IMPLEMENTANDO SEGURIDAD EN GNU/LINUX

Freddy Ferney Garnica Martinez
e-mail: ffgarnicam@unadvirtual.edu.co
Kevin Alejandro Castano Mendoza
e-mail: kacastanom@unadvirtual.edu.co
Diego David Betancur Ciprian
e-mail: ddbetancurc@unadvirtual.edu.co

RESUMEN: *La finalidad de esta actividad es poner en marcha sistemas de seguridad perimetrales en un ambiente GNU/Linux, utilizando para ello la plataforma Endian Firewall y una segmentación de red que se compone de las zonas Green (LAN), Orange (DMZ) y Red (WAN). El procedimiento se llevó a cabo conforme a las pautas definidas en la Guía de Aprendizaje de la Etapa 7, y trató sobre el establecimiento de servicios, normas de acceso, NAT, protocolos para una navegación segura y la implementación de servidores en la DMZ. La metodología abarcó la instalación, la validación y la verificación por medio de consola, lo que demostró que las comunicaciones y los servicios entre las áreas funcionan con seguridad. Los hallazgos evidencian que se han implementado adecuadamente políticas de seguridad que robustecen la integridad y salvaguarda de los recursos de red.*

PALABRAS CLAVE: DMZ, Endian Firewall, Seguridad Perimetral, GNU/Linux.

1 INTRODUCCIÓN

La seguridad perimetral constituye un pilar fundamental en la administración de redes y sistemas operativos basados en GNU/Linux, ya que permite proteger los recursos frente a accesos no autorizados y garantizar la integridad de la información. En el marco de la Etapa 7 del Diplomado de profundización en administración de sistemas operativos Open Source, se implementó Endian Firewall como plataforma unificada de seguridad, configurando una infraestructura segmentada en zonas LAN, WAN y DMZ.

Este proceso permitió comprender y aplicar conceptos clave como la traducción de direcciones (NAT), la restricción y habilitación de servicios, la definición de políticas de tráfico entre áreas y el uso de un proxy con autenticación. Además, se enfatizó el trabajo desde la línea de comandos, fortaleciendo las competencias administrativas en GNU/Linux.

El presente artículo expone de manera ordenada los procedimientos, configuraciones y pruebas realizadas, así como las conclusiones técnicas derivadas de la implementación, siguiendo el formato académico IEEE.

2 PROCEDIMIENTO TEMATICA 1

2.1 Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.

Se implementó una red perimetral usando la distribución GNU/Linux Endian, a través de la aplicación de máquina virtual VirtualBox; con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).

2.2 INSTALACION GNU/LINUX ENDIAN

Se descargó la versión de la distribución GNU/Linux Endian, desde la página web oficial

Figura 1. Página de descarga de Endian

Fuente: Autoría propia

Muestra el sitio oficial desde donde se obtiene la distribución Endian Firewall

Figura 2. Creación de máquina virtual

Fuente: Autoría propia

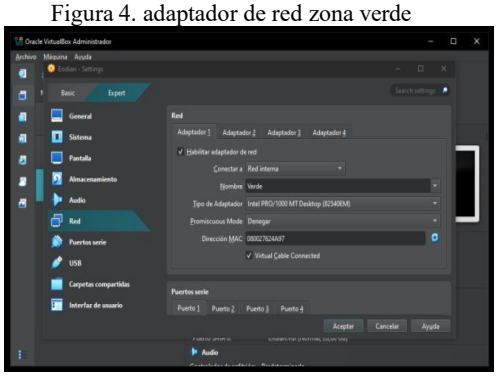
Se observa el proceso de creación de la máquina virtual en VirtualBox para alojar Endian.

Figura 3. adaptador de red zona roja

Fuente: Autoría propia

Configuración del adaptador de red en modo NAT para la zona WAN

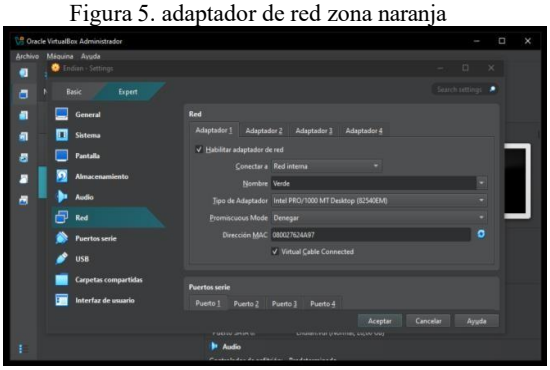
Figura 4. adaptador de red zona verde



Fuente: Autoría propia

Configuración del adaptador de red en modo red interna para la zona LAN.

