

A glowing green padlock is positioned on the left side of the image, set against a dark blue background with a complex circuit pattern. The padlock is illuminated with a bright green light, giving it a digital or cybernetic appearance. The circuit lines are white and intricate, with small circles at various points, resembling a microchip or a network map.

SEGURIDAD EN LINUX

PROFA. HAZEM AR

Marzo 2022/ Agosto 2024/Agosto 2025

CONTENIDO

01

Actualizaciones

02

Desactivar
servicios no
utilizados

03

Usuarios y
grupos

04

Limitar acceso
a root y
usuarios

05

Utilizar
Firewall

- Habilitar reglas,
puertos e IP's

06

IPTables

APT

APT - "**Advanced Packaging Tool**" o Herramienta Avanzada de Paquetes), es un potente sistema de gestión de paquetes en el cual están basados los programas gráficos **Añadir/Eliminar Programas** y **Adept**.

APT maneja automáticamente las dependencias y realiza otras operaciones en paquetes del sistema para permitir la instalación de los paquetes seleccionados.

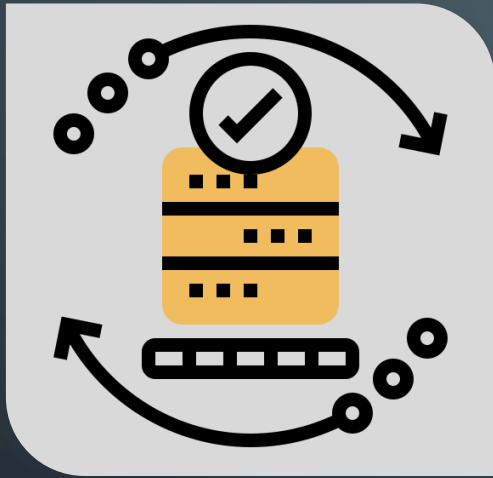
Nota:

Ejecutar **APT** requiere privilegios administrativos ("Usuario "root" y sudo").



ACTUALIZACIONES

Una de las fuentes más significativas de vulnerabilidades de seguridad son los sistemas que están corriendo un software antiguo con brechas de seguridad conocidas.



Por lo que se recomienda ejecutar actualizaciones, lo cual ayuda a evitar intrusiones de seguridad. Puede utilizar los siguientes comandos:

1. Actualizar la lista de paquetes disponibles, **apt-get update**
2. Actualizar el sistema con las actualizaciones de paquetes disponibles, **apt-get upgrade**
3. Obtener una lista de opciones del comando,
sudo apt-get help
4. En caso de tener aplicaciones compiladas manualmente y que requiera eliminarlas, utilice el comando:
make uninstall

ACTIVIDAD. PAQUETES INSTALADOS

Revise el siguiente recurso [Cómo listar los paquetes instalados en cualquier distribución de Linux](#) y posteriormente realice lo siguiente:

1. Muestre todos los paquetes instalados en su distro Linux,
2. Muestre el total de paquetes instalados,
3. Exporte la lista de paquetes al archivo txt con nombre PkgInstallAgo25.txt

Evidencia,

1. Tome screenshot de cada uno los comandos ejecutados
2. Recuerde que en sus screenshot debe mostrarse fecha y hora de ejecución
3. Agregue una descripción detalla de cada comando y resultado mostrado en pantalla.
4. Complemente su trabajo con caratula y referencias



TAREA. PAQUETES ROTOS Y DEPENDENCIAS

- ✓ A continuación, se describen seis preguntas, las cuales deberá de investigar para ejecutar uno a uno de los comandos descritos entre paréntesis,
- ✓ Agregue captura de pantalla de cada ejecución y descripción del cada comando empleado en un archivo PDF
- ✓ Recuerde agregar fuentes de información

1. Describa la diferencia entre Upgrade y Update
2. ¿Qué es un paquete roto en Linux (distro de su preferencia)?
3. ¿Qué son las dependencias incumplidas?
4. ¿Cómo reparar paquetes rotos y dependencias incumplidas?
 - i. Uso de *dpkg* y *apt*
 - ii. ¿Qué significa dependencias insatisfechas?
5. ¿Cómo se eliminan paquetes (*dpkg --remove ...*)?
6. ¿Cómo Limpiar cache?
7. ¿Cuál es la diferencia entre *purge* y *remove*?



