

Walkthrough Tryhackme Free Roadmap

Linux Fundamentals Part I

Presentado por:

Ian E. Acosta Sian
Pentester Jr.

Este es un documento confidencial y contiene información sensible.
No debe ser impreso ni compartido por terceras entidades

14 de Abril de 2025

Indice

1. Conceptos Básicos de Linux Part I	2
1.1. Introducción	2
1.2. ¿Que es Linux?	2
1.3. ¿Por que Linux?	2
1.4. Uso de la terminal	2
1.4.1. Comandos basicos	2
1.4.2. Interactuando con el sistema de archivos	4
1.4.3. Busqueda y filtrado de archivos en Linux	6
1.4.4. Operadores en Linux	8

1. Conceptos Básicos de Linux Part I

1.1. Introducción

Linux es el sistema operativo preferido en el mundo de la ciberseguridad, servidores web, desarrollo y administración de sistemas. Aprender los fundamentos de Linux es un paso esencial para cualquier profesional que aspire a dominar el entorno técnico donde operan la mayoría de las herramientas y servicios modernos.

En esta room, aprenderás los conceptos básicos del sistema operativo Linux, desde la navegación del sistema de archivos y la gestión de permisos hasta la ejecución de comandos en la terminal. No se requiere experiencia previa: este espacio está diseñado para ayudarte a desarrollar una base sólida que te permita avanzar con confianza hacia tareas más avanzadas como el pentesting, la administración de sistemas o el análisis de malware.

1.2. ¿Que es Linux?

Linux es un sistema operativo de código abierto basado creado en 1991 en Unix, utilizado ampliamente en servidores, dispositivos móviles (como Android), supercomputadoras y sistemas embebidos. Es conocido por su estabilidad, seguridad y flexibilidad, y es especialmente popular en el mundo de la programación, la ciberseguridad y la administración de sistemas.

A diferencia de otros sistemas operativos como Windows o macOS, Linux permite a los usuarios ver, modificar y distribuir su código fuente. Esto ha dado lugar a múltiples "distribuciones" (o distros), como Ubuntu, Debian, Kali Linux, CentOS, Fedora, entre muchas otras, cada una adaptada para distintos usos.

En resumen, Linux es el motor silencioso que impulsa una gran parte del mundo digital, desde servidores web hasta redes corporativas y dispositivos del día a día.

1.3. ¿Por que Linux?

- Código abierto.
- Seguro y menos vulnerable a virus.
- Optimizado para hardware antiguo.
- Fiable para servidores y sistemas criticos.

1.4. Uso de la terminal

La terminal es la herramienta principal para interactuar con Linux cuando no hay una interfaz gráfica (GUI).

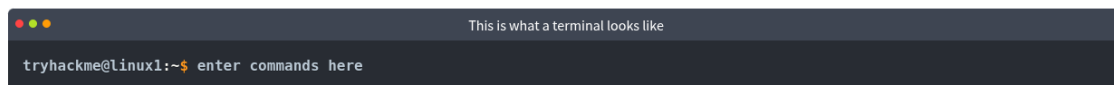
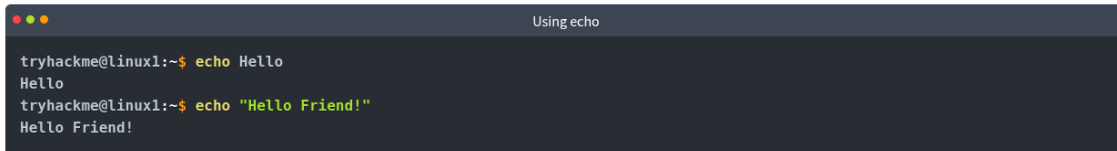


Figura 1: Ejemplo terminal de Linux

1.4.1. Comandos basicos

- echo → muestra texto en la pantalla.
- whoami → muestra usuario actual.

Ejemplo:

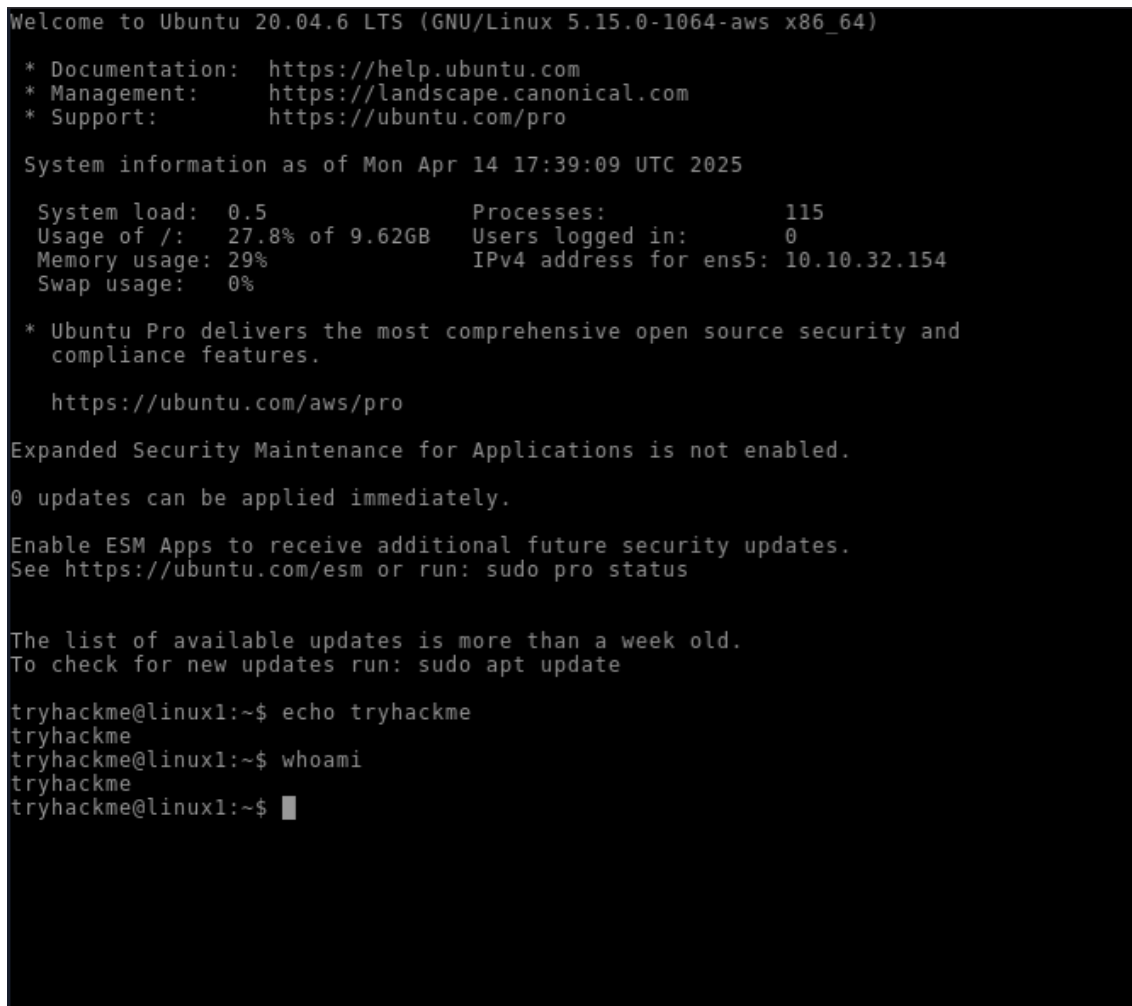


```
tryhackme@linux1:~$ echo Hello
Hello
tryhackme@linux1:~$ echo "Hello Friend!"
Hello Friend!
```

Figura 2: Ejemplo echo y whoami

respondiendo Preguntas

1. Si quisiéramos emitir el texto "TryHackMe", ¿cuál sería el comando?
2. ¿Cuál es el nombre de usuario de quién ha iniciado sesión como en su máquina Linux implementada?



```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1064-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

System information as of Mon Apr 14 17:39:09 UTC 2025

System load:  0.5               Processes:           115
Usage of /:   27.8% of 9.62GB   Users logged in:    0
Memory usage: 29%              IPv4 address for ens5: 10.10.32.154
Swap usage:   0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

tryhackme@linux1:~$ echo tryhackme
tryhackme
tryhackme@linux1:~$ whoami
tryhackme
tryhackme@linux1:~$ █
```

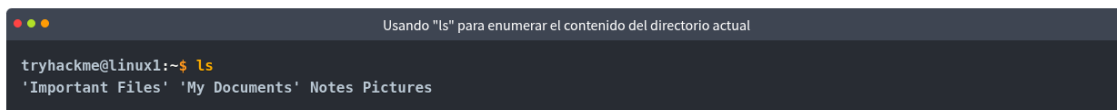
Figura 3: Respuestas a las preguntas

1.4.2. Interactuando con el sistema de archivos

- `ls` → lista los archivos y carpetas de una directorio.
- `cd` → cambia de directorio.
- `cat` → muestr contenido de un archivo.
- `pws` → muestra la ruta completa del directorio actual.

