Universidad Central del Ecuador

Facultad de Ingeniería y Ciencias Aplicadas

Computación

Criptografía y Seguridad de la Información

Tema:

Configuración entorno Hacking Ético

Curso:

C8-001

Estudiantes:

- Michael Barrionuevo
- Kevin Celi
- Jhony Ninabanda
- Dylan Lema
- Joan Santamaria

16/Enero/2026

1. Introducción

El presente documento describe el proceso completo de instalación, configuración y validación de un entorno de Hacking Ético, utilizando máquinas virtuales y herramientas de seguridad informática. El laboratorio tiene como finalidad comprender la importancia de la virtualización, la segmentación de red y la implementación de mecanismos básicos de defensa en sistemas informáticos.

2. Objetivo

Objetivo General

Configurar un entorno controlado de Hacking Ético mediante el uso de máquinas virtuales, implementando dispositivos de seguridad informática y documentando todo el proceso realizado.

Objetivos Específicos

Instalar y configurar un sistema operativo Host.

Instalar una máquina virtual con Kali Linux.

Verificar la conectividad entre ambas máquinas.

Implementar dispositivos de seguridad informática.

Documentar el proceso completo de instalación y configuración.

3. Herramientas Utilizadas

- Oracle VM VirtualBox (Hipervisor)
- Ubuntu Server 24.04 (Sistema Operativo Host)
- Kali Linux 2025 (Sistema Operativo de pruebas)
- Cowrie Honeypot
- Firewall UFW
- Gestor de contraseñas PASS
- GitHub (Repositorio del proyecto)

4. Instalación del Hipervisor

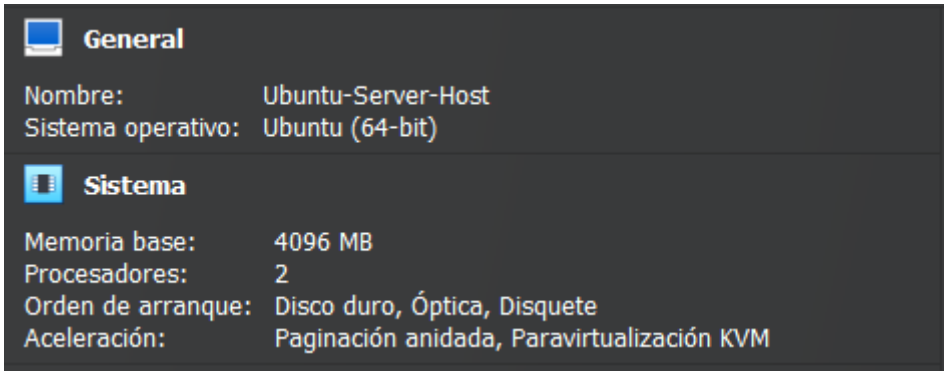
Se utilizó Oracle VM VirtualBox como hipervisor para la creación y gestión de las máquinas virtuales. El hipervisor fue instalado en el sistema anfitrión y configurado para permitir la creación de máquinas virtuales con adaptador de red en modo NAT.

