Implementación de un Entorno Virtualizado Seguro

Configuración de Máquinas Virtuales, Usuarios y Dispositivos de Seguridad Informática

Integrantes

Tapia Rea Freddy Xavier
Trujillo Vistin Dennis Adrian
Loya Cadena Bryan Eduardo
Rosero Lema Ruth Estefanía
Lascano Puruncajas Ángelo Damián
Condolo Narváez Byron Paul

Fecha: 16 de enero de 2026

Universidad Central del Ecuador
Facultad de Ingeniería y Ciencias Aplicadas
Cátedra de Criptografía y Seguridad de la Información

Resumen

El presente informe documenta de manera detallada el desarrollo de un entorno virtualizado seguro, realizado por el Grupo 6 de la Cátedra de Criptografía y Seguridad de la Información, cuyo objetivo principal fue la aplicación práctica de conceptos fundamentales relacionados con la virtualización, la administración de sistemas operativos y la implementación de mecanismos de seguridad informática.

Como sistema operativo anfitrión (Host) se utilizó Windows Server 2019, instalado y configurado sobre una máquina virtual mediante el hipervisor Oracle VirtualBox. Durante el proceso de montaje del entorno, se documentó desde la instalación del hipervisor en el sistema anfitrión, la descarga y uso de las imágenes ISO correspondientes, hasta la creación y configuración completa de las máquinas virtuales. En el sistema Windows Server 2019 se aseguró el acceso administrativo mediante el establecimiento de una contraseña robusta para el usuario Administrador, garantizando así una adecuada protección inicial del sistema.

Adicionalmente, se llevó a cabo la creación de dos usuarios del sistema operativo a través de la consola de comandos, cumpliendo con los lineamientos establecidos en la asignación. El usuario `UserAG06` fue configurado con privilegios administrativos totales, mientras que el usuario `UserBG06` fue creado con privilegios mínimos, permitiendo evidenciar la correcta gestión de roles y permisos dentro del sistema operativo anfitrión.

Como máquina atacante se instaló Kali Linux, empleando la versión oficial optimizada para Oracle VirtualBox, descargada directamente desde el sitio web oficial del proyecto Kali Linux. Esta máquina virtual fue configurada con los parámetros necesarios para garantizar su correcta integración en la red del entorno virtualizado, permitiendo la comunicación efectiva entre el sistema atacante y el sistema anfitrión.

Uno de los aspectos clave del proyecto fue la verificación de la conectividad entre ambas máquinas virtuales, asegurando que compartieran el mismo segmento de red. Para ello, se configuraron los adaptadores de red adecuados y se realizaron pruebas de comunicación mediante herramientas de red, confirmando el intercambio de paquetes entre Windows Server 2019 y Kali Linux.

Asimismo, en la máquina Host se instalaron, activaron y configuraron tres dispositivos de seguridad informática, seleccionados de acuerdo con los requerimientos del proyecto. Estos mecanismos permitieron reforzar la protección del sistema operativo anfitrión frente a posibles amenazas, demostrando la importancia de una defensa en capas dentro de un entorno virtualizado. Cada proceso de instalación y configuración fue debidamente documentado mediante descripciones técnicas y capturas de pantalla, integradas dentro de las secciones correspondientes del informe.

Finalmente, este trabajo evidencia la correcta aplicación de conocimientos teóricos y prácticos en el ámbito de la criptografía y la seguridad de la información, destacando la importancia de la virtualización como herramienta fundamental para la simulación, análisis y fortalecimiento de entornos seguros. El proyecto desarrollado por el Grupo 6 constituye una base sólida para futuras prácticas relacionadas con la administración de sistemas, el análisis de vulnerabilidades y la implementación de estrategias de seguridad informática.

Índice

1. Introducción

La seguridad de la información constituye uno de los pilares fundamentales en el ámbito de las tecnologías de la información, especialmente en entornos donde la confidencialidad, integridad y disponibilidad de los datos resultan críticas. En este contexto, la virtualización se ha consolidado como una herramienta esencial que permite simular infraestructuras reales de forma controlada, facilitando la implementación, evaluación y fortalecimiento de mecanismos de seguridad informática.

El presente proyecto, desarrollado por el Grupo 6 de la Cátedra de Criptografía y Seguridad de la Información, se enfoca en la creación de un entorno virtualizado seguro que integra un sistema operativo anfitrión basado en Windows Server 2019 y una máquina virtual atacante con Kali Linux. Este entorno permite la aplicación práctica de conceptos teóricos abordados durante el curso, relacionados con la administración de sistemas, la gestión de usuarios y la protección de infraestructuras digitales.

1.1. Contexto del Proyecto

La creciente complejidad de los sistemas informáticos y el aumento constante de amenazas cibernéticas han impulsado la necesidad de contar con entornos de prueba que permitan analizar escenarios reales sin comprometer sistemas productivos. En este sentido, la virtualización ofrece una solución eficiente y segura, ya que posibilita la ejecución de múltiples sistemas operativos sobre un mismo hardware físico, manteniendo un adecuado aislamiento entre ellos.

Dentro de este proyecto, se emplea Oracle VirtualBox como hipervisor, herramienta que facilita la creación y gestión de máquinas virtuales. A través de esta plataforma, se implementa un entorno controlado donde se simulan tanto un sistema servidor como un sistema atacante, permitiendo evaluar la interacción entre ambos bajo distintas configuraciones de seguridad.

1.2. Importancia de la Virtualización en la Seguridad Informática

La virtualización desempeña un rol clave en la seguridad informática, ya que permite la ejecución de pruebas de configuración, análisis de vulnerabilidades y simulación de ataques sin afectar infraestructuras reales. Además, posibilita la rápida recuperación ante fallos, el control de accesos y la implementación de políticas de seguridad específicas para cada entorno virtual.

En el contexto de la criptografía y la seguridad de la información, la virtualización facilita la comprensión práctica de conceptos como la segmentación de redes, la gestión de privilegios de usuarios y la implementación de mecanismos de defensa, tales como firewalls, sistemas de detección y prevención de intrusos, y soluciones de protección perimetral.

1.3. Descripción General del Entorno Implementado

El entorno virtualizado desarrollado por el Grupo 6 está compuesto por dos máquinas virtuales principales. La primera corresponde a un sistema anfitrión con Windows Server 2019, el cual actúa como servidor y plataforma principal para la

configuración de usuarios y la implementación de dispositivos de seguridad informática. En este sistema se establecen políticas de acceso y se garantiza la protección del usuario administrador mediante el uso de contraseñas seguras.

La segunda máquina virtual corresponde a Kali Linux, instalada utilizando la imagen oficial optimizada para Oracle VirtualBox. Este sistema se utiliza como entorno atacante, permitiendo realizar pruebas de conectividad y análisis desde una perspectiva ofensiva controlada. Ambas máquinas fueron configuradas para operar dentro del mismo segmento de red virtual, asegurando la correcta comunicación entre ellas.

1.4. Alcance del Documento

El presente informe describe de forma detallada cada una de las fases del proyecto, iniciando con la instalación del hipervisor y la preparación de los recursos necesarios, continuando con la configuración de los sistemas operativos y la gestión de usuarios, y finalizando con la implementación y análisis de distintos dispositivos de seguridad informática. Cada procedimiento se encuentra debidamente documentado mediante explicaciones técnicas y evidencias gráficas, con el fin de garantizar la trazabilidad y reproducibilidad del entorno implementado.

De esta manera, el documento constituye una guía práctica que evidencia la correcta aplicación de los conocimientos adquiridos en la cátedra, así como la importancia de la planificación y documentación en la implementación de entornos seguros basados en virtualización.

2. Objetivos

2.1. Objetivo General

Implementar y documentar un entorno virtualizado seguro mediante el uso de un sistema operativo anfitrión Windows Server 2019 y una máquina virtual atacante basada en Kali Linux, con el fin de aplicar de manera práctica los principios de la criptografía y la seguridad de la información, garantizando una adecuada gestión de usuarios, conectividad en red y mecanismos de protección informática.

2.2. Objetivos Específicos

- Instalar y configurar el hipervisor Oracle VirtualBox en un entorno Windows, documentando el proceso completo desde la descarga hasta su correcta puesta en funcionamiento.
- Implementar una máquina virtual con Windows Server 2019, asegurando el acceso administrativo mediante el uso de una contraseña robusta y configurando parámetros básicos de seguridad del sistema operativo.
- Crear y administrar usuarios del sistema operativo desde la consola de comandos, estableciendo distintos niveles de privilegio, donde el usuario `UserAG06` cuente con privilegios administrativos y el usuario `UserBG06` posea privilegios mínimos.

- Instalar y configurar una máquina virtual con Kali Linux, utilizando la imagen oficial optimizada para Oracle VirtualBox, descargada desde el sitio web oficial del proyecto.
- Configurar la red virtual de manera que ambas máquinas virtuales se encuentren dentro del mismo segmento de red, verificando la conectividad mediante pruebas de comunicación.
- Instalar, activar y configurar al menos tres dispositivos de seguridad informática en la máquina Host, con el propósito de fortalecer la protección del sistema operativo frente a posibles amenazas.
- Documentar de forma detallada cada una de las fases del proyecto, incorporando evidencias gráficas y descripciones técnicas que respalden los procedimientos realizados por el Grupo 6.

3. Marco Teórico

El marco teórico constituye la base conceptual que sustenta el desarrollo del presente proyecto, permitiendo contextualizar las tecnologías, metodologías y conceptos relacionados con la virtualización y la seguridad informática. A través de este apartado se describen los fundamentos teóricos necesarios para comprender la implementación del entorno virtualizado seguro desarrollado por el Grupo 6 en el marco de la Cátedra de Criptografía y Seguridad de la Información.

3.1. Virtualización

La virtualización es una tecnología que permite la creación de versiones virtuales de recursos físicos, tales como servidores, sistemas operativos, dispositivos de almacenamiento y redes. Su principal objetivo es optimizar el uso del hardware disponible, proporcionando aislamiento, flexibilidad y escalabilidad en la ejecución de múltiples entornos sobre una misma plataforma física.

En el ámbito de la seguridad informática, la virtualización facilita la creación de entornos de prueba controlados, donde es posible simular escenarios reales de ataque y defensa sin comprometer infraestructuras productivas. Además, permite la rápida restauración de sistemas, la segmentación de recursos y la implementación de políticas de seguridad específicas para cada máquina virtual.

3.2. Hipervisores

El hipervisor es el componente de software encargado de gestionar y coordinar la ejecución de las máquinas virtuales sobre el hardware físico. Existen principalmente dos tipos de hipervisores: de tipo 1 o nativos, que se ejecutan directamente sobre el hardware, y de tipo 2, que se ejecutan sobre un sistema operativo anfitrión.

En este proyecto se utiliza Oracle VirtualBox, un hipervisor de tipo 2 ampliamente utilizado en entornos académicos y profesionales debido a su facilidad de uso, compatibilidad multiplataforma y soporte para diversos sistemas operativos. VirtualBox permite la configuración detallada de recursos como memoria, almacenamiento y red, facilitando la implementación de entornos seguros y controlados.

3.3. Windows Server 2019

Windows Server 2019 es un sistema operativo orientado a servidores, desarrollado por Microsoft, diseñado para ofrecer servicios de red, administración de usuarios y recursos, así como mecanismos avanzados de seguridad. Este sistema operativo incluye herramientas integradas para la gestión de identidades, control de accesos y protección frente a amenazas.

Dentro del contexto del proyecto, Windows Server 2019 actúa como sistema operativo anfitrión, permitiendo la creación y administración de usuarios con distintos niveles de privilegio. Su uso facilita la implementación de políticas de seguridad, la activación de servicios de protección como el firewall y el antivirus integrado, y la gestión centralizada de la configuración del sistema.

