Implementación de Medidas de Seguridad GNU/Linux mediante Endian firewall

Juan Felipe Zuluaga Galindo
jfzuluaga@unadvirtual.edu.co

RESUMEN: *La seguridad en sistemas operativos GNU/Linux es un elemento fundamental para preservar la integridad, disponibilidad y confidencialidad de la información en entornos organizacionales. En esta actividad se implementan medidas de seguridad perimetral empleando la distribución Endian Firewall (EFW) dentro de un entorno virtualizado mediante VirtualBox. El desarrollo práctico permite comprender conceptos esenciales de protección de redes, tales como la segmentación por zonas (LAN, WAN y DMZ), la creación de reglas de acceso, la configuración de NAT y la aplicación de políticas de proxy con autenticación. La actividad fortalece las competencias del estudiante en la administración y aseguramiento de infraestructuras basadas en GNU/Linux, promoviendo la adopción de buenas Prácticas para la protección de servicios críticos en redes corporativas.*

PALABRAS CLAVE: GNU/Linux, Seguridad Perimetral, Endian Firewall, VirtualBox, NAT, DMZ, Proxy, Administración de Redes, Seguridad Informática, Infraestructura TI.

1 INTRODUCCIÓN

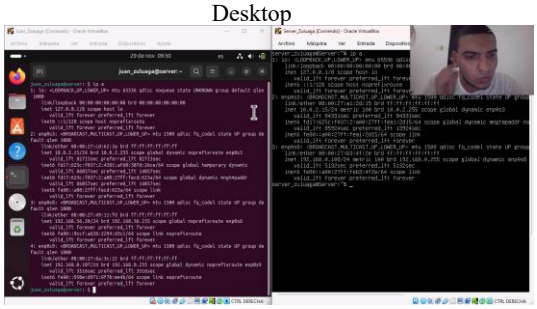
La seguridad en los sistemas operativos GNU/Linux constituye un componente esencial para garantizar la integridad, disponibilidad y confidencialidad de la información dentro de las organizaciones. En esta etapa se busca que el estudiante implemente medidas de seguridad perimetral utilizando herramientas y distribuciones especializadas como Endian Firewall (EFW), dentro de entornos virtualizados gestionados con VirtualBox. El desarrollo de la actividad permite comprender y aplicar conceptos de seguridad de redes como la segmentación por zonas (LAN, WAN y DMZ), la creación de reglas de acceso, la configuración de NAT, y la implementación de políticas de proxy con autenticación. De esta manera, se fortalece la capacidad del estudiante para administrar y asegurar infraestructuras basadas en GNU/Linux, garantizando la protección de servicios críticos y el cumplimiento de buenas prácticas de administración de sistemas.

2 REGLAS DE ACCESO PARA PERMITIR O DENEGAR EL TRÁFICO

En esta sección documento el proceso completo de configuración del firewall, la verificación de conectividad y la validación funcional del tráfico entre las zonas LAN, DMZ y WAN

.

Figura 1. Configuración de interfaces en Ubuntu Desktop



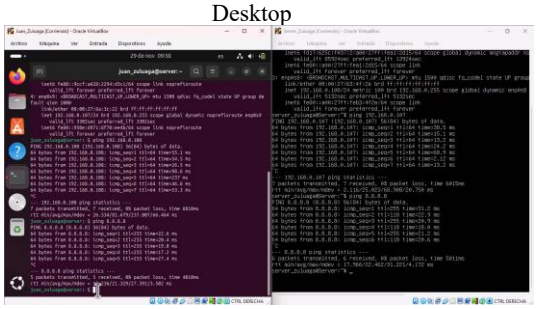
. Fuente: Autoría Propia

En esta imagen podemos ver la salida del comando ip a en el equipo Ubuntu Desktop. Aquí se evidencia la presencia de tres interfaces principales:

- enp0s3 (10.0.2.15) asociada a NAT,
- enp0s8 (192.168.56.20) correspondiente a la red interna de VirtualBox,
- enp0s9 (192.168.0.107) que pertenece a la red física (Bridged).
  Esta configuración confirma que el Desktop forma parte de la zona LAN (verde).

Así mismo se observa la salida del comando ip a ejecutado en Ubuntu Server. Es visible la interfaz enp0s3 con la IP 10.0.2.15 correspondiente a la zona WAN simulada, y la interfaz enp0s9 con IP 192.168.0.108, que funcionará como segmento DMZ para esta actividad. Aunque comparte subred con la LAN, la segmentación se realizará mediante firewall.

