Implementación de Seguridad en Sistemas GNU/LINUX usando Endian Firewall y Virtualización

Luis Estevan Cardenas Esterling, *Universidad Nacional Abierta y a Distancia - UNAD, estebancardenassterling@gmail.com*

Resumen- Este artículo presenta una implementación de seguridad perimetral en sistemas GNU/Linux mediante la distribución Endian Firewall en un entorno virtualizado con VirtualBox. Se describe la configuración de zonas de red segmentadas (LAN, DMZ, WAN), la aplicación de reglas de firewall y Network Address Translation (NAT), y la implementación de un proxy HTTP no transparente con autenticación. Los resultados demuestran la efectividad de estas medidas para mitigar riesgos de intrusión, controlar el tráfico de red y asegurar los recursos internos. Se destaca la importancia de la segmentación de red y las políticas de acceso para garantizar la seguridad y la continuidad operativa en entornos GNU/Linux.

Palabras clave: Seguridad en Linux, Endian Firewall, Virtualización, NAT, Proxy HTTP, Segmentación de red, Administración de sistemas.

I. Introducción

La seguridad informática en sistemas operativos GNU/Linux es un aspecto crítico para garantizar la integridad, confidencialidad y disponibilidad de la información en entornos empresariales y académicos. Con el creciente uso de redes virtualizadas y la proliferación de amenazas cibernéticas, es fundamental implementar soluciones robustas que permitan segmentar y controlar el tráfico de red, minimizando riesgos de intrusión y accesos no autorizados. En este contexto, la distribución Endian Firewall ofrece una plataforma integrada para la gestión de seguridad perimetral, combinando funcionalidades de firewall, NAT y proxy con autenticación.

Este trabajo se enfoca en la implementación práctica de un entorno seguro basado en GNU/Linux utilizando Endian Firewall en un entorno virtualizado con VirtualBox. Se busca demostrar cómo la segmentación de red en zonas LAN, DMZ y WAN, junto con políticas de acceso y autenticación, contribuyen a fortalecer la seguridad y facilitar la administración de sistemas. Los objetivos principales son configurar una infraestructura segura, validar la efectividad de las reglas de firewall y NAT, y controlar el acceso a Internet mediante un proxy autenticado.

[*] Universidad Abierta y a Distancia - UNAD.

II. Estado del arte / Trabajos relacionados

La seguridad en sistemas Linux ha sido ampliamente estudiada, con diversas soluciones que abordan la protección perimetral y la segmentación de redes. Firewalls tradicionales como iptables y nftables ofrecen control granular del tráfico, pero requieren configuraciones complejas y no siempre integran servicios adicionales como proxy o autenticación [1]. Distribuciones especializadas como Endian Firewall, pfSense y OPNsense proporcionan interfaces gráficas y funcionalidades integradas que facilitan la administración y mejoran la seguridad [2][3].

La virtualización, por su parte, permite crear entornos aislados y replicables para pruebas y despliegues seguros, siendo VirtualBox una herramienta popular por su accesibilidad y compatibilidad [4]. Estudios recientes han demostrado que la combinación de firewalls especializados con entornos virtualizados mejora la flexibilidad y reduce costos operativos [5]. Sin embargo, la implementación práctica y la validación de estas soluciones en entornos educativos o de pequeña escala aún requieren mayor difusión y documentación.

III. Metodología

La implementación de la seguridad perimetral en sistemas GNU/Linux utilizando Endian Firewall y virtualización se llevó a cabo siguiendo una metodología estructurada en varias etapas:

A. Diseño del entorno virtualizado

Se utilizó Oracle VirtualBox para crear un entorno virtualizado que simulara una red con tres zonas: LAN (Local Area Network), DMZ (Demilitarized Zone) y WAN (Wide Area Network). Se creó una máquina virtual (VM) con las siguientes especificaciones:

Sistema operativo: GNU/Linux
Memoria RAM: 2 GB
Espacio en disco: 20 GB

Adaptadores de red: 3
Configuración de los adaptadores de red:
Adaptador 1: Modo NAT (Network Address Translation), conectado a la red WAN (simulando acceso a Internet).
Adaptador 2: Modo "Red Interna", nombre "Verde_LAN", conectado a la red LAN.
Adaptador 3: Modo "Red Interna", nombre "Naranja_DMZ", conectado a la red DMZ.