5. Instalación y Configuración del Sistema Operativo Host

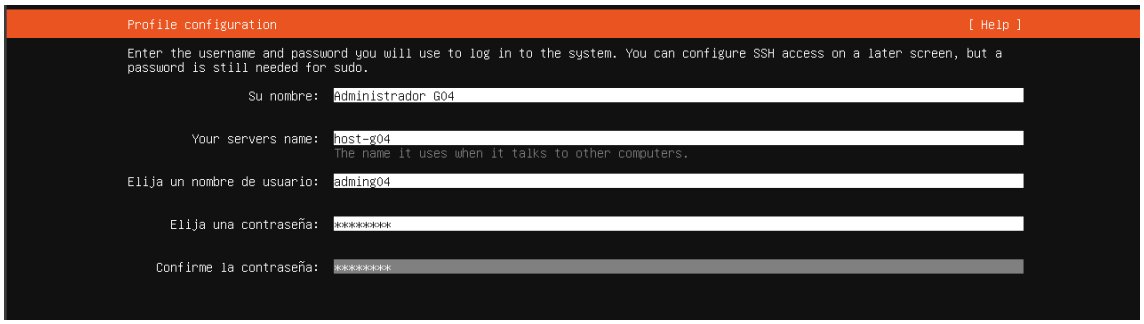
5.1 Instalación de Ubuntu Server

Se descargó la imagen ISO de Ubuntu Server 24.04 y se procedió a su instalación en una máquina virtual.

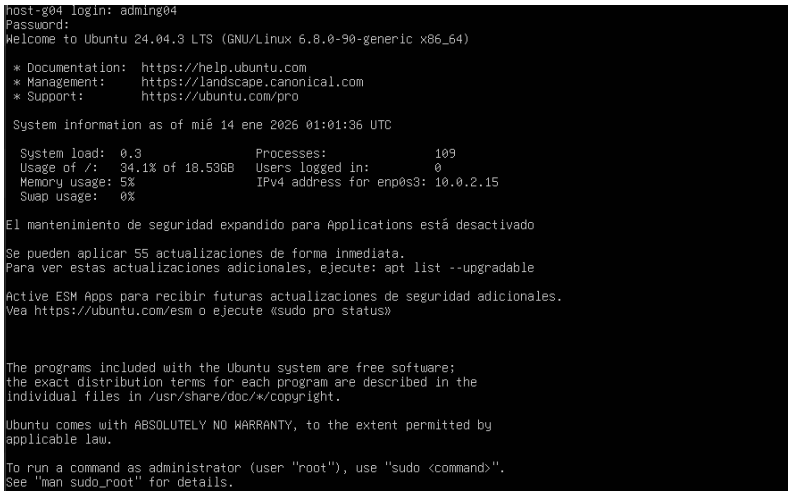
- Información del Sistema



- Usuario administrador con contraseña segura



5.2 Iniciar Sesión en Ubuntu Server



5.3 Creación de Usuarios del Sistema

Desde la consola de comandos se crearon los siguientes usuarios:

- **UserAGxx**: Usuario con privilegios administrativos.
- **UserBGxx**: Usuario con privilegios mínimos.

Esto se realizó para aplicar el principio de mínimo privilegio y mejorar la seguridad del sistema.

```
adming04@host-g04:~$ sudo usermod -aG sudo userag04
adming04@host-g04:~$
adming04@host-g04:~$ groups userag04
userag04 : userag04 sudo users
adming04@host-g04:~$
adming04@host-g04:~$ getent passwd userag04
userag04:x:1001:1001:,,,:/home/userag04:/bin/bash
adming04@host-g04:~$ getent passwd userbg04
userbg04:x:1002:1002:,,,:/home/userbg04:/bin/bash
```

5.4 Verificar IP de la Máquina Host

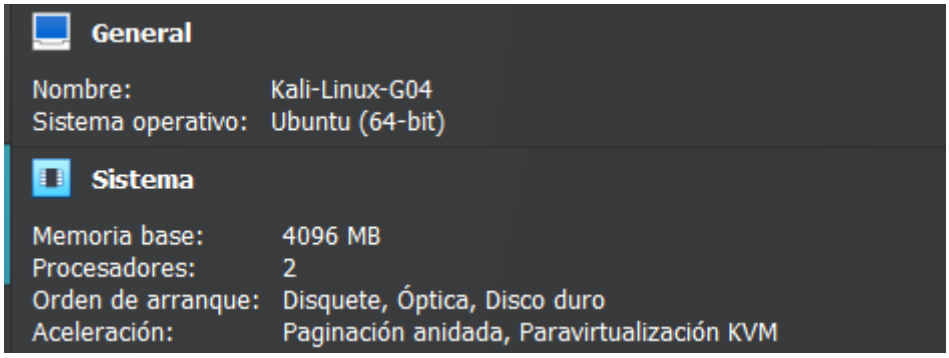
- **Interfaz de red activa:** enp0s3
- **IP del Host: 10.0.2.15**
- **Red:** 10.0.2.0/24

```
adming04@host-g04:~$ ip a
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 08:00:27:47:c0:11 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 85492sec preferred_lft 85492sec
    inet6 fe80::a00:27ff:fe47:c011/64 scope link
       valid_lft forever preferred_lft forever
```

