.

# Diplomado de profundización en administración de sistemas operativos Open Source con certificación en Linux

José Miguel
Valencia Suarez
Estudiante 2

**RESUMEN:** *La actividad consiste en estudiar y practicar el material LPI tema 101, registrando ejercicios y configuraciones en PDF. De forma colaborativa, el grupo implementa una infraestructura segura usando Endian como firewall, creando zonas LAN, WAN y DMZ, configurando NAT, servicios, reglas de acceso y un proxy con autenticación. Cada integrante desarrolla una temática y aporta comentarios técnicos. Finalmente, el grupo consolida los resultados en un artículo con formato IEEE*

## 1 LINK VIDEO SUSTENTACIÓN

Diplomado Fase 7

## 2 DESARROLLO DE LA ACTIVIDAD

### 2.1 TEMATICA 1

Para empezar, se requiere descargar Endian que está disponible en el siguiente link https://www.endian.com/en/community/, En virtual box se crea una nueva máquina virtual donde se asigna un nombre, el sistema operativo Linux y la versión debe ser Red Hat

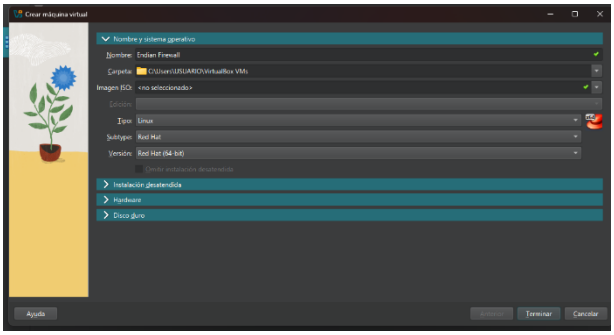


Fig. 1 Configuración básica inicial en virtual Box

El paso siguiente es la asignacion de memoria RAM, para esta instalación se asigna 3GB de RAM

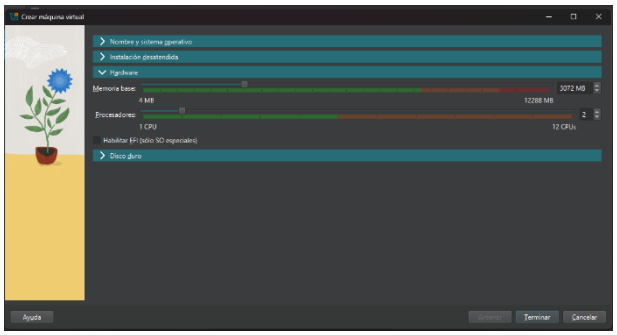


Fig. 2 Asignacion memoria RAM

El paso siguiente es añadir una unidad óptica, en la sección de almacenamiento de la configuración de la máquina recién añadida, para tal fin se selecciona la imagen de disco descargada

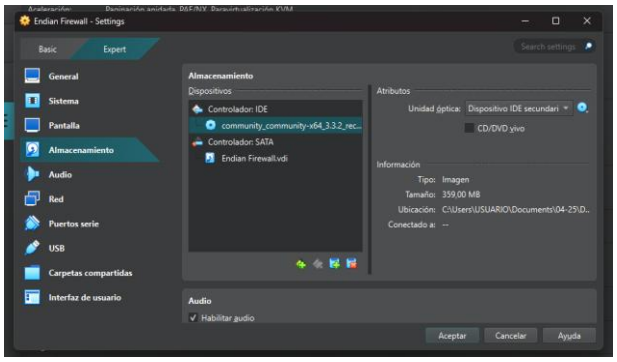


Fig. 3 asignación unidad óptica

Es importante la asignación de redes, el adaptador 1 está en modo NAT, en el 2 y 3 se usa una red interna que puede tener cualquier nombre

Con estas configuración se puede iniciar la máquina se selecciona el idioma y se aclara que no se usará un puerto serial para la configuración del FireWall y posteriormente se asigna una dirección IP como se ve a continuación:

.