3.4. Kali Linux

Kali Linux es una distribución de Linux especializada en pruebas de penetración, auditorías de seguridad y análisis forense digital. Desarrollada y mantenida por Offensive Security, esta distribución incluye una amplia variedad de herramientas orientadas al análisis de vulnerabilidades y evaluación de la seguridad de sistemas informáticos.

En el presente proyecto, Kali Linux se utiliza como máquina virtual atacante, empleando la imagen oficial optimizada para Oracle VirtualBox. Su implementación permite simular escenarios de ataque controlados, evaluar la conectividad de red y analizar el comportamiento del sistema anfitrión frente a posibles amenazas, reforzando así el enfoque práctico de la cátedra.

3.5. Seguridad de la Información

La seguridad de la información se enfoca en la protección de los datos frente a accesos no autorizados, alteraciones indebidas o pérdidas, garantizando los principios de confidencialidad, integridad y disponibilidad. Estos principios, conocidos como la triada CIA, constituyen la base fundamental de cualquier estrategia de seguridad informática.

En entornos virtualizados, la seguridad de la información adquiere una relevancia especial, ya que la coexistencia de múltiples sistemas en una misma infraestructura requiere controles estrictos de acceso, segmentación de redes y monitoreo constante de actividades sospechosas.

3.6. Gestión de Usuarios y Control de Accesos

La correcta gestión de usuarios y privilegios es un elemento clave en la seguridad de los sistemas operativos. Asignar roles y permisos adecuados permite minimizar el riesgo de accesos no autorizados y limitar el impacto de posibles incidentes de seguridad.

En este proyecto se implementa la creación de usuarios desde la consola de comandos en Windows Server 2019, estableciendo un usuario con privilegios administrativos (`UserAG06`) y un usuario con privilegios mínimos (`UserBG06`). Esta diferenciación permite evidenciar la importancia del principio de mínimo privilegio dentro de un entorno seguro.

3.7. Dispositivos de Seguridad Informática

Los dispositivos de seguridad informática son herramientas diseñadas para prevenir, detectar y responder ante amenazas que puedan comprometer la integridad de los sistemas. Entre los más utilizados se encuentran los firewalls, los sistemas de detección y prevención de intrusos, los antivirus, las redes privadas virtuales y los gestores de contraseñas.

La implementación de múltiples capas de seguridad, conocida como defensa en profundidad, permite reducir significativamente la superficie de ataque y mejorar la capacidad de respuesta ante incidentes. En el entorno desarrollado por el Grupo 6, se seleccionan y configuran diversos dispositivos de seguridad en el sistema anfitrión, fortaleciendo su protección frente a posibles amenazas provenientes del entorno atacante.

3.8. Importancia de la Documentación en Seguridad Informática

La documentación técnica es un componente esencial en cualquier proyecto de seguridad informática, ya que permite registrar procedimientos, configuraciones y decisiones adoptadas durante la implementación de un sistema. Una documentación clara y detallada facilita la reproducibilidad del entorno, el mantenimiento de los sistemas y la auditoría de las medidas de seguridad aplicadas.

En el presente informe, cada fase del proyecto es documentada de manera detallada, incorporando descripciones técnicas y evidencias gráficas que respaldan el trabajo realizado, garantizando así la trazabilidad y el correcto entendimiento del entorno virtualizado seguro implementado.

4. Herramientas y Recursos

Para el desarrollo del presente proyecto, el Grupo 6 empleó un conjunto de herramientas de software y recursos tecnológicos que permitieron la correcta implementación del entorno virtualizado seguro. La selección de estas herramientas se realizó considerando su estabilidad, compatibilidad y uso extendido en el ámbito académico y profesional de la seguridad informática.

4.1. Sistema Operativo Anfitrión

Como sistema operativo anfitrión se utilizó Windows Server 2019, una plataforma orientada a la administración de servidores y servicios de red. Este sistema operativo fue seleccionado debido a su robustez, sus mecanismos integrados de seguridad y su amplia adopción en entornos empresariales. Windows Server 2019 proporciona herramientas nativas para la gestión de usuarios, control de accesos, configuración de políticas de seguridad y protección frente a amenazas, aspectos fundamentales para el cumplimiento de los objetivos del proyecto.

4.2. Hipervisor

El hipervisor empleado para la virtualización fue Oracle VirtualBox, una herramienta de tipo 2 que permite la ejecución de múltiples sistemas operativos sobre un

mismo equipo físico. VirtualBox ofrece compatibilidad con diversos sistemas operativos, facilidad de configuración y soporte para características avanzadas como redes virtuales, instantáneas y extensiones de hardware, lo que lo convierte en una solución adecuada para la implementación de entornos de prueba seguros.

Adicionalmente, se utilizó el Extension Pack de VirtualBox, el cual amplía las capacidades del hipervisor, habilitando soporte para dispositivos USB, mejoras en el rendimiento y opciones avanzadas de red necesarias para el correcto funcionamiento de las máquinas virtuales.

4.3. Máquina Virtual Host

La máquina virtual Host fue configurada con Windows Server 2019, asignando recursos adecuados de procesamiento, memoria y almacenamiento para garantizar un funcionamiento estable. En este sistema se llevaron a cabo tareas de administración, creación de usuarios, configuración de seguridad y verificación de conectividad, actuando como el principal punto de análisis dentro del entorno virtualizado.

4.4. Máquina Virtual Atacante

Como sistema operativo atacante se utilizó Kali Linux, empleando la imagen oficial optimizada para Oracle VirtualBox, descargada desde el sitio web oficial del proyecto Kali Linux. Esta versión fue seleccionada por su facilidad de despliegue y por incluir de forma preinstalada una amplia gama de herramientas orientadas a pruebas de penetración y análisis de seguridad.

Kali Linux permitió simular un entorno de ataque controlado, facilitando la evaluación de la conectividad de red y el comportamiento del sistema anfitrión frente a posibles interacciones maliciosas, siempre dentro de un contexto académico y ético.

4.5. Imágenes y Archivos de Instalación

Para la implementación del entorno se utilizaron imágenes de instalación oficiales, garantizando la autenticidad y seguridad del software empleado. Entre los principales recursos utilizados se encuentran:

- Instalador oficial de Oracle VirtualBox para sistemas Windows.
- Extension Pack correspondiente a la versión de VirtualBox instalada.
- Imagen de instalación de Windows Server 2019.
- Imagen oficial de Kali Linux para Oracle VirtualBox.

El uso de fuentes oficiales permitió reducir riesgos asociados a software malicioso y asegurar la compatibilidad entre los distintos componentes del entorno virtualizado.

4.6. Recursos de Hardware

El proyecto fue desarrollado sobre un equipo físico que cumple con los requisitos mínimos necesarios para la virtualización, incluyendo soporte para virtualización por hardware, memoria RAM suficiente y capacidad de almacenamiento adecuada.

Estos recursos permitieron la ejecución simultánea de las máquinas virtuales sin afectar la estabilidad del sistema anfitrión.

4.7. Herramientas Complementarias

Adicionalmente, se emplearon herramientas nativas y de apoyo para la correcta ejecución del proyecto, entre las cuales se incluyen la consola de comandos y PowerShell en Windows Server 2019, utilizadas para la creación y administración de usuarios, así como herramientas de red básicas empleadas para la verificación de conectividad entre las máquinas virtuales.

En conjunto, las herramientas y recursos seleccionados permitieron al Grupo 6 implementar un entorno virtualizado seguro, coherente con los objetivos académicos de la Cátedra de Criptografía y Seguridad de la Información.

5. Instalación de Oracle VirtualBox

En esta sección se describe de manera detallada el proceso de instalación del hipervisor Oracle VirtualBox en el sistema operativo Windows, el cual constituye la base fundamental para la creación y administración de las máquinas virtuales empleadas en el desarrollo del entorno virtualizado seguro. A partir de esta etapa, se incorporan capturas de pantalla como evidencias del trabajo realizado por el Grupo 6.

5.1. Descarga del Hipervisor

El primer paso consistió en la descarga del instalador oficial de Oracle VirtualBox desde el sitio web del fabricante. Se seleccionó la versión compatible con sistemas operativos Windows, asegurando así la correcta ejecución del hipervisor sobre el equipo anfitrión. La descarga desde fuentes oficiales garantiza la integridad del software y reduce el riesgo de incorporar componentes maliciosos al sistema.

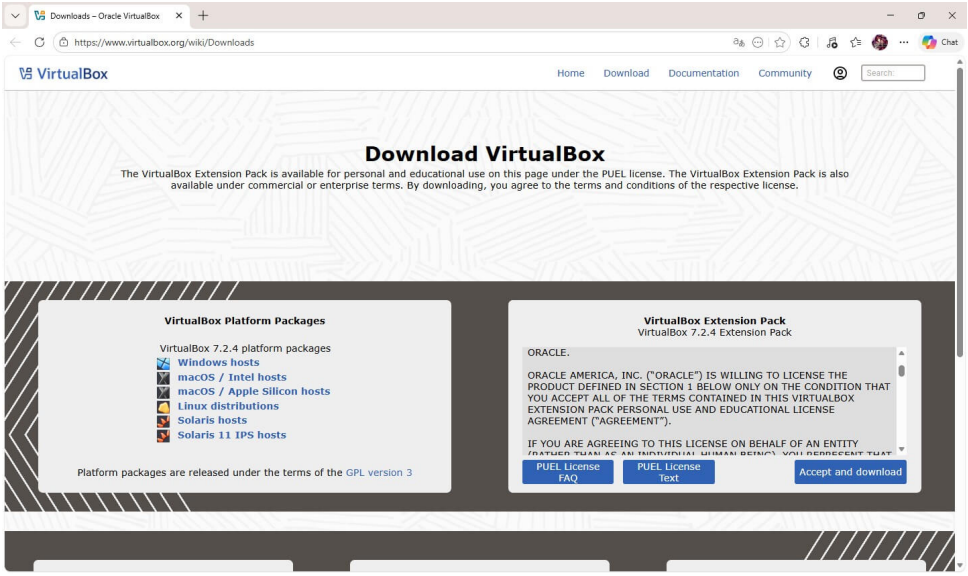

Figura 1: Descarga del instalador oficial de Oracle VirtualBox

5.2. Proceso de Instalación

Una vez finalizada la descarga, se ejecutó el instalador de Oracle VirtualBox en el sistema operativo Windows. Durante el proceso de instalación, se mantuvieron las opciones predeterminadas, las cuales incluyen los componentes esenciales para el funcionamiento del hipervisor, tales como los controladores de red y las herramientas de gestión de máquinas virtuales.

En esta etapa, el instalador notificó breves interrupciones en la conectividad de red, propias de la instalación de adaptadores virtuales. Dichas interrupciones fueron temporales y no afectaron de manera permanente el funcionamiento del sistema anfitrión.