6. Instalación y Configuración de Kali Linux

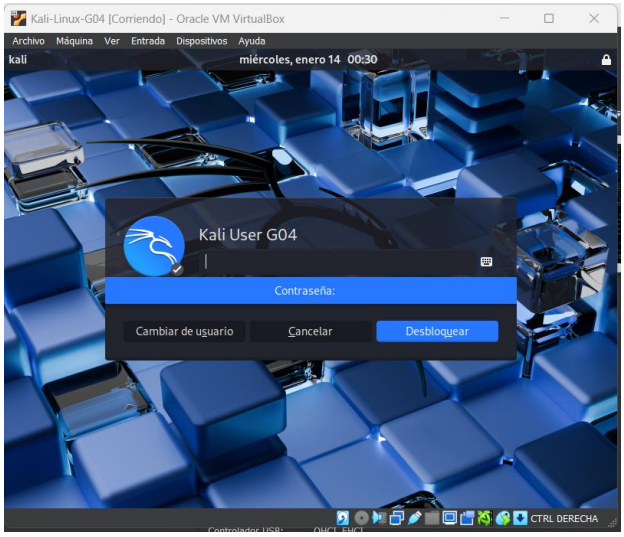
En un segundo entorno virtual se instaló Kali Linux utilizando la imagen installer-amd64. El sistema fue configurado correctamente y se verificó su funcionamiento.

- Información del Sistema



Se instaló Kali Linux utilizando la imagen oficial installer-amd64 en una máquina virtual independiente. Durante el proceso de instalación se realizó la configuración básica del sistema, incluyendo idioma, zona horaria, usuario principal y contraseña segura.

Posteriormente, se configuró la interfaz de red en modo NAT, permitiendo la asignación automática de una dirección IP y garantizando la conectividad con la máquina Host.



7. Pruebas de Conectividad de Red

7.1 Verificación de Configuración de Red

En primer lugar, se verificó la configuración de red en ambas máquinas virtuales mediante el comando ip a, confirmando que las interfaces de red estuvieran activas y que cada sistema contara con una dirección IP válida asignada automáticamente por el hipervisor.

En el sistema Host Ubuntu Server se obtuvo una dirección IP perteneciente a la red 10.0.2.0/24, lo que confirmó el correcto funcionamiento del adaptador de red configurado en modo NAT.

