

UNIVERSIDAD CENTRAL DEL ECUADOR
Facultad de Ingeniería y Ciencias Aplicadas



Criptografía y seguridad de la información

Tema:

Laboratorio - Configuración entorno Hacking ético

Integrantes:

Arias Basantes Joffre David

Fiallos Checa Fátima Carolina

Flores Armijo Byron Rigoberto

Hurtado Tinoco Kevin David

Lechon Lechon Cristian Alexander

Pila Aguaisa Jordi Fernando

Pujota Pineda Angelo Fabricio

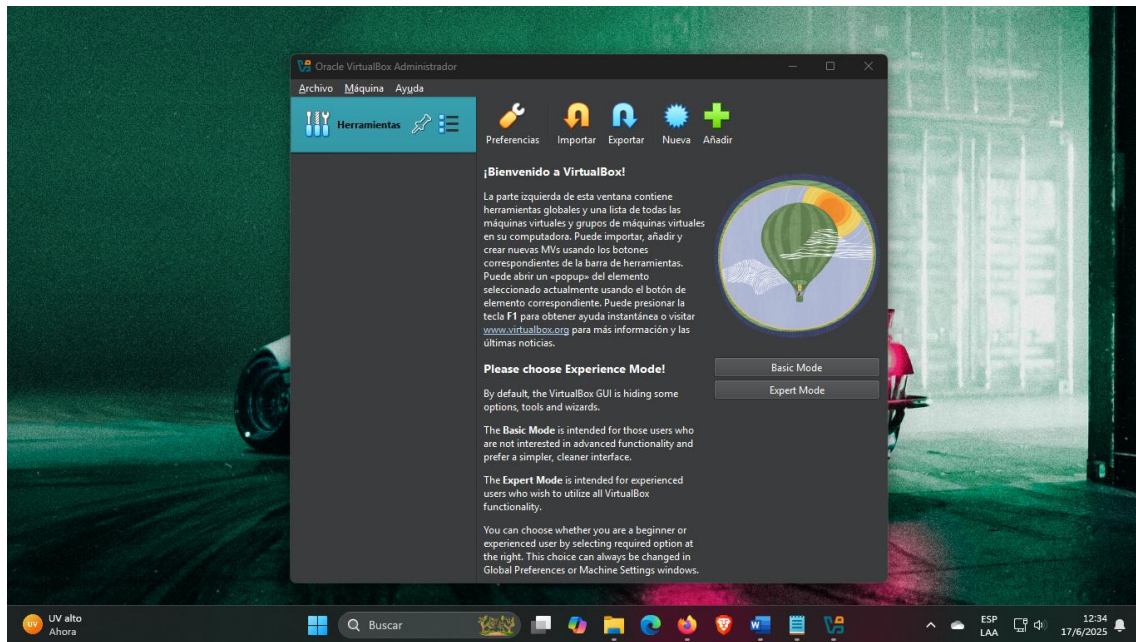
Tipán López Edgar Vinicio

20/06/2025

1. Instale un *Hipervisor* o *WSL* y realice el proceso de montaje y configuración de una máquina virtual *Host* con *Sistema Operativo Windows o Linux (Server)*.

