EXPLORANDO LA GESTIÓN Y SEGURIDAD EN GNU/LINUX: APRENDIZAJES DE UN DIPLOMADO EN SISTEMAS ABIERTOS.

Dabiam Arley Pulido Layton
e-mail: dapulidol@unadvirtual.edu.co
Erika Lorena Suarez Moreno
e-mail: elsuarezm@unadvirtual.edu.co

RESUMEN: *Este artículo documenta el camino recorrido en el diplomado de administración de sistemas operativos Open Source, destacando los aprendizajes prácticos en la configuración y seguridad de GNU/Linux. Se abordaron temas clave como la organización del disco duro, la instalación del gestor de arranque GRUB, el manejo de librerías esenciales y la administración de paquetes. Un componente central fue la implementación de medidas de seguridad a través de la configuración de GNU/Linux Endian Firewall en VirtualBox, detallando cómo se establecieron las zonas de red para proteger un entorno virtual. El objetivo fue el de compartir las experiencias y los "hallazgos" obtenidos durante esta etapa de profundización.*

PALABRAS CLAVE: Endian Firewall, GNU/Linux, paquetes, redes.

1 INTRODUCCIÓN

Esta etapa del diplomado fue una excelente oportunidad para consolidar lo que se conoce acerca de cómo se arma un sistema Linux y cómo se manejan sus programas. Abordando los comandos más importantes de GNU/Linux. La base de este trabajo fue el material "Linux Essentials" del Linux Professional Institute (LPI), específicamente el Módulo 102, que es fundamental para entender la instalación y gestión de paquetes [1]. Así mismo, se efectuó la configuración y puesta en marcha del Endian Firewall en VirtualBox, prestando especial atención a cómo se organizan las tarjetas de red para su funcionamiento efectivo. Fue un proceso de aprendizaje tanto práctico como enriquecedor.

2 INSTALACION ENDIAN

2.1 CARACTERÍSTICAS GENERALES

En primer lugar, se descarga la distribución de Endian UTM desde su sitio oficial y se instala en plataformas como VirtualBox o en hardware físico. Es compatible con arquitecturas x86 [1].

Se utiliza el programa Oracle VM VirtualBox para la creación de una máquina virtual con las siguientes configuraciones:

- Tipo: Linux
- Versión: Oracle Linux (64 bit)
- Unidad óptica virtual: ISO

2.2 INSTALACION

En este apartado se detalla el proceso de instalación de Endian y la respectiva evidencia de su inicio.

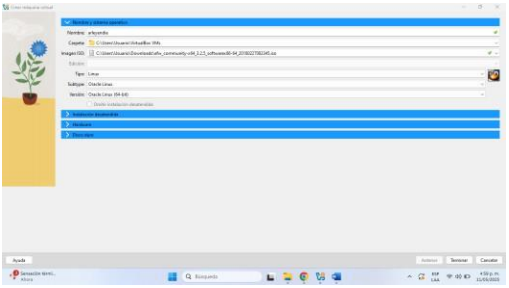

Figura 1. Creación de máquina virtual

Como se muestra en la figura 1 se crea una nueva maquina virtual y se monta la ISO en dicha máquina, colocando el respectivo nombre de la maquina y escogiendo el tipo de sistema operativo [1].

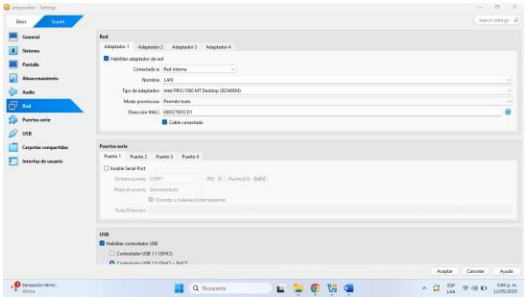

Figura 2. Configuración de adaptador puente 1.

Como se muestra en la figura 2 Se asignan adaptadores en modo puente (bridge), lo cual es esencial para que la VM tenga conectividad en la red física del entorno, permitiendo así un control preciso y una simulación cercana a un entorno real de red [1]. Se configuran múltiples adaptadores (puentes) para segmentar diferentes zonas de red, como la interna (LAN) y la DMZ.