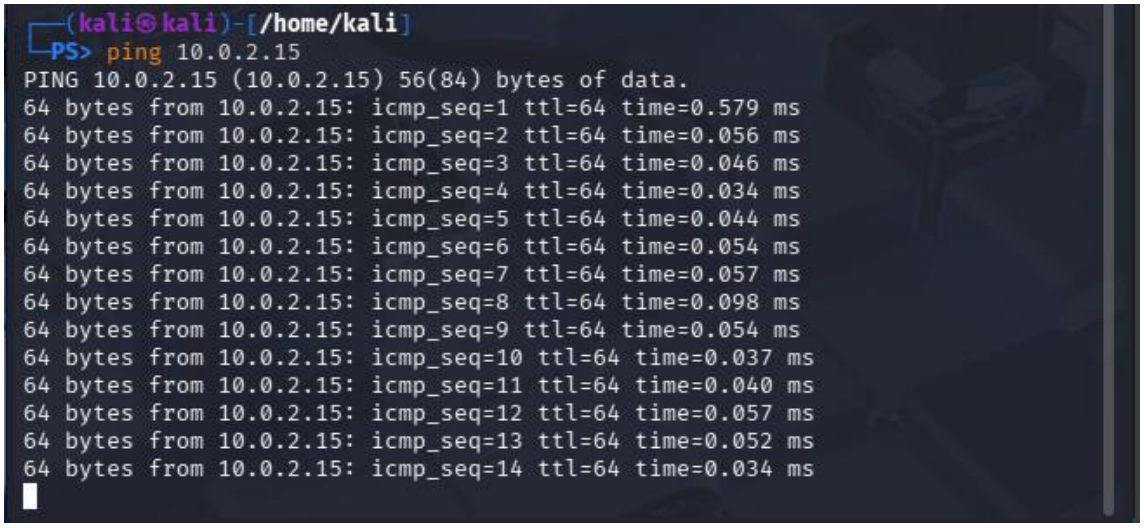
```
adming04@host-g04:/$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       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 08:00:27:47:c0:11 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 79508sec preferred_lft 79508sec
    inet6 fe80::a00:27ff:fe47:c011/64 scope link
       valid_lft forever preferred_lft forever
```