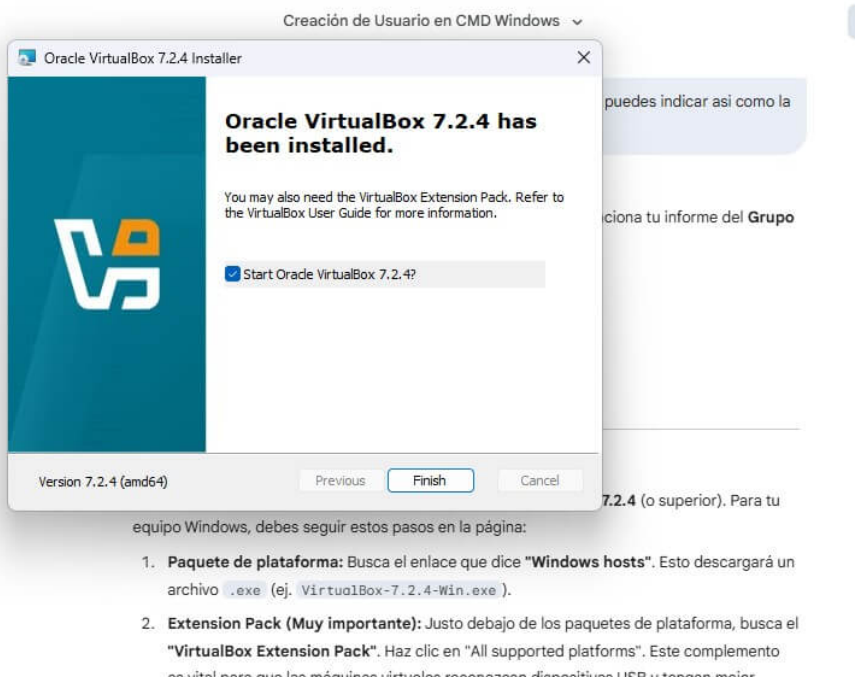

Figura 2: Proceso de instalación de Oracle VirtualBox en Windows

5.3. Finalización de la Instalación

Al concluir el proceso de instalación, el sistema confirmó que Oracle VirtualBox fue instalado correctamente. Posteriormente, se ejecutó el hipervisor para verificar su correcto funcionamiento y comprobar que la interfaz gráfica se encontraba operativa, permitiendo la creación y gestión de máquinas virtuales.

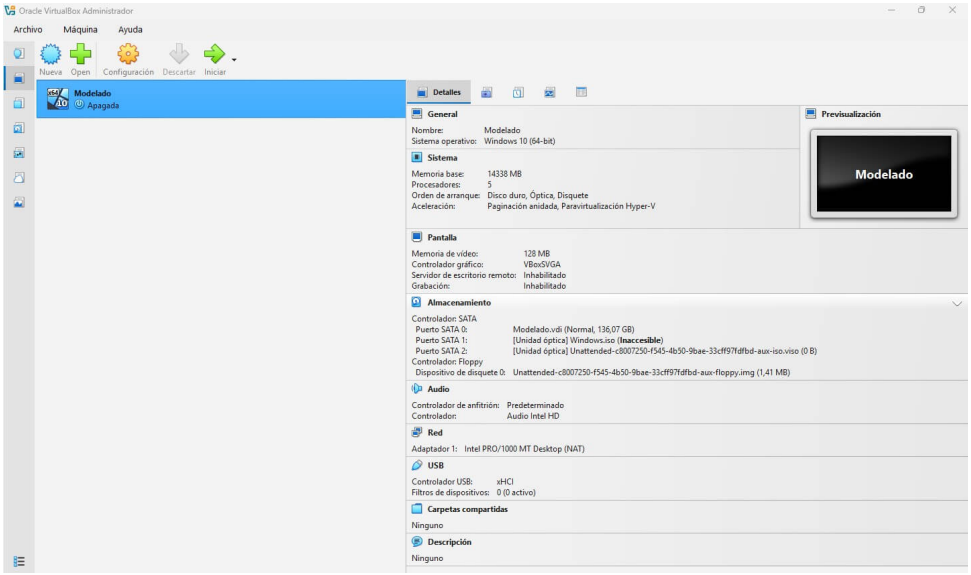

Figura 3: Interfaz principal de Oracle VirtualBox tras la instalación

5.4. Instalación del Extension Pack

Con el fin de ampliar las capacidades del hipervisor, se procedió a la instalación del Extension Pack correspondiente a la misma versión de Oracle VirtualBox instalada previamente. Este componente adicional proporciona soporte para dispositivos USB, mejoras en la gestión de red y otras funcionalidades avanzadas necesarias para el correcto funcionamiento del entorno virtualizado.

El Extension Pack fue descargado desde el sitio oficial de Oracle y su instalación se realizó directamente desde la interfaz de VirtualBox, aceptando los términos de la licencia de uso.

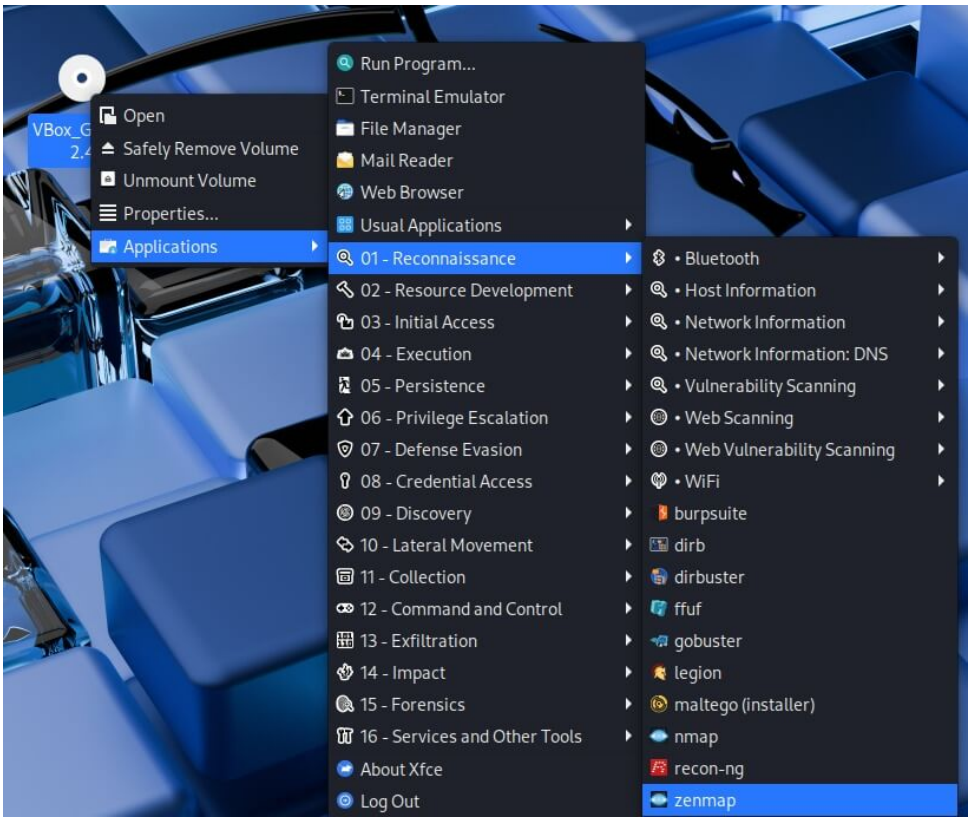

Figura 4: Instalación del Extension Pack de Oracle VirtualBox

5.5. Verificación del Entorno de Virtualización

Como paso final, se realizó una verificación general del entorno de virtualización, comprobando que Oracle VirtualBox reconocía correctamente los recursos del sistema, tales como la memoria RAM, el procesador y las opciones de virtualización por hardware. Esta verificación permitió asegurar que el hipervisor se encontraba listo para la creación de las máquinas virtuales con Windows Server 2019 y Kali Linux.

La correcta instalación de Oracle VirtualBox constituye un requisito esencial para las siguientes fases del proyecto, en las cuales se procederá con la configuración del sistema operativo anfitrión y la implementación de la máquina virtual atacante.

6. Configuración del Host Windows Server 2019

En esta sección se documenta de manera detallada el proceso de montaje, instalación y configuración de la máquina virtual Host con sistema operativo Windows Server 2019, cumpliendo los requisitos planteados en la práctica de laboratorio. Todos los procesos se realizaron desde el hipervisor Oracle VirtualBox previamente instalado. A partir de este punto se incluyen capturas de pantalla como evidencia del trabajo realizado por el Grupo 6.

6.1. Creación de la Máquina Virtual

El primer paso consistió en crear la máquina virtual que alojaría el Sistema Operativo Windows Server 2019. Para ello se accedió a la interfaz principal de Vir-

tualBox y se seleccionó la opción *Nueva*, especificando los parámetros necesarios para el funcionamiento adecuado del sistema.

Los parámetros definidos fueron los siguientes:

- **Nombre:** Windows Server 2019 - Grupo 06
- **Tipo:** Microsoft Windows
- **Versión:** Windows 2019 (64-bit)
- **Memoria RAM:** 4096 MB
- **Procesadores:** 2 vCPU
- **Disco Duro:** 60 GB en formato VDI (dinámico)

La siguiente imagen muestra el proceso de creación de la máquina virtual:

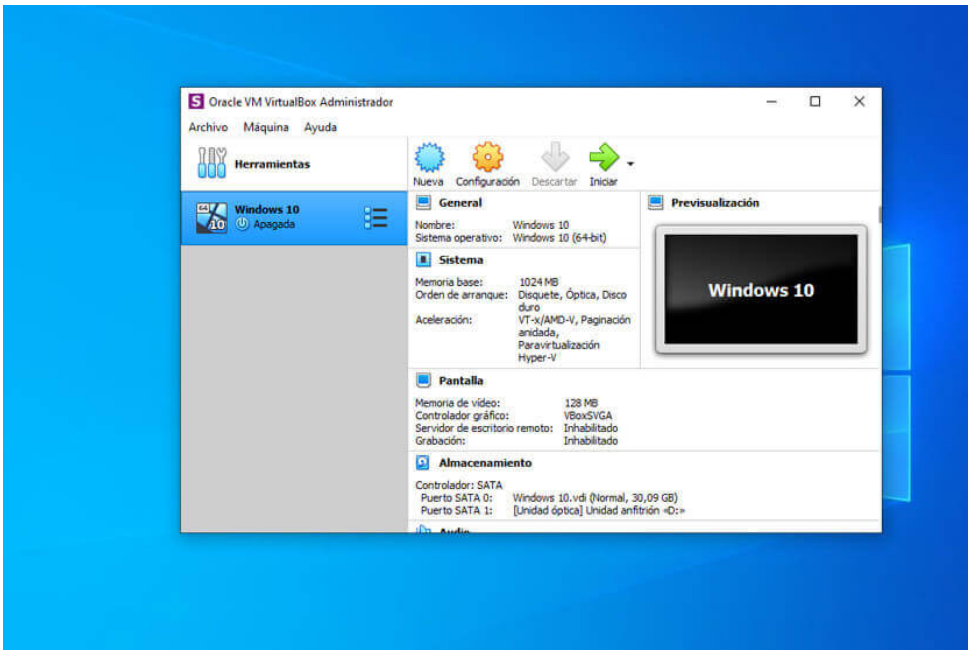

Figura 5: Creación de la máquina virtual Windows Server 2019 en VirtualBox

6.2. Montaje de la Imagen ISO

Una vez creada la máquina virtual, se procedió a montar la imagen ISO de Windows Server 2019 descargada desde el Centro de Evaluación de Microsoft. Esto permitió iniciar el proceso de instalación del sistema operativo durante el primer arranque de la máquina virtual.