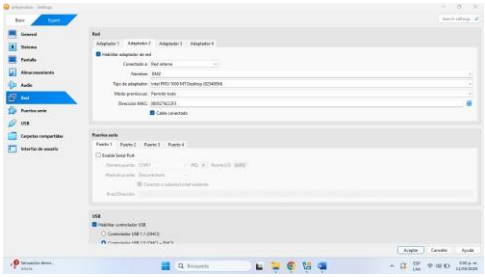

Figura 3. Configuración de adaptador puente 2.

Como se muestra en la figura 3 se configura el adaptador 2 como red interna LAN (GREEN), la cual corresponde a la zona interna y se configura la interacción con el entorno virtual, incluyendo la deshabilitación de puertos seriales si no son necesarios [2].

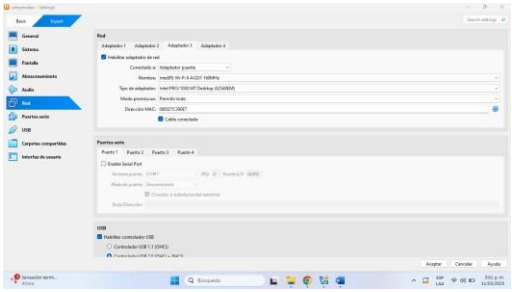

Figura 4. Configuracion de adaptador puente 3.

Como se muestra en la figura 4 se configura el adaptador 3 como red interna DMZ (ORANGE).

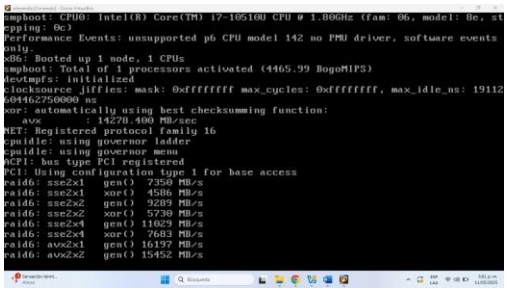

Figura 5. Se da inicio a la máquina virtual de Endian.

Como se muestra en la figura 5 se da inicio a la máquina virtual de endian.

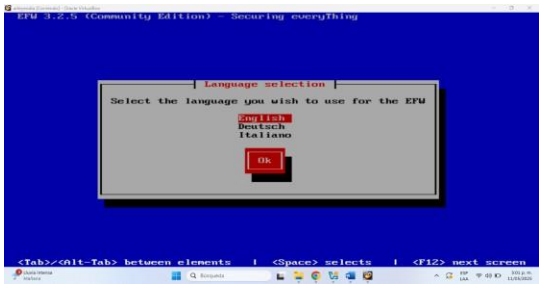

Figura 6. Selección del idioma.

Como se muestra en la figura 6 se selecciona el idioma de inglés.

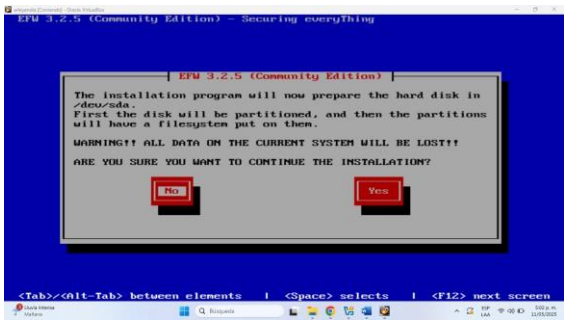

Figura 7. Creación de la partición para instalación del sistema.

Como se muestra en la figura 7 se selecciona la opción *yes* para que cree una partición e instale el sistema.

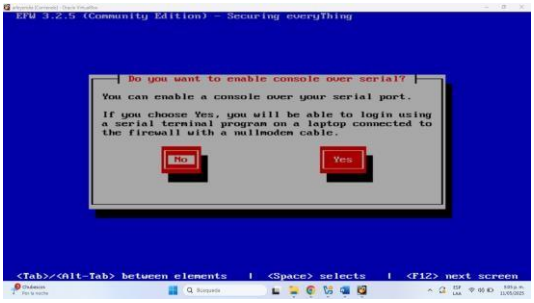

Figura 8. Selección *No* a la habilitacion de puerto serial.

