

# Etapa 7 - Implementando Seguridad en GNU/Linux

Alejandro Palacios Arévalo

[apalaciosar@unadvirtual.edu.co](mailto:apalaciosar@unadvirtual.edu.co)

**Resumen:** En el marco del desarrollo de competencias en administración de sistemas GNU/Linux y seguridad perimetral, como estudiantes debemos abordar una actividad grupal compuesta por dos fases. La primera consiste en el estudio individual del material educativo "Linux Essentials" del Linux Professional Institute (LPI), específicamente el tema 102, disponible en LPI Learning Platform. Los estudiantes deben registrar en un documento PDF los ejercicios guiados y exploratorios correspondientes a cada lección.

**Palabras clave:** GNU/Linux, Linux Essentials, Endian Firewall, seguridad perimetral, DMZ, intranet, extranet, redes LAN/WAN, administración de servicios, direccionamiento IP.

## 1. Introducción

Esta actividad tiene como propósito fortalecer las habilidades en administración de sistemas GNU/Linux y configuración de seguridad perimetral. Los estudiantes deben estudiar el tema 102 del curso Linux Essentials del LPI, registrar ejercicios prácticos y, de forma colaborativa, implementar una solución de seguridad utilizando Endian Firewall (EFW). La solución busca proteger servidores ubicados en una DMZ, garantizando la integridad de datos y servicios en redes LAN y WAN.

## 2. Contenidos

### A. Estudio del Tema 102 – Linux Essentials (LPI)

Debemos acceder al material del tema 102 disponible en la plataforma oficial del Linux Professional Institute (LPI), donde se

revisaron conceptos clave relacionados con la administración básica de sistemas Linux. Se realizaron ejercicios guiados y exploratorios correspondientes a cada lección, incluyendo temas como:

- Gestión de procesos.
- Permisos de archivos y directorios.
- Comandos esenciales de administración.
- Conceptos básicos de red.

### B. Implementación de la Solución de Seguridad Perimetral

Como parte del desarrollo se propuso la protección de servidores ubicados en una red interna (LAN/DMZ) mediante la implementación de la distribución Endian Firewall (EFW). Este firewall se configuró para controlar el acceso entre la red interna y la externa (WAN), utilizando las siguientes estrategias:

- Instalación y configuración inicial de Endian Firewall.
- Revisión de servicios activos mediante comandos como `systemctl status`, `start`, `stop`, y `restart`, con evidencia de fecha y hora de ejecución.
- Segmentación de red en tres zonas:
  - LAN: estaciones de trabajo GNU/Linux.
  - DMZ: servidor GNU/Linux con aplicaciones web y bases de datos.
  - WAN: acceso externo simulado.

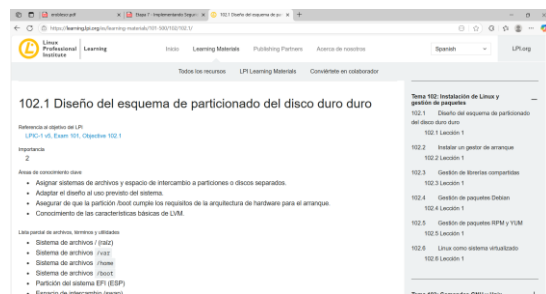
### C. Asignación de Direccionamiento IP y Configuración de Red

Se planificó una topología de red en la que todos los integrantes del grupo utilizaron un esquema de direccionamiento IP unificado para garantizar compatibilidad en las configuraciones. Las direcciones IP asignadas a LAN, DMZ y WAN fueron configuradas manualmente en los dispositivos participantes, y documentadas para replicabilidad y pruebas de conectividad.

## D. Trabajo Colaborativo e Individual

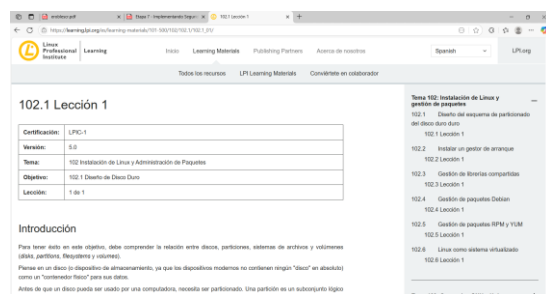
Cada integrante abordó una temática específica propuesta en la guía de actividades, ejecutando y documentando su desarrollo de forma individual. Posteriormente, los aportes fueron compartidos en el entorno de aprendizaje colaborativo para su integración

### 102.1. Diseño del esquema de particionado del disco duro



The screenshot shows a learning management system interface. The main content area displays the course title '102.1 Diseño del esquema de particionado del disco duro' and a search bar. Below the search bar, there are several sections: 'Área de conocimiento', 'Objetivos de aprendizaje', 'Temas', and 'Contenido'. The 'Temas' section lists several topics related to Linux installation and disk partitioning, such as '102.1 Diseño del esquema de particionado del disco duro', '102.2 Instalar un gestor de arranque', '102.3 Creación de bibliotecas compartidas', '102.4 Gestión de paquetes Debian', '102.5 Gestión de paquetes RPM y YUM', and '102.6 Linux como sistema virtualizado'.

