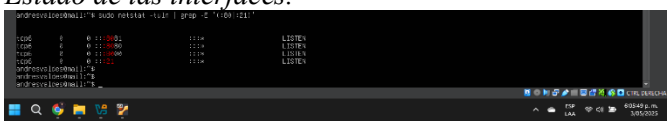
Verificación estado actual de firewall.



- Hay que asegurar que Apache y vsftpd están escuchando en las interfaces correctas, esto implica revisar que los servicios estén funcionando y aceptando conexiones en las IP correctas (por ejemplo, en 0.0.0.0 o en la IP de la red interna).

Figura 4

Estado de las interfaces.



- Para probar HTTP, se puede abrir un navegador en otro equipo de la red e ingresar la dirección IP del servidor.

Figura 5

Verificación estado del servidor en OS escritorio

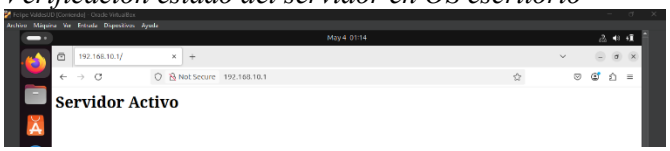
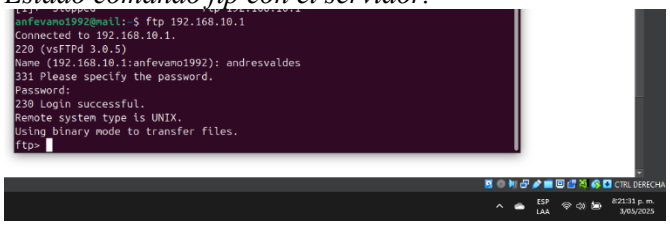


Figura 6

Estado comando ftp con el servidor.

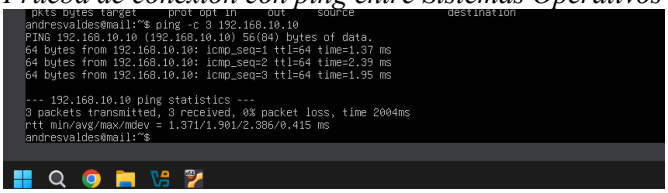


Denegar el protocolo ICMP (Puerto 8 y puerto 30) para no permitir hacer ping en la red. Probar a través de una consola o terminal la no respuesta del comando ping hacia una IP de la red.

Verificación de PING entre las redes para verificar conexión.

Figura 7

Prueba de conexión con ping entre Sistemas Operativos



Se bloquea el ICMP saliente (ping) desde el servidor hacia otros equipos

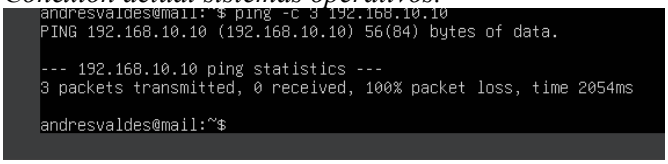
Figura 8

Bloqueo ICPM

Al verificar nuevamente ya no se puede realizar el ping entre la red de los sistemas operativos.

Figura 9

Conexión actual sistemas operativos.



Resultados de prueba

De los servicios HTTP y FTP, se comprobó exitosamente el acceso desde un cliente web y cliente FTP hacia el servidor Ubuntu configurado, confirmando el correcto funcionamiento de los puertos 80 y 21.

Las pruebas de los Protocolo ICMP, realizadas desde otra máquina indicaron que el servidor no responde a peticiones ping, cumpliendo con la política de denegación definida.

3. Conclusiones

- La habilitación controlada de servicios como HTTP y FTP, junto con la restricción de protocolos como ICMP, constituye una práctica básica pero crucial en la administración de servidores GNU/Linux.

- Esta configuración permite ofrecer servicios esenciales de forma segura, limitando la exposición del servidor a potenciales ataques de reconocimiento o escaneo en la red.

- La implementación de reglas en el firewall del servidor debe ir acompañada de pruebas

constantes para validar su eficacia, garantizando así un entorno robusto y alineado con los principios de ciberseguridad y administración eficiente de recursos.

4. Citas y referencias

[1] Canonical Ltd. "Ubuntu Server Documentation.": https://ubuntu.com/server/docs (accedido: 18-ago-2025).

[2] Apache Software Foundation. "Apache HTTP Server Project.": https://httpd.apache.org (accedido: 18-ago-2025).

[3] Chris Evans. vsftpd – Very Secure FTP Daemon: https://security.appspot.com/vsftpd.html (accedido: 18-ago-2025).

[4] Canonical Ltd. "UFW – Uncomplicated Firewall.": https://help.ubuntu.com/community/UFW (accedido: 18-ago-2025).

5. Referencias

[1] Apache Software Foundation. (2025). Apache HTTP Server Project. Apache. https://httpd.apache.org

[2] Canonical Ltd. (2025). UFW – Uncomplicated Firewall. Ubuntu Documentation. https://help.ubuntu.com/community/UFW

[3] Evans, C. (2025). vsftpd – Very Secure FTP Daemon. Security. https://security.appspot.com/vsftpd.html

[4] Internet Engineering Task Force. (1981). Internet Control Message Protocol (ICMP) (RFC 792). IETF. https://datatracker.ietf.org/doc/html/rfc792

[5] TuxNoob. (2024, junio 24). How to configure UFW to block ICMP request on Ubuntu 22.04. TuxNoob. https://www.tuxnoob.com/posts/How-To-Configure-Block-ICMP-Request-ubuntu-22.04/