Como se muestra en la figura 8 se selecciona la opción *No* porque no es necesario habilitar el acceso al firewall a través de un puerto serial.

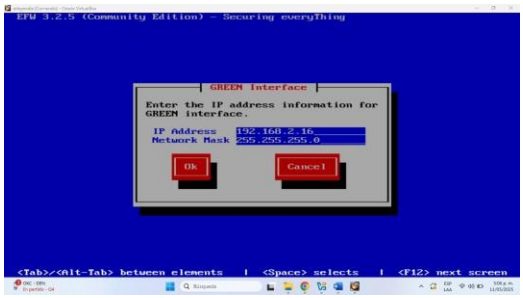

Figura 9. Establecimiento de ip GREEN.

Como se muestra en la figura 9 se establece la ip y la máscara de (GREEN).

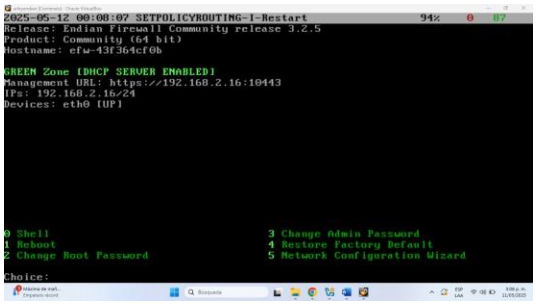

Figura 10. Evidencia de inicio de endian.

Como se muestra en la figura 10 de forma exitosa se logra dar inicio a endian, donde no se muestra la ip de (GREEN).

Este proceso ilustra un enfoque práctico para aprender a instalar un firewall en un entorno controlado y simulado, resaltando la importancia de la segmentación de red y de mantener la seguridad desde la fase inicial de instalación.

3 DESARROLLO TEMATICAS

3.1 TEMATICA 5: IMPLEMENTAR UN PROXY HTTP (NO TRANSPARENTE) CON POLÍTICAS DE AUTENTICACIÓN PARA NAVEGACIÓN EN INTERNET.

Producto esperado: El producto esperado consiste en crear un perfil y establecer una lista negra que bloquee los sitios www.hotmail.com, www.youtube.com y www.elnuevodia.com.co. Además, se debe implementar la autenticación por usuario, creando un usuario y asignándolo a un grupo, estableciendo una política de acceso y vinculando esta política con el perfil creado. Finalmente, se debe probar el acceso a los sitios bloqueados desde la LAN utilizando un navegador web [4] [5].

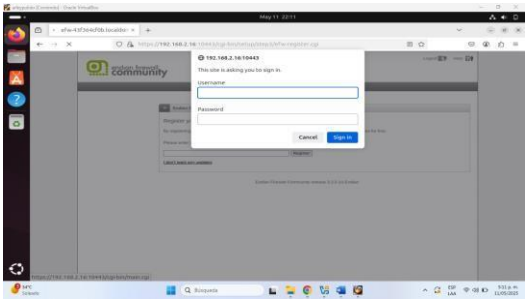

Figura 11. Autenticación de usuario y contraseña Endian.

Como se muestra en la figura 11 se ingresa a Firefox y con la ip de GREEN https://192.168.2.16:10443 se entra a endian [6].

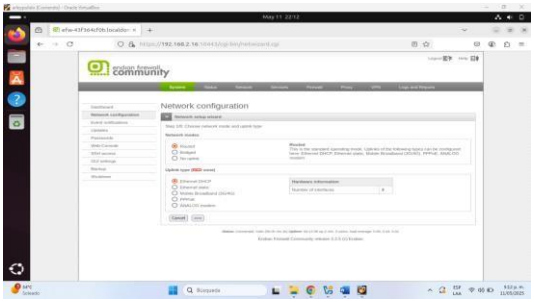

Figura 12. Configuración de RED en modo DHCP.

Como se muestra en la figura 12 se ingresa al módulo de Network configuration y se procede a configurar RED de manera DHCP.

Figura 13. Definición de segmento de red.

Como se muestra en la figura 13, se configura el tipo de red para las zonas del firewall. Posteriormente se selecciona ORANGE para definir el segmento de red que será accesible desde Internet (DMZ).