MONITOREAR PROCESOS

```
1  [|||||] 13.4% Tasks: 196 total, 1 running
2  [|] 2.0% Load average: 0.53 0.45 0.39
Mem[|||||||||] 1148/3936MB Uptime: 2 days, 06:34:19
Swp[|] 38/4863MB
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
25353	geek	5	-10	655M	552M	540M	S	6.7	12.0	8:17.62	/usr/lib/vmware
25366	geek	15	0	655M	552M	540M	S	6.7	12.0	8:05.04	/usr/lib/vmware
7542	geek	5	-10	494M	421M	405M	S	4.7	9.2	2h38:57	/usr/lib/vmware
7552	geek	15	0	494M	421M	405M	S	4.0	9.2	2h33:25	/usr/lib/vmware
5689	root	15	0	193M	111M	23972	S	2.0	2.4	7:00.51	/usr/bin/X -br
25995	geek	16	0	19440	1392	1020	R	1.3	0.0	0:00.25	htop
21041	geek	15	0	605M	98848	36632	S	0.7	2.1	7:06.94	amarokapp
21049	geek	15	0	605M	98848	36632	S	0.7	2.1	0:49.27	amarokapp
21048	geek	15	0	605M	98848	36632	S	0.7	2.1	0:52.10	amarokapp
25816	geek	15	0	65328	25204	13156	S	0.0	0.5	0:06.08	x11vnc -nap -bg
11799	geek	15	0	140M	16560	11028	S	0.0	0.4	0:27.12	kwin [kdeinit]
25996	geek	15	0	192M	28008	19208	S	0.0	0.6	0:00.49	kate [kdeinit]
19734	geek	15	0	644M	154M	28236	S	0.0	3.4	6:23.13	kaffeine /media
11706	geek	15	0	118M	9016	1688	S	0.0	0.2	1:54.70	/usr/bin/synerg

F1Help F2Setup F3Search F4Invert F5Tree F6SortBy F7Nice F8Nice +F9Kill F10Qu

Recuperado de <https://onx.la/e0eeb>

Los ataques se aprovechan de las aplicaciones inutilizadas. Por lo que es recomendado revisar qué procesos están ejecutándose actualmente en el servidor y para ello se puede emplear **htop**. Este permite mostrar el uso del CPU, muestra de formar gráfica el uso de la memoria y la swap empleada, así como desde cuando se encuentra activo el servidor.

1. Para instalar htop, utilice: **apt-get install htop**
2. Para ejecutar ejecute: **htop**
3. Emplee las opciones de Función que se se describen en la misma herramienta.

DESACTIVAR SERVICIOS NO UTILIZADOS

Los ataques se aprovechan de las aplicaciones inutilizadas. Por lo que es recomendado deshabilitar demonios (servicios) que no sean utilizados.

Para revisar qué procesos están ejecutándose actualmente en el servidor, se puede utilizar **htop**:

- Para instalar htop, utilice: **apt-get install htop**
- Para ejecutar ejecute: **htop**

Revise Servicios en Linux



USUARIOS & GRUPOS

- Para gestionar los **usuarios** y grupos en modo grafico, se debe instalar
`sudo apt-get install gnome-system-tools`
- Para crear un grupo, seleccione “Gestionar grupos” y agregue un nuevo grupo, agregue dos usuarios al grupo creado.

ACTIVIDAD 1

Investigue en su cuaderno ¿Qué es, para que sirve y cual es la diferencia entre?

- | | |
|---------|------------|
| 1. Su | 3. sudoers |
| 2. Sudo | 4. visudo |

Recuperado de <http://www.ubuntu-guia.com/2009/09/gestion-de-usuarios-y-grupos-en-ubuntu.html>

LIMITAR ACCESO A ROOT Y USUARIOS

En general, los usuarios y aplicaciones que no tienen acceso al servidor, ya sea en virtud de las reglas de acceso limitado o por capacidades limitados de ingreso en su sistema, no pueden hacer daño al sistema. Aun que pueden comprometer un sistema y engañarlo para que piense que un usuario tiene derechos de acceso mayores de los que realmente tiene.