Para ello se accedió a:

`Configuración → Almacenamiento → Controlador IDE → Elegir disco → Seleccionar ISO`

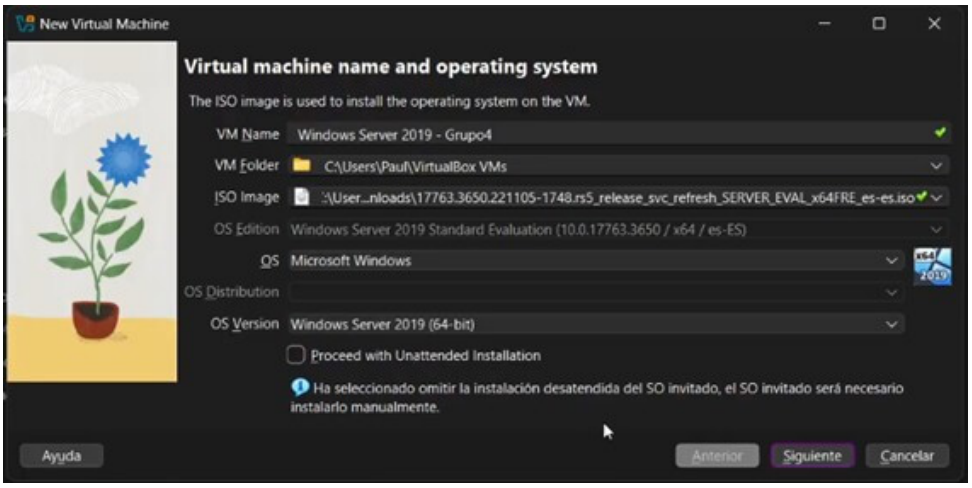

Figura 6: Montaje de la imagen ISO de Windows Server 2019

6.3. Instalación del Sistema Operativo

Con la ISO montada, se encendió la máquina virtual y se inició el asistente de instalación de Windows Server 2019. Durante este proceso se seleccionaron las opciones de configuración inicial y se decidió instalar:

Windows Server 2019 Standard (Experiencia de escritorio)

La experiencia de escritorio es necesaria para las futuras configuraciones guiadas, asegurando un entorno visual para manipular herramientas administrativas del sistema operativo.

El proceso se desarrolló siguiendo los siguientes pasos:

1. Selección de idioma, formato de hora y teclado.
2. Selección de versión del sistema operativo.
3. Aceptación de términos de licencia.
4. Instalación personalizada (avanzada).
5. Selección del disco de 60 GB.
6. Proceso automático de copia de archivos y reinicios.

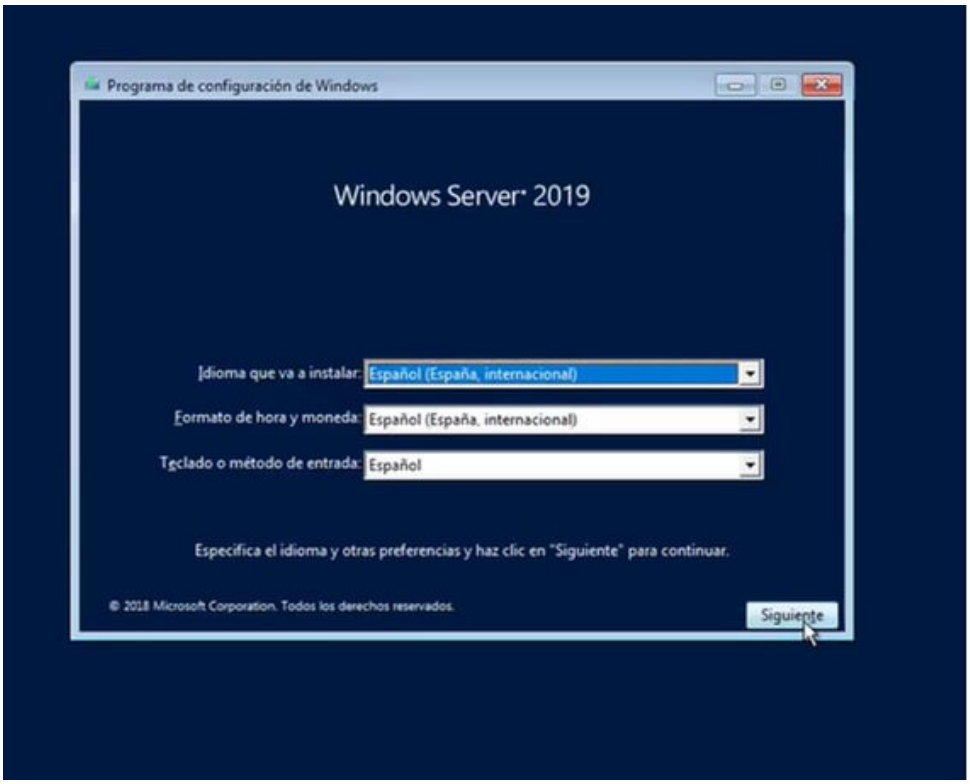

Figura 7: Instalación de Windows Server 2019 en progreso

6.4. Configuración Inicial y Contraseña del Administrador

Una vez finalizada la instalación, el asistente solicitó establecer una contraseña para la cuenta local `Administrator`. El Grupo 6 definió una contraseña robusta cumpliendo los requisitos de seguridad del sistema operativo, incluyendo:

- Mínimo 12 caracteres
- Letras mayúsculas y minúsculas
- Números
- Caracteres especiales

Ejemplo ilustrativo aplicado:

Gr06@Server-2024!Seguro

La siguiente imagen evidencia la fase de asignación de contraseña:

Figura 8: Asignación de contraseña para la cuenta Administrator

6.5. Creación de Usuarios por Consola

Una vez dentro del entorno de escritorio de Windows Server 2019, se procedió a crear dos usuarios desde la consola `CMD` como lo solicita la asignación:

- **UserAG06** — con privilegios administrativos
- **UserBG06** — con privilegios mínimos

6.5.1. Creación del Usuario con Privilegios Totales

Para crear al usuario con privilegios administrativos se ejecutaron los siguientes comandos:

```
net user UserAG06 Gr06@Admin-2024! /add /comment:"Usuario
    Administrador Grupo 06" /expires:never /passwordchg:yes
net localgroup Administradores UserAG06 /add
```

La siguiente captura muestra la ejecución correcta:

Figura 9: Creación del usuario UserAG06 con privilegios administrativos

6.5.2. Creación del Usuario con Privilegios Mínimos

Posteriormente, se creó el usuario de privilegios limitados utilizando:

```
net user UserBG06 Gr06@Basico-2024? /add /comment:"Usuario B sico
    Grupo 06" /expires:never /passwordchg:yes
```

La siguiente imagen demuestra la creación satisfactoria del usuario:

Figura 10: Creación del usuario UserBG06 con privilegios mínimos

6.6. Verificación de Privilegios

Para comprobar el estado de los usuarios y sus permisos se utilizaron los comandos:

```
net user
net localgroup Administradores
```

En la verificación se confirmó que:

- `UserAG06` pertenece al grupo **Administradores**
- `UserBG06` no posee privilegios elevados

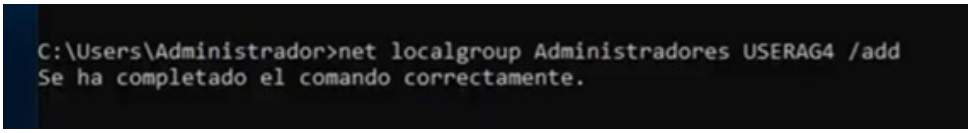

Figura 11: Verificación de grupos y privilegios de usuarios

6.7. Estado Final del Host Windows

Tras completar los pasos anteriores, el equipo Host Windows Server 2019 quedó configurado con:

- Contraseña del Administrador segura
- Estructura de usuarios con políticas de privilegios
- Preparación para instalación de dispositivos de seguridad informática

Este sistema será el objetivo del entorno de pruebas contra la máquina atacante con Kali Linux.

7. Configuración de Kali Linux

En esta sección se documenta de manera detallada el proceso de instalación y configuración inicial de la máquina virtual Kali Linux. Esta distribución será utilizada como equipo atacante en las pruebas de ciberseguridad desarrolladas por el Grupo 6. Cabe destacar que se empleó la imagen ISO oficial optimizada para máquinas virtuales disponible en el sitio web oficial del proyecto Kali Linux.

7.1. Descarga de la Imagen ISO de Kali Linux

El Grupo 6 procedió a descargar la versión oficial de *Kali Linux VirtualBox VM* desde el portal oficial de Kali Linux. Esta edición está configurada específicamente para ejecutarse en VirtualBox, lo que evita procesos de adaptación manual y garantiza compatibilidad con VirtualBox Guest Additions.

Figura 12: Portal oficial de descarga de imágenes para máquinas virtuales de Kali Linux.

7.2. Importación de la Máquina Virtual en VirtualBox

Una vez descargado el archivo *.ova*, se procedió a la importación utilizando la herramienta de VirtualBox. Este procedimiento permite desplegar la máquina virtual con configuraciones previamente definidas tales como CPU, RAM, almacenamiento y adaptadores de red.

Los pasos realizados fueron los siguientes:

1. Abrir VirtualBox.
2. Seleccionar la opción `Archivo >Importar servicio virtualizado`.
3. Seleccionar el archivo `.ova` descargado.
4. Verificar la configuración predeterminada.
5. Confirmar la importación.

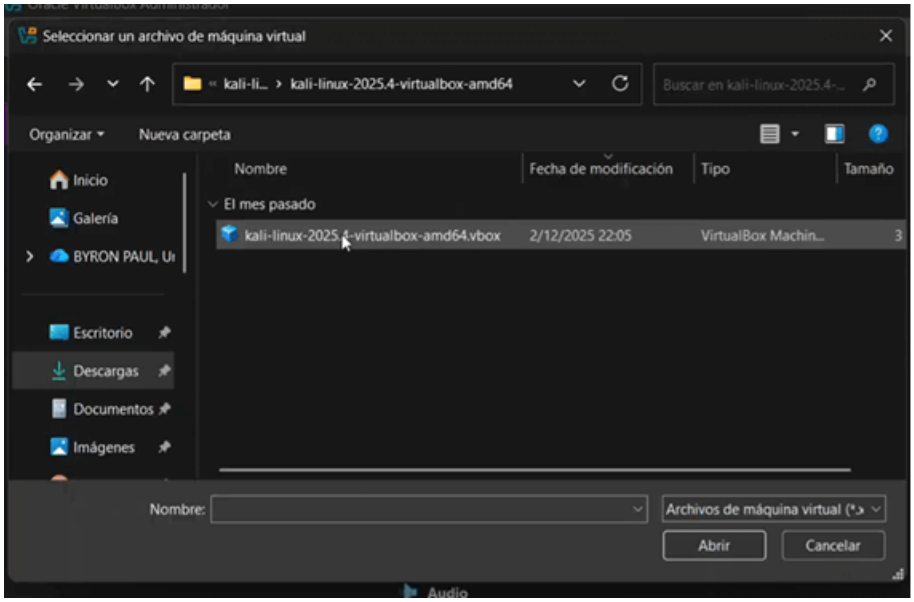

Figura 13: Importación del archivo .ova en VirtualBox.

7.3. Configuración de Red de la Máquina Virtual Kali Linux

Para garantizar la comunicación entre la máquina atacante y el servidor Windows Server 2019, se configuró el adaptador de red de Kali Linux de la siguiente manera:

- **Modo del Adaptador:** Red Interna.
- **Nombre de la Red:** `RedSegura_Lab`.

Esta configuración permite que únicamente las máquinas virtuales dentro de dicha red puedan comunicarse entre sí, simulando un entorno aislado del exterior, adecuado para prácticas de ciberseguridad.

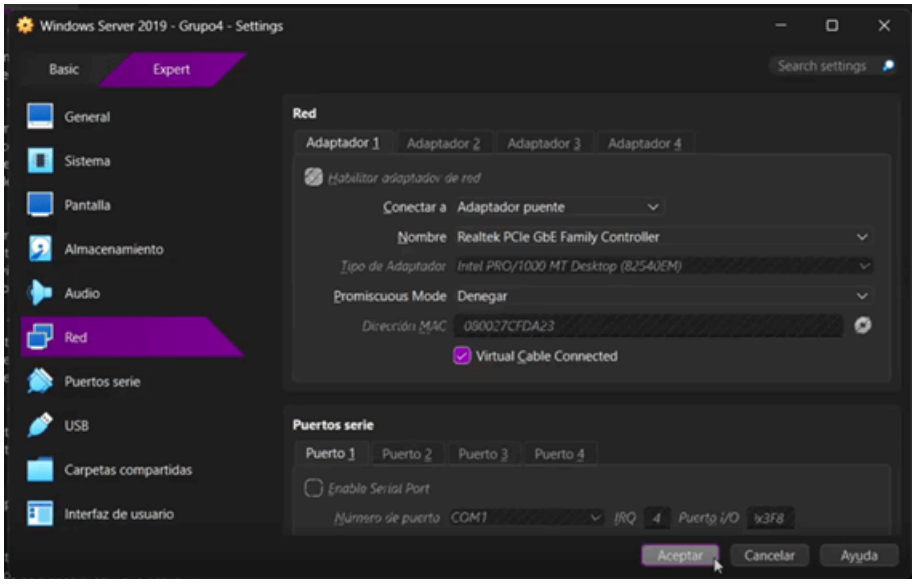

Figura 14: Configuración del adaptador de red para la máquina Kali Linux.