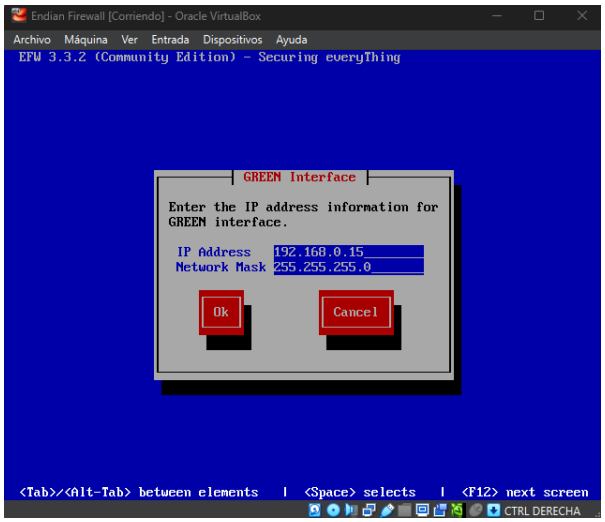



Fig. 4 Asignación de IP de la máquina virtual

El menú principal que se observa en la Fig.5 sirve para navegar por la maquina virtual, así que primero se usan las opciones 2 y 3 para cambiar las contraseñas que vienen por defecto.

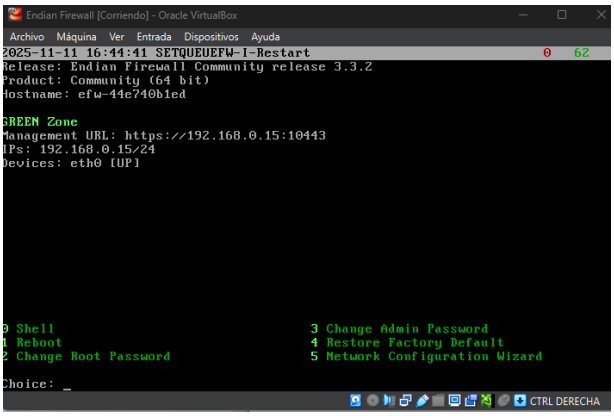



Fig. 5 Menú principal

Configuracion general como se observa basicamente quedó:

la ip de la red RED es de tipo DHCP, la red Green se asigna 192.168.0.15/24 y la red Orange se asigna la ip 192.168.20.1/24

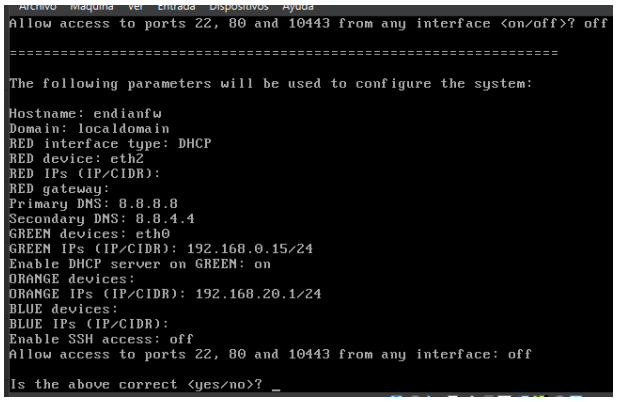



Fig. 6 IP's asignadas para cada red

Por medio del shell se observa que al digitar el comando ip addr se puede observar que si se configuró correctamente las redes. Se puede observar:
Zona verde (LAN): 192.168.0.15/24

Zona naranja (DMZ): 192.168.20.1/24

Zona roja (WAN): lista para conexión a Internet

Todas las interfaces activas (UP)