Figura 5. adaptador de red zona naranja



Fuente: Autoría propia

Configuración del adaptador de red en modo red interna para la zona DMZ

Adaptador ethernet 1

IP: 192.168.20.1
Máscara de subred: 255.255.255.0

Figura 6. Asignación IP zona verde

Fuente: Autoría propia

Pantalla de configuración de la dirección IP para la interfaz GREEN.

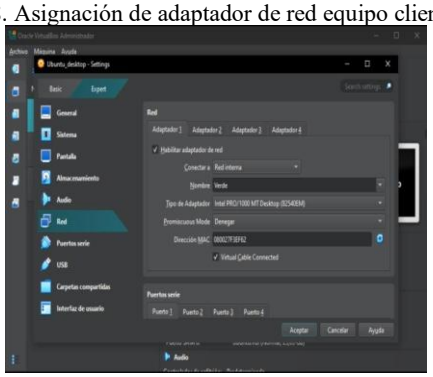
Figura 7. Entorno de Endian con las IP de las zonas

Fuente: Autoría propia

2.3 ACCESO A INTERFAZ WEB DESDE EQUIPO CLIENTE

Se modificó el adaptador de red en el equipo cliente con Ubuntu Desktop para la zona verde en VirtualBox.

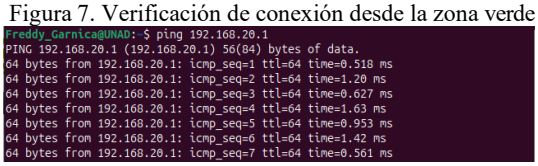
Figura 8. Asignación de adaptador de red equipo cliente



Fuente: Autoría propia

Se validó la conexión desde el equipo cliente de la zona verde a Endian por medio de terminal usando el comando:
ping 192.168.20.1

Figura 7. Verificación de conexión desde la zona verde



Fuente: Autoría propia

Se Ingresó desde el equipo cliente a la URL de Administración en la web, correspondiente a la IP de la Zona Verde 192.168.20.1

Figura 8. Acceso al entorno web de Endian

Fuente: Autoría propia

2.4 CONFIGURACION DE ZONA NARANJA DESDE EL ENTORNO WEB

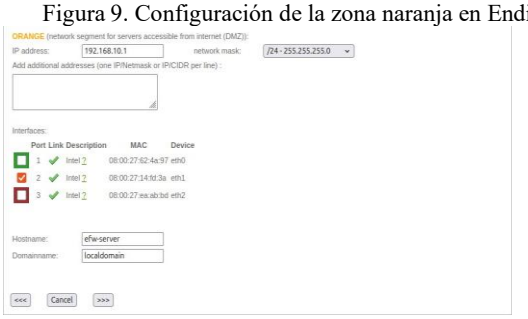
Se realizó la configuración del paso a paso dentro del entorno web para establecer los siguientes parámetros:

- Idioma y zona horaria.
- Restauración copia de Seguridad (en el caso de que sea necesario).
- Contraseña para el administrador de la interfaz web y SSH
- Modo de la red en enrutamiento y tipo de enlace DHCP para la Zona Roja

Se finalizó con la configuración de la zona naranja, asignando la dirección IP, el puerto de red ethernet 2 y el nombre del servidor.

Adaptador ethernet 2
IP: 192.168.10.1
Máscara de subred: 255.255.255.0

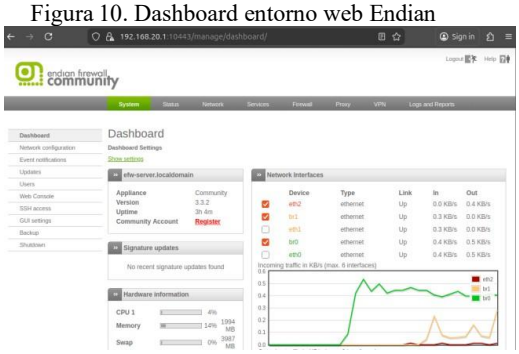
Figura 9. Configuración de la zona naranja en Endian



Fuente: Autoría propia

Se aplicaron los parámetros establecidos para ingresar al panel principal desde el entrono web de Endian para la administración de los servicios.