### 102.1. Lección 1



The screenshot shows a learning management system interface for the course '102.1 Lección 1'. The main content area displays the course title and a search bar. Below the search bar, there are several sections: 'Certificación', 'Versión', 'Tema', 'Objetivo', and 'Lección'. The 'Objetivo' section lists several topics related to Linux installation and disk partitioning, such as '102.1 Diseño de Disco Duro', '102.2 Instalar un gestor de arranque', '102.3 Creación de bibliotecas compartidas', '102.4 Gestión de paquetes Debian', '102.5 Gestión de paquetes RPM y YUM', and '102.6 Linux como sistema virtualizado'.

## Ejercicios Guiados

### 1. En sistemas Linux, ¿dónde se almacenan los archivos para el gestor de arranque GRUB?

**R:** Los archivos de GRUB normalmente se almacenan en el directorio:

`/boot/grub` o `/boot/grub2` (dependiendo de la distribución Linux).

### 2. ¿Dónde debe terminar la partición de arranque para garantizar que una PC siempre pueda cargar el kernel?

**R:** La partición de arranque debe estar completamente contenida dentro de los primeros 2 TB del disco para garantizar que sea reconocida por el firmware, especialmente en sistemas con BIOS/MBR.

### 3. ¿Dónde se suele montar la partición EFI?

**R:** La partición EFI (ESP) se monta generalmente en: `/boot/efi`

### 4. Al montar manualmente un sistema de archivos, ¿en qué directorio se debe montar normalmente?

**R:** Normalmente se monta en un punto bajo el directorio `/mnt`, por ejemplo:

`/mnt` o `/mnt/nombre_directorio_temporal`

## Ejercicios Exploratorios

### 1. ¿Cuál es la unidad más pequeña dentro de un grupo de volúmenes?

**R:** La unidad más pequeña es el Physical Extent (PE) o Extensión Física.

### 2. ¿Cómo se define el tamaño de un volumen lógico?

**R:** El tamaño de un volumen lógico se define al momento de crearlo, y puede basarse en una cantidad específica de extents o en un tamaño en MB/GB utilizando herramientas como `lvcreate`.

### 3. En un disco formateado con el esquema de partición MBR, ¿cuál es el ID de la partición del sistema EFI?

**R:** El esquema MBR no soporta particiones EFI nativamente. Sin embargo, si se intenta usar EFI en MBR, el ID de tipo sería:

0xEF

#### 4. Además de las particiones de intercambio, ¿cómo puede aumentar rápidamente el espacio de intercambio en un sistema Linux?

R: Se puede aumentar el espacio de intercambio creando un archivo de intercambio (swap file)

#### Pasos Comunes

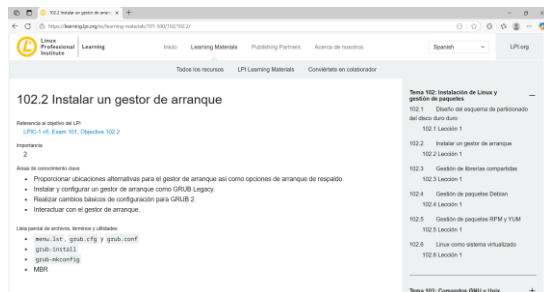
```
sudo fallocate -l 1G /swapfile
```

```
sudo chmod 600 /swapfile
```

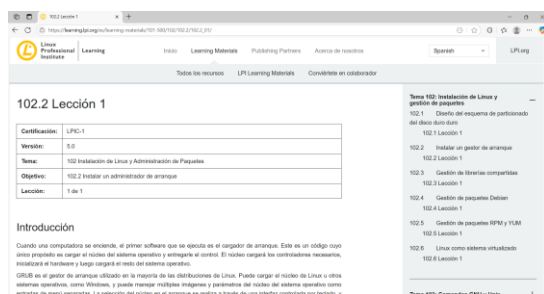
```
sudo mkswap /swapfile
```

```
sudo swapon /swapfile
```

### 102.2 Instalar un gestor de arranque



#### 102.2 Lección 1



#### Ejercicios Guiados

##### 1. ¿Cuál es la ubicación predeterminada para el archivo de configuración GRUB 2?

R: /boot/grub/grub.cfg

##### 2. ¿Cuáles son los pasos necesarios para cambiar la configuración de GRUB 2?

R: Editar el archivo /etc/default/grub o archivos en /etc/grub.d/.

Guardar los cambios.

Ejecutar sudo update-grub para regenerar el archivo grub.cfg.