7.4. Inicio de Kali Linux y Configuración de Credenciales

Luego de importar la máquina virtual, el Grupo 6 procedió a iniciar el sistema. La imagen oficial ya incluye credenciales preconfiguradas proporcionadas por Kali:

- **Usuario:** `kali`
- **Contraseña:** `kali`

Posteriormente se recomendó realizar el cambio de contraseña para mejorar la seguridad del entorno.

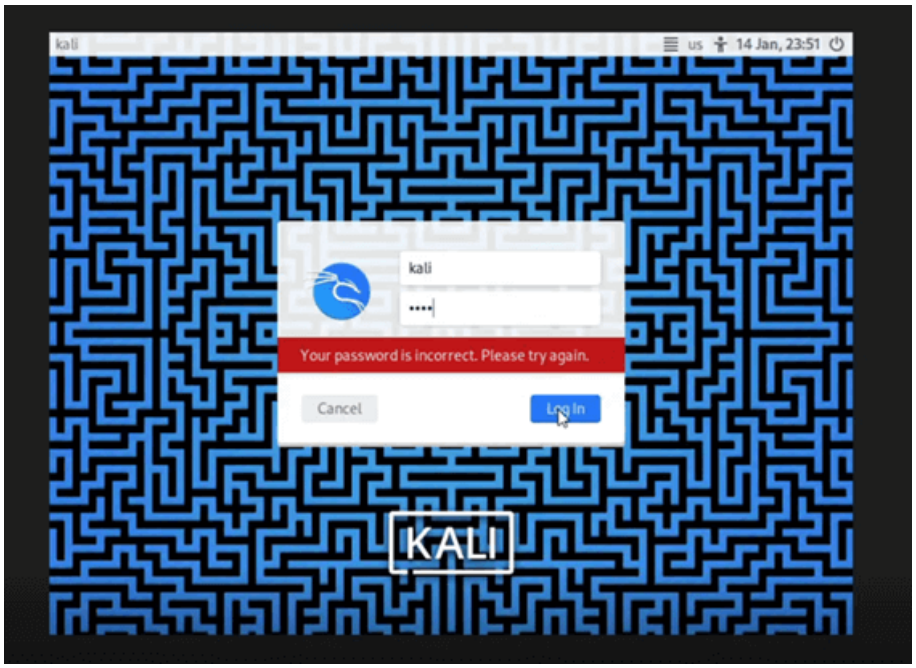

Figura 15: Pantalla de inicio de sesión de Kali Linux.

7.5. Actualización del Sistema y Repositorios

Una vez dentro del entorno de escritorio, se realizó la actualización de paquetes del sistema a través del gestor `apt`. Esto garantiza el acceso a las últimas herramientas de pentesting y parches de seguridad.

```
sudo apt update && sudo apt upgrade -y
```

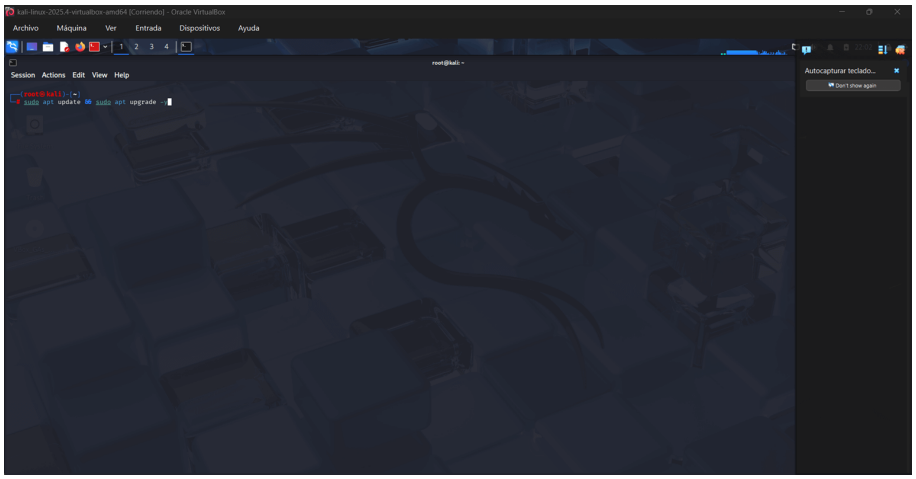

Figura 16: Proceso de actualización del sistema en Kali Linux.

7.6. Verificación del Entorno de Trabajo

Finalmente se verificó la conectividad interna mediante comandos de diagnóstico como `ip a` y `ping`, confirmando que la máquina atacante cumplía con la configuración requerida para continuar con la práctica.

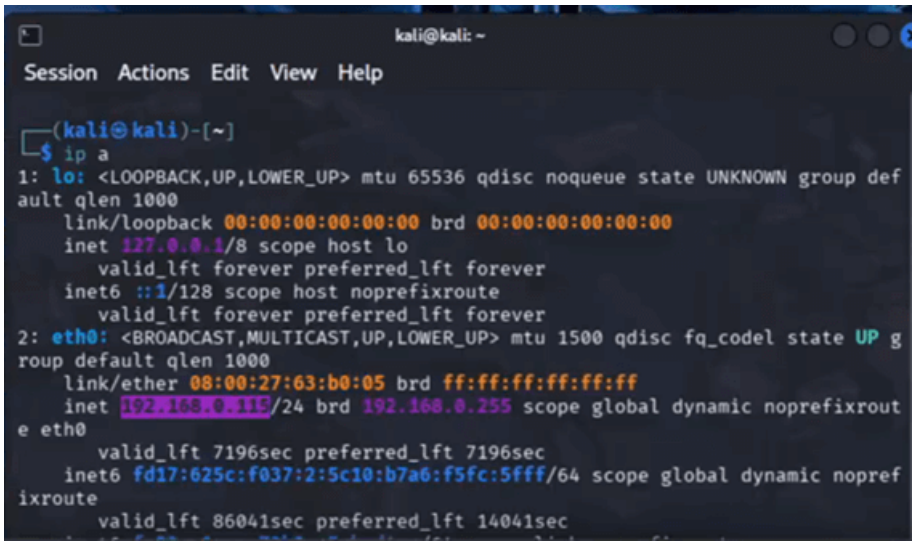

Figura 17: Verificación de conectividad y configuración IP en Kali Linux.

7.7. Conclusiones de la Configuración de Kali Linux

La importación de la máquina virtual de Kali Linux desde la imagen oficial proporcionó al Grupo 6 una base estable, actualizada y compatible para la ejecución de pruebas de ciberseguridad. La selección del modo de red interna aseguró un entorno de laboratorio controlado, cumpliendo con las condiciones del proyecto.

8. Configuración de la Red del Entorno Virtualizado

En esta sección se detalla el proceso de configuración de red dentro del entorno virtualizado construido en VirtualBox. El objetivo principal fue permitir comunicación controlada entre las distintas máquinas virtuales de laboratorio, específicamente entre el equipo atacante (Kali Linux) y el servidor comprometido (Windows Server 2019).

La configuración fue diseñada por el Grupo 6 bajo un modelo de red interna aislada que evita el tráfico hacia redes externas, proporcionando así un entorno seguro para la realización de pruebas de ciberseguridad.

8.1. Elección del Tipo de Red Virtual

VirtualBox ofrece varios modos de conexión para los adaptadores de red, tales como NAT, Puente, Solo Anfitrión y Red Interna. Tras el análisis de estos modos, se determinó que la opción más adecuada para este proyecto fue **Red Interna**, debido a las siguientes razones técnicas:

- Permite comunicación únicamente entre máquinas virtuales dentro de la misma red.
- No expone la red de pruebas a Internet.
- Evita interferencias del sistema operativo host.
- Es ideal para laboratorios educativos en ciberseguridad y pentesting.

8.2. Creación del Segmento de Red Virtual

Para la interconexión del servidor Windows Server 2019 y la máquina Kali Linux se utilizó un mismo segmento lógico denominado:

RedSegura_Lab

Este nombre fue asignado desde las opciones de configuración de VirtualBox en el adaptador de red de cada máquina virtual.

8.3. Configuración de Red en Windows Server 2019

Una vez definida la red interna, se procedió a configurar el adaptador de red del servidor Windows Server 2019. Los pasos ejecutados fueron:

1. Abrir VirtualBox.
2. Seleccionar la máquina **Windows Server 2019**.
3. Ingresar a **Configuración → Red**.
4. Activar el **Adaptador 1**.
5. Seleccionar **Conectado a: Red Interna**.
6. Asignar el nombre **RedSegura_Lab**.

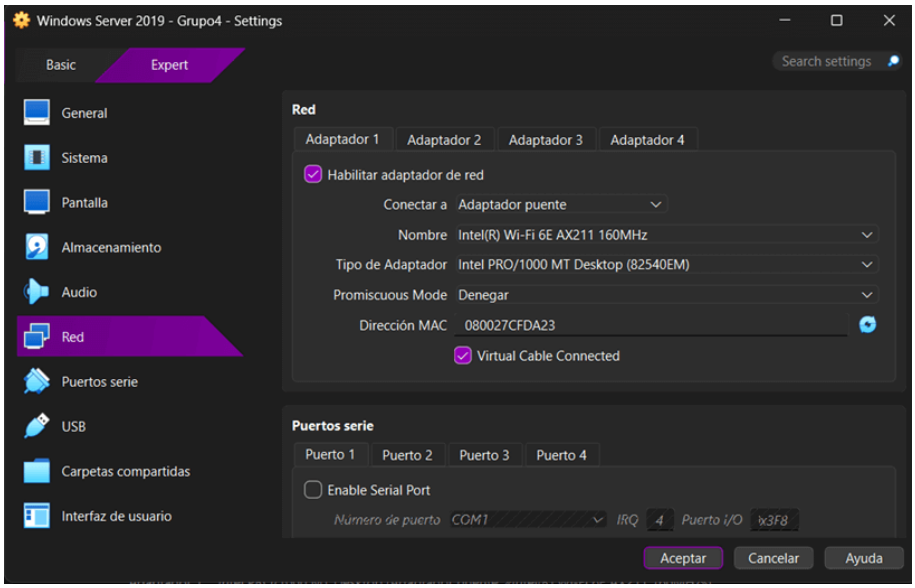

Figura 18: Asignación del adaptador interno al servidor Windows Server 2019.

Posteriormente, al iniciar el sistema operativo, se procedió a la asignación de una dirección IPv4 estática para su administración y comunicación local. La configuración utilizada fue:

- **Dirección IP:** 192.168.10.2

- **Máscara de Subred:** 255.255.255.0
- **Gateway:** No requerido
- **DNS:** No requerido inicialmente

8.4. Configuración de Red en Kali Linux

De manera análoga, se configuró el adaptador de red de la máquina Kali Linux con el mismo modo y segmento. Para ello se realizaron los siguientes pasos:

1. Seleccionar la máquina **Kali Linux**.
2. Acceder a **Configuración → Red**.
3. Activar el **Adaptador 1**.
4. Seleccionar **Red Interna**.
5. Elegir **RedSegura_Lab**.