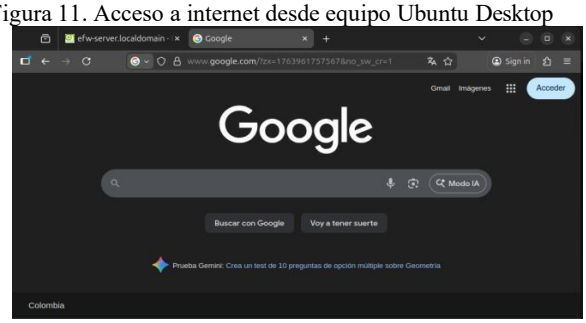
Figura 10. Dashboard entorno web Endian



Fuente: Autoría propia

Se verificó el acceso a internet desde el equipo Desktop ubicado en la zona verde

Figura 11. Acceso a internet desde equipo Ubuntu Desktop

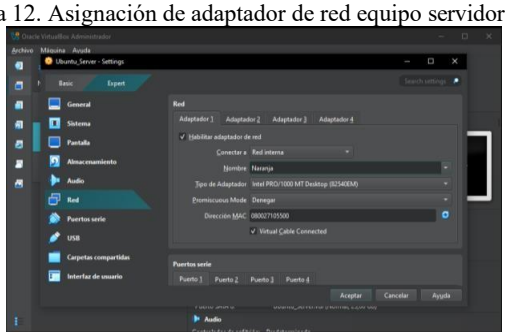


Fuente: Autoría propia

2.5 CONFIGURACION DE IP EQUIPO SERVER PARA ZONA NARANJA

Se modificó el adaptador de red en el equipo servidor con Ubuntu Server para la zona naranja en VirtualBox.

Figura 12. Asignación de adaptador de red equipo servidor



Fuente: Autoría propia

Se modificó la IP por medio del archivo 50-cloud-init.yaml con el comando: Sudo nano 50-cloud-init.yaml

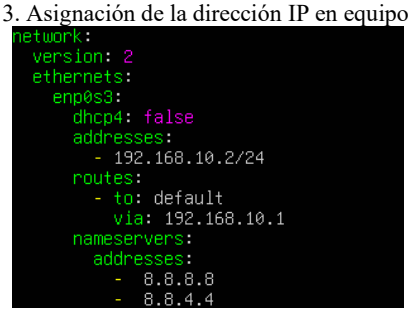
Desactivación del DHCP
Dhcp: false

Asignación de la IP fija
Addresses:
- 192.168.10.2/24

Asignación de la puerta de enlace
Routes:
- to: default
  via: 192.168.10.1

Asignación de los dominios de búsqueda
nameservers:
addresses:
- 8.8.8.8
- 8.8.4.4

Figura 13. Asignación de la dirección IP en equipo servidor



Fuente: Autoría propia

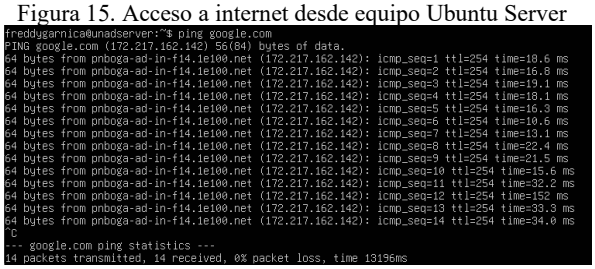
Posteriormente se aplicaron los cambios de IP mediante el comand: netplan apply y se validó la conexión con Endian a través de un Ping a la IP 192.168.10.1 correspondiente a la zona naranja.

Figura 14. Verificación de conexión desde la zona naranja

Fuente: Autoría propia

Se verificó ingreso a internet con un ping a la URL de Google

Figura 15. Acceso a internet desde equipo Ubuntu Server



Fuente: Autoría propia

3 PROCEDIMIENTO TEMATICA 2

3.1 IMPLEMENTACIÓN Y CONFIGURACIÓN DE NAT EN ENDIAN PARA COMUNICACIÓN LAN-WAN Y DMZ-INTERNET

Se detalla la creación de reglas NAT y el reenvío de puertos para garantizar el acceso controlado a servicios desde diferentes zonas de la red.