Hipervisor: VirtualBox

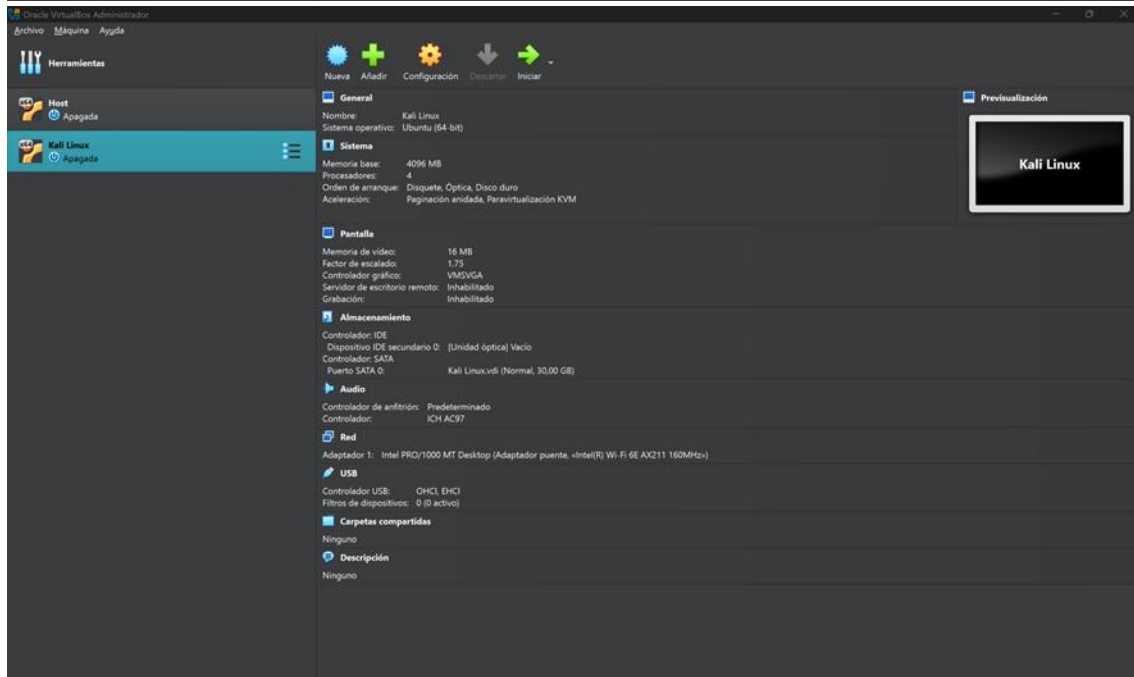
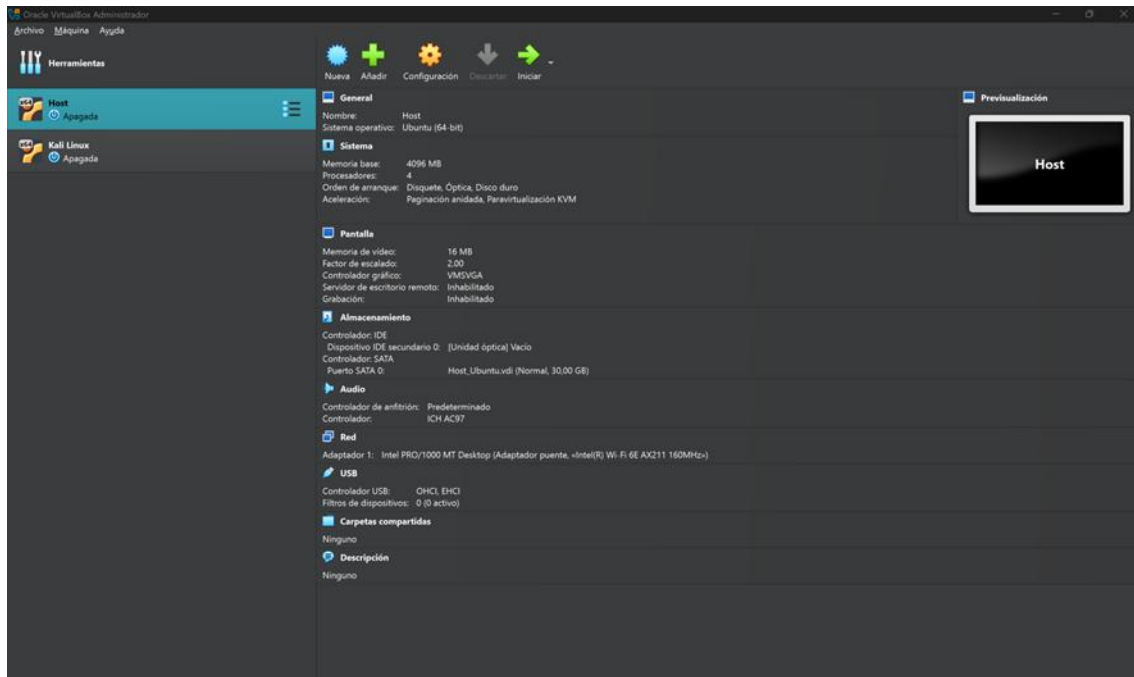
VirtualBox es un hipervisor desarrollado por Oracle Corporation. Es una solución de virtualización gratuita y de código abierto que permite a los usuarios ejecutar múltiples sistemas operativos en un único hardware físico de manera simultánea. Esto se logra al crear máquinas virtuales (VMs), cada una de las cuales puede ejecutarse de forma independiente, como si se tratara de un equipo físico separado.



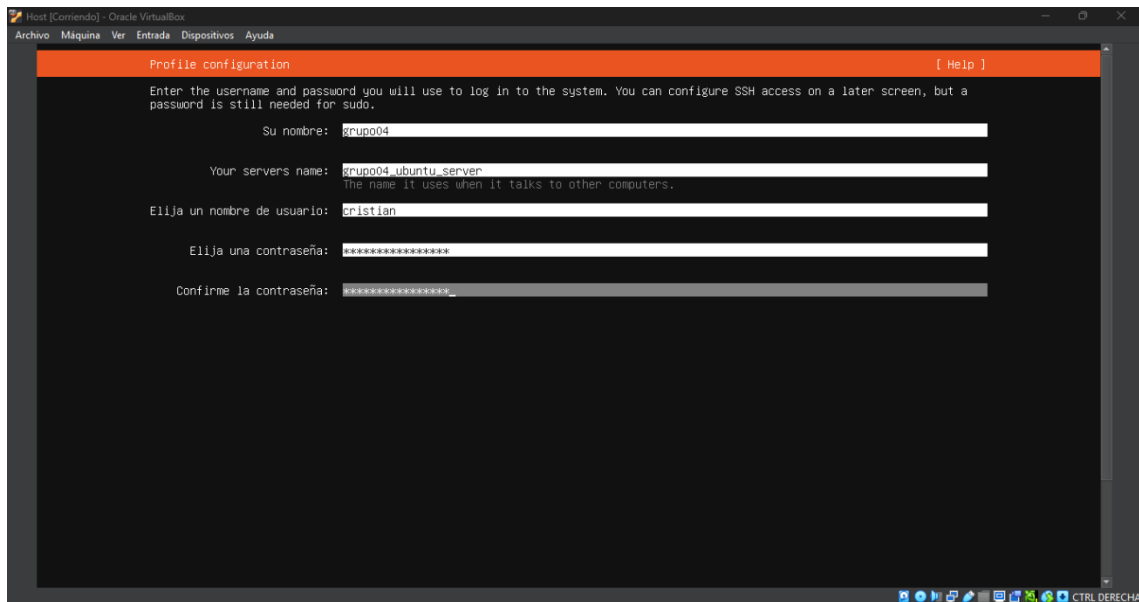
Distro: Ubuntu Server 24.04.2 LTS y Kali Linux