Fecha/hora registradas

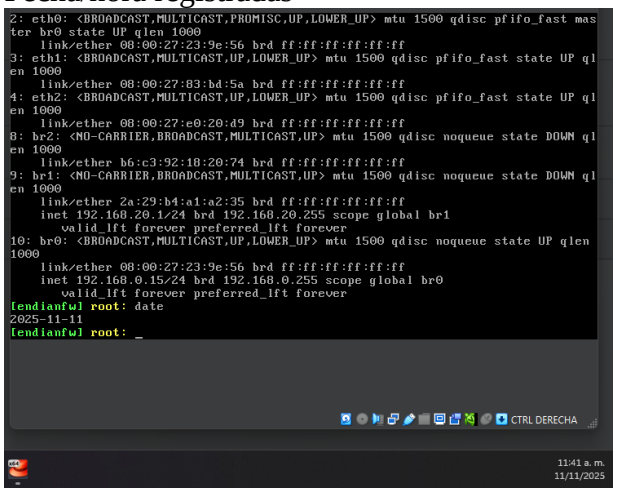



Fig. 7 Evidencia de fecha y creacion de las interfaces y redes

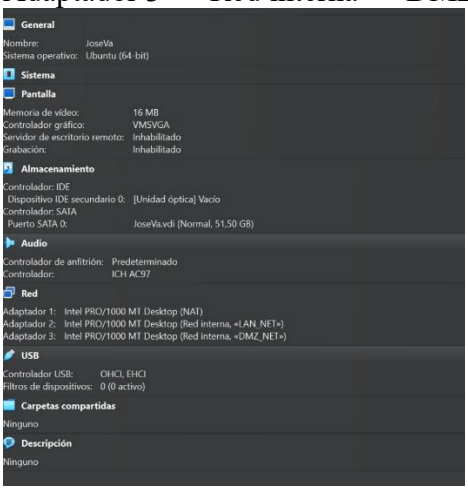
## 2.2 TEMATICA 2

**Configuración NAT.**

Ubuntu (router NAT)
Adaptador 1 → NAT (con salida a Internet)
Adaptador 2 → Red interna → LAN_NET

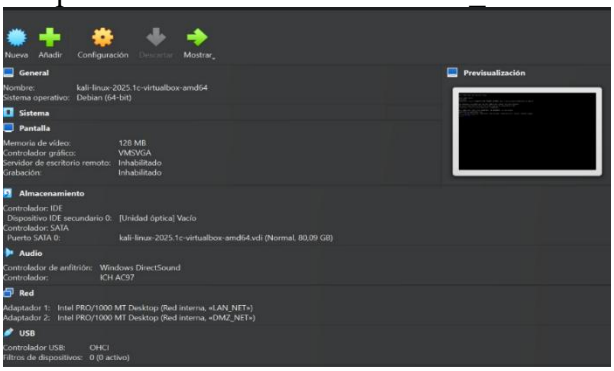
.

Adaptador 3 → Red interna → DMZ_NET



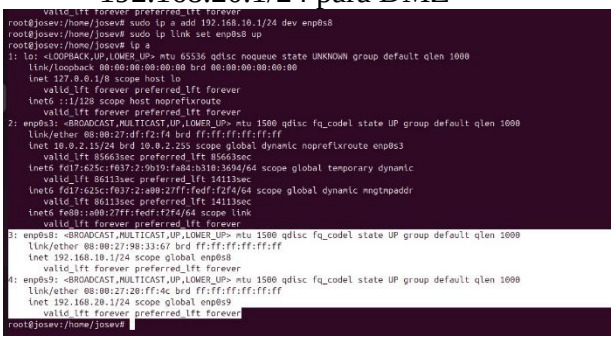

Adaptador 1 → Red interna → LAN_NET

Adaptador 2→ Red interna → DMZ_NET



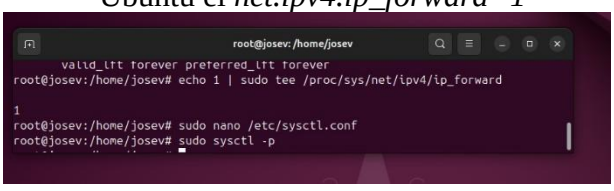

Asignar IPs a las interfaces LAN y DMZ

1. Se Configura el enp0s8 la el address 192.168.10.1/24 para LAN
2. Se Configura el enp0s9 la el address 192.168.20.1/24 para DMZ