3.2 CONFIGURACIÓN DE LA INFRAESTRUCTURA

Se implementó Endian en VirtualBox con tres zonas principales:

Zona Verde (LAN): Red interna con estaciones de trabajo.

Zona Naranja (DMZ): Servidores con servicios web y bases de datos.

Zona Roja (WAN): Acceso a Internet.

Cada zona está configurada con interfaces de red específicas y rangos IP definidos para segmentar el tráfico.

3.2 CONFIGURACIÓN NAT EN ENDIAN

Se configuró una regla de NAT para que el tráfico originado en la zona verde pueda salir hacia la zona roja, traduciendo las direcciones IP privadas a la IP pública o IP de la zona roja.

Ejemplo de regla iptables para NAT (simplificado):

iptables -t nat -A POSTROUTING -o eth_red -s 192.168.20.0/24 -j MASQUERADE

Donde eth_red es la interfaz de la zona roja y 192.168.20.0/24 la red LAN.

NAT para DMZ hacia WAN

Se configuró una regla similar para la zona naranja que permite que los servidores accedan a Internet para actualizaciones o servicios externos.

Reenvío de puertos (Port Forwarding)

Para permitir el acceso desde Internet a servicios específicos en la DMZ (por ejemplo, servidor web HTTP en puerto 80), se configuraron reglas de reenvío de puertos.

Ejemplo:

iptables -t nat -A PREROUTING -i eth_red -p tcp --dport 80 -j DNAT --to-destination 192.168.10.10:80
iptables -A FORWARD -p tcp -d 192.168.10.10 --dport 80 -j ACCEPT

3.3 VERIFICACIÓN Y PRUEBAS

Se realizaron pruebas de conectividad:

- Desde una estación en LAN se pudo acceder a Internet.
- Desde Internet se pudo acceder al servidor web en DMZ mediante el puerto 80.
- Se verificó que solo los puertos permitidos estuvieran accesibles, manteniendo la seguridad.

4 PROCEDIMIENTO TEMATICA 3

4.1 DESCRIPCIÓN GENERAL DE LA TEMÁTICA

La Temática 3 se enfocó en habilitar de forma controlada los servicios FTP (puerto 21/TCP) y HTTP (puerto 80/TCP) desde la zona GREEN (LAN) a la zona ORANGE (DMZ). En esta última, se ha implementado una máquina virtual con Ubuntu Server que funciona como servidor web y FTP. Además, se pidió que el protocolo ICMP fuera bloqueado en las dos direcciones para evitar respuestas a peticiones (ping) y así fortalecer la seguridad perimetral.

4.2 CONFIGURACIÓN DEL SERVIDOR EN LA DMZ

El servidor Ubuntu ubicado en la zona ORANGE fue configurado con la dirección IP:

IP: 192.168.10.10
Mascara: 255.255.255.0
Puerta de enlace: 192.168.10.1

La configuración fue editada en el archivo netplan mediante el comando:

sudo nano /etc/netplan/00-installer-config.yaml
sudo netplan apply

4.3 INSTALACIÓN DE SERVICIOS REQUERIDOS EN EL UBUNTU SERVER (SERVIDOR)

Se actualizó el servidor y se procedió con la instalación de los servicios web y FTP:

sudo apt update && sudo apt upgrade -y
sudo apt install apache2 vsftpd -y

Una vez instalados los servicios se validó el estado de los servicios:

systemctl status apache2
systemctl status vsftpd

4.4 CONFIGURACIÓN DE LAS REGLAS EN ENDIAN FIREWALL

4.4.1 PERMITIR TRÁFICO HTTP Y FTP DESDE GREEN → ORANGE

En el módulo Firewall → Trafico de Salida, se crearon las siguientes reglas:

Tabla 1.

Origen	Destino	Servicio	Puerto	Acción
GREEN	ORANGE	HTTP	TCP/ :80	Permitir
GREEN	ORANGE	FTP	TCP/ :21	Permitir

Fuente: Autoría Propia

Estas reglas fueron aplicadas y definidas en la tabla de tráfico de salida.

4.4.2 BLOQUEO DEL PROTOCOLO ICMP

El requerimiento indica denegar ping (tipo 8) y tipo (30)

En el Firewall ENDIAN se configuro de la siguiente manera:

Tabla 2.