Ubuntu Server es una distribución de Linux enfocada en servidores, ideal para alojar servicios web, bases de datos y entornos en la nube. Destaca por su estabilidad, soporte a largo plazo y facilidad de integración con herramientas de automatización y contenedores como Docker o Kubernetes.

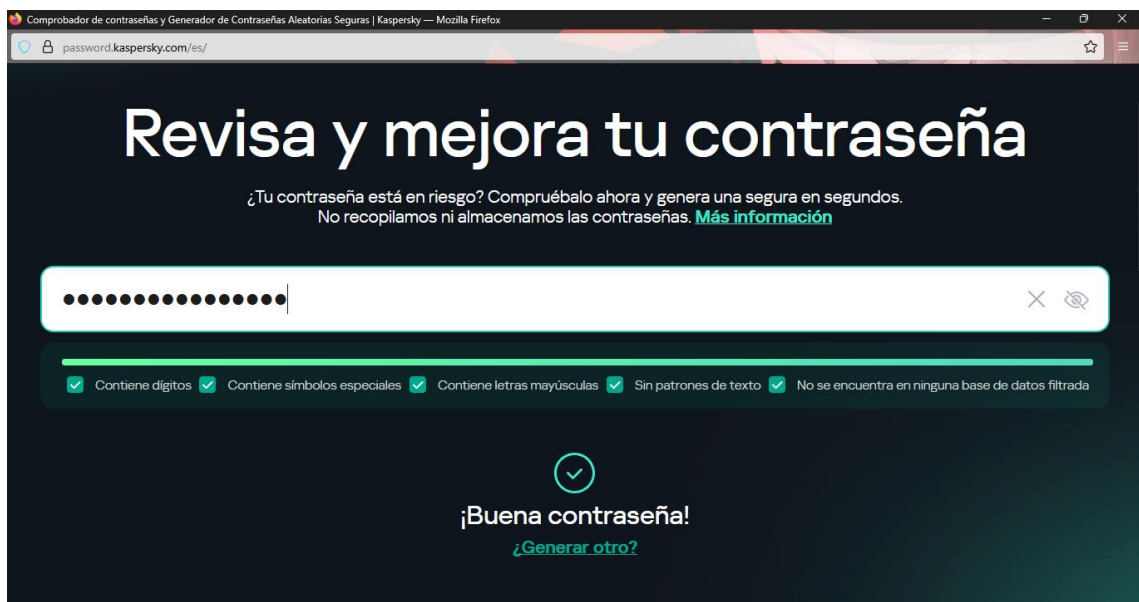
Por otro lado, Kali Linux está diseñada para hackers éticos y profesionales de ciberseguridad que necesitan herramientas avanzadas para pruebas de penetración, análisis forense y auditorías de red.