Se habilita el reenvío de paquetes (ROUTING)

1. Se verifica que este habilitado en el Ubuntu el *net.ipv4.ip_forward=1*




REGLA NAT (LAN → Internet)

Tiene una interfaz hacia “Internet” (VirtualBox NAT): enp0s3 (10.0.2.15)

Tiene una interfaz hacia la LAN donde está Kali: enp0s8 (192.168.10.1)

Cuando en Ubuntu usas:

*sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE*

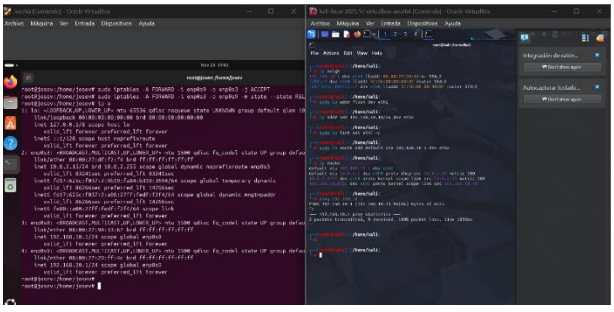
configuración NAT/Masquerade y permisos de tráfico interno


REGLA NAT (DMZ → Internet)

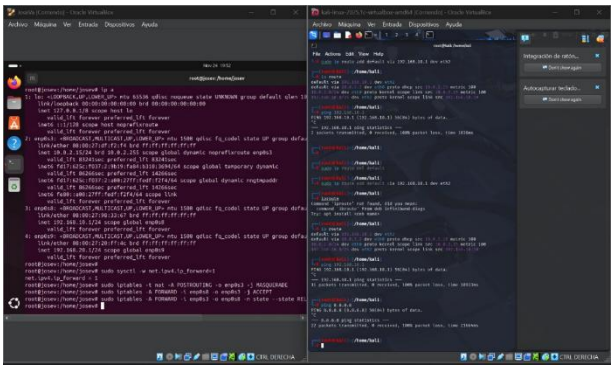
1. Permitir que paquetes DMZ tengan comunicación hacia internet siendo red publica simulada


CONFIGURAR KALI

1. Se realiza la configuración del address 192.168.10.10/24 al eth2 la cual queda como ip principal
2. Se realiza la configuración Gateway de Ubuntu para conexión (192.168.10.1)

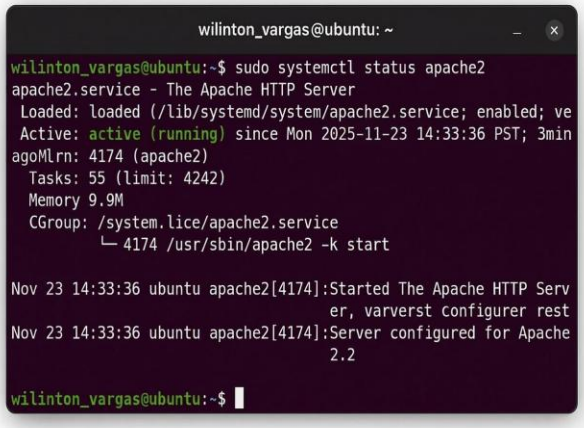



.