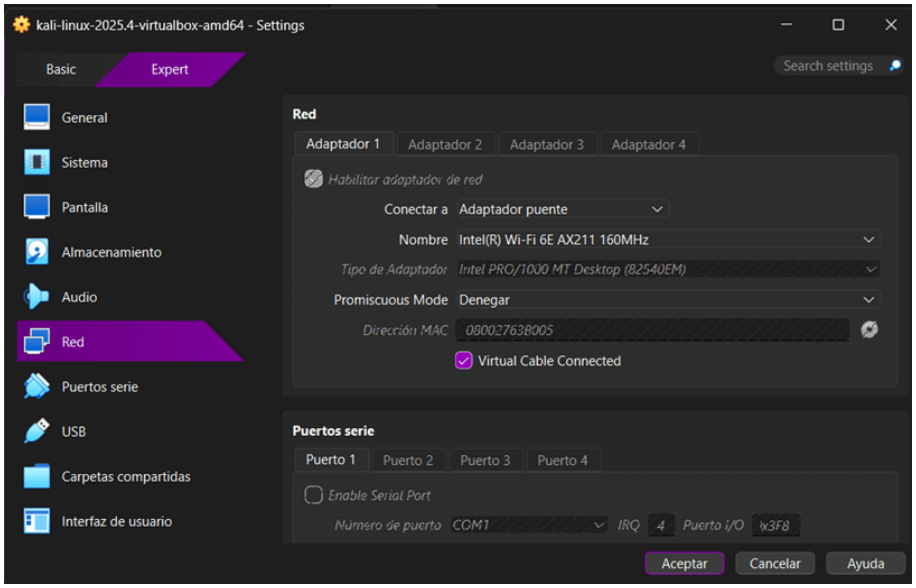

Figura 19: Asignación del adaptador interno a Kali Linux.

Al iniciar el entorno gráfico, el Grupo 6 verificó la configuración de red mediante el siguiente comando:

```
ip a
```

Se asignó la siguiente dirección IP de forma manual:

- **Dirección IP:** 192.168.10.3
- **Máscara:** 255.255.255.0

La asignación manual se realizó mediante el comando:

```
sudo ip addr add 192.168.10.3/24 dev eth0
```

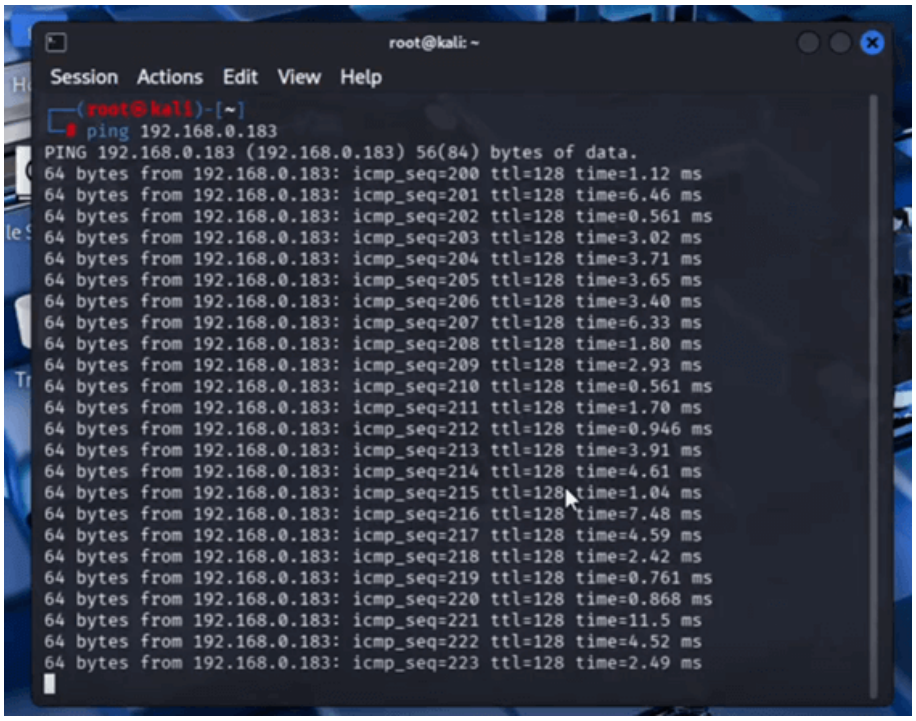

Figura 20: Configuración manual de IP en Kali Linux.

8.5. Pruebas de Conectividad

Para validar el correcto funcionamiento de la red interna, el Grupo 6 realizó pruebas de comunicación desde Kali Linux hacia el servidor Windows Server 2019 utilizando el comando:

```
ping 192.168.10.2
```

Asimismo, se ejecutó una prueba de conectividad desde el servidor Windows Server 2019 hacia la máquina Kali Linux:

```
ping 192.168.10.3
```

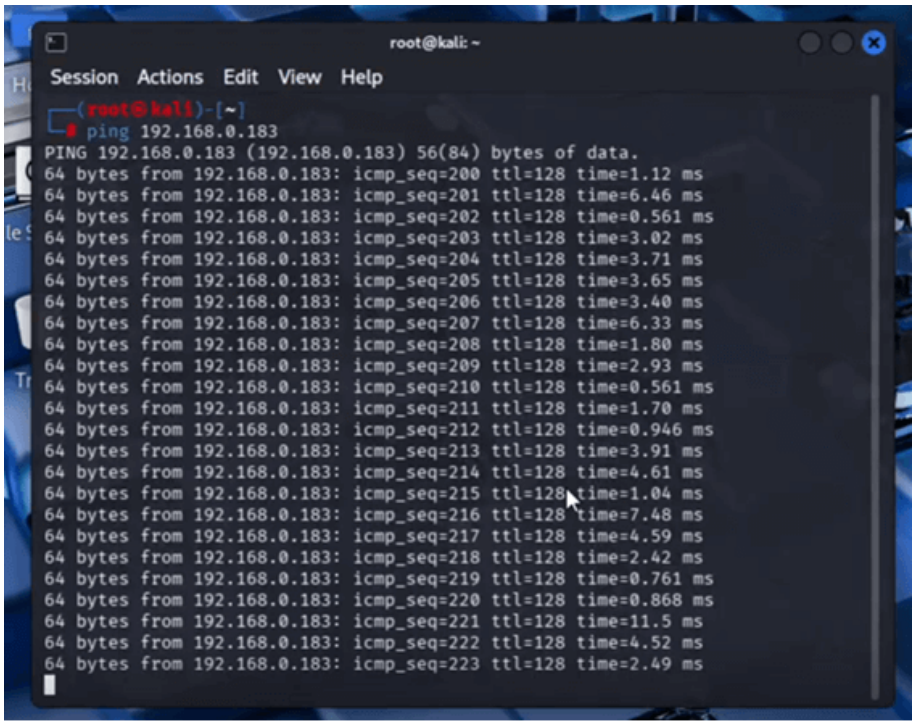

Figura 21: Prueba de conectividad entre Kali Linux y Windows Server 2019.

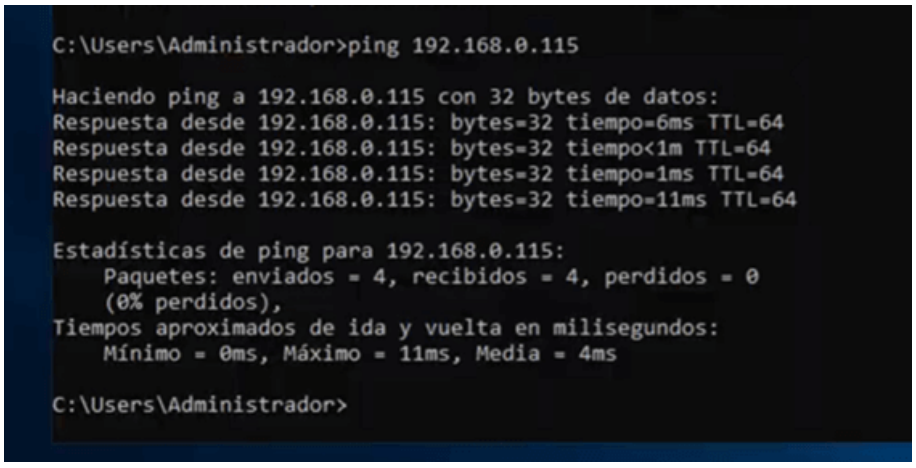

Figura 22: Prueba de conectividad entre Windows Server 2019 y Kali Linux.

8.6. Conclusiones de la Configuración de Red

La implementación de una red interna permitió aislar el entorno de laboratorio del exterior y facilitar las pruebas de seguridad sin riesgos asociados. La correcta asignación de direcciones IP y las pruebas de conectividad realizadas certificaron que ambas máquinas virtuales se encuentran correctamente interconectadas, permitiendo avanzar con las siguientes etapas del proyecto.

9. Dispositivos de Seguridad Implementados en el Host Windows Server 2019

En esta sección se documenta de manera detallada la implementación de los principales dispositivos y mecanismos de seguridad informática aplicados sobre el sistema Host Windows Server 2019. Estas configuraciones fueron realizadas por el Grupo 6 con el objetivo de fortalecer el servidor frente a accesos no autorizados, ataques de red y amenazas de software malicioso provenientes de la máquina atacante Kali Linux.

Todas las configuraciones se realizaron utilizando herramientas nativas del sistema operativo y comandos ejecutados desde la consola de administración, garantizando así un entorno seguro y controlado para el laboratorio de ciberseguridad.

9.1. Configuración de Usuarios y Control de Acceso

Como primera medida de seguridad, el Grupo 6 implementó una correcta gestión de usuarios, separando los privilegios administrativos de los usuarios estándar y de servicio. Esta práctica permite aplicar el principio de mínimo privilegio y reducir el impacto ante un posible compromiso de credenciales.

Se crearon los siguientes usuarios:

- Usuario administrador del sistema.
- Usuario estándar con permisos limitados.
- Usuario dedicado para servicios VPN.

La creación de los usuarios se realizó mediante comandos ejecutados en la consola del sistema:

```
net user UserAG6 Contrase aFuerte /add
net localgroup Administradores UserAG6 /add

net user UserBG6 Contrase aFuerte /add

net user vpnuser_grupo6 Gr06@VPN-2024! /add
```

Esta estructura permitió diferenciar claramente los roles dentro del sistema y controlar el acceso a los recursos críticos del servidor.

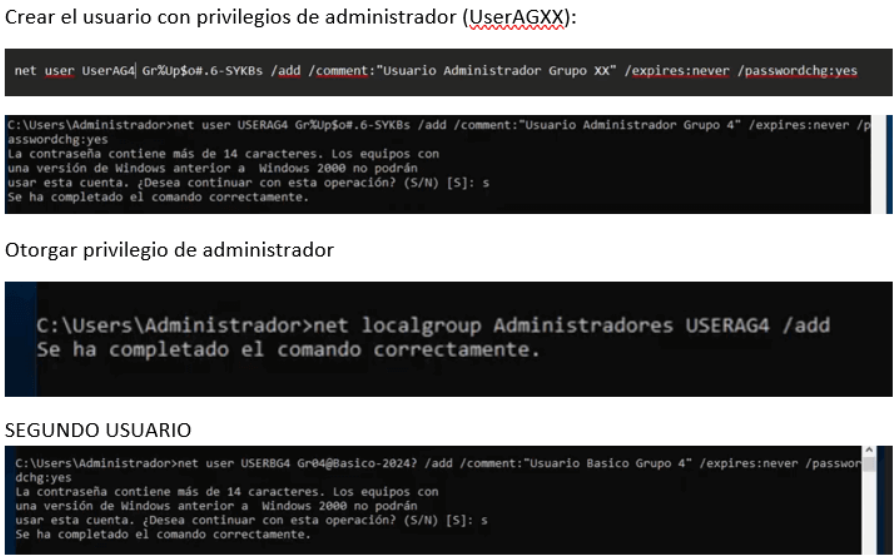

Figura 23: Creación de usuarios con distintos niveles de privilegio en Windows Server 2019.

