IMPLEMENTACION DE SERVICIOS HTTP Y FTP EN UNA ZONA DMZ BAJO GNU/LINUZ ENDIAN

Fabian Dario Martinez Jiménez
e-mail: fdmartinezj@unadvirtual.edu.co

RESUMEN: *En este articulo y la presente práctica se implementó una zona DMZ utilizando GNU/Linux Endian como firewall perimetral y Ubuntu Server como servidor ubicado en la zona naranja. Se configuraron los servicios HTTP y FTP mediante Apache2 y VSFTPD, permitiendo el acceso controlado a los servicios publicados. Adicionalmente, se implementaron reglas de seguridad para bloquear el protocolo ICMP y evitar respuestas a solicitudes ping. Finalmente, se realizaron pruebas de conectividad y validación de servicios desde consola, verificando el correcto funcionamiento de la configuración implementada.*

PALABRAS CLAVE: DMZ(Demilitarized Zone o Zona Desmilitarizada), GNU/Linux, Apache2, VSFTPD(Very Secure FTP Daemon), Firewall, ICMP(Internet Control Message Protocol).

1 INTRODUCCIÓN

La seguridad perimetral en redes informáticas es fundamental para proteger los recursos internos frente a accesos no autorizados y amenazas externas. Una de las estrategias más utilizadas es la implementación de una zona DMZ (Demilitarized Zone), la cual permite aislar los servidores públicos del resto de la red interna.

En esta actividad se realizó la configuración de servicios HTTP (HyperText Transfer Protocol) y FTP (File Transfer Protocol) sobre un servidor Ubuntu Server ubicado en la zona DMZ, utilizando GNU/Linux Endian como plataforma de firewall. Además, se implementaron reglas de filtrado para bloquear el protocolo ICMP, fortaleciendo la seguridad de la infraestructura de red.

2 OBJETIVO DEL PROYECTO

Objetivo General

Implementar servicios HTTP y FTP en una zona DMZ bajo GNU/Linux, aplicando reglas de seguridad para controlar el tráfico de red.

Objetivos específicos

- Configurar el servicio Apache2 en el servidor GNU/Linux para habilitar conexiones mediante el protocolo HTTP, permitiendo el acceso a contenidos web desde equipos clientes y garantizando la correcta disponibilidad de los servicios.
- Implementar y configurar el servicio VSFTPD en el servidor GNU/Linux para permitir el acceso y la transferencia de archivos mediante el protocolo FTP.
- Diseñar y aplicar reglas de firewall orientadas al bloqueo del protocolo ICMP, con el fin de restringir determinadas solicitudes de red, fortalecer la seguridad en el sistema.
- Verificar el correcto funcionamiento de los servicios Apache2 y VSFTPD mediante herramientas y comandos de administración en GNU/Linux.

3 METODOLOGIA

La presente práctica se desarrolló bajo una metodología de carácter práctico y experimental, orientada a la implementación y validación de servicios de red en un entorno controlado de laboratorio. Para ello, se utilizaron máquinas virtuales configuradas en VirtualBox, donde GNU/Linux Endian actuó como firewall perimetral y Ubuntu Server como servidor ubicado en la zona DMZ.

4 DESARROLLO DE CONTENIDO

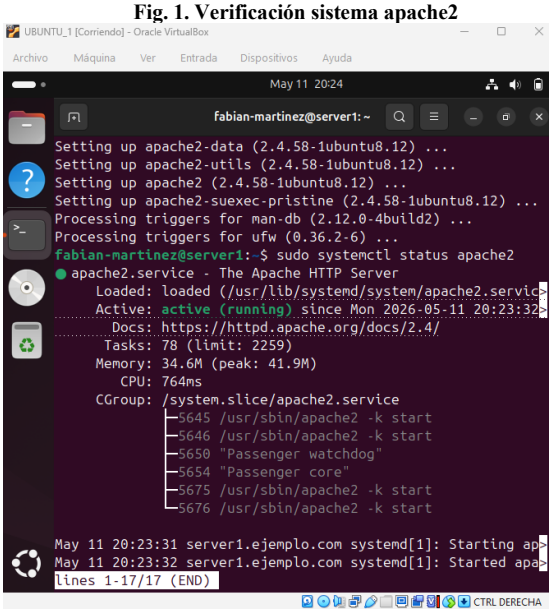
4.1 TEMATICA 1 IMPLEMENTACION DE SERVICIOS HTTP Y FTP EN UNA ZONA DMZ BAJO GNU/LINUZ ENDIAN