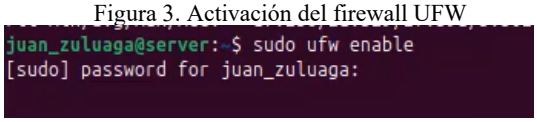
Figura 2. Verificación de conectividad desde Ubuntu Desktop



. Fuente: Autoría Propia

En esta imagen se observa la ejecución de los comandos ping 192.168.0.108 y ping 8.8.8.8. Aquí podemos ver que el Desktop logra comunicarse correctamente con la DMZ y con Internet, confirmando el enlace de red en la zona LAN. También, se ve al servidor realizando pruebas de ping hacia el Desktop (192.168.0.107) y hacia Internet (8.8.8.8). La respuesta positiva indica que el servidor tiene comunicación con la LAN y con la WAN simulada.

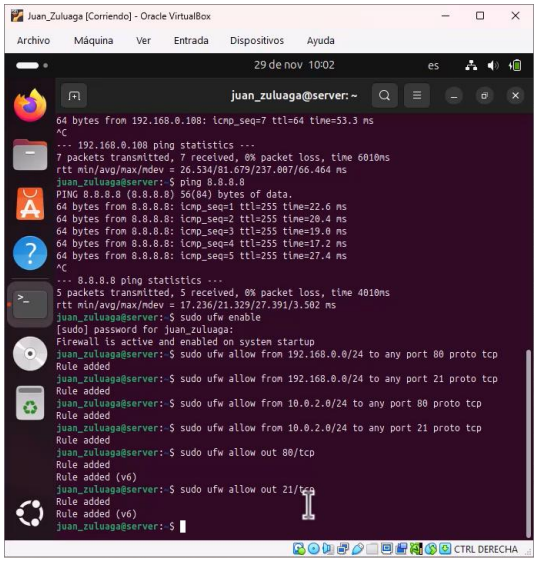
Figura 3. Activación del firewall UFW



. Fuente: Autoría Propia

En esta captura se muestra la activación del firewall mediante sudo ufw enable. Aquí se evidencia el mensaje de confirmación que indica que UFW quedó habilitado en el sistema.

Figura 4. Reglas añadidas para permitir HTTP y FTP desde la LAN

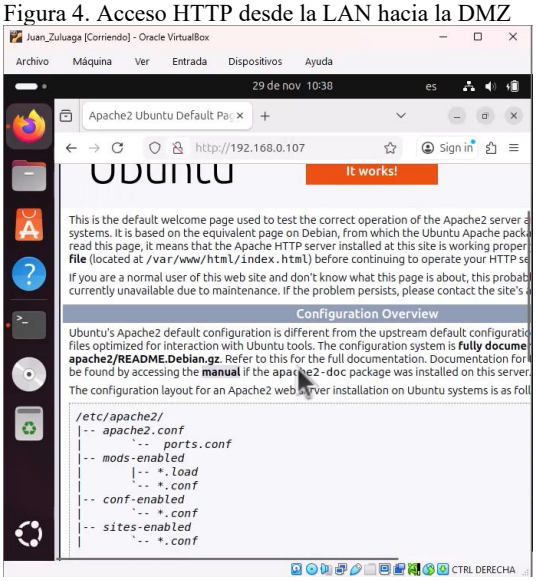


. Fuente: Autoría Propia

En esta imagen podemos ver la adición de las reglas que permiten tráfico HTTP (puerto 80) y FTP (puerto 21) desde la red LAN 192.168.0.0/24 hacia la DMZ. Estas reglas establecen la comunicación LAN → DMZ exigida por la actividad. Aquí se observa la configuración que permite que la WAN simulada (10.0.2.0/24) acceda a los servicios publicados en la DMZ.

Se evidencia la apertura controlada del servidor a redes externas. Además, se visualiza la autorización de tráfico saliente HTTP y FTP desde la DMZ hacia la WAN. Con ello, el servidor puede consultar recursos externos como páginas web o servidores FTP remotos.

Figura 4. Acceso HTTP desde la LAN hacia la DMZ



. Fuente: Autoría Propia

Aquí se observa el navegador Firefox del Ubuntu Desktop accediendo a http://192.168.0.107. En esta imagen se ve la página por defecto de Apache, lo que confirma la conectividad HTTP LAN → DMZ.

Figura 5. Acceso HTTP desde la LAN hacia la WAN

. Fuente: Autoría Propia

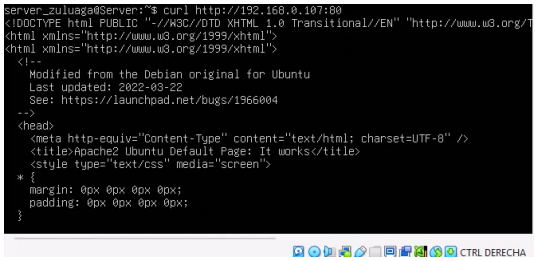
En esta captura se muestra cómo el Desktop accede a https://google.com. La correcta carga del sitio evidencia que la red LAN tiene salida hacia Internet usando la ruta configurada en el servidor.