2. Proteja con una *contraseña segura* al usuario *Administrador* del Sistema Operativo.

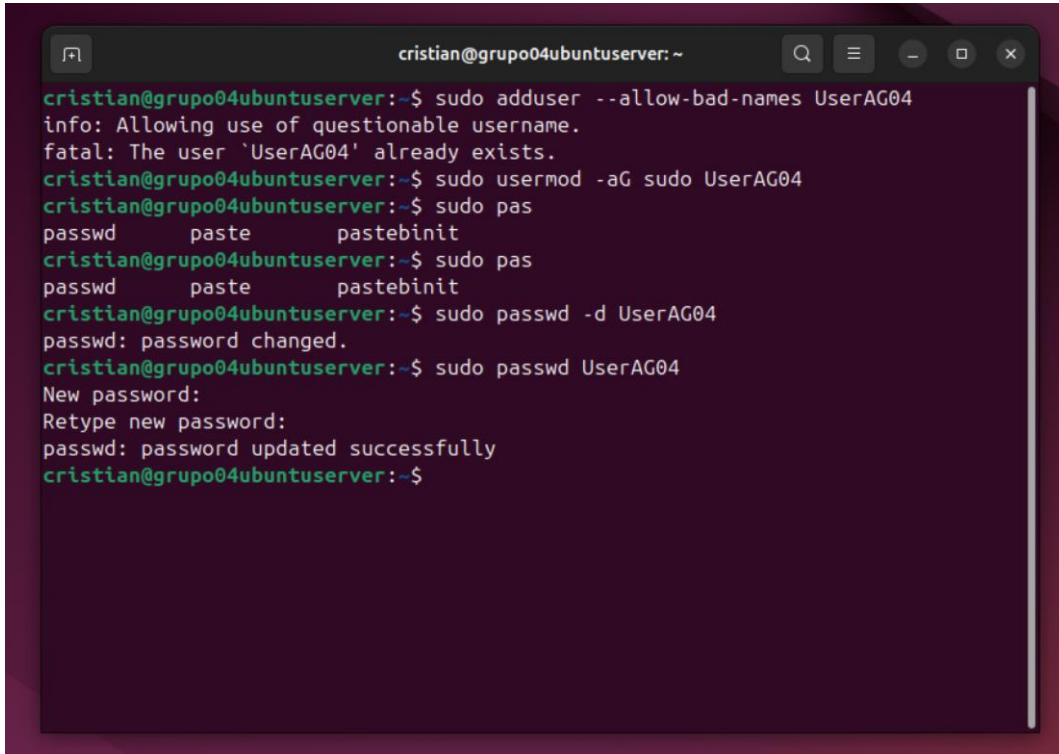


Verificación de la contraseña del usuario administrador con la página password checker de Kaspersky.



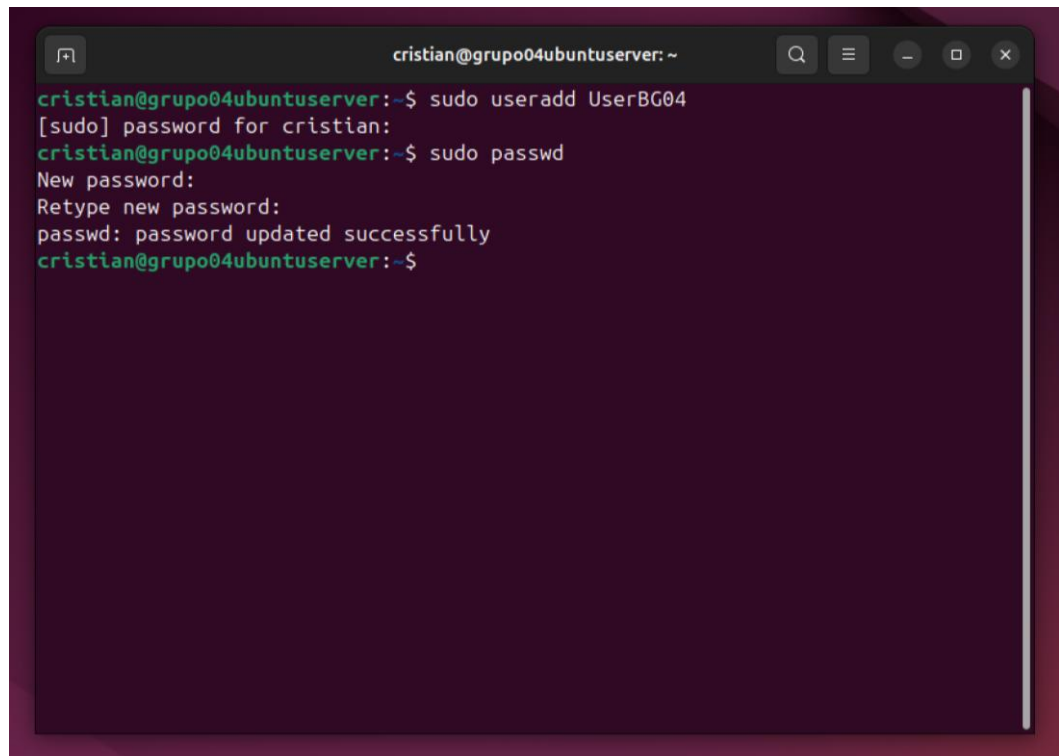
3. *Cree dos usuarios en el Sistema Operativo desde la consola de comandos. **UserAGxx** con todos los privilegios y **UserBGxx** con privilegios mínimos. xx corresponde al número de grupo.*

Creación del usuario UserAG04 y otorgando todos los privilegios.

A terminal window titled 'cristian@grupo04ubuntuserver: ~' showing the process of creating a user with full privileges. The user 'UserAG04' already exists, so 'adduser' fails. Instead, 'usermod' is used to add the user to the 'sudo' group. Then, 'passwd' is used to set a password for the user, and 'sudo passwd' is used to update the password successfully.