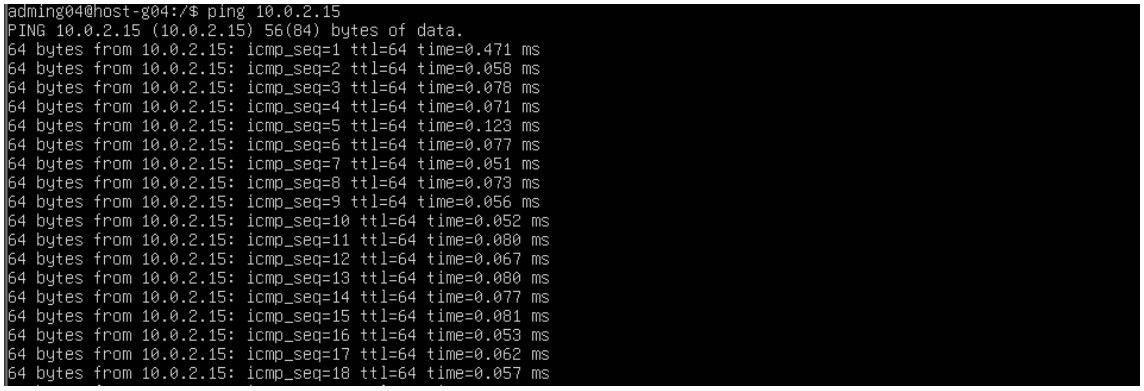
```
┌──(kali㉿kali)-[/home/kali]
└─PS> ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:4f:18:d3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 79052sec preferred_lft 79052sec
    inet6 fe80::a00:27ff:fe4f:18d3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

7.2 Pruebas de Conectividad entre Máquinas

Posteriormente, se realizaron pruebas de conectividad utilizando el comando ping desde Kali Linux hacia el sistema Host y viceversa. Estas pruebas permitieron comprobar la comunicación bidireccional entre ambos equipos dentro del entorno virtual.

La recepción de respuestas exitosas (paquetes ICMP recibidos sin pérdida) confirmó que ambas máquinas se encontraban en la misma red y que no existían bloqueos de conectividad a nivel de red.





7.3 Importancia de las Pruebas de Conectividad

Las pruebas de conectividad son fundamentales en un entorno de Hacking Ético, ya que garantizan que las herramientas de análisis y seguridad puedan interactuar correctamente con los sistemas objetivo. En este laboratorio, la conectividad exitosa permitió la implementación y validación de los dispositivos de seguridad configurados en el sistema Host.

8. Implementación de Dispositivos de Seguridad Informática

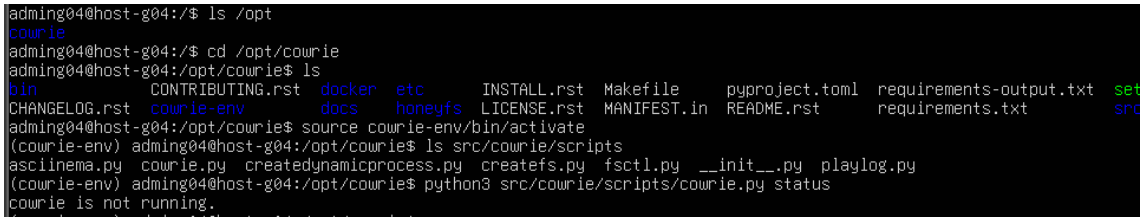
La implementación de dispositivos de seguridad informática tuvo como objetivo fortalecer el sistema Host frente a posibles accesos no autorizados y demostrar el uso práctico de mecanismos de defensa en un entorno controlado de Hacking Ético.

8.1 Honeypot – Cowrie

Se instaló y configuró el honeypot Cowrie en el sistema Host Ubuntu Server. Para su instalación se utilizó un entorno virtual de Python, lo que permitió aislar las dependencias del sistema y evitar conflictos con otras aplicaciones.

Cowrie fue configurado para simular servicios vulnerables, como accesos tipo SSH, con el fin de registrar intentos de conexión no autorizados. El servicio fue ejecutado y verificado correctamente mediante comandos de inicio y consulta de estado, confirmando su funcionamiento activo.

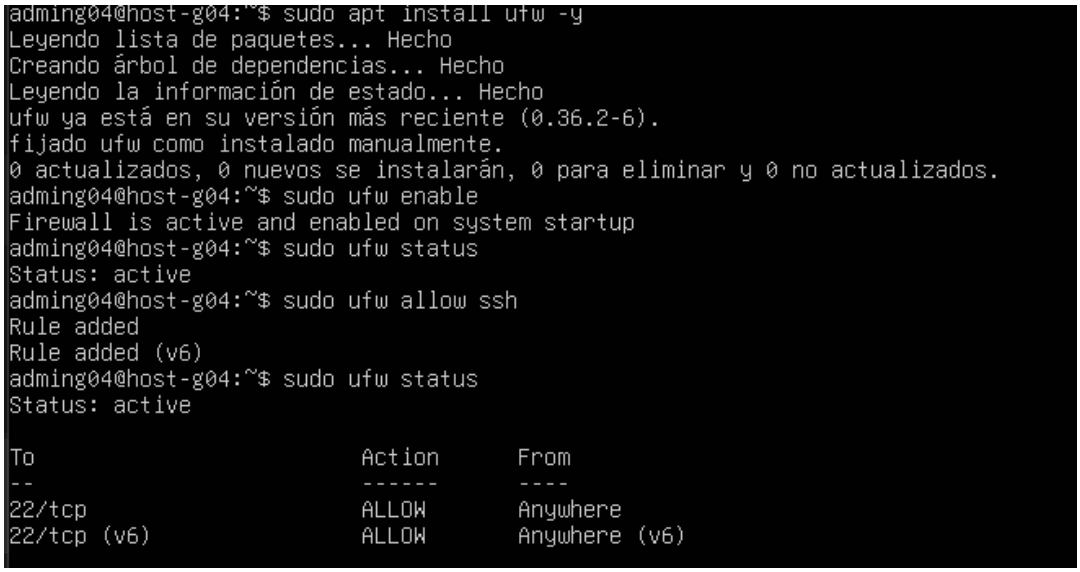
La implementación del honeypot permite analizar el comportamiento de posibles atacantes sin comprometer el sistema real, contribuyendo a la detección temprana de amenazas.



8.2 Firewall – UFW

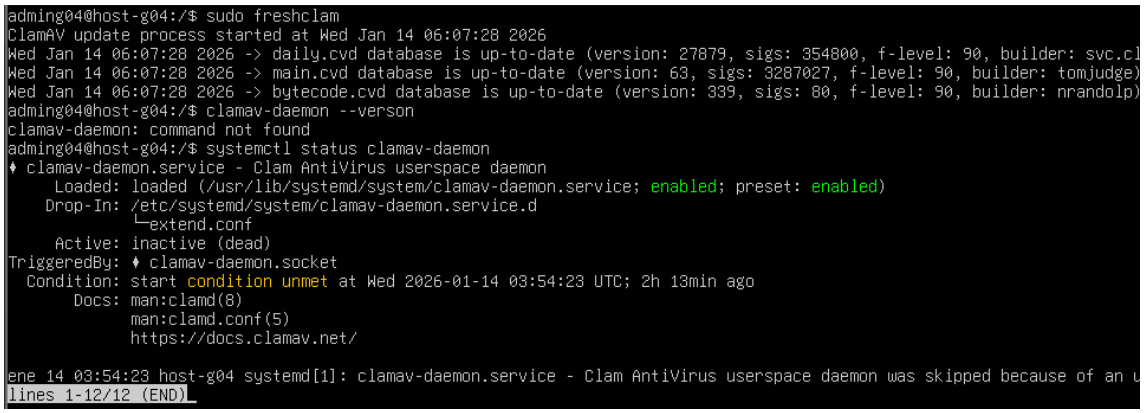