Origen	Destino	Servicio	Puerto	Acción
Cualquiera	Cualquiera	ICMP	ICMP/ :8 / :30	Denegar

Fuente: Autoría Propia

Esta regla impide realizar ping a cualquier dirección de la red y desde cualquier zona.

4.5 VERIFICACIÓN DE ACCESO A SERVICIOS PERMITIDOS

4.5.1 VALIDACIÓN DEL SERVICIO HTTP DESDE LA LAN

Desde un equipo Ubuntu Desktop en GREEN se ingresó mediante el navegador web a:

http://192.168.10.10

Figura 1. Validación acceso WEB

Fuente: Autoría Propia

Respuesta obtenida: página por defecto de Apache, demostrando acceso correcto.

4.5.2 VALIDACIÓN DEL SERVICIO FTP

Desde la Terminal del equipo desktop (Green) se digitó:

ftp 192.168.10.10

Figura 2. Validación conexión FTP

Fuente: Autoría Propia

El servidor vsftpd respondió confirmando la conexión, asegurando de esta manera la conectividad.

4.5.3 VALIDACIÓN DEL BLOQUEO DE ICMP

Desde la Terminal del equipo desktop (Green) se digitó:

ping 192.168.10.10

Figura 3. Validación conexión FTP

Fuente: Autoría Propia

Se obtuvo como resultado:

Destination Host Unreachable

Lo cual confirma que la regla de negación de ICMP funciona correctamente.

5 RESULTADOS

Los hallazgos alcanzados corroboran que los servicios permitidos funcionan correctamente y que los bloqueos requeridos son eficaces.

1. El servidor Ubuntu en la DMZ, con Apache2 y vsftpd funcionando de manera adecuada, se mostró a través de comandos systemctl status.

2. Se logró con éxito el tráfico FTP y HTTP desde GREEN hacia ORANGE, lo que evidencia que las reglas de Endian se crearon y aplicaron sin fallos.

3. El bloqueo del protocolo ICMP se realizó correctamente, dado que no hubo respuesta a los intentos de ping desde la LAN hacia la DMZ.

4. La ejecución se adaptó de manera rigurosa al método requerido por la guía: operación a través de consola, configuración real y verificación funcional sobre la infraestructura DMZ.

6 CONCLUSIONES

La implementación de una red perimetral mediante Endian Firewall en un entorno virtual demostró ser una estrategia eficaz para robustecer la seguridad en infraestructuras GNU/Linux. La segmentación en zonas LAN, DMZ y WAN permitió un control granular del tráfico y la exposición controlada de servicios.

La configuración de NAT y el reenvío de puertos evidenció la importancia de definir reglas precisas para garantizar la conectividad sin comprometer la seguridad. Asimismo, la habilitación de servicios HTTP y FTP, junto con el bloqueo del protocolo ICMP, mostró cómo las políticas de firewall pueden equilibrar disponibilidad y protección.

El uso de VirtualBox como entorno de pruebas facilitó la validación previa a un despliegue real, reduciendo riesgos y permitiendo ajustes en un ambiente controlado.

En conclusión, la práctica reafirma que una adecuada planificación y segmentación de red, acompañada de políticas de seguridad bien definidas, constituye un componente esencial para la administración de sistemas operativos Open Source en escenarios corporativos y educativos.

7 REFERENCIAS

[1] Endian. (2016). Endian UTM 3.2 – Manual de referencia. http://docs.endian.com/3.2/utm/index.html

[2] Endian Firewall Community. (2023). Manual de usuario y documentación oficial. https://www.endian.com/community

[3] Linux Professional Institute. (2022). Linux Essentials – Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

[4] LPI LPIC-1 Exam 101. (2022). Tema 101: Determinar y configurar los ajustes de hardware. https://learning.lpi.org/es/learning-materials/101-500/101/101.1/

[5] Ubuntu Documentation. (2024). Official Ubuntu Server Guide. https://ubuntu.com/server/docs
[6] Oracle (2020). Manual de usuario VirtualBox. https://www.virtualbox.org/manual/
[7] Install and Configure Endian Firewall on VirtualBox - kifarunix.com. (2019, May 21). Kifarunix.com. https://kifarunix.com/install-and-configure-endian-firewall-on-virtualbox/