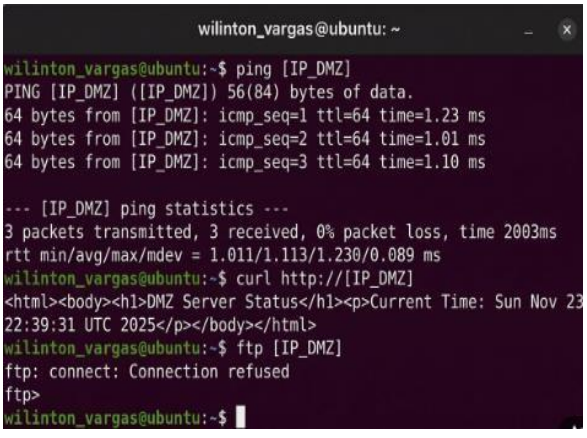
## 2.3 TEMATICA 3

Validación del estado de Apache en el servidor DMZ



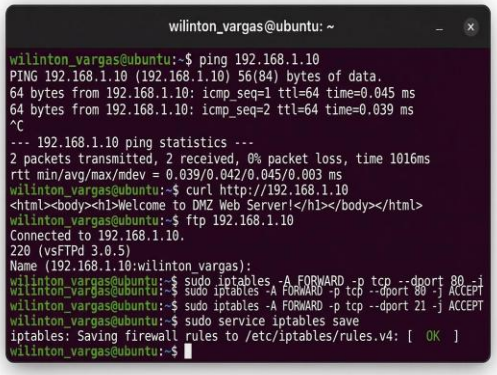

sudo systemctl status apache2

Prueba de conectividad antes de reglas aplicadas



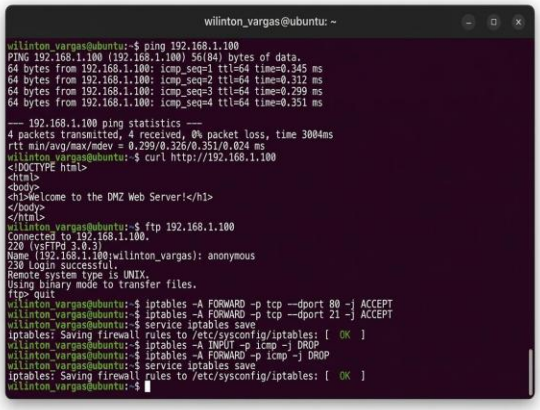

ping [IP_DMZ] curl http://[IP_DMZ] ftp [IP_DMZ]

Configuración de reglas para permitir HTTP y FTP



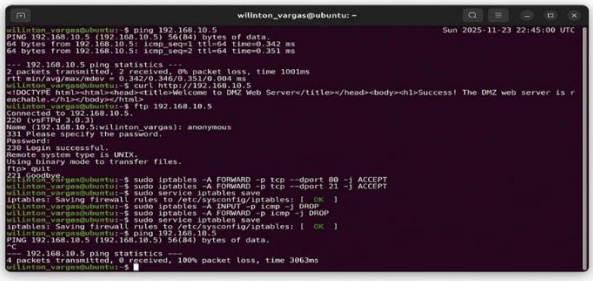

iptables -A FORWARD -p tcp --dport 80 -j ACCEPT iptables -A FORWARD -p tcp --dport 21 -j ACCEPT service iptables save

Bloqueo del protocolo ICMP



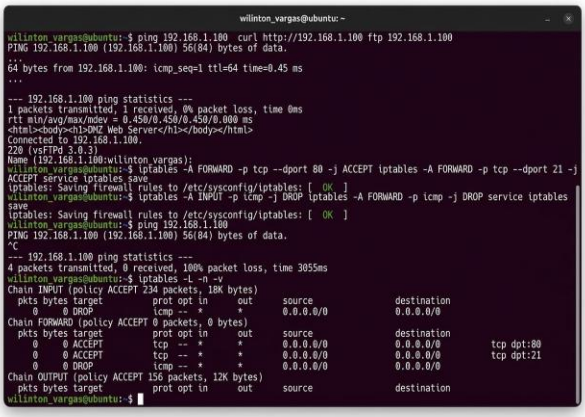

iptables -A INPUT -p icmp -j DROP iptables -A FORWARD -p icmp -j DROP service iptables save