##### 3. ¿En qué archivo se deben agregar entradas de menú personalizadas de GRUB 2?

R: /etc/grub.d/40\_custom

##### 4. ¿Dónde se almacenan las entradas de menú para GRUB Legacy?

R: /boot/grub/menu.lst

##### 5. Desde un menú GRUB 2 o GRUB Legacy, ¿cómo puede ingresar a la consola de GRUB?

R: Presionando la tecla c en el menú de GRUB.

#### Ejercicios Exploratorios

##### 1. Imagine un usuario que configura GRUB Legacy para arrancar desde la segunda partición del primer disco. Escribe la siguiente entrada de menú personalizada:

title My Linux Distro

root (hd0,2)

kernel /vmlinuz root=/dev/hda1

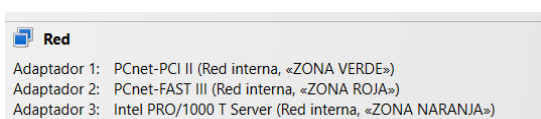
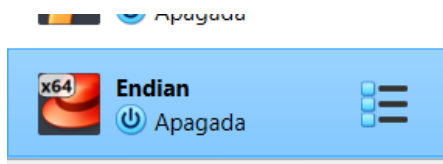
initrd /initrd.img

Sin embargo, el sistema no se iniciará. ¿Qué está mal?

R: El problema está en root (hd0,2), que indica la tercera partición, pero luego el kernel intenta montar /dev/hda1, que es la primera. Debe haber coherencia entre la partición indicada en root y la especificada en root=/dev/hdaX.

## Temática 1: Configuración de la instancia para GNU/Linux Endian en Virtualbox (tarjetas de red) e instalación efectiva del mismo.

Implementación de GNU/Linux Endian con las zonas verde, roja y naranja, así: Zona verde: Red interna (LAN), Zona roja: Acceso a internet (WAN) y Zona naranja: Servidores (DMZ).



## Temática 2: Configuración NAT.

Producto esperado:

1. Configurar la regla de NAT (Network Address Translation / Traducción de Direcciones de Red), demostrando el establecimiento de la comunicación desde la LAN hacia la WAN (Red simulada de Internet).

```
The following parameters will be used to configure the system:
Hostname: efw-0aac5e02ff
Domain: localdomain
RED interface type: STATIC
RED device: eth1
RED IPs (IP/CIDR): 192.168.0.25/24
RED gateway: 255.255.255.0
Primary DNS: 192.168.0.15
Secondary DNS: 0.0.0.0
GREEN devices: eth0
GREEN IPs (IP/CIDR): 192.168.0.15/24
Enable DHCP server on GREEN: on
ORANGE devices: eth2
ORANGE IPs (IP/CIDR): 192.168.0.35/24
```

2. Configurar la regla de NAT, demostrando el establecimiento de la comunicación de la Zona DMZ hacia la Internet. Verificar en el re-envío de puertos / NAT, la creación de las reglas.

```
2025-06-07 07:32:52 [V2020]-I-Restart
Release: Endian Firewall Community release 3.3.2
Product: Community (64 bit)
Hostname: efw-0aac5e02ff

GREEN Zone [DHCP SERVER ENABLED]
Management URL: https://192.168.0.15:10443
IPs: 192.168.0.15/24
Devices: eth0 [UP]

IpLink - main [ACTIVE]
IPs: 192.168.0.25/24 [STATIC]
Device: eth1 [UP]

0 Shell
1 Reboot
2 Change Root Password
3 Change Admin Password
4 Restore Factory Default
5 Network Configuration Wizard
Choice:
```

## 3. Referencias

SourceForge. (2023, October 4).

SourceForge.

<https://sourceforge.net/projects/efw>

/

LPI LPIC-1 Exam 101. (2022). Tema

102: Comandos GNU y Unix.

<https://learning.lpi.org/es/learning-materials/101-500/102/>

Canonical (2023). Guía del Ubuntu

desktop 20.04 LTS. Help Ubuntu.

<https://help.ubuntu.com/20.04/ubuntu-help/index.html>

Debian (2023). El manual del

administrador de Debian 12.5.0.

Debian

<https://www.debian.org/releases/stable/amd64/index.es.html>

Oracle (2020), Manual de usuario

VirtualBox. VirtualBox.

<https://www.virtualbox.org/manual/>

□ Endian (2016), Endian UTM 3.2

Manual referencia. Endian.

<http://docs.endian.com/3.2/utm/index.htm>

1

□ Jay LaCroix. (2020). Mastering

Ubuntu Server : Gain Expertise in

the Art of Deploying, Configuring,

Managing, and Troubleshooting

Ubuntu Server. Packt Publishing.

<https://research-ebSCO->

[com.bibliotecavirtual.unad.edu.co/](https://research-ebSCO-com.bibliotecavirtual.unad.edu.co/)

[linkprocessor/plink?id=b881bf72-20a7-](https://research-ebSCO-linkprocessor/plink?id=b881bf72-20a7-)

[343c-94a8-f12e88b41952](https://research-ebSCO-linkprocessor/plink?id=b881bf72-20a7-343c-94a8-f12e88b41952)