- Deshabilitar las cuentas de usuario no utilizadas,

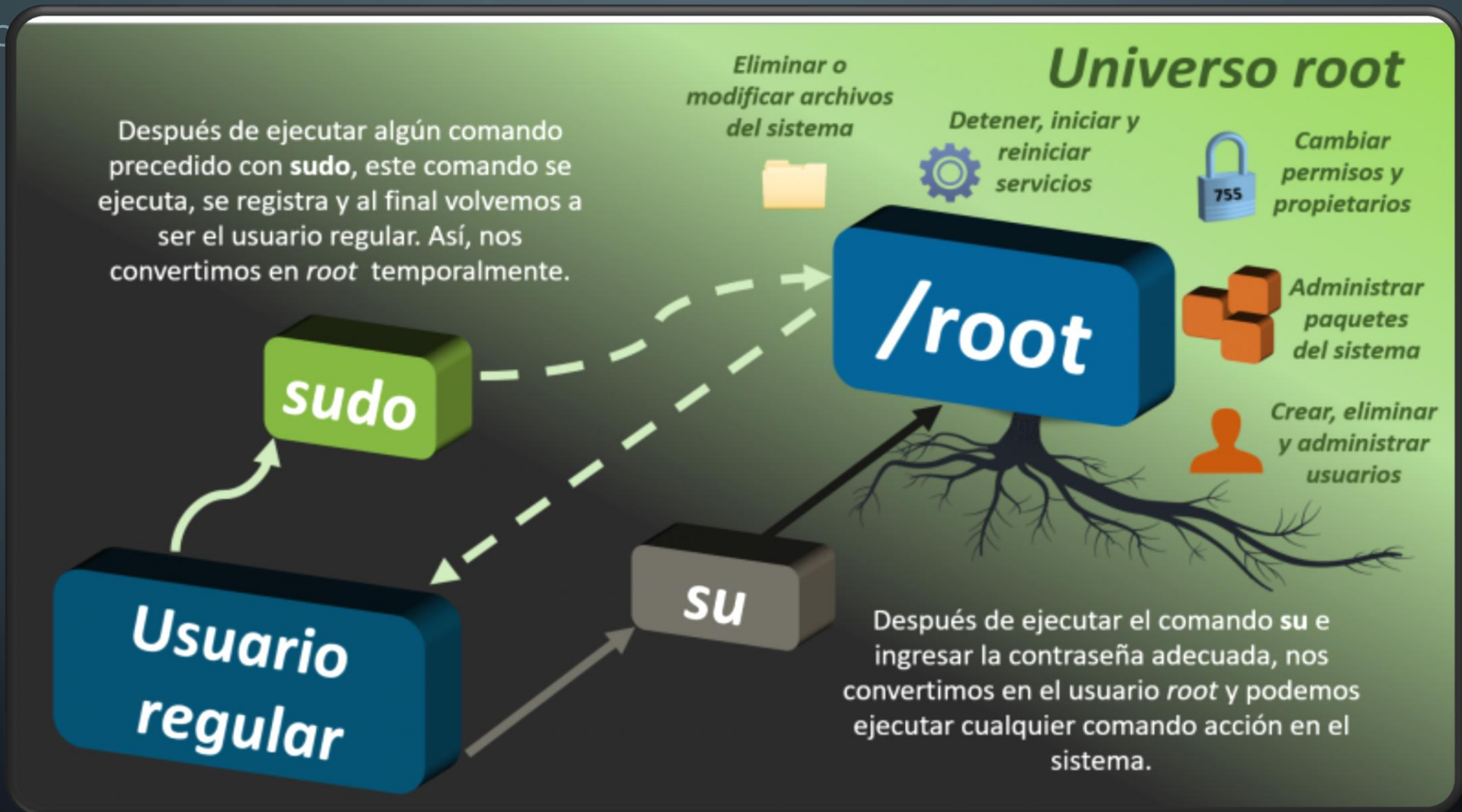
usermod --L NOMBRE-USUARIO

- En caso de que el usuario necesite acceder nuevamente,

usermod --U

- Eliminar las cuentas completamente, con el comando:

userdel



De la teoría a la práctica: sudo, sudoers y visudo [On line] BlueHosting. Recuperado de <https://docs.bluehosting.cl/tutoriales/servidores/de-la-teoria-a-la-practica-sudo-sudoers-y-visudo.html>

UTILIZAR FIREWALL

Un firewall puede ser un componente de hardware o software cuya función es gestionar y administrar todo el tráfico de red, entrante y saliente, que hay entre dos o más redes. Dentro de las principales ventajas que encontramos al usar un firewall tenemos:

1. Proteger la red.
2. Mantener la integridad de la información almacenada en el equipo.
3. Evitar ataques de denegación del servicio.
4. Preservar la privacidad propia y de la organización.
5. Evitar intrusiones de usuarios no autorizados al sistema.



TIPOS DE REGLAS EN FIREWALL

Los firewalls son filtros de tráfico que pueden utilizarse para limitar y restringir el tráfico entrante en el servidor. El objetivo es prevenir que llegue tráfico (o restringirlo adecuadamente) desde ciertas direcciones IP o sobre ciertos puertos donde exista tráfico malicioso o no deseado.



Cuando gestionamos un firewall podemos administrar diversos tipos de reglas por ejemplo, algunas de estas son:


- ✓ Controlar el número de conexiones.
- ✓ Registrar los eventos de entrada y salida de conexiones.
- ✓ Administrar y gestionar los accesos de los usuarios.
- ✓ Controlar qué aplicaciones y programas pueden acceder a Internet.
- ✓ Detección de puertos.

Cuando gestionamos un firewall podemos administrar diversos tipos de reglas para el mismo, algunas de estas son:

TIPOS DE REGLAS EN FIREWALL

- ✓ Controlar el número de conexiones.
- ✓ Registrar los eventos de entrada y salida de conexiones.
- ✓ Administrar y gestionar los accesos de los usuarios.
- ✓ Controlar qué aplicaciones y programas pueden acceder a Internet.
- ✓ Detección de puertos.

UFW es una herramienta que nos permite administrar nuestro Firewall mediante el uso de la línea de comandos con la cual gestionamos la configuración de Firewall. Además permite trabajar con diferentes políticas de seguridad en función de los parámetros de seguridad. Tener un usuario como **root** o **sudo** es vital para poder ejecutar todas estas tareas administrativas.



UFW es una herramienta de configuración de Firewall para iptables que se incluye con Fundamentos de UFW: Reglas y Comandos de Firewall más Comunes en Ubuntu de forma predeterminada.

HAR - SO - 2025B

UFW

UFW es una herramienta que nos permite administrar nuestro Firewall mediante el uso de la línea de comandos con la cual gestionamos la configuración de Firewall. Además permite trabajar con diferentes políticas de seguridad en función de los parámetros de seguridad. Tener un usuario como **root** o **sudo** es vital para poder ejecutar todas estas tareas administrativas.