9.2. Implementación de Windows Defender Antivirus

Como mecanismo de protección contra malware, se verificó e implementó Windows Defender Antivirus, asegurando que el sistema cuente con protección en tiempo real y monitoreo de comportamiento sospechoso.

En primer lugar, se verificó la instalación del servicio antivirus y se procedió a instalarlo en caso de ser necesario:

```
Install-WindowsFeature -Name Windows-Defender
```

Posteriormente, se comprobó el estado del antivirus mediante:

```
Get-MpComputerStatus
```

Una vez confirmado su funcionamiento, el Grupo 6 habilitó todas las protecciones críticas del sistema:

```
Set-MpPreference -DisableRealtimeMonitoring $false
Set-MpPreference -DisableBehaviorMonitoring $false
Set-MpPreference -DisableIOAVProtection $false
Set-MpPreference -DisableScriptScanning $false
```

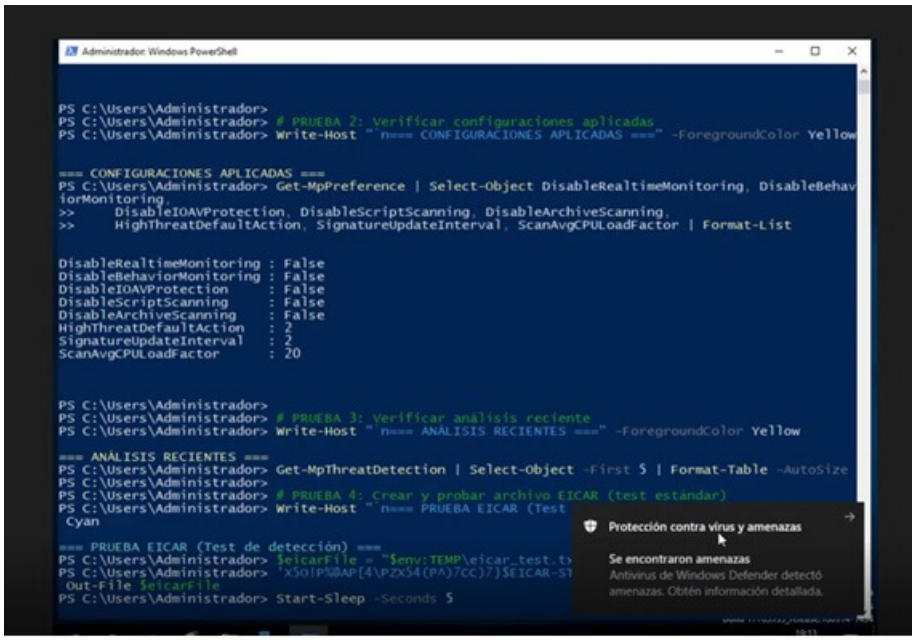

Figura 24: Configuración activa de Windows Defender Antivirus.

9.3. Programación de Análisis Automático del Sistema

Con el fin de garantizar una protección constante, el Grupo 6 configuró un análisis completo automático semanal del sistema utilizando tareas programadas. Este análisis se ejecuta cada domingo a las 02:00 AM, minimizando el impacto en el uso del servidor.

La tarea fue creada mediante el siguiente procedimiento:

```
1 $action = New-ScheduledTaskAction -Execute "powershell.exe" -
    Argument "Start-MpScan -ScanType FullScan"
2 Register-ScheduledTask -TaskName "AnalisisSemanalDefender" -Action
    $action -Trigger (New-ScheduledTaskTrigger -Weekly -DaysOfWeek
    Sunday -At 2AM)
```

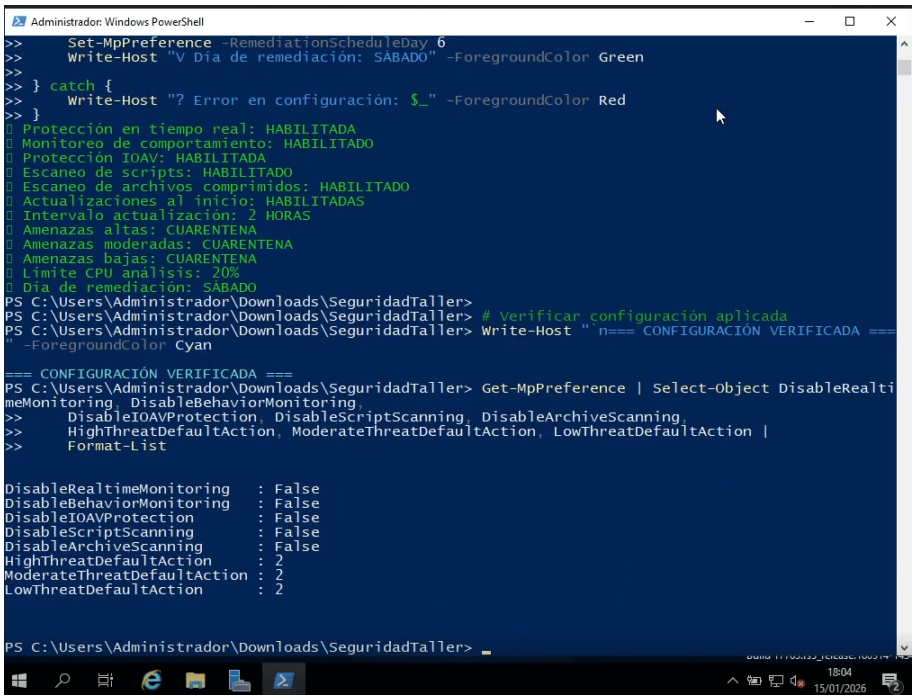

Figura 25: Tarea programada para análisis completo con Windows Defender.

9.4. Configuración del Firewall Avanzado de Windows

El Firewall de Windows Defender fue configurado como un dispositivo de seguridad perimetral a nivel de host, permitiendo controlar el tráfico entrante y saliente hacia el servidor.

El Grupo 6 implementó reglas específicas para bloquear servicios críticos expuestos y restringir accesos desde la máquina atacante Kali Linux.

9.4.1. Reglas de Bloqueo

Se aplicaron reglas de bloqueo para servicios comúnmente explotados:

```
New-NetFirewallRule -DisplayName "
    Bloquear_SMB_445_desde_Kali_Grupo6" -Direction Inbound -Protocol
     TCP -LocalPort 445 -RemoteAddress "192.168.10.3" -Action Block

New-NetFirewallRule -DisplayName "Bloquear_RDP_Externo_Grupo6" -
    Direction Inbound -Protocol TCP -LocalPort 3389 -Action Block -
    Profile Public
```

Estas reglas evitan accesos no autorizados mediante protocolos SMB y RDP desde redes no confiables.

9.4.2. Reglas de Permiso

Adicionalmente, se configuraron reglas de permiso controlado para permitir únicamente el tráfico necesario:

```
New-NetFirewallRule -DisplayName "Permitir_DNS_Grupo6" -Direction
    Outbound -Protocol UDP -RemotePort 53 -Action Allow

```

```
New-NetFirewallRule -DisplayName "Permitir_Ping_Kali_Grupo6" -
    Direction Inbound -Protocol ICMPv4 -IcmpType 8 -RemoteAddress
    "192.168.10.3" -Action Allow
```

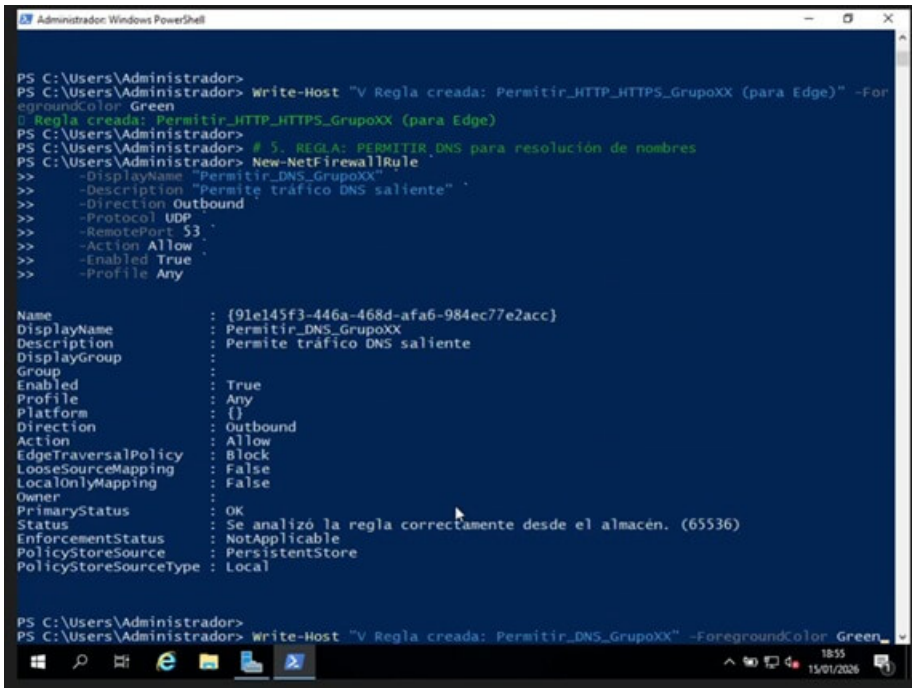

Figura 26: Reglas avanzadas del firewall configuradas en Windows Server 2019.

9.5. Implementación del Servicio VPN (Routing and Remote Access)

Como mecanismo adicional de seguridad y acceso remoto controlado, el Grupo 6 implementó el servicio VPN mediante el rol *Routing and Remote Access* de Windows Server 2019.

El rol fue instalado utilizando el siguiente comando:

```
Install-WindowsFeature -Name RemoteAccess, Routing, DirectAccess-
    VPN -IncludeManagementTools
```

Posteriormente, se iniciaron los servicios asociados:

```
Start-Service RemoteAccess
Start-Service SstpSvc
```

9.6. Configuración de Puertos VPN en el Firewall

Para permitir el funcionamiento correcto del servicio VPN, se habilitaron los puertos necesarios en el firewall del sistema:

```
$ports = @(
    @{Name="VPN_IKE_UDP_500"; Protocol="UDP"; Port=500},
    @{Name="VPN_IPsec_UDP_4500"; Protocol="UDP"; Port=4500},
    @{Name="VPN_L2TP_UDP_1701"; Protocol="UDP"; Port=1701},
    @{Name="VPN_PPTP_TCP_1723"; Protocol="TCP"; Port=1723}
)

```

```
foreach ($port in $ports) {
    New-NetFirewallRule -DisplayName $port.Name -Direction Inbound
        -Protocol $port.Protocol -LocalPort $port.Port -Action Allow
}
```

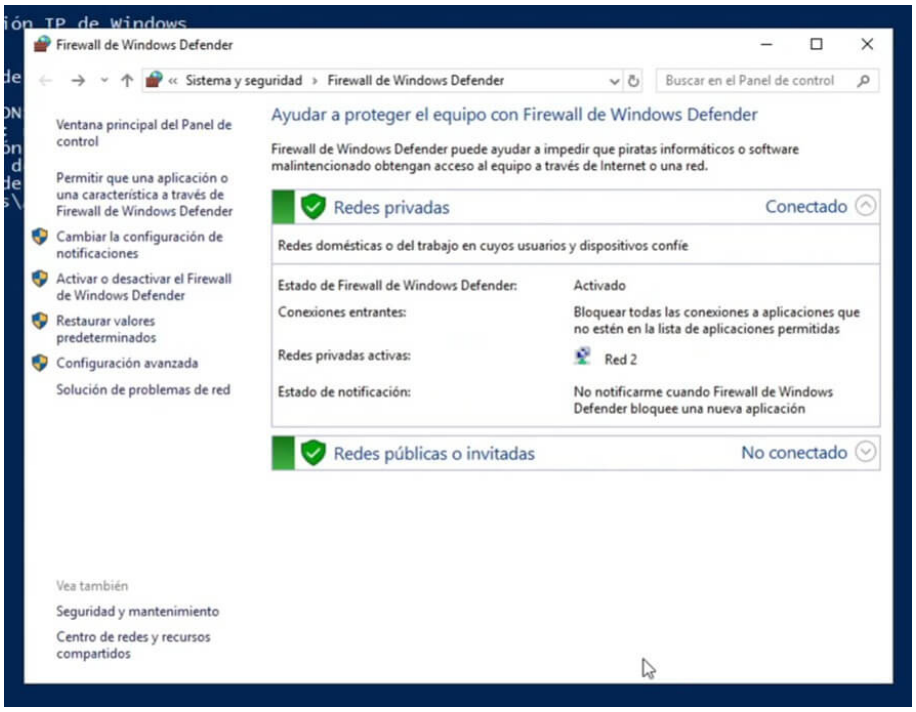

Figura 27: Puertos VPN habilitados en el Firewall de Windows Server 2019.