4.1.1 CONFIGURACION DEL SERVICIO HTTP

Inicialmente se realizó la instalación del servicio Apache2 sobre Ubuntu Server mediante el gestor de paquetes APT.
Comando utilizado:

sudo systemctl status apache2

Fig. 1. Verificación sistema apache2



Fuente: Autoría Propia

El servicio quedó en estado “active (running)”, indicando un funcionamiento correcto. También se realizaron pruebas locales utilizando el comando curl y acceso desde navegador mediante la dirección IP asignada al servidor.

4.1.2 CONFIGURACION DEL SERVICIO FTP

Se instaló el servicio VSFTPD para permitir conexiones FTP dentro de la zona DMZ.
Comando:

Sudo apt install vsftpd -y

Fig. 2. Instalación FTP

Fuente: Autoría Propia

Para la verificación del sistema FTP se usa el comando **sudo systemctl status vsftpd**, el estado debe estar en Active (running)

Fig. 3. Verificación sistema FTP

Fuente: Autoría Propia

Se verifica el servicio con la dirección IP

Fig. 4. Validación correcta del sistema FTP

Fuente: Autoría Propia

Posteriormente se realizaron pruebas de autenticación mediante el comando FTP desde consola, logrando establecer conexión exitosa con el servidor.

4.1.3 BLOQUEO DEL PROTOCOLO ICPM

Con el objetivo de aumentar la seguridad de la red y evitar respuestas a solicitudes ping, se implementó una regla de firewall utilizando **iptables**.
Comando ejecutado:
sudo iptables -A INPUT -p icmp –icmp-type echo-request -j DROP

Fig. 5. Implementación de reglas

Fuente: Autoría Propia

Finalmente se verificó el bloqueo mediante pruebas de conectividad utilizando el comando ping desde otra máquina de la red, obteniendo como resultado la ausencia de respuesta.

5 RESULTADOS

Los servicios HTTP y FTP fueron implementados exitosamente en el servidor Ubuntu Server ubicado en la zona DMZ. Las pruebas de funcionamiento permitieron validar el acceso correcto a ambos servicios mediante protocolos de red permitidos.
Asimismo, el bloqueo del protocolo ICMP demostró el correcto funcionamiento de las reglas de seguridad implementadas, evitando respuestas a solicitudes de reconocimiento de red.

6 CONCLUSIONES

La implementación de los servicios HTTP y FTP en una zona DMZ bajo GNU/Linux permitió habilitar el acceso controlado a recursos y aplicaciones alojadas en el servidor Ubuntu Server, garantizando una adecuada separación entre la red interna y los servicios expuestos al exterior. Mediante el uso de herramientas administrativas de GNU/Linux y la configuración de políticas de seguridad en Endian Firewall, fue posible gestionar, monitorear y verificar el correcto funcionamiento de los servicios de red desde la consola, fortaleciendo las competencias en administración de sistemas y asi su seguridad. Asimismo, la aplicación de reglas de firewall para bloquear el protocolo ICMP contribuyó a reducir la visibilidad de los dispositivos dentro de la infraestructura, mejorando la protección frente a actividades de reconocimiento y posibles intentos de acceso no autorizado y protección de los servicios desplegados.

7 REFERENCIAS

[1] [Instructivo de instalacion]Debian (2023). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/index.es.html
[2] [Material de estudio] https://learning.lpi.org/es/learning-materials/101-500/
[3] Hernandez, P. F., & Sánchez, J. (2022). Monitoreo y administración de sistemas Linux. [Objeto_virtual_de_información_OVI]. Repositorio Institucional UNAD.
[4] Debian Project, El manual del administrador de Debian 12.5.0, 2023. [En línea]. Disponible en: https://www.debian.org/releases/stable/amd64/index.es.html
[5] Endian. (2016). Endian Firewall Manual. http://docs.endian.com/
Disponible en: https://docs.endian.com/3.2/utm/index.html
[6] Linux Professional Institute. (2022). LPIC-1 Exam 101. https://learning.lpi.org/es/learning-materials/101-500/