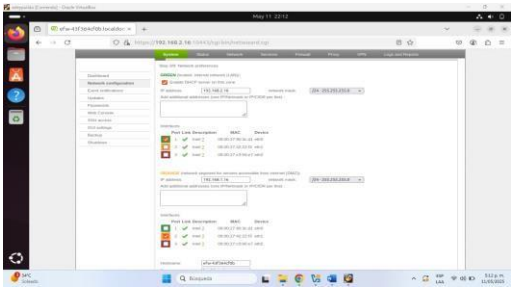

Figura 14. Confirmación de ip de GREEN y ORANGE.

Como se muestra en la figura 14 se configuran las ip de GREEN (192.168.2.16 (eth1)) y ORANGE (192.168.1.16 (eth2)).

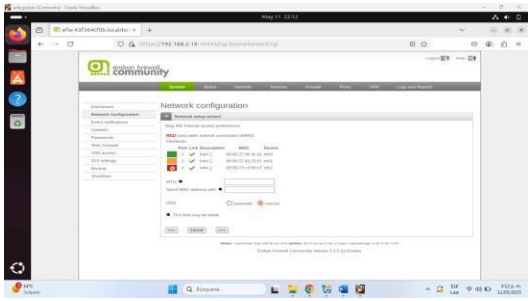

Figura 15. Confirmación de configuración de RED en DHCP.

De igual forma como se muestra en la figura 15 se realiza la confirmación a RED (DHCP (eth0)).

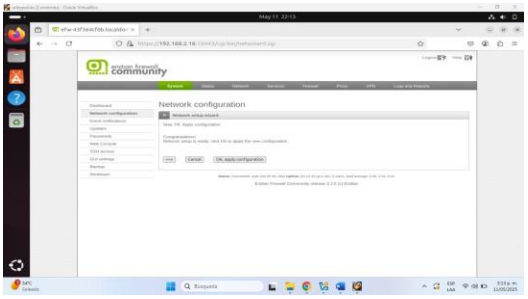

Figura 16. Aplicación de cambios.

Como se muestra en la figura 16, se aplican todos los cambios de la configuracion de la red.

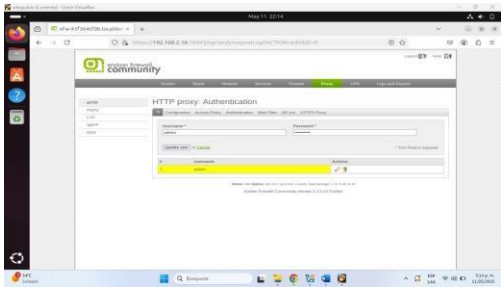

Figura 17. Creacion de usuarios.

De igual forma como se muestra en la figura 17, se procede al ingreso del modulo de autenticacion y se crea el usuario admin, con la respectiva contraseña.

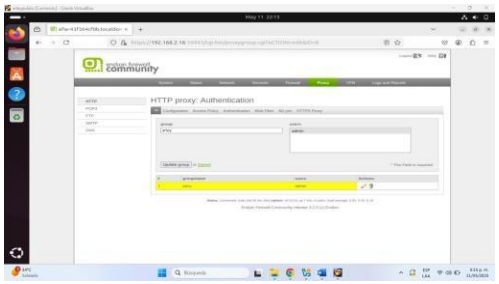

Figura 18. Creacion de grupo.

De igual forma como se muestra en la figura 18, se procede dar ingreso al modulo de autenticacion y se crea el grupo neftali, con la respectiva contraseña y se asocia el usuario creado a dicho grupo.

La política de acceso se vincula a este perfil, de modo que solo los usuarios autenticados puedan acceder a ciertos recursos o sitios en la red, reforzando así la seguridad de navegación [6].

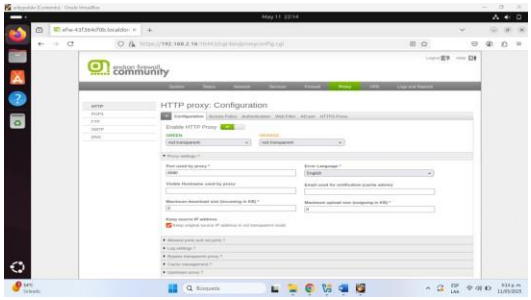

Figura 19. Habilitacion de proxy y modo no transparente.