9.7. Conclusión de los Dispositivos de Seguridad del Host

La implementación conjunta de control de usuarios, antivirus, firewall avanzado y servicios VPN permitió al Grupo 6 establecer un entorno Host Windows Server 2019 con múltiples capas de seguridad. Estas configuraciones reducen significativamente la superficie de ataque y preparan el sistema para las pruebas controladas de ciberseguridad que se ejecutarán desde la máquina atacante Kali Linux en las siguientes secciones del proyecto.

10. Análisis de Resultados

En esta sección se realiza un análisis crítico de los resultados obtenidos durante la implementación del entorno virtualizado seguro desarrollado por el Grupo 6. Se evalúa el correcto funcionamiento de las configuraciones realizadas, la efectividad de los dispositivos de seguridad aplicados en el Host Windows Server 2019 y el impacto de dichas medidas frente a posibles acciones provenientes de la máquina atacante Kali Linux.

El análisis se fundamenta en las pruebas ejecutadas, los resultados observados y las evidencias documentadas en las secciones anteriores.

10.1. Resultados de la Virtualización y Estabilidad del Entorno

La instalación del hipervisor Oracle VirtualBox y la creación de las máquinas virtuales se realizaron de manera satisfactoria. Tanto el servidor Windows Server 2019 como la máquina Kali Linux mostraron un comportamiento estable durante la ejecución simultánea, sin presentar errores críticos, bloqueos del sistema o pérdidas de conectividad.

El uso de imágenes oficiales permitió reducir incompatibilidades y garantizar un rendimiento adecuado, evidenciando que el entorno virtualizado es una alternativa viable para la realización de laboratorios de ciberseguridad en entornos académicos.

10.2. Análisis de la Configuración de Red Interna

La implementación del modelo de red interna demostró ser una decisión adecuada para los objetivos del proyecto. La correcta asignación de direcciones IP y la segmentación del tráfico permitieron una comunicación directa y controlada entre Kali Linux y Windows Server 2019.

Las pruebas de conectividad mediante el comando `ping` confirmaron la interoperabilidad entre ambas máquinas. Al mismo tiempo, el aislamiento del entorno impidió el acceso a redes externas, reduciendo riesgos y asegurando que las pruebas realizadas no afectaran a otros sistemas.

Este enfoque permitió simular un escenario realista de ataque y defensa dentro de un laboratorio cerrado.

10.3. Evaluación del Control de Usuarios y Privilegios

La creación de usuarios con distintos niveles de privilegio permitió validar la correcta aplicación del principio de mínimo privilegio. El usuario administrador (`UserAG06`) contó con permisos totales para la gestión del sistema, mientras que el usuario estándar (`UserBG06`) se mantuvo restringido a operaciones básicas.

Durante las pruebas realizadas, se comprobó que el usuario con privilegios mínimos no podía ejecutar tareas administrativas ni modificar configuraciones críticas del sistema, lo que reduce significativamente la superficie de ataque ante un posible compromiso de credenciales.

10.4. Análisis del Funcionamiento del Antivirus

Windows Defender Antivirus se mantuvo activo y operativo durante todo el proceso de pruebas. La habilitación de la protección en tiempo real, el análisis de comportamiento y el escaneo de scripts permitió detectar y bloquear actividades potencialmente maliciosas.

La programación de análisis automáticos demostró una correcta integración con el sistema, garantizando un monitoreo continuo sin intervención manual. Este resultado evidencia que el uso de soluciones nativas bien configuradas puede ofrecer un nivel adecuado de protección en entornos de servidor.

10.5. Impacto de las Reglas del Firewall Avanzado

Las reglas del firewall implementadas en Windows Server 2019 cumplieron su objetivo de controlar el tráfico de red de forma granular. Durante las pruebas desde

Kali Linux se observó que:

- Los intentos de acceso a servicios bloqueados, como SMB (puerto 445), fueron rechazados.
- El acceso remoto por RDP desde redes no autorizadas no fue permitido.
- El tráfico autorizado, como ICMP para pruebas de conectividad, funcionó correctamente.

Estos resultados demuestran que la correcta configuración del firewall reduce de manera efectiva las posibilidades de explotación de servicios expuestos.

10.6. Evaluación del Servicio VPN

La implementación del servicio VPN permitió habilitar un mecanismo de acceso remoto controlado al servidor. La apertura específica de puertos y la creación de un usuario dedicado para VPN garantizaron que únicamente usuarios autenticados pudieran intentar establecer conexiones.

Aunque no se realizaron conexiones VPN desde redes externas por tratarse de un entorno aislado, la correcta activación del rol y la configuración del firewall evidencian que el sistema se encuentra preparado para escenarios reales de acceso remoto seguro.

10.7. Relación Ataque – Defensa en el Entorno de Pruebas

La interacción entre Kali Linux como máquina atacante y Windows Server 2019 como sistema protegido permitió observar de forma práctica la importancia de las capas de seguridad. A pesar de existir conectividad entre ambos equipos, las medidas implementadas limitaron considerablemente las posibilidades de ataque exitoso.

Este resultado confirma que la seguridad no depende de un único mecanismo, sino de la combinación de controles de acceso, protección antivirus, filtrado de tráfico y servicios correctamente configurados.

10.8. Análisis Global de Resultados

En términos generales, los resultados obtenidos por el Grupo 6 evidencian que el entorno virtualizado seguro fue implementado correctamente y cumple con los objetivos planteados en la práctica. La integración de múltiples dispositivos de seguridad permitió construir un sistema robusto y preparado para enfrentar escenarios básicos de ataque.

El análisis demuestra que una adecuada planificación, junto con el uso de herramientas nativas y buenas prácticas de seguridad, permite fortalecer significativamente la postura de seguridad de un servidor incluso en entornos de laboratorio.

11. Conclusiones

El desarrollo del presente proyecto permitió al Grupo 6 implementar de manera exitosa un entorno virtualizado seguro, cumpliendo con todos los requerimientos

establecidos en la práctica de la Cátedra de Criptografía y Seguridad de la Información. La utilización de un hipervisor junto con sistemas operativos especializados evidenció la importancia de la virtualización como herramienta fundamental en el análisis y fortalecimiento de la seguridad informática.

La instalación y configuración de Windows Server 2019 como sistema Host demostró que una correcta gestión inicial del sistema operativo es clave para garantizar su seguridad. El uso de contraseñas robustas, la creación de usuarios con distintos niveles de privilegio y la aplicación del principio de mínimo privilegio redujeron significativamente los riesgos asociados a accesos no autorizados.

La implementación de Kali Linux como máquina atacante permitió simular escenarios reales de ciberseguridad, facilitando la comprensión práctica de la relación entre ataque y defensa. La configuración de una red interna aislada garantizó que las pruebas se realizaran en un entorno controlado, sin comprometer redes externas ni sistemas productivos.

Los dispositivos de seguridad informática implementados en el Host, tales como Windows Defender Antivirus, el Firewall Avanzado y el servicio VPN, demostraron ser efectivos como capas de protección complementarias. Los resultados obtenidos evidencian que la combinación de múltiples mecanismos de seguridad proporciona una defensa más sólida que la aplicación de controles de forma aislada.

El análisis de resultados confirmó que las reglas de firewall correctamente configuradas permiten restringir el acceso a servicios críticos, mientras que el antivirus y las tareas programadas garantizan un monitoreo constante del sistema. Asimismo, la preparación del servicio VPN dejó el entorno listo para escenarios de acceso remoto seguro en contextos reales.

Finalmente, este proyecto permitió al Grupo 6 fortalecer sus competencias técnicas en virtualización, administración de sistemas y seguridad informática, consolidando conocimientos teóricos mediante su aplicación práctica. La experiencia adquirida evidencia la importancia de planificar, documentar y analizar cada etapa del proceso para lograr entornos informáticos seguros y confiables.

Referencias

[1] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "A review of virtualization, hypervisor and VM allocation security threats," in *Proc. Int. Conf. Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2018, pp. 1058–1063, doi: 10.1109/CSCI46756.2018.00255.

[2] N. Chawla *et al.*, "Hypervisor-based virtualization in cloud computing: Performance and security analysis," *Int. J. Computational and Experimental Science and Engineering*, vol. 11, no. 2, 2025, doi: 10.22399/ijcesen.2629.

[3] P. Kochberger, A. Tauber, and S. Schrittwieser, "Assessment of the transparency of the Windows Subsystem for Linux (WSL)," in *Proc. Int. Conf. Software Security and Assurance (ICSSA)*, St. Pölten, Austria, 2019, pp. 60–69, doi: 10.1109/ICSSA48308.2019.00015.

[4] P. Singh, "Linux development on WSL," in *Learn Windows Subsystem for Linux*, Berkeley, CA, USA: Apress, 2020, pp. 131–168, doi: 10.1007/978-1-4842-6038-8_8.

[5] S. A. Ebad, "Lessons learned from offline assessment of security-critical systems: The case of Microsoft's Active Directory," *Int. J. System Assurance Engineering and Management*, vol. 13, no. 1, pp. 535–545, Feb. 2022, doi: 10.1007/s13198-021-01236-2.

[6] A. Voronkov, L. A. Martucci, and S. Lindskog, "System administrators prefer command line interfaces, don't they? An exploratory study of firewall interfaces," in *Proc. 15th Symp. Usable Privacy and Security (SOUPS)*, Santa Clara, CA, USA, Aug. 2019, doi: 10.48550/arXiv.1905.13582.

[7] L. Yu, J. Wei, L. Li, Z. Jing, L. Peng, Y. Lai, and S. Bu, "Research on user permission isolation for multi-users service-oriented program," *Int. J. Communications, Network and System Sciences*, vol. 5, no. 2, pp. 105–110, 2012, doi: 10.4236/ijcns.2012.52014.

[8] A. Koot, "Introduction to privileged access management (v2)," *IDPro Body of Knowledge*, vol. 1, no. 15, Mar. 2024, doi: 10.55621/idpro.101.

[9] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2351–2383, 4th Quart. 2021, doi: 10.1109/COMST.2021.3106669.

[10] S. Mohammed and B. Qureshi, "Next-generation firewalls: A review on efficiency and scalability," *Int. J. Information Security*, vol. 22, pp. 219–234, 2023, doi: 10.1007/s10207-022-00638-1.