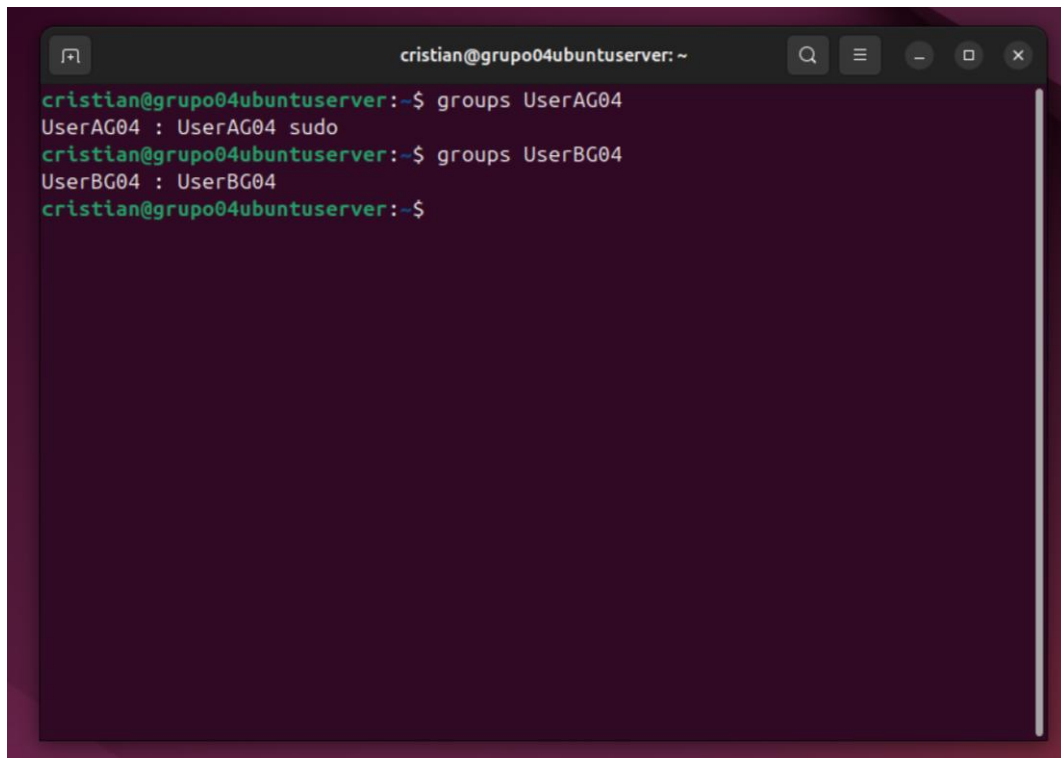
```
cristian@grupo04ubuntuserver:~$ sudo adduser --allow-bad-names UserAG04
info: Allowing use of questionable username.
fatal: The user 'UserAG04' already exists.
cristian@grupo04ubuntuserver:~$ sudo usermod -aG sudo UserAG04
cristian@grupo04ubuntuserver:~$ sudo pas
passwd      paste      pastebinit
cristian@grupo04ubuntuserver:~$ sudo pas
passwd      paste      pastebinit
cristian@grupo04ubuntuserver:~$ sudo passwd -d UserAG04
passwd: password changed.
cristian@grupo04ubuntuserver:~$ sudo passwd UserAG04
New password:
Retype new password:
passwd: password updated successfully
cristian@grupo04ubuntuserver:~$
```

Creación del usuario UserBG04 con privilegios mínimos.

A terminal window titled 'cristian@grupo04ubuntuserver: ~' showing the process of creating a user with minimal privileges. The user 'UserBG04' is created using 'useradd'. Then, 'passwd' is used to set a password for the user, and 'sudo passwd' is used to update the password successfully.

```
cristian@grupo04ubuntuserver:~$ sudo useradd UserBG04
[sudo] password for cristian:
cristian@grupo04ubuntuserver:~$ sudo passwd
New password:
Retype new password:
passwd: password updated successfully
cristian@grupo04ubuntuserver:~$
```

Viendo los privilegios de los usuarios.

A terminal window titled 'cristian@grupo04ubuntuserver: ~' with standard window controls. The terminal shows the following commands and output:

```
cristian@grupo04ubuntuserver:~$ groups UserAG04
UserAG04 : UserAG04 sudo
cristian@grupo04ubuntuserver:~$ groups UserBG04
UserBG04 : UserBG04
cristian@grupo04ubuntuserver:~$
```

4. En *otro Hipervisor*, instale **Kali Linux** (<https://www.kali.org/>).



5. Compruebe que ambos equipos se encuentren en la misma red.

IP Kali Linux


```
cristian@kali: ~
Archivo Acciones Editar Vista Ayuda
(cristian@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.27 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe48:a9b2 prefixlen 64 scopeid 0<link>
    ether 08:00:27:48:a9:b2 txqueuelen 1000 (Ethernet)
    RX packets 405 bytes 34080 (33.2 KiB)
    RX errors 0 dropped 79 overruns 0 frame 0
    TX packets 819 bytes 69978 (68.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 248 bytes 27360 (26.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 248 bytes 27360 (26.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(cristian@kali)-[~]
$
```