UFW es una herramienta de configuración de Firewall

para iptables que se incluye con Fundamentos de

UFW: Reglas y Comandos de Firewall más Comunes

en Ubuntu de forma predeterminada.



UFW

- UFW suele no estar instalado de forma predeterminada en Ubuntu, pero podemos instalarlo con ***sudo apt install ufw***
- Posteriormente podemos verificar el estado del mismo con, ***sudo ufw status verbose***
- Verificamos el estado de UFW, ***sudo ufw status***
- Generalmente se encuentra inactivo por lo que Podemos ver que su estado ha cambiado y ahora se encuentra activo desde el arranque del sistema, ***sudo ufw enable***



COMANDOS UFW

Entre los comandos que utiliza UFW, se encuentran:

- Para verificar el estado de su firewall utilice: **sudo ufw status**
- Para bloquear una dirección ip: **sudo ufw deny from direcciónIP/subred**
- Para mostrar las reglas activas: **ufw status verbose**
- Para ver los perfiles para aplicaciones en UFW: **sudo ufw app list**



HABILITAR REGLAS , PUERTOS E IP'S CON UFW

- Configurar políticas predeterminadas,

sudo ufw default deny incoming

sudo ufw default allow outgoing

- Habilitar conexiones SSH

sudo ufw allow ssh o sudo ufw allow 22*

- Habilitar otras conexiones

sudo ufw allow http o sudo ufw allow 80

- Direcciones IP específicas

sudo ufw allow from 203.0.113.4

sudo ufw allow from 203.0.113.4 to any port 22

* Crea reglas en el puerto 22 y UFW registra el significado del puerto allow ssh porque está enumerado como servicio en el archivo `/etc/services`

<https://www.digitalocean.com/community/tutorials/como-configurar-un-firewall-con-ufw-en-ubuntu-18-04-es>

✓ Revise el siguiente documento



Como configurar Firewall con UFW en Ubuntu Linux.pdf



Cómo configurar Firewall con UFW en Ubuntu Linux

Escrito por [Solvetic Sistemas](#) sep 20 2019 11:40 [ubuntu](#)

Cuando de [incrementar la seguridad](#) en los equipos cliente de una organización, o propios, se trata, existen numerosas herramientas y buenas prácticas que podemos implementar que ayudan a conservar los estándares de seguridad adecuados para tal fin. Aunque recurrimos a herramientas externas muchas veces no podemos dejar a un lado las utilidades que vienen incluidas dentro del propio Sistema Operativo las cuales han sido desarrolladas para ejecutar tareas específicas de una [forma correcta](#) y totalmente compatible con el Sistema Operativo en uso.

IPTABLES

Linux dispone de un firewall llamado IPtables. Es un firewall incluido en el kernel de Linux desde la versión 2.4 ; esta basado en reglas las cuales el mismo firewall debe ejecutar. Estas IPtables también se encuentran en los firmwares basados en Linux y en los dispositivos Android.

1. Actualizar paquetes y versiones; `sudo apt-get update`
2. Instalar iptables, `sudo apt-get install iptables`
3. Revisar las reglas que se tienen; `sudo iptables -nL`
4. Revisar el estado de iptables; `sudo iptables -L -v`

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination
```