Listado de Archivos en Nuestro Directorio Actual (`ls`)

Antes de que podamos hacer algo como descubrir el contenido de cualquier archivo o carpeta, necesitamos saber qué existe en primer lugar. Esto se puede hacer usando el comando "`ls`" (abreviatura de listado).



```
tryhackme@linux1:~$ ls
'Important Files' 'My Documents' Notes Pictures
```

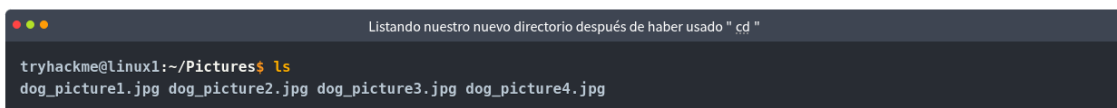
Figura 4: Terminar listando directorios

En la captura anterior podemos ver que se listan los siguiente directorios/carpetas:

- Archivos Importantes
- Mis Documentos
- Notas
- Imágenes

Cambiar Nuestro Directorio Actual (`cd`)

Ahora que sabemos qué carpetas existen, necesitamos usar el "`cd`" comando (abreviatura de change directory) para cambiar a ese directorio. Digamos que si quisiera abrir el directorio "Imágenes", haría "`cd Imágenes`". De nuevo, queremos averiguar el contenido de este directorio "Imágenes" y para hacerlo, usaríamos "`ls`" otra vez:



```
tryhackme@linux1:~/Pictures$ ls
dog_picture1.jpg dog_picture2.jpg dog_picture3.jpg dog_picture4.jpg
```

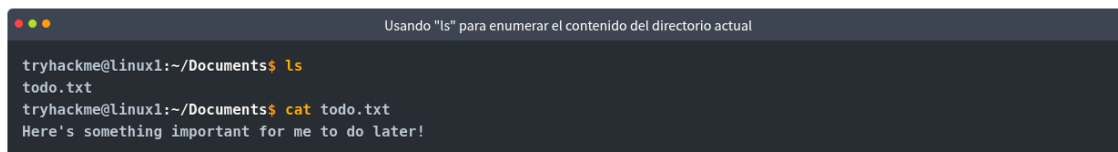
Figura 5: Terminal cambiando de directorio

Salida del Contenido de un Archivo (cat)

Si bien saber sobre la existencia de archivos es genial — no es tan útil a menos que podamos ver el contenido de ellos.

Vamos a venir a discutir algunas de las herramientas disponibles para nosotros que nos permite transferir archivos de una máquina a otra en una habitación posterior. Pero por ahora, vamos a hablar de simplemente ver el contenido de los archivos de texto usando un comando llamado "Cat". "Cat" es la abreviatura de concatenación y es una forma fantástica de generar el contenido de los archivos (¡no solo archivos de texto!).

En la captura de pantalla a continuación, puede ver cómo he combinado el uso de "ls" para enumerar los archivos dentro de un directorio llamado "Documentos":

A terminal window with a dark background and light text. The title bar at the top says "Usando 'ls' para enumerar el contenido del directorio actual". The terminal shows the following commands and output:

```
tryhackme@linux1:~/Documents$ ls
todo.txt
tryhackme@linux1:~/Documents$ cat todo.txt
Here's something important for me to do later!
```

Figura 6: Terminal mostrando contenido del archivo todo.txt

Consejo: Se puede listar o ver archivos sin cambiar de directorio.

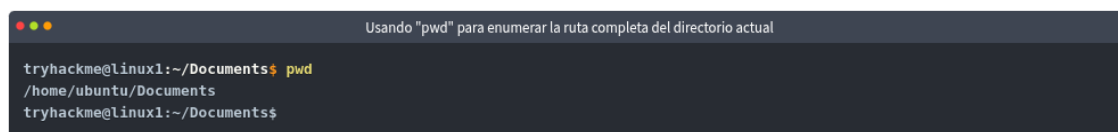
```
ls /home/usuario/Documents
cat /home/usuario/Documents/archivo.txt
```

Descubriendo el Camino completo a nuestro Directorio de Trabajo Actual (pwd)

Te darás cuenta a medida que avanzas navegando Linux máquina, el nombre del directorio en el que está trabajando actualmente aparecerá en su terminal.

Es fácil perder la noción de dónde estamos exactamente en el sistema de archivos, por lo que quiero presentar "pwd". Esto significa print working directory.