IP Ubuntu Server

```
cristian@grupo04ubuntuserver: ~
cristian@grupo04ubuntuserver:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:77:2e:62 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.31/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 80748sec preferred_lft 80748sec
    inet6 fe80::a00:27ff:fe77:2e62/64 scope link
        valid_lft forever preferred_lft forever
cristian@grupo04ubuntuserver:~$
```

Probaremos haciendo ping

```
cristian@grupo04ubuntuserver: ~  
cristian@grupo04ubuntuserver:~$ ping 192.168.1.27  
PING 192.168.1.27 (192.168.1.27) 56(84) bytes of data.  
64 bytes from 192.168.1.27: icmp_seq=1 ttl=64 time=0.765 ms  
64 bytes from 192.168.1.27: icmp_seq=2 ttl=64 time=1.49 ms  
64 bytes from 192.168.1.27: icmp_seq=3 ttl=64 time=1.04 ms  
64 bytes from 192.168.1.27: icmp_seq=4 ttl=64 time=0.373 ms  
64 bytes from 192.168.1.27: icmp_seq=5 ttl=64 time=1.10 ms  
64 bytes from 192.168.1.27: icmp_seq=6 ttl=64 time=0.355 ms  
64 bytes from 192.168.1.27: icmp_seq=7 ttl=64 time=0.998 ms  
64 bytes from 192.168.1.27: icmp_seq=8 ttl=64 time=0.453 ms  
^C  
--- 192.168.1.27 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7118ms  
rtt min/avg/max/mdev = 0.355/0.821/1.494/0.381 ms  
cristian@grupo04ubuntuserver:~$
```

```
cristian@kali: ~  
Archivo Acciones Editar Vista Ayuda  
(cristian@kali)-[~]  
$ ping 192.168.1.31  
PING 192.168.1.31 (192.168.1.31) 56(84) bytes of data.  
64 bytes from 192.168.1.31: icmp_seq=1 ttl=64 time=0.779 ms  
64 bytes from 192.168.1.31: icmp_seq=2 ttl=64 time=1.17 ms  
64 bytes from 192.168.1.31: icmp_seq=3 ttl=64 time=1.04 ms  
64 bytes from 192.168.1.31: icmp_seq=4 ttl=64 time=0.875 ms  
64 bytes from 192.168.1.31: icmp_seq=5 ttl=64 time=2.46 ms  
64 bytes from 192.168.1.31: icmp_seq=6 ttl=64 time=1.24 ms  
64 bytes from 192.168.1.31: icmp_seq=7 ttl=64 time=0.440 ms  
^C  
--- 192.168.1.31 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6152ms  
rtt min/avg/max/mdev = 0.440/1.143/2.457/0.591 ms  
(cristian@kali)-[~]  
$
```

VirtualBox Bridge (modo de red "Bridge" o puente) es una configuración de red en **Oracle VirtualBox** que permite que las máquinas virtuales (VM) se conecten directamente a la red física a la que está conectado el equipo anfitrión. En este modo, la máquina virtual actúa como si estuviera directamente conectada a la red local (LAN), obteniendo su propia dirección IP y acceso completo a los recursos de la red, como impresoras, servidores o dispositivos conectados.

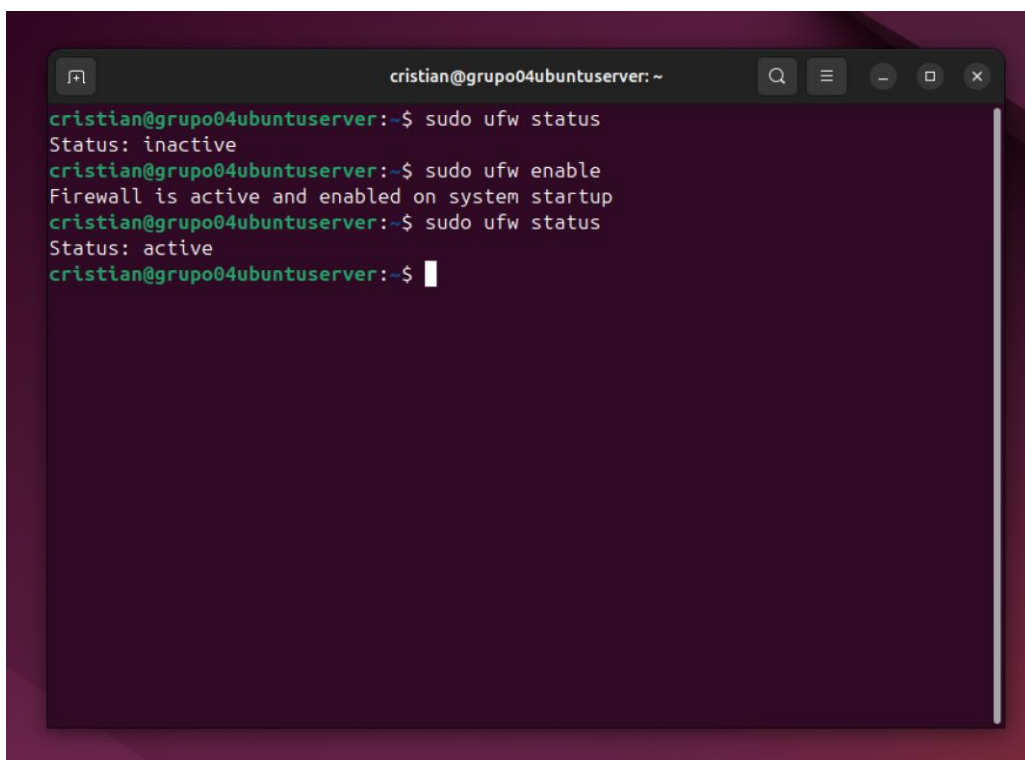
6. En la máquina **Host instale, active y/o configure 3** de los siguientes dispositivos de seguridad informática:

Dispositivos Elegidos:

- **Firewall: UFW**

UFW (Uncomplicated Firewall) es una herramienta simple para gestionar reglas de iptables en Linux, como Ubuntu. Controla el tráfico de red, permitiendo o bloqueando conexiones para proteger contra accesos no autorizados y malware.

Activar el firewall y verificar que está activo:

A terminal window with a dark purple background. The title bar shows 'cristian@grupo04ubuntuserver: ~'. The terminal text is as follows:

```
cristian@grupo04ubuntuserver:~$ sudo ufw status
Status: inactive
cristian@grupo04ubuntuserver:~$ sudo ufw enable
Firewall is active and enabled on system startup
cristian@grupo04ubuntuserver:~$ sudo ufw status
Status: active
cristian@grupo04ubuntuserver:~$
```

- **Antivirus: ClamAV (Clam AntiVirus)**

ClamAV es un antivirus de código abierto diseñado especialmente para detectar malware, virus, troyanos y otros tipos de software malicioso en sistemas Linux, Windows y macOS.

Es ampliamente utilizado en servidores de correo, gateways de red, y sistemas donde se requiere escanear archivos de manera automatizada o bajo demanda.

Instalación:

```
cristian@grupo04ubuntuserver:~
cristian@grupo04ubuntuserver:~$ sudo apt install clamav clamav-daemon -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
clamav ya está en su versión más reciente (1.4.3-1).
Se instalarán los siguientes paquetes adicionales:
  clamav-base clamav-freshclam clamdscan libclamav11t64
Paquetes sugeridos:
  libclamunrar clamav-docs daemon libclamunrar11
Se instalarán los siguientes paquetes NUEVOS:
  clamav-base clamav-daemon clamav-freshclam clamdscan libclamav11t64
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 2 no actualizados.
Se necesita descargar 7.170 kB de archivos.
Se utilizarán 30,0 MB de espacio de disco adicional después de esta operación.
Des:1 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-base a
ll 1.0.8+dfsg-0ubuntu0.24.04.1 [93,5 kB]
Des:2 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 libclamav11t6
4 amd64 1.0.8+dfsg-0ubuntu0.24.04.1 [6.714 kB]
Des:3 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-freshc
lam amd64 1.0.8+dfsg-0ubuntu0.24.04.1 [97,6 kB]
Des:4 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamav-daemon
amd64 1.0.8+dfsg-0ubuntu0.24.04.1 [213 kB]
Des:5 http://ec.archive.ubuntu.com/ubuntu noble-updates/main amd64 clamdscan amd
64 1.0.8+dfsg-0ubuntu0.24.04.1 [51,2 kB]
```

```
cristian@grupo04ubuntuserver:~
Saving to: 'eicar.com'

eicar.com          [  <=>          ] 276,62K  270KB/s   in 1,0s

2025-06-19 02:34:59 (270 KB/s) - 'eicar.com' saved [283258]

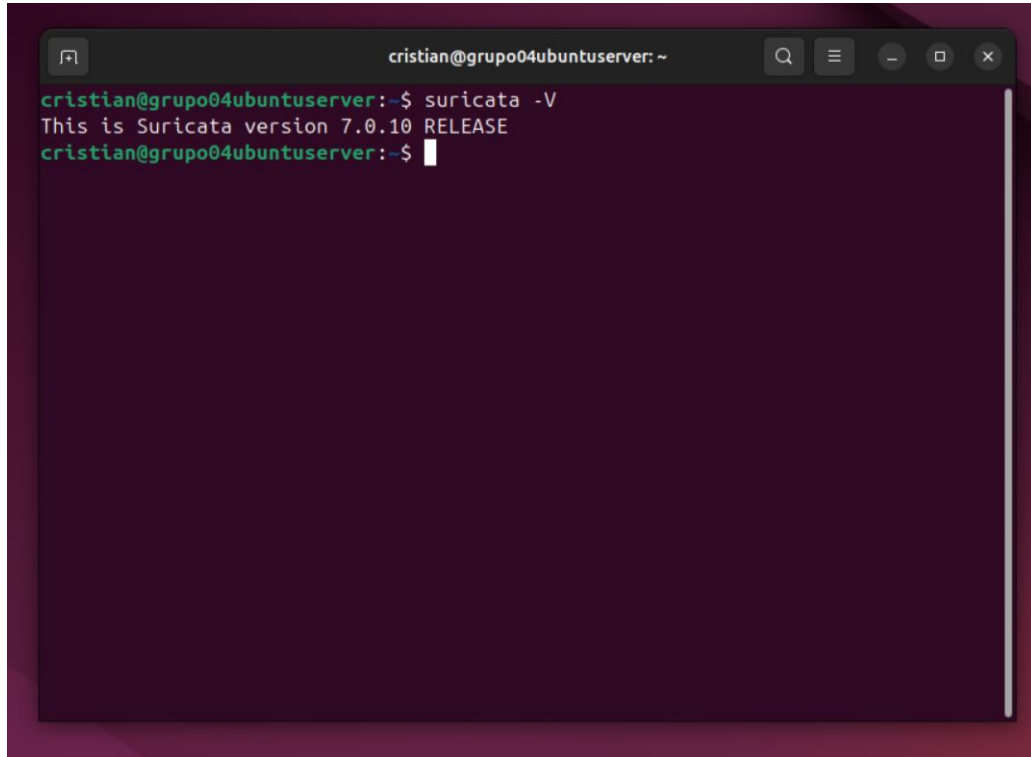
cristian@grupo04ubuntuserver:~$ clamscan eicar.com
Loading:   19s, ETA:   0s [=====>]      8.71M/8.71M sigs
Compiling:  4s, ETA:   0s [=====>]      41/41 tasks

/home/cristian/eicar.com: OK

----- SCAN SUMMARY -----
Known viruses: 8707532
Engine version: 1.0.8
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.51 MB
Data read: 0.27 MB (ratio 1.90:1)
Time: 23.590 sec (0 m 23 s)
Start Date: 2025:06:19 02:35:07
End Date: 2025:06:19 02:35:30
cristian@grupo04ubuntuserver:~$
```