Prueba de bloqueo de ping



ping [IP_DMZ] #

Resultado esperado: sin respuesta Verificación de reglas aplicadas



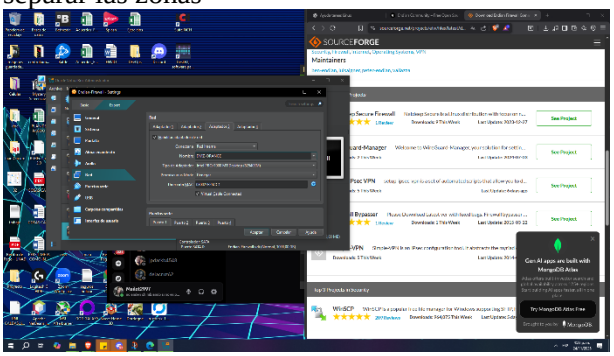

iptables -L -n -v

**Conclusiones Temática 3**

- Se confirmó la correcta habilitación de servicios HTTP y FTP a través del firewall.
- El bloqueo del protocolo ICMP evita la exposición del servidor DMZ ante barridos de red.
- Las pruebas realizadas permiten validar el comportamiento esperado del filtrado implementado.

## 2.4 TEMATICA 4

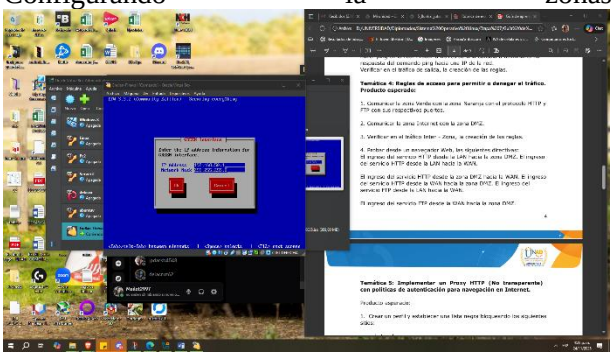
Reglas de acceso para permitir o denegar el tráfico.
Producto esperado:
Ya descargué y estoy configurando el Endian para separar las zonas



1. Comunicar la zona Verde con la zona Naranja con el protocolo HTTP y

FTP con sus respectivos puertos.

Configurando la zonas



2. Comunicar la zona Internet con la zona DMZ.
3. Verificar en el tráfico Inter - Zona, la creación de las reglas.
4. Probar desde un navegador Web, las siguientes directivas:

El ingreso del servicio HTTP desde la LAN hacia la zona DMZ. El ingreso
del servicio HTTP desde la LAN hacia la WAN.
El ingreso del servicio HTTP desde la zona DMZ hacia la WAN. El ingreso
del servicio HTTP desde la WAN hacia la zona DMZ. El ingreso del
servicio FTP desde la LAN hacia la WAN.
El ingreso del servicio FTP desde la WAN hacia la zona DMZ.

## 2.5 TEMATICA 5

## 3 REFERENCIAS

[1] G. Obregón-Pulido, B. Castillo-Toledo and A. Loukianov, *"A globally convergent estimator for n frequencies"*, IEEE Trans. On Aut. Control. Vol. 47. No 5. pp 857-863. May 2002.
[2] H. Khalil, *"Nonlinear Systems"*, 2nd. ed., Prentice Hall, NJ, pp. 50-56, 1996.
[3] Francis. B. A. and W. M. Wonham, *"The internal model principle of control theory"*, Automatica. Vol. 12. pp. 457-465. 1976.
[4] E. H. Miller, *"A note on reflector arrays"*, IEEE Trans. Antennas Propagat., Aceptado para su publicación.
[5] *Control Toolbox* (6.0), User´s Guide, The Math Works, 2001, pp. 2-10-2-35.
[6] J. Jones. (2007, Febrero 6). Networks (2nd ed.) [En línea]. Disponible en: http://www.atm.com.