Usando la máquina de ejemplo de antes, actualmente estamos en la carpeta "Documentos" —, pero ¿dónde está esto exactamente en el Linux ¿el sistema de archivos de la máquina? Podemos encontrar esto usando este comando "pwd" como en la captura de pantalla a continuación:

A terminal window with a dark background and light text. The title bar at the top says "Usando 'pwd' para enumerar la ruta completa del directorio actual". The terminal shows the following command and output:

```
tryhackme@linux1:~/Documents$ pwd
/home/ubuntu/Documents
tryhackme@linux1:~/Documents$
```

Figura 7: Terminal mostrando camino completo del directorio de trabajo

Respondiendo preguntas

1. En la máquina Linux que implementa, ¿cuántas carpetas hay?
2. ¿Qué directorio contiene un archivo?
3. ¿Cuál es el contenido de este archivo?
4. Utilice el comando cd para navegar a este archivo y averiguar el nuevo directorio de trabajo actual. ¿Cuál es el camino?

```
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ ls folder1
tryhackme@linux1:~$ ls folder2
tryhackme@linux1:~$ ls folder3
tryhackme@linux1:~$ ls folder4
note.txt
tryhackme@linux1:~$ cat folder4/note.txt
Hello World!
tryhackme@linux1:~$ pwd
/home/tryhackme
tryhackme@linux1:~$ cd /home/tryhackme/folder4/
tryhackme@linux1:~/folder4$ pwd
/home/tryhackme/folder4
tryhackme@linux1:~/folder4$ █
```

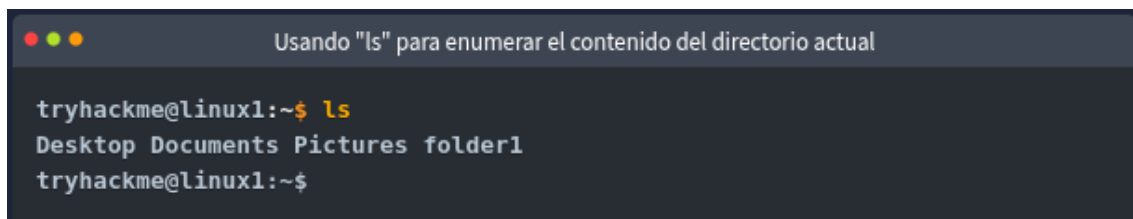
Figura 8: Respuesta de las preguntas anteriores

1.4.3. Búsqueda y filtrado de archivos en Linux

Find

El comando find es fantástico en el sentido de que se puede usar de manera muy simple o bastante compleja dependiendo de qué es lo que desea hacer exactamente. Sin embargo, sigamos primero los fundamentos.

Tome el fragmento a continuación; podemos ver una lista de directorios disponibles para nosotros:



```
tryhackme@linux1:~$ ls
Desktop Documents Pictures folder1
tryhackme@linux1:~$
```

Figura 9: Terminal ejecutando Find

- `find -name nombre_archivo` → busca un archivo por su nombre.
- `find -name *.txt` → busca todos los archivos con extensión .txt.

Ejemplo:

```
find -name password.txt
```

Salida:

```
./folder/password.txt
```

```
find -name *.txt
```

Salida:

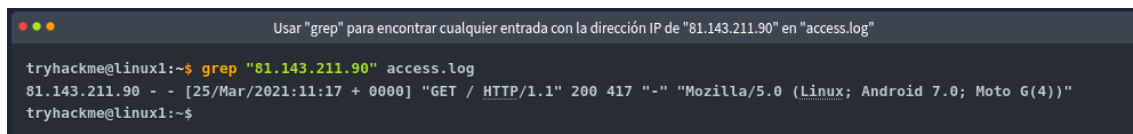
```
./folder/password.txt
```

```
./Documents/archivo.txt
```

Grep

Otra gran utilidad que es excelente para aprender es el uso de grep. El grep el comando nos permite buscar en el contenido de los archivos los valores específicos que estamos buscando.

Tomemos, por ejemplo, el registro de acceso de un servidor web. En este caso, el log de acceso de un servidor web tiene 244 entradas.



```
Usar "grep" para encontrar cualquier entrada con la dirección IP de "81.143.211.90" en "access.log"

tryhackme@linux1:~$ grep "81.143.211.90" access.log
81.143.211.90 - - [25/Mar/2021:11:17 + 0000] "GET / HTTP/1.1" 200 417 "-" "Mozilla/5.0 (Linux; Android 7.0; Moto G(4))"
tryhackme@linux1:~$
```

Figura 10: Terminal filtrando con grep

Filtrar contenido con grep

`grep 'texto' archivo` → busca una palabra o frase dentro del archivo.