- **IPS: Suricata**

Suricata es una solución de código abierto avanzada para la detección de intrusiones (**IDS**), prevención de intrusiones (**IPS**) y monitoreo de tráfico en red. Desarrollada por la **Open Information Security Foundation (OISF)**, es una herramienta robusta ampliamente utilizada por profesionales de la ciberseguridad para analizar el tráfico de red y detectar actividades sospechosas o maliciosas.

A terminal window with a dark purple background. The title bar at the top reads "cristian@grupo04ubuntuserver: ~". The terminal shows the command "suricata -V" being executed, which outputs "This is Suricata version 7.0.10 RELEASE". The prompt "cristian@grupo04ubuntuserver:~\$" is visible on the line below the output.

```
cristian@grupo04ubuntuserver:~$ suricata -V
This is Suricata version 7.0.10 RELEASE
cristian@grupo04ubuntuserver:~$
```

Bibliografía

- [1] Oracle Corporation, "VirtualBox User Manual," Oracle VM VirtualBox. Accedido el 17 de junio de 2025. [En línea]. Disponible: <https://www.virtualbox.org/manual/>
- [2] "Get ubuntu server | download | ubuntu". Ubuntu. Accedido el 18 de junio de 2025. [En línea]. Disponible: <https://ubuntu.com/download/server>
- [3] "Get kali | kali linux". Kali Linux. Accedido el 17 de junio de 2025. [En línea]. Disponible: <https://www.kali.org/get-kali/#kali-platforms>
- [4] Tech TodAI. *Cómo instalar ubuntu server en virtualbox (paso a paso)*. (15 de marzo de 2025). Accedido el 18 de junio de 2025. [Video en línea]. Disponible: <https://www.youtube.com/watch?v=38BrwWUAqG0>
- [5] solvetic.com. *INSTALAR KALI LINUX en VIRTUALBOX*. (6 de marzo de 2023). Accedido el 17 de junio de 2025. [Video en línea]. Disponible: <https://www.youtube.com/watch?v=rJzX5tQCe6c>
- [6] "2. Quickstart guide — Suricata 8.0.0-dev documentation". Suricata User Guide — Suricata 8.0.0-dev documentation. Accedido el 18 de junio de 2025. [En línea]. Disponible: <https://docs.suricata.io/en/latest/quickstart.html>
- [7] "UFW - community help wiki". Official Ubuntu Documentation. Accedido el 19 de junio de 2025. [En línea]. Disponible: <https://help.ubuntu.com/community/UFW>
- [8] Cisco Talos Intelligence Group, "ClamAV: Open-Source Antivirus Engine," Cisco, 2024. [En línea]. Disponible: <https://www.clamav.net/>. [Accedido: 17 de junio, 2025].