Como se muestra en la figura 19, se situan las redes en tipo no transparente, puerto 8080 y demás configuración, asegurando que toda la navegación pase por el proxy y su política de control.

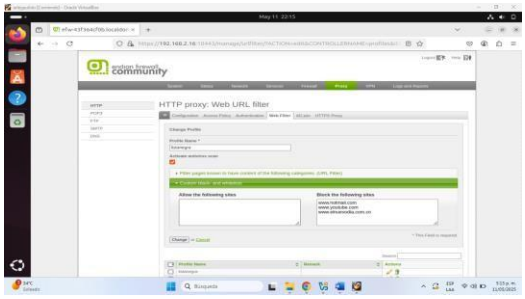

Figura 20. Creacion de lista negra.

Como se muestra en la figura 20 se crea un nuevo filtro con el nombre lista_negra, donde se procede a bloquear 3 páginas, www.hotmail.com, www.youtube.com, y www.elnuevodia.com.co.

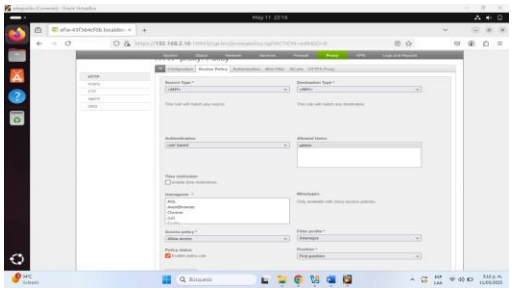

Figura 21. Aplicación de politicas de acceso.

Como se muestra en la figura 21 se crea una política de acceso donde se asocia el usuario admin, luego se selecciona la opción para que se apruebe la regla que se creó llamada lista_negra y se diligencia la demás configuración.

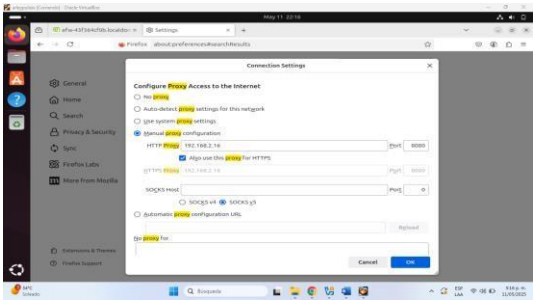

Figura 22. Configuracion de proxy en firefox.

Como se muestra en la figura 22 se ingresa a la configuración de proxy en el buscador Firefox y manualmente se realiza la configuración del Proxy donde se pone la ip 192.168.2.16 y se diligencia la opción para usar el mismo proxy en HTTPS.

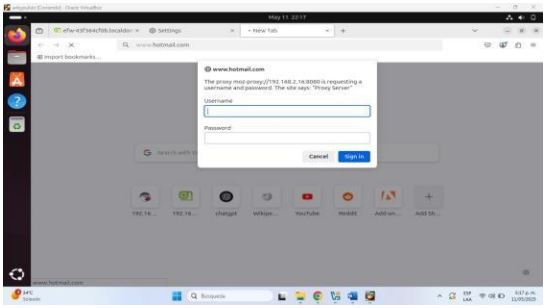

Figura 23. Autenticacion de usuario y contraseña.

Como se muestra en la figura 23 se realizan intentos de ingreso las páginas bloqueadas y éstas piden autenticación de usuario.

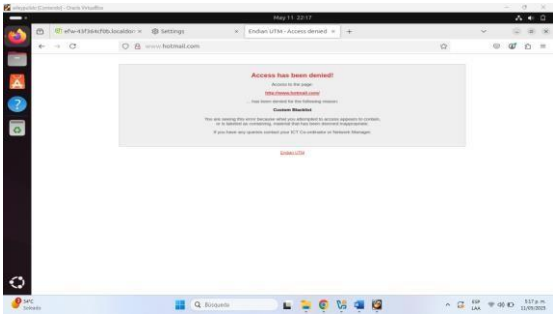

Figura 24. Acceso denegado de www.hotmail.com.