B. Instalación y configuración de Endian Firewall

Se descargó la imagen ISO de Endian Firewall Community desde el sitio web oficial. La imagen ISO se montó en la unidad virtual de la VM. Se inició la VM y se siguió el asistente de instalación de Endian Firewall, realizando las siguientes configuraciones:

Idioma: English
Aceptación de términos de licencia
Selección del disco virtual para la instalación
Configuración de la contraseña de root
Configuración de la red:
Asignación de interfaces de red a las zonas:
eth0: Zona Roja (WAN)
eth1: Zona Verde (LAN)
eth2: Zona Naranja (DMZ)
Configuración de direcciones IP:
Zona Verde (LAN): Dirección IP estática 192.168.10.1/24
Zona Naranja (DMZ): Dirección IP estática 192.168.20.1/24
Zona Roja (WAN): Configuración DHCP (obtener dirección IP automáticamente)
Finalización de la instalación y reinicio de la VM

C. Configuración de NAT y reglas de firewall

Se accedió a la interfaz web de administración de Endian Firewall (https://192.168.10.1:10443) desde una máquina en la red LAN. Se realizaron las siguientes configuraciones:

Habilitación de NAT (Network Address Translation) para permitir que las zonas LAN y DMZ accedan a Internet a través de la zona WAN. Esto se configuró en la sección "Firewall" -> "NAT" -> "Masquerading".
Creación de reglas de firewall para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) desde la LAN hacia la DMZ. Esto se configuró en la sección "Firewall" -> "Traffic between zones".
Creación de una regla de firewall para denegar todo otro tráfico desde la LAN hacia la DMZ.
Creación de una regla de firewall para denegar todo el tráfico desde la DMZ hacia la LAN.

D. Implementación de Proxy HTTP no transparente

Se configuró un proxy HTTP no transparente en Endian Firewall para controlar y filtrar el tráfico web. Esto se realizó en la sección "Proxy" -> "HTTP". Se realizaron las siguientes configuraciones:

Habilitación del proxy HTTP en modo "No transparente".
Configuración del puerto del proxy en 8080.
Habilitación de la autenticación local.
Creación de usuarios y contraseñas para permitir el acceso a Internet a través del proxy.
En las máquinas cliente de la red LAN, se configuró el navegador web para utilizar el proxy HTTP con la dirección IP 192.168.10.1 y el puerto 8080.

E. Pruebas y validación

Se realizaron pruebas de conectividad y seguridad para validar la efectividad de la configuración:

Pruebas de conectividad: Se verificó que las máquinas en la LAN y DMZ podían acceder a Internet a través de la zona WAN.
Pruebas de acceso a servicios: Se verificó que las máquinas en la LAN podían acceder a los servicios HTTP y FTP en la DMZ.
Pruebas de autenticación: Se verificó que los usuarios debían autenticarse para navegar a través del proxy HTTP.

IV. Resultados

La configuración de la instancia Endian en VirtualBox permitió establecer una infraestructura segmentada con tres zonas de red claramente definidas. Se verificó la correcta asignación de IPs y la comunicación entre zonas mediante pruebas de conectividad (ping, acceso HTTP y FTP). La habilitación de NAT facilitó el acceso a Internet desde las zonas LAN y DMZ, mientras que las reglas de firewall garantizaron la restricción de tráfico no autorizado.

A. Configuración de la instancia Endian en VirtualBox

Se creó una máquina virtual en VirtualBox con 2 GB de RAM y un disco duro virtual de 20 GB, configurando tres adaptadores de red para representar las zonas LAN (verde), DMZ (naranja) y WAN (roja). La distribución Endian Firewall fue instalada exitosamente, asignando direcciones IP estáticas para las zonas LAN (192.168.10.1/24) y DMZ (192.168.20.1/24), mientras que la zona WAN obtuvo su IP mediante DHCP proporcionado por VirtualBox.