Se activó y configuró el firewall UFW (Uncomplicated Firewall) en el sistema Host como mecanismo de control de tráfico de red. UFW fue utilizado para permitir únicamente los servicios necesarios para el funcionamiento del sistema y bloquear accesos no autorizados.

La activación del firewall refuerza la seguridad perimetral del sistema, reduciendo la superficie de ataque y evitando conexiones innecesarias desde la red.

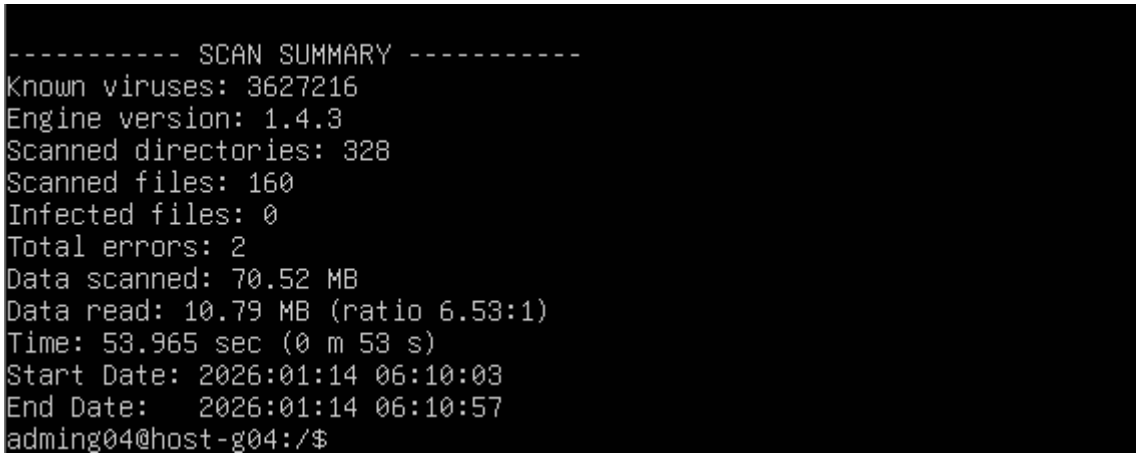


8.3 ANTIVIRUS – CLAMAV (SECCIÓN 9.X)

Se instaló y configuró el antivirus ClamAV en el sistema Host Ubuntu Server. Se actualizó la base de datos de firmas de malware y se verificó el correcto funcionamiento del servicio. Finalmente, se realizó un escaneo de prueba sobre el sistema, confirmando la ausencia de amenazas y demostrando la correcta implementación del antivirus.



Escaneo de prueba



9. Resultados Obtenidos

Como resultado del desarrollo del laboratorio de Configuración de un Entorno de Hacking Ético, se obtuvieron los siguientes resultados, los cuales evidencian el correcto cumplimiento de los objetivos planteados:

- Se logró la instalación y configuración exitosa de un hipervisor (Oracle VM VirtualBox), permitiendo la creación y administración de máquinas virtuales de forma eficiente y controlada.
- Se implementó correctamente un sistema operativo Host basado en Ubuntu Server, asegurando el acceso al sistema mediante credenciales protegidas y la creación de usuarios con distintos niveles de privilegios, aplicando el principio de mínimo privilegio.

- Se instaló Kali Linux como máquina de pruebas, configurando adecuadamente su red y verificando la conectividad con el sistema Host, lo que permitió validar la comunicación entre ambos entornos virtuales.
- Se comprobó que ambas máquinas virtuales se encontraban dentro de la misma red virtual, garantizando un entorno controlado y funcional para la realización de pruebas relacionadas con la seguridad informática.
- Se implementaron diversos dispositivos de seguridad informática en el sistema Host, incluyendo un honeypot (Cowrie), un firewall (UFW) y un antivirus (ClamAV), fortaleciendo la protección del sistema frente a posibles accesos no autorizados y amenazas.
- Se verificó el funcionamiento de cada uno de los dispositivos de seguridad mediante comandos de administración y pruebas prácticas, obteniendo resultados satisfactorios que evidencian su correcta implementación.