`grep 'error' logs.txt` → encuentra todas las líneas que contienen 'error' en logs.txt

Resolviendo las preguntas:

- Utilice grep en "access.log" para encontrar la bandera que tiene un prefijo de "THM". ¿Qué es la bandera? Nota: El archivo "access.log" se encuentra en el directorio "/home/tryhackme/".

```
tryhackme@linux1:~$ ls
access.log  folder1  folder2  folder3  folder4
tryhackme@linux1:~$ cat access.log | grep "THM"
13.127.130.212 - - [04/May/2021:08:35:26 +0000] "GET THM{ACCESS} lang=en HTTP/1.1"
404 360 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, l
ike Gecko) Chrome/77.0.3865.120 Safari/537.36"
tryhackme@linux1:~$
```

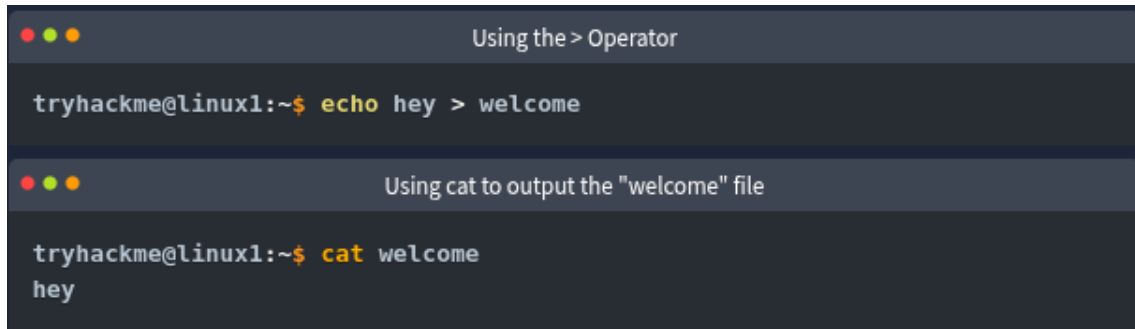
Figura 11: Respuesta a la pregunta

1.4.4. Operadores en Linux

Los operadores en Linux permiten optimizar el uso de comandos, automatizar tareas y gestionar archivos de manera eficiente.

&	Ejecuta un comando en segundo plano.
&&	Ejecuta múltiples comandos en secuencia(el segundo solo si el primero es exitoso)
>	Redirige la salida de un comando a un archivo, y lo sobrescribe si ya existe.
>>	Redirige la salida de un comando a un archivo, agrega sin sobrescribir.

Cuadro 1: Operadores comunes en Linux



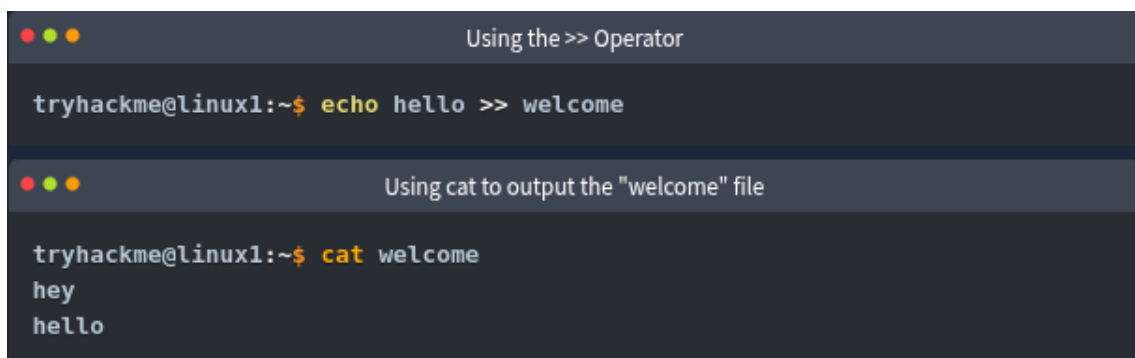
```
Using the > Operator

tryhackme@linux1:~$ echo hey > welcome

Using cat to output the "welcome" file

tryhackme@linux1:~$ cat welcome
hey
```

Figura 12: Ejemplo de >



```
Using the >> Operator

tryhackme@linux1:~$ echo hello >> welcome

Using cat to output the "welcome" file

tryhackme@linux1:~$ cat welcome
hey
hello
```

Figura 13: Ejemplo de >>

Respondiendo las preguntas

- Si quisiéramos ejecutar un comando en segundo plano, ¿qué operador querríamos usar?
R: &
- Si quisiera reemplazar el contenido de un archivo llamado "passwords" con la palabra "password123", ¿cuál sería mi comando?
R: echo password123 >passwords
- Ahora, si quisiera agregar "tryhackme." a este archivo llamado "passwords", pero también mantener "passwords123", ¿cuál sería mi comando?
R: echo tryhackme >>passwords