Como se muestra en la figura 24, se realizan los intentos para acceder a www.hotmail.com y se muestra el mensaje de la figura 24.

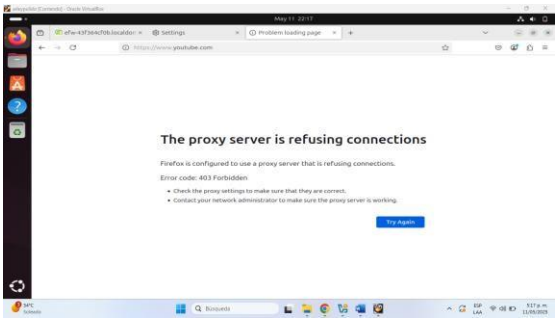

Figura 25. Acceso denegado a www.youtube.com.

Como se muestra en la figura 25, se realiza el intento de acceder a www.youtube.com.

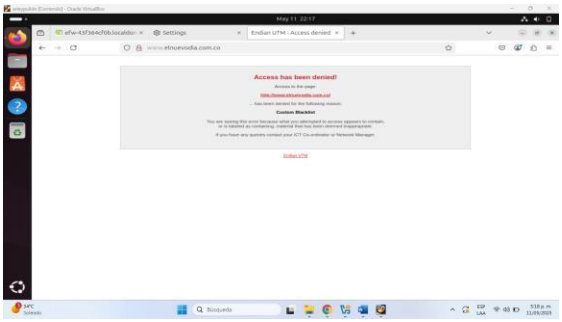

Figura 26. Acceso denegado a www.elnuevodia.com.co.

Como se muestra en la figura 26, se efectúa el intento de acceder a www.elnuevodia.com.co.

El proceso anterior ejemplifica cómo un proxy no transparente, combinado con políticas de listas negras y autenticación, puede ser una herramienta eficaz de gestión y control del acceso a contenidos en una red, fortaleciendo la seguridad y el cumplimiento de las políticas de uso [6] [7].

4 CONCLUSIONES

El diplomado reforzó conocimientos sobre la organización del sistema de archivos, la gestión de paquetes y la utilización de comandos esenciales. La instalación y puesta en marcha práctica de Endian en VirtualBox contribuyó a consolidar el entendimiento de cómo administrar un sistema operativo basado en Linux desde cero, reforzando la importancia de herramientas como RPM, YUM, DNF y Zypper.

La configuración de Endian Firewall y su integración en una red virtual evidenció su potencial para proteger y segmentar redes internas. La aplicación de políticas de acceso, listas negras y autenticación de usuarios en el proxy fueron prácticas que demostraron un enfoque integral para fortalecer la seguridad en entornos corporativos y académicos.

La implementación de reglas específicas de bloqueo y autenticación en el proxy permitió controlar y monitorear el tráfico web, contribuyendo a prevenir accesos no autorizados o peligrosos. Esto resalta la importancia de políticas precisas y del uso de herramientas de gestión para mantener la integridad y confidencialidad de los datos en redes organizadas.

La creación de políticas específicas, listas negras, y la configuración de autenticación de usuario en el proxy, demostraron cómo aplicar controles efectivos al acceso a recursos web. La configuración adecuada en los navegadores permitió verificar en tiempo real el correcto funcionamiento de dichas políticas, asegurando una navegación controlada y segura.

5 REFERENCIAS

[1] LPI LPIC-1 Exam 101. (2022). Tema 102: Comandos GNU y Unix. https://learning.lpi.org/es/learning-materials/101-500/102/

[2] Canonical (2023). Guía del Ubuntu desktop 20.04 LTS. Help Ubuntu. https://help.ubuntu.com/20.04/ubuntu-help/index.html

[3] Debian (2023). El manual del administrador de Debian 12.5.0. Debian https://www.debian.org/releases/stable/amd64/index.es.html

[4] Oracle (2020), Manual de usuario VirtualBox. VirtualBox. https://www.virtualbox.org/manual/

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

[6] Jay LaCroix. (2020). Mastering Ubuntu Server : Gain Expertise in the Art of Deploying, Configuring, Managing, and Troubleshooting

[7] Ubuntu Server. Packt Publishing. https://research-ebsco-com.bibliotecavirtual.unad.edu.co/linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952