4.1 Como se muestra, las tres cadenas contienen **ACCEPT** en forma predeterminada. Actualmente no hay reglas para ninguna de las cadenas.

IPTABLES

5. Limpiar regla, *iptables -F*

6. Política en DROP, *iptables -P INPUT DROP*

7. Agregar Excepciones, *IPlocal/24 -j ACCEPT*, permite realizar ping a nuestro equipo

8. Trafico por un solo puerto, *iptables -A INPUT -p tcp -dport PUERTO -j ACCEPT*

8. 1 verificar que se agregado la regla en IPTABLES, *iptables -nL*

9. Para permitir el trafico bloqueado con DROP, puede utilizar,

iptables -P INPUT ACCEPT

9. 1 Verificar que ha cambiado DROP por ACCEPT,

ACTIVIDAD

1. Muestre las reglas de IPTABLES en su equipo (antes de iniciar la actividad),
2. Cree dos reglas diferentes en IPTABLES, de las cuales:
<https://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/>
 - 1.1 Describa que hace cada una de estas reglas,
 - 1.2 Acompañe con la captura de los comandos utilizados para crear las reglas,
3. Muestre nuevamente las reglas en IPTABLES, donde identifique las nuevas reglas creadas anteriormente
4. Elimine una de las reglas creadas
5. Muestre las reglas en IPTABLES
6. Describa que acciones realiza ACCEPT, DROP & RETURN, en IPTABLES



REFERENCIAS

1. Cómo configurar un firewall con UFW en Ubuntu 18.04 [On Line] DigitalOcean.
Recuperado de <https://www.digitalocean.com/community/tutorials/como-configurar-un-firewall-con-ufw-en-ubuntu-18-04-es>
2. De la teoría a la práctica: sudo, sudoers y visudo [On line] BlueHosting.
Recuperado de <https://docs.bluehosting.cl/tutoriales/servidores/de-la-teoria-a-la-practica-sudo-sudoers-y-visudo.html>
3. Cómo configurar UFW en Ubuntu 18 o Debian[On line]- Klvst3r -.Recuperado de <https://klvst3r.medium.com/c%C3%B3mo-configurar-ufw-en-ubuntu-18-o-debian-67dab8c72170>