Figura 6. Acceso HTTP desde la DMZ hacia la WAN

. Fuente: Autoría Propia

En esta imagen se muestra la ejecución del comando curl google.com en Ubuntu Server. La respuesta HTML obtenida indica que la DMZ puede consultar recursos en Internet.

Figura 7. Acceso HTTP desde la WAN simulada hacia la DMZ



. Fuente: Autoría Propia

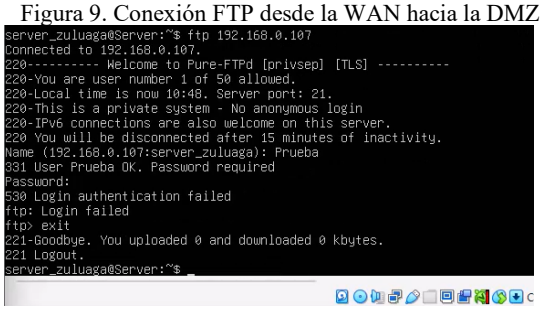
Aquí se observa el resultado de curl http://192.168.0.108:80 ejecutado desde la interfaz NAT del servidor. La salida confirma que la WAN puede acceder al servicio HTTP alojado en la DMZ.

Figura 8. Conexión FTP desde la LAN hacia la DMZ

. Fuente: Autoría Propia

En esta captura se aprecia la conexión FTP iniciada desde el Desktop hacia el servidor (192.168.0.108). La solicitud de credenciales indica que el servicio está activo y accesible.

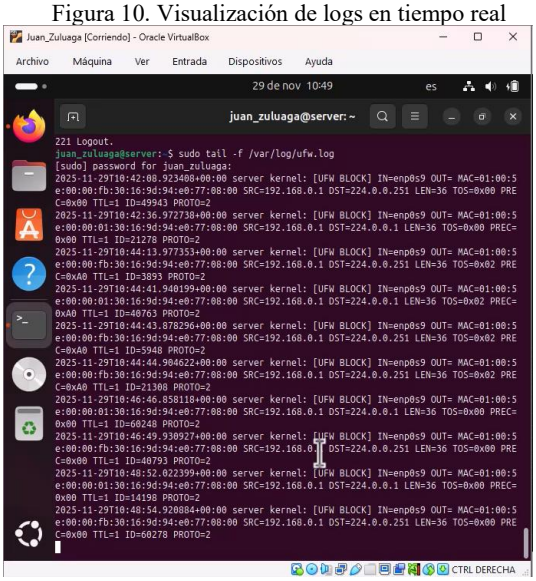
Figura 9. Conexión FTP desde la WAN hacia la DMZ



. Fuente: Autoría Propia

Aquí se observa la conexión FTP iniciada desde la interfaz WAN del servidor hacia su propia DMZ. Esto simula el acceso externo al servidor FTP.

Figura 10. Visualización de logs en tiempo real



. Fuente: Autoría Propia

En esta imagen se presenta la ejecución del comando sudo tail -f /var/log/ufw.log. Aquí se pueden ver las entradas UFW ALLOW que corresponden a cada una de las pruebas realizadas (HTTP y FTP).

En conjunto, las reglas de acceso configuradas permitieron gestionar adecuadamente el tráfico entre las zonas LAN, DMZ y WAN, demostrando control granular sobre los servicios HTTP y FTP. Las pruebas funcionales confirmaron que la comunicación autorizada fluye correctamente y que los accesos no permitidos son bloqueados según lo esperado. Las capturas de pantalla y los logs verifican que el firewall UFW desempeña correctamente el rol de segmentación en la topología simulada.

3 CONCLUSIONES.

La implementación de medidas de seguridad en GNU/Linux mediante la distribución Endian Firewall (EFW) permitió fortalecer las competencias en administración de sistemas operativos, demostrando la importancia de segmentar la red en zonas (LAN, WAN y DMZ) y aplicar reglas de acceso, NAT y proxy para garantizar la integridad y protección de los servicios. Este proceso evidenció cómo las herramientas de código abierto ofrecen soluciones eficientes para el control del tráfico, la autenticación de usuarios y la prevención de amenazas, consolidando así una comprensión integral de la seguridad perimetral y la gestión segura de redes bajo entornos Linux.

4 REFERENCIAS

[1] Debian. (2023). El manual del administrador de Debian 12.5.0.
[2] LPI LPIC-1 Exam 101. (2022). Tema 101: Arquitectura del Sistema. Linux Professional Institute.
[3] LPI LPIC-1 Exam 101. (2022). Tema 102: Instalación de Linux y gestión de paquetes. Linux Professional Institute.
[4] Oracle. (2020). Manual de usuario VirtualBox.