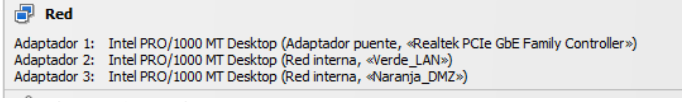

Ilustración 1 Configuración de adaptadores de red en VirtualBox para Endian Firewall

Ilustración 2 Asignación de IPs en Endian Firewall

Esta configuración permitió simular un entorno de red segmentado, fundamental para la implementación de políticas de seguridad perimetral.

B. Configuración NAT y reglas de firewall

Se habilitó el enmascaramiento NAT (Network Address Translation) para permitir que las zonas LAN y DMZ accedan a Internet a través de la zona WAN. Se definieron reglas específicas en el firewall para permitir el tráfico HTTP (puerto 80) y FTP (puerto 21) desde la LAN hacia la DMZ, mientras que se denegaron otros servicios no autorizados y se bloqueó el acceso desde la DMZ hacia la LAN para proteger los recursos internos.

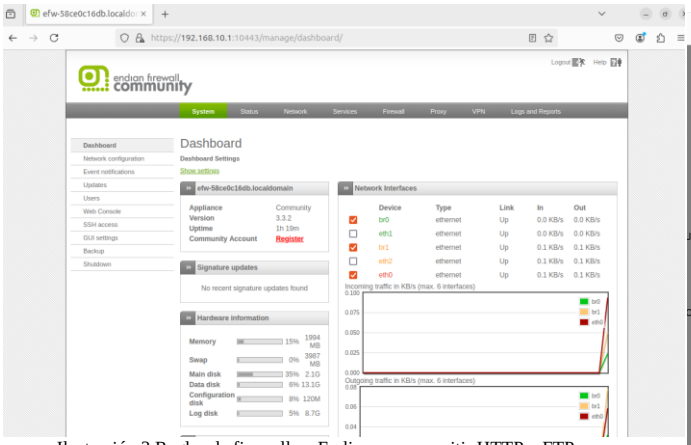

Ilustración 3 Reglas de firewall en Endian para permitir HTTP y FTP

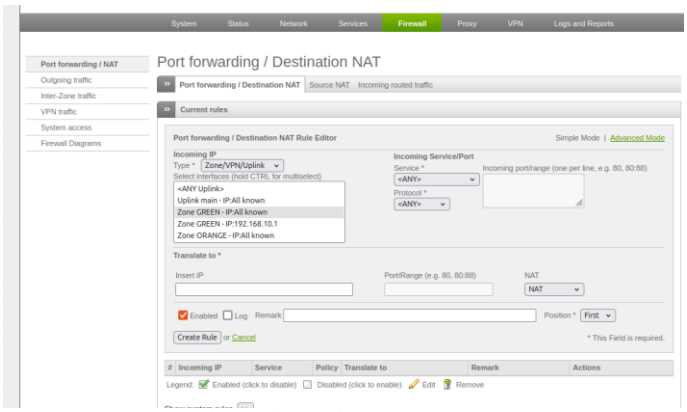

Ilustración 4 Configuración NAT en Endian Firewall

Las pruebas de conectividad confirmaron que los dispositivos en la LAN y DMZ podían acceder a Internet y a los servicios permitidos, mientras que se mantenía la segregación y seguridad entre las zonas.

C. Implementación de Proxy HTTP no transparente

Se configuró un proxy HTTP no transparente en Endian Firewall con autenticación local para controlar y filtrar el tráfico web. Los usuarios de la red LAN debían autenticarse para navegar, lo que permitió registrar y restringir el acceso a Internet según políticas definidas.