- El entorno configurado permitió simular un escenario realista de **Hacking Ético**, facilitando el aprendizaje práctico sobre la detección, prevención y mitigación de riesgos de seguridad en sistemas informáticos.

En conclusión, los resultados obtenidos demuestran que el entorno de Hacking Ético fue implementado de manera correcta y funcional, cumpliendo con los requerimientos establecidos en el laboratorio y proporcionando una base sólida para el desarrollo de competencias en seguridad informática.

10. Conclusiones

- El desarrollo del laboratorio permitió comprender la importancia de la virtualización como herramienta fundamental para la creación de entornos seguros y controlados, facilitando la realización de pruebas sin afectar sistemas reales.
- La configuración del sistema operativo Host y la máquina virtual con Kali Linux demostró la relevancia de una correcta administración de usuarios, credenciales y configuraciones de red para garantizar la seguridad y estabilidad del entorno.
- La implementación de dispositivos de seguridad informática como el honeypot Cowrie, el firewall UFW, el gestor de contraseñas PASS y el antivirus ClamAV evidenció cómo la combinación de diferentes mecanismos de defensa permite fortalecer significativamente la protección de un sistema frente a posibles amenazas.
- Las pruebas de conectividad realizadas confirmaron el correcto funcionamiento de la red virtual, asegurando la comunicación entre los equipos y permitiendo validar las configuraciones realizadas durante el laboratorio.
- El uso de herramientas de seguridad en un entorno controlado de **Hacking Ético** contribuyó al desarrollo de habilidades prácticas en el análisis, prevención y detección de riesgos de seguridad informática.

Bibliografía:

- [1] Kali Linux, “Kali Linux Documentation,” 2025. [Online]. Available: https://www.kali.org/docs/ . Accessed: Jan. 2026.

- [2] Ubuntu, “Ubuntu Server Guide,” 2025. [Online]. Available: https://ubuntu.com/server/docs . Accessed: Jan. 2026.

- [3] Oracle, “VirtualBox User Manual,” 2025. [Online]. Available: https://www.virtualbox.org/manual/ . Accessed: Jan. 2026.

- [4] Cowrie Honeypot, “Cowrie GitHub Repository,” 2025. [Online]. Available: https://github.com/cowrie/cowrie . Accessed: Jan. 2026.