Ilustración 5 Configuración del proxy HTTP no transparente en Endian

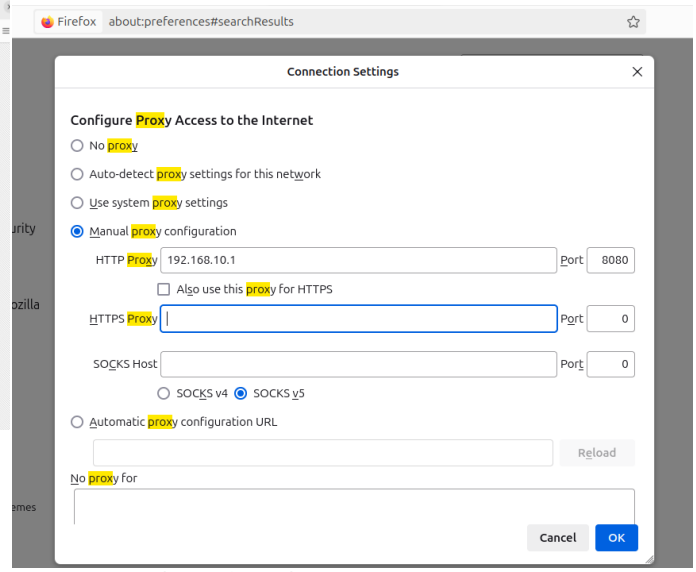

Ilustración 6 Configuración del navegador cliente para usar el proxy

Esta implementación mejoró el control sobre el uso de recursos de red y contribuyó a la seguridad general del entorno.

V. Discusión

La segmentación de la red mediante Endian Firewall en un entorno virtualizado demostró ser una solución efectiva para mejorar la seguridad perimetral en sistemas GNU/Linux. La integración de reglas de firewall, NAT y proxy con autenticación permite un control granular del tráfico y reduce la superficie de ataque. Sin embargo, la implementación presenta limitaciones, como la dependencia del rendimiento del hardware subyacente y la necesidad de una configuración cuidadosa para evitar bloqueos accidentales.

Futuras mejoras podrían incluir la automatización de políticas mediante scripts, la integración con sistemas de detección de intrusiones (IDS) y la ampliación a entornos con alta disponibilidad. Además, la incorporación de métricas de seguridad más avanzadas y pruebas de estrés permitirían validar la escalabilidad y robustez del sistema en escenarios reales.

VI. Conclusiones

Este trabajo presenta una implementación práctica y documentada de seguridad perimetral en sistemas GNU/Linux utilizando Endian Firewall en un entorno virtualizado. Se logró configurar una infraestructura segmentada que controla eficazmente el tráfico entre zonas LAN, DMZ y WAN, aplicando reglas de firewall y NAT que garantizan la protección de recursos internos. La implementación de un proxy HTTP no transparente con autenticación local permitió controlar y registrar el acceso a Internet, mejorando la gestión y seguridad de la red.

Las contribuciones principales incluyen la demostración de la viabilidad de soluciones integradas de seguridad en entornos virtualizados accesibles para entornos educativos y de pequeña escala, así como la documentación detallada de procedimientos replicables. Este trabajo sienta las bases para futuras investigaciones y desarrollos en administración segura de sistemas Linux.

Agradecimientos

Se agradece al tutor Martin Camilo Cancelado Ruiz, al Linux Professional Institute (LPI) por los recursos y estándares proporcionados a través de Linux Essentials, y a la Universidad Nacional Abierta y a Distancia (UNAD) por el apoyo en el desarrollo de este trabajo.

Referencias

[1] Canonical, "Guía del Ubuntu desktop 20.04 LTS," 2023. [Online]. Available: https://help.ubuntu.com/20.04/ubuntu-help/index.html

[2] Debian, "El manual del administrador de Debian 12.5.0," 2023. [Online]. Available: https://www.debian.org/releases/stable/amd64/index.es.html

[3] Endian, "Endian UTM 3.2 Manual referencia," 2016. [Online]. Available: http://docs.endian.com/3.2/utm/index.html

[4] Linux Professional Institute, "Linux Essentials - Tema 102: Comandos GNU y Unix," 2022. [Online]. Available: https://learning.lpi.org/es/learning-materials/101-500/102/

[5] Oracle, "Manual de usuario VirtualBox," 2020. [Online]. Available: https://www